



STRRAT MALWARE CAMPAIGN

DROPPER, REMOTE ACCESS TROJAN, STEALER

Vairav Advisory Report

23rd May 2024

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairav.net

EXECUTIVE SUMMARY

The banking sector in Nepal has increasingly become a focal point for cyber threats, with numerous financial institutions facing a surge in cyberattacks. The StrRAT malware has recently emerged as a prominent threat, specifically targeting banks, and compromising their security. This wave of cyberattacks highlights the urgent need for enhanced cybersecurity measures and proactive strategies to protect sensitive financial data and maintain the integrity of Nepal's banking system. Phishing email campaigns continue to be the primary method used by threat actors to deploy STRRAT against victims. These emails often imitate the branding and logos of reputable organizations to appear authentic.

STRRAT is a remote access trojan (RAT) that enables attackers to take full control of a victim's computer system, allowing them to steal sensitive information, monitor activities, and deploy other malware. Active since mid-2020, STRRAT is a Java-based malware continuously updated to enhance its complexity and evade detection. Its malicious functions include data exfiltration from browsers and email clients, keylogging, file theft, and dropping additional malware. The identities of STRRAT's creators remain unknown, but the malware's ongoing evolution indicates active development to boost its capabilities.

Despite Java's decline in popularity over the past decade, STRRAT successfully infects numerous machines globally each year. Earlier versions of the malware required the Java Runtime Environment (JRE) on the victim's computer, but newer versions can install JRE from remote servers if it's absent. While STRRAT is commonly distributed via simple .jar files, it can also be spread through weaponized .pdfs and .xlsbs. Additionally, attackers use the polyglot technique (CVE-2020-1464), combining file formats like .msi and .jar to bypass security systems. These malicious files are typically sent as email attachments disguised as legitimate documents, such as receipts and invoices, within spam or phishing campaigns.

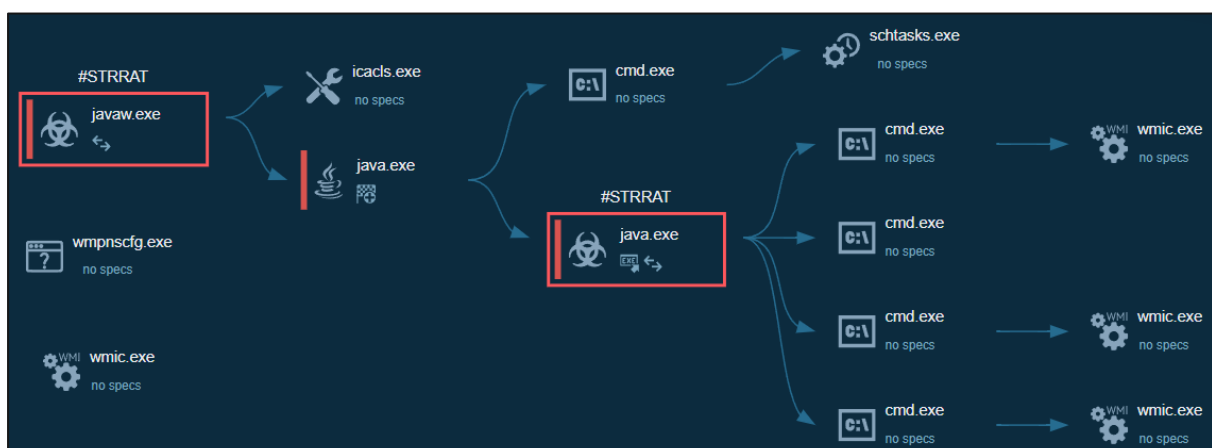
Key Points:

- **Remote Control:** The malware enables its operators to access the victim's computer, view its screen, and even reboot the device.
- **Data Theft:** It facilitates the collection of sensitive information, such as passwords, credit card details, and browser history.
- **File Management:** The malware can extract files from various directories, as well as upload, delete, and open files.
- **Malware Installation:** STRRAT can deploy additional malicious software.
- **Webcam and Microphone Recording:** The malware's spying features allow attackers to record conversations and capture photos using the device's webcam and microphone.
- **Keylogging:** It can capture all keystrokes on the infected machine and transmit them to its command-and-control server or record the information offline and send it once a connection is reestablished.

