Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

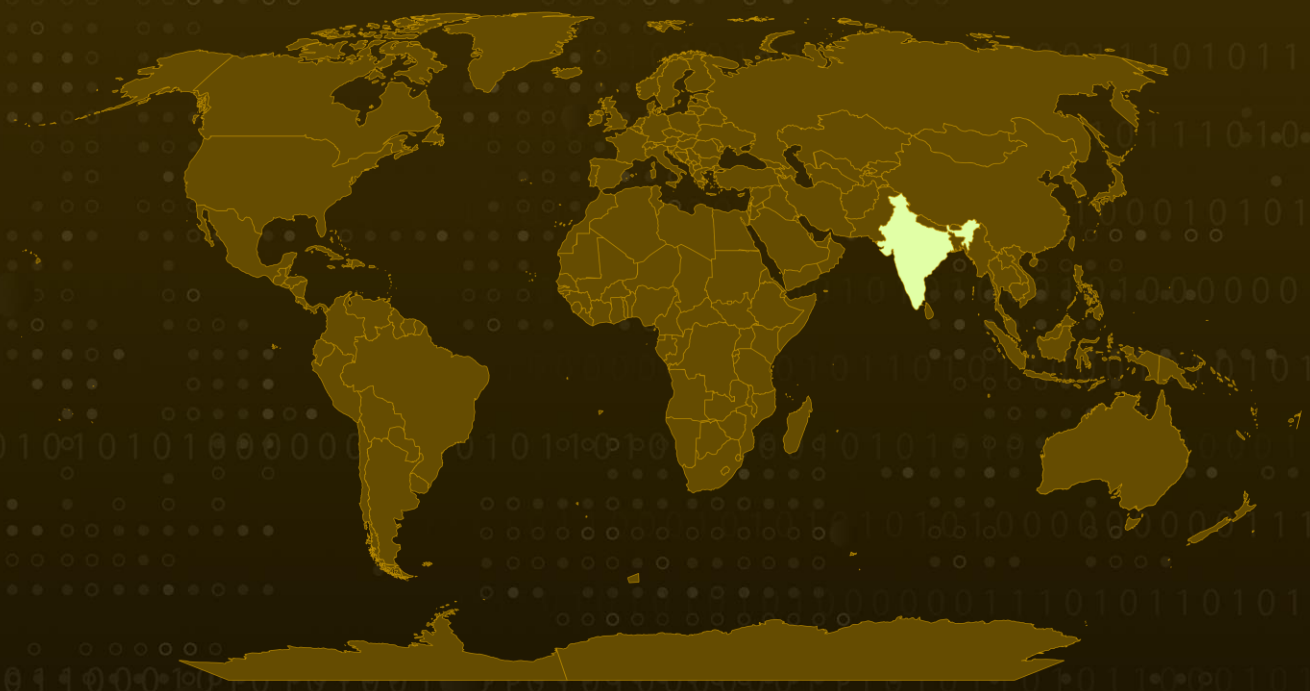
Operation RusticWeb: Coordinated Strikes on Indian Government

Date of Publication	Admiralty Code	TA Number
December 27, 2023	A1	TA2023521

Summary

Active Began: October 2023
Malware: Rust-based Malware
Campaign: Operation RusticWeb
Attack Region: India
Targeted Industries: Government, Defense
Attack: Since October 2023, an orchestrated phishing campaign named 'Operation RusticWeb' has been systematically targeting the Indian government and defense sector, deploying Rust-based malware for sophisticated intelligence gathering.

Attack Regions



Attack Details

#1 An orchestrated phishing campaign named 'Operation RusticWeb' has been systematically targeting multiple aspects of the Indian government and defense sector since October 2023. It involves the use of Rust-based malware for sophisticated intelligence gathering. The attackers have skillfully utilized innovative Rust-based payloads and encrypted PowerShell commands to extract confidential documents covertly.

#2 Notably, instead of relying on a dedicated command-and-control (C2) server, the malicious data is discreetly transmitted to a web-based service engine. Significant tactical similarities have emerged between this malicious cluster and previously monitored entities operating under the handles Transparent Tribe and SideCopy, both of which are believed to have ties to Pakistan.

#3 The recent series of attacks begins with a carefully crafted phishing email, employing advanced social engineering tactics to trick targets into interacting with malicious PDF files. These files act as carriers for Rust-based payloads, allowing silent enumeration of the file system in the background while displaying a decoy file to the unsuspecting victim. The malware is designed to collect system information and transmit it covertly to the designated C2 server.

