Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

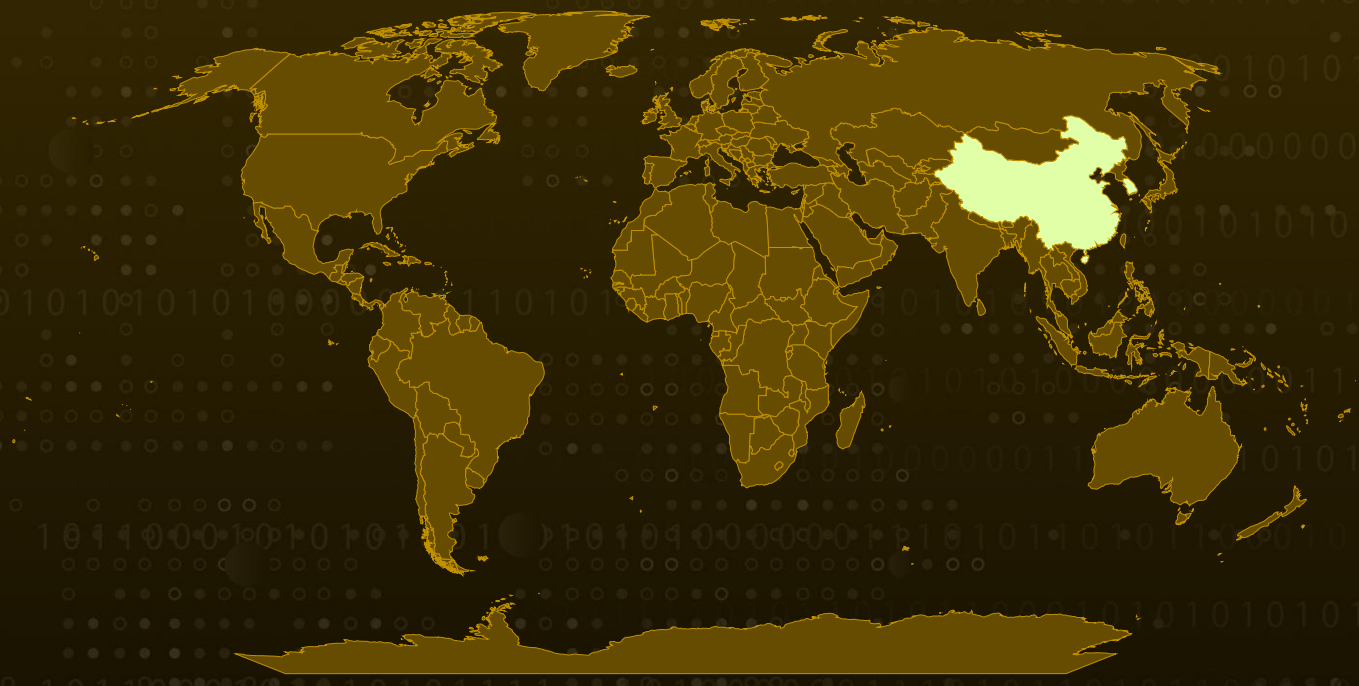
UULoader Malware Emerges: Targeting Users with Advanced Evasion Tactics

Date of Publication	Admiralty Code	TA Number
August 20, 2024	A1	TA2024318

Summary

Attack Discovered: July 2024
Attack Region: Korea, China
Malware: UULoader, Gh0st RAT, Mimikatz
Attack: A newly identified malware variant, known as UULoader, is currently being utilized by threat actors to deploy next-stage payloads like Gh0st RAT and Mimikatz. This malware is distributed via malicious installers masquerading as legitimate applications, with a primary focus on Korean and Chinese-speaking users. The presence of Chinese strings within the program database (PDB) files embedded in the DLL suggests that UULoader may have been developed by a Chinese-speaking individual or group.

Attack Regions



Attack Details

#1 A new type of malware called UULoader has been discovered, used by cybercriminals to spread harmful software like Gh0st RAT and Mimikatz. This loader is particularly tricky because it disguises itself as legitimate applications, mainly targeting users who speak Korean and Chinese.

#2 In July 2024, a surge in malicious Windows Installer files (.msi) was noticed. These installers, pretending to be real applications or updates, were actually spreading UULoader. Researchers believe the malware was developed by a Chinese-speaking person and named it "UULoader" based on certain patterns found in the code.

#3 UULoader uses a method called file header stripping to avoid detection by security software. Normally, file headers help identify what type of file it is, but by removing these headers, the malware can hide its true nature. The malware's key files are stored in a Microsoft Cabinet (.cab) archive, which contains two important files—a .exe and a .dll—both of which have had their headers removed to make them harder to detect.

