Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

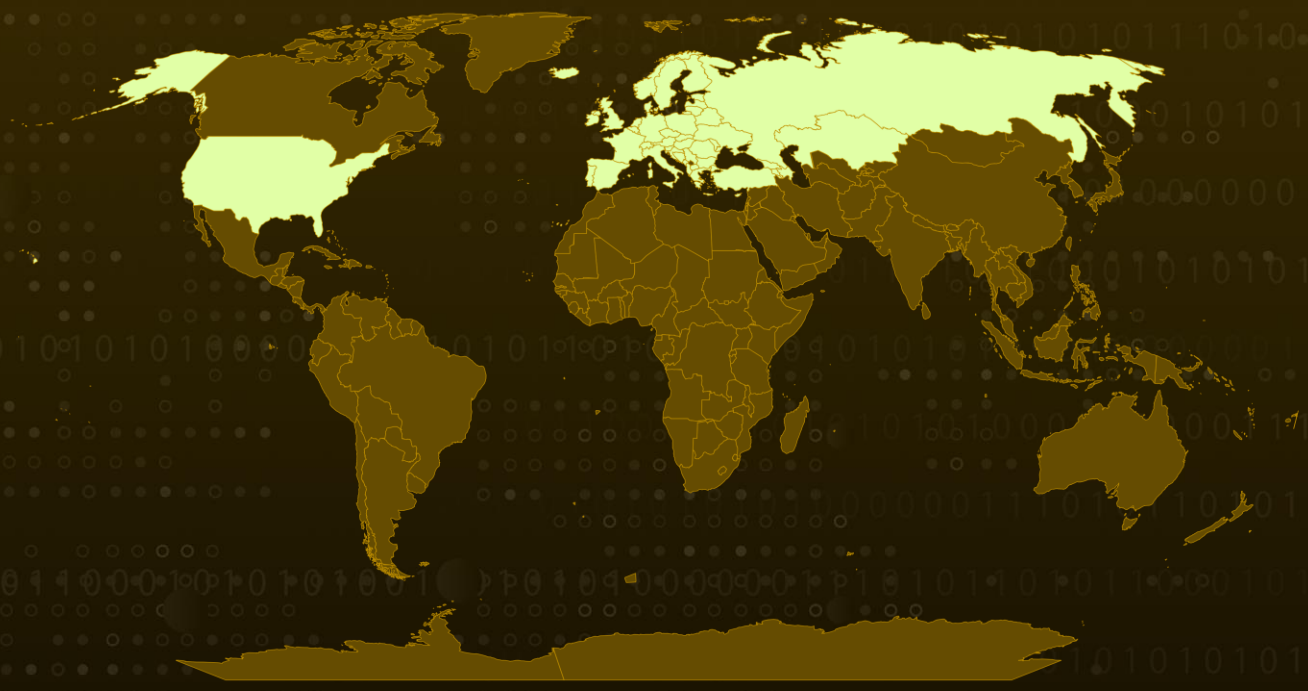
Malevolent EvilExtractor Stealer Attacks Strike Europe and US

Date of Publication	Admiralty Code	TA Number
April 26, 2023	A1	TA2023199

Summary

Attack Began: March 30, 2023
Malware: EvilExtractor (also spelled Evil Extractor)
Affected Product: Microsoft Windows
Attack Region: Europe and US
Attack: A novel type of comprehensive malware called EvilExtractor has emerged in the cybercriminal marketplace. This malicious software is specifically designed to extract sensitive information and files from Windows operating systems. EvilExtractor has gained notoriety in Europe and the United States due to a recent increase in attacks.

Attack Regions



Attack Details

#1

EvilExtractor is a novel type of malware that functions as an all-in-one stealer, allowing cybercriminals to extract sensitive information and files from Windows operating systems. The malicious software is equipped with multiple modules that operate via an FTP service, making it a powerful tool for targeted attacks on endpoint devices.

#2

Despite being marketed by its developer, Kodex, as a legitimate subscription-based service for $59 per month, EvilExtractor has gained notoriety in the cybersecurity community for its use by threat actors, who have reportedly been promoting it on various hacking forums since 2022.

#3

On March 30, 2023 a phishing email campaign was discovered to be distributing the EvilExtractor malware. The malicious software disguises itself as legitimate files, such as Adobe PDF or Dropbox files, but upon execution, it deploys PowerShell-based malicious activities. In addition, it is equipped with environment checking and Anti-VM features.

#4

The primary objective of EvilExtractor is to extract browser data and other sensitive information from compromised endpoints and upload it to the attacker's FTP server. When the target attempts to open the file, a PyInstaller file is triggered, which launches a .NET loader that executes a base64-encoded PowerShell script, ultimately launching the EvilExtractor executable.

#5

It is important to note that EvilExtractor also possesses a ransomware function, which is incorporated into the .Net loader. The module, known as the "Kodex ransomware," can download a file from the evilextractor[.]com domain.

