Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

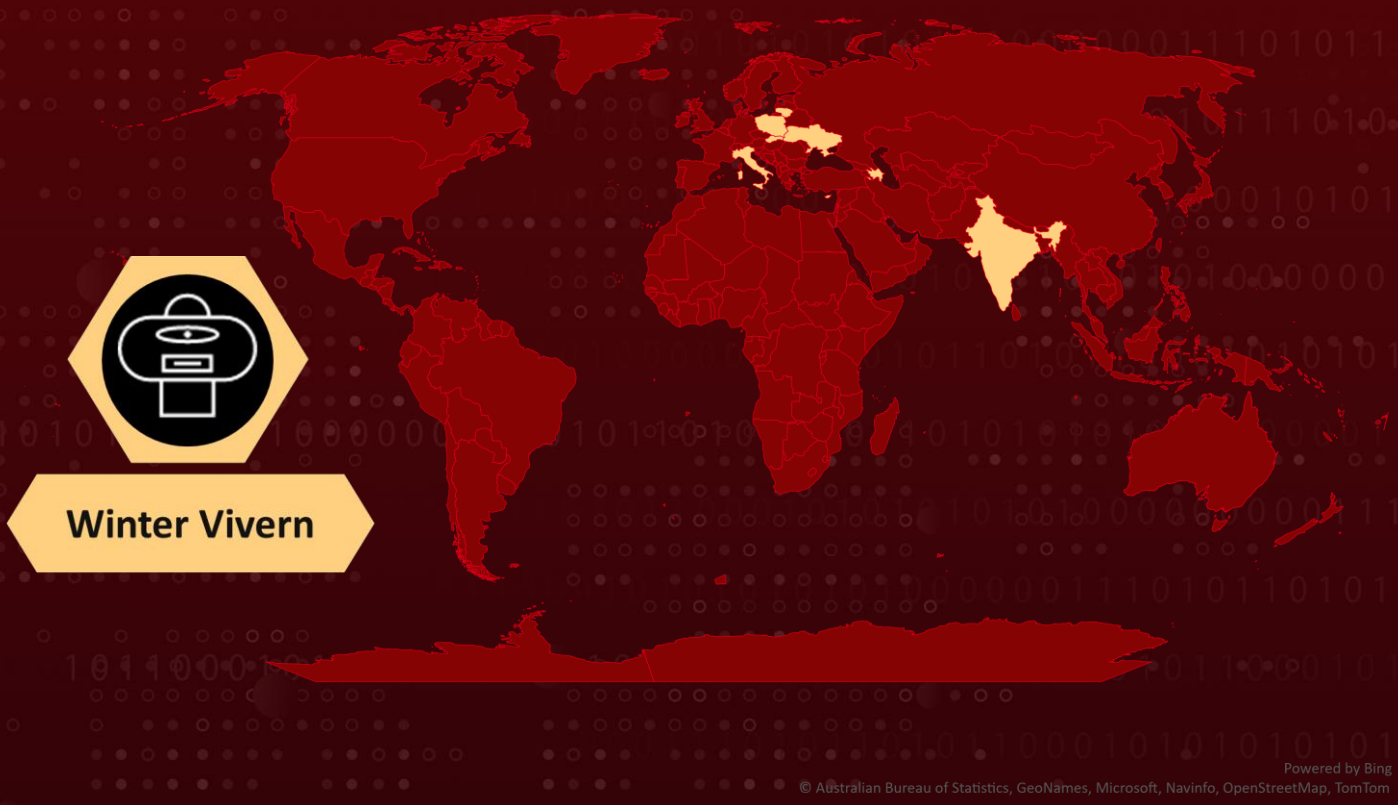
Winter Vivern with Pro-Russian Objectives Targets Government

Date of Publication	Admiralty code	TA Number
March 21, 2023	A1	TA2023149

Summary

First Appearance: July 2021
Actor Name: Winter Vivern (UAC-0114)
Target Industries: Government, Telecommunications, Private businesses.
Target Region: Azerbaijan, Cyprus, Poland, Lithuania, India, Vatican, Ukraine, Italy, and Slovakia.
Malware: APERETIF Trojan

Actor Map



Actor Details

#1 The Winter Vivern is a Russian-speaking Advanced Persistent Threat (APT) group that aligns its activities with global objectives that serve the interests of the governments of Belarus and Russia. The Winter Vivern utilizes multiple tactics, such as phishing websites, customized loaders, and malicious documents, to gain unauthorized access to sensitive information.

#2 The Winter Vivern APT has employed a macro-enabled Excel spreadsheet to infect the targeted system in its recent attacks. To prompt malware downloads from attacker-controlled servers, batch scripts that disguise as virus scanners are used in the infection process. One of the Trojans detected in the recent activities, named APERETIF, is designed to automate the collection of victim details, maintain access, and transmit data to the actor-controlled domain.

