Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

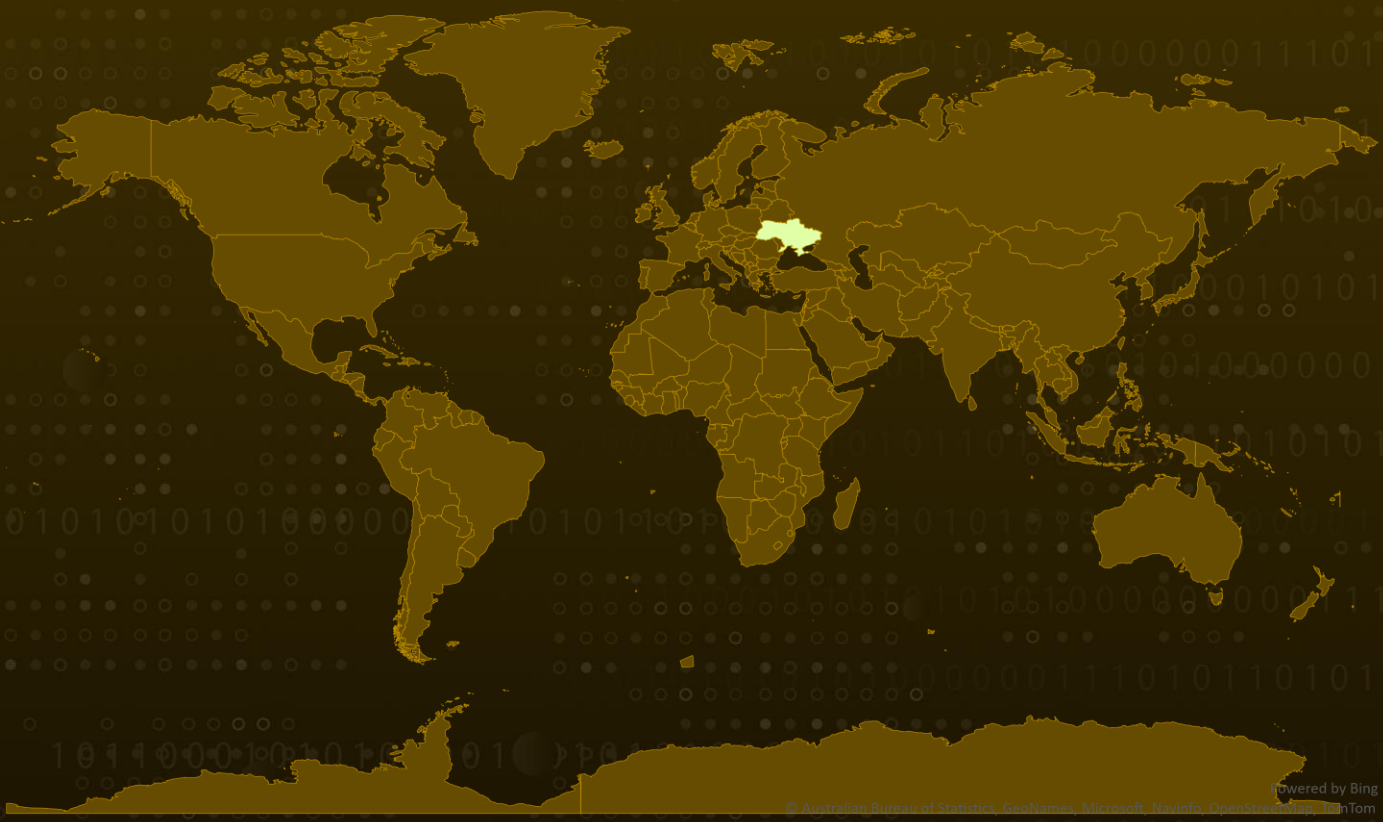
Malware Attack Targets Windows Users with Spoofed Energoatom Document

Date of Publication	Admiralty Code	TA Number
April 14, 2023	A1	TA2023185

Summary

First appeared: April 2022
Attack Region: Ukraine
Malware: Havoc Demon Backdoor
Affected Platforms: Windows
Targeted Industry: Energy
Attack: The malware comes in the form of a spoofed document from Energoatom and is believed to be part of a larger campaign against Ukraine's energy sector, which has been under constant cyberattacks since the conflict with Russia began.

Attack Regions



Attack Details

#1 A Havoc Demon Backdoor malware attack targets Windows users through a spoofed document from Energoatom, a state-owned enterprise that operates Ukraine's nuclear power plants. The document is named "approved list of persons to receive" in Ukrainian and is designed to look like it's protecting sensitive information with the help of the popular Ukrainian document management system, M.E. Doc.

#2 Once the macro is enabled, the user is presented with an announcement about a list of people who are supposedly approved to receive protective equipment. The code also used simple encoding to hide strings and added seemingly random nonsensical comments to the code.

#3 The malware uses several techniques to evade detection and gain control of the compromised machine, allowing the threat actor to perform various malicious activities. This attack is believed to be part of a larger campaign against Ukraine's energy sector, which has been under constant cyberattacks since the conflict with Russia began.

