Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

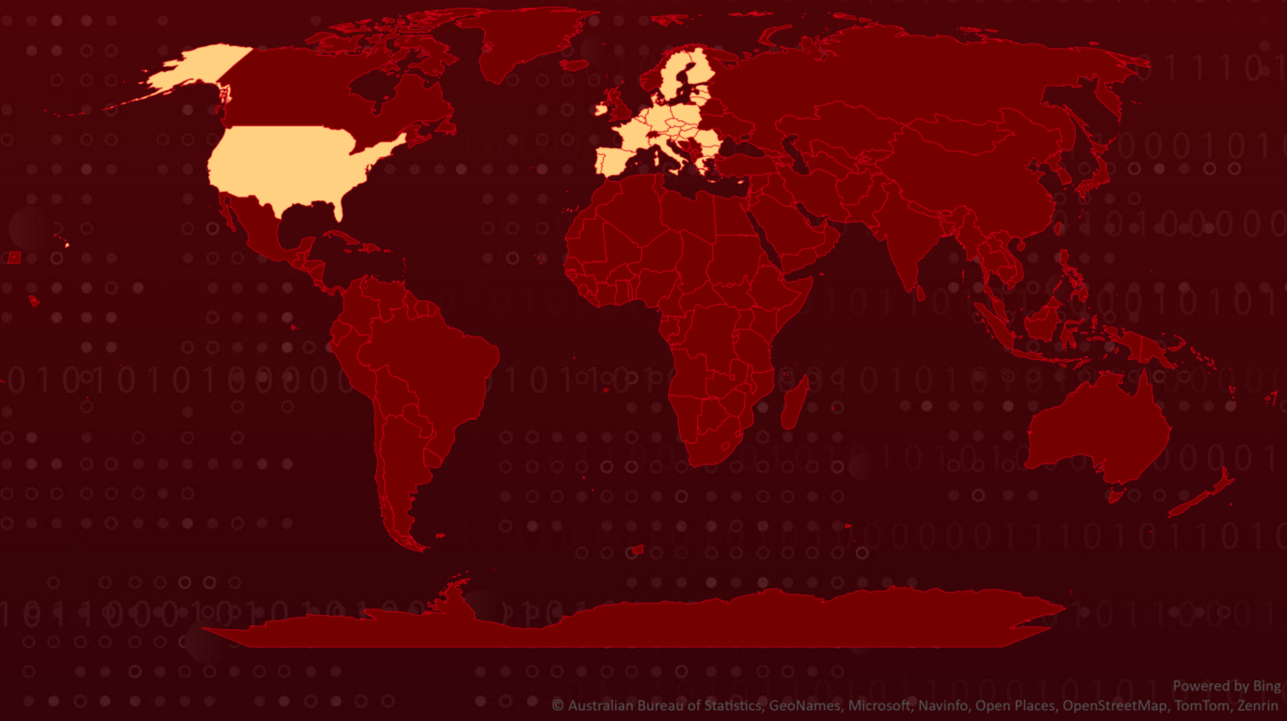
StrelaStealer Resurfaces with Upgraded Attack Chain

Date of Publication	Admiralty Code	TA Number
March 26, 2024	A1	TA2024118

Summary

First Discovered: November 2022
Attack Region: EU and U.S.
Affected Industries: High Tech, Finance, Professional and Legal Services, Manufacturing, State and Local Government, Utilities and Energy, Insurance, Construction
Malware: StrelaStealer
Attack: A recent wave of phishing attacks has been detected, targeting over 100 organizations across the United States and the European Union. These attacks aim to distribute StrelaStealer, a dynamic information-stealing malware. The attackers employ spam emails containing attachments that ultimately initiate the StrelaStealer DLL payload.

Attack Regions


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

A new surge of phishing attacks has been identified, aiming to distribute StrelaStealer, a rapidly evolving information-stealing malware. These campaigns have impacted approximately 100 organizations across the United States and the European Union. The significant large-scale campaign occurred in November 2023. However, threat actors behind StrelaStealer intensified their efforts in early 2024, targeting businesses in the same regions with another large-scale campaign.

#2

StrelaStealer, an email credential theft malware, was initially discovered in November 2022. It is notorious for its capability to steal email login credentials from well-known email clients and send them to an attacker-controlled server. The latest iteration of StrelaStealer features an improved DLL payload obfuscation technique and is disseminated through a compressed JScript file. Despite these updates, the payload DLL remains identifiable by its "strela" string and continues to align closely with its core objective.

