Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

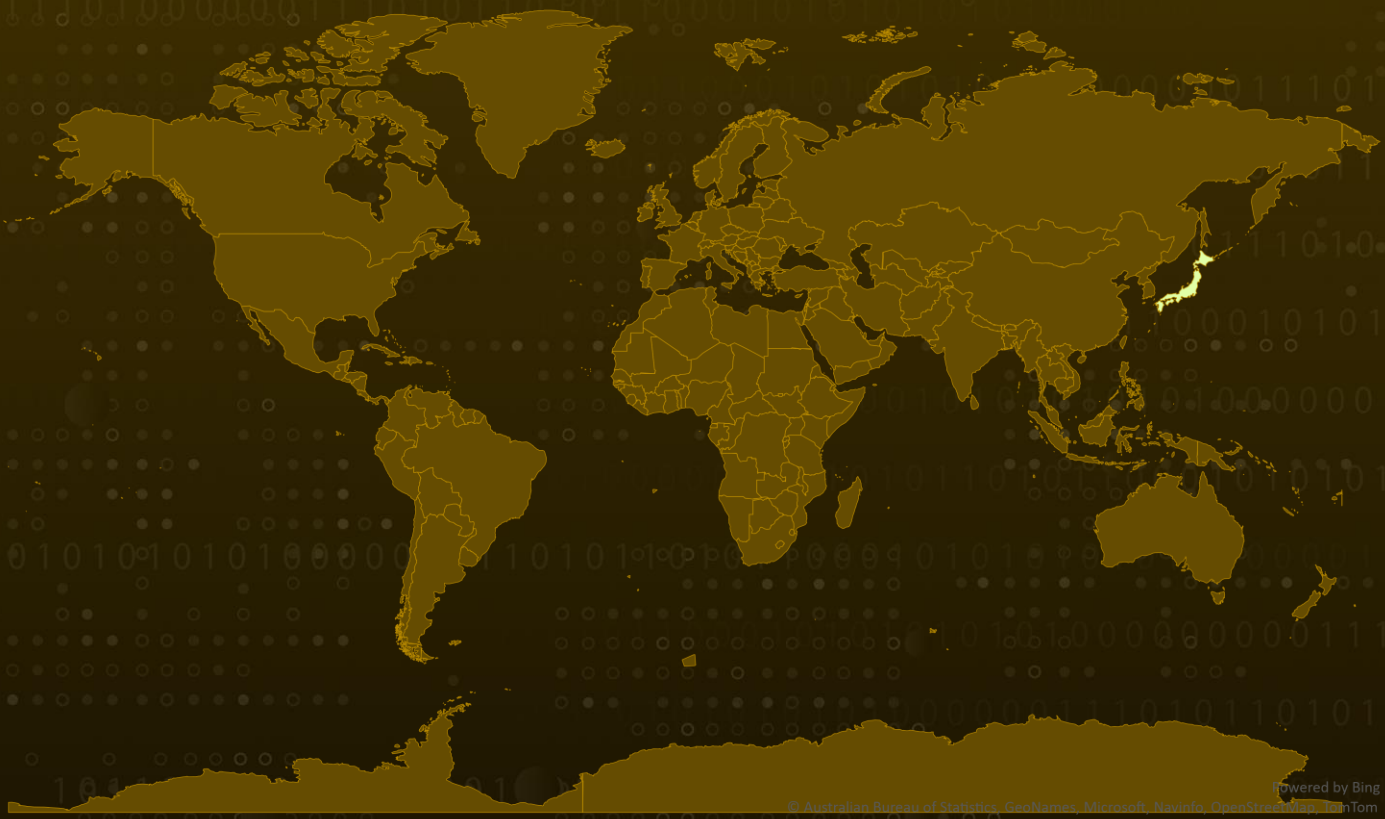
The SteelClover Group is Spreading Malware via Google Ads in Japan

Date of Publication	Admiralty Code	TA Number
February 8, 2023	A1	TA2023070

Summary

First appeared: 2019
Attack Region: Japan
Attack: SteelClover is an attack group that has been operating for several years and is now using Google Ads to spread malicious files that infect systems with Ursnif and Redline Stealer malware.

Attack Regions



Attack Details

#1

SteelClover is a malicious attack group that has been active since 2019 and has been observed to conduct various attacks for financial gain. SteelClover recently saw a rise in malware downloading incidents through Google Ads at Japanese companies. It is responsible for the Malsmoke campaign, which uses malware such as Batloader and overlaps with other attack groups like DEV-0569 and Water Minyades. The group is known for information theft and has been linked to eventual ransomware execution.

