Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

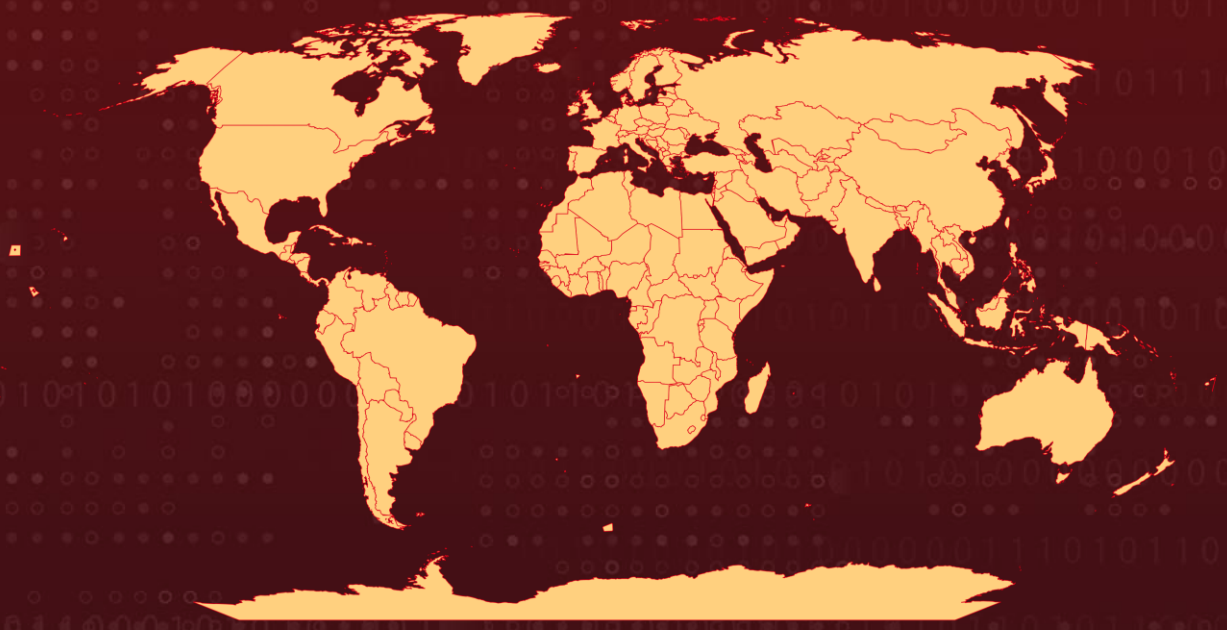
Inside ViperSoftX: Exploiting AutoIt and CLR for Stealthy PowerShell Execution

Date of Publication	Admiralty Code	TA Number
July 11, 2024	A1	TA2024268

Summary

Attack Discovered: 2020
Attack Region: Worldwide
Malware: ViperSoftX
Attack: The sophisticated malware known as ViperSoftX has been observed being distributed as eBooks over torrent networks. The latest variants of the ViperSoftX info-stealing malware employ the Common Language Runtime (CLR) to load and execute PowerShell commands within AutoIt scripts, effectively evading detection. ViperSoftX leverages CLR to load code within AutoIt, a scripting language used for automating Windows tasks that is typically trusted by security solutions. CLR, a key component of Microsoft's .NET Framework, serves as the execution engine and runtime environment for .NET applications.

Attack Regions



Attack Details

#1 ViperSoftX is a sophisticated malware that has evolved since 2020, becoming increasingly complex and difficult to detect. Initially spread through pirated software and torrents, it now hides within eBooks shared via torrents. The latest version utilizes the Common Language Runtime (CLR) to execute PowerShell commands through AutoIt, a Windows automation tool, enabling it to carry out harmful activities while evading detection.

#2 The attack initiates with a RAR file disguised as an eBook, which is hosted on a malicious torrent link. Upon opening the file, a JPG shortcut file is revealed. Executing this file sets off a chain reaction that activates hidden PowerShell code. This code performs various malicious actions such as hiding folders, checking disk sizes, scheduling tasks in Windows Task Scheduler, copying files to hidden directories, and deleting its own tracks.

