Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

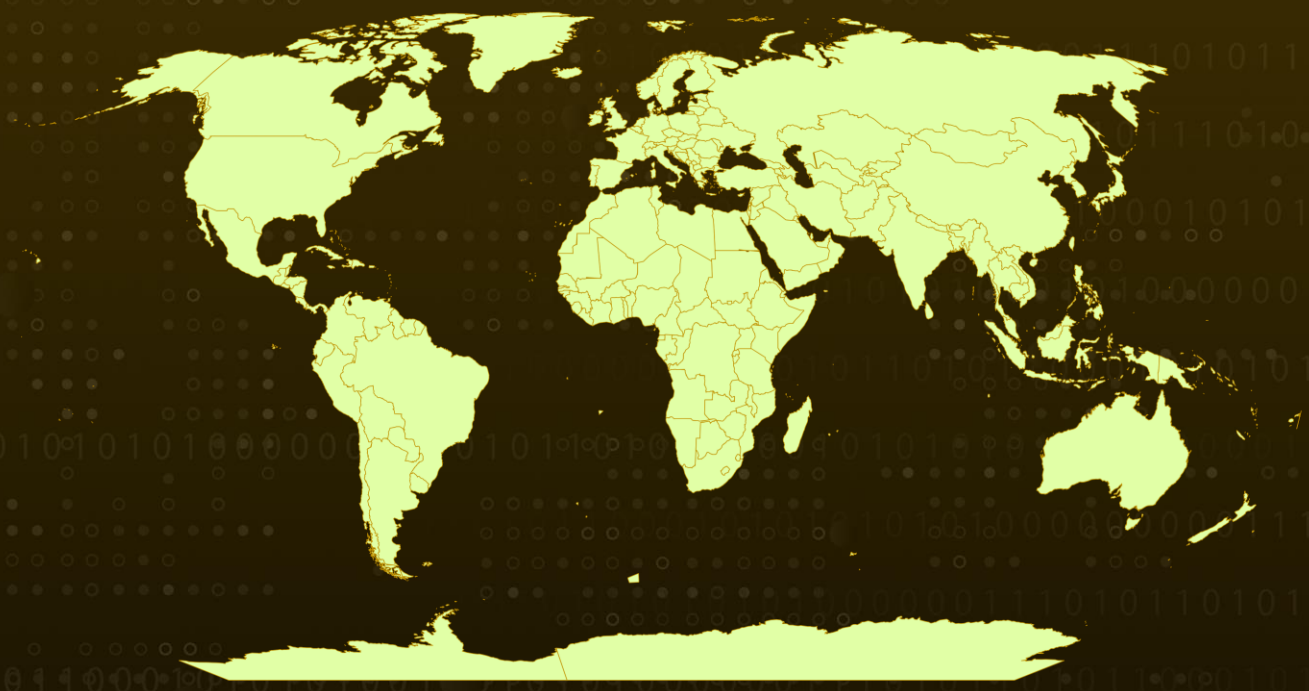
Decoding MrAnon Stealer's Plot through Deceptive Emails

Date of Publication	Admiralty Code	TA Number
December 11, 2023	A1	TA2023497

Summary

Attack Commenced: October 2023
Malware: MrAnon Stealer
Attack Region: Worldwide
Affected Platform: Microsoft Windows
Attack: A phishing email campaign employs misleading booking details to lure victims, aiming to deploy a Python-based information stealer known as MrAnon Stealer. This malicious software is designed to pilfer victims' credentials, system details, browser sessions, and cryptocurrency extensions.

Attack Regions



Attack Details

#1 A scheming email campaign employs deceptive booking details, masquerading as a legitimate company seeking hotel reservations. The subject line, "December Room Availability Query," is strategically designed to lure recipients into interacting with a malicious PDF attachment.

#2 This PDF, upon activation, initiates the download of a .NET executable file, meticulously crafted using PowerGUI. Subsequently, a PowerShell script is executed to deploy the ultimate malware payload, identified as MrAnon Stealer. Originally distributing Cstealer in July and August, the campaign transitioned to disseminating MrAnon Stealer in October and November.

#3 MrAnon Stealer is a Python-based information-stealing tool, cleverly compressed with cx-Freeze to avoid detection. cx_Freeze is a cross-platform utility, that transforms Python scripts into standalone executables compatible with specific operating systems, eliminating the need for users to install Python. MrAnon Stealer covertly collects victims' credentials, system data, browser sessions, and cryptocurrency extensions.

#4 Upon deployment, MrAnon Stealer actively identifies and terminates specific processes running on the victim's system. Using "ImageGrab," the malicious software captures a screenshot, saving it with the filename "Screenshot (Username).png." Furthermore, it establishes connections with legitimate websites to retrieve the system's IP address, country name, and country code.

#5 Following data acquisition, the malware compresses the information, secures it with a password, and designates the file as "Log (Username).zip." The compressed file is subsequently uploaded to a publicly accessible file-sharing platform.

#6 The malware then appends the download link and system details to a message transmitted to the attacker's Telegram channel via a bot token. The support channel for MrAnon Stealer actively promotes its suite of products, including MrAnon- Crypter, Stealer, and Loader, complete with a dedicated purchase page.

