Mphasis SOC – Information Security News
Date & Time Issued: 24-06-2024, 16:00 IST

Title	Multiple Threat Actors Deploying Open-Source Rafel RAT to Target Android Devices
Summary	• Android, as the most widely used mobile operating system globally, faces significant security challenges due to its open-source nature. One such threat is the Rafel Remote Administration Tool (RAT), an open-source malware that offers malicious actors a robust toolkit for remote control and manipulation of Android devices. • Rafel RAT's capabilities include remote access, data exfiltration, surveillance, and persistent control, making it a potent tool for cybercriminals. Its widespread use across various malicious campaigns has raised concerns among security experts about its potential for espionage, data theft, and other malicious activities. • Researchers identified around 120 different malicious campaigns employing Rafel RAT, targeting high-profile organizations including the military sector. These campaigns spanned across the United States, China, Pakistan, Indonesia, and other regions, highlighting the extensive geographical reach of the attacks. • The majority of victims were users of Samsung devices, followed by Xiaomi, Vivo, and Huawei users. Most affected devices were running outdated Android versions, which are no longer supported with security updates, making them vulnerable to malware exploitation. This trend emphasizes the need for users to keep their devices updated to mitigate security risks.
Severity	Medium
Attack Vectors	• The threat actors behind Rafel RAT utilize a PHP-based command and control (C&C) panel that relies on JSON files for storage and management. This panel allows attackers to monitor and control infected devices, providing detailed information about the device's specifications and enabling a suite of remote commands. These commands range from extracting contact lists and SMS messages to changing the device wallpaper and encrypting files. The C&C panel's capabilities facilitate extensive data collection and manipulation, posing significant risks to the privacy and security of the infected devices' users.

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	Domain	• districtjudiciarycharsadda.gov[.]pk • kafila001.000webhostapp[.]com • uni2phish[.]ru • zetalinks[.]tech • ashrat.000webhostapp[.]com • bazfinc[.]xyz • discord-rat23.000webhostapp[.]com
	File Hash	• d1f2ed3e379cde7375a001f967ce145a5bba23ca668685ac96907ba8a0d29320 • 442fbbb66efd3c21ba1c333ce8be02bb7ad057528c72bf1eb1e07903482211a9 • 344d577a622f6f11c7e1213a3bd667a3aef638440191e8567214d39479e80821 • c94416790693fb364f204f6645eac8a5483011ac73dba0d6285138014fa29a63 • 9b718877da8630ba63083b3374896f67eccdb61f85e7d5671b83156ab182e4de • 5148ac15283b303357107ab4f4f17caf00d96291154ade7809202f9ab8746d0b

Recommendations	• Block all threat indicators at your respective controls. • Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Keep Android devices updated with the latest OS versions and security patches to mitigate vulnerabilities. • Use reputable antivirus and antimalware software to detect and block threats. • Educate users about phishing tactics and encourage them to avoid clicking on suspicious links or downloading attachments from unknown sources. • Implement two-factor authentication (2FA) for additional security, but be vigilant about safeguarding 2FA codes. **NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**

References	• https://thehackernews.com/2024/06/iranian-hackers-deploy-rafel-rat-in.html • https://research.checkpoint.com/2024/rafel-rat-android-malware-from-espionage-to-ransomware-operations/