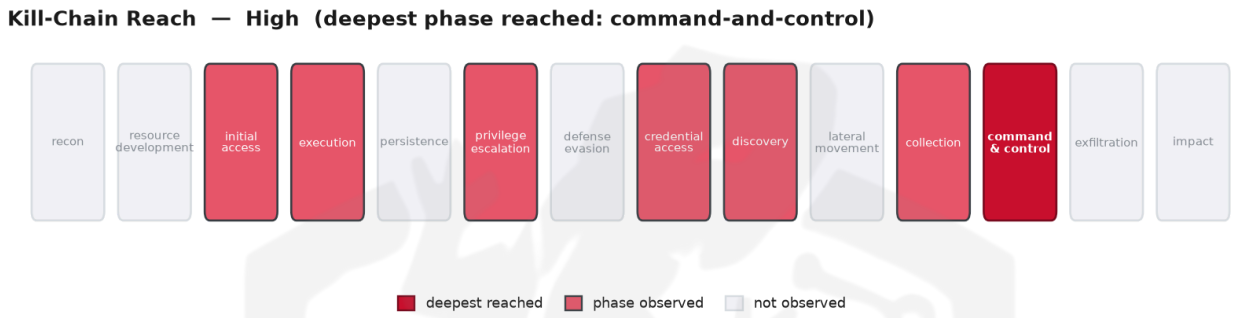
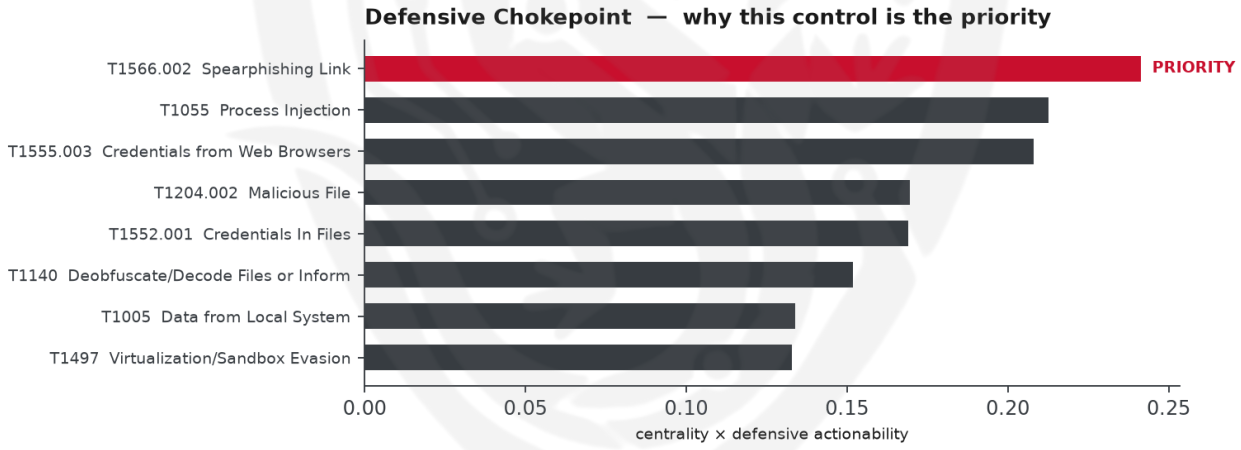
THREAT REPORT: UNKNOWN_ADVERSARY MALWARE DISTRIBUTION ECOSYSTEM

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 distributing malware, including SessionGate, RemusStealer, and AnimateClipper, targeting countries such as Brazil, France, Germany, Poland, Russia, and the UK. The threat actor's tactics involve various techniques to steal sensitive information. Priority should be given to defensive actions that mitigate the impact of spearphishing links. Enablement of security measures such as attachment sandboxing and link rewriting is crucial to counter this threat.

Threat Overview

The threat actor, whose identity is insufficient to determine, is utilizing a range of malware families including SessionGate, RemusStealer, and AnimateClipper. The targeted countries include Brazil, France, Germany, Poland, Russia, and the UK, although specific sectors targeted are not well-defined. The

malware distribution ecosystem involves exploiting various vulnerabilities and using multiple techniques to achieve its goals.

