Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

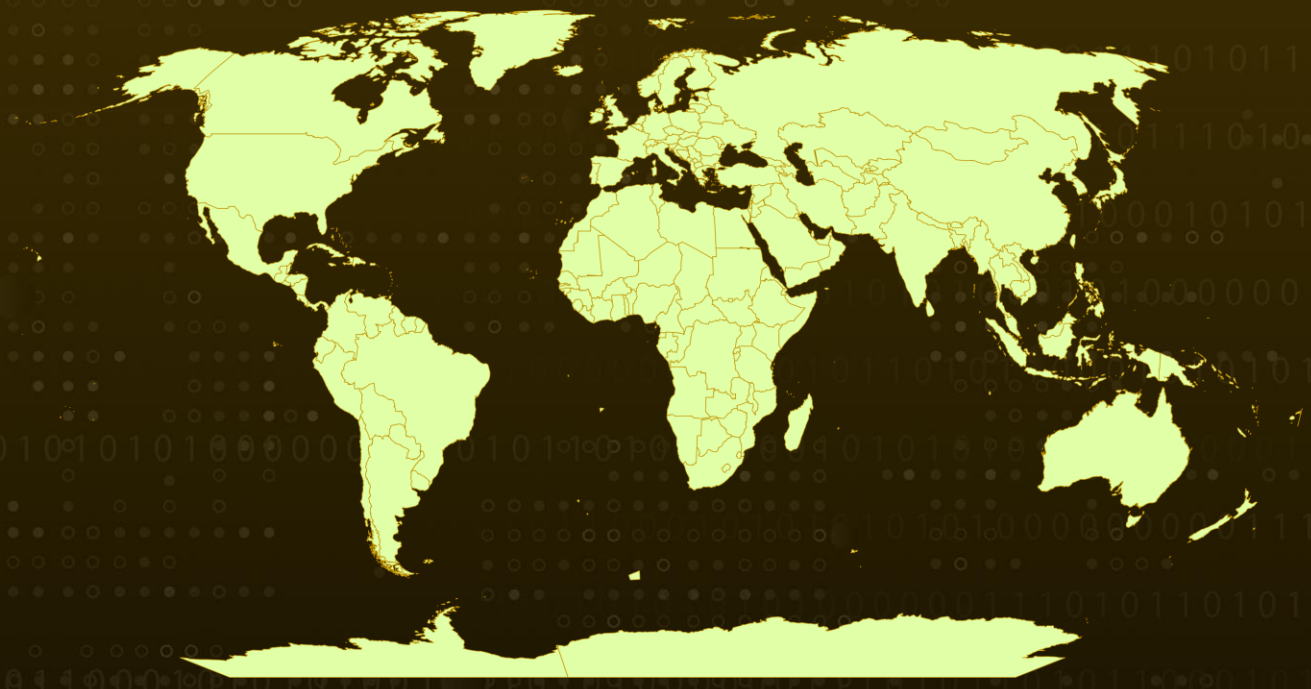
Sync-Scheduler: The Premier Document Stealer

Date of Publication	Admiralty Code	TA Number
April 3, 2024	A1	TA2024127

Summary

Malware: SYNC-SCHEDULER stealer
Attack Region: Worldwide
Attack: The Sync-Scheduler Infostealer, developed in C++, has emerged as a significant threat, hidden within Office document files. This malicious software boasts sophisticated anti-analysis features, allowing it to swiftly terminate operations upon detecting any analytical environment.

Attack Regions



Attack Details

#1 An Infostealer called Sync-Scheduler, developed in C++, has been discovered to be covertly distributed within Office document files. Armed with anti-analysis capabilities, Sync-Scheduler promptly terminates its processes upon detecting any analytical environment.

#2 The threat actor associated with Sync-Scheduler has been actively involved in malicious activities since at least November 2023. Sync-Scheduler employs a technique known as File-nesting to hide its malicious code within a PowerPoint presentation embedded in a Word document, which serves as the main method for its distribution.

#3 The title of the PowerPoint presentation file contains a portion of the malware code. By utilizing Base-64 encoding, the malware's code remains concealed, while VBA macros skillfully use Task Scheduler to decode, generate, and execute the malicious payload.

#4 The VBA macros nested within the PowerPoint presentation file streamline the decoding and execution of the malware, utilizing Task Scheduler to effectively disguise its activities and avoid detection. Sync-Scheduler specifically targets documents within User directories, such as Word documents, Excel spreadsheets, PowerPoint presentations, PDFs, and ZIP files.

#5 Following this, it relocates the targeted files to the OneDrive folder within the User's "AppData\Roaming" directory, altering the file extension to a specific string corresponding to the file type. Moreover, it exfiltrates the compromised files by communicating with a command-and-control server and network in the form of encrypted data.

