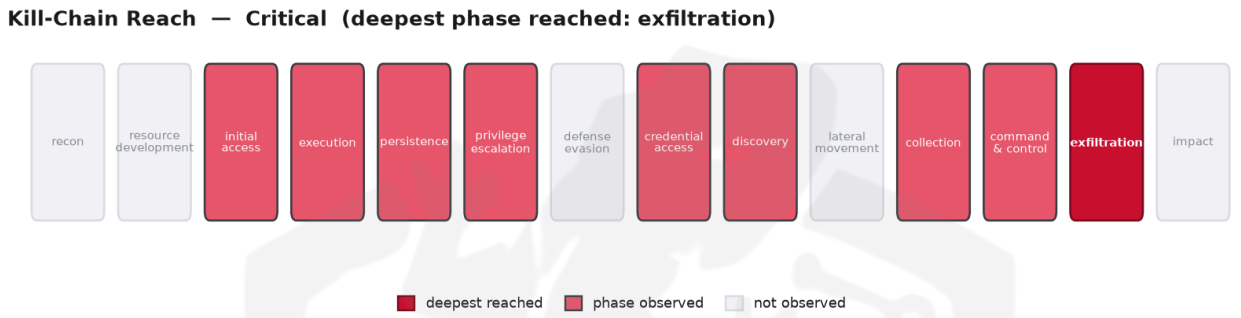
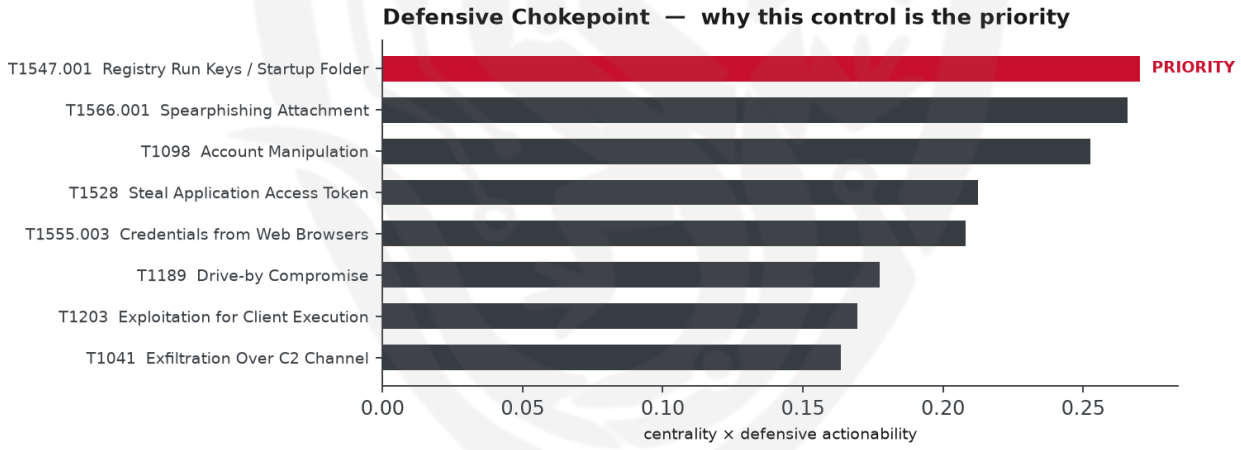
THREAT REPORT: TA488 TARGETS OUTLOOK WITH OWAREAPER AND ZIMREAPER MALWARE

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 TA488, a threat actor exploiting CVE-2026-42897 to target various sectors including Government, Telecommunications, Finance, Hospitality, Aerospace, and Defense. The malware families used are OWAReaper and ZimReaper. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries, as well as patching CVE-2026-42897 on all affected systems. The threat actor's techniques include keylogging, spearphishing, and exfiltration over C2 channels, posing a critical operational risk.

Threat Overview

TA488 is exploiting CVE-2026-42897, utilizing malware families OWAReaper and ZimReaper, to target multiple sectors. The victimology indicates that the threat actor is targeting organizations in various

industries, although the specific country targeted is insufficiently documented. The central vulnerability exploited is CVE-2026-42897, with the threat actor employing a range of techniques to achieve their objectives.

Attack Chain and Priority Control

The observed techniques employed by TA488 form a complex attack chain, involving standard encoding, keylogging, JavaScript, and DNS techniques, among others. The priority technique identified is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the 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-2026-42897 on all affected systems.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this activity. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with a confidence level of 80% or higher by AbuseIPDB, 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)

- T1132.001 Standard Encoding
- T1056.001 Keylogging
- T1059.007 JavaScript
- T1071.004 DNS
- T1074.001 Local Data Staging
- T1114.001 Local Email Collection
- T1566.001 Spearphishing Attachment
- T1140 Deobfuscate/Decode Files or Information
- T1555.003 Credentials from Web Browsers
- T1528 Steal Application Access Token
- T1087.004 Cloud Account
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1098 Account Manipulation
- T1027 Obfuscated Files or Information
- T1203 Exploitation for Client Execution
- T1189 Drive-by Compromise
- T1071.001 Web Protocols
- T1102.001 Dead Drop Resolver

- T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2846).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3868; 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
APT33	0.3868
APT19	0.375
BRONZE BUTLER	0.3714
MuddyWater	0.3647
Inception	0.3638

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	acocdn[.]com
Domain	dnsrecursive[.]eu
Domain	tdndns[.]com
Hash	6897b649f29e54d8910459963bbf94ed5c7a4fe66a56bc5962540b226b8e48c4

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:** T1053 Scheduled Task/Job (persistence)
- **Basis:** of the 37+ groups that use Registry Run Keys / Startup Folder, this pairing runs 1.9x above base rate, a disproportionately-coupled move rather than the obvious one.

The adversary could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence, as this technique allows them to execute malicious code at a specified time or interval, potentially evading detection by blending in with legitimate system tasks. This technique may be particularly appealing to TA488, as it enables them to schedule tasks that can run under the context of a privileged account, increasing the likelihood of achieving their objectives. To counter this potential pivot, the defensive control of alerting on new scheduled tasks (Event ID 4698), restricting schtasks/at to admins, and baselining legitimate task creators should be implemented.

Also plausible (same tactic): T1543 Create or Modify System Process (n=18, lift 1.8), T1112 Modify Registry (n=17, lift 1.7)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File