Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Emansrepo: Python Infostealer with Tailored Email Exfiltration

Date of Publication	Admiralty Code	TA Number
September 5, 2024	A1	TA2024340

Summary

Attack Discovered: November 2023
Malware: Emansrepo Stealer
Impacted Users: Microsoft Windows
Attack: Emansrepo is a Python-based infostealer, first observed in November 2023, that spreads via phishing emails disguised as purchase orders and invoices. This malware primarily targets browser directories and specific file paths, collecting sensitive data from victims. The exfiltrated data is bundled into a zip file and sent directly to the attacker's email address. The stolen information could be leveraged in future attacks, potentially leading to further exploitation or data compromise.

Attack Regions

Attack Details

#1 In August 2024, security researchers identified Emansrepo, a Python-based infostealer distributed through phishing emails disguised as fake purchase orders and invoices. Active since November 2023, the malware collects data from compromised systems, compresses it into a zip file, and sends it to the attacker's email. Phishing emails usually contain an HTML file that directs recipients to download Emansrepo, packaged using PyInstaller for easy deployment on target systems.

#2 Emansrepo's attack methods have evolved to include three distinct payload delivery techniques. Chain 1 involves a fake download page that delivers a 7z file with an AutoIt-compiled executable. Chain 2 uses an HTA file embedded with JavaScript to download and execute PowerShell and VBScript, with the payload coming through a batch file. Chain 3 employs an obfuscated batch file protected by BatchShield to download and run a PowerShell script. In all cases, the final payload is a zip archive containing Python modules and `tester.py`, the malicious script designed to steal information.

#3 By July and August 2024, attackers began using multiple email accounts to receive various types of stolen data, complicating detection. Emansrepo consists of three main components. The first collects user information and text files from the Desktop, Documents, and Downloads folders. The second gathers PDF files and compresses browser extensions, cryptocurrency wallets, and gaming platform data for exfiltration. The third targets browser cookies, packaging them into a file named `{process_name}_cookies.zip`. After gathering the data, all stolen information is sent directly to the attacker via email, allowing for further exploitation or compromise.

#4 Researchers also uncovered a related campaign using Remcos malware, likely managed by the same threat actor. This attack involves DBatLoader, delivered via phishing emails, which downloads and decrypts an evolved Remcos variant. Given the increasing sophistication of threats like Emansrepo and Remcos, organizations must strengthen their cybersecurity posture to defend against these evolving attacks.

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.

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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration	T1566 Phishing
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.005 Visual Basic	T1059.006 Python
T1555 Credentials from Password Stores	T1552 Unsecured Credentials	T1552.001 Credentials In Files	T1020 Automated Exfiltration
T1217 Browser Information Discovery	T1560 Archive Collected Data	T1027 Obfuscated Files or Information	T1074 Data Staged
T1036 Masquerading	T1070 Indicator Removal	T1070.004 File Deletion	T1204 User Execution

T1048 Exfiltration Over Alternative Protocol	T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//bafybeigm3wrvmyw5de667rzdgdnct2fvwumyf6zyzybzh3tqvv5jhlx2ta[.]ipfs[.]dweb[.]link/wetrankfr[.]zip, hxxps[:]//bafybeifhhbimsau6a6x4m2ghdmzer5c3ixfztpocqqudlo4oyzer224q4y[.]ipfs[.]w3s[.]link/myscr649612[.]js, https[:]//estanciaferreira[.]com[.]br/wp-includes/TIANJIN-DOC-05082024-xls[.]7z, hxxps[:]//dasmake[.]top/reader/timer[.]php, hxxps[:]//hedam[.]shop/simple/Enquiry[.]7z
IPv4	191[.]101[.]130[.]185, 192[.]236[.]232[.]35
Email Addresses	stealsmtp[@]dasmake[.]xyz, hanbox[@]dasmake[.]xyz, publicsmtp[@]dasmake[.]xyz, publicbox[@]dasmake[.]xyz, minesmtp8714[@]dasmake[.]xyz, minestealer8412[@]dasmake[.]xyz, minesmtp8714[@]maternamedical[.]top, minestealer8412[@]maternamedical[.]top, extensionsmtp[@]maternamedical[.]top, filelogs[@]maternamedical[.]top, cookiesmtp[@]maternamedical[.]top, cooklielogs[@]maternamedical[.]top
SHA256	a6c2df5df1253f50bd49e7083fef6cdac544d97db4a6c9c30d7852c4fd651921, 9e5580d7c3c22e37b589ec8eea2dae423c8e63f8f666c83edabecf70a0948b99, 9bd3b8d9ac6ad680b0d0e39b82a439feedd87b9af580f37fa3d80d2c252fef8c, 915bad0e2dbe0a18423c046f84d0ff7232fff4e5ba255cc710783f6e4929ab32, 64e5c9e7b8dfb8ca8ca73895aa51e585fa7e5414f0e1d10659d3a83b9f770333, b343cce5381b8633b3fd3da56698f60db70c75422e120235a00517d519e37d8d,

