مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Emerging Threat of FakeCall Malware

Tracking #:432316466

Date:04-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new variant of the FakeCall malware has been identified, posing a significant threat to Android users.

TECHNICAL DETAILS:

A new variant of the FakeCall malware has been identified, posing a significant threat to Android users. This malware employs advanced vishing (voice phishing) techniques to deceive victims into disclosing sensitive information such as login credentials, credit card numbers, and banking details. FakeCall is part of a broader category of mobile-targeted phishing techniques known as "Mishing," which exploits unique features of mobile devices.

Infection Process:
FakeCall's infection typically begins when victims download an APK file onto their Android device through a phishing attack. This initial dropper installs the actual malicious payload, which is heavily obfuscated to evade detection.

Malware Capabilities:
The latest FakeCall variant demonstrates several sophisticated capabilities:

1. **Call Interception**: As the default call handler, FakeCall can manage all incoming and outgoing calls, potentially redirecting them to fraudulent numbers
2. **UI Manipulation**: The malware can create convincing fake interfaces that mimic legitimate apps, such as the native Android dialer
3. **Data Exfiltration**: FakeCall can upload contacts, call logs, SMS messages, and device location to the C2 server
4. **Remote Control**: Attackers can remotely control the device, including taking pictures, recording audio, and streaming video
5. **Accessibility Exploitation**: The malware leverages Android's Accessibility Service to monitor user interactions and automatically grant permissions

New Features:
Recent variants introduce additional functionalities:

- Bluetooth and screen state monitoring
- Enhanced accessibility services for greater device control
- Remote UI manipulation, including simulated button presses and screen unlocking
- Screen content capture and transmission capabilities

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

- **App Installation**: Only download apps from official stores like Google Play. Avoid sideloading APKs from unknown sources.
- **Permissions Review**: Carefully review app permissions, especially those requesting

access to calls, SMS, or accessibility services.

- **Default App Settings**: Regularly check and verify your device's default app settings, particularly for crucial functions like phone calls.
- **Security Software**: Install and maintain up-to-date mobile security software from reputable providers.
- **OS Updates**: Keep your Android operating system and all apps updated to the latest versions.
- **Phishing Awareness**: Be cautious of unsolicited messages or calls, especially those requesting sensitive information.
- **Two-Factor Authentication**: Enable 2FA for all critical accounts, preferably using authenticator apps rather than SMS.
- **Regular Audits**: Periodically review installed apps and remove any that are suspicious or no longer needed.
- **Network Security**: Use VPNs when connecting to public Wi-Fi networks to protect your data in transit.
- **Backup**: Regularly backup your device data to a secure, external source.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.zimperium.com/blog/mishing-in-motion-uncovering-the-evolving-functionality-of-fakecall-malware/