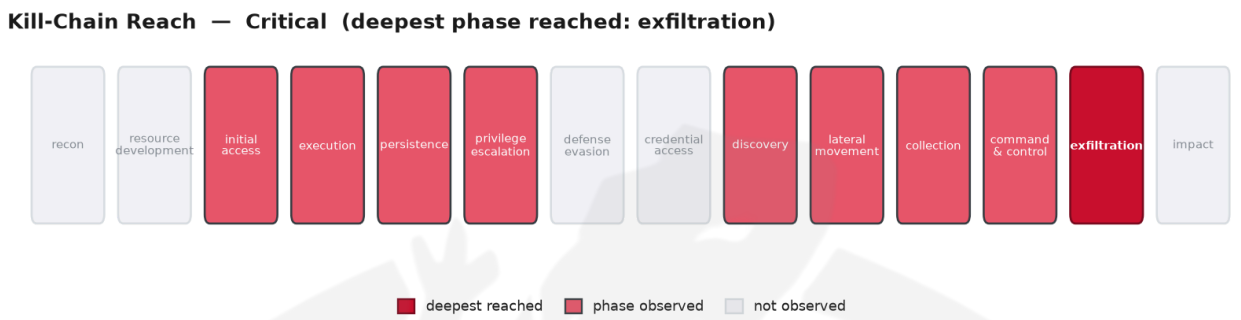
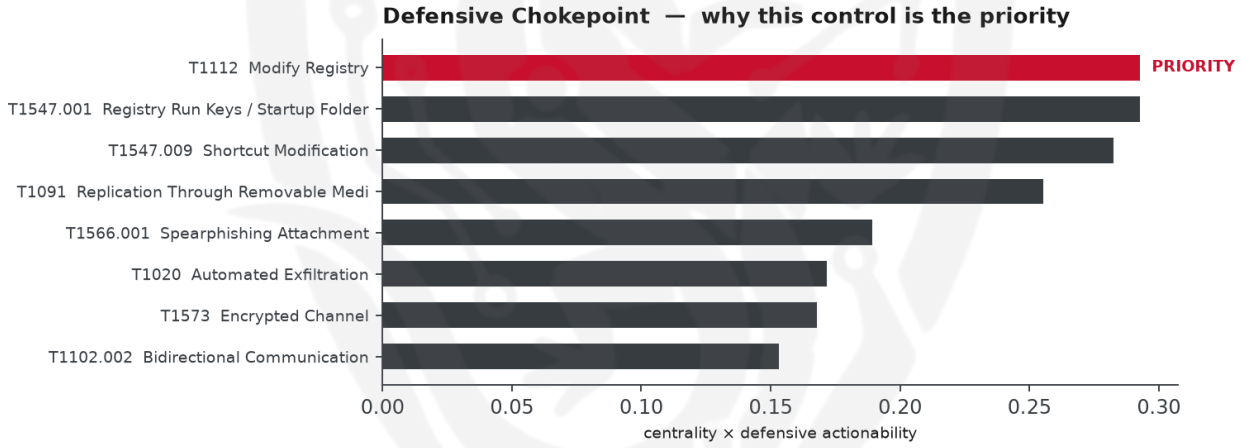
THREAT REPORT: GAMAREDON

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The source attributes this activity to Gamaredon, a threat actor targeting Ukraine's government and defense sectors with a range of malware families, including GammaPhish, GammaLoad, GammaWorm, and GammaSteal. The actor's campaign involves exploiting various techniques to gain access to sensitive information. Priority should be given to monitoring and restricting access to sensitive registry keys to prevent further damage. The threat actor's use of multiple techniques, including spearphishing and malicious file execution, poses a significant risk to the targeted sectors.

Threat Overview

Gamaredon, the attributed threat actor, utilizes a variety of malware families, including GammaPhish, GammaLoad, GammaWorm, and GammaSteal, to target Ukraine's government and defense sectors. The central vulnerability exploited is currently unknown, but the actor is also leveraging CVE-2025-8088. The victimology indicates a focus on Ukrainian government and defense entities.

Attack Chain and Priority Control

The observed techniques employed by Gamaredon form a complex attack chain, involving scheduled tasks, standard encoding, malicious files, and spearphishing attachments, among others. The priority technique identified is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

There is currently no observed hosting provider or ASN information available for the malicious infrastructure. Additionally, no malware families have been corroborated by abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1053.005 Scheduled Task
- T1132.001 Standard Encoding
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1091 Replication Through Removable Media
- T1005 Data from Local System
- T1547.009 Shortcut Modification
- T1112 Modify Registry
- T1020 Automated Exfiltration
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1102.002 Bidirectional Communication
- T1071.001 Web Protocols
- T1059.005 Visual Basic
- T1204.001 Malicious Link
- T1564.004 NTFS File Attributes
- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3082).

- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.508; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
APT37	0.508
Windshift	0.5015
APT19	0.5011
RedCurl	0.488
Inception	0.4862

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator
Domain	iiwdsxwamylbwwsoyrmj[.]supabase[.]co
Domain	quitethepastry[.]ru
Domain	efficiency-planes-emotions-fascinating[.]trycloudflare[.]com
Domain	moment-cat-qld-place[.]trycloudflare[.]com
URL	hxxps://efficiency-planes-emotions-fascinating[.]trycloudflare[.]com
URL	hxxps://moment-cat-qld-place[.]trycloudflare[.]com/sylvilagus
URL	hxxps://quitethepastry[.]ru
Hash	1794369214b7f62e70a0485e61335c61

Type	Indicator
Hash	8e1624d110c090ff57d4b493a9107c66