TYPE	VALUE
SHA256	32bcbce53bfee33112b447340e7114d6d46be4ccf1a5391ad685431afdc8fb86, bee8da411e71547ac765a5e63e177b59582df438432cc3b540b57a6f1a56dd16, 70ba3d67b476e98419ecbbbb5d81efcb5a07f55a92c96e7b9207176746e3b7a6, a2fa6790035c7af64146158f1ed20cb54f4589783e1f260a5d8e4f30b81df70d, 4cd8c9fa7f5e2484b73ed9c7be55aa859969c3f21ca2834610102231d337841d, 6670e5c7521966e82d091e7adff4e16335f03f2e2740b653adcc9bfe35c7bf9b, dd656953a6844dd9585f05545a513c4e8c2ded13e06cdb67a0e58eda7575a7a4, 9866934dd2b4e411cdabaa7a96a63f153921a6489f01b0b40d7febed48b02c22, e346f6b36569d7b8c52a55403a6b78ae0ed15c0aaae4011490404bdb04ff28e5, 8e43c97e5bc62211b3673dee13e376a1f5026502ebe9fd9f7f455dc17c253b7f, ae2a5a02d0ef173b1d38a26c5a88b796f4ee2e8f36ee00931c468cd496fb2b5a, 7a9826be22b6d977d6a0e5179f84d8e88b279fe6d9df8f6c93ebc40a6ba70f06, 18459be33cd4f59081098435a0fbaa649f301f985647a75d21b7fc337378e59b, 6e7313b6aa37a00b602e620a25a0b71a74503ea967f1814c6c7b8b192535a043, 222dd76c461e70c3cb330bacfcf465751b07331c4f8a4415c09f4cd7c4e6fcd9, 6e7313b6aa37a00b602e620a25a0b71a74503ea967f1814c6c7b8b192535a043

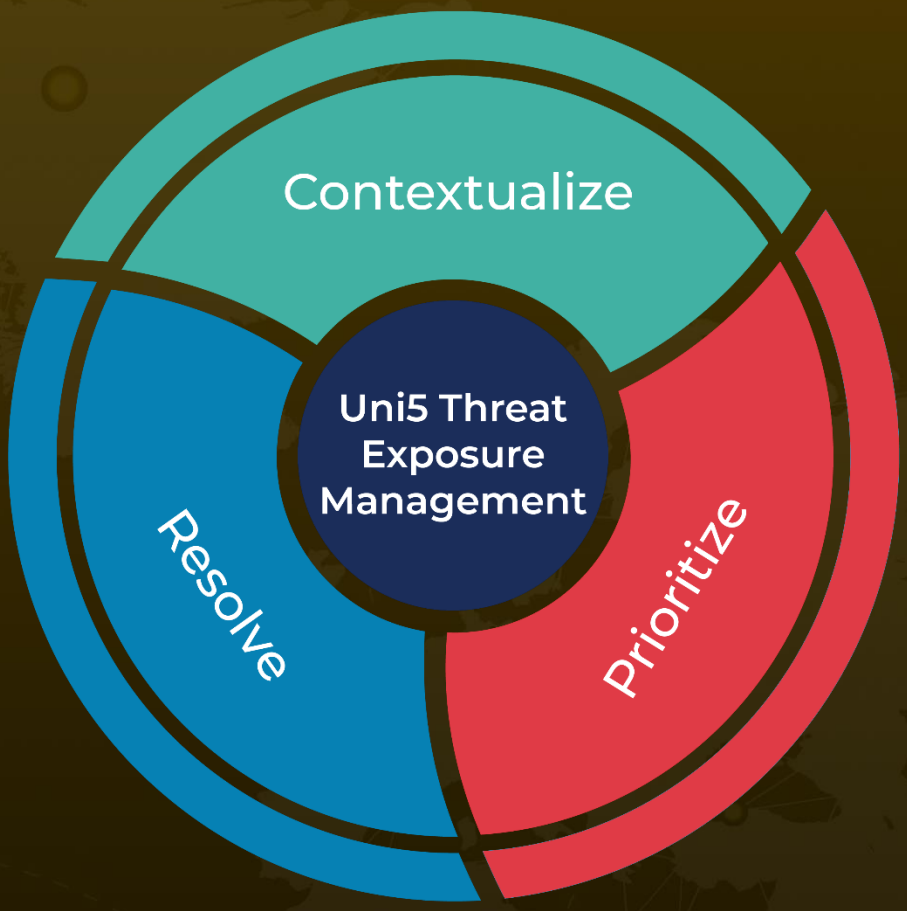
References

https://www.fortinet.com/blog/threat-research/emansrepo-stealer-multi-vector-attack-chains

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

September 5, 2024 • 7:30 AM

More at www.hivepro.com