Recommendations

Email Security: Implement robust email filtering solutions to reduce the likelihood of spam and phishing emails reaching users' inboxes, thereby helping to filter out potentially harmful content.

Behavioral Analysis and Anomaly Detection: Incorporate behavioral analysis and anomaly detection tools to identify and stop processes initiated by the malware. Monitor for unusual system behavior, such as termination of specific processes or connections to unfamiliar websites.

Network Traffic Monitoring: Implement network traffic monitoring to detect unusual patterns or connections, especially those related to downloader URLs. Continuously monitor and analyze network activities for potential signs of a security threat.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**T1082** System Information Discovery	**T1204** User Execution
T1176 Browser Extensions	**T1036.004** Masquerade Task or Service	**T1562.001** Disable or Modify Tools	**T1036** Masquerading
T1027 Obfuscated Files or Information	**T1059.001** PowerShell	**T1569.002** Service Execution	**T1033** System Owner/User Discovery
T1053.005 Scheduled Task	**T1598.002** Spearphishing Attachment	**T1057** Process Discovery	**T1113** Screen Capture
T1560 Archive Collected Data			

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxps[:]//store1[.]gofile[.]io/uploadFile
Hostnames	anonbin[.]ir, anoncrypter[.]com

TYPE	VALUE
Path	%USERPROFILE%\AppData\Local\Temp\Quest Software\PowerGUI
SHA256	075e40be20b4bc5826aa0b031c0ba8355711c66c947bbbaf926b92edb2844cb0, 48e09b8043c0d5dfc2047b573112ead889b112108507d400d2ce3db18987f6c9, 0efba3964f4b760965e94b4d1a597e6cd16241b8c8bf77a664d6216d1420b312, 8a8c9acf09c84ab5ea4c098eace93888a88b82a1485255073c93ce6080d05ec7, 96ec8ef2338d36b7122a76b0398d97e8d0ed55c85e31649ea00e57d6b1f53628, 8b71525ca378463784ce2d81a8371714580c58f0d305a2aa4630dc964c8c0ee0, 45ee224e571d0fd3a72af1d7a7718e61a1aad03b449cf85377411d51c135bb22

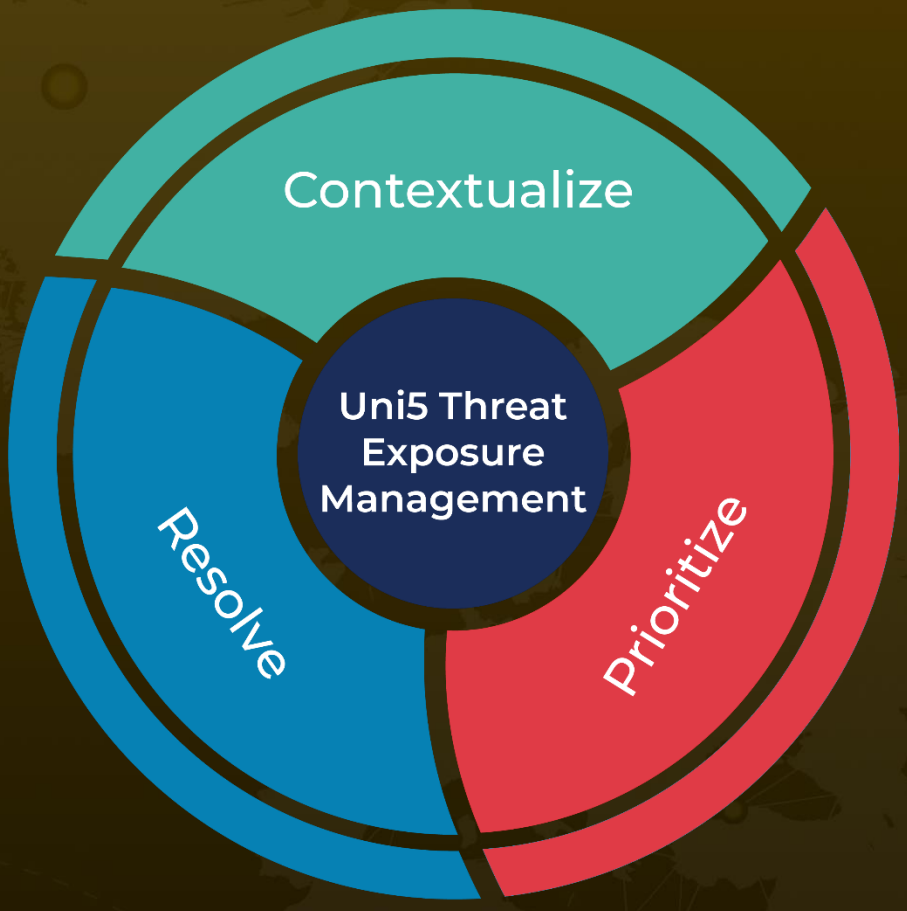
References

https://www.fortinet.com/blog/threat-research/mranon-stealer-spreads-via-email-with-fake-hotel-booking-pdf

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

December 11, 2023 • 4:00 AM

More at www.hivepro.com