Hive Pro

Threat Level
Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

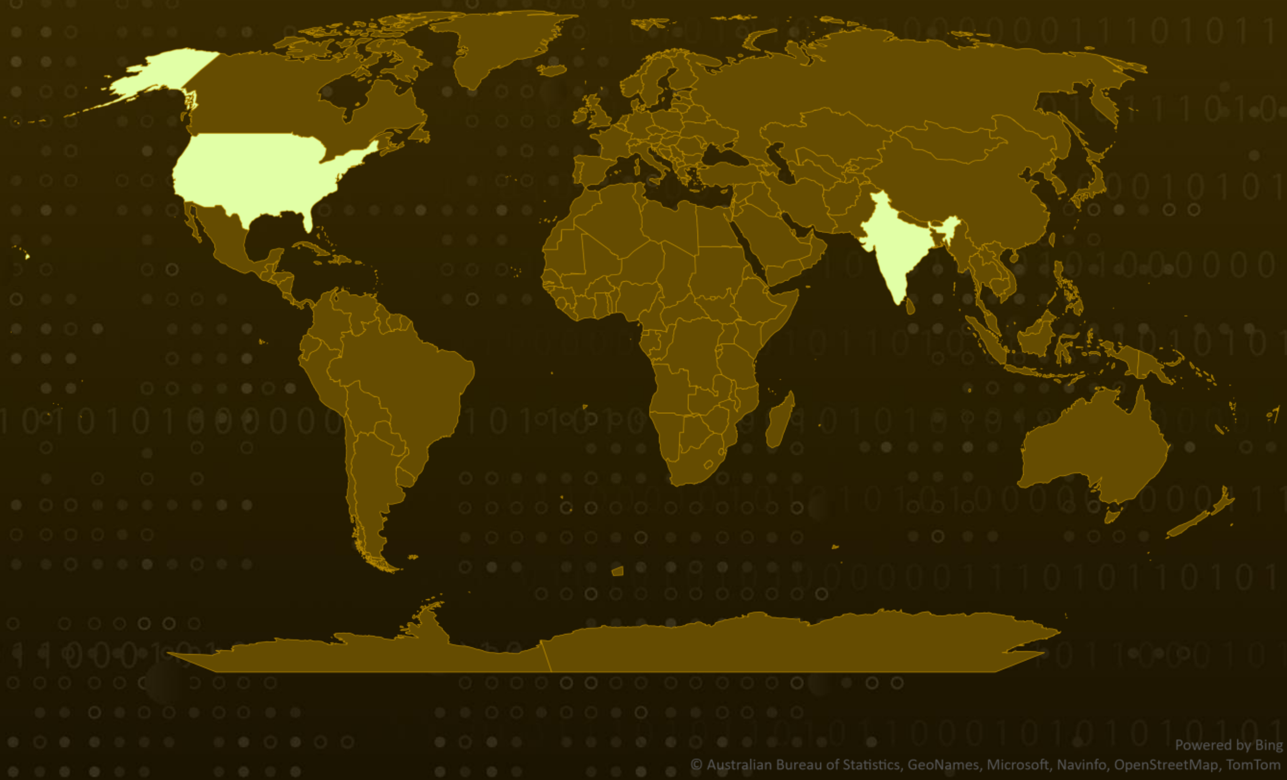
MULTI#STORM Campaign Sets Sights on India and U.S. with RAT

Date of Publication	Admiralty Code	TA Number
June 27, 2023	A1	TA2023281

Summary

Attack Began: May 2023
Malware: Warzone RAT, Quasar RAT
Attack Region: US and India.
Attack: The MULTI#STORM phishing campaign employs JavaScript files to disseminate RATs throughout compromised systems. This intricate attack utilizes a multi-stage procedure that commences when the victim engages with a phishing email. The email includes a Python-based Loader that masquerades as OneDrive Utilities.

Attack Regions


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 The MULTI#STORM a phishing campaign, leverages JavaScript files to distribute remote access trojans across compromised systems. This sophisticated attack unfolds in multiple stages, commencing with the recipient's interaction with a phishing email that contains an embedded link.

#2 Upon clicking the link, a request redirects the user to a Microsoft OneDrive file. Subsequently, the unsuspecting victim is prompted to download a password-protected ZIP file. The MULTI#STORM campaign targets primarily reside in the United States and India. The loader responsible for the initial compromise exhibits striking resemblances to the notorious DBatLoader.

