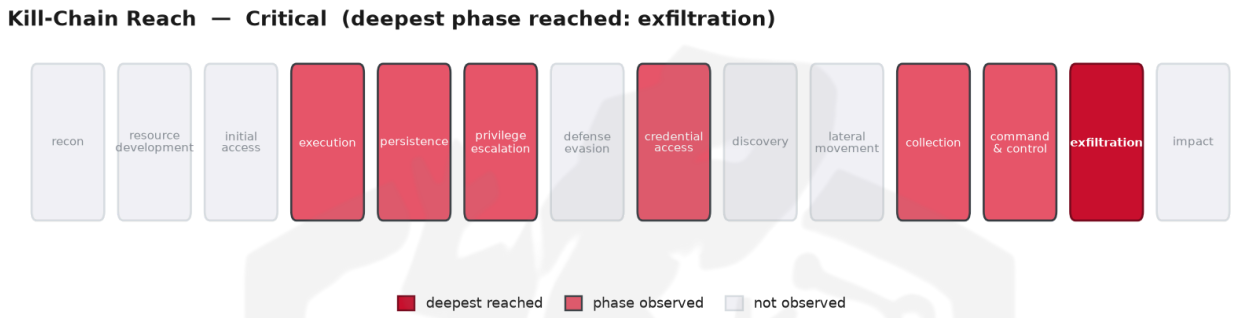
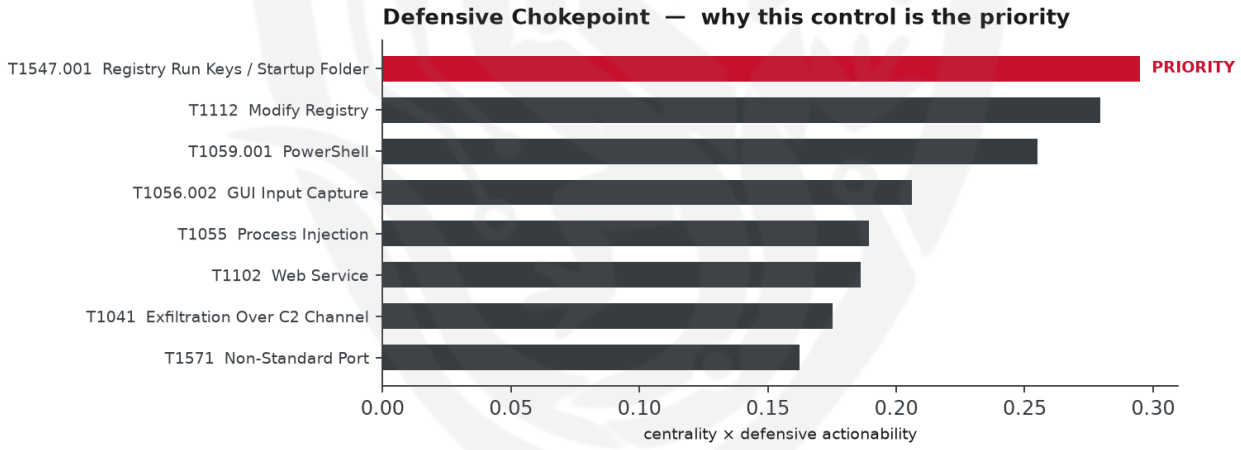
THREAT REPORT: GAMAREDON'S GAMMASTEEL INFOSTEALER

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 GammaSteel, GammaLoad, and others. The threat actor's primary goal is to collect and exfiltrate sensitive data. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to mitigate the threat. The actor's use of various techniques, including data staging and process injection, poses a significant risk to affected organizations.

Threat Overview

Gamaredon, the attributed threat actor, utilizes a variety of malware families to target Ukrainian government and defense entities. The malware families involved include GammaSteel, GammaLoad,

GammaPhish, GammaWorm, and GammaWipe. Although the central CVE is insufficient, the threat actor employs multiple techniques to achieve their objectives, including data collection, staging, and exfiltration.

Attack Chain and Priority Control

The observed attack chain involves various techniques, including data collection from local systems, automated collection, and exfiltration over command and control channels. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended priority control is to "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

There is no notable infrastructure or corroboration from third-party sources, as no hosting providers or ASNs have been observed, and no malware families have been corroborated by abuse.ch. Additionally, 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)

- T1025 Data from Removable Media
- T1074.001 Local Data Staging
- T1119 Automated Collection
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1112 Modify Registry
- T1102 Web Service
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1056.002 GUI Input Capture
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information
- T1567.002 Exfiltration to Cloud Storage
- T1059.005 Visual Basic
- T1008 Fallback Channels
- T1564.004 NTFS File Attributes

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.3105).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3831; 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
Gorgon Group	0.3831
Confucius	0.3472
Gamaredon Group	0.3424
Threat Group-3390	0.3361
Leviathan	0.3345

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	justsstop[.]ru
URL	hxxps://justsstop[.]ru/

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert.k@3sdragon.eu

- **Control applied:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Observed here:** Gamaredon used T1112 Modify Registry here as an alternative persistence technique.
- **Projected pivot:** T1112 Modify Registry (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The Gamaredon actor could pivot to modifying registry keys using T1112 to maintain persistence or gain elevated privileges, potentially by altering registry values that affect system or security settings. They may attempt to use this technique to bypass the blocked control, exploiting weaknesses in registry key permissions or using compromised credentials to make modifications. The defensive countermeasure would be to Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users.

Detection and hardening for the pivot (T1112 Modify Registry)

- **Telemetry:** Sysmon (registry); EDR registry telemetry
- **Detect:**
  - Sysmon 12/13/14 (registry object add/set/rename) on sensitive keys
  - Writes to Run keys, service keys, security-provider and policy keys
  - reg.exe / regsvr32 spawned by office or script interpreters
- **Harden:**
  - Audit and restrict write access to security-sensitive registry hives
  - Application control to limit who can modify policy/security keys
- **MITRE:** M1047 Audit, M1024 Restrict Registry Permissions · DS0024 Windows Registry, DS0009 Process