#4 The malware uses an old Realtek executable to load its malicious .dll file. The .cab file also includes two small files labeled "M" and "Z," which help restore the stripped headers. Some versions of UULoader even include a legitimate file, like a Chrome update, to distract the user while the malware does its work.

#5 UULoader creates a folder named "Microsoft Thunder" and uses a .vbs script to carry out its malicious actions. This script hides the folder from Windows Defender, restores the file headers, and runs the malware. It also executes a decoy file to keep the user unaware of what's happening. The final payloads of UULoader often include remote access tools like Gh0st RAT and hacking tools like Mimikatz.

#6 UULoader is sophisticated malware that targets Korean and Chinese-speaking users. It highlights the increasing trend of cyber threats that focus on specific cultural and language groups. Organizations in these regions should be especially cautious, ensuring strong security measures are in place to block such disguised malware.

Recommendations

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.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

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	TA0005 Defense Evasion	TA0011 Command and Control
T1204 User Execution	T1204.002 Malicious File	T1218 System Binary Proxy Execution	T1218.007 Msiexec
T1564 Hide Artifacts	T1564.012 File/Path Exclusions	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1059 Command and Scripting Interpreter	T1059.005 Visual Basic
T1036 Masquerading	T1566 Phishing	T1105 Ingress Tool Transfer	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	5c698edeba5260b1eb170c375015273324b86bae82722d85d2f013b22ae52d0c, 240999322f426e0e3d4921e691e10afe20f0b7383038f57f39840c14a5cdf92c, e8d2a953c4423dc1836165d3cb734418f5276aa5ed46297d03bf01dbc78c8e70, 4b25b4306cf8da05456484178e8e935d9f9a66f2e385b080e36cd652ab6880bc, bb64e8f94742afec20156e75915070f6c23ca13021a80c4637f92c2760009d72, 4dfa9e07224c1d7ef6a6ffae2027b1df2f08c4ed2910d872ca248785bb35dad8, dc8925a926456878860c37ed01a996de4f858f33ac18cfcf9b29a997d7e38e5c, cd09451ba2d5ff87387087f75ad2fd4943c2c83b9ff6f87a2b8910e39bc3459b, 0df0ff0ce0162b4498ad6a25b6e536cffb119316262cf89e4ccf77535ebc13a5, 7846c4aa9d6bc5a1d12fd1b885c28809203c5df4920df31220b7140ea206b7be, c675f276611ef53f8b74b8eb7b33590de19b07fc4b3b6d846ebca6f63a056ff7, c729bd033e705a2fddd3591c1e52a48932aeef628f6f63f460e56bfffe39c3ab, 092ca5a50a0bf1d8f7b4e38fd80474f31f1d4eb8036ac13e101421b5df1687db, 0821a3f021856adf31bb07531030e922cbd33483402547daf3d1b98d5c4c1a57, ca543ff1fe2963a8daf5042b29c86e3d4abc0eb1365feb3ca53d006abc48f0cc, 598042a211e7c25ce34390851d344f084d3c625c478945c3bf4501ed65a18097, 81c25e14af8c4ca37b6fb7ed0d8122a6a5d3054943af89e839bffff907fe128f, d5a429457405c018e2536e3750044d93bf547f4dfa397a6d9b7dc9a691cfcddd, 45e1ad56a97a92633f41d873fd8cb6b6da8e0e8e4ef094ba433d1c90ea195874, 48df25302ef5df40e692acac546ed3713e28a0c02f563b98e65cbb28d9f1b675, b172b565dc16b29af83689cf6a26f62372e33f2640109a4ddb15d89f6bff3e6d,

