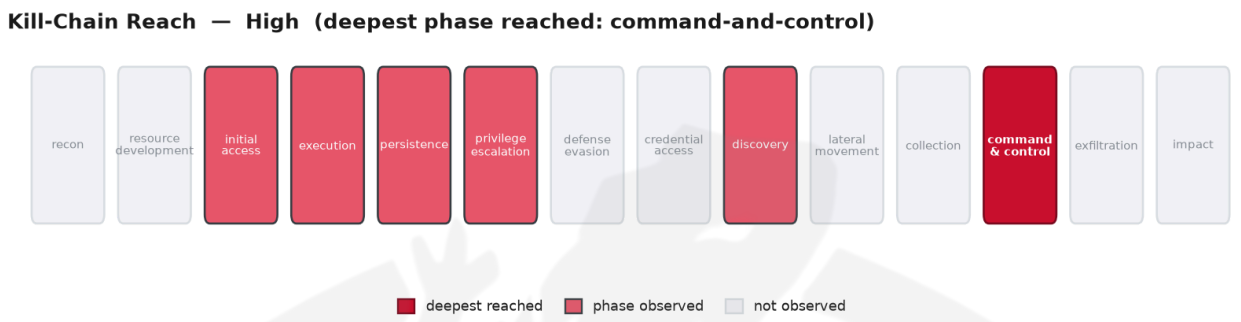
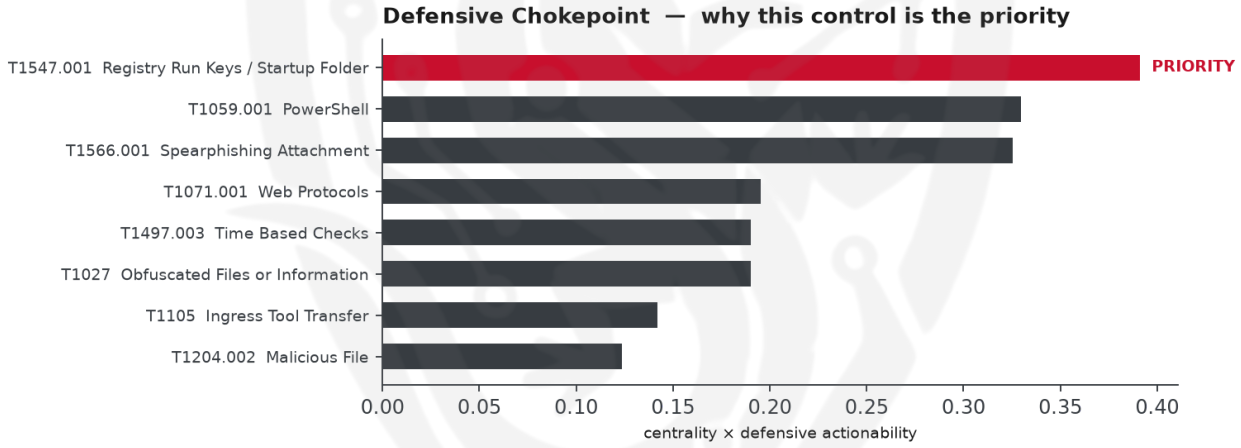
THREAT REPORT: GAMAREDON

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 defense and government sectors by exploiting CVE-2025-8088. The campaign's impact is considered high due to its potential for command-and-control. Priority should be given to patching the vulnerability and auditing Windows Startup folders and registry keys for unauthorized entries. The actor's use of malicious files and spearphishing attachments poses a significant threat to the targeted sectors.

Threat Overview

Gamaredon, the attributed threat actor, is utilizing the exploited vulnerability CVE-2025-8088 to target Ukraine. Although the specific malware families used are not sufficiently identified, the actor's techniques include malicious file usage, system checks, and spearphishing attachments. The targeted sectors, defense and government, are at risk due to the actor's tactics.

Attack Chain and Priority Control

The observed techniques form a chain that includes malicious file usage, system checks, and spearphishing attachments, ultimately leading to the exploitation of CVE-2025-8088. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which serves as a chokepoint in the attack chain. To mitigate this threat, the priority control is: Patch CVE-2025-8088 on all affected systems as the top priority, then: Audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries; alert on .lnk or script creation in Startup by browser/email temp paths.

Infrastructure and Corroboration

Although specific hosting providers or ASNs are not observed, abuse.ch corroborates the involvement of the Gamaredon malware family. However, according to AbuseIPDB, there are no 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)

- T1204.002 Malicious File
- T1497.001 System Checks
- T1566.001 Spearphishing Attachment
- T1497.003 Time Based Checks
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1564.004 NTFS File Attributes

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.4118).
- Operational risk: High (score 0.594, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.603; 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
Nomadic Octopus	0.603
Windshift	0.5613
APT19	0.5303
TA459	0.5303
Gallmaker	0.5276

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Gamaredon.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
Hash	2add9429d2822ae0c01c08bbd66c3a110ef2e9c3a00cded1477657e9024e391e	Gamaredon
Hash	cb65f5873c72d707371ec56fb8ba501a5c7f5940e9c5a2d28c9b379ce216900c	Gamaredon
Hash	1c170b7470d507378ddb78e9d66305f1184e965baaf2d27ededb23a318a58953	
Hash	507b2fcdae058cebbd550965b90c44e878d7a2463058c846eeb68f0dc1b48eda	
Hash	bf338d88f60c0d352cd0d1b5e4bc6a1d9f1ac8fe1df48516ec0042cafda821e9	
Hash	f668bd551859007cf2cc2a62bf0bf5414870a04e9782590c9bf85c849ddb308b	
Hash	f9d2907d6b1de3078a0f111cc98764a92baf5ebd06cc8ab02637a65eff3b7f3a	
Hash	0a9bc91e7ea2c3931f662eea37c00c7c26c8996b65f6f7afe6cce8f6114f94b6	
Hash	39dd1bd3bccc314d8933e5c41ed2ab084e4e20af569f77b7cf09abc5855b9483	
Hash	1ebbdf3671cd5ca25a8a8e7ca2f6e46dd22c631e01bfcc5c909ae2fd680bf458	
Hash	a113090d748d0dac7d488c97f1305af2	Gamaredon
Hash	473c65b922d3308a98c6b76c7d99a196	Gamaredon

Type	Indicator	Context
Hash	4082096ec0b8f723a79a224a6b6d37cd	
Hash	587a464ffc174288d3f66d1845133229	
Hash	8ca36b9cbd72d1f4ab4a9c8fcf85fe7e	
Hash	addf25d1f994729f2d3cbb3d0ab49897	
Hash	ea610ea6a8d69cb1e93fb79d4a8fa26f	
Hash	02462fa8f816b2ff21898612552d7845abcb9070	
Hash	1f34a8fad545554420650a8518d4199431fc2920	Gamaredon
Hash	23e076f5db64fb51226ef56a60bae6424b06a432	
Hash	42428f21b0114e390c6129f1fb24b42e97a8f7f7	
Hash	4f29c2059dcba412c3ef0100e839cf85fb0f62c1	
Hash	ad102478adda75ef6c6985187fc1e8b0bc1edded	
Hash	d8d789af0ede2ce38a50b516f7603376589ae141	Gamaredon

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.