Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

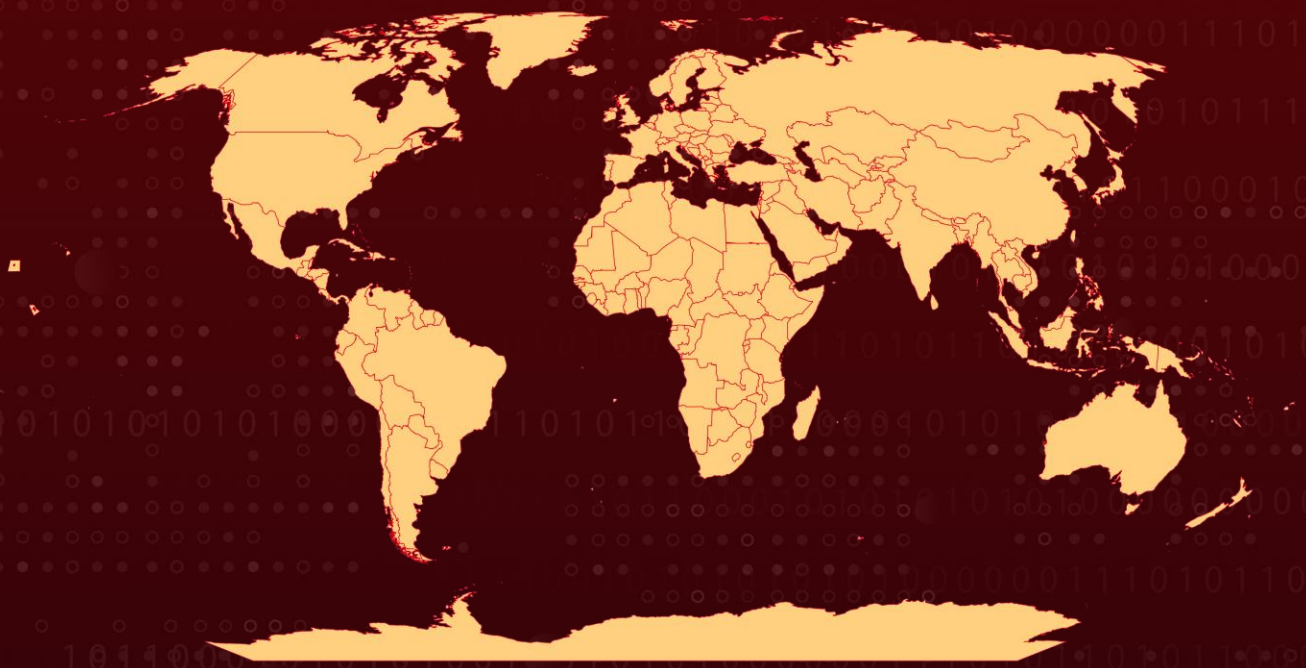
Mint Stealer: A New Python-Based Information Stealer

Date of Publication	Admiralty Code	TA Number
August 2, 2024	A1	TA2024292

Summary

First Appearance: December 12, 2022
Malware: Mint Stealer
Targeted Countries: Worldwide
Affected Platforms: Windows
Attack: The info stealer market is continuously evolving, with a recent addition being Mint Stealer. This Python-based malware is designed to steal sensitive information, including browser data and cryptocurrency wallets. To evade detection, it employs encryption and obfuscation techniques, and it uploads the stolen data to file-sharing sites. Distributed through various websites and supported via Telegram, Mint Stealer underscores the dynamic and growing threats in the threat landscape.

Attack Regions



Attack Details

#1

Mint Stealer is a Python-based information stealer that operates as Malware-as-a-Service (MaaS). Developed since December 2022 but became active in June 2023, Mint Stealer is designed to extract sensitive data from infected systems. Mint Stealer serves as a versatile tool for cybercriminals, targeting a variety of critical data sources. Its primary targets include web browsers, cryptocurrency wallets, VPN clients, and messaging applications. This allows the malware to gather a broad range of valuable information, such as login credentials, financial data, and personal communications.

#2

The attack process begins with the malware being delivered via phishing campaigns, malicious downloads, or compromised websites. Once installed on a victim's system, Mint Stealer employs advanced encryption and obfuscation techniques to avoid detection by security systems. This makes the malware difficult to identify and remove. The stolen data is collected and encrypted before being uploaded to free file-sharing sites. The malware then sends the download URLs of the stolen data to its command-and-control server, ensuring that attackers have easy access to the information while reducing the risk of interception.

#3

Mint Stealer is marketed on various platforms, including dedicated websites where it is offered for subscription prices ranging from $8 per week to $75 for three months. It is capable of extracting critical information such as web browser data, cryptocurrency wallet recovery phrases, gaming credentials, messaging app data, and VPN client information. The distribution strategy is supported by communication channels like Telegram, which are used for both marketing and technical support, highlighting the organized nature of the cybercriminal groups behind it.

#4

The emergence of Mint Stealer reflects the evolving threat landscape in cybersecurity, demonstrating how malware can become more sophisticated and accessible. To counter such threats, organizations and individuals must remain vigilant. Regular updates to antivirus software, cautious browsing practices, and awareness of phishing attempts are crucial in defending against this and similar malware threats.

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Mint Stealer, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Keep Systems Updated: Regularly update your operating system and applications to patch known vulnerabilities that malware can exploit.

Practice Safe Browsing: Avoid downloading software or clicking on links from untrusted sources. Verify the authenticity of emails and attachments before opening them.

