Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

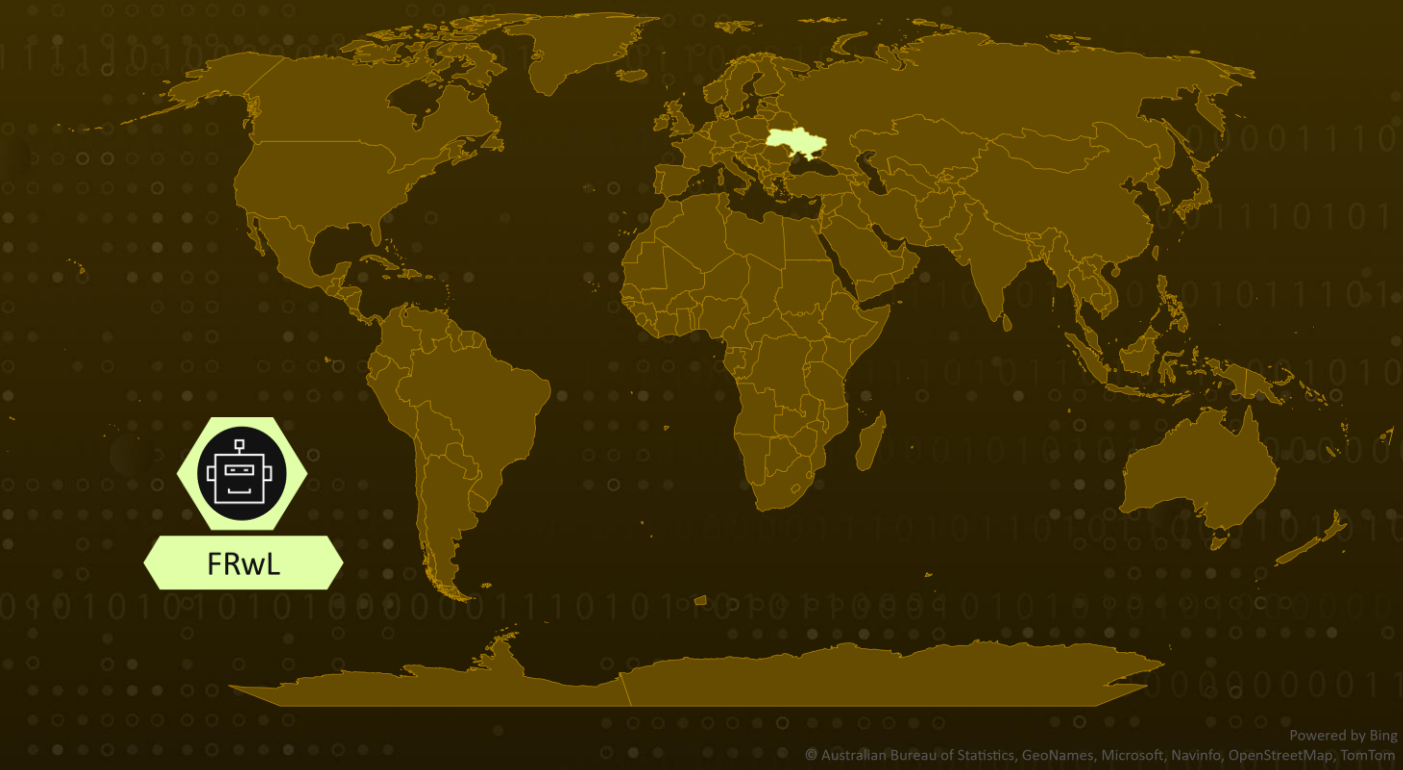
FRwL destroys data with Somnia to disrupt operations in Ukraine

Date of Publication	Admiralty Code	TA Number
November 14, 2022	A1	TA2022254

Summary

Date: November 11, 2022
Attack Region: Ukraine
Threat Actor: FRwL
Attack: FRwL encrypts data with Somnia malware; destroys data;

Attack Regions



Attack Details

#1 FRwL(From Russia with Love) group, tracked as UAC-0118 uses a fake website to trick Ukrainian organization employees into downloading the Advanced IP Scanner software. Upon installation, the system is infected with the Vidar stealer, which intercepts Telegram session data and takes control of the victim's account.

