Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

Gamaredon Tools Revive Turla's Kazuar Backdoor to Target Ukraine

Date of Publication	Admiralty Code	TA Number
September 23, 2025	A1	TA2025291

Summary

Attack Commenced: January 2025

Threat Actors: **Gamaredon** (aka Primitive Bear, Winterflounder, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Shuckworm, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard), **Turla** (aka Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Secret Blizzard, Pensive Ursa)

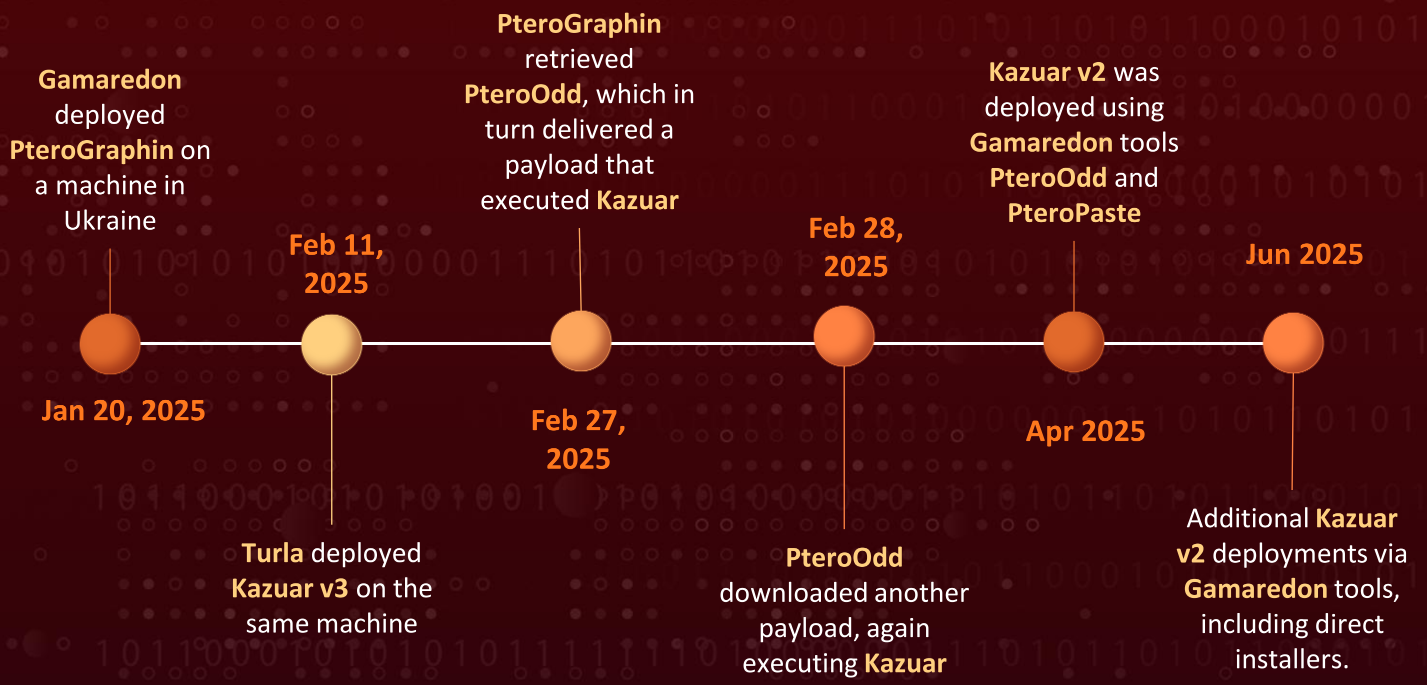
Malware: Kazuar backdoor, PteroOdd

Targeted Country: Ukraine

Targeted Industries: Government, Defense, Diplomatic Entities

Attack: Turla and Gamaredon, two long-standing cyber-espionage groups linked to Russia's Federal Security Service (FSB), have intensified joint operations against Ukraine, combining Turla's sophisticated Kazuar backdoor with Gamaredon's expanding Ptero toolset. A recent 2025 campaign showcased how their collaboration bridges broad access with deep, sustained espionage, underscoring the growing convergence of Russia's intelligence arms in pursuit of strategic objectives.

Attack Timeline



Jan 20, 2025
Gamaredon deployed **PteroGraphin** on a machine in Ukraine

Feb 11, 2025
Turla deployed **Kazuar v3** on the same machine

Feb 27, 2025
PteroGraphin retrieved **PteroOdd**, which in turn delivered a payload that executed **Kazuar**

