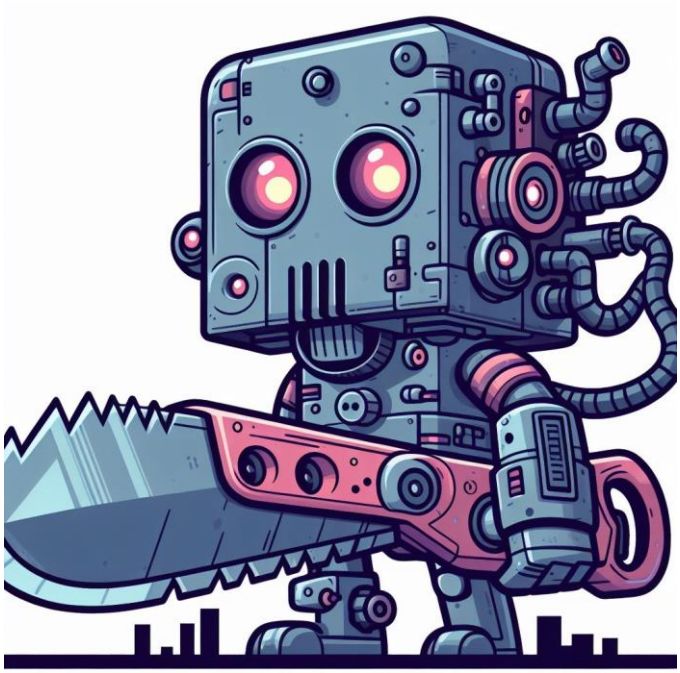

Abstract – This document presents an analysis of the "Infamous Chisel" malware, a sophisticated cyber threat attributed to the Sandworm group. The analysis delves into various aspects of the malware, including its capabilities, components, and the implications of its deployment against specific targets, notably Android devices.

By dissecting the malware's components and tactics, the document sheds light on the sophisticated nature of cyber threats and their potential to compromise sensitive information and disrupt operations. The findings underscore the critical need for vigilance and proactive defense measures in the face of such advanced threats.

For cybersecurity professionals and other specialists across various sectors, this analysis serves as a valuable resource for understanding the mechanics and implications of advanced malware threats like Infamous Chisel. The document's insights can inform the development of more effective defense strategies and technologies, enhancing the security posture of organizations and protecting against the ever-evolving landscape of cyber threats.

I. INTRODUCTION

The Chisel malware targets Android devices, enabling remote access and exfiltrating information from these devices. Sandworm has used this malware in a campaign targeting Android devices used by the military sector. The malware is a collection of components that enable persistent access to an infected Android device over the Tor network and periodically collates and exfiltrates victim information from compromised devices. The information exfiltrated includes system device information, commercial application information, and applications specific to the military sector.

II. COMPONENTS OF INFAMOUS CHISEL

Infamous Chisel is a collection of components associated with Sandworm, designed to enable remote access and exfiltrate information from Android phones.

The components of Infamous Chisel include:

- **netd**: This component is used to perform automated device information collection and exfiltration. It also searches multiple directories for files matching a predefined set of extensions which are then exfiltrated.
- **killer**: This component kills the malicious netd process.
- **blob**: This component is executed by netd and is responsible for configuring and executing the Tor utility td.
- **td**: This utility is Tor with no obvious modifications.
- **tcpdump**: This utility is tcpdump with no obvious modifications.
- **ndbr_armv7l and ndbr_i686**: These utilities are multi-call containing: dropbear, dropbearkey, ssh, scp, nmap, dbclient, watchdog, rmflag, mkflag.
- **db**: This utility is multi-call containing: dropbear, dropbearkey, ssh, scp, nmap, dbclient, watchdog, rmflag, mkflag.

III. NETWORK AND OTHER FEATURES

Infamous Chisel is designed to persist on the system by replacing the legitimate netd system binary at the path /system/bin/netd. When the malicious netd is executed, it will check if init is the parent process which executed it. This parent process is responsible for creating the processes listed in the script init.rc. The malicious replacement netd when executed in this way will fork and execute the legitimate process backed up at the path /system/bin/netd_ passing through the command line parameters. This retains the normal functionality of netd, while allowing the malicious netd to execute as root.

