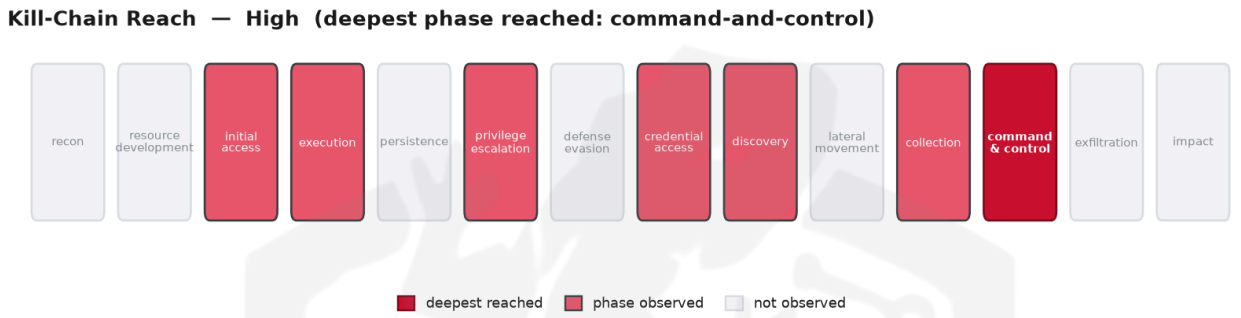
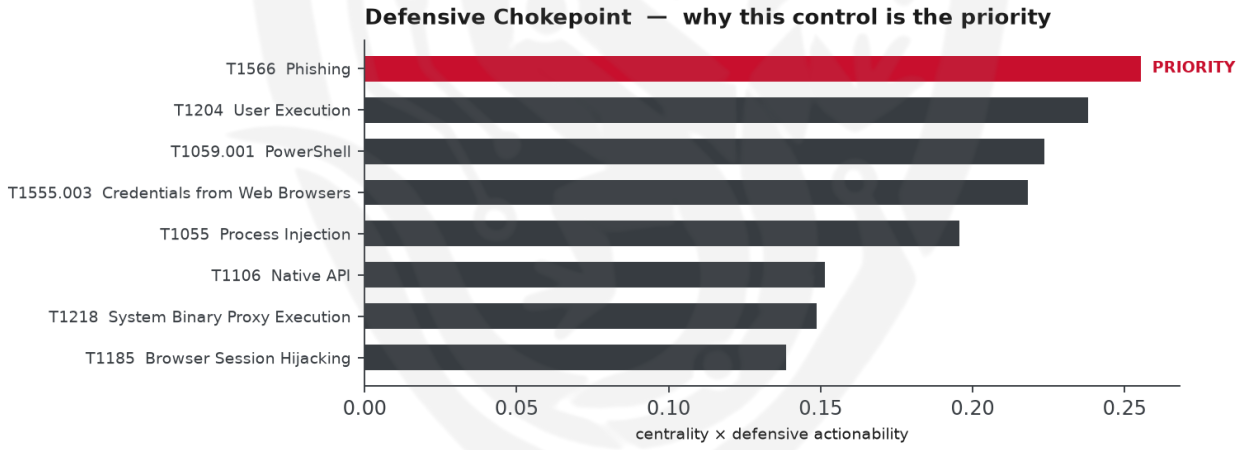
THREAT REPORT: CASTLELOADER AND NEEDLESTEALER CONNECTION CAMPAIGN

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 involves the use of various malware families, including CastleLoader, CastleStealer, and NeedleStealer, to target unknown sectors and countries. The threat actor's goals and motivations are not well understood due to insufficient data. Priority should be given to defending against social-engineering delivery methods, as the threat actor's techniques include phishing and other tactics to gain initial access. The campaign's use of multiple malware families and techniques suggests a high level of sophistication and adaptability.

Threat Overview

The threat actor, whose identity is not known, utilizes a range of malware families, including CastleLoader, CastleStealer, PythonRAT, NetSupport RAT, NeedleStealer, Lobshot, and BoryptGrab. The actor's targets

and the central vulnerability exploited are not specified due to insufficient data. The threat actor's techniques include stealing web session cookies, code signing, system information discovery, and process injection, among others.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving initial access, execution, and persistence. The priority technique is T1566 Phishing, which serves as a key entry point for the threat actor. To mitigate this threat, the priority control is to "Harden against social-engineering delivery across email, links and voice/callback lures: attachment sandboxing and link rewriting, block macro-enabled Office docs from the internet zone, train users to verify unexpected requests out-of-band, deploy a report-phish button, and enforce phishing-resistant MFA."

