Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

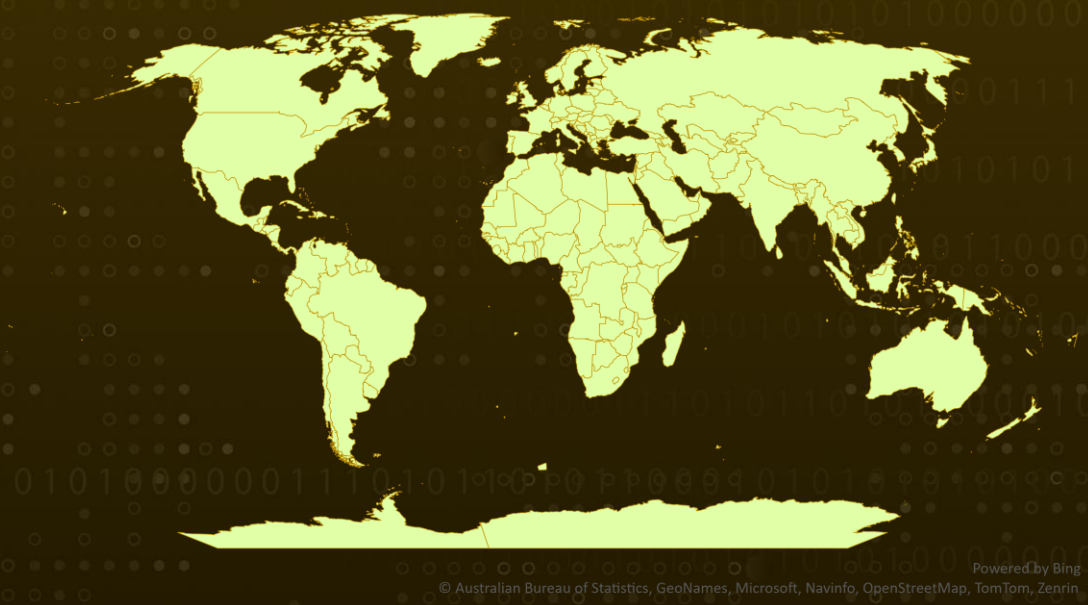
RedLine Stealer Used in Spear-Phishing Campaign Targeting Hospitality Industry

Date of Publication	Admiralty Code	TA Number
March 7, 2023	A1	TA2023121

Summary

First Appeared: March 2020
Attack Region: Worldwide
Attack Industry: Hospitality
Attack: A spear-phishing campaign targeting the hospitality industry used subject lines and text to trick hotel staff into clicking on malicious links that led to the download of malware, including the RedLine Stealer infostealer, which collected a wide range of data and sent it to its command-and-control server.

Attack Regions



Attack Details

#1

A spear-phishing campaign aimed at the hospitality industry has been uncovered. The emails had subject lines meant to grab attention, with text that enticed hotel staff to click on Dropbox links or Bitly-shortened URLs that contained malicious files. Some users were deceived into downloading malware, which had large file sizes ranging from 494.7 MB to 929.7 MB. The perpetrator poses as an elderly man, offering a shortened link to images of his route for hotel staff to verify, which leads to a malware payload instead.

#2

The campaign can be divided into four stages, with the final stage involving the RedLine Stealer infostealer. The RedLine Stealer gathers information, such as operating system, video controller, processor, antivirus, processes, and disk drive data, and sends it to its command and control (C&C) server, 77.73.134[.]13:12785. It can also gather data from browsers, cryptocurrency wallets, VPN applications, and other installed applications. The malware samples employ NetTcpBinding for message delivery and lack named commands.

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	TA0005 Defense Evasion
TA0006 Credential Access	TA0009 Collection	TA0010 Exfiltration	T1027 Obfuscated Files or Information
T1036 Masquerading	T1059 Command and Scripting Interpreter	T1037 Boot or Logon Initialization Scripts	T1074 Data Staged
T1105 Ingress Tool Transfer	T1055 Process Injection	T1106 Native API	T1560 Archive Collected Data
T1041 Exfiltration Over C2 Channel	T1005 Data from Local System	T1113 Screen Capture	T1003 OS Credential Dumping
T1056 Input Capture	T1056.001 Keylogging	T1566 Phishing	T1566.002 Spearphishing Link
T1204 User Execution	T1204.001 Malicious Link		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	bf803adb5695fce143062e6f51980d46537167b7a9e0e85ad13a999e35bd0466 6c5a4a8b7554000d5ab5221c43f25f093ba6a37c6b2511335e002f333c5af6c4 6c5a4a8b7554000d5ab5221c43f25f093ba6a37c6b2511335e002f333c5af6c4 bf803adb5695fce143062e6f51980d46537167b7a9e0e85ad13a999e35bd0466 9bacf20a00f73124039c4476d600e70293ae60d1d1d28290a63000b510f313f0