Recommendations

Behavior-Based Monitoring: Implement behavior-based monitoring to detect unusual activity patterns, such as unauthorized network connections or suspicious processes, facilitating early threat detection.

Continuous Monitoring and Analysis: Implement continuous monitoring and analysis of network traffic and system logs. This proactive approach can help identify anomalies and potential threats before they escalate.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0002** Execution	**TA0005** Defense Evasion	**TA0007** Discovery
TA0011 Command and Control	**TA0010** Exfiltration	**T1592** Gather Victim Host Information	**T1059.003** Windows Command Shell
T1053.005 Scheduled Task	**T1204.002** Malicious File	**T1622** Debugger Evasion	**T1497** Virtualization/Sandbox Evasion
T1140 Deobfuscate/Decode Files or Information	**T1564.001** Hidden Files and Directories	**T1070.004** File Deletion	**T1027.009** Embedded Payloads
T1041 Exfiltration Over C2 Channel	**T1059.005** Visual Basic	**T1083** File and Directory Discovery	**T1071.001** Web Protocols
T1137.001 Office Template Macros			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	146[.]70[.]157[.]120
MD5	c1ab783d60cf05636eb4f72d17c6cf1d, 39122a2bcf6c360271e8edb503bc2761, df6b768247a9cdb5607819c79f02099d, 004101dc501b9de8965e6b45debd07b6
SHA256	2027a5acbfea586f2d814fb57a97dcfce6c9d85c2a18a0df40811006d74aa7e3, 203d60fe1ebbfafc835e082774ee56088273d9455fb12ac1de2c1be410cceeec, 6e4a4d25c2e8f5bacc7e0f1c8b538b8ad61571266f271cfdfc14725b3be02613, 316e01b962bf844c3483fce26ff3b2d188338034b1dbd41f15767b06c6e56041
URL	hxxp[:]//syncscheduler[.]com/r3diRecT/redirector/proxy[.]php

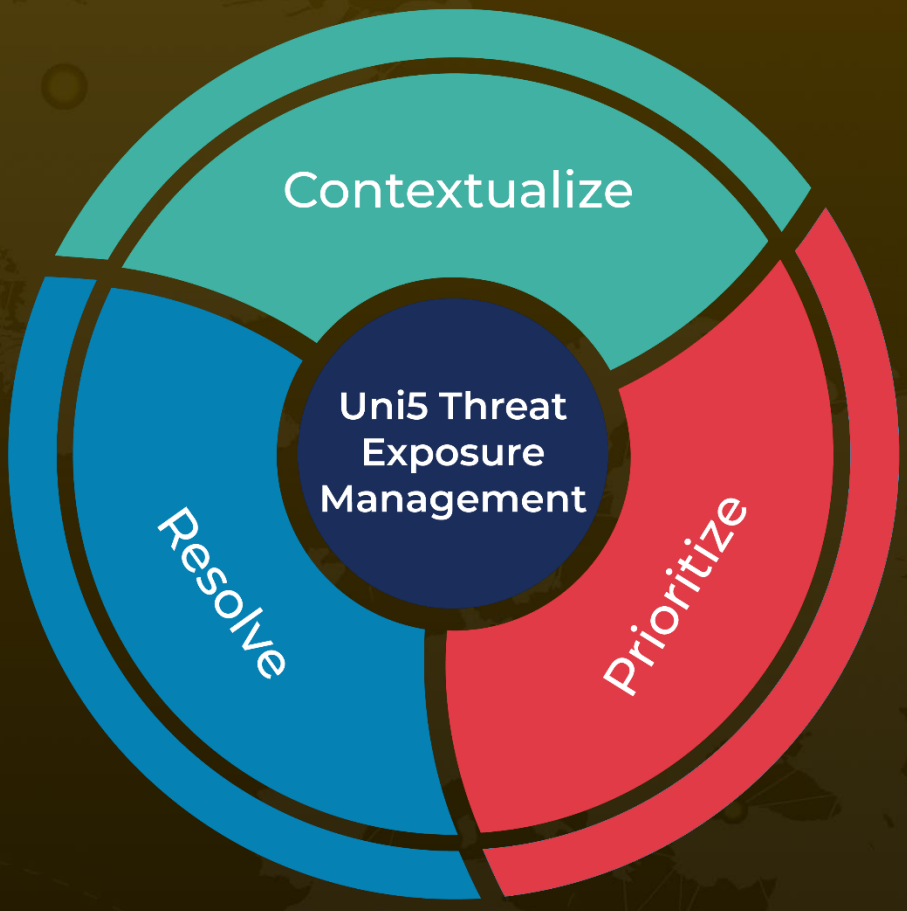
References

https://www.cyfirma.com/research/sync-scheduler-a-dedicated-document-stealer/

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

April 3, 2024 • 5:00 AM

More at www.hivepro.com