#2 As a next step, the threat actors abused the victim's Telegram account in some unspecified manner to steal VPN connection data (authentication and certificates). A VPN account without two-factor authentication allowed hackers to access the victim's employer's network without authorization.

#3 After this, the intruders use Cobalt Strike beacons, exfiltrate data, and use Netscan, Rclone, Anydesk, and Ngrok to monitor and access the network remotely.

#4 To encrypt data, the attackers use the latest version of Somnia ransomware which relies on the AES algorithm. Encrypted files will have the .somnia extension appended. The operators of Somnia do not ask victims to pay a ransom for a working decryptor, since their goal is to disrupt the victim's operations rather than make money.

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

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0003** Persistence	**TA0011** Command and Control
TA0042 Resource Development	**T1588** Obtain Capabilities	**T1588.001** Malware	**T1595** Active Scanning
T1590 Gather Victim Network Information	**T1195** Supply Chain Compromise	**T1133** External Remote Services	**T1573** Encrypted Channel
T1573.001 Symmetric Cryptography	**T1219** Remote Access Software		

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	c7948d1ffab0d0a165c56c35e1ae320c abaca1fac308ce6627c1d823c410b174 638725d249839aaf29fa122dc7aeb41e 93d7636729e908444ab21fb8213f809e dc792b8e287f2f7ddea0469f26d88fb7 47cd55b63e8e90d8f49352396f76bed6 7a4ab857659a40a69c0d29650d991a79 c87261c139ecba1989a88e157a71e3af 58c40d0ad81f25bcd68a5523d867eb34
SHA256	100c5e4d5b7e468f1f16b22c05b2ff1cfaa02eafa07447c7d83e2983e42647f0 ac5e68c15f5094cc6efb8d25e1b2eb13d1b38b104f31e1c76ce472537d715e08 99cf5c03dac82c1f4de25309a8a99dcabf964660301308a606cdb40c79d15317 156965227cbeeb0e387cb83adb93ccb3225f598136a43f7f60974591c12fafcf e449c28e658bafb7e32c89b07ddee36cadeddfc77f17dd1be801b134a6857aa9 fbed7e92caefbd74437d0970921bfd7cb724c98c90efd9b6d0c2ac377751c9e5 06fe57cadb837a4e3b47589e95bb01aec1cfb7ce62fdba1f4323bb471591e1d2

TYPE	VALUE
SHA256	1e0facd62d1958ccf79e049270061a9fce3223f7986c526f6f3a93ef85180a72 1f4c5ab072f384b9adfafd35903c5b54b8a3ad167250728d0d400454300a4367
URLS	hXXps://t[.]me/cheaptrains hXXps://mastodon[.]social/@ffolegg94 hXXp://193[.]43.146.42:80 hXXps://advanced-ip-scanner.com.vuxuancuong[.]com/ hXXps://advanced-ip-scanner[.]website/en/ hXXps://onedrive[.]live.com/download?cid=E8A357DC635F5F11&resid=E8A357DC635F5F11!552&authkey=AN-tOu0N0SGFnpg hXXps://zambeziz[.]com/jquery-3.3.1.min.js hXXps://gofile[.]io/d/7KbRYr hXXps://gofile[.]io/d/nycrb4 hXXps://store1.gofile[.]io/download/27a73fd4-a939-4a05-9c0e-54c0c5dfef3d/1.exe hXXps://store3.gofile[.]io/download/939fad81-10ba-438e-b396-c2f42f209ab0/netscan_portable.7z hXXps://store8.gofile[.]io/download/43571707-464b-40c8-bf5e-2d9e07c554b8/Somnia_07_08_22_with_FunnySomnia.exe hXXps://store8.gofile[.]io/download/8b9f91c9-b770-4ed5-b60f-ec1dd5ca8b43/1.jpeg hXXps://advanced-ip-scanner[.]click/en/ hXXps://advanced-ip-scanner[.]site/en/ hXXps://www.dropbox[.]com/s/26gri1ashi4rydb/Ip_scanner.zip?dl=1 hXXp://185[.]96.163.102:80
IPV4	209[.]222.101.65 139[.]60.161.52 193[.]43.146.42 139[.]60.161.165 139[.]60.161.167 139[.]60.161.213 139[.]60.161.47 139[.]60.161.63 185[.]170.144.217 185[.]96.163.102 193[.]43.146.39 5[.]252.22.96 94[.]232.41.105 95[.]217.244.218