#3 In addition to employing obfuscation techniques, the JS file incorporates an extensive amount of padding at the end of the script, precisely consisting of 509,992 zero characters. This approach serves multiple purposes: it can aid in evading detection by antivirus software in binary files, or it may be an attempt to inflate the size of the original ZIP file, thereby impeding AV analysis or brute-force attacks.

#4 Among the two files involved in the scheme, the first assumes the guise of a decoy PDF document, cleverly displayed to deceive the victim, while the second file, a Python-based executable, quietly operates in the background. Functioning as a dropper, the binary extracts and executes the primary payload, which is concealed within it as Base64-encoded strings ("Storm.exe"), after establishing persistence through modifications in the Windows Registry.

#5 The culmination of this attack chain results in the victim's machine becoming infected with multiple distinct instances of RAT (remote access trojan) malware, including the notorious Warzone RAT and Quasar RAT. It is worth noting that this variant of the Warzone RAT specifically attempts to extract cookies and credentials.

Recommendations

Exercise caution when encountering email attachments, particularly those originating from external sources or unexpected senders. Take extra care when dealing with ZIP files associated with this campaign. Additionally, implement a stringent application whitelisting policy to limit the execution of unfamiliar binaries.

Regularly monitor publicly writable directories, including temporary directories like "C:\Users\Public" and "C:\ProgramData". These locations are commonly targeted for malware staging, emphasizing the need for proactive inspection and detection of any suspicious activity. Strengthen your logging capabilities by implementing additional process-level logging such as Sysmon and PowerShell logging, enabling early identification and swift response to emerging threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0011 Command and Control	TA0010 Exfiltration	T1566 Phishing	T1566.001 Spearphishing Attachment
T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1059.007 JavaScript	T1027 Obfuscated Files or Information	T1027.010 Command Obfuscation	T1055 Process Injection
T1055.002 Portable Executable Injection	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1053 Scheduled Task/Job
T1053.005 Scheduled Task	T1573 Encrypted Channel	T1573.001 Symmetric Cryptography	T1105 Ingress Tool Transfer
T1571 Non-Standard Port	T1041 Exfiltration Over C2 Channel	T1056 Input Capture	T1056.001 Keylogging
T1113 Screen Capture	T1115 Clipboard Data		

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps://lo3kcg.bl.files.1drv[.]com/y4mtafF_tQM7vAFHxOASpTWOq0M5qmXCnd8FhdFvHvKOxYaA1h-ocJsybIp-r0iMVcK8UH6WP-fFspS6l-aP6uTlpsy11crZ_p_HfMxTI4yymzBqVkLX-v4nQLrn2Ty0-ilIRzICAbtwbooanM9U97qPmTgUNxhC9ab_4VfNvcmiWFeami9lwl35D8Eb7UiF7TCJTo_0XyAatlemjaXw9zAlw/REQUEST.zip?download&psid=1 – redirects to — hxxps://onedrive.live[.]com/download?cid=D09BFD4EBDA21A3D&resid=D09BFD4EBDA21A3D!152&authkey=AErksvWpjzpD_Ag hxxps://onedrive.live[.]com/download?cid=D09BFD4EBDA21A3D&resid=D09BFD4EBDA21A3D%21151&authkey=AGCMruhQJESxca4 hxxps://onedrive.live[.]com/download?cid=D09BFD4EBDA21A3D&resid=D09BFD4EBDA21A3D%21148&authkey=ADY1aqOba7HnNZs&em=2 hxxps://onedrive.live[.]com/download?cid=4A89E2A4EA0448C0&resid=4A89E2A4EA0448C0%21130&authkey=ABwx94zEGC3SmxA 134[.]19.179.147:38046/dominion46.ddns[.]net 134[.]19.179.147:29185/dominion46.ddns[.]net
SHA256	8674817912be90a09c5a0840cd2dff2606027fe8843eb868929fc33935f5511e 3783acc6600b0555dec5ee8d3cc4d59e07b5078dd33082c5da279a240e7c0e79 18c876a24913ee8fc89a146ec6a6350cdc4f081ac93c0477ff8fc054cc507b75 31960a45b069d62e951729e519e14de9d7af29cb4bb4fb8fead627174a07b425 02212f763b2d19e96651613d88338c933ddfd18be4cb7e721b2fb57f55887d64 5a11c5641c476891aa30e7ecfa57c2639f6827d8640061f73e9afec0adbbd7d2 30951db8bfc21640645aa9144cfeaa294bb7c6980ef236d28552b6f4f3f92a96 37c59c8398279916cfce45f8c5e3431058248f5e3bef4d9f5c0f44a7d564f82e f9130b4fc7052138a0e4dbaaec385ef5fae57522b5d61cb887b0327965ccc02a 0e799b2f64cd9d10a4dfed1109394ac7b4ccc317a3c17a95d4b3565943213257 455ed920d79f9270e8e236f14b13ed4e8db8dd493d4dabb05756c867547d8bc7