Attack Chain and Priority Control

The attack chain involves a series of techniques including screen capture, keylogging, stealing web session cookies, and process injection, among others. The priority technique identified is T1566.002 Spearphishing Link, which serves as a critical chokepoint in the attack chain. To counter this, the priority control is to "Enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button."

Infrastructure and Corroboration

Although specific hosting providers or ASNs are not identified, third-party sources such as abuse.ch corroborate the presence of malware families including ACR Stealer, Remus, RemusStealer, and Unknown malware. However, according to AbuseIPDB, there are no indicators with a confidence level 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)

- T1113 Screen Capture
- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1115 Clipboard Data
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1555.003 Credentials from Web Browsers
- T1083 File and Directory Discovery
- T1497 Virtualization/Sandbox Evasion
- T1552.001 Credentials In Files
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1132 Data Encoding
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1566.002 Spearphishing Link (centrality 0.2413).
- 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 0.4869; 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
Ajax Security Team	0.4869
Darkhotel	0.4621
RedCurl	0.4472
OilRig	0.4361
APT42	0.4211

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: ACR Stealer, Remus, RemusStealer, 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
Domain	guiformat[.]com	
Domain	forestoaker[.]com	
Domain	arch2[.]maxdatahost1[.]cyou	
Domain	buccstanor[.]pics	

Type	Indicator	Context
Domain	gluckcreek[.]online	Remus
Domain	intem[.]lat	Remus
Domain	ropea[.]top	Remus
Domain	ilspy[.]org	
Domain	cdn-1415[.]brightcanvas[.]digital	ACR Stealer
Domain	flame-guard[.]cc	Unknown malware
Domain	appfreshstart[.]com	
Domain	appgetonline[.]com	
Domain	appmakingcenter[.]com	
Domain	carlessclapped[.]com	
Domain	crystaldiskmark[.]org	
Domain	dnspy[.]org	
Domain	ghidralite[.]com	
Domain	grpcurl[.]com	
Domain	integritycrc[.]com	
Domain	javascriptapiusa[.]com	
Domain	mfcmapi[.]com	
Domain	mobileversioncrc[.]com	
Domain	mqttexplorer[.]com	
Domain	originaldownloads[.]info	
Domain	ukentaspectsofc[.]org	
Domain	unlockcontent[.]org	
Domain	webcrcprove[.]com	
Domain	webinnosetup[.]com	
Domain	winsetupfromusb[.]org	

Type	Indicator	Context
Domain	yourfastcrc[.]com	
URL	hxxp://194[.]150[.]220[.]218/4SLEYpfAk57hGubo/fo0suc2ki2[.]rtf	malware_download
URL	hxxp://baxe[.]pics:48261	
URL	hxxp://buccstanor[.]pics:28313	
URL	hxxp://buccstanor[.]pics:48261	
URL	hxxp://forestoaker[.]com:6290	
URL	hxxp://gluckcreek[.]online:48261	
URL	hxxp://intem[.]lat:9592	
URL	hxxp://ropea[.]top:28313	
URL	hxxp://oundhertobeconsist[.]org/	
URL	hxxps://cdn-1415[.]brightcanvas[.]digital/fo0suc2ki2[.]rtf	

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:** T1566.002 Spearphishing Link (initial-access)
- **Observed here:** T1566.002 Spearphishing Link was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1189 Drive-by Compromise (initial-access)
- **Basis:** 27 of 170 documented groups that use Spearphishing Link also use Drive-by Compromise (conditional 0.28, lift 1.5, i.e. ~1.5x base rate). Strongest same-tactic neighbour.

The actor could pivot to T1189 Drive-by Compromise by exploiting vulnerabilities in software or plugins to compromise a user's system, potentially achieving their objective if the user visits a malicious website. This technique may be used in conjunction with previous attempts, as the actor could compromise a website and have it serve malicious content to unsuspecting users. The defensive control to mitigate this would be to enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.

Also plausible (same tactic): T1195 Supply Chain Compromise (n=9, lift 1.4), T1199 Trusted Relationship (n=9, lift 1.3)

- **Defensive countermeasure:** Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.