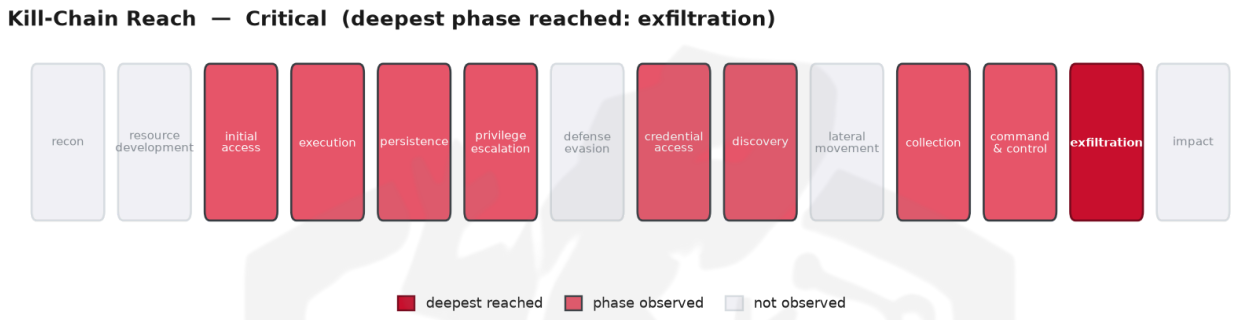
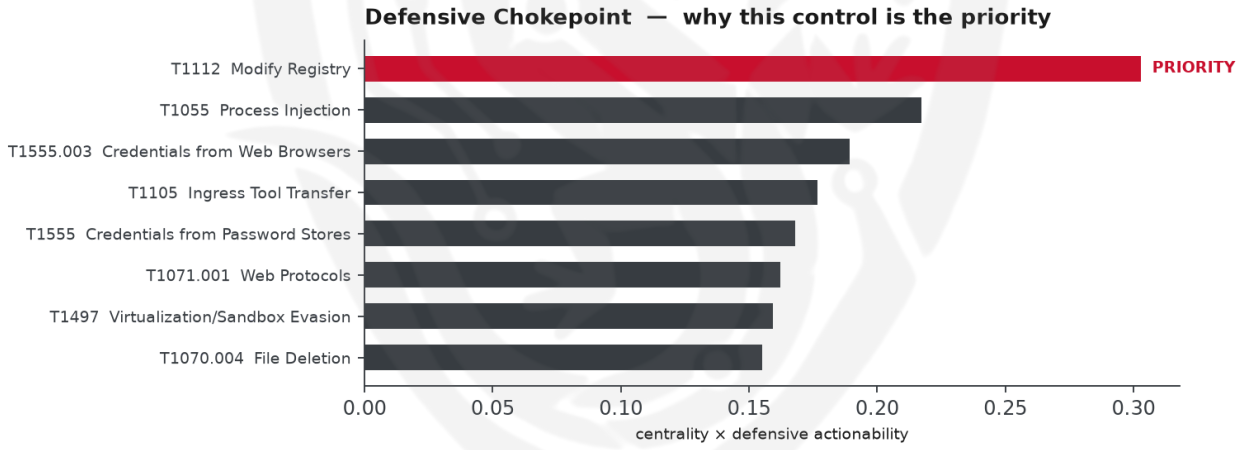
THREAT REPORT: UNKNOWN_ADVERSARY MALWARE CAMPAIGN

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 has been linked to the DeerStealer and Vidar malware families, although the targeted country and sectors remain unknown. The threat actor's use of various techniques, including spearphishing and process injection, poses a significant risk to affected systems. Priority should be given to monitoring sensitive registry keys for modification to prevent further damage. The operational risk band for this threat is Critical, as it reaches the stage of exfiltration.

Threat Overview

The threat actor, whose identity is unknown, has been observed using the DeerStealer and Vidar malware families to target unknown countries and sectors. The central vulnerability exploited by the threat actor is

also unknown. The actor's techniques include malicious links, spearphishing, and process injection, among others.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with initial access through malicious links or spearphishing, followed by the use of PowerShell and obfuscated files. The priority technique in this chain is T1112 Modify Registry, which is the graph chokepoint. To mitigate this threat, the priority control is to Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users.

Infrastructure and Corroboration

The malware families used by the threat actor have been corroborated by abuse.ch, which has identified IClickFix, Unknown malware, and Vidar as related families. However, no indicators have been flagged with high confidence 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)

- T1204.001 Malicious Link
- T1566.002 Spearphishing Link
- T1059.001 PowerShell
- T1027 Obfuscated Files or Information
- T1140 Deobfuscate/Decode Files or Information
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1055 Process Injection
- T1112 Modify Registry
- T1497 Virtualization/Sandbox Evasion
- T1070.004 File Deletion
- T1082 System Information Discovery
- T1555.003 Credentials from Web Browsers
- T1555 Credentials from Password Stores
- T1539 Steal Web Session Cookie
- T1005 Data from Local System
- T1041 Exfiltration Over C2 Channel
- T1027.002 Software Packing

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3187).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5262; 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
Evilnum	0.5262
TA505	0.4672
Molerats	0.4587
Patchwork	0.4466
Malteiro	0.4305

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: IClickFix, Unknown malware, Vidar.
- 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
Domain	www[.]fidestrento[.]com	
Domain	kiitec[.]ac[.]tz	
Domain	aqarco[.]com	
Domain	game-corp[.]net	
Domain	pickleballmastery[.]com	
Domain	itechhardware[.]com	

Type	Indicator	Context
Domain	shadesking[.]com	
Domain	mlm-dra[.]com	
Domain	dynastyroofingfl[.]com	
Domain	foodturerebels[.]com	Vidar
Domain	sanramontaxis[.]com	
Domain	mobilepricesbot[.]com	IClickFix
Domain	aikomart[.]com	
Domain	artillac[.]com	
Domain	royalkimons[.]com	
Domain	youthupglobal[.]com	
Domain	terabyte[.]computer	
Domain	rabbleallied[.]com	
Domain	davisonbooks[.]com	
Domain	ranklinko[.]com	
Domain	thistrending[.]com	
Domain	afroteaonline[.]com	
Domain	regardfengshui[.]com	
Domain	antimids[.]com	
Domain	ladywear[.]net	
Domain	waltonpalmeronline[.]com	Unknown malware
Domain	octawolf[.]com	
Domain	plan1pmc[.]com	
Domain	rak-lok[.]com	
Domain	matiasbayma[.]net	
Domain	packersmoversudaipur[.]com	

Type	Indicator	Context
Domain	gazaltours[.]com	
Domain	creativehomeprojects[.]com	
Domain	dickfordays[.]com	
Domain	goodearthsixty9[.]com	
Domain	alligatorcreations[.]com	
Domain	paginas-web-baratas[.]com	
Domain	earthscapenj[.]com	
Domain	neatroots[.]com	
Domain	auggieeats[.]com	

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:** T1112 Modify Registry (persistence)
- **Observed here:** T1112 Modify Registry 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:** 19 of 170 documented groups that use Modify Registry also use Scheduled Task/Job (conditional 0.66, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

The actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious tasks at a later time, potentially evading detection by scheduling tasks to run under legitimate system processes. This technique may allow the actor to regain a foothold in the system, as scheduled tasks can be used to execute malicious code or scripts. To counter this, the defensive control would involve alerting on new scheduled tasks (Event ID 4698); restricting schtasks/at to admins; and baselining legitimate task creators.

Also plausible (same tactic): T1078 Valid Accounts (n=18, lift 1.6), T1547 Boot or Logon Autostart Execution (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