Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

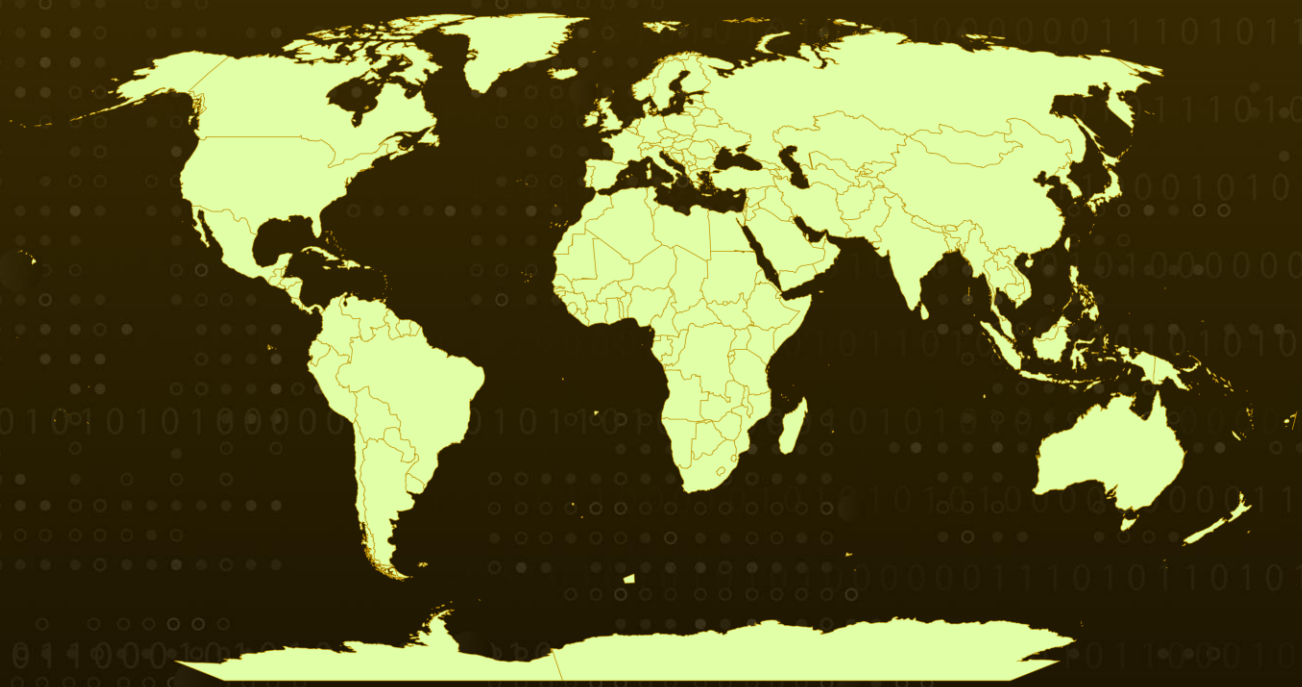
zEus Stealer's Undercover Operation on YouTube and Minecraft

Date of Publication	Admiralty Code	TA Number
May 8, 2024	A1	TA2024177

Summary

Malware: zEus stealer
Affected Platform: Microsoft Windows
Attack Region: Worldwide
Attack: The zEus stealer has successfully infiltrated both a source pack circulated on YouTube and a Minecraft pack concealed within a WinRAR file, cleverly masquerading as a Windows screensaver. Its proficiency in collecting a wide range of data presents a significant threat, empowering future attacks and reinforcing strategies in social engineering.

Attack Regions



Attack Details

#1 The zEus stealer malware has been integrated into a source pack circulating on YouTube. Derived from a previous iteration of this malicious software, the name "zEus" persists. This variant is also distributed through a Minecraft source pack, hidden within a WinRAR self-extracting archive cleverly disguised as a Windows screensaver file.

#2 Upon activation, the zEus stealer conducts a preemptive analysis, scrutinizing the computer's name and active processes against predefined blacklists to detect any attempts at analysis. If such efforts are absent, it proceeds to covertly harvest sensitive data while depositing script files to enhance its operational flexibility.

#3 The zEus stealer establishes directories within the C:\ProgramData directory to store stolen data and malicious script files. A comprehensive range of information is captured by the zEus stealer. Each piece of data is meticulously recorded into separate text files, which are then organized into corresponding folders.

#4 Leveraging the victim's IP address, zEus employs various tools to gather additional intelligence, including details about the internet service provider, and geographical coordinates. Upon completion, zEus compiles the results of its intrusion and sends them alongside a compressed file labeled "STEALER.zip". zEus strategically deploys "debugerkiller.bat" to obscure its execution, thwarting attempts to terminate its processes via Task Manager.