TACTICS, TECHNIQUES, AND PROCEDURE

STRRAT typically follows these execution stages:



- Using `icacls` to grant permissions.
- Executing a copy of the malware in the `C:\Users\admin` folder
- Establishing persistence through `schtasks`.
- Executing another copy of the malware in the `C:\Users\admin\AppData\Roaming` folder
- Collecting data and transmitting it to a specified server.



Replication is immediately noticeable. When the object is executed from the desktop, STRRAT first creates a copy of the file in the C:\Users\admin folder, followed by another copy in C:\Users\admin\AppData\Roaming. These copies then run sequentially.



```
CmdChild: "C:\Program Files\Java\jre1.8.0_271\bin\java.exe" -jar
"C:\Users\admin\AppData\Roaming\27f117c2cdae0c702f1095bb7c6fe40d7efb18e4ac14d3eca5570ce1d24bac2c.jar"
CmdParent: "C:\Program Files\Java\jre1.8.0_271\bin\java.exe" -jar "C:\Users\admin\27f117c2cdae0c702f1095bb7c6fe40d7efb18e4ac14d3eca5570ce1d24bac2c.jar"
Image: C:\Program Files\Java\jre1.8.0_271\bin\java.exe
```

The next step involves the malware using the `icacls` command to manage file access. This command grants all users access to the `.oracle_jre_usage` folder.

Command line  

```
C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_us
age /grant "everyone":(OI)(CI)M
```

The malware then creates a scheduled task using the command line. The task is configured to use the Task Scheduler to run the malware under the guise of the legitimate Skype program every 30 minutes.

Command line  

```
schtasks /create /sc minute /mo 30 /tn Skype /tr "C:\Users\admin\AppData\R
oaming\27f117c2cdae0c702f1095bb7c6fe40d7efb18e4ac14d3eca5570ce1d2
4bac2c.jar"
```

Then it changes the autorun value and writes malware into the startup menu.

```
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Name: 27f117c2cdae0c702f1095bb7c6fe40d7efb18e4ac14d3eca5570ce1d24bac2c
Operation: write
TypeValue: REG_NONE
Value: "C:\Program Files\Java\jre1.8.0_271\bin\javaw.exe" -jar
"C:\Users\admin\AppData\Roaming\27f117c2cdae0c702f1095bb7c6fe40d7efb18e4ac14d3eca5570ce1d24bac2c.jar"
```

```
Created: NONE
Device: DISK_FILE_SYSTEM
Name: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\27f117c2cdae0c702f1095bb7c6fe40d7efb18e4ac14d3eca5570ce1d24bac2c.jar
Object: UNKNOWN TYPE
Operation: WRITE
```

Therefore, it is anticipated that STRRAT will initiate again following an OS reboot. The process associated with STRRAT generates additional JAR files sourced from public repositories. These JAR archives generate files within the user directory. The trojan downloads and subsequently generates library files from the internet. Afterward, it establishes a connection with its command-and-control (C2) server to carry out its objectives.

MITRE ATT&CK TECHNIQUE

The malware makes the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

Tactic	Technique	Details
Execution	Command and Scripting Interpreter	Windows Command Shell
	Scheduled Task/Job	Scheduled Task
	Windows Management Instrumentation	
	User Execution	Malicious File
Persistence	Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder
	Scheduled Task/Job	Scheduled Task
Privilege Escalation	Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder
	Scheduled Task/Job	Scheduled Task
Defense evasion	Virtualization/Sandbox Evasion	Time Based Evasion
Discovery	Query Registry	
	System Information Discovery	
	Virtualization/Sandbox Evasion	Time Based Evasion
	System Network Configuration	
	Discovery	
	Software Discovery	Security Software Discovery
C & C	Non-Standard Port	

INDICATOR OF COMPROMISE (IOCs)

