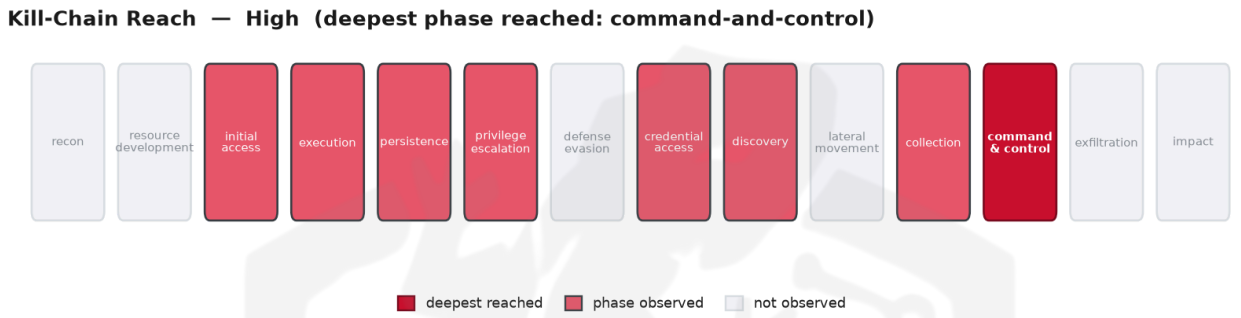
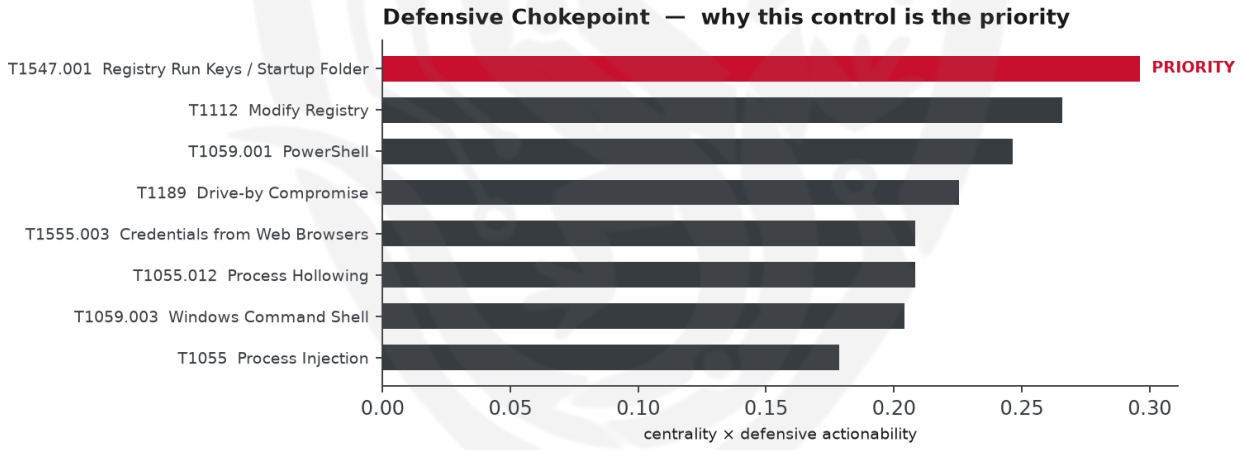
THREAT REPORT: ERRTRAFFIC MALWARE CAMPAIGN

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 observed cluster of activity, associated with the ErrTraffic malware campaign, has been exploiting CVE-2026-48294 to target unspecified countries and sectors. The campaign involves multiple malware families, including Vidar, Okobot, and LegionLoader. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries, as well as patching the exploited vulnerability. The threat actor's identity remains unknown.

Threat Overview

The threat actor, associated with the ErrTraffic malware campaign, utilizes a range of malware families, including Vidar, Okobot, LegionLoader, OnionDrop, BabaDedaLoader, TELEPUZ, and ClipBanker, to exploit the CVE-2026-48294 vulnerability. The campaign's victimology and targeted sectors are currently

unknown. The malware families and exploited vulnerability suggest a complex and potentially widespread threat.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including keylogging, process injection, and registry modification. 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 following control is recommended: 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-2026-48294 on all affected systems.