#3 Winter Vivern employs additional intrusion techniques, such as exploiting vulnerabilities in applications to infect specific targets. The group also uses staging servers as a supplemental resource to scan target networks and potentially compromise WordPress sites for hosting malware.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Winter Vivern (UAC-0114)	Unknown **MOTIVE** Information theft and espionage	Azerbaijan, Cyprus, Poland, Lithuania, India, Vatican, Ukraine, Italy, and Slovakia.	Government, Telecommunications , and Private businesses.

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 actor 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
TA0007 Discovery	TA0011 Command and Control	T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter
T1059.005 Visual Basic	T1137 Office Application Startup	T1055 Process Injection	T1055.011 Extra Window Memory Injection
T1036 Masquerading	T1497 Virtualization/Sandbox Evasion	T1202 Indirect Command Execution	T1010 Application Window Discovery
T1018 Remote System Discovery	T1057 Process Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery
T1518 Software Discovery	T1518.001 Security Software Discovery	T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol
T1573 Encrypted Channel	T1071.001 Web Protocols	T1497.003 Time Based Evasion	T1564 Hide Artifacts

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA1	0fe3fe479885dc4d9322b06667054f233f343e20 83f00ee38950436527499769db5c7ecb74a9ea41 a19d46251636fb46a013c7b52361b7340126ab27 a574c5d692b86c6c3ee710af69fccbb908fe1bb8 c7fa6727fe029c3eaa6d9d8bd860291d7e6e3dd0 f39b260a9209013d9559173f12fbc2bd5332c52a
URLs	hxxps[:]//applesaltbeauty[.]com/wordpress/wp-includes/widgets/classwp/521734i hxxps[:]//marakanas[.]com/Kkdn7862Jj6h2oDASGmpqU4Qq4q4.php hxxps[:]//natply[.]com/wordpress/wp-includes/fonts/ch/097214o hxxps[:]//ocs-romastassec[.]com/goog_comredira3cf7ed34f8.php
IPV4	176.97.66[.]57 179.43.187[.]175 179.43.187[.]207 195.54.170[.]26 80.79.124[.]135
Domains	bugiplaysec[.]com marakanas[.]com mfa_it_sec@outlook[.]com ocs-romastassec[.]com ocspdep[.]com security-ocsp[.]com troadsecow[.]com

Recent Breaches

https://hochuzhit.com/
https://mfa.gov.ua/en
https://www.esteri.it/en/
https://email.gov.in/

References

https://www.sentinelone.com/labs/winter-vivern-uncovering-a-wave-of-global-espionage/

https://www.domaintools.com/resources/blog/winter-vivern-a-look-at-re-crafted-government-maldocs/

https://cert.gov.ua/article/3761023

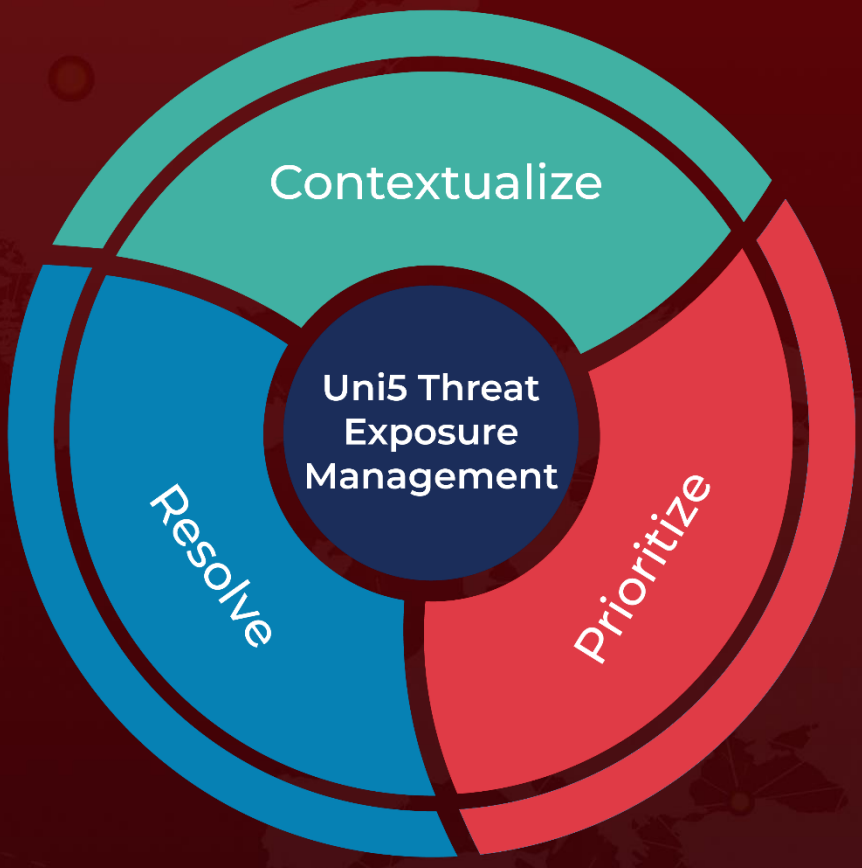
https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1lj/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1lj.pdf

https://lab52.io/blog/winter-vivern-all-summer/

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

March 21, 2023 • 5:16 AM

More at www.hivepro.com