Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

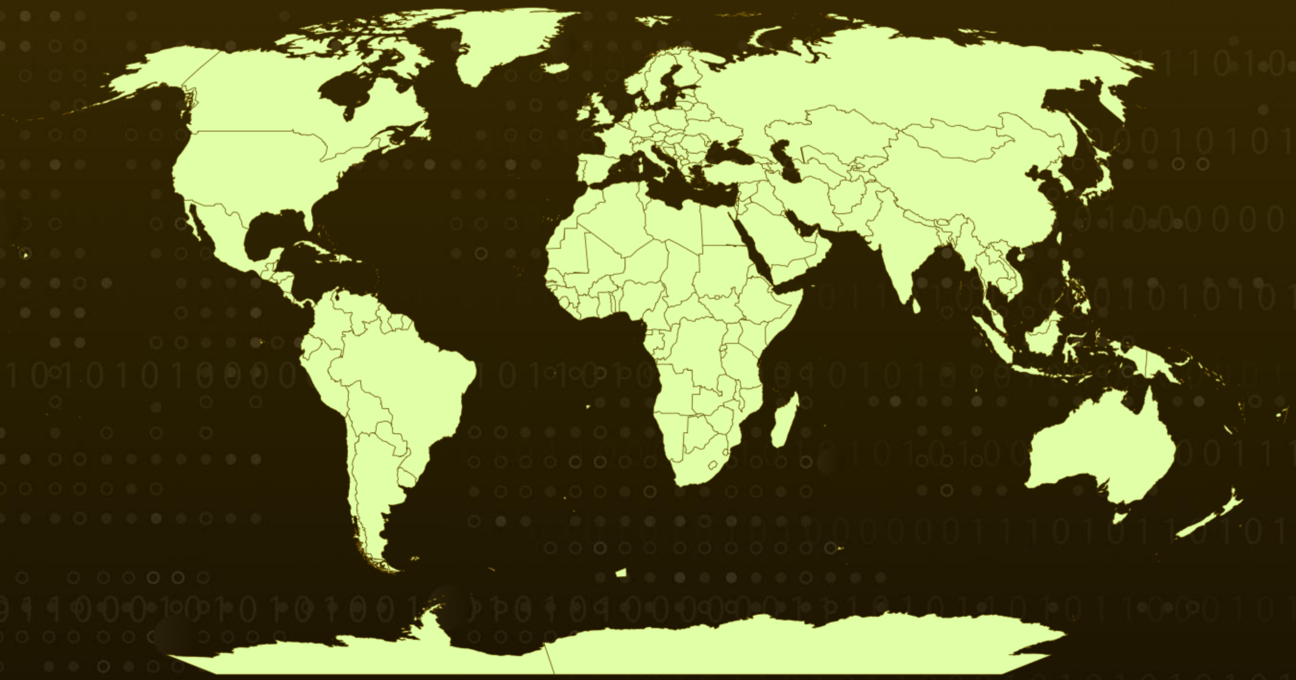
Icarus a Versatile Infostealer with Rootkit and hVNC Capabilities

Date of Publication	Admiralty Code	TA Number
February 23, 2023	A1	TA2023099

Summary

First appeared: July 2022
Attack Region: Worldwide
Attack: The Icarus Stealer malware is equipped with a Hidden Virtual network computing (hVNC) feature, which enables the attacker to generate a concealed desktop and traverse the compromised system without any contact with the primary desktop. Furthermore, Icarus Stealer is considerably less expensive than other widely used infostealers available on the dark web.

Attack Regions



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

Attack Details

#1

Icarus Stealer has numerous functionalities that include bypassing 2FA, using a rootkit with hVNC to create a hidden desktop for navigating through the computer system without affecting the primary desktop, establishing an encrypted connection, employing XOR/AES payload encryption, using a fake login page, deploying a shellcode payload, exporting the payload as a macro, implementing the RunPE (process hollowing technique), stealing data from Telegram and Discord, recovering passwords, and more.

