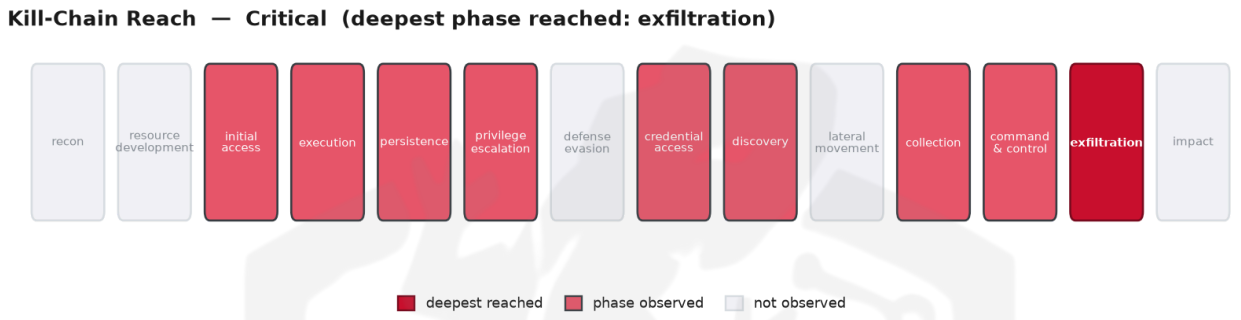
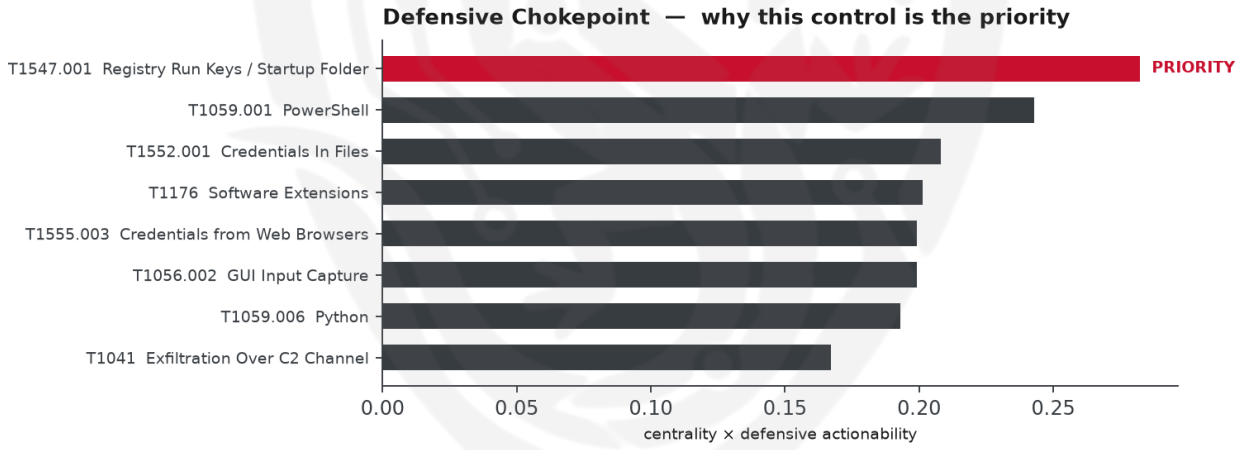
THREAT REPORT: UNK_DEADDROP PHISHING CAMPAIGN

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 UNK_DeadDrop, a threat actor targeting developers in the United States of America, particularly in the Finance, Technology, and Education sectors, to steal cryptocurrency. The campaign involves phishing and the use of various malware families, including Overlord, OtterCookie, Invisible Ferret, and FlexibleFerret. 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 multiple techniques to steal web session cookies, credentials, and other sensitive information poses a significant risk to the targeted organizations.

Threat Overview

The threat actor, UNK_DeadDrop, is using a range of malware families, including Overlord, OtterCookie, Invisible Ferret, and FlexibleFerret, to target developers. The central vulnerability exploited is not specified due to insufficient data. The victimology indicates that the threat actor is targeting organizations in the United States of America, specifically in the Finance, Technology, and Education sectors.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including stealing web session cookies, spearphishing, system information discovery, and data exfiltration over a command and control channel. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which is the graph chokepoint. 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."

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this campaign. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators 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)

- T1539 Steal Web Session Cookie
- T1071.004 DNS
- T1566.002 Spearphishing Link
- T1082 System Information Discovery
- T1176 Software Extensions
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1555.003 Credentials from Web Browsers
- T1552.001 Credentials In Files
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1056.002 GUI Input Capture
- T1027 Obfuscated Files or Information
- T1059.006 Python
- T1555.004 Windows Credential Manager
- T1070.004 File Deletion
- T1071.001 Web Protocols

- T1059.005 Visual Basic
- T1204.001 Malicious Link

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2973).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5514; 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
RedCurl	0.5514
Molerats	0.4828
APT39	0.4596
Windshift	0.4549
Inception	0.4459

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	alphanonega[.]org
Domain	asteara[.]org
Domain	careerpredictto[.]space
Domain	careerpulsynk[.]xyz

Type	Indicator
Domain	careertrixauvex[.]ink
Domain	ceronet[.]work
Domain	ceronetwork[.]org
Domain	connectptogether[.]ink
Domain	contactpredicttogether[.]ink
Domain	contactpulsynk[.]ink
Domain	contacttrixauvex[.]ink
Domain	coslyintra[.]online
Domain	cotrixauvex[.]ink
Domain	culyrax[.]us
Domain	deep-ai-guard[.]store
Domain	domatisc[.]ink
Domain	doxxela[.]ink
Domain	elsavora[.]us
Domain	empowerpharmacy[.]space
Domain	hyperdevpipline[.]org
Domain	mailpredicttogether[.]ink
Domain	mailpulsynk[.]xyz
Domain	mailtrixauvex[.]ink
Domain	migadyn[.]info
Domain	nemesis[.]work
Domain	nemesistrade[.]work
Domain	notifypulsynk[.]ink
Domain	nowurisch[.]fit
Domain	nxlog[.]tech

Type	Indicator
Domain	ondofinance[.]tech
Domain	onoplainai[.]ink
Domain	onoplanoai[.]ink
Domain	optixauvex[.]us
Domain	predictcareertogether[.]space
Domain	predicttocareer[.]space
Domain	predicttogerecruit[.]store
Domain	predicttogether[.]ink
Domain	predicttogetherrecruit[.]store
Domain	pulsnyk[.]org
Domain	pulsynk[.]org