Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

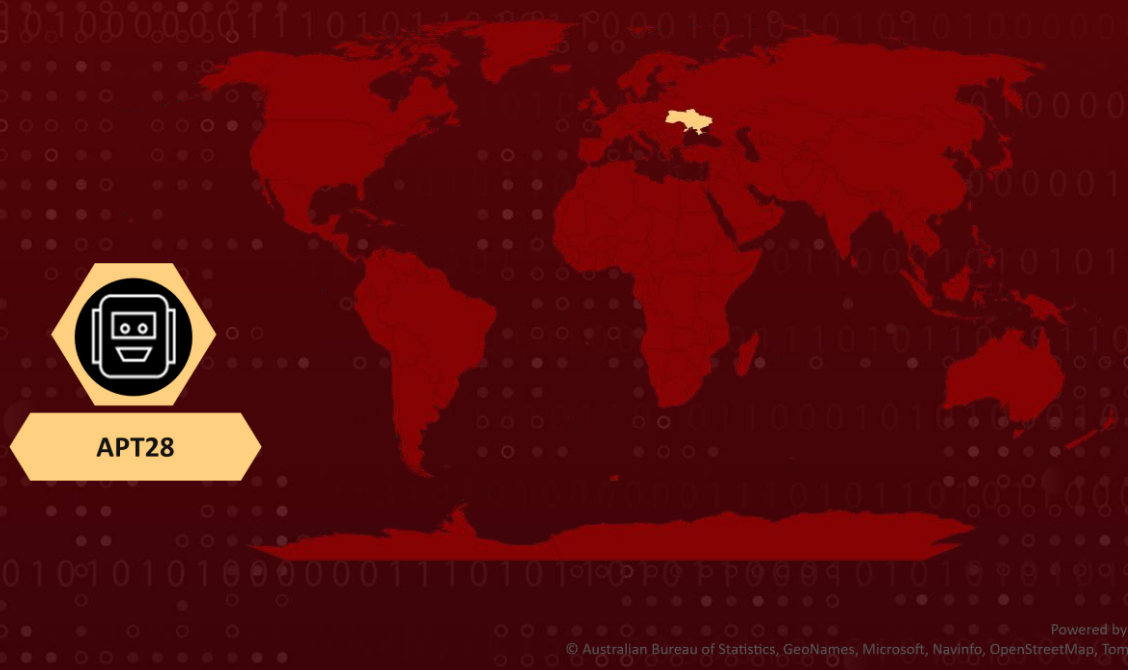
APT28's Cyber Espionage Campaigns Targeting Ukraine

Date of Publication	Admiralty Code	TA Number
May 22, 2023	A1	TA2023240

Summary

Attack began: 2023
Actor: APT28 (aka FANCY BEAR, STRONTIUM, Sofacy, Zebrocy, Sednit, Pawn Storm, TG-4127, Tsar-Team, Iron Twilight, Swallowtail, SNAKEMACKEREL, Frozen Lake)
Attack Region: Ukraine
Targeted Sectors: Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and Gas, Think Tanks, and Intelligence organizations.
Attack: The APT28 intrusion group, linked to the Russian GRU and renowned for its cyber espionage and sabotage endeavors, was observed employing various phishing methodologies to target the Ukrainian civic community.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-23397	Microsoft Office Outlook Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓

Attack Details

#1

The APT28 intrusion group, affiliated with the Russian GRU and widely recognized for its cyber espionage and sabotage campaigns, has been observed employing a diverse array of phishing methodologies to specifically target Ukraine. These tactics encompass the utilization of HTTP webhook services like Pipedream and Webhook, as well as compromised Ubiquiti routers to pilfer victims' credentials. Notably, there was an instance where APT28 employed the "Browser in the Browser" technique, displaying a fraudulent login page to the victim under the guise of decrypting a document.

#2

The Microsoft Office Outlook Privilege Escalation Vulnerability (CVE-2023-23397) has been exploited by APT-28, who have recently employed compromised Ubiquiti Edge devices, running on EdgeOS, as operational platforms to host Responder instances on port 445. The attackers have shown a particular interest in EdgeOS, a Debian fork called Vyatta, due to its default password, WAN accessibility, and Aptitude package management functionalities. These inherent features facilitate the attackers' seamless deployment of their scripts.

