Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

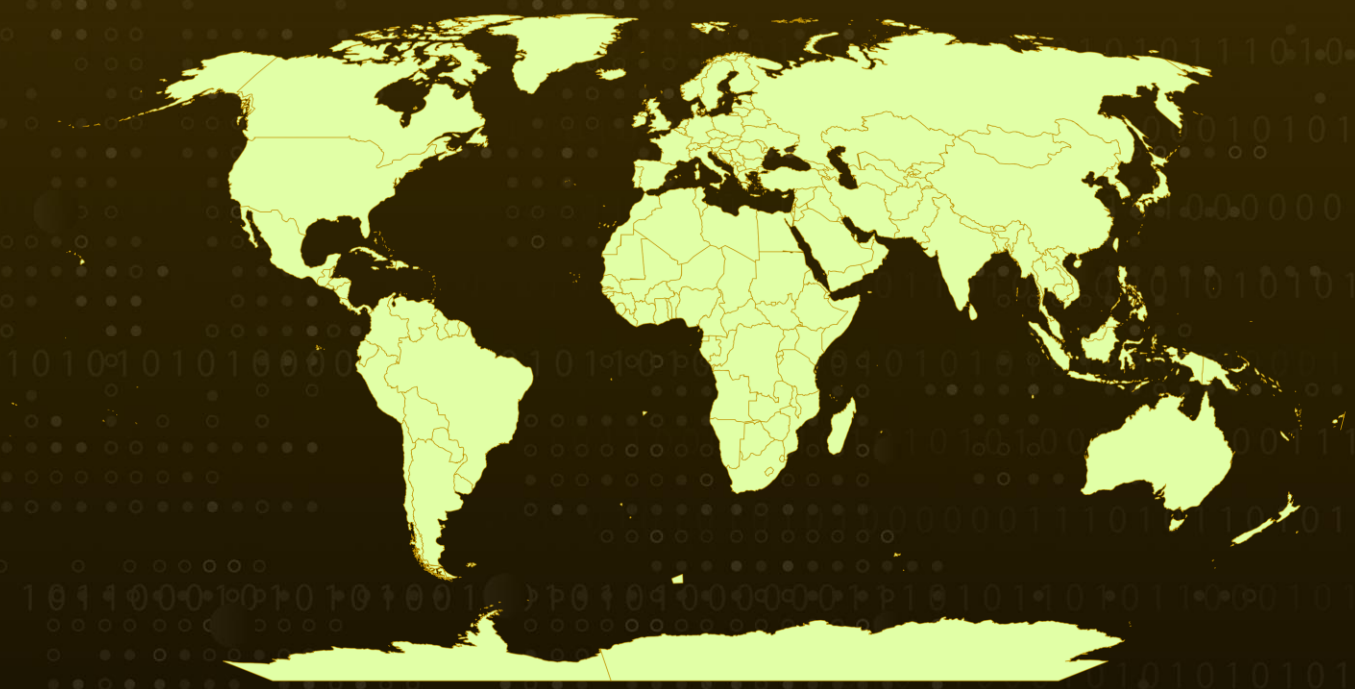
STRRAT a Java-Powered Versatile Remote Access Trojan

Date of Publication	Admiralty Code	TA Number
August 7, 2023	A1	TA2023323

Summary

Attack Began: March 2023
Malware: STRRAT
Affected Platform: Chrome, Firefox, Internet Explorer, Outlook, Thunderbird, and Foxmail
Attack Region: Worldwide
Attack: STRRAT, a Java-based RAT, excels in utilizing a wide array of capabilities. Its latest version, STRRAT 1.6, is notable for employing diverse infection paths and conducting startup host queries to understand system architecture and anti-virus defenses. Its primary objective is data extraction from compromised hosts. This modern STRRAT version employs a sophisticated dual-string obfuscation technique.

Attack Regions



Attack Details

#1 STRRAT, a sophisticated Remote Access Trojan with a history tracing back to at least mid-2020, exhibits a unique trait by being Java-based. Its delivery method involves the exploitation of spam emails, meticulously crafted to appear as originating from technology companies. Within these emails, an attached PDF file, cleverly masked as an invoice, plays a pivotal role.

