Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

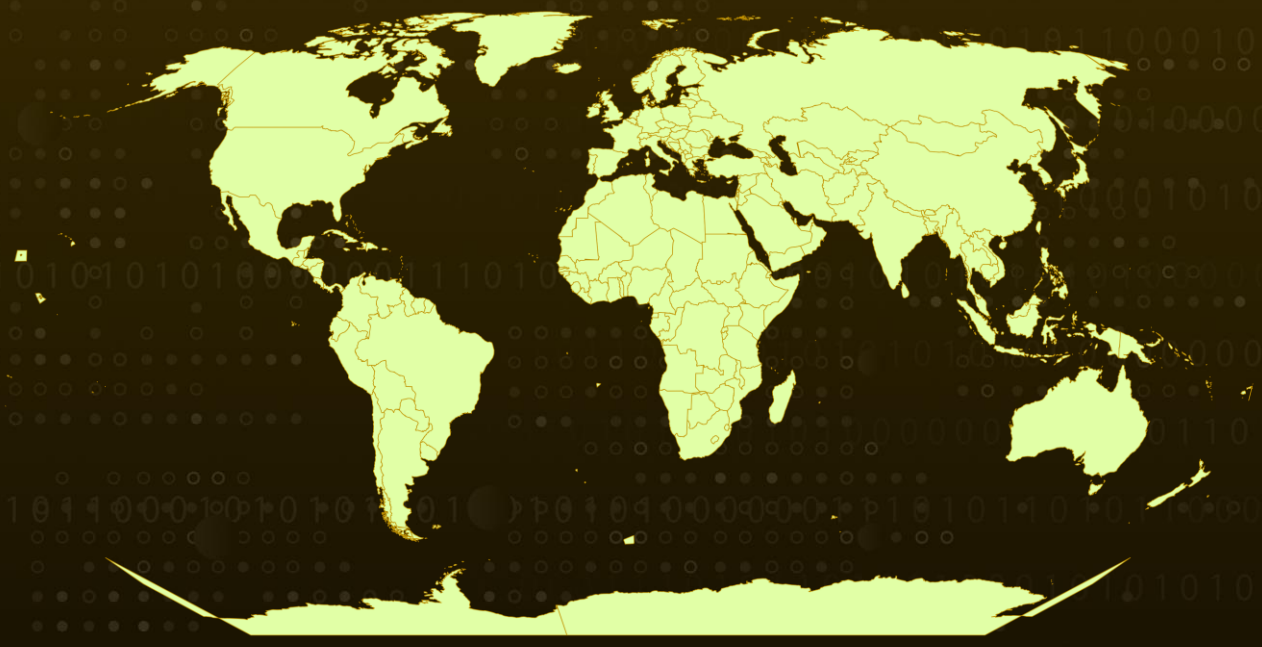
ExelaStealer: A New Entrant in the InfoStealer Landscape

Date of Publication	Admiralty Code	TA Number
October 25, 2023	A1	TA2023432

Summary

First appeared: August 2023
Malware: ExelaStealer
Attack Region: Worldwide
Affected Platform: Windows
Attack: ExelaStealer is a newly discovered InfoStealer malware that emerged in August 2023. Its distinctive feature lies in being an open-source tool, customizable for a fee. Primarily coded in Python, ExelaStealer can integrate other languages like JavaScript as needed. Its primary target is Windows-based systems, and its main purpose is to clandestinely acquire a broad spectrum of sensitive data, including passwords, credit card information, cookies, sessions, and keystrokes. One of its notable features is its extensive use of anti-debugging and anti-virtual machine techniques, enhancing its effectiveness as a tool for threat actors.

Attack Regions



Attack Details

#1 ExelaStealer is a relatively new InfoStealer malware that came to light in 2023. It's notable for being open-source and customizable for a fee. The malware is primarily coded in Python, but it can utilize other programming languages like JavaScript as necessary. It primarily focuses on Windows-based systems as its target and is designed to pilfer a wide range of sensitive information, including passwords, credit card details, cookies, sessions, and keystrokes.

#2 Advertising for ExelaStealer on the Dark Web is segmented into two offerings: an open-source version and a customized paid version. The prices for the paid version can vary based on the specific features included. ExelaStealer's open-source nature allows individuals with the requisite skills to compile their own ExelaStealer binary using the freely accessible source code. The primary file for this InfoStealer is "Exela.py," and it's obfuscated using "obf.py" to increase its complexity and make it more challenging to analyze.

#3 The ExelaStealer also detects processes and system settings related to debugging or virtualization. It collects the system's UUID and computer name, compares it against predefined lists, and terminates if a match is found. It also scans running processes and checks for specific files, strings, and process names to evade detection and analysis.

#4 In the recent campaign, one of the binaries containing ExelaStealer is named "sirket-ruhsat-pdf.exe." This binary is designed to appear as a counterfeit Turkish vehicle registration certificate. Upon execution of this binary, it initiates a sequence of actions include collecting system information, taking screenshots, copying data from the Clipboard, and exporting WLAN profiles. Subsequently, this gathered data is transmitted to the attacker through a Discord webhook. Notably, ExelaStealer was also found to steal session details from a variety of applications, including popular social media platforms and gaming platforms.

#5 The specific infection method employed by ExelaStealer has not been conclusively determined, but it could potentially utilize various techniques common in malware delivery, including phishing, watering holes, or other tactics. Its open-source nature makes it even more potent, as individuals with the necessary skills can freely customize and adapt it to suit their specific needs, potentially resulting in various customized variants.