The netd component of Infamous Chisel provides the bulk of the custom functionality which the actor deploys. The main purpose of netd is to collate and exfiltrate information from the compromised device at set intervals. It uses a combination of shell scripts and commands to collect device information. It also searches multiple directories to which files matching a predefined set of extensions are exfiltrated.

Infamous Chisel has several other capabilities:

- **Network Monitoring and Traffic Collection**: Infamous Chisel can monitor network activity and collect network traffic data. This allows it to gather information about the network environment and potentially capture sensitive data transmitted over the network
- **SSH Access**: Infamous Chisel can establish SSH connections, which can be used for remote command execution and data transfer
- **Network Scanning**: The malware can scan the local network, collating information about active hosts, open ports, and banners. This can help identify other potential targets within the network

- **SCP File Transfer**: Infamous Chisel can use the Secure Copy Protocol (SCP) for file transfers. This can be used to exfiltrate data from the infected device or to transfer malicious files onto the device
- **Information Exfiltration**: Infamous Chisel performs periodic scanning of files and network information for exfiltration. System and application configuration files are exfiltrated from an infected device
- **Device Information Collection**: Infamous Chisel collects various system device information, commercial application information, and applications specific to the military sector
- **Automated Exfiltration**: Infamous Chisel automatically exfiltrates files at regular intervals
- **Service Stop**: Infamous Chisel can stop the legitimate netd service

IV. Exploited Vulnerabilities

The Infamous Chisel campaign exploits a variety of vulnerabilities and techniques to enable unauthorized access and control over targeted Android devices. the Infamous Chisel campaign exploits a combination of system vulnerabilities, insecure configurations, and network protocols to achieve its objectives. These include gaining persistence and elevated privileges, evading detection, accessing credentials, collecting sensitive information, establishing covert command and control channels, and potentially moving laterally within the network.

The primary vulnerabilities and techniques exploited by Infamous Chisel include (without specific CVE):

- **Persistence and Privilege Escalation**: Infamous Chisel achieves persistence on the infected device by replacing the legitimate netd system binary. This replacement allows the malicious netd to execute as root, thereby gaining elevated privileges.
- **Defense Evasion**: The malware employs several defense evasion techniques. For instance, it checks that it is executed by init and at the path for the legitimate netd, ensuring its malicious activities are less likely to be detected. Additionally, the blob component decompresses executables from bzip archives, which could be a method to evade detection by unpacking its payload only after it has bypassed initial security checks.
- **Credential Access**: Infamous Chisel uses the tcpdump utility to sniff network interfaces and monitor network traffic, potentially capturing credentials transmitted over the network. It also scrapes multiple files containing credentials and key information, exploiting the storage and handling of sensitive information on the device to gain unauthorized access to accounts and services.
- **Discovery and Collection**: The malware performs extensive discovery and collection activities, such as enumerating data directories to discover files of interest, collecting GPS information, listing installed packages, and gathering various system information. This indicates that Infamous Chisel exploits the lack of secure storage and inadequate permissions settings on the device to access and collect sensitive information.
- **Command and Control (C2) and Exfiltration**: Infamous Chisel configures and executes Tor with a hidden service, which forwards to a modified Dropbear binary providing an SSH connection. This setup allows the malware to establish a covert communication channel with the infected device, exploiting network protocols and services to maintain control over the device and exfiltrate collected data.
- **Network Scanning and Lateral Movement**: The malware contains functionality to scan the local network, collating information about active hosts, open ports, and banners. This capability suggests that Infamous Chisel exploits the network environment of the infected device to identify other potential targets within the network for lateral movement or further exploitation

V. Infiltration

The Infamous Chisel campaign exfiltrates information from infected Android devices through a series of automated and manual processes. The malware, associated with the Sandworm threat actor, performs periodic scanning of files and network information for exfiltration. It searches for files matching a predefined set of extensions and exfiltrates system and application configuration files from the infected device.

The exfiltration process is detailed as follows:

- **File Hashing and Avoiding Duplication**: When a file is selected for exfiltration, it is hashed using MD5 and cross-referenced with a list of previously sent file hashes held in a file at one of three locations supporting different Android versions. This ensures that the same file isn't sent multiple times.
- **File exfiltration from data directories**: The malware searches specified directories for files with certain extensions and exfiltrates them.
- **Exfiltration of configuration and configuration backup files**: The malware searches for .json or .json.bak files in specified directories and exfiltrates them.
- **File Exfiltration**: The malware exfiltrates files using a HTTP POST request. The server response is expected to be HTTP, and the exfiltration is considered complete when the server sends 'Success' anywhere in its response.
- **Information Gathering and Exfiltration**: Infamous Chisel collects various hardware configuration information about the device and writes this information to files in the /data/local directory, which are then exfiltrated. This includes the Android ID, networking information, a list of installed applications, and various device hardware information.
- **Local Area Network Scanning**: The malware includes a built-in network scanner that performs IP

scanning of the local network to discover other devices. The results of this scan are exfiltrated immediately, providing the attackers with information that could facilitate lateral movement within the network.

- **Exfiltration Frequency**: The malware is designed to automatically exfiltrate files at regular intervals, with specific intervals set for different types of data collection. For example, file and device information compilation takes place every 23 hours and 53 minutes, while sensitive military information is siphoned every 10 minutes.
- **Use of Tor and SSH for Secure Exfiltration**: Infamous Chisel uses Tor and SSH for command and control communications, providing an encrypted channel that can be difficult to detect and intercept. This setup allows the malware to maintain a covert communication channel with the infected device, making detection and mitigation more challenging

When a file is selected for exfiltration, it is MD5-hashed and cross-referenced with a list of previously sent file hashes held in a file at one of three locations supporting different Android versions. The first existing directory path will be used: /sdcard/Android/data/.google.index, /storage/emulated/0/Android/data/.google.index, or /storage/emulated/1/Android/data/.google.index.

The file exfiltration is considered complete when the server sends "Success" anywhere in its response. This exfiltration uses a Hypertext Transfer Protocol (HTTP) POST, and this server response is also expected to be HTTP, but this is not explicitly checked for. The 16 raw bytes of the MD5 are appended to the end of the .google.index file, ensuring that the same file isn't sent multiple times. As the .google.index file contains raw bytes, without prior knowledge, it would appear to contain random data. The initial allocation size is 256 Kb filled with NULLs providing space for up to a maximum of 16,384 file hashes. All hash entries will be checked for every file prior to exfiltration. When the end of the .google.index file is reached, the position is reset to the start, overwriting the previous hashes. This means if the number of files to exfiltrate from the device exceeds 16,384, files will be sent multiple times

The netd component of Infamous Chisel enters a main loop upon execution, where various timers trigger the execution of different tasks, including file and device information exfiltration. This process occurs every 86,000 seconds (approximately 23 hours, 53 minutes, and 20 seconds), during which the malware searches specified directories for files matching a list of extensions and collects various hardware configuration information about the device. The collected information is written to files in the /data/local directory and then exfiltrated.

VI. Impact & Geo scope

The impact of Infamous Chisel on Android devices is significant. It leads to loss of sensitive information, privacy breaches, and potential misuse of the device for further malicious activities.

The Infamous Chisel campaign primarily targeted Android devices used by the military sector. The malware, associated with the Sandworm activity, was designed to enable remote access and exfiltrate information from these devices. The campaign was identified and reported by multiple organizations including the UK National Cyber Security Centre (NCSC), the US National Security Agency (NSA), US Cybersecurity and Infrastructure Security Agency (CISA), US Federal Bureau of Investigation (FBI), New Zealand's National Cyber Security Centre (NCSC-NZ), the Canadian Centre for Cyber Security, and Australian Signals Directorate (ASD).

VII. Infecting ways

Based on the capabilities and methods of operation described in the document, we can infer some potential infection vectors that such a sophisticated malware campaign use:

- **Phishing Attacks**: Attackers may use phishing techniques to trick users into installing malicious applications or clicking on links that lead to the download of the malware.
- **Exploiting Vulnerabilities**: The malware may exploit known vulnerabilities in the Android operating system or in installed applications to gain unauthorized access and install itself.
- **Social Engineering**: Social engineering tactics could be used to convince users to grant permissions or disable security features that would otherwise prevent the malware from executing or gaining persistence.
- **Third-Party App Stores**: Infamous Chisel could be distributed through third-party app stores or websites offering infected applications that appear legitimate.
- **Malvertising**: Malicious advertisements could redirect users to websites that automatically download and install the malware on their devices.
- **Spear Phishing**: Targeted spear-phishing campaigns could be used to infect devices of specific individuals or organizations with the malware.
- **Supply Chain Attack**: Compromising software supply chains to inject malicious code into legitimate applications could be another method, although this is a more sophisticated and less common approach.

VIII. Proactive and Reactive measures

The approach to defending against such sophisticated malware campaigns typically involves a combination of proactive and reactive cybersecurity practices. It is important for organizations to adopt a layered security approach that includes both preventive and detective controls to protect against sophisticated malware campaigns. Additionally, staying informed about the latest cyber threats and collaborating with cybersecurity agencies and industry partners can enhance an organization's ability to defend against such threats

Proactive measures include:

- **Cybersecurity Awareness and Training**: Educating employees about the risks of malware and the

importance of following security best practices, such as not clicking on suspicious links or downloading unverified attachments.

- **Regular Software Updates**: Ensuring that all software, including operating systems and applications, are kept up-to-date with the latest security patches to mitigate known vulnerabilities.
- **Robust Anti-Virus and Anti-Malware Solutions**: Deploying comprehensive anti-virus and anti-malware solutions that can detect and prevent the execution of malicious code on organizational devices.
- **Network Security**: Implementing network security measures such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and control incoming and outgoing network traffic based on an applied rule set.
- **Access Controls**: Enforcing strict access controls and using the principle of least privilege to ensure that users have only the access necessary to perform their job functions.
- **Incident Response Planning**: Developing and maintaining an incident response plan to quickly and effectively respond to potential security incidents.

Reactive measures include:

- **Threat Intelligence Sharing**: Participating in threat intelligence sharing with other organizations and cybersecurity agencies to stay informed about the latest threats and mitigation strategies.
- **Monitoring and Detection**: Continuously monitoring systems for signs of compromise and having detection mechanisms in place to alert on suspicious activities.
- **Forensic Analysis**: Conducting forensic analysis in the event of a security breach to understand the scope of the compromise, eradicate the threat, and recover affected systems.
- **Regular Security Audits**: Performing regular security audits and vulnerability assessments to identify and address security gaps in the organization's infrastructure.
- **Backup and Recovery**: Maintaining regular backups of critical data and having a disaster recovery plan to restore operations in the event of a malware attack.

Android Device measures:

- **Keep Software Updated**: Regularly update the Android operating system and all installed applications to ensure that known vulnerabilities are patched. Malware often exploits security flaws in outdated software.
- **Install Security Software**: Use reputable antivirus and anti-malware solutions designed for Android devices. These can help detect and remove malicious software.
- **Avoid Unknown Sources**: Disable the installation of apps from unknown sources in the device settings. Only download apps from trusted sources like the Google Play Store.
- **Be Cautious with Links and Attachments**: Do not click on links or download attachments from unknown or suspicious sources. Phishing is a common method used to distribute malware.
- **Use a VPN**: When connecting to public Wi-Fi networks, use a Virtual Private Network (VPN) to encrypt your internet connection and protect against network sniffing.
- **Enable Two-Factor Authentication (2FA)**: Use 2FA for online accounts to add an extra layer of security, making it harder for attackers to gain access even if they manage to steal credentials.
- **Monitor Network Traffic**: For organizations, monitoring network traffic for unusual activity can help detect the presence of malware like Infamous Chisel. Implement network segmentation to limit the spread of malware.
- **Educate Users**: Raise awareness among users about the risks of malware and the importance of following best security practices.
- **Backup Important Data**: Regularly backup important data stored on the device. In case of a malware infection, having backups can prevent data loss.
- **Use Device Encryption**: Enable device encryption to protect the data on your device. This makes it more difficult for attackers to access your information if the device is compromised.
- **Restrict App Permissions**: Review and restrict the permissions granted to applications. Limiting permissions can reduce the amount of data an app can access, thereby limiting what can be exfiltrated by malware.