#2 Upon opening the PDF attachment, a conspicuous download icon beckons from within the document. Interacting with this icon initiates the download of a zip file that houses a JavaScript file encapsulating the encrypted payload of STRRAT. An evolved iteration, STRRAT version 1.6, has been actively disseminated since March 2023, utilizing diverse infection pathways.

#3 Upon execution, STRRAT conducts host queries to ascertain system architecture and anti-virus safeguards. It further investigates active processes, local storage, and network capabilities. Presently, STRRAT employs a pair of string obfuscation techniques, specifically identified as "Allatori" and "Zelix KlassMaster (ZKM)."

#4 This sophisticated STRRAT malware maintains its inclination for targeting prominent web browsers, including Chrome, Firefox, and Internet Explorer, alongside widely embraced email clients such as Outlook, Thunderbird, and Foxmail. Its primary aim remains the extraction of sensitive information from the compromised host system.

Recommendations

- Implement robust email filtering to counteract spam, phishing, and malicious attachments, and exercise caution with unverified links and email attachments by validating their authenticity before opening.
- Utilize URL filtering to prevent access to malicious domains and reduce the risk of inadvertent malware downloads. Additionally, vigilantly monitor network beacons to halt data exfiltration driven by malware.
- Implement robust endpoint security solutions that encompass antivirus and anti-malware software. Keep these security tools up-to-date to ensure comprehensive defense against emerging threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0010** Exfiltration	**TA0040** Impact
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1204** User Execution	**T1204.002** Malicious File
T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell	**T1053** Scheduled Task/Job
T1053.005 Scheduled Task	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1140** Deobfuscate/Decode Files or Information
T1027 Obfuscated Files or Information	**T1027.009** Embedded Payloads	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers
T1056 Input Capture	**T1056.001** Keylogging	**T1518** Software Discovery	**T1041** Exfiltration Over C2 Channel
T1486 Data Encrypted for Impact			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3d3cb10a1a9059900ddeb58209edcfa52461806558ebbee422c417c6535aa3a5, 8250d324bbc14e3b3a7abc032b6b55aa0699ff9bc784d6c67fdd381edc3b9e56,

TYPE	VALUE
SHA256	c9380f51f0dd7167f833669eda3063a1a8f34cc3e2d536f29153952772dc8b20, 9714dce49616e48fc4851d05453056939ab08bf140fe9a786616fa914debb4f4, c9380f51f0dd7167f833669eda3063a1a8f34cc3e2d536f29153952772dc8b20, 6ec3e682fbbd0c23fb4e3a2c2b28f03431b90a88651d227ae3f33b6fadf507cf, 058c764614c8b0b457852a71ab93b559f81abb9e13b7fc2d6c6a4962881bf062, 5536bd8910de7571b6e14b2dd8af6da658f0f702321966d5bef85e9d41f6de21, 5536bd8910de7571b6e14b2dd8af6da658f0f702321966d5bef85e9d41f6de21, cbe7d5663fd5359a72f88e44d083703d9625235929c31e0f5b16a0b42cb44d35, 8cae71910574fa96fdf20ddab8897e90d155e50036ddb2f3d033a7b13a45b90f, c9380f51f0dd7167f833669eda3063a1a8f34cc3e2d536f29153952772dc8b20, b74a0e8adc5f0681405c94a684d6b887fdc20cd6d198d069f0981d6ba7d658c6, 31c2e51efcbff0aa489aa6af1a48cf78f6a9febfb449a19d029f8cc8ebb4495f, ab6f8c51d1f15a18cd23e1ad5a34c82c83746befb7d11cce2860c971be35adaa, d634982709d3ebf1641b1160ed6452fa9e3bf2cc8d28f397e56ca9687b28ec84, a0670c21968e2b1256d72799c22a512e503597ab375d20c49d9ec43428c4c3b2, 3a74d083e1c4e30f1eedcb90c842bf1a7e65a979edab40e37885607bd566bee8, 569f5f6de156bec90f9b0b0e4e707a702c0fea26ab6a0711e32f4a413995ae7c, 176e45016749ec233b8fe1ce32ce2cd47dd5bc8da3663f1c6cf054f6ad58a187, 3094952f4e4c826cdfbc7b146212eec6094f5104b4ba0d70d3b2920a263add27, 4bf781354d02ca0d67a3a180fd6f0d183c6fba763caa660f986752be8b4bb586, 6f7180a451691ee975f516cfc6fb3f0c983bc80aebd1d662a899ff4344e4077e