Feb 28, 2025
PteroOdd downloaded another payload, again executing **Kazuar**

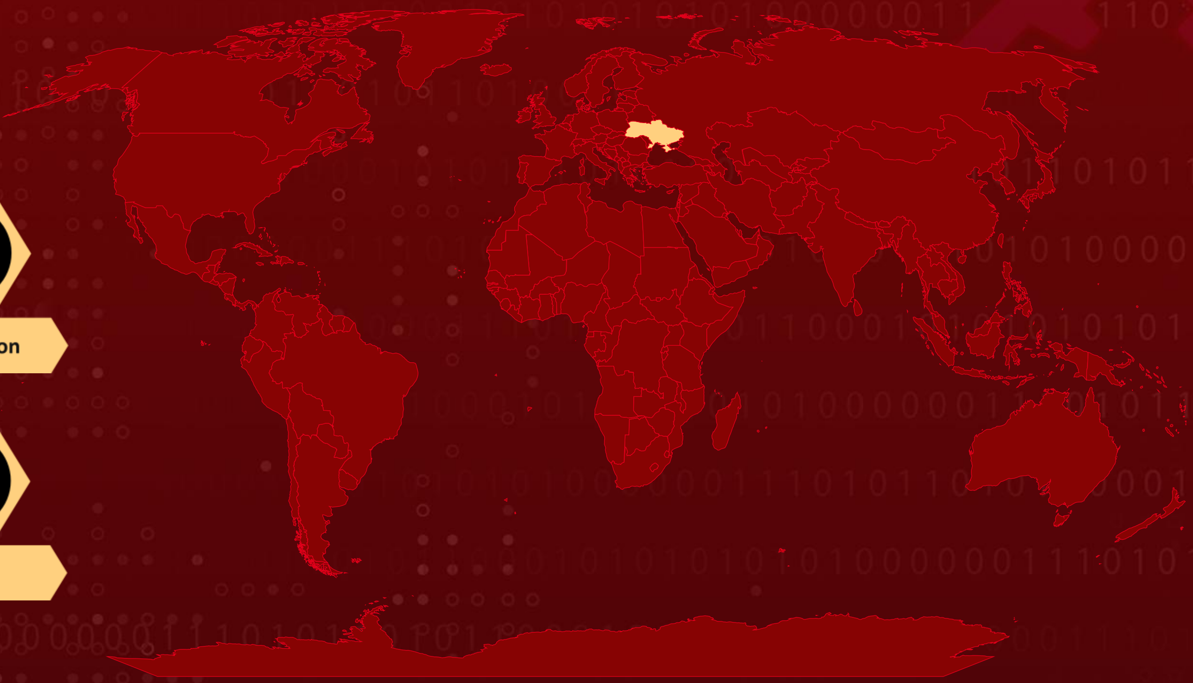
Apr 2025
Kazuar v2 was deployed using **Gamaredon** tools **PteroOdd** and **PteroPaste**

Jun 2025
Additional **Kazuar v2** deployments via **Gamaredon** tools, including direct installers.

Attack Regions

Gamaredon

Turla



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

Attack Details

#1

Turla and Gamaredon, two threat groups linked to the Russian Federal Security Service (FSB), have been observed conducting coordinated cyber operations against Ukraine. Both groups, tied to Moscow's intelligence structure, bring distinct capabilities that, when combined, create a potent espionage partnership.

#2

Turla has been active since at least 2004, with possible origins tracing back to the late 1990s. Gamaredon has operated since 2013 and is noted for persistent campaigns against Ukrainian organizations. Turla is attributed to the FSB's Center 16, the agency's primary signals intelligence unit, while Gamaredon is believed to be operated from Center 18, which is tied to counterintelligence operations.

#3 In February 2025, Gamaredon deployed multiple tools, including PteroLNK, PteroStew, PteroOdd, PteroEffigy, and the PowerShell-based PteroGraphin. During this campaign, PteroGraphin was used to restart Turla's Kazuar v3 backdoor, an advanced C# espionage implant exclusively linked to Turla since 2016. While the initial entry point remains unidentified, the incident illustrates how the two groups align their efforts: Gamaredon provides broad access through its toolset, while Turla leverages Kazuar for deeper, long-term espionage.

#4 Gamaredon continues to expand its Ptero family of tools, including PteroGraphin, PteroOdd, and PteroPaste, which are designed to deliver additional payloads. PteroGraphin, in particular, establishes persistence through Microsoft Excel add-ins and scheduled tasks, while using the Telegraph API for command-and-control. Together, these evolving capabilities underscore the convergence of Russia's intelligence branches in pursuing long-term strategic objectives in Ukraine.

Recommendations

Enhanced Endpoint Monitoring: Deploy advanced endpoint detection and response (EDR) solutions to identify suspicious activity related to Kazuar backdoor and other tools. Monitor for unusual execution of PowerShell scripts, scheduled tasks, and Microsoft Excel add-ins.

Network and C2 Traffic Analysis: Monitor outbound traffic for connections to known command-and-control channels, including the Telegraph API used by PteroGraphin. Implement anomaly detection for unusual network patterns indicative of exfiltration or lateral movement.

Segmentation and Access Controls: Isolate critical systems and sensitive networks to limit lateral movement. Use multi-factor authentication (MFA) and strict access controls for administrative and privileged accounts.