IP ADDRESS	DOMAINS
185[.]196[.]10[.]116	elastsolek21[.]duckdns[.]org
94[.]156[.]79[.]213	chongmei33[.]publicvm[.]com
193[.]25[.]215[.]58	freki[.]duckdns[.]org
79[.]134[.]225[.]92	rumpantus[.]ddns[.]net
87[.]98[.]245[.]48	twart[.]myfirewall[.]org
79[.]110[.]62[.]41	sandshoe[.]myfirewall[.]org
107[.]175[.]229[.]141	axe[.]ydns[.]eu
67[.]207[.]161[.]230	elastsolek22[.]duckdns[.]org
91[.]193[.]75[.]134	HASHES
93[.]123[.]39[.]147	146E04AD28CEDA68230C9085A4198FA74D6482760B9EAF0 AD575E50C200F09CC
193[.]25[.]214[.]209	655954E2D7D2E71F7C2CDCFB278F9154B94A50904EE3315 824DE204AA14E0100
173[.]254[.]204[.]77	DF24B51772FF4959E9BBFE481F72F0E88BA6E7C031D60ED B3B1A47C69F69A6D0
185[.]222[.]58[.]38	URLS
94[.]156[.]65[.]18	hxxp://jbfrost.live/strigoi/server/
193[.]25[.]214[.]192	hxxp://str-master.pw/strigoi/server/ping.php
185[.]203[.]116[.]210	
23[.]94[.]159[.]198	
91[.]92[.]255[.]88	
192[.]169[.]6[.]153	
65[.]21[.]212[.]74	

THREAT SUMMARY

Name	StrRAT (Remote Administration Trojan)
Threat Type	Dropper, Remote Access Trojan, Stealer
Detection Names	Avast: Java:Malware-gen [Trj], BitDefender: Trojan.GenericKD.43308841, ESET-NOD32: VBS/TrojanDropper.Agent.OIY, Kaspersky: HEUR:Trojan-Downloader.VBS.SLoad.gen
Symptoms	Remote Administration Trojans are crafted to clandestinely penetrate the target's computer and operate without detection, thereby concealing any distinctive symptoms on an afflicted system.
Additional Information	It's important to remember that it may not be the only malware present in an infected system. It can work in conjunction with other malicious samples and can be downloaded by notorious Trojans such as Emotet or TrickBot.
Distribution methods	Email attachments carry infections, deceptive online ads, manipulation through social engineering, and illicit software cracks.
Damage	Steal sensitive information, data loss, downtime, and financial loss.
Malware Removal (Windows)	Use reputable antivirus software to run a full system scan and remove all detected files and objects.

VAIRAV RECOMMENDATIONS

Implement robust email security: Organizations should implement email security measures such as spam filters, email gateways, and advanced threat protection to block malicious emails, including those containing malware.

Blocking unwanted extension files in emails: The organization should block the receiving of unwanted file extensions to be delivered via email. Some suggested file extensions to block are .js, .exe, .com, .cmd, .jar, .scr, .ps1, .vbs, and .lnk. However, as threat actors discover new file extensions to abuse, this list may be bypassed by other malicious file types.

Educate employees about phishing: Employees should be educated on identifying and avoiding phishing emails, which are often used to spread malware. This can include providing training on how to spot and report suspicious emails, as well as regularly testing employees with simulated phishing emails.

Implement multi-factor authentication: Organizations should implement multi-factor authentication for all remote access and sensitive systems to prevent attackers from stealing login credentials.

Keep software and operating systems up to date: Organizations should ensure that all software and operating systems are kept up to date with the latest security patches and updates. This is especially important for software that is commonly targeted by malware, such as web browsers and Office applications.

Use endpoint protection software: Organizations should use endpoint protection software to detect and remove malware from infected systems. This software should be kept up to date with the latest malware signatures and configured to conduct regular scans.

Regularly back up important data: Organizations should regularly back up important data and store it in a secure location in case the data is lost or stolen due to a malware infection.

Monitor network traffic: Organizations should monitor network traffic for signs of malware and investigate any suspicious activity. This can include monitoring for data exfiltration and connections to known command and control servers.

Have an incident response plan: Organizations should have an incident response plan in place and ensure that all employees know how to respond in the event of a malware infection. This should include procedures for isolating infected systems and reporting the incident to the appropriate parties.

Perform Vulnerability Assessment and Penetration Testing: We recommend performing vulnerability assessment and penetration testing of the networks, server, and end-user zones. The host-based vulnerability assessment is a must.

Have a Threat Intelligence: Threat intelligence keeps organizations apprised about active and emerging threats in the wild, to help recognize them and fend them off (or remediate them)

It is important to remember that the cyber adversaries behind are likely to constantly evolve their methods, tools, and techniques to evade detection and continue to be successful in their attacks. Therefore, organizations and individuals must stay informed about the latest TTPs and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairav.net

Website: <https://vairav.net>