TYPE	VALUE
SHA256	79aaa25a384729b3a6f04091459e09f9c5935cba7d27182ff6794337413886b8, 359fabc75c195ebec1fea4237aa011092f4080d82236652f2be1252275ed7b4f, 267abb405b8010dda2546d0ac1e59d2e83a23754fc8af68a866335dd76422781, 4a4efcf4c80c5ec4f6479549097e04c272d640664b4f8d0768f159f9f295f24a, 69605f9958127a28e8448077ff9610c2da584a7528485c14046e6f4e13fe0f90, 165a1ef58ee6f29291685d98863f82d1875d78b16d0a1207b34a7719b2b4d43a, 63c07d1feb2402e92d57b637497372e8e8e2ef88419f482465c549dd0b90fe13, 5b5e8f9d1e317fd0963be2b5b46ca7a4710c5fec145a5a8bcb7eec1ff519a842, 591a2fb480864f0c793d055dee3d948e3cb150fc56df0644bb424bf912557440, b3e0aaf9a5c37408fca964220c9d294e4842a2901feaa373f056c191b8c6896d, e5459a53509b40edc3c6019cf0f7b0d05e14cd1a0641824e1cfecfe952a33f64, 972f9dc83a69fa5297e4d0e05113b6fab86bcefb0b3af913f7349bfe0e79fc87, eabd8606040bda54ad02062091e9af1840f557c61cb736f1c2f3d68a678f2798, fd0c66d3899702138f893f919f21b6d155a53a93a2181eaf4b602030c7adf5c7, 63b065324ea96ec5785c4d18c78ccc2e7d071a8e2f92a06835e2366567bbf31d, 3761a7ac0427692e4194d0a988b0d7985d7a909de69c3fc0ce028eb76a1297f9, f144be0bd8d377de067e4cdf5256a33f8ba03c8f0b15afb2593fa258b71a4005, ea193e1c13a142ed7d9f499a814d9480441f18c75e0617de8fdcc8443f7d1eae, b562b190f6c3174943993f0da38133d4b4b20f80ac8d11f0757d45e1ad462154, 5d3c87c115092f7c3da9a9144c1b594b0229830b258cbc27fe20841f38b78ca9, 962d1fd45f1e164ec54c2f62eb71acacbd70c425bae8dfce0e8d5612baedef75, 742e6e4db5056b45254125f809ec158fdb5303c6c378fc1a23c599965a4aaa67, eaff614d9223fe13ebe45c04eacf31acf970e0aedbe1811bab32e55718395625,

TYPE	VALUE
SHA256	596ffd75ab3512cba1e7328d902460b55401c094ddb67fe9f98263c06d10b517, 796466e5146bb76e9e81ca32014842b355d7df96d6c6bab0dcf02e6a8f9be11e

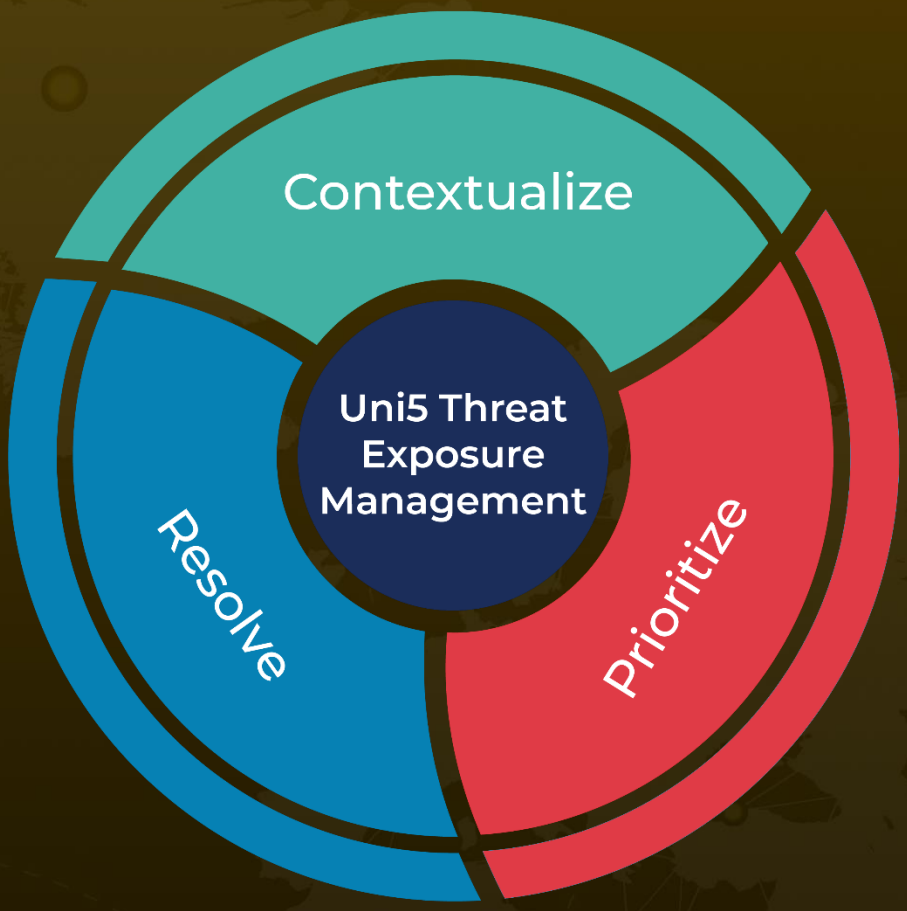
References

https://cyberint.com/blog/research/meet-uuloader-an-emerging-and-evasive-malicious-installer/

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 20, 2024 • 5:45 AM

More at www.hivepro.com