Infrastructure and Corroboration

The malicious infrastructure associated with the ErrTraffic malware campaign is hosted on Omegatech LTD. Additionally, abuse.ch has corroborated the presence of malware families such as ClearFake, Lumar, Unknown Webinject, and Unknown malware. However, AbuseIPDB has not flagged any indicators with high confidence, with the highest confidence seen being 7%.

Technical Appendix

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

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

- T1218.011 Rundll32
- T1056.001 Keylogging
- T1036.005 Match Legitimate Resource Name or Location
- T1497.001 System Checks
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1112 Modify Registry
- T1555.003 Credentials from Web Browsers
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1059.003 Windows Command Shell
- T1189 Drive-by Compromise
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow
- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.3119).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4423; 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
APT19	0.4423
Dark Caracal	0.4415
Patchwork	0.4364
Darkhotel	0.4291
RedCurl	0.3975

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 7%.
- Malware families corroborated by abuse.ch: ClearFake, Lumar, Unknown Webinject, Unknown malware.
- 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
IP	158[.]94[.]208[.]104	AbuseIPDB 7% (DE) · Unknown malware · AS202412 Omegatech LTD
Domain	networksolutionson[.]sbs	Unknown malware

Type	Indicator	Context
Domain	verification-cdn-cloud[.]beer	Unknown malware · malware_download
Domain	istile-c-cloud[.]beer	Unknown malware
Domain	ghdnsserverns[.]beer	Unknown malware
Domain	mnoskemp[.]beer	Unknown malware
Domain	ap7[.]supportly[.]au	Unknown malware
Domain	dreff-nsdns[.]beer	Unknown malware
Domain	letsgomakemoneyoncaptcha[.]beer	ClearFake
Domain	bootstrup-cdn-ns[.]beer	Unknown malware
Domain	nslsconscloud[.]beer	Unknown malware
Domain	webflare[.]beer	Unknown malware
Domain	web-protection[.]beer	Unknown malware
Domain	web-safe[.]beer	Unknown malware
Domain	pohuimne[.]lol	Unknown malware
Domain	etomoidomen[.]cfd	Unknown malware · malware_download
Domain	dtc[.]victorramarisimobiliaria[.]com[.]br	
Domain	ns-claude-js[.]beer	Unknown malware

Type	Indicator	Context
Domain	vhyip[.]monster	Unknown malware
Domain	best-claudns-js[.]beer	Unknown malware
Domain	framesavecloudjs[.]beer	Unknown malware · malware_download
Domain	remoteshcontrol[.]com	ClearFake
Domain	mnepohui[.]sbs	Unknown Webinject
Domain	anakondabob[.]club	Unknown malware
Domain	bcncdncl-ns[.]beer	Unknown malware
Domain	kyjpwnw[.]monster	Lumar
Domain	grovalstandard[.]monster	
Domain	ssns-cdn-ns[.]beer	Unknown malware
Domain	adflow[.]monster	Unknown malware
Domain	exportearth[.]monster	Unknown malware
Domain	adtraffic[.]monster	Unknown malware
Domain	jogosdecarrobr[.]monster	Unknown malware
Domain	slndcdnclaud[.]beer	Unknown malware
Domain	adzeta[.]monster	Unknown malware

Type	Indicator	Context
Domain	travel-js-ns[.]beer	Unknown malware
Domain	biletors[.]cfd	Unknown malware
Domain	totalads[.]monster	Unknown malware
Domain	moonglide[.]monster	Unknown malware
Domain	lsikjsns[.]beer	Unknown Webinject
Domain	equinixad[.]monster	

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

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 actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious code at a later time, potentially leveraging the Windows Task Scheduler to blend in with legitimate system activity, which may allow them to bypass defenses that are focused on immediate execution. This technique in particular could be appealing to the actor because it enables them to schedule tasks to run under the context of a specific user or system account, which would likely facilitate their objective of maintaining access to the system. The defensive countermeasure would be to alert on new scheduled tasks (Event ID 4698), restrict schtasks/at to admins, and baseline legitimate task creators.

Also plausible (same tactic): T1543 Create or Modify System Process (n=18, lift 1.8), T1098 Account Manipulation (n=12, lift 2.0)

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