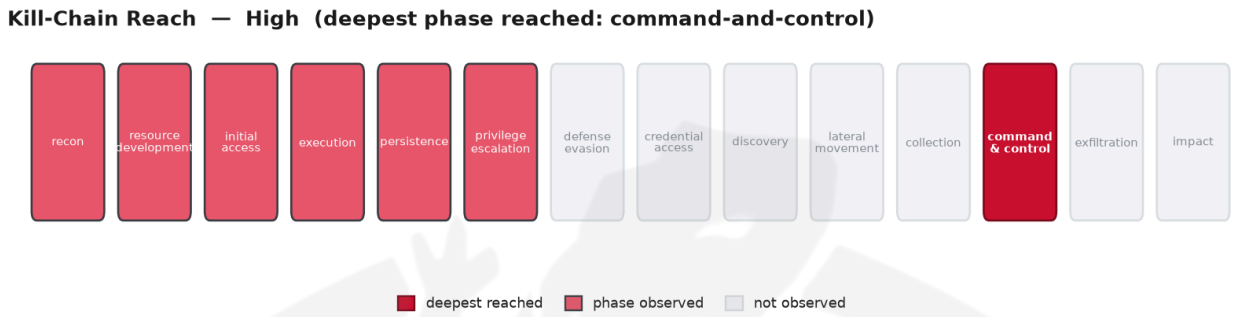
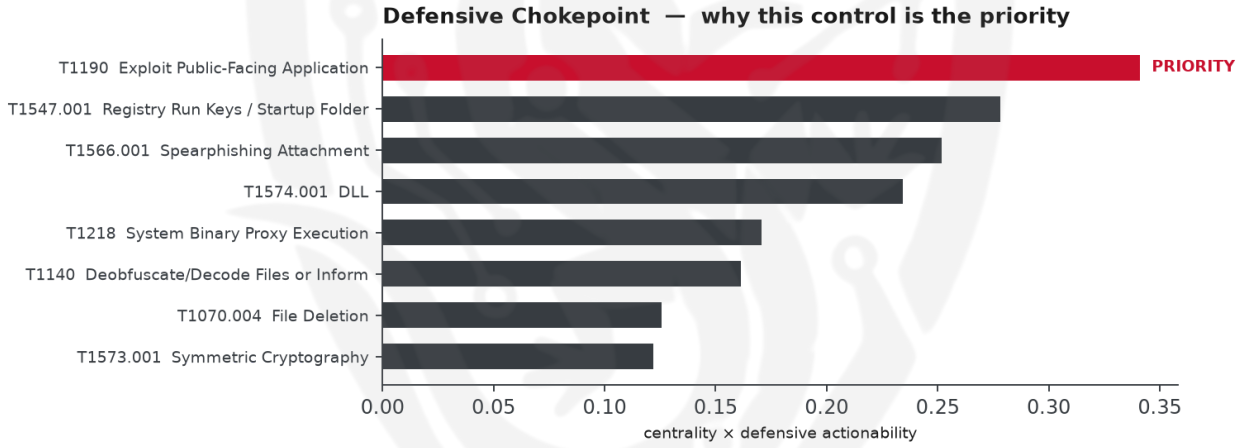
THREAT REPORT: JADEPROX

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 JadeProx, a threat actor that has been observed exploiting the CVE-2021-31755 vulnerability to target organizations in the healthcare, government, and education sectors. The actor utilizes a range of malware families, including TriBack Loader and PlugX, to gain access to systems. Priority should be given to patching the exploited vulnerability to prevent further attacks. The threat actor's tactics, techniques, and procedures (TTPs) indicate a high level of operational risk, reaching command-and-control levels.

Threat Overview

JadeProx, the observed threat actor, employs various malware families, including TriBack Loader, AdaptixC2, and PlugX, to exploit the central vulnerability CVE-2021-31755. The actor targets organizations in the healthcare, government, and education sectors, although the targeted country is not specified. The exploited vulnerability and malware families used suggest a sophisticated attack chain.

Attack Chain and Priority Control

The attack chain involves various techniques, including exploiting public-facing applications, using malicious files, and symmetric cryptography. The priority technique is T1190 Exploit Public-Facing Application, which is the graph chokepoint. To mitigate this threat, the priority action is to: Patch CVE-2021-31755 on all affected systems as the top priority, then: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Infrastructure and Corroboration

Although the hosting providers and ASNs observed are not available, abuse.ch has corroborated the presence of malware families such as Fscan and PlugX. However, AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. These corroboration efforts provide additional context to the threat actor's TTPs.

