AL2024_11 New Medusa Malware Variants Target Android Users in Seven Countries (26th June 2024)

Description

New variants of the Medusa malware have been identified, specifically targeting Android users across seven countries. This development underscores the ongoing efforts by threat actors to expand their reach and enhance their attack strategies against mobile platforms.

Details

The latest versions of Medusa were detected in early June 2024. Medusa is a sophisticated malware with capabilities such as credential theft, keylogging, screen capturing, and remote control functionalities. According to Vumetric Cybersecurity, these new variants show significant advancements in evasion techniques and are designed to bypass traditional security measures on Android devices. The malware's spread has been noted in countries including the United States, Canada, Germany, France, Australia, India, and Brazil.

BleepingComputer reported that the Medusa attack chain begins with phishing campaigns that distribute malicious APK files. These files are often disguised as legitimate applications or updates. Once installed, the malware can access sensitive information, intercept communications, and manipulate device functions. The new variants also exploit vulnerabilities in older versions of the Android operating system, making it crucial for users to keep their devices updated.

Version 2024 of Medusa includes new features such as enhanced obfuscation techniques, improved command-and-control (C2) infrastructure, and capabilities to disable security applications. These improvements make detection and removal more challenging, posing a significant risk to affected users.

Indicators of Compromise (IoCs)

Organizations should monitor for the following indicators of compromise:

- Installation of unexpected or unfamiliar APK files.
- Phishing emails or messages prompting users to download software or updates.
- Unusual network traffic patterns connecting to known Medusa C2 servers.
- Reports of unauthorized access or suspicious activity on Android devices.

Remediation

To mitigate the risk posed by Medusa, organizations can:

- Implement robust mobile security solutions to detect and block malicious APKs.
- Regularly update Android devices to the latest operating system versions.
- Educate users about the dangers of phishing and the importance of downloading apps only from trusted sources.
- Monitor network traffic for unusual patterns that may indicate C2 communications.
- Apply patches for known vulnerabilities and ensure security applications are up to date.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- BleepingComputer. (2024, June 25). New Medusa Malware Variants Target Android Users in Seven Countries. Retrieved from https://www.bleepingcomputer.com/news/security/new-medusa-malware-variants-target-android-users-in-seven-countries/
- Vumetric Cybersecurity. (2024, June 25). New Medusa Malware Variants Target Android Users in Seven Countries. Retrieved from https://cyber.vumetric.com/security-news/2024/06/25/new-medusa-malware-variants-target-android-users-in-seven-countries/