#5 Furthermore, it introduces "RAT.bat" to facilitate Command and Control (C2) communication. While its attack method may seem straightforward, the zEus stealer adeptly gathers a diverse range of information, providing valuable data for subsequent attacks and strengthening social engineering tactics. This serves as a stark reminder of the risks associated with downloading and using files from unverified sources.

Recommendations

Enable Multi-Factor Authentication (MFA): Implement MFA mechanisms to add an extra layer of security to your authentication process, making it harder for attackers to gain unauthorized access to sensitive systems or data compromised by zEus Stealer.

Implement Application Whitelisting: Use application whitelisting to only allow approved applications to run on your systems, reducing the risk of unauthorized or malicious software like zEus Stealer gaining a foothold.

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.

Use Reliable Sources: Download files only from trusted and reputable sources. Avoid downloading files from dubious websites or sources with a questionable reputation.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1036 Masquerading	T1036.005 Match Legitimate Name or Location
T1056 Input Capture	T1082 System Information Discovery	T1016 System Network Configuration Discovery	T1119 Automated Collection
T1005 Data from Local System	T1041 Exfiltration Over C2 Channel	T1102 Web Service	T1027 Obfuscated Files or Information

Indicators of Compromise (IOCs)

TYPE	VALUE
File Path	%appdata%\Battle.net, %localappdata%\Electronic Arts, %localappdata%\EpicGamesLauncher\Saved\Config, %localappdata%\EpicGamesLauncher\Saved\Data, %localappdata%\EpicGamesLauncher\Saved\Logs, %appdata%\Telegram Desktop\tdata, %userprofile%\.lunarclient\settings\game*.json, %appdata%\.minecraft*.json, %localappdata%\protonvpn, %localappdata%\Ubisoft Game Launcher
File Name	debugerkiller.bat, Screen.bat, SYSTEMLOCK.bat, configSYSLOCK.vbs, bsod.hta, CHATBOX.bat, RAT.bat, COMMANDS.txt, HISTORY.txt
URLs	onlinecontroler[.]000webhostapp[.]com/, panel-controller[.]000webhostapp[.]com/, hxxps[:]//discord[.]com/api/webhooks/1212818346157015070/2v0xe2vrxFGv65MRE9qvICmsJw-5e_pq_28xscGybiY1ScEyEiSKMC_zFffr3KkuAimX, hxxps[:]//discord[.]com/api/webhooks/1212821302671581224/L30ylYucowXO_rm7sUpdwA8DLbYet6NyvUsNV60EP1o1HnF-2M-UPsvatVGQY0ctO9Vk, hxxps[:]//discord[.]com/api/webhooks/1216834085205311708/2Rx-yUIHeCnuhuLskpz25Ghf-YWeP6Si6oiUSN4SMQYNkeJfVJiYNC4Xy_Oj0ZNQ1qTC, hxxps[:]//discord[.]com/api/webhooks/1117543783714787458/U_DdPjJm7rM7Q2asPiMISLTrbd3oGw3oVQ25_XU37HCmM6QIQ804SJAH4_h0AT2Vr_cv, hxxps[:]//discord[.]com/api/webhooks/1191890861622050848/iJVVE3x3xilf4TeZNiERydXZPF5TRE1UhM4Ew06uHn95b0k0KDViw3YnhdynrXn17OKa, hxxps[:]//discord[.]com/api/webhooks/1215746939635892344/CmKTGdIvizEpR4FgvvLJm3Bcbjg3AKlNGlwd2S-yIO-GRBXZZbn0OwG39kKnx7mDur4T,