TYPE	VALUE
SHA1	4651326299d02ac07c0b51c0abb7067f24293a65, 8fa3c76f427f73cbfa864c380769825018cf72f5, f726bf1b6bc380c02d76d273765c888f6b41f197, 433b6ac1169a9bd7e0cfe7029954070cc2b4ebdf,
MD5	9af7e66c85e07a1e182fcb024e7048a2, c7130bf8bca520792f6eff1592a112b2, 61522d1e3290906215d580b8b59e6341, 9bc8ac6d3a38357488de33952e929143
Domain	talibangeneral[.]dynamic-dns[.]net
URLs	hxxp://jbfrost[.]live/strigoi/server/?hwid=1&lid=m&ht=5, hxxps://tatchumbemerchants[.]co.ke/Invo-0728403[.]zip.
File Name	Invo-0728403.zip

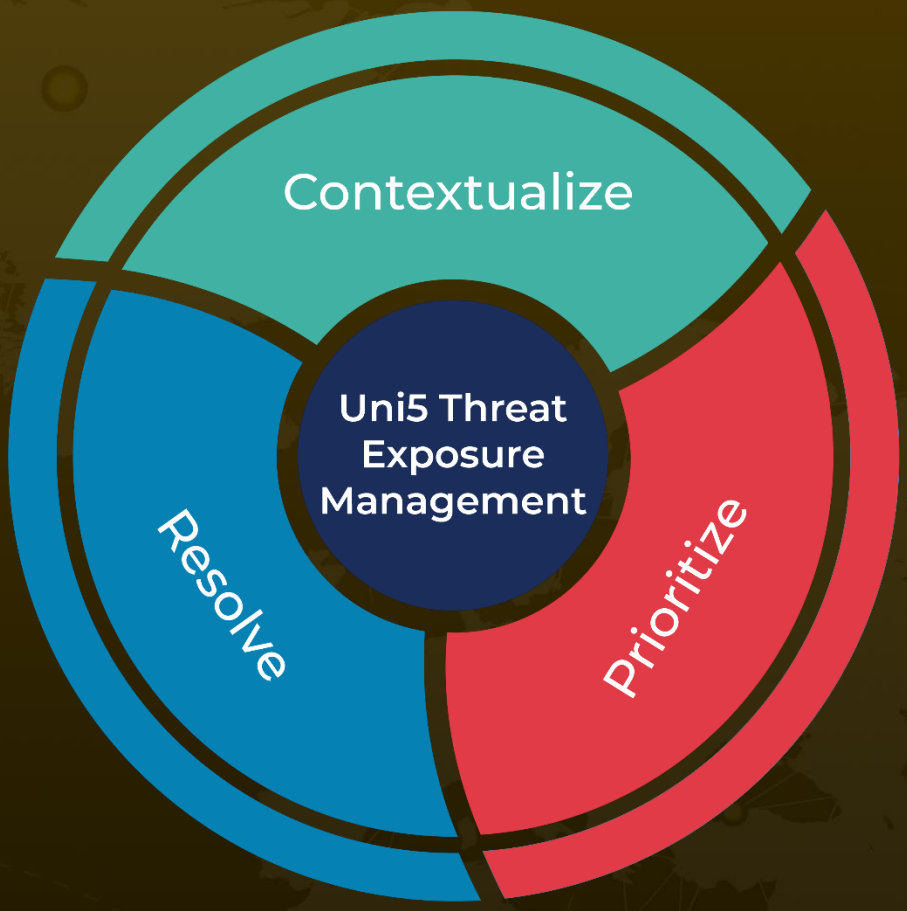
References

https://cyble.com/blog/strrats-latest-version-incorporates-dual-obfuscation-layers/

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

August 7, 2023 • 4:00 AM

More at www.hivepro.com