#4 In December, a separate infection chain was identified, following a similar multi-stage process but differing by replacing the Rust malware with a PowerShell script. This script adeptly handles the enumeration and exfiltration phases. The pilfered information is ultimately uploaded to the 'oshi[.]at' domain, functioning as an anonymous public file-sharing engine known as OshiUpload.

#5 The overarching narrative suggests that Operation RusticWeb may indicate an Advanced Persistent Threat (APT), given its noticeable similarities with various groups associated with Pakistan. Noteworthy is the observed strategic shift among threat actors, moving from well-established compiled languages to newer alternatives such as Golang, Rust, and Nim. This intentional move ensures cross-compatibility while simultaneously complicating traditional detection methods.

Recommendations

Email Security: Implement robust email filtering solutions to reduce the likelihood of spam and phishing emails reaching users' inboxes, thereby helping to filter out potentially harmful content.

Behavioral Analysis and Anomaly Detection: Incorporate behavioral analysis and anomaly detection tools to identify and stop processes initiated by the malware. Monitor for unusual system behavior, such as termination of specific processes or connections to unfamiliar websites.

Network Traffic Monitoring: Implement network traffic monitoring to detect unusual patterns or connections, especially those related to downloader URLs. Continuously monitor and analyze network activities for potential signs of a security threat.

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	**T1583.001** Domains	**T1587.001** Malware	**T1588.002** Tool
T1608.001 Upload Malware	**T1608.005** Link Target	**T1566.002** Spearphishing Link	**T1566** Phishing
T1106 Native API	**T1129** Shared Modules	**T1059** Command and Scripting Interpreter	**T1047** Windows Management Instrumentation
T1204.002 Malicious File	**T1547.001** Registry Run Keys / Startup Folder	**T1027** Obfuscated Files or Information	**T1036** Masquerading
T1140 Deobfuscate/Decode Files or Information	**T1016** System Network Configuration Discovery	**T1033** System Owner/User Discovery	**T1083** File and Directory Discovery
T1005 Data from Local System	**T1119** Automated Collection	**T1105** Ingress Tool Transfer	**T1020** Automated Exfiltration
T1567 Exfiltration Over Web Service	**T1608** Stage Capabilities	**T1587** Develop Capabilities	**T1588** Obtain Capabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	56cb95b63162d0dfceb30100ded1131a, 13ee4bd10f05ee0499e18de68b3ea4d5, de30abf093bd4dfe6b660079751951c6, c9969ece7bb47efac4b3b04cdc1538e5, f14e778f4d22df275c817ac3014873dc, 501a6d48fd8f80a134cf71db3804cf95, 6d29fc0a73096433ff9449c4bbc4cccc, a9182c812c7f7d3e505677a57c8a353b, f5d8664cbf4a9e154d4a888e4384cb1d, 3ce8dfb3f1bff805cb6b85a9e950b3a2, a696c50dd5d15ba75c9e7f8d3c64997c, e0102071722a87f119b12434ae651b48, ee8d767069faf558886f1163a92e4009, 9f3359ae571c247a8be28c0684678304, b0b6629d35451bcc511c0f2845934c3e, f2501e8b57486c427579eeda20b729fd, 20b4eb5787faa00474f7d27c0fea1e4b, 635864ff270cf8e366a7747fb5996766, da745b60b5ef5b4881c6bc4b7a48d784, f68b17f1261aaa4460d759d95124fbd4, 237961bbba6d4aa2e0fae720d4ece439, d2949a3c4496cb2b4d204b75e24390d9, fc61b985d8c590860f397d943131bfb5, 04557782d7017f18ec059fc96d7f2dc8
File Names	IPR_2023-24.pdf.zip, IPR_2023-24.pdf.lnk, DSOP-NOM.ppam, in.ps1, Mail_check.ps1, sys.ps1, Ipr.pdf, abc009.pdf, 1.pdf
Domains	awesscholarship[.]in, parichay.epar[.]in, oshi[.]at, alfa-aeafa-default-rtdb.firebaseio[.]com
IPv4	89.117.188[.]126, 13.232.102[.]189