Recommendations

Strengthen Endpoint Security Measures: Organizations should bolster their endpoint security measures to mitigate the impact of APT28 threat actor. This includes implementing the security patch provided by Microsoft to mitigate the Microsoft Office Outlook Privilege Escalation Vulnerability (CVE-2023-23397) and prevent potential exploitation by APT28. Timely patching is crucial to safeguard systems and data from cyberattacks.

Enhance Phishing Awareness and Education: It is crucial to prioritize comprehensive training programs to educate Ukrainian organizations and individuals about the various phishing techniques employed by APT-28. By raising awareness about the risks posed by phishing attacks and providing guidance on identifying suspicious emails, links, and login pages, the likelihood of falling victim to such campaigns can be significantly reduced.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0009 Collection	T1176 Browser Extensions
T1014 Rootkit	T1114 Email Collection	T1566 Phishing	T1056 Input Capture
T1134 Access Token Manipulation	T1204 User Execution		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	robot-876.frge[.]io setnewcred.ukr.net.frge[.]io panelunregistertle-348[.]frge.io settings-panel.frge[.]io ukrprivacysite.frge[.]io config-panel.frge[.]io smtp-relay.frge[.]io packinstall.kozow[.]com
IPV4	68.76.150[.]97 174.53.242[.]108 24.11.70[.]85 202.175.177[.]238 85.240.182[.]23 69.28.64[.]137
MD5	acbb64c3de5ea5e5936df4a1eecf1235

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

Recent Breaches

https://www.ukr.net/

https://www.yahoo.com

References

https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/

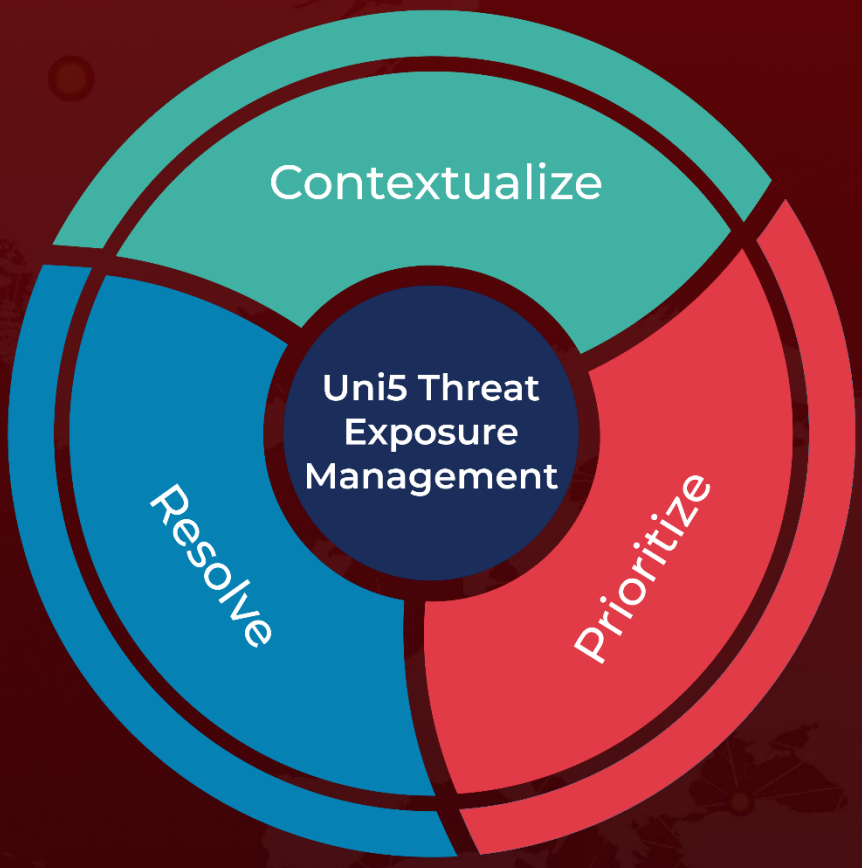
https://www.hivepro.com/apt28-exploits-follina-to-deploy-credomap/

https://attack.mitre.org/groups/G0007/

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

May 22, 2023 • 7:00 AM

More at www.hivepro.com