Patch Management and System Hardening: Ensure all endpoints and servers are up to date with security patches, particularly those running Microsoft Office and Windows environments. Enforce least-privilege policies to reduce the impact of compromised accounts.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	T1583 Acquire Infrastructure
T1583.001 Domains	T1583.004 Server	T1583.007 Serverless	T1584 Compromise Infrastructure
T1584.003 Virtual Private Server	T1608 Stage Capabilities	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1574 Hijack Execution Flow	T1574.001 DLL	T1140 Deobfuscate/Decode Files or Information	T1480 Execution Guardrails
T1480.001 Environmental Keying	T1036 Masquerading	T1036.005 Match Legitimate Resource Name or Location	T1057 Process Discovery
T1012 Query Registry	T1082 System Information Discovery	T1083 File and Directory Discovery	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1573 Encrypted Channel	T1573.001 Symmetric Cryptography	T1102 Web Service

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3ecb09e659bcb500f9f40d022579a09acb11aec3a92c03e7d3fd2e56982d9eea
Filenames	scrss.ps1, ekrn.ps1, Sandboxie.vbs

TYPE	VALUE
SHA1	7db790f75829d3e6207d8ec1cbcd3c133f596d67, 2610a899fe73b8f018d19b50be55d66a6c78b2af, 3a24520566bbe2e262a2911e38fd8130469ba830, da7d5b9ab578ef6487473180b975a4b2701fda9e, d7df1325f66e029f4b77e211a238aa060d7217ed, ff741330cc8d9624d791de9074086bbfb0e257dc, a7acee41d66b537d900403f0e6a26ab6a1290a32, 54f2245e0d3adec566e4d822274623bf835e170c, 371ab9eb2a3da44099b2b7716de0916600450cfd, 4a58365eb8f928ec3cd62ff59e59645c2d8c0ba5, 214dc22fa25314f9c0dda54f669ede72000c85a4
IPv4	64[.]176[.]173[.]164, 85[.]13[.]145[.]231, 91[.]231[.]182[.]187, 185[.]118[.]115[.]15, 77[.]46[.]148[.]242, 168[.]119[.]152[.]19, 217[.]160[.]0[.]33, 217[.]160[.]0[.]159
Domains	lucky-king-96d6[.]mopig92456[.]workers[.]dev, eset[.]ydns[.]eu, hauptschule-schwalbenstrasse[.]de, ekrn[.]ydns[.]eu, fjsconsultoria[.]com, ingas[.]rs, abrargeospatial[.]ir, www[.]brannenburger-nagelfluh[.]de, www[.]pizzeria-mercy[.]de

References

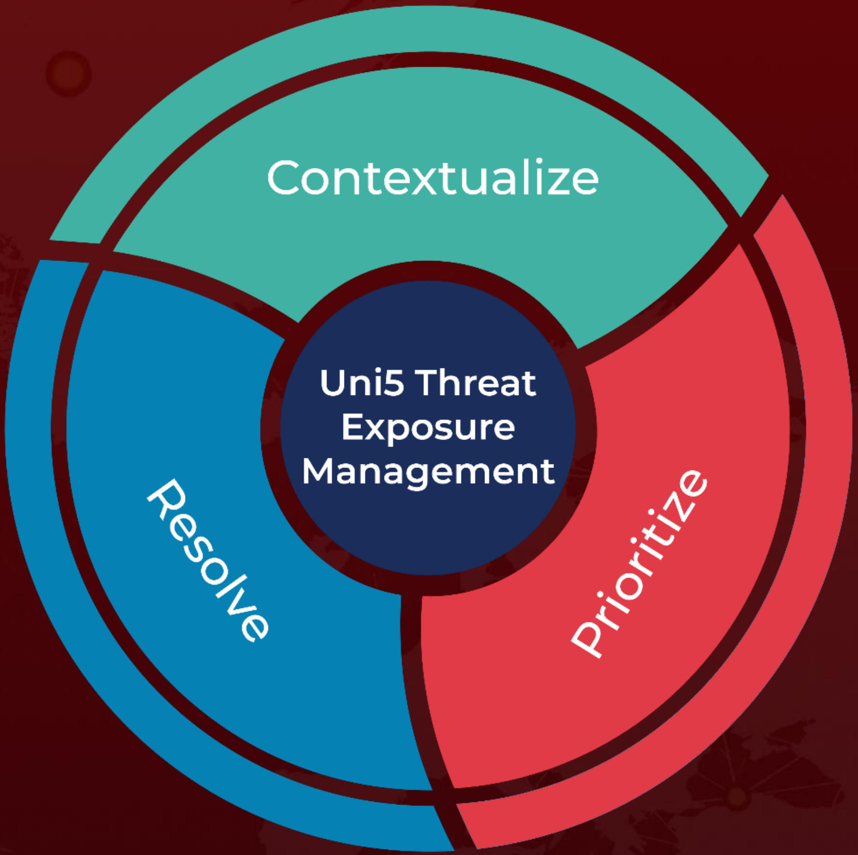
https://www.welivesecurity.com/en/eset-research/gamaredon-x-turla-collab/

https://hivepro.com/threat-advisory/turla-updates-kazuar-backdoor-to-target-ukraines-defense-sector/

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

September 23, 2025 • 1:00 AM

More at www.hivepro.com