CIRT.GY Guyana National Computer Incident Response Team

AL2024_12 Snowblind Malware Abuses Android Security Feature to Bypass Security (26th June 2024)

Description

A new malware known as Snowblind has been identified, exploiting an Android security feature to bypass existing anti-tampering protections in apps handling sensitive user data. This malware's novel attack vector poses a significant threat to Android users by allowing malicious actions to be performed undetected.

Details

Snowblind has been observed abusing 'seccomp' (secure computing), a Linux kernel feature integrated into Android for application integrity checks. This feature is intended to reduce the attack surface by filtering system calls (syscalls) that applications can make. However, Snowblind repackages target apps to avoid detection of its abuse of accessibility services, gaining access to user inputs such as credentials and enabling remote control to perform malicious activities.

Promon, a mobile app security company, analyzed Snowblind after receiving a sample from i-Sprint, a partner company providing access and identity system protections. Their findings revealed that Snowblind injects a native library into target apps, installing a seccomp filter that intercepts syscalls like 'open()' used for file access. This interception prevents the anti-tampering code from detecting the malware, making the attack invisible to users.

Promon demonstrated that Snowblind can disable various app security features, including two-factor authentication and biometric verification. The malware can read sensitive information, navigate the device, control apps, and exfiltrate personally identifiable information and transaction data. This sophisticated technique is not widely known and could be adopted by other adversaries to bypass Android protections.

Indicators of Compromise (IoCs)

Organizations should monitor for the following indicators of compromise:

- Unexpected behavior or performance issues in Android apps handling sensitive data.
- Unusual system call patterns or syscalls being intercepted.
- Reports of unauthorized access or suspicious activities within Android apps.
- Phishing emails or messages prompting users to download malicious APK files

Remediation

To mitigate the risk posed by DarkGate, organizations can:

- Implement robust mobile security solutions to detect and block malicious activities.
- 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 malicious activity.
- Ensure security applications and anti-tampering measures are up to date and properly configured.

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

References

- BleepingComputer. (2024, June 26). Snowblind malware abuses Android security feature to bypass security. Retrieved from https://www.bleepingcomputer.com/news/security/snowblind-malware-abuses-android-security-feature-to-bypass-security/
- DarkReading. (2024, June 26). Snowblind tampering technique may drive Android users adrift. Retrieved from https://www.darkreading.com/remote-workforce/snowblind-tampering-technique-may-drive-android-users-adrift