#3 ViperSoftX leverages AutoIt's interaction with .NET CLR to run PowerShell commands covertly, enabling it to gather system information, scan for cryptocurrency wallets, and send encrypted data to a command-and-control (C2) server. It employs sophisticated network techniques like using fake hostnames and disguising communication to evade detection. The malware can also capture clipboard contents, download additional payloads based on server responses, and check for antivirus presence.

#4 This collected data is sent to a remote server, where it sets up a web client, configures headers with a custom user agent, and uploads the data. A unique trick it uses is sending a POST request with no content, trying to slip past detection systems.

#5 To bypass traditional security measures, ViperSoftX patches the Antimalware Scan Interface (AMSI) before executing PowerShell scripts. Organizations defending against ViperSoftX and similar threats require advanced detection strategies, regular security updates, and user education on recognizing and mitigating potential threats.

Recommendations

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. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Implement Proactive PowerShell Security Measures: Configure PowerShell execution policies to limit script execution solely to those that are signed or originate from trusted locations. Additionally, enhance security by creating a firewall rule to block outbound traffic for PowerShell and using Endpoint Application Control to whitelist approved applications and scripts.

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.

Trusted Installers: Always download software from the official website of the software vendor. Avoid third-party websites as they may host tampered versions of the software.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	TA0011 Command and Control	T1189 Drive-by Compromise
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.010 AutoHotKey & AutoIT	T1204 User Execution
T1204.002 Malicious File	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1047 Windows Management Instrumentation

T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1140 Deobfuscate/Decode Files or Information	T1564 Hide Artifacts
T1564.001 Hidden Files and Directories	T1070 Indicator Removal	T1070.004 File Deletion	T1036 Masquerading
T1036.008 Masquerade File Type	T1027 Obfuscated Files or Information	T1027.013 Encrypted/Encoded File	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1518 Software Discovery	T1518.001 Security Software Discovery	T1087 Account Discovery
T1087.001 Local Account	T1217 Browser Information Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery
T1005 Data from Local System	T1033 System Owner/User Discovery	T1115 Clipboard Data	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1573 Encrypted Channel	T1132 Data Encoding	T1132.001 Standard Encoding

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1177fb1b6b4a6ac1cd75c0f0784bb87a3202c70fe748bf5bc7fd0dd0fd41169b, 07ee16f72b1dd81e7cf79aa1396f44f3ed29d343dd8fa0c6aecf1bb3d36d4e34, f2503068aa274eb6c73dfd1a31c7e878f84f3fb60f3ae23f001bb143eb6f196f, 96a1666152dfe5cc4113b855a059195227f55773d8ad46cc92fe5090010035f1, de05f6f97b475ed6464541665e59252869b5d531c63698a9ad70c3875954c92c, acf98f0c2b3823f9213b220fcd79237037d0d3f087a3faa4f10ea6d147a9f059, 7701e4bf5074f0527c0126fff1dbd0e6368ddb7d0131bac1fba72b19511af127, 4d365958397af1b7c2c62f62d21b35b948c03dd17f730a58b6145cd003a7922c,

