Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

AgentTesla Trojan Returns with Phishing Campaigns Using GuLoader to Steal Secrets

Date of Publication

February 28, 2023

Admiralty Code

A1

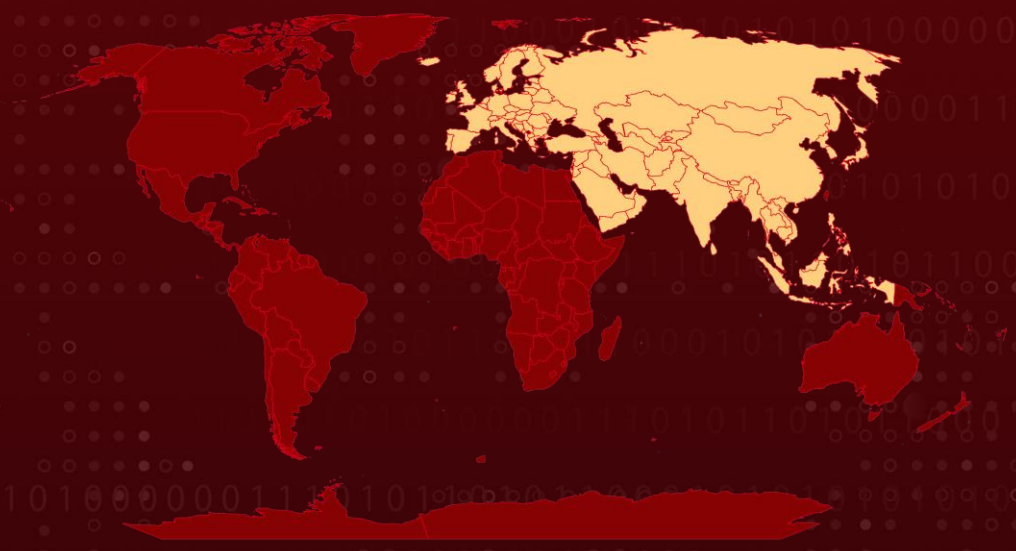
TA Number

TA2023106

Summary

Attack Begin: February 2023
Affected Industry: Government, Education, Manufacturing, Energy, Automobile and Internet
Attack Regions: Europe and Asia
Attack: The AgentTesla Trojan continues to pose a threat as attackers use GuLoader to deliver it in new phishing campaigns targeting various industries and countries.

Attack Regions



Attack Details

#1 AgentTesla Trojan has remained active and has been targeting government agencies, businesses, and universities to steal secrets. Since February of this year, attackers have been using GuLoader to deliver the AgentTesla Trojan in a new round of phishing attacks. These attacks have been aimed at companies in the manufacturing, energy, and internet industries in various Asian and European countries, with phishing emails posing as product quotation requests.

#2 GuLoader is a malicious file loader that first emerged in late 2019. It distributes and loads other malicious files through phishing emails and employs various obfuscation and anti-reverse analysis methods to evade detection by security products and researchers. In this latest campaign, the attackers targeted a Chinese automobile company with a phishing email containing an attachment named after a project and inducing the recipient to execute a VBS script, which loaded GuLoader into the device's memory. The final payload was the AgentTesla Trojan, which is a commercial .NET-based Trojan that steals secrets through functions such as keylogging, screen capture, and password theft.

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

TA0042 Resource Development	TA0001 Initial Access	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	T1113 Screen Capture	T1033 System Owner/User Discovery	T1583 Acquire Infrastructure
T1003 OS Credential Dumping	T1564 Hide Artifacts	T1119 Automated Collection	T1115 Clipboard Data
T1082 System Information Discovery	T1140 Deobfuscate/Decode Files or Information	T1555 Credentials from Password Stores	T1567 Exfiltration Over Web Service
T1552 Unsecured Credentials	T1055 Process Injection	T1620 Reflective Code Loading	T1560 Archive Collected Data
T1112 Modify Registry	T1087 Account Discovery	T1059 Command and Scripting Interpreter	T1020 Automated Exfiltration
T1204 User Execution	T1057 Process Discovery	T1566 Phishing	T1027 Obfuscated Files or Information
T1056 Input Capture	T1012 Query Registry	T1124 System Time Discovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps://portal-test.xperiorlist.com/DCQxHDrDFYuN76.toc hxxps://emilie.businessup.be/wp-includes/chn/OSEYggrugye738uhddwhudrwhJHD.php
MD5	DE7CFF093920A47ECAFFE6566E3BF66C 0D6AE3ECEBF610F5718B7C43AE14239F 8A1C57092616A9BF581E4B89A280B0B9

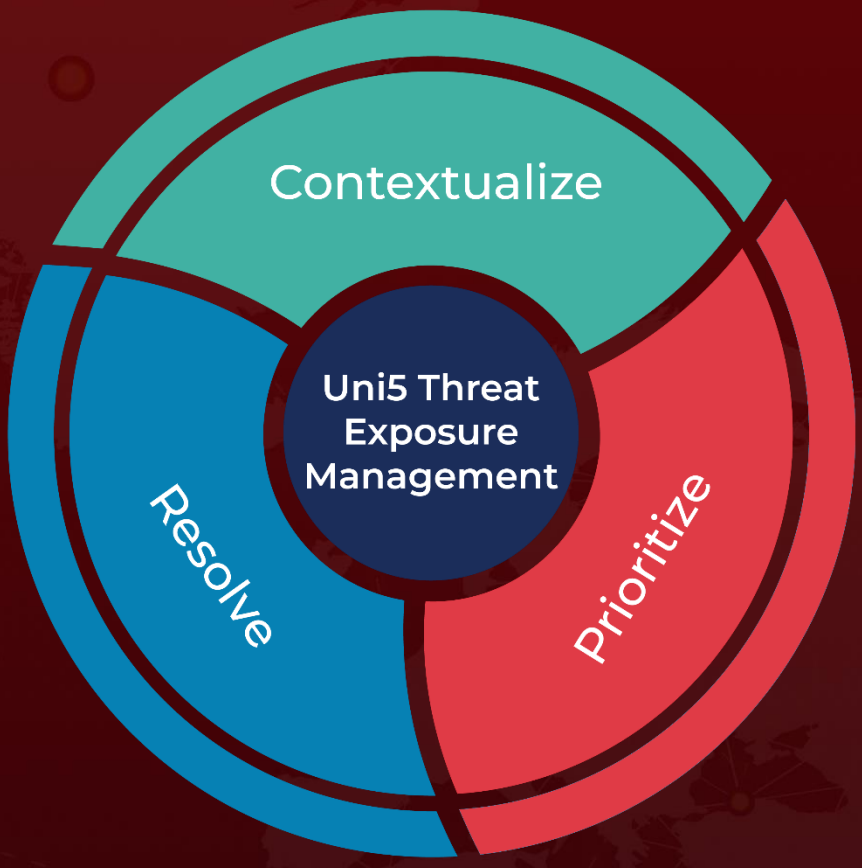
References

https://mp.weixin.qq.com/s/rF4p-PHQrV33svltk44vOg

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 28, 2023 • 1:00 PM

More at www.hivepro.com