Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

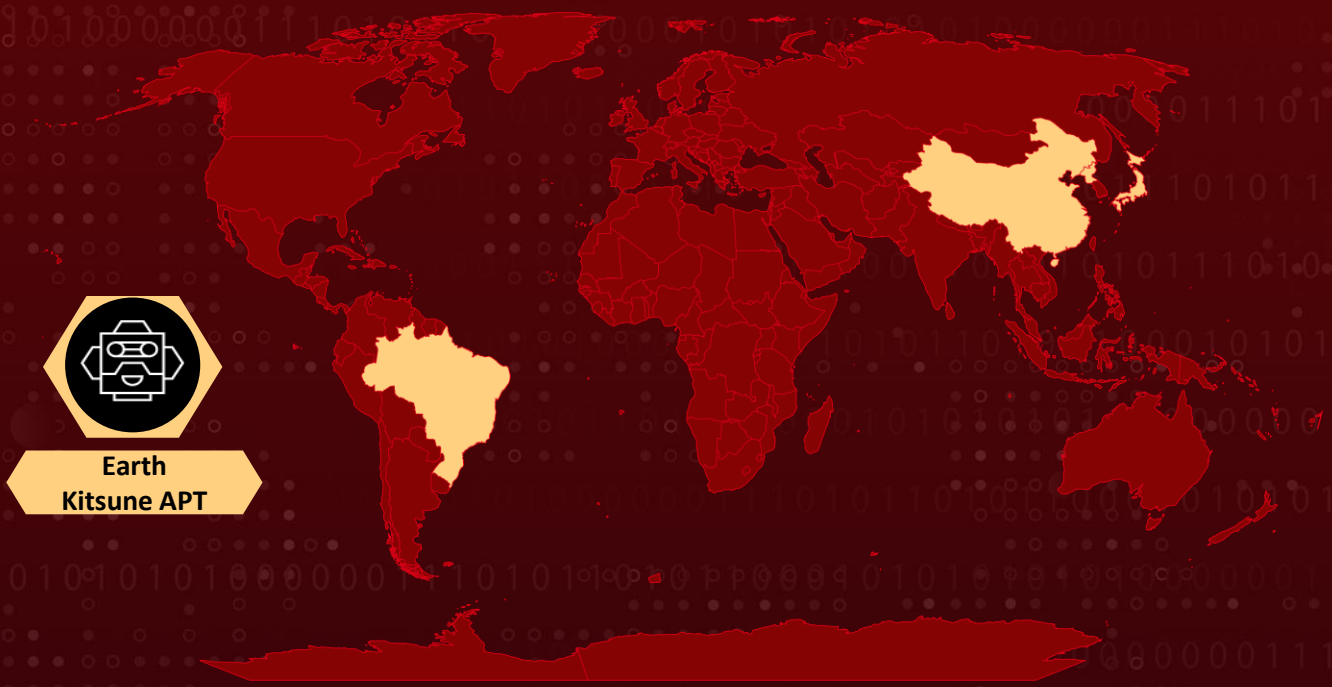
APT Earth Kitsune delivers new WhiskerSpy malware via watering hole attack

Date of Publication	Admiralty Code	TA Number
February 20, 2023	A1	TA2023089

Summary

First Appearance: 2019
Actor Name: Earth Kitsune APT
Target Countries: North Korea, China, Brazil, and Japan.
Attack: Earth Kitsune APT used a social engineering tactic to distribute a trojanized codec installer, with a new backdoor "WhiskerSpy," and also abused Google Chrome's native messaging host and OneDrive side-loading vulnerabilities for persistence.

Attack Regions



Attack Details

#1

Earth Kitsune, an advanced persistent threat (APT) actor known for targeting individuals interested in North Korea, also China, Brazil, and Japan and has been found to be using a new backdoor called "WhiskerSpy" in a recent campaign. The group used a social engineering tactic in a watering hole attack, luring visitors to a pro-North Korean website with a fake error message and offering a trojanized codec installer that loaded the WhiskerSpy backdoor on their systems.

#2

In addition to this, Earth Kitsune abused Google Chrome's native messaging host to establish persistence. They added a listener to the startup message that sends the "inject" command to the native messaging host, which effectively executes the malicious payload every time the Chrome browser is started. This unique method of persistence allows the group to maintain control over the infected systems even if other security measures are put in place.