TYPE	VALUE
URLs	hxxps://rb[.]gy/gbfsi, hxxps://awesscholarship[.]in/upload/file.zip, hxxps://awesscholarship[.]in/upload/file1.zip, hxxps://awesscholarship[.]in/upload/in.ps1, hxxps://awesscholarship[.]in/upload/upload.php, hxxps://awesscholarship[.]in/upload/Ipr.pdf, hxxps://awesscholarship[.]in/upload/abc009.pdf, hxxps://awesscholarship[.]in/upload/1.pdf, hxxps://awesscholarship[.]in/upload/DSOP-NOM.zip, hxxps://awesscholarship[.]in/ppam/Mail_Check.ps1, hxxps://awesscholarship[.]in/ppam/syscheck.zip, hxxps://parichay.epar[.]in/Win/1.pdf, hxxps://parichay.epar[.]in/Win/Mail_Check.ps1
File Paths	%UserProfile%\Desktop\Syscheck\target\release\deps\syscheck.pdb, %UserProfile%\Desktop\Alam\target\release\deps\alam.pdb, %UserProfile%\Desktop\Aplet\target\release\deps\Aplet.pdb, D:\HOME\DESKTOP NEW DATA\Zew\target\release\deps\Zew.pdb, C:\ProgramData\syscheck\file.zip, C:\ProgramData\syscheck\MySystem.exe, C:\ProgramData\syscheck\MySystem.txt, C:\ProgramData\Micro\logs.txt, C:\ProgramData\Micro\records.txt, C:\ProgramData\Files\Log.txt, C:\ProgramData\Files\Records.txt, %UserProfile%\Documents\downloadAndExecuteLog.txt, %UserProfile%\Documents\file.ps1, %UserProfile%\Documents\myfile.zip, %UserProfile%\Documents\unzippedFolder\file.exe, %UserProfile%\Documents\Downloads\myfile.pdf, %UserProfile%\Documents\paths.txt, %UserProfile%\Documents\suc_logs.txt, %UserProfile%\Documents\Mail_Check.ps1, %UserProfile%\Documents\syscheck.zip, %UserProfile%\Downloads\1.pdf, %UserProfile%\Pictures\sys.ps1, %appdata%\Microsoft\Windows\Start Menu\Programs\Startup\MySystem.exe, %appdata%\Microsoft\Windows\Start Menu\Programs\Startup\syscheck.exe

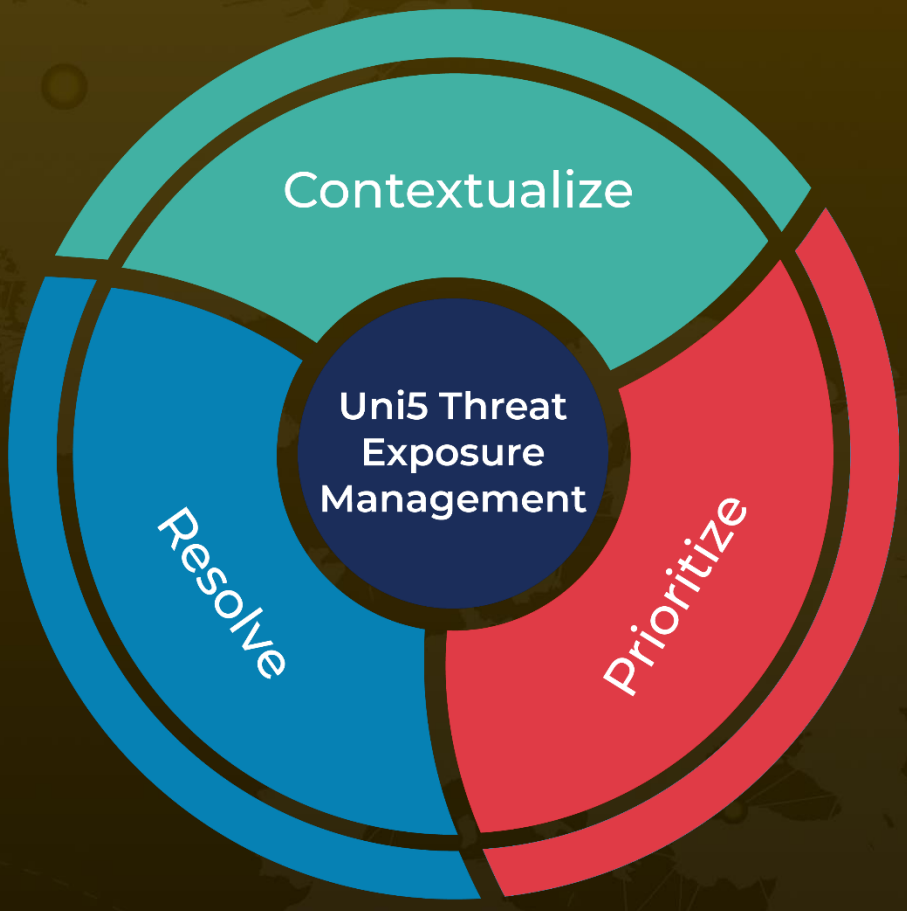
References

https://www.seqrite.com/blog/operation-rusticweb-targets-indian-govt-from-rust-based-malware-to-web-service-exfiltration/

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

December 27, 2023 • 4:00 AM

More at www.hivepro.com