Recommendations

To safeguard against EvilExtractor attacks, businesses should stay alert and implement necessary measures. Regular phishing simulations, education, and awareness training are vital, but they may not fully consider MFA fatigue and web browser hygiene.

It is crucial to integrate and communicate all learned lessons. Also, verifying the authenticity of email attachments and untrusted links before opening them is crucial to prevent attacks.

Regularly back it up offline to protect critical data and install reliable anti-virus and internet security software on all connected devices. Enable automatic software updates whenever possible and practical. Additionally, consider implementing proactive security measures, such as blocking indicators of compromise (IoCs), to stay ahead of potential threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0011 Command and Control	TA0040 Impact	T1059 Command and Scripting Interpreter
T1566 Phishing	T1486 Data Encrypted for Impact	T1056 Input Capture	T1127 Trusted Developer Utilities Proxy Execution
T1055 Process Injection	T1001 Data Obfuscation	T1059.001 PowerShell	T1059.006 Python
T1129 Shared Modules	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1140 Deobfuscate/Decode Files or Information
T1497 Virtualization/Sandbox Evasion	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1027 Obfuscated Files or Information
T1003 OS Credential Dumping	T1057 Process Discovery	T1082 System Information Discovery	T1005 Data from Local System
T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol	T1105 Ingress Tool Transfer	T1010 Application Window Discovery
T1016 System Network Configuration Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery	T1027.002 Software Packing

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	352efd1645982b8d23a841107007c8b4b024eb6bb5d6b312e5783ce4aa62b685 023548a5ce0de9f8b748a2fd8c4d1ae6c924c40acbde32e9599c868115d11f4e 75688c32a3c1f04df0fc02491180c8079d7fdc0babed981f5860f22f5e118a5e 826c7c112dd1ae80469ef81f5066003d7691a349e6234c8f8ca9637b0984fc45 b1ef1654839b73f03b73c4ef4e20ce4ecdef2236ec6e1ca36881438bc1758dcd 17672795fb0c8df81ab33f5403e0e8ed15f4b2ac1e8ac9fef1fec4928387a36d
IPV4	45[.]87[.]81[.]184 193[.]42[.]33[.]232
Domain	evilextractor[.]com

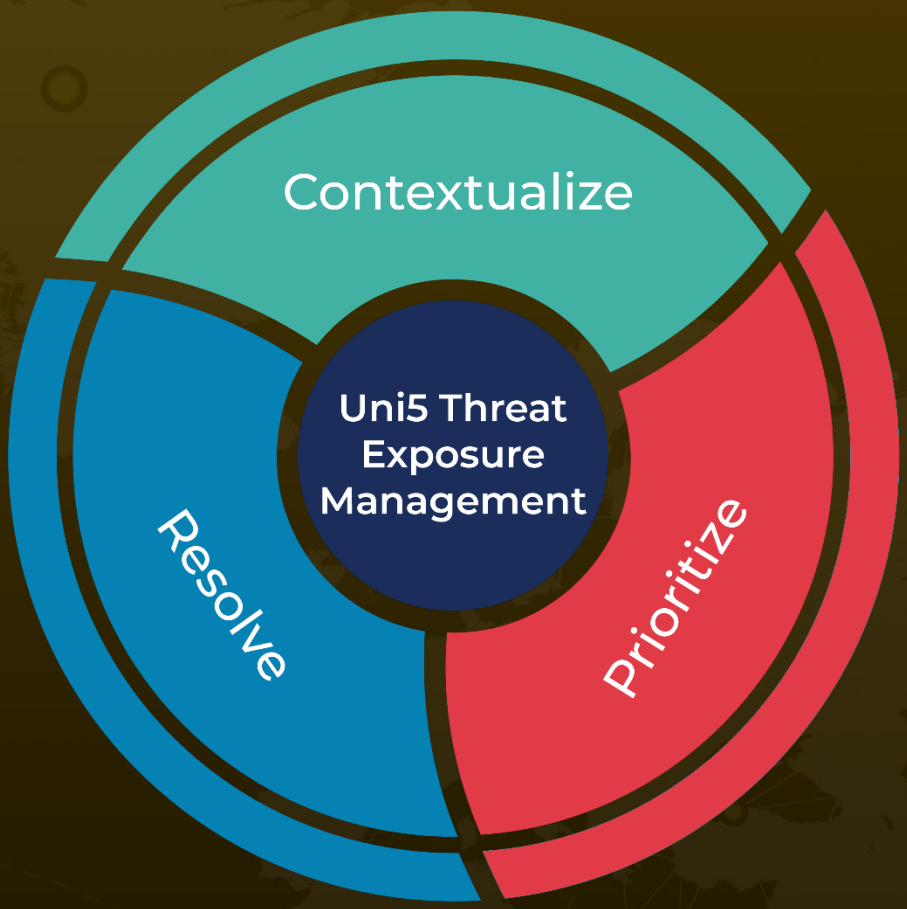
References

https://www.fortinet.com/blog/threat-research/evil-extractor-all-in-one-stealer

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

April 26, 2023 • 6:17 AM

More at www.hivepro.com