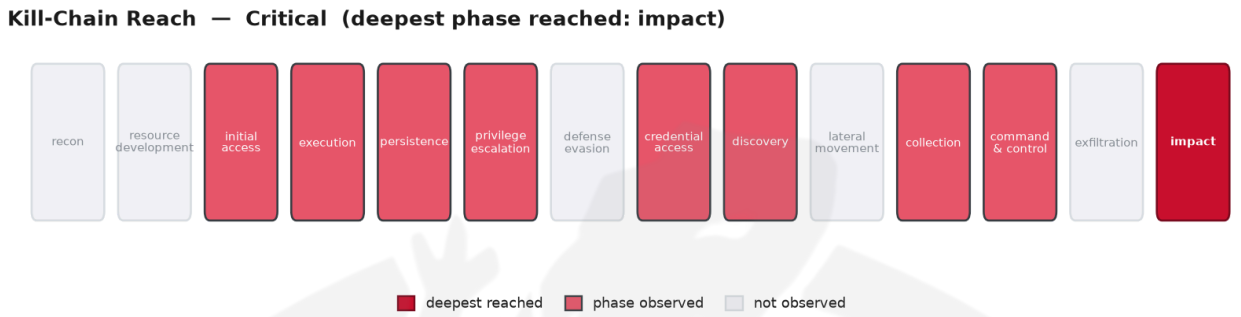
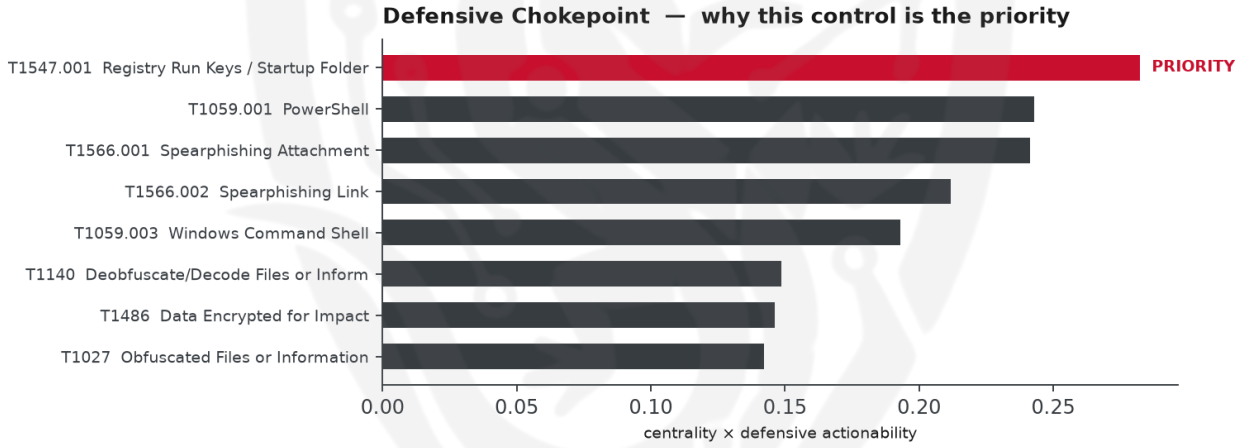
THREAT REPORT: LARVA-26005 CAMPAIGN

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 Larva-26005, a threat actor that has been observed exploiting the CVE-2017-8291 vulnerability to target organizations in the Defense and Technology sectors. The actor utilizes a range of malware families, including Xctdoor and Hydraq, to gain unauthorized access to systems. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries, as well as patching the CVE-2017-8291 vulnerability on all affected systems. The threat actor's activities have been assessed as posing a critical operational risk.

Threat Overview

Larva-26005, the attributed threat actor, has been observed using various malware families, including Xctdoor, Hydraq, and others, to exploit the CVE-2017-8291 vulnerability. The victimology of this campaign is focused on the Defense and Technology sectors, although the targeted country is not specified. The

malware families used by the actor are designed to capture screen data, log keystrokes, and discover system information, among other techniques.

Attack Chain and Priority Control

The observed techniques used by Larva-26005 form a complex attack chain, involving scheduled tasks, screen capture, keylogging, and other methods. The priority technique in this chain is T1547.001 Registry Run Keys / Startup Folder, which serves as a graph chokepoint. 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. In parallel, patch CVE-2017-8291 on all affected systems."

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this campaign, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with an AbuseIPDB confidence 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
- T1113 Screen Capture
- T1056.001 Keylogging
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1057 Process Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1059.005 Visual Basic
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer
- T1055.001 Dynamic-link Library Injection

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2973).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6047; 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
Molerats	0.6047
Windshift	0.5786
APT37	0.5677
Rancor	0.5669
Confucius	0.5357

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	www[.]fabioluciani[.]com
Domain	casinolegit[.]info
Domain	ntsgo[.]name
Domain	ntsgo-corp[.]com
Domain	casinolegit[.]fun
Domain	casinosec[.]info

Type	Indicator
Domain	cristiantirira[.]com
Domain	desk-azureft[.]info
Domain	hesenorm[.]info
Domain	koramate[.]fun
Domain	grace2019[.]teamernst[.]net
Hash	0d2e61c8a5e6280e065b61e75b848c68
Hash	12391f66ee33d379108fd649a999e1a0
Hash	01b58f2ff2c14feed46a0768ea46686d
Hash	07766e6e9d9f86775ad564a65af292c1
Hash	08e19a0d516d14e564359ee111ed2586

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@salacti.com

- **Control applied:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Observed here:** T1547.001 Registry Run Keys / Startup Folder was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1543 Create or Modify System Process (persistence)
- **Basis:** of the 18+ groups that use Registry Run Keys / Startup Folder, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The Larva-26005 actor could pivot to creating or modifying system processes (T1543) as a means to maintain persistence and execute malicious code, potentially by disguising their payloads as legitimate system services to evade detection. This technique may be particularly appealing as it allows the actor to leverage existing system processes to carry out their objectives, which could be more challenging to detect than creating new startup entries. To counter this, the mandated defensive control of restricting service/daemon creation to admins and monitoring service and driver installs would likely be effective.

Also plausible (same tactic): T1098 Account Manipulation (n=12, lift 2.0), T1112 Modify Registry (n=17, lift 1.7)

Detection and hardening for the pivot (T1543 Create or Modify System Process)

- **Telemetry:** Windows Security / System log; Sysmon

- **Detect:**
  - System 7045 (new service installed); Security 4697 (service installed)
  - Sysmon 1 for sc.exe / services created; unusual ImagePath or user-context services
  - Registry writes under HKLM\SYSTEM\CurrentControlSet\Services
- **Harden:**
  - Restrict service creation to admins; application control on service binaries
  - Baseline installed services and alert on new/anomalous ones
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0019 Service, DS0024 Windows Registry, DS0009 Process