Technical Appendix

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

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

- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1566.001 Spearphishing Attachment
- T1574.001 DLL
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1583.001 Domains
- T1218 System Binary Proxy Execution
- T1595.002 Vulnerability Scanning
- T1547.001 Registry Run Keys / Startup Folder
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1059.005 Visual Basic
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.3412).
- 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 0.541; 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
Higaisa	0.541
BRONZE BUTLER	0.4801
WIRTE	0.4751
Ferocious Kitten	0.4642
Inception	0.4621

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Fscan, PlugX.
- 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	192[.]252[.]186[.]62	
Domain	sylverixstrategy[.]com	
Domain	claude-pro[.]com	PlugX
Domain	gouvvbo[.]top	PlugX
Domain	update-crowdstrike[.]com	
Domain	update-sentinelone[.]com	
Domain	update-trellix[.]com	PlugX
Domain	license[.]claude-pro[.]com	PlugX

Type	Indicator	Context
Domain	vertextrust-advisors[.]com	
Domain	photo[.]pokok[.]edu[.]hk	
Domain	pta[.]sfaeps[.]edu[.]hk	
Hash	b8053bcd04ce9d7d19c7f36830a9f26b	Fscan
Hash	3ba9a74f8faeff3de03e4c834f266582e2eb46a8	Fscan
Hash	e82ecbe3823046a27d8c39cc0a4acb498f415549946c9ff0e241838b34ed5a21	Fscan
Hash	35feef0e6806c14f4ccdb4fceff8a5757956c50fb5ec9644dedae665304f9f96	
Hash	d5590802bf0926ac30d8e31c0911439c35aead82bf17771cfd1f9a785a7bf143	
Hash	88ac1c5fc9ee89491c70ea16131e264a	
Hash	910465739b3170584150e9260bfba6a65e633f35	
Hash	c64eda499e2a21ad158841b9dbc7adc9	
Hash	3de213252d98348a7d833c4956a099bfcd36b9e2	
Hash	0482d6053f96e6bde0a92af25497f3c0	
Hash	0e6d22c2a81d29b1f9d8395d44e19e53	
Hash	35cdbf8a16da1245d574a0365cb87287	
Hash	38e317af0fc0efcc88265f243a264542	
Hash	39d4012e49f58092ec5cefed13dbbcfd	
Hash	3b3dd8f3a5e1ff85c63f2453ad270415	
Hash	3fe9c84025f4401f8cd661675642c526	
Hash	4faf4fd91d28e014b4f2362d6a7bb8ac	
Hash	5222a31cf24f9f57ae3d1831f264a983	
Hash	5b75b00a4b4c32b6e213514e80500a65	
Hash	7840f30b395fac347f85b38633c2d08d	
Hash	796f82a4833be330b1e35af63e55b597	
Hash	7c84e75817349adcdea9925b86f67670	

Type	Indicator	Context
Hash	8002ab4d0cf7e1888ee72de0b9f4282c	
Hash	853f760f76de3201b0af0e41f1f65fba	
Hash	9e01bf0e28c86435cfb1afaef44238e9	
Hash	a4cdecc57a215243d279cdb065863308	
Hash	aedd185b76ccda8d65dbd26204cc0e9a	
Hash	bb5c88de9e04e6306260b9f3a4498933	
Hash	bef0b8599d18acf1c74192ae9f198f85	

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:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** JadeProx used T1566.001 Spearphishing Attachment here as an alternative initial-access technique.
- **Projected pivot:** T1566.001 Spearphishing Attachment (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

JadeProx could pivot to T1566.001 Spearphishing Attachment to maintain their campaign momentum by sending targeted emails with malicious attachments, which may bypass initial defenses if not properly inspected. This technique would likely be used to trick users into opening attachments that could lead to further compromise, potentially exploiting trust in familiar communication channels. To counter this, the mandated defensive control of sandboxing and detonating email attachments, blocking executable/script archive contents at the gateway, stripping mark-of-the-web bypass, and implementing a user report-phish button should be applied.

Detection and hardening for the pivot (T1566.001 Phishing)

- **Telemetry:** Email security gateway logs; Endpoint (Office child processes); Proxy/DNS
- **Detect:**
  - Office apps (winword/excel) spawning script or LOLBIN child processes
  - Mark-of-the-Web bypass; ISO/IMG/LNK/HTML-smuggling attachments detonating
  - First-contact domains and newly registered domains in mail links
- **Harden:**
  - Attachment sandboxing; block high-risk types (iso, img, lnk, htm) at the gateway

    - Attack-surface-reduction rules for Office child processes; user reporting button
- **MITRE:** M1049 Antivirus/Antimalware, M1031 Network Intrusion Prevention, M1017 User Training, M1021 Restrict Web-Based Content · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic