Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

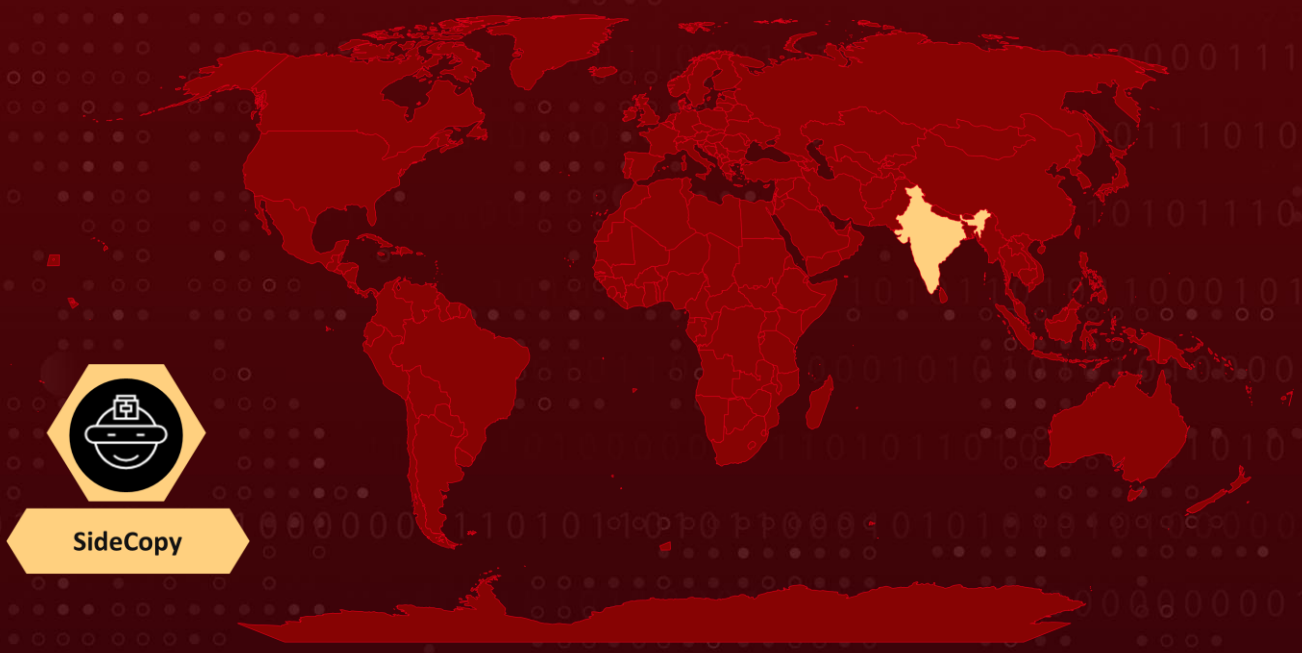
SideCopy Leverages Multi-platform RAT, Assaults Indian Government Entities

Date of Publication	Admiralty Code	TA Number
November 08, 2023	A1	TA2023451

Summary

Attack Discovered: November 2023
Attack Region: India
Targeted industries: Indian government entities
Actor: SideCopy
Malware: AllaKore RAT, Ares RAT, DRat, Key RAT
Attack: A threat actor linked to Pakistan named SideCopy is capitalizing on WinRAR's CVE-2023-38831 vulnerability to target Indian government agencies. This security vulnerability facilitates distribution of various trojans, enabling attackers to gain remote access to compromised systems. The latest campaign is multi-platform and includes attacks designed to use an Ares RAT to infiltrate Linux computers.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-38831	RARLAB WinRAR Code Execution Vulnerability	WinRAR	✓	✓	✓

Attack Details

#1 SideCopy, a threat actor group with connections to Pakistan, has been observed exploiting the WinRAR security vulnerability CVE-2023-38831 in their attacks targeting Indian government organizations. This exploitation is used to distribute trojans, which grant remote access to the compromised systems. Some of the RATs involved in these attacks include DRat, Ares RAT, and AllaKore RAT.

#2 SideCopy has been actively targeting South Asian countries, particularly Indian defense organizations and Afghan government entities, since at least 2019. The group has an arsenal of various tools and malware, including Action RAT, AllaKore RAT, Reverse RAT, Margulas RAT. It's worth noting that SideCopy is linked to another APT subgroup known as Transparent Tribe (APT36), which has been involved in attacks against the Indian Military.

#3 The first campaign initiated by distributing an archive file via a phishing link. This campaign utilized a decoy PDF file associated with NSRO, particularly targeting the Linux variant of the Ares RAT. In both the Linux and Windows campaigns, the same IP address was used. The archive files, hosted on different domains, shared the same name. The decoy PDF itself contained two embedded files: one was a decoy PDF, and the other was a DLL. This DLL file was responsible for downloading an HTA file and the final DLL contents and the final DLL payload was executed based on the presence of antivirus software.

#4 In the second campaign conducted by the SideCopy APT group, they utilized a security vulnerability known as CVE-2023-38831 found in the WinRAR archiving tool. This vulnerability allowed the threat actors to execute malicious code. As a result, they deployed a variety of trojans, including AllaKore RAT, Ares RAT, as well as two new trojans named DRat and Key RAT. These trojans are designed to provide remote access and control over compromised systems.

#5 The group was linked to a phishing attempt earlier in May that used lures associated with India's DRDO to spread malware that harvested personal information. In its current campaign, the SideCopy APT group has expanded its efforts to be multi-platform, targeting not only Windows but also Linux platform. The group has employed an Ares RAT-compatible version to compromise Linux machines.

Recommendations

Upgrade WinRAR: If you use WinRAR, upgrade to the latest version to mitigate the risk associated with CVE-2023-38831 and other potential vulnerabilities.

Remain vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Exercise caution when dealing with email attachments: Avoid downloading attachments from unsolicited or suspicious emails. Be cautious when opening archive files (e.g., ZIP, RAR) from unknown sources, as they could contain malware.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1583 Acquire Infrastructure	T1583.001 Domains	T1584 Compromise Infrastructure
T1584.001 Domains	T1588 Obtain Capabilities	T1588.001 Malware	T1588.002 Tool
T1608 Stage Capabilities	T1608.001 Upload Malware	T1608.005 Link Target	T1566 Phishing

T1566.001 Spearphishing Attachment	**T1566.002** Spearphishing Link	**T1106** Native API	**T1129** Shared Modules
T1059 Command and Scripting Interpreter	**T1047** Windows Management Instrumentation	**T1203** Exploitation for Client Execution	**T1204** User Execution
T1204.001 Malicious Link	**T1204.002** Malicious File	**T1053** Scheduled Task/Job	**T1053.003** Cron
T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1547.013** XDG Autostart Entries	**T1036** Masquerading
T1036.005 Match Legitimate Name or Location	**T1140** Deobfuscate/Decode Files or Information	**T1218** System Binary Proxy Execution	**T1218.005** Mshta
T1574 Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1222** File and Directory Permissions Modification	**T1222.002** Linux and Mac File and Directory Permissions Modification
T1027 Obfuscated Files or Information	**T1027.009** Embedded Payloads	**T1027.010** Command Obfuscation	**T1012** Query Registry
T1033 System Owner/User Discovery	**T1057** Process Discovery	**T1082** System Information Discovery	**T1083** File and Directory Discovery
T1016 System Network Configuration Discovery	**T1016.001** Internet Connection Discovery	**T1518** Software Discovery	**T1518.001** Security Software Discovery
T1005 Data from Local System	**T1056** Input Capture	**T1056.001** Keylogging	**T1074** Data Staged
T1074.001 Local Data Staging	**T1119** Automated Collection	**T1113** Screen Capture	**T1125** Video Capture
T1105 Ingress Tool Transfer	**T1571** Non-Standard Port	**T1573** Encrypted Channel	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1041** Exfiltration Over C2 Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	eb07a0063132e33c66d0984266afb8ae, 8bee417262cf81bc45646da357541036, 9e9f93304c8d77c9473de475545bbc23, 9379ebf1a732bfb1f4f8915dbb82ca56, 49b29596c81892f8fff321ff8d64105a, 75f9d86638c8634620f02370c28b8ebd, fc5eae3562c9dbf215384ddaf0ce3b03, a52d2a0edccdc0f533c7b04e88fe8092, 02c444c5c1ad25e6823457705e8820bc, d6e214fd81e7afb57ea77b79f8ff1d45, d0c80705be2bc778c7030aae1087f96e, 31340EA400E6611486D5E57F0FAB5AF2, FE0250AF25C625E24608D8594B716ECB, C872F21B06C4613954FFC0676C1092E3, ff13b07eaabf984900e88657f5d193e6, 6f37dacf81af574f1c8a310c592df63f, 9f5354dcf6e6b5acd4213d9ff77ce07c, CCB6723C14EBB0A12395668377CF3F7A, acec2107d4839fbb04defbe376ac4973, f759b6581367db35e3978125f4f6ff80, B6FBCAE7980D4E02CE9ED9876717F385, 4f541ec8cd238737e4e77a55fbcbb4f3, 7cba23cfd9587211e7a214a88589cf25, 04a65069054085cd81daabe4fc15ce76, c61b19cbedcb878aff45c067d503d556, eccc72deb8ce41433ed13591b4557343, 9375e3c13c85990822d2f09a66b551d9, 42a696ef6f7acf0919fea9748029a966, 54473E0D8CAFD950AFE32DE1A2F3A508, 36933B05B7E3060955E6A1FDFD7D8EC1, 508F4BFAD9F2482992AC7926910BD551, 921915ecfe17593476648ad20cd61ecd, 5e32703e3704b2b5c299c242713b1ec5, af3ec4f8a072779eb0cac18eaafc256d, 0799e17933b875e3a54f01416e7505d5, b4854c420bc39c8c77a0fcd9395a8748, 4cd0ee8186dc4203aad0cba48a8e5778, 088b89698b122454666e542b1e1d92a4, b992b03b0942658a516439b56afbf41a, ebbc1c4fc617cda7a0b341b12f45d2ad

TYPE	VALUE
IP	38.242.149[.]89:61101, 38.242.149[.]89:9828, 38.242.220[.]166:9012, 161.97.151[.]220:7015, 207.180.192[.]77:6023, 162.241.85[.]104, 103.76.213[.]95
Domains	sunfireglobal[.]in, occoman[.]com, elfinindia[.]com, ssynergy[.]in, rockwellroyalhomes[.]com, isometricsindia[.]co.in
URL	hxxps://www.rockwellroyalhomes[.]com/js/FL/DocScanner-Oct.zip, hxxps://www.rockwellroyalhomes[.]com/js/content/msfnt.hta, hxxps://www.rockwellroyalhomes[.]com/js/content/2023-06-21-0056.pdf, hxxps://www.rockwellroyalhomes[.]com/js/content/, hxxps://www.rockwellroyalhomes[.]com/js/FL/2023-06-21-0056.pdf, hxxps://www.rockwellroyalhomes[.]com/crm/asset/css/files/file/, hxxps://www.rockwellroyalhomes[.]com/crm/asset/css/files/doc/, hxxps://www.rockwellroyalhomes[.]com/crm/asset/css/files/doc/DocScanner_AUG_2023.zip, hxxps://sunfireglobal[.]in/public/core/homo/, hxxps://sunfireglobal[.]in/public/assests/files/db/acr/, hxxps://sunfireglobal[.]in/public/assests/files/auth/av, hxxps://sunfireglobal[.]in/public/assests/files/auth/dl, hxxps://sunfireglobal[.]in/public/assests/files/auth/ht, hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/files/tls, hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/files/, hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/pdf/in, hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/files/bossupdate, hxxps://futureuniform[.]ca/wp/wp-content/files/01/main.hta, hxxps://futureuniform[.]ca/email.gov.in/briefcase/Meeting_Notice-reg.pdf, hxxps://futureuniform[.]ca/mail.gov.in/briefcase/updated_draft_PPT.pptx, hxxps://futureuniform[.]ca/mail.gov.in/briefcase/draft_letter_nov_2023.docx, hxxps://futureuniform[.]ca/mail.gov.in/briefcase/DocScanner_Updated_letter.pdf, hxxps://keziaschool[.]com/wp/wp-content/uploads/2023/files/bossupdate, hxxps://keziaschool[.]com/wp/wp-content/uploads/2023/38, hxxp://38.242.220[.]166:9012/api/root_149371139681480/upload, hxxp://38.242.220[.]166:9012/api/root_149371139681480/hello, hxxp://38.242.220[.]166:9012/api/root_168683512566649/upload, hxxp://38.242.220[.]166:9012/api/root_168683512566649/hello, hxxp://38.242.220[.]166:9012/api/root_175170531258512/upload, hxxp://38.242.220[.]166:9012/api/root_175170531258512/hello, hxxp://161.97.151[.]220:7015/api/root_36854582802642/upload, hxxp://161.97.151[.]220:7015/api/root_36854582802642/hello

