Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

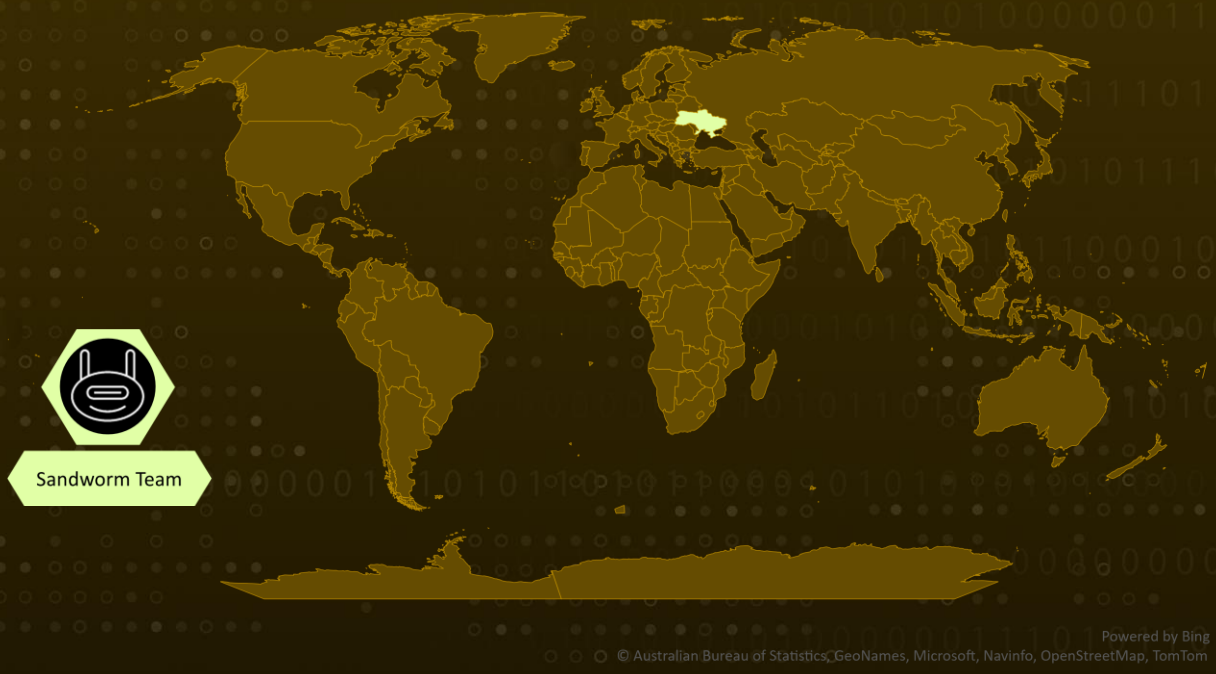
Cyber Attack on Ukrainian National Information Agency

Date of Publication	Admiralty Code	TA Number
January 30, 2023	A1	TA2023051

Summary

Attack Initiated: December 7, 2022
Threat Actor: Sandworm Team(UAC-0082)
Attack Countries: Ukraine
Attack Sectors: Media
Attack: The Ukrainian National Information Agency "Ukrinform" was the target of a partially successful cyber attack by the UAC-0082 (Sandworm) group associated with the Russian Federation.

Attack Regions



Attack Details

#1

On 17th January 2023, the Ukrainian National Information Agency "Ukrinform" suffered a partial cyber attack. The Government Computer Emergency Response Team of Ukraine (CERT-UA) initiated an investigation into the attack at the Agency's request. The attack was initiated on 17th January 2023, but it was only partially successful in relation to several data storage systems.

#2

As part of the investigation, 5 malicious programs were detected, including CaddyWiper, ZeroWipe, SDelete, AwfulShred, and BidSwipe. The attackers attempted to disrupt the regular operation of users' computers using these programs, but their efforts were unsuccessful. The group policy object (GPO) was created for the centralized distribution of these malicious programs and ensured the creation of corresponding scheduled tasks.

#3

The cyber attack was carried out by the UAC-0082 (Sandworm) group, associated with the Russian Federation. The group is known for its destructive activities, as highlighted in the Telegram channel "CyberArmyofRussia_Reborn", which exclusively highlights the group's destructive activities, including DDoS attacks and defaces. An element of ICS was also identified during the investigation, which created the prerequisites for unauthorized remote access to the Agency's information resources.