Use Multi-Factor Authentication (MFA): Employ MFA for sensitive accounts to add an extra layer of security, making it harder for attackers to gain access even if credentials are compromised.

Regular Backups: Maintain regular backups of important data. Ensure that backups are stored securely and are not connected to your main network to prevent them from being compromised by malware.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0010 Exfiltration	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	T1566 Phishing
T1592 Gather Victim Host Information	T1204 User Execution	T1622 Debugger Evasion	T1497 Virtualization/Sandbox Evasion
T1140 Deobfuscate/Decode Files or Information	T1204.002 Malicious File	T1083 File and Directory Discovery	T1071.001 Web Protocols

T1071 Application Layer Protocol	T1041 Exfiltration Over C2 Channel	T1059 Command and Scripting Interpreter	T1047 Windows Management Instrumentation
T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow	T1055 Process Injection	T1036 Masquerading
T1003 OS Credential Dumping	T1552.002 Credentials in Registry	T1552 Unsecured Credentials	T1124 System Time Discovery
T1518.001 Security Software Discovery	T1057 Process Discovery	T1010 Application Window Discovery	T1016 System Network Configuration Discovery
T1082 System Information Discovery	T1560 Archive Collected Data	T1185 Browser Session Hijacking	T1005 Data from Local System
T1573 Encrypted Channel	T1095 Non-Application Layer Protocol		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1064ab9e734628e74c580c5aba71e4660ee3ed68db71f6aa81e30f148a5080fa, db47e673cccdbe2abb11cc07997aeabf4d2bdc9bec286674b58c6baafa09b82
Domains	mint-c2[.]top, mint-stealer[.]top, mint-c2[.]top/api/won, mint-c2[.]top/api/injection, cashout[.]pw, mint-stl[.]ru
MD5	9f037593071344bc1354e5a619f914f4, e6e620e5cac01f73d0243dc9cf684193, afefdbd2bf7a6a622eaf09ab4a1adb3b , 4629bd8e5e8cfe7256d1505e444c7db8 , c66ee818a2295aac69baa17df301de34 , ac449f08bd7edcecabfbf7c1231c02e8 , a1671d1d339b188fa3f437e79ccf21d1, 3832f42b8a1655a1ff2cce00aec7435b

TYPE	VALUE
IPv4	109[.]236[.]93[.]59, 2[.]58[.]57[.]168, 77[.]91[.]77[.]81, 104[.]21[.]94[.]45, 172[.]67[.]219[.]160, 172[.]67[.]211[.]144, 85[.]114[.]96[.]2, 104[.]21[.]96[.]39, 104[.]21[.]67[.]23, 172[.]67[.]205[.]20, 104[.]21[.]22[.]131, 185[.]216[.]70[.]231, 95[.]214[.]25[.]207, 188[.]114[.]96[.]3, 94[.]156[.]79[.]162

References

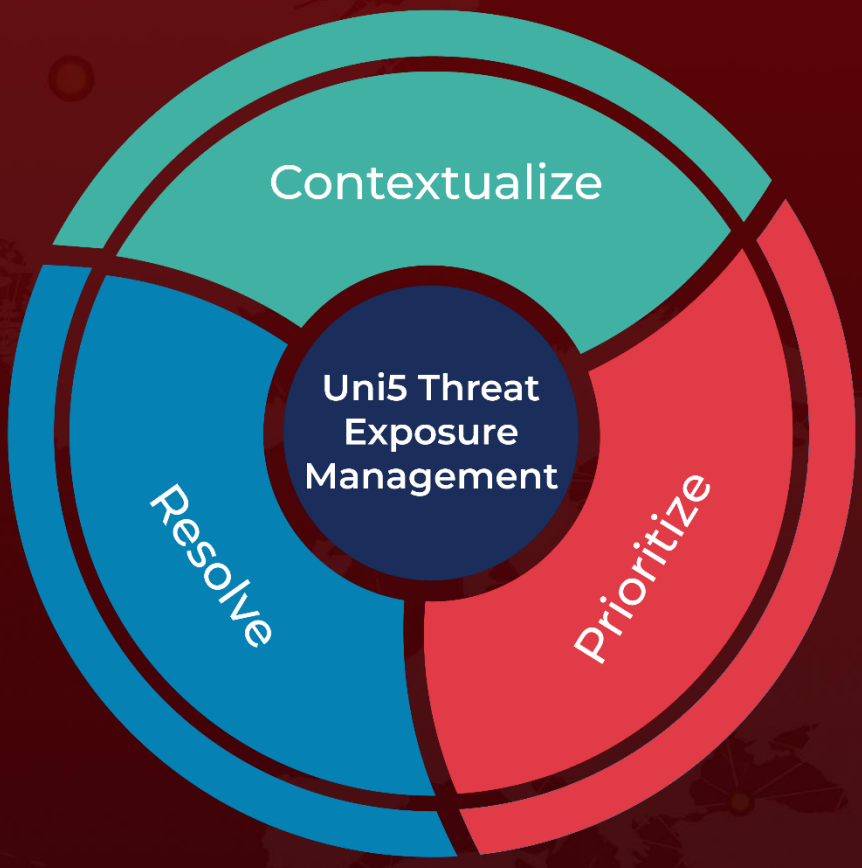
https://www.cyfirma.com/research/mint-stealer-a-comprehensive-study-of-a-python-based-information-stealer/

https://medium.com/coinmonks/mint-stealer-running-by-a-bulletproof-hoster-0983df47a411

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 2, 2024 . 6:30 AM

More at www.hivepro.com