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted on providers such as Dedik Services Limited, Telefonica Brasil S.A, and Latitude.sh, as observed by third-party sources. Additionally, abuse.ch has corroborated the presence of malware families such as ClearFake and DarkVNC, although the confidence level of AbuseIPDB flags is below the threshold, with no indicators reaching an 80% confidence level.

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
- T1553.002 Code Signing
- T1082 System Information Discovery
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1055 Process Injection
- T1218 System Binary Proxy Execution
- T1185 Browser Session Hijacking
- T1555.003 Credentials from Web Browsers
- T1083 File and Directory Discovery
- T1204 User Execution
- T1059.001 PowerShell
- T1566 Phishing
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1070.004 File Deletion

- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2553).
- 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 0.4899; 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	0.4899
TA505	0.4573
Inception	0.4551
Tropic Trooper	0.4364
Silence	0.4358

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: ClearFake, DarkVNC, 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	94[.]26[.]90[.]112	AbuseIPDB 0% (DE) · AS207043 Dedik Services Limited
IP	179[.]132[.]128[.]189	AbuseIPDB 0% (BR) · AS26599 Telefonica Brasil S.A

Type	Indicator	Context
IP	216[.]107[.]139[.]188	AbuseIPDB 0% (US) · AS396356 Latitude.sh
IP	91[.]92[.]33[.]167	AbuseIPDB 0% (DE) · AS207043 Dedik Services Limited
Domain	teamsvoicepremium[.]com	
Domain	italianhitech[.]com	
Domain	ebedidance[.]com	
Domain	drrajivparti[.]com	
Domain	p-rala[.]com	
Domain	avivtech[.]org	Unknown malware
Domain	claudettes[.]net	Unknown malware
Domain	skipraid[.]com	Unknown malware
Domain	claudenell[.]net	ClearFake
Domain	eazysitebuilder[.]com	
Domain	fangorinaf[.]com	
Domain	garrigin[.]com	
Domain	goodbytetelegramm[.]com	
Domain	grenagana[.]com	

Type	Indicator	Context
Domain	grorriner[.]com	
Domain	hobtech[.]net	
Domain	kaneta[.]cc	
Domain	monblare[.]com	
Domain	noidret[.]com	
Domain	quiantar[.]com	
Domain	qxvnrta[.]com	
Domain	socom-game[.]com	
Domain	strainted[.]com	
Domain	thenugcompany[.]org	
Domain	urutyka[.]com	
URL	hxxp://94[.]26[.]90[.]112/dl-callback/6dkcdpd7-4jacbuf9-prutgux4-2ybssc8v/traffic1[.]exe/1390903f57b21f346193aefbbfd36759	
URL	hxxp://eazysitebuilder[.]com:4889	
URL	hxxp://goodbytetelegramm[.]com/xxx/main	
URL	hxxp://socom-game[.]com:5500	
URL	hxxp://urutyka[.]com/xxx/viewer32	
Hash	d26ea6828cc01ae151d99bbee78c4e6d132e9077842a558bce3901fa0970d9be	
Hash	2fcf553b9656523b3207c08cdf16f7be9a25e55cf8c29f5caf933151c9214367	DarkVNC

Type	Indicator	Context
Hash	1390903f57b21f346193aefbbfd36759	
Hash	4d5f81bf79554aa7a2187e6ffbc9702a	
Hash	6728b11f74fd435f926ed25c5f2952bb	
Hash	0c48fd6a18ad9c701b254bbdd412efbf7dfdd2be6534a61c14bce719d259df9f	

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:** T1566 Phishing (initial-access)
- **Observed here:** T1566 Phishing was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 38+ groups that use Phishing, this pairing runs 1.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1203 Exploitation for Client Execution to maintain their objective, as this technique may allow them to execute malicious code on the client-side by exploiting vulnerabilities in commonly used software, potentially bypassing the phishing block by directly targeting the client application. This technique in particular could be appealing as it would likely enable the actor to leverage existing vulnerabilities in software that the target may have, potentially leading to a successful execution of malicious code. To counter this, the mandated defensive control of patching client applications, enabling exploit mitigations such as ASLR, DEP, and CFG, and implementing application isolation should be applied.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=43, lift 1.3), T1559 Inter-Process Communication (n=13, lift 1.6)

Detection and hardening for the pivot (T1203 Exploitation for Client Execution)

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs

    - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
    - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
    - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
    - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log