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	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0003 Persistence	TA0005 Defense Evasion	TA0040 Impact
T1059 Command and Scripting Interpreter	T1047 Windows Management Instrumentation	T1569 System Service	T1189 Drive-by Compromise
T1055 Process Injection	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1622 Debugger Evasion
T1068 Stage Capabilities	T1608.001 Upload Malware		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	FBAC7B40A12970CDCC36F48945BEB83BF9461F14C59CB8106AD8E43E5D22A970 7365F661AD9E558FDD668D3563E0A1B85CCF1A543BE51CB942DB508F9CCBCF5E 3D4107C738B46F75C5B1B88EF06F82A5779DDD830527C9BECC951080A5491F13 84E9BCC055225BD50534147E355834325B97AD948C3A10D792928B48C56C1712 CE7016067C97421E3050FA8BD7F1950E0707E6DEEAC20003F5F30F1C58F435BC 1C24D9013B3EAE373FC28D40F9E475E1DD22C228E8F1E539ED9229E21807839D 076BA1135B2F9F4DBC38E306DC533AF71B311C1DC98788C18253448FCA096C46 371CFA10A7262438E5BC0694BA5628EB21E044DC8173710DF51826DAFA11E300 E01399D47CDA45F1AF496FA460F20620A5B08C39714875FE292A5FC3D1C7A215 6F0A0AC477C73C2533A39CB3D8FBF45365761D11B7368460964A4572E91C5FCB C357E572DD7C618C54F8333313266A8A9CF07C1038D6B2F711CDBAE714BC2654 902902B5457C6945C2B3878521D23D05D448DE179D19761C718FB67C15A4BCC0

TYPE	VALUE
SHA256	3D62E122E31D7929E76633773D752B8BEE31462BB79CB5B8B7C6952341E93482 20C214D58CCFB5AD797F1A02667078D182629AC7E157162566C123519E039D55 66C8E0ACFE030C4EEC474CD75C4D831601DAE3EF4E1CEF78B624DE3C346C186D C78CB41F4FB4E5F5476EB2C1414F138643494C2B8ABE2CF539FAFC54199E2AEF
Domains	icrosoftwindow[.]sytes[.]net updategoogle[.]servehttp[.]com londoncity[.]hopto[.]org windowsupdate[.]sytes[.]net florida[.]serveblog[.]net googlemap[.]hopto[.]org liveupdate[.]servepics[.]com chromecast[.]hopto[.]org googlemap[.]serveblog[.]net selectorioi[.]ddns[.]net rs[.]myftp[.]biz

References

https://www.trendmicro.com/en_us/research/23/b/earth-kitsune-delivers-new-whiskerspy-backdoor.html

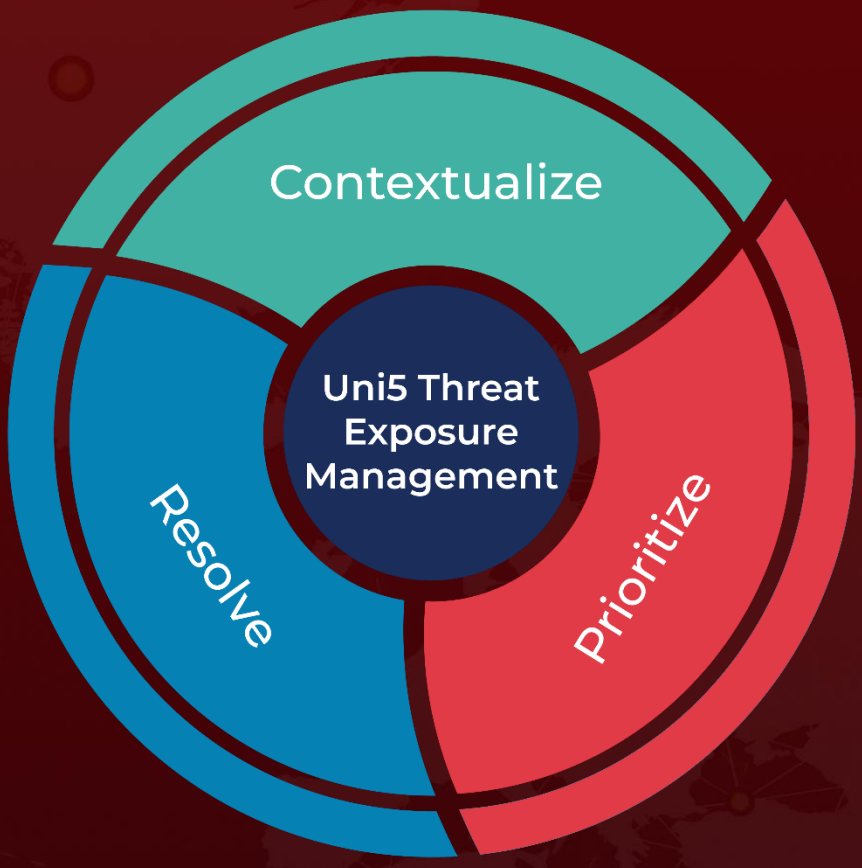
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/b/earth-kitsune-delivers-new-whiskerspy-backdoor-via-watering-hole-attack/Earth_Kitsune_WhiskerSpy_iocs.txt

https://www.bleepingcomputer.com/news/security/new-whiskerspy-malware-delivered-via-trojanized-codec-installer/

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 20, 2023 • 2:00 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com