#2

SteelClover has been seen to have 5 different attack campaigns, with the BatApp and FakeGPG campaigns being the most recent. The group continues to update its attack methods on a daily basis. SteelClover's attack flow involves the display of malicious advertisements in Google Ads that redirect to its malicious file distribution sites.

#3

The sites mimic well-known software websites and are used to distribute MSI files that execute PowerShell code to download and execute Ursnif and Redline Stealer. SteelClover does not develop its own exploit kits or malware, but uses those sold on the market. The group has made many mistakes and its characteristics are reflected in its attacks. For example, the use of Gpg4Win and the function name used in Zeip .exe suggest a connection to Russia.

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
TA0001 Initial Access	**TA0008** Lateral Movement	**TA0011** Command and Control	**TA0040** Impact
T1204 User Execution	**T1204.002** Malicious File	**T1189** Drive-by Compromise	**T1059** Command and Scripting Interpreter
T1059.001 PowerShell	**T1543** Create or Modify System Process	**T1140** Deobfuscate/Decode Files or Information	**T1471** Data Encrypted for Impact
T1003 OS Credential Dumping	**T1021.005** VNC	**T1021** Remote Services	**T1036** Masquerading

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	47[.] 251.52.170 37[.] 220.83.95 5[.] 178.2.159 81[.] 177.136.237 81[.] 177.6.46 62[.] 204.41.176

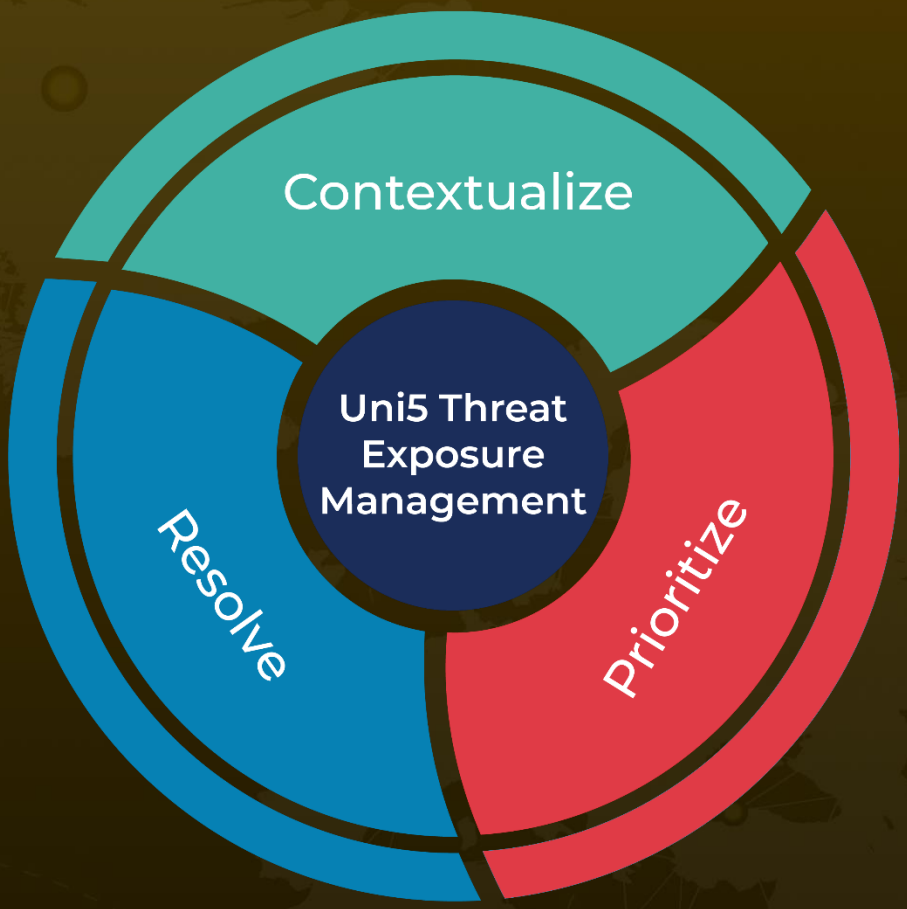
References

https://insight-jp.nttsecurity.com/post/102i7af/steelclovergoogle

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 8, 2023 • 10:30 AM

More at www.hivepro.com