مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RAFEL RAT - Malware Targeting Android Users

Tracking #:432315980

Date:25-06-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new malware, "RAFEL RAT", targeting Android systems, providing remote administration and control.

TECHNICAL DETAILS:

RAFEL, an open-source remote administration tool (RAT), equips an attacker with various capabilities, such as remote access, surveillance, data exfiltration, and persistence mechanisms, making it a potent tool for conducting covert operations and infiltrating high-value targets.

Features:

- **Remote Access**: Allows attackers to control infected devices remotely.
- **Surveillance**: Enables monitoring of user activity and data exfiltration.
- **Persistence Mechanisms**: Ensures long-term presence on compromised devices.

Targeted Platform:

- **Android devices:** Rafel RAT specifically targets Android smartphones and tablets.

Propagation Methods:

- **App Downloads:** Malicious apps distributed via third-party stores or websites.
- **Phishing Attacks:** Deceptive messages or links trick users into installing the RAT.
- **System Vulnerabilities:** Exploits security flaws to infiltrate devices.

Impact:

- **Privacy Threat:** User data theft, including phone book exfiltration.
- **Financial Risk:** Stolen two-factor authentication messages can lead to account takeovers.
- **High-Profile Targets:** Successful campaigns have targeted military sectors and organizations.

INDICATORS OF COMPROMISE(IOCs):

SHA256
d1f2ed3e379cde7375a001f967ce145a5bba23ca668685ac96907ba8a0d29320
442fbbb66efd3c21ba1c333ce8be02bb7ad057528c72bf1eb1e07903482211a9
344d577a622f6f11c7e1213a3bd667a3aef638440191e8567214d39479e80821
c94416790693fb364f204f6645eac8a5483011ac73dba0d6285138014fa29a63
9b718877da8630ba63083b3374896f67eccdb61f85e7d5671b83156ab182e4de
5148ac15283b303357107ab4f4f17caf00d96291154ade7809202f9ab8746d0b

Command & Control Servers
districtjudiciarycharsadda.gov[.]pk
kafila001.000webhostapp[.]com
uni2phish[.]ru
zetalinks[.]tech
ashrat.000webhostapp[.]com
bazfinc[.]xyz
discord-rat23.000webhostapp[.]com

RECOMMENDATIONS:

- App Source Verification: Install from trusted sources only. Review app permissions before installation. Avoid apps that request excessive access.
- Patch Management: Prioritize regular updates for operating systems, applications, and security software to address vulnerabilities.
- Security Awareness Training: Educate employees on phishing, social engineering, and how to identify suspicious activity.
- Network Security: Avoid public Wi-Fi networks for sensitive activities. Enable the device's built-in firewall for additional protection.
- Security Software: Use reputable mobile security apps to detect and remove malware. Run periodic scans to identify any malicious activity.

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://research.checkpoint.com/2024/rafel-rat-android-malware-from-espionage-to-ransomware-operations/?web_view=true