TYPE	VALUE
URLs	hxxps[:]//discord[.]com/api/webhooks/1223978005127364659/3E0hHtDqDOHQJBaG8ifspilk2mY8E1s4KeQY36inBq-tq5q6aZex8U0YJVxVlloFJj5X, hxxps[:]//discord[.]com/api/webhooks/1224075124005929020/kA4IFZrIXBl_d1Y4I0sMHhF1cZzXvC-yEo5HzSk6Jzq_I0k1PCc1idn4FmqSC2UMljdD
SHA256	aabfbef31ab073d99c01ecae697f66bbf6f14aa5d9c295c7a6a548879381fb24, c9687714cf799e5ce9083c9afa3e622c978136d339fc9c15e272b0df9cd7e21c, d9d394cc2a743c0147f7c536cbb11d6ea070f2618a12e7cc0b15816307808b8a, c2c8a7050b28d86143f4d606a6d245b53c588bc547a639094fce857962246da4, be9ea302bcfb52fbfdf006b2df8357388cd4c078059aabc5b5928676c3361e50, 9d3409852348caa65d28e674008dd6bb986eed4fb507957c7a8b73a41e00be70, b6e8b612e99c54dd98af1756f7c9b8a8c19e31ed9b2836878c2a5144563ff1b2, 8a2f6d5f6cf7d1a7534454e3c3007337b71d7da470e86f7636eb02d68b2db8cc, df6156fdbbcc7b6f8c9cb4c5c1b0018fc3f1e1ca7d949b5538ec27dc86d026a4, 5840f3e43a0c635be94b5fbf2e300d727545371b582361a52682b4a9e08bcebd, 51ede75315d858209f9aa60d791c097c18d38f44b9d050b555ff1f4de0ae672d, d1865d2aaf11e3f8bccefe9c4847510234f14aaa5378ce9e8e97553537cf2ca1, 9ba19d614af029c3c198b576ccdf1de87d80ac14b12103e8a15376229a2a7860, 6063c8285e13d10eabbe363e2ab0d8748bcd595b470698e0cffee31ba255a566, d1a18b436f947611914ced09e4465b49807cec4f3a62b0973c9017b6d82c9f70, 1cdd580176eeb4342a0333b50454da061e473358274e6e543df1411186c12042, ed59a797521db06abdf4c88dad7b1666e5978aaa6670a5952a55b7e11f7b790e, 2ceae724f0e96e2d8c47296dd1e73ac592e22ee3288eabf11c8d039c6d6d4f8b, 03983b56d8b1a6cc43109f6cd67a13666367595a2ea07766127cb1fe4d4bb1a5,

TYPE	VALUE
SHA256	9940da9d02d29489c3e26d27feb15b6f4bbf49547b962592125441917c952f12, fbf967295dac00f1e9cb67e9a40b6729b003dd12cf022eb15d626df09716442d, 4e0a96ab28570936d095ac3910dcd239c7ceeb2b38a070468404584f8b902dd1, 20009fd157a898ad6d50fae6b8127056c5b1f50e31f90f01d2e6c13e6b4c38f8

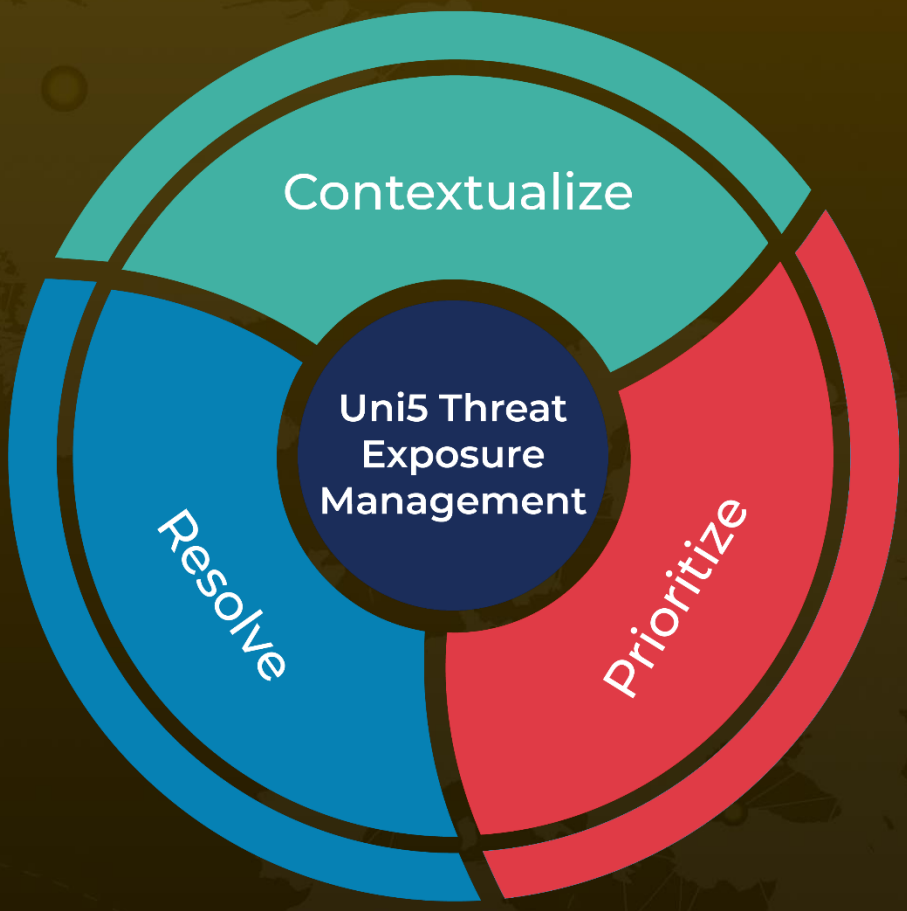
References

https://www.fortinet.com/blog/threat-research/zeus-stealer-distributed-via-crafted-minecraft-source-pack

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

May 8, 2024 • 6:00 AM

More at www.hivepro.com