TYPE	VALUE
Path	C:\Users\Public\aque\up.hta, C:\Users\Public\aque\cdrzip.exe, C:\Users\Public\aque\rekeywiz.exe, C:\Users\Public\aque\DUser.dll, C:\Users\Public\aque\data.bat, C:\Users\Public\Msfront\Msfront.exe, C:\Users\Public\winowimg.jpg, C:\Users\Public\stremoe\steistem.exe, C:\Users\Public\stremoe\stremoe.bat, C:\ProgramData\Intel\cdrzip.exe, C:\ProgramData\Intel\DUser.dll, C:\ProgramData\WinGfx\credwiz.exe, C:\ProgramData\WinGfx\wingfx.bat, C:\ProgramData\WinGfx\DUser.dll, C:\ProgramData\HP\jquery.hta, C:\ProgramData\HP\jscy.hta, %AppData%\Msfront\Msfront.exe, %AppData%\Msfront\DUser.dll, %AppData%\Msfront\crezly.exe, %Temp%\cache.bat, %Temp%\Msfont\Msfont.exe, d:\Projects\C#\D-Rat\DRat Client\Tenure\obj\Release\MSEclipse.pdb, C:\Users\Boss\Desktop\test\Client\Client\obj\Release\Onlyme.pdb

Patch Details

Update WinRAR to latest version 6.23 and later.

References

https://www.seqrite.com/blog/sidecopys-multi-platform-onslaught-leveraging-winrar-zero-day-and-linux-variant-of-ares-rat/

https://www.hivepro.com/threat-advisory/sidecopy-resurfaces-to-target-indian-defense/

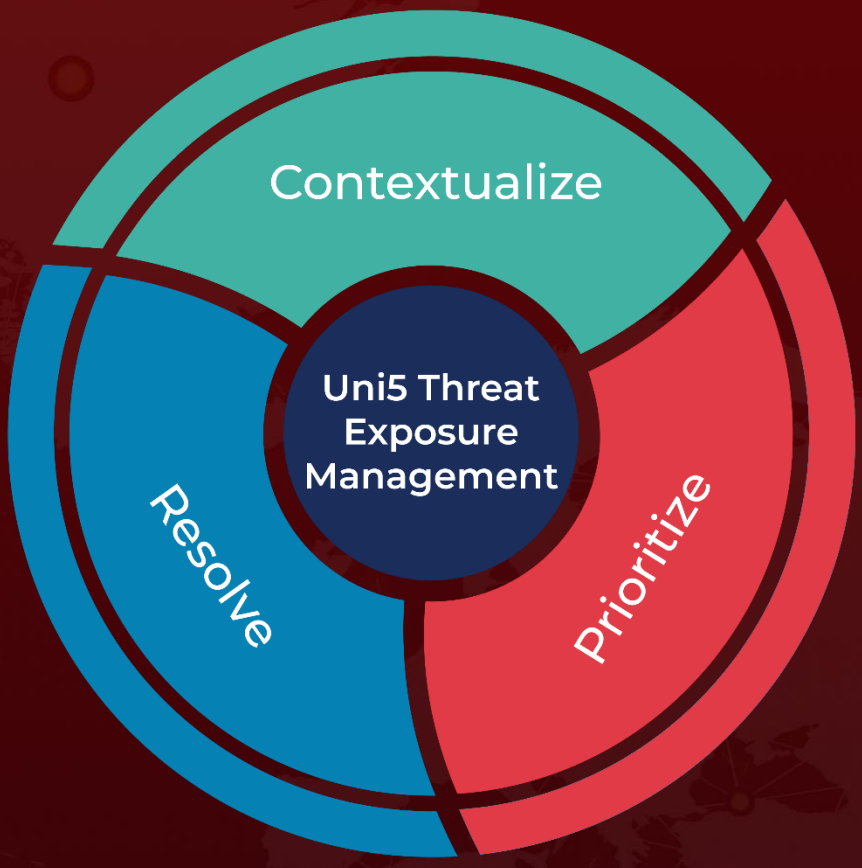
https://www.hivepro.com/threat-advisory/sidecopy-apt-launches-phishing-campaign-against-indian-government/

https://www.hivepro.com/threat-advisory/winrar-zero-day-exploit-targeting-traders-since-april/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 08, 2023 . 4:40 AM

More at www.hivepro.com