#3

In previous attack chains, the malware was distributed through email attachments in the form of an ISO file, which contained both an HTML page and a .lnk file. The HTML file utilized rundll32.exe to execute the embedded StrelaStealer payload. However, in a recent campaign, StrelaStealer has been observed spreading through ZIP file attachments in emails. Upon extraction, a JScript file is dropped onto the victim's system.

#4

The JScript file further fetches StrelaStealer as a Base64-encoded payload along with a batch file. Encoded payload is decoded and executed via rundll32.exe. In latest version of StrelaStealer, introduced in the January 2024 campaign, the packer has been updated to utilize a control flow obfuscation method.

#5

StrelaStealer malware poses a persistent threat in the realm of email credential theft by continuously updating its attachments and DLL payloads to evade detection. While its core functionality remains consistent, it employs various evasion techniques and undergoes frequent updates, rendering it a significant and persistent threat in the current threat landscape.

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	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0009 Collection	TA0010 Exfiltration	T1497 Virtualization/Sandbox Evasion
T1114 Email Collection	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1027 Obfuscated Files or Information
T1140 Deobfuscate/Decode Files or Information	T1566 Phishing	T1566.001 Spearphishing Attachment	T1204 User Execution
T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1041 Exfiltration Over C2 Channel
T1218 System Binary Proxy Execution	T1218.011 Rundll32	T1003 OS Credential Dumping	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0d2d0588a3a7cff3e69206be3d75401de6c69bcff30aa1db59d34ce58d5f799a, e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1, f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f5619b30f3a2e, aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054, b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680, 3189efaf2330177d2817cfb69a8bfa3b846c24ec534aa3e6b66c8a28f3b18d4b, 544887bc3f0dccb610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45
IP	193[.]109[.]85[.]231

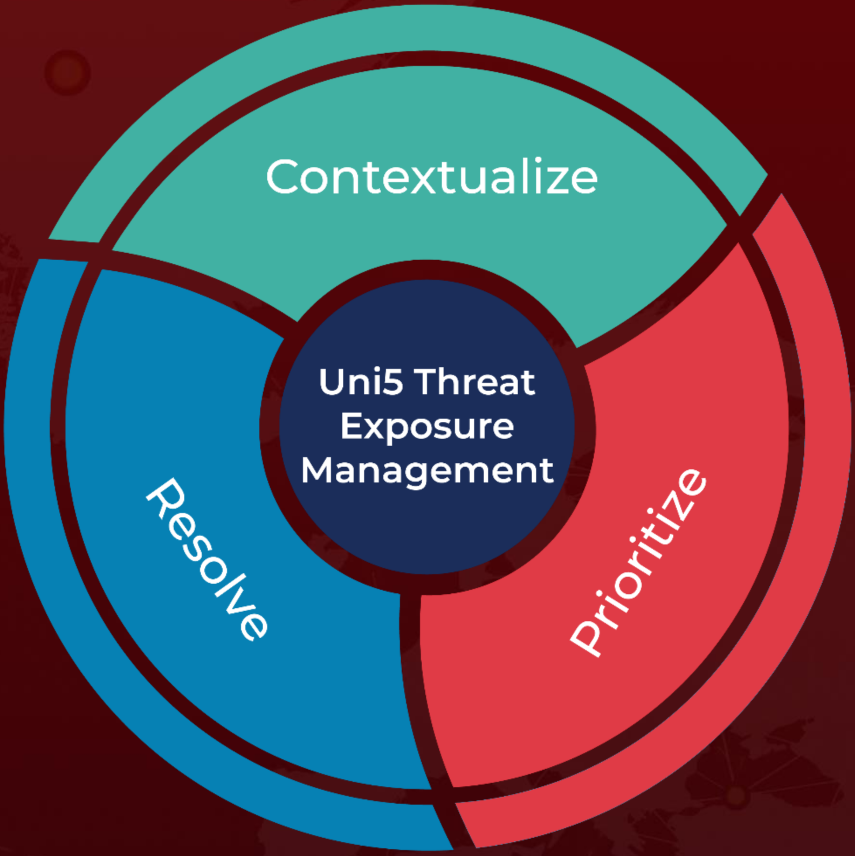
References

https://unit42.paloaltonetworks.com/strelastealer-campaign/

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

March 26, 2024 • 6:45 AM

More at www.hivepro.com