#2

The Payload Builder is a primary functionality of Icarus Stealer that enables an attacker to manually specify the listener port for maintaining a constant connection with infected machines. With the rootkit capability, the main stealer payload can run as a concealed process. Upon execution with rootkit capabilities, the stealer initially retrieves the rootkit and installation module. Compared to Redline Stealer and Raccoon Stealer, Icarus Stealer is significantly less expensive, with a monthly fee of $79.99 and lifetime access priced at $899.99. Additionally, other users distribute the Stealer on Telegram channels.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	T1204 User Execution	T1204.002 Malicious File
T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1546 Event Triggered Execution	T1546.010 AppInit DLLs
T1546 Event Triggered Execution	T1546.015 Component Object Model Hijacking	T1548 Abuse Elevation Control Mechanism	T1548.002 Bypass User Account Control
T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks	T1036 Masquerading	T1036.004 Masquerade Task or Service
T1622 Debugger Evasion	T1055 Process Injection	T1057 Process Discovery	T1518 Software Discovery
T1082 System Information Discovery			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	8d54e4abe1762f96134a0c874cfb8cdc bf2ac81c25ebc55e88af9233c6c0e1b5 735ad7684fdb6230972cf600980c0392 348bf87a67949890a3b6229cae3f767d f09903496c341436ce74625bbaafeb81 a532918af845ed035c6882d6ae173d03
IPV4	193.31.116[.]239
URLs	hxxp://193.31.116[.]239/crypt/public/Update_Downloads/AdvKillBot.jpg hxxp://193.31.116[.]239/crypt/public/Update_Downloads/bb.jpg

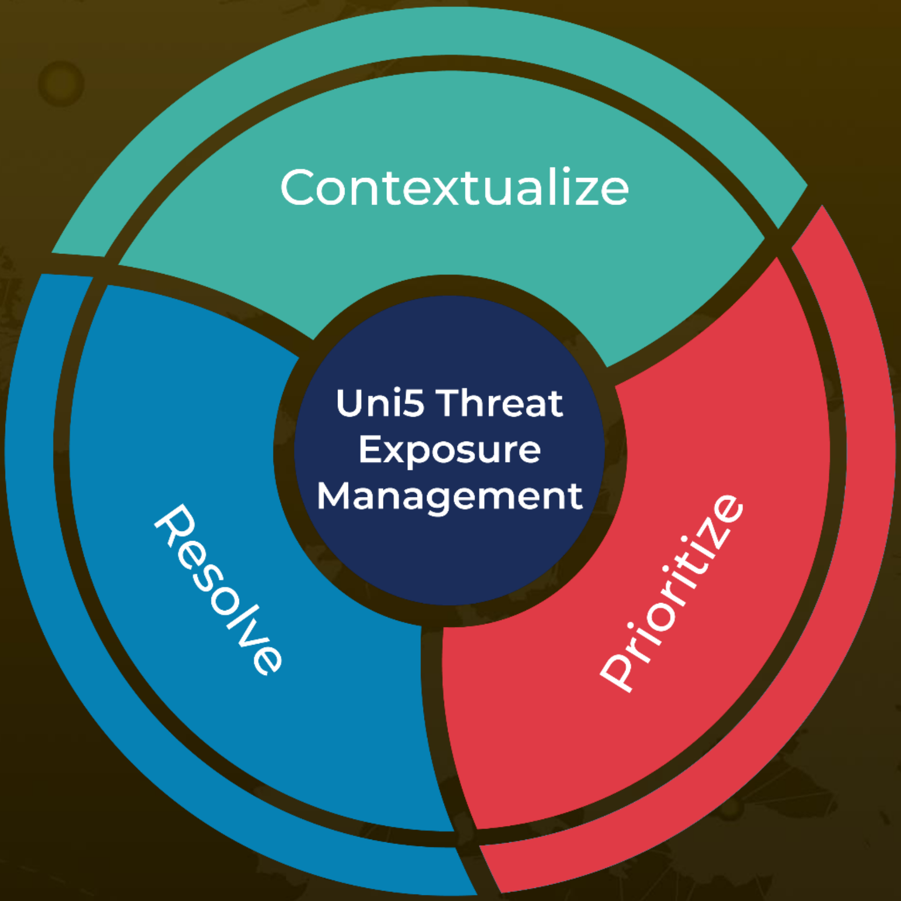
References

https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-icarus-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

February 23, 2023 • 2:45 AM

More at www.hivepro.com