TYPE	VALUE
SHA256	62e7d750df3bb49f9535e8b4ba91d5ba8f5c655a0027643b52a3d9ffb0b64208 af23af4d4b3ba82c76a50bb631b4aca8d98e9a1560000d5c6fce39977cb9d362 84910fcdcb2edb3feeb3307bee0e6b33fc91caf8de344a3be71452b04b4595f0 6cbe9be190f521408438262d0c7f2ccbfab32a6df558cec2a264285fdfffe5c2 53af2c266c7f18e7c1ab16460d3c09d773fe93ac0a840fa83a30cc1020d1019a 4f1c1565afc782e688945c07a486205c59d43a98ae577c5d065bfed9a47a983d b5d8caa15cbf53d002edc6194abd0de43e4a139cc04f9703ae7bfc397bca66c8 9bacf20a00f73124039c4476d600e70293ae60d1d1d28290a63000b510f313f0 43328f774db70b98c4cbe83cc3be18de20a29b073b483eec49c64c6c301e4079 1b5f1e505e57b9915418f251f9c2343302f0737bdd85126666dbb56a27f0142f2 b83e50fa2c5c54e027f3bfe859e2a69e883bbb0080fed20aca176f77ad120fa1
IPV4:PORT	77.73.134[.]13:12785

References

https://www.trendmicro.com/en_us/research/23/c/managed-xdr-exposes-spear-phishing-campaign-targeting-hospitalit.html

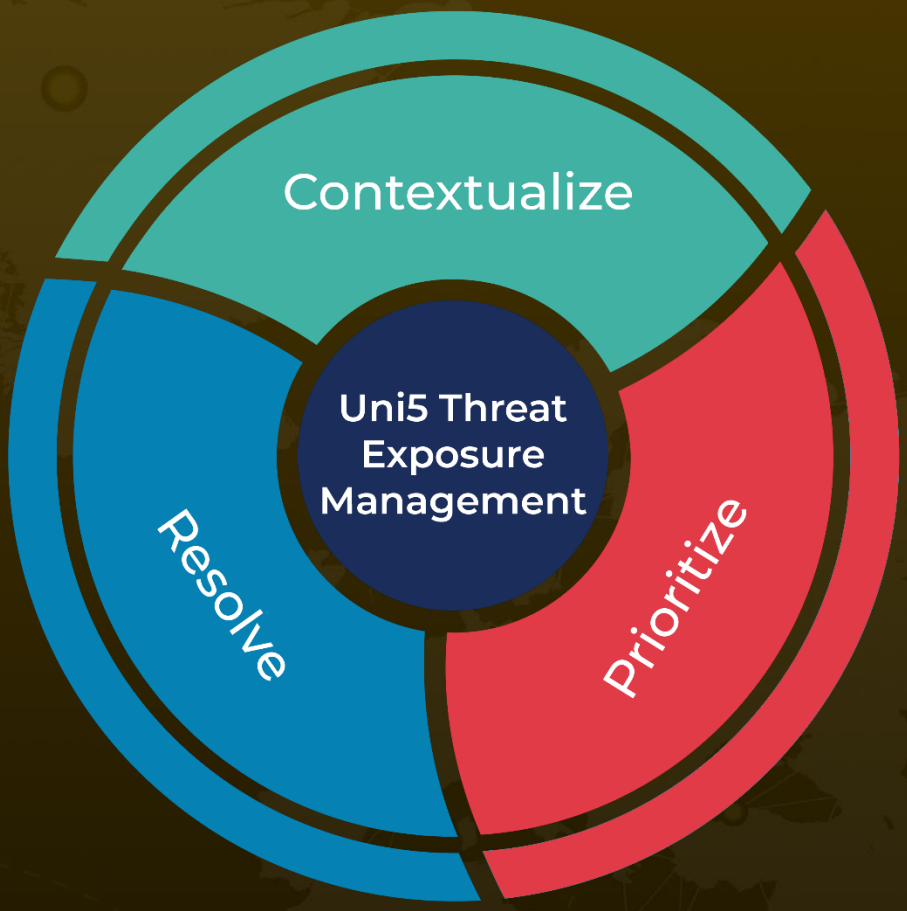
https://securityscorecard.com/research/detailed-analysis-redline-stealer/

https://otx.alienvault.com/pulse/6400c076dc224c9b94db8734/

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 7, 2023 • 12:15 AM

More at www.hivepro.com