TYPE	VALUE
SHA256	39e0199d3d501acc3377af56c4e79ec4c4f8aaa21ac1a449fe8da69c4c267dd7, f8ef5f403474624e61ef0b83adc9e15ea6ca47534f7316c4c43db6f064e21c76, 655afdb9fc4ab05875c790c22e505b4eda3492323631ed3c951b4fe60806770a, 2b807f42e32684768fa5e514ee0674836f3774ec83e73fc0be0afde34f8ee11c, f30aeb1877ddd30c0d2b79c78bffa7f990df56d37dd78ab0d5c563db02b1ab37, 2526a840c91d03c804a8f73cc35a9a993f4dcddf12950566c419a8addf52fd39, a544293ad41861129c77aaaea1620b884982378721bed31c60702b3e3d3c1590, 9b5869e4d37894571923607dce7c23a324ae2f93820384b99aefe619a7fa3fad, 87982fe34bfcb26fd06714e0bb4c3341dfaa66b51e918fcf048554be60d29307, 87d809543079ae5770b6cdc1849e7be55dec1a37c3f90ea63a5d5f5a2b3d4c32, 3d5d95b4e51ce5b7597c3f2b8da50951bd8152493e3ea27f0b8f7ab32596a526, 4ab0bc4c0841cf65f6c78356327337cdea436e1c1d008e8e0a5f5e400aaed39c, 10e1dbb3c19c6a3b905434cae98fe0c6d4e68a8d9bcd316175160efd834a2d23, 829a3a3525fae23ea0e56a0049b9ba56f9a061315d023940defb00661a74b767, 8af9b0cdb301febc64ac05b8acb701d0f1b6f88cc22a4c83929078d04bfca657, 594948597aae36cd9fcf30dec7ef1be70bc70ee618f0e33dd8268c12982da7c9, F83a0b46b9d424d338342b509d9e12b467d25f400db62dc57815db33b1b26feb
URLs	hxxps[:]//security-microsoft[.]com/connect, hxxps[:]//borcano[.]org/connect

References

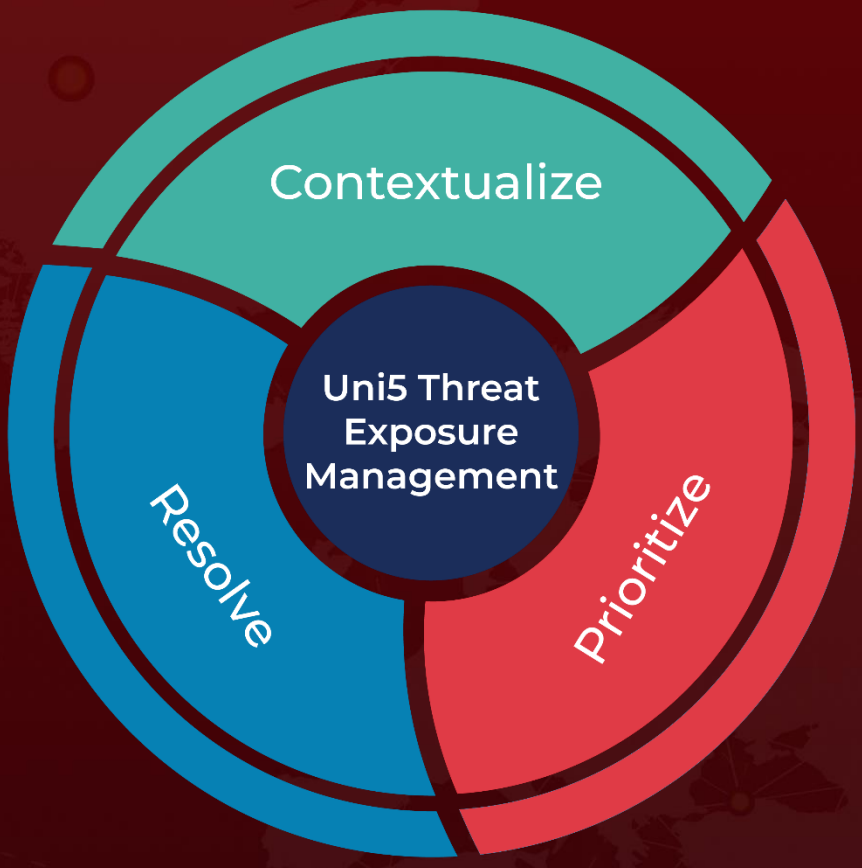
https://www.trellix.com/blogs/research/the-mechanics-of-vipersofts-exploiting-autoit-and-clr-for-stealthy-powershell-execution/

https://hivepro.com/threat-advisory/new-version-of-vipersoftx-malware-targets-password-managers-and-cryptocurrency-wallets/

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

July 11, 2024 • 6:00 AM

More at www.hivepro.com