Recommendations

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.

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.

Monitor Network Traffic: Use network monitoring tools to keep an eye on your network for unusual or suspicious activity. This can help detect infostealer attempts.

Limit User Privileges: Follow the principle of least privilege. Users and systems should have only the minimum permissions necessary to perform their tasks. This reduces the potential damage an infostealer can do.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
T1566 Phishing	T1059 Command and Scripting Interpreter	T1059.006 Python	T1059.001 PowerShell
T1518 Software Discovery	T1518.001 Security Software Discovery	T1189 Drive-by Compromise	T1005 Data from Local System
T1056 Input Capture	T1113 Screen Capture	T1497 Virtualization/Sandbox Evasion	T1547 Boot or Logon Autostart Execution
T1027 Obfuscated Files or Information			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f96bc306a0e3bc63092a04475dd4a1bac75224df242fa9fca36388a1978ce048, 95d860570b2777d7af213f9b48747d528251facada54842d7a07a5798fcbfe51, 5aff2c5e65d8e4e7fa0b0c310fbaef1e1da351de34fa5f1b83bfe17eeabac7ef, 34dca3c80cd5125091e6e4de02e86dcc6a2a6f9900e058111e457c9bce6117c0, c56b23602949597352d99aff03411d620b7a5996da2cab91368de275dcfbaa44, b9bc445af6729a95599f1a39e37f559f3ca18dbbc8ae4e60263af565ef4f4db3, 882484b56ad4418786852f401b1b81f31030bec8566b6b07c9798d4ea3033516, ccb1337383351bb6889eb8478c18c0142cb99cbb523acc85d0d626d323f5d7ad, d8488f93b8c096838b3d9b335091216667ce4ffc7ae2cf3c8925271f0f190c11, b6ca47065e68aebb007657ff0e6b0dfa0fc4e19823f336ab73f42b25dd5cfc22, 206278545b897a7e2ebb1ec4687e6ec31d7ca8f1828792a34f4fca745db8e3d4, 53b1b3c6f73312cdae7be69d16a42d298fae0cb3721c7fc11252f65b10f5a323, 2db54628a877ab40463a128496cb94523ccae6186d1648c6f372c719f6ed8152
URL	hXXps://discord[.]com/api/webhooks/1139506512302194789/X_VYZdAHscWQNKWvya9KWqqqTK6UjVvS86_kUy8P8OyCcPhKykCQpEqf93S_qDFVuzp8

References

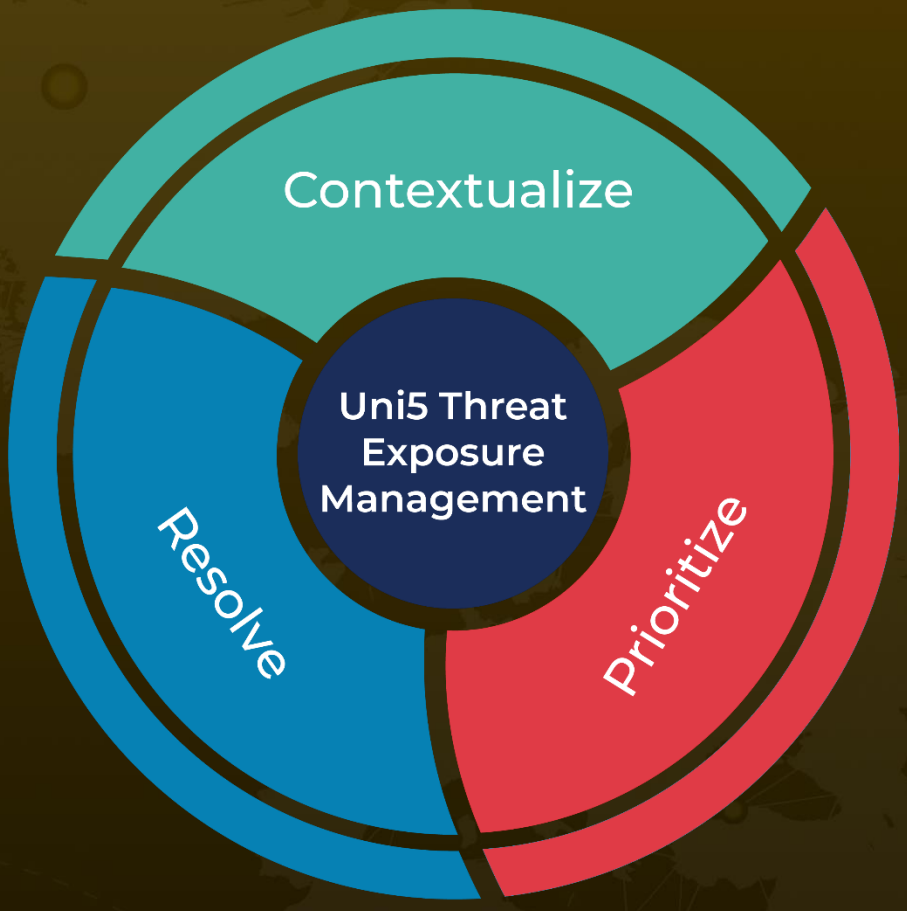
https://www.fortinet.com/blog/threat-research/exelastealer-infostealer-enters-the-field

https://cyble.com/blog/exela-stealer-spotted-targeting-social-media-giants/

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

October 25, 2023 . 5:55 AM

More at www.hivepro.com