Recommendations

Block these files VBA/Havoc.FGLT!tr, W64/Havoc.FGLTA!tr.bdr, W64/Havoc.FGLTB!tr.bdr using antivirus software. Be cautious when opening email attachments, especially from unknown senders. Verify the sender's identity and scan attachments for malware before opening them and discourage them from enabling macros in Microsoft Word documents unless absolutely necessary.

Keep your systems and software up to date, and regularly update your operating system and software with the latest security patches and updates to ensure that you have the latest security protections. Use reputable antivirus and antimalware software to help protect your systems against malware attacks.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0001 Initial Access
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	T1007 System Service Discovery
T1204 User Execution	T1566 Phishing	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter
T1059.005 Visual Basic	T0872 Indicator Removal on Host	T1622 Debugger Evasion	T1221 Template Injection
T1106 Native API	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1137 Office Application Startup
T1137.001 Office Template Macros	T1204.002 Malicious File	T1027 Obfuscated Files or Informatio	T1036 Masquerading
T1113 Screen Capture	T1573 Encrypted Channel	T1140 Deobfuscate/Decode Files or Information	T1104 Multi-Stage Channels

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps://ukrtatnafta[.]org hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/avias.js hxxps://ukrtatnafta[.]org/wpcontent/themes/pressa/js/mobile_menu.js hxxps://ukrtatnafta[.]org/wp-content/plugins/contact-form-7/includes/js/scripts.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/bootstrap.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/hovermenu.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/retina1.1.0.js hxxps://ukrtatnafta[.]org/wpcontent/plugins/js_composer/assets/lib/bower/isotope/dist/isotope.pkgd.min.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/custom-script.js hxxps://ukrtatnafta[.]org/wp-includes/js/wp-emoji-release.min.js hxxps://ukrtatnafta[.]org/maps-api-v3/api/js/52/1/intl/uk_ALL/util.js hxxps://ukrtatnafta[.]org/wp-includes/js/wp-embed.min.js

TYPE	VALUE
SHA256	b773fa65bb375e6fe6d387f301f6bf33219189ea1d4a06762e965a9eba7de4e8 17637fac7f989549acd248ca9e5293d2b9a1a2e4bb0f7e4edf5571df35129f0c 9f797d705facebd1687b7765cbf65231e71821eb3c38dcc171a3fc88b9f52328 b6cb8a7cdce0bfd3a7402d22fb0014dedb259d6c91c1538ac74097b8ca22ca5c

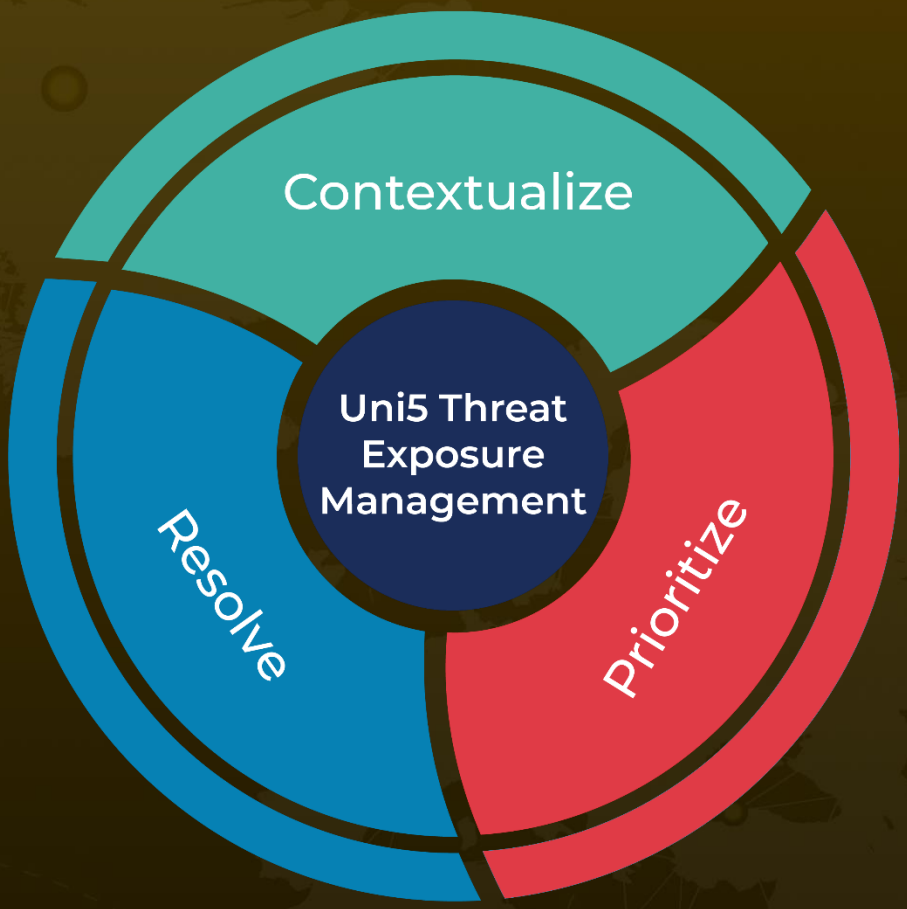
References

https://www.fortinet.com/blog/threat-research/malware-disguised-as-document-ukraine-energoatom-delivers-havoc-demon-backdoor

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

April 14, 2023 • 2:30 AM

More at www.hivepro.com