Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

Gamaredon APT cyber feud strikes Ukrainian entities

Date of Publication	Admiralty Code	TA Number
December 21, 2022	A1	TA2022310

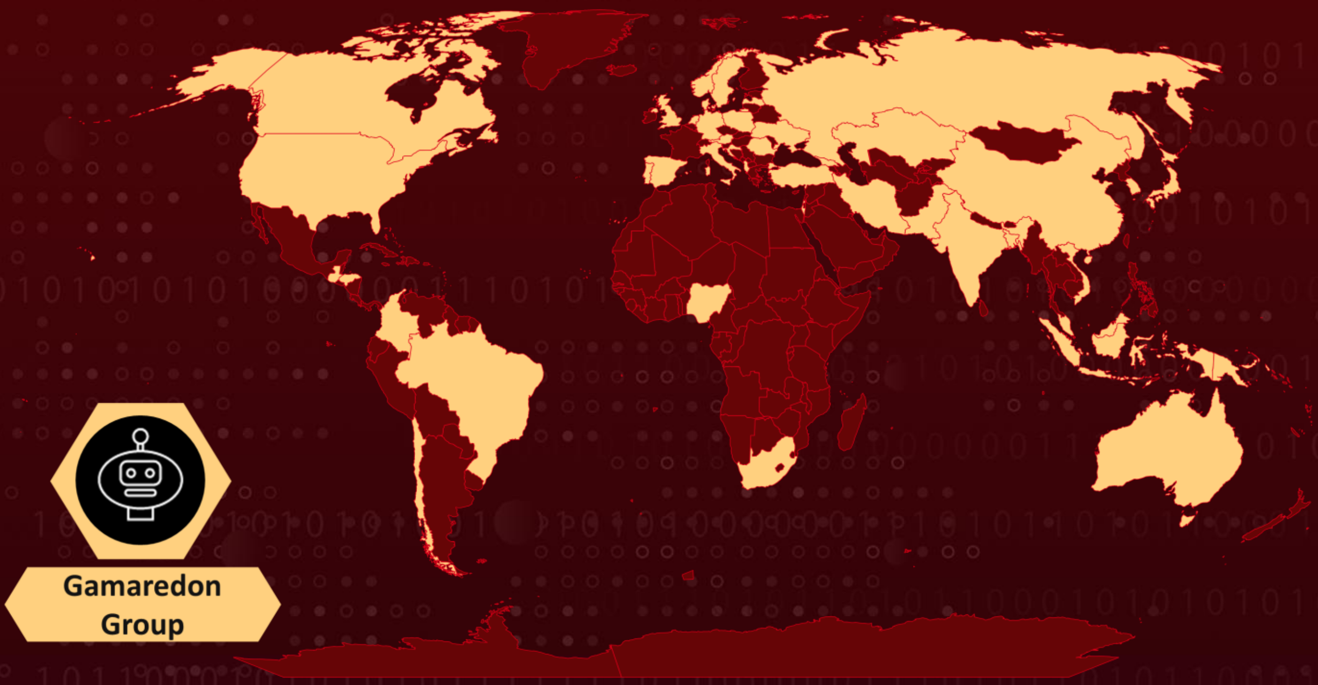
Summary

First appeared: 2013
Threat Actors: Gamaredon Group
Attack Region: Albania, Austria, Australia, Bangladesh, Brazil, Canada, Chile, China, Colombia, Croatia, Denmark, Georgia, Germany, Guatemala, Honduras, India, Indonesia, Iran, Israel, Italy, Japan, Kazakhstan, Latvia, Malaysia, Netherlands, Nigeria, Norway, Pakistan, Papua New Guinea, Poland, Portugal, Romania, Russia, South Africa, South Korea, Spain, Sweden, Turkey, UK, Ukraine, USA, Vietnam.

Attack Industries: Defense, Government, Law enforcement, NGO.

Attack: Gamaredon Group remains an active and resilient APT that poses a considerable threat to Ukraine, with increased obfuscation, domains, and tactics.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

One of the most ubiquitous, intrusive, consistently active, and laser-focused APTs targeting Ukraine in cyberspace is the Gamaredon group, also known as the Shuckworm. Gamaredon Group has employed fast flux DNS to improve functional efficacy. Fast flux DNS pivots through multiple IPs frequently, using each for a brief time to make IP-based block listing challenging. Threat actors frequently hijack legitimate services to query IP addresses in order to avoid DNS logging for malicious domains.

#2

The adversary adopted a variety of techniques to first infiltrate target devices, including VBScripts with randomly generated variable names and string concatenation for obfuscation. The threat actors employ two droppers. The first, typically referred to as 7ZSfxMod x86.exe, is a standard 7-Zip self-extracting (SFX) bundle that executes an integrated VBScript via Windows Script Host. The second dropper, generally called myfile.exe, drops two files and then runs them as VBScript using wscript.