TYPE	VALUE
SHA256	9c14375fbbce08bcf3dc7f2f1100316b2fb745fa2c510f5503e07db57499bfc8 b452a2ba481e881d10a9741a452a3f092dfb87ba42d530484d7c3b475e04da11 ab0212f8790678e3f76ed90fba5a455ac23fbb935cf99cabc2515a1d7277676f 4a834b03e7faffef929a2932d8e5a1839190df4d5282cef35da4019fe84b19a5 11408368f4c25509c24017b9b68b19ce5278681f6f12ce7db992d3c6124b0a23

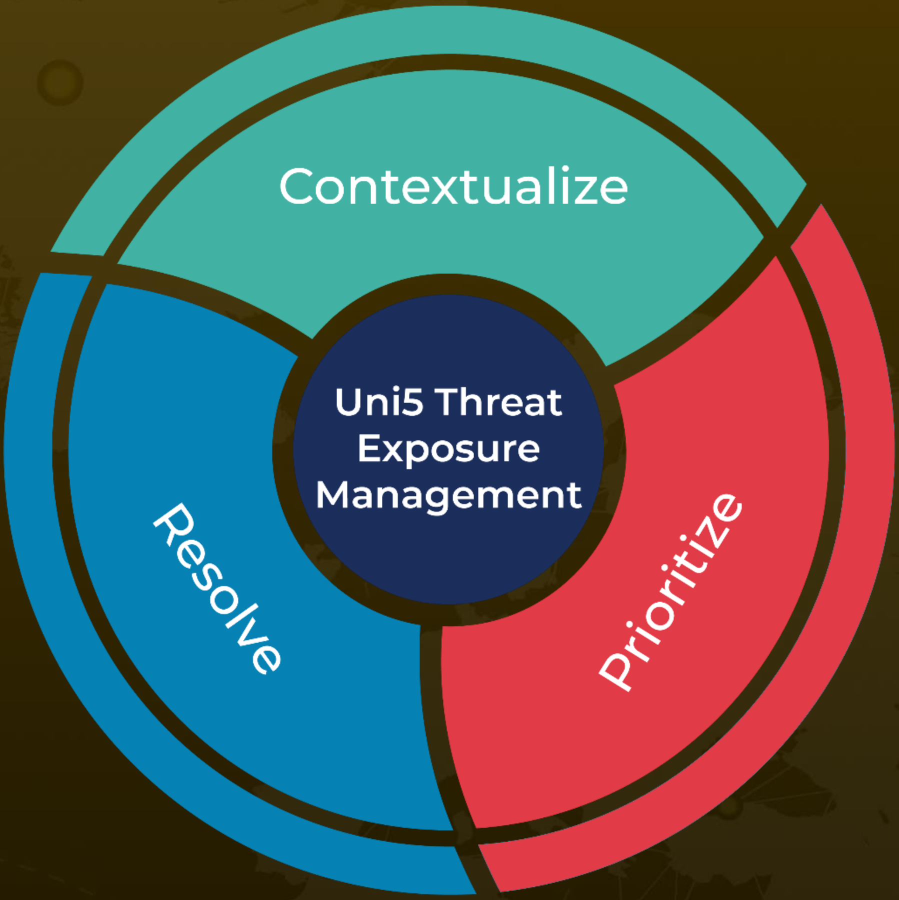
References

https://www.securonix.com/securonix-threat-labs-security-advisory-multistorm-leverages-python-based-loader-as-onedrive-utilities-to-drop-rat-payloads/

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

June 27, 2023 • 4:48 AM

More at www.hivepro.com