TYPE	VALUE
Domains	vuxuancuong[.]com advanced-ip-scanner.com.vuxuancuong[.]com zambeziz[.]com franygreat@outlook.com advanced-ip-scanner[.]click advanced-ip-scanner[.]site agrikoz[.]com aluaadin[.]com arminext[.]com benokij[.]com fudupdate[.]com sinergil[.]com softloadup[.]com survefuz[.]com vinergil[.]com zbignef[.]com

References

https://cert.gov.ua/article/2724253

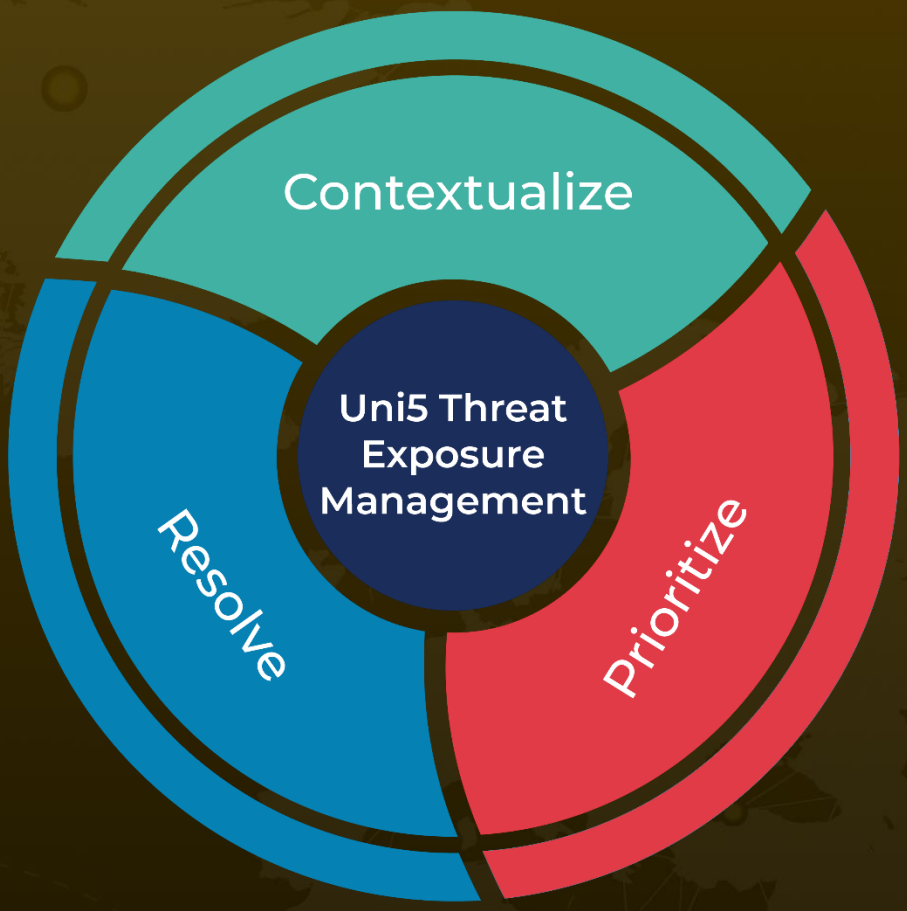
https://otx.alienvault.com/pulse/636e3b374fdb611f956d3fe1/

https://www.bleepingcomputer.com/news/security/ukraine-says-russian-hacktivists-use-new-somnia-ransomware/

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 14, 2022 . 4:30 AM

More at www.hivepro.com