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
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
T1203 Exploitation for Client Execution	**T1059** Command and Scripting Interpreter	**T1129** Shared Modules	**T1569** System Services
T1569.002 Service Execution	**T1543** Create or Modify System Process	**T1543.003** Windows Service	**T1547** Boot or Logon Autostart Execution
T1547.008 LSASS Driver	**T1055** Process Injection	**T1497** Virtualization/Sandbox Evasion	**T1562** Impair Defenses
T1562.001 Disable or Modify Tools	**T1027** Obfuscated Files or Information	**T1222** File and Directory Permissions Modification	**T1056** Input Capture
T1016 System Network Configuration Discovery	**T1018** Remote System Discovery	**T1082** System Information Discovery	**T1083** File and Directory Discovery
T1518 Software Discovery	**T1518.001** Security Software Discovery	**T1012** Query Registry	**T1071** Application Layer Protocol
T1095 Non-Application Layer Protocol			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	cc213200daf4202e2454dc2c363db04f 54e5773071b193e109cbacc82565c6a9 6aa899b47596323da573fb218f3a8266 803df907d936e08fbbd06020c411be93 3a1070b882d6843fcfa9490c24700bd1 4a5863d34fc99e91af11dd7976c36c27

TYPE	VALUE
SHA256	00782ccd65a1e03e3e74ce1e59e752926e0a050818fa195bd7e5a5b359500758 e3bc3689f01fd431cd2ed368ae91eceaa7c465c2781fa7b7dc2ec9143a404f79 301b248a8291df6c7f3565a3dac17ee69609f36ef474b4f20eebe134746a9cac e8eaa39e2adfd49ab69d7bb8504ccb82a902c8b48fbc256472f36f41775e594c 246607235d560e90590dcf1b0507ab18de74afcc4429d8d5f3ba97eacc92d73f 66548ba6ca6d34b7d17e42ab2e1405db1c581a516e0b1a4942d373d6d5396ba4
IPV4	185[.]220.101.185 185[.]220.102.244 185[.]220.102.245 185[.]220.102.248 185[.]220.102.250 185[.]220.102.251 45[.]154.98.225 77[.]91.123.136 80[.]67.167.81 194[.]28.172.172 194[.]28.172.81
Domains	digitalcourage[.]de as210558[.]net stark-industries[.]solutions milkywan[.]fr besthosting[.]ua torguard[.]net secureconnect[.]me
Path	C:\Users\new.exe C:\VLOG\dd_vcredist_x86_20200324195140_001_vcRuntimeAdditional_x64.log C:\Windows\SYSVOL\domain\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\news.bat C:\Windows\SYSVOL\domain\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\upd.exe C:\Windows\new.bat C:\Windows\up.exe C:\windows\temp\BRN3C2AF47629AB.log C:\windows\temp\TS_4318.tmp C:\windows\temp\b8WTBWCoF5.log

Recent Breaches

https://www.ukrinform.net/

References

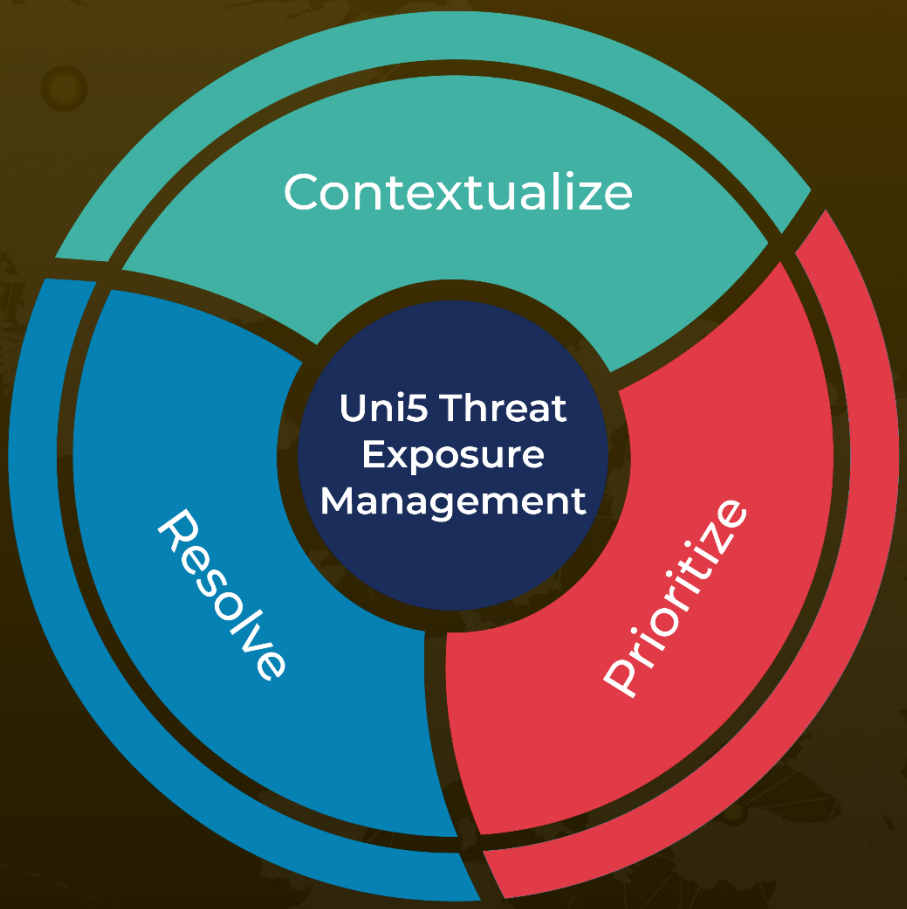
https://cert.gov.ua/article/3718487

https://www.bleepingcomputer.com/news/security/ukraine-sandworm-hackers-hit-news-agency-with-5-data-wipers/

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

January 30, 2023 . 2:10 AM

More at www.hivepro.com