Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Information Stealer LummaC2 Targets Browsers and Crypto Wallets

Date of Publication	Admiralty Code	TA Number
January 9, 2023	A1	TA2023012

Summary

First appeared: August 2022
Attack Region: Worldwide
Attack: LummaC2 Information stealer is been sold on Russian website.

Attack Regions

Attack Details

#1

LummaC2 Stealer is an information stealer that targets Chromium and Mozilla-based browsers. It is designed to steal sensitive information from a victim's machine, including crypto wallets, extensions, and two-factor authentication (2FA). The malware is sold on a Russian website for prices ranging from $250 to $20000. The creators of LummaC2 Stealer have also created two Telegram channels in Russian for sharing information about the stealer and reporting bugs.

#2

Upon execution, the stealer extracts various pieces of information from the system, including hardware and system details, and stores this information in the memory. It also searches for and steals sensitive information from installed browsers, crypto wallets, and 2FA extensions. The stolen data is encrypted and sent to a command-and-control server. The stolen information can be used by threat actors to steal cryptocurrencies or sold to other threat actors for financial gain.

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

TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1140 Deobfuscate/Decode Files or Information	T1562 Impair Defenses	T1083 File and Directory Discovery
T1005 Data from Local System	T1071 Application Layer Protocol	T1020 Automated Exfiltration	T1082 System Information Discovery
T1119 Automated Collection			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1995a54dba0e05d80903d3d210c1e3da a09daf5791d8fd4b5843cd38ae37cf97 5aac51312dfd99bf4e88be482f734c79 c9c0e32e00d084653db0b37a239e9a34
SHA1	b97965e4a793ec0fa10abc86d0c6be5718716d8a 9ac88b93fee8f888cabc3d0c9d81507c6dad7498 2c11592f527a35c3dac75139e870dd062b12dfe1 c43316ddcb51e143ab53f996587c23ea4985f6ea
SHA256	277d7f450268aeb4e7fe942f70a9df63aa429d703e9400370f06 21a438e918bf 60247d4ddd08204818b60ade4bfc32d6c31756c574a5fe2cd52 1381385a0f868 9b742a890aff9c7a2b54b620fe5e1fcfa553648695d79c892564d e09b850c92b d932ee10f02ea5bb60ed867d9687a906f1b8472f01fc5543b06f 9ab22059b264
IPV4	195[.]123[.]226[.]91 144[.]76[.]173[.]247

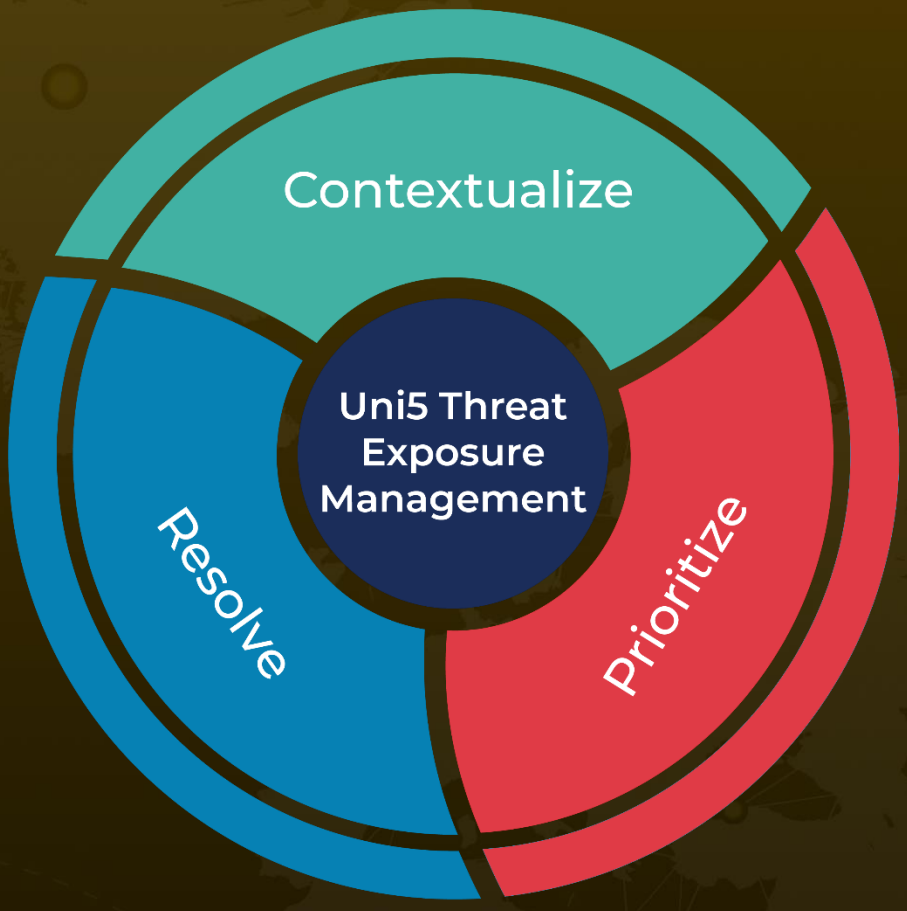
References

https://blog.cyble.com/2023/01/06/lummac2-stealer-a-potent-threat-to-crypto-users/

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

January 9, 2023 • 1:45 AM

More at www.hivepro.com