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	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control
T1047 Windows Management Instrumentation	T1036 Masquerading	T1027 Obfuscated Files or Information	T1053 Scheduled Task/Job
T1102 Web Service	T1140 Deobfuscate/Decode Files or Information	T1547 Boot or Logon Autostart Execution	T1557 Adversary-in-the-Middle
T1559 Inter-Process Communication	T1566 Phishing	T1204 User Execution	

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	007483ad49d90ac2cabe907eb5b3d7eef6a5473217c83b0fe99d087ee7b3f6b3 00ca57feac8695e915664398e82131d9c70a45a68f741b78f13c88ad61c49cda 019e0910c6d62d6948ea6f2c83c62491b24cefa4dedc830b93b3c6176a7d9c76 01bead955437c198ddd134236a9fbe0442bb0e6170a59b039352929028972384 01da7d2722477522bf5cb0a757d922cfe07575984e15df56cd3658722a907f1b 02ed10858a777d2cf2c6cd22dfeccb338aa7ce381273de4eebaf6894334c7a34 0608ae0f28510591798a1603adabde86a9dbd67e1bfb1713c3f397d0d1a306d1 0720a9b5ecd98163208ad5d6d041679c0a6954d80685695df55b0e105dca7b09 07661128749c960ea28126cf6b76f9a223d6523c0df917e3ece46bfce2d0d3e9 08ff31342b174a2e07d6f81d9c2844f90b44b03f6a531fc06cd131b838d3e571 09472d6bfb1c142a3b02f73175254a5e961f91e792dc9b347b099944bcfeab6f
Domains	kyoungo[.]org labutens[.]ru muscarias[.]ru

TYPE	VALUE
Domains	ovinuso[.]ru pafamar[.]ru quyenzo[.]ru radiumo[.]ru a0662337.xsph[.]ru abbasa[.]ru bahadurdo[.]ru caccabius[.]ru dandani[.]ru eunogo[.]org faico[.]ru gypaetus[.]ru hafniumo[.]ru itidis[.]ru jadxv[.]ru
IP Addresses	104.248.36.191 140.82.29.65 141.164.45.200 155.138.138.195 155.138.252.221 159.89.31.49 162.33.178.129 167.99.138.16 188.166.43.183 194.180.191.105 199.247.14.64 206.81.0.182 45.77.11.107 45.77.229.187 45.77.237.252 82.146.39.104 91.188.222.50 95.179.216.77

References

https://unit42.paloaltonetworks.com/trident-ursa/

https://github.com/pan-unit42/iocs/blob/master/Gamaredon/Gamaredon_IoCs_DEC2022.txt

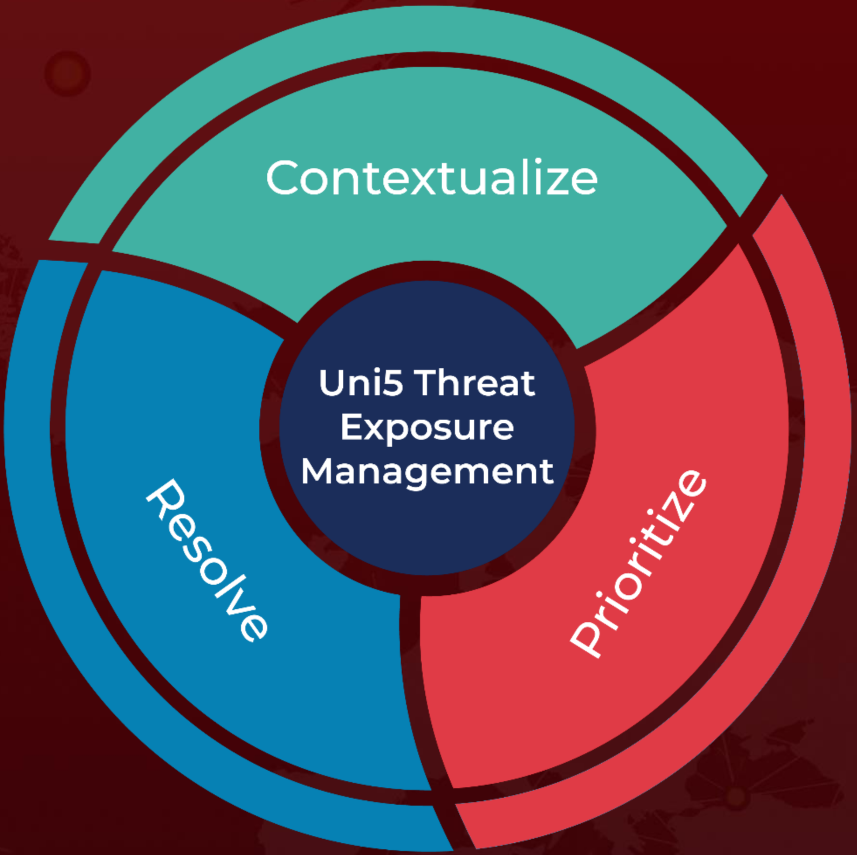
https://www.hivepro.com/attacks-on-european-union-and-ukrainian-government-entities-carried-out-by-the-armageddon-group/

https://attack.mitre.org/groups/G0047/

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

December 21, 2022 • 4:15 AM

More at www.hivepro.com