Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

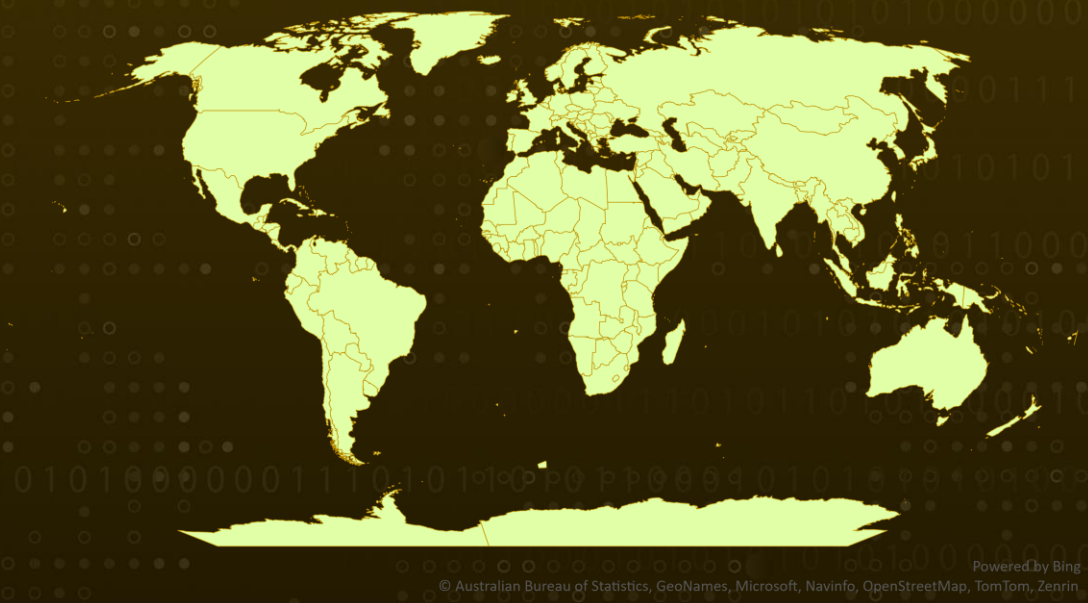
Unveiling the Malicious Tactics of LokiBot Malware

Date of Publication	Admiralty Code	TA Number
March 6, 2023	A1	TA2023118

Summary

First Appeared: 2015
Attack Region: Worldwide
Attack: LokiBot is a constantly evolving information-stealing malware that creates a backdoor on infected machines to collect sensitive data, and it uses ISO files and API hashing techniques to bypass detection and inject malicious code.

Attack Regions



Attack Details

#1

LokiBot is a notorious information-stealing malware that collects sensitive data from web browsers, email clients, FTP servers, and crypto wallets. The malware can create a backdoor on the infected machine, enabling an attacker to install further malicious software. In 2022, researchers identified a particular HTTP payload as malicious and found that it belonged to a LokiBot infection. The malware was delivered via an ISO file attached to a ZIP file in an email related to a business email compromise (BEC) campaign.

#2

During the end of 2022, the number of LokiBot occurrences peaked in the last three days of December, likely due to increased attack efforts during holidays. The malware uses process hollowing and API hashing techniques to inject malicious code and retrieve export functions from loaded libraries, respectively. Attackers use the ISO file format to bypass malspam detection technologies that usually focus on detecting file types more commonly used in malware infection chains.

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

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1566 Phishing	T1566.001 Spearphishing Attachment	T1204 User Execution
T1204.002 Malicious File	T1027 Obfuscated Files or Information	T1106 Native API	T1056 Input Capture
T1056.001 Keylogging	T1114 Email Collection	T1041 Exfiltration Over C2 Channel	T1547 Boot or Logon Autostart Execution
T1102 Web Service			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	188.114.96[.]13
Domains	efvsx[.]gq
SHA256	4edd01345f58b9cc04a88ca15d6b82895f44f5b9cb51ad63b809de09029670ac 8a5a024272361bb1ae12860c033bb52685d7b0ea3bce5fac46439f3f3ad36a84 1b574a66c84924886daec4841e1b107258e019aaf6f336329ae8fae7cbd52a34

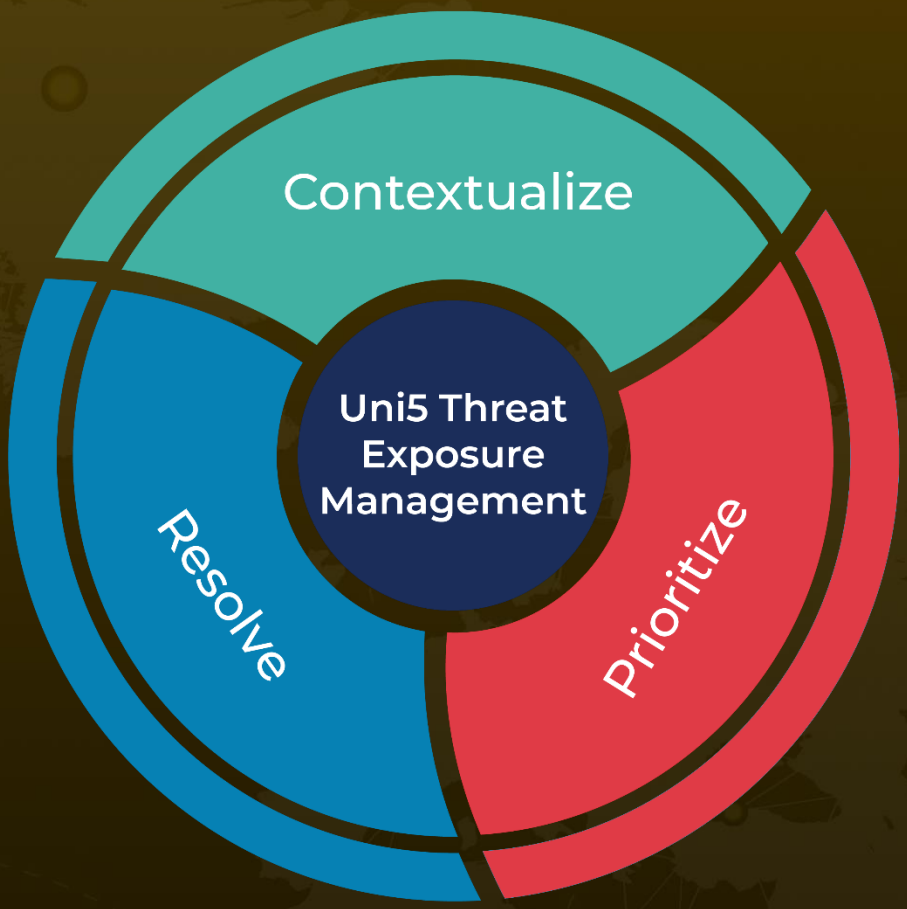
References

https://unit42.paloaltonetworks.com/lokibot-spike-analysis/

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 6, 2023 • 12:40 AM

More at www.hivepro.com