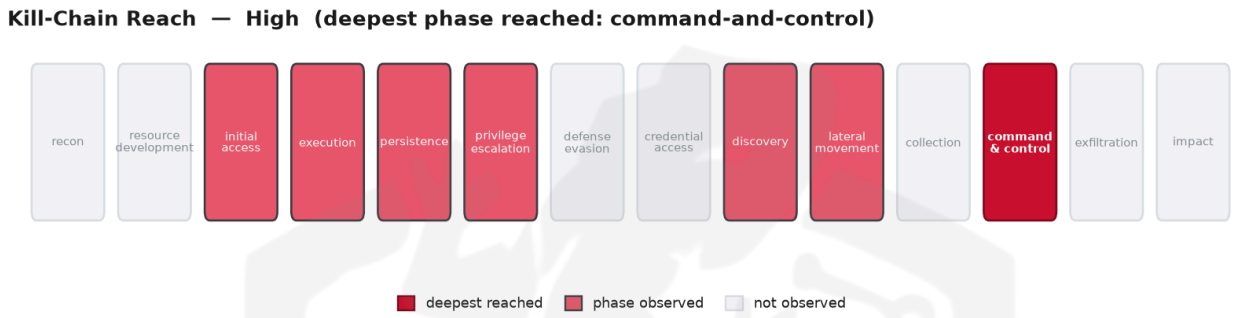
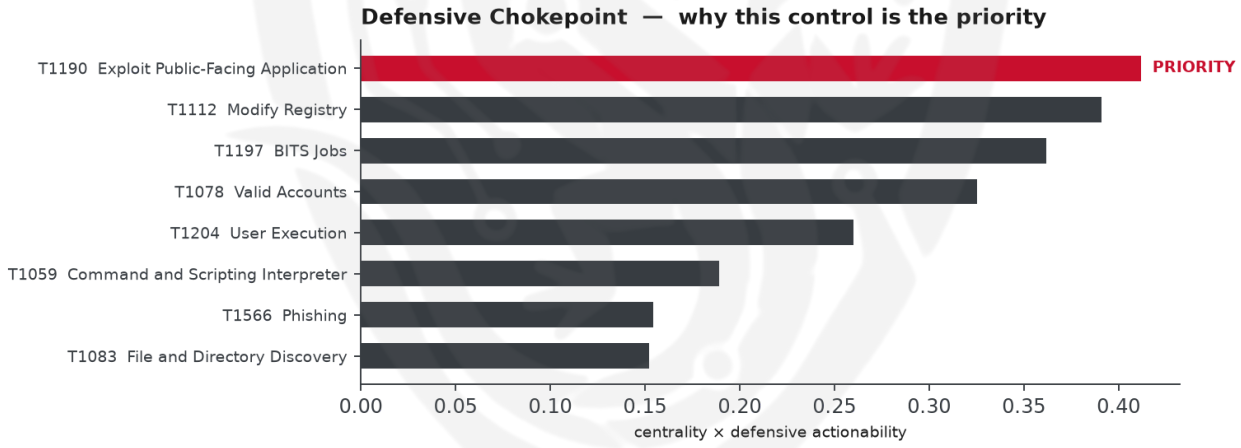
THREAT REPORT: CLICKFIX DENO ABUSE TO CASTLERAT CAMPAIGN

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 exploitation of public-facing applications, targeting unknown sectors and countries. The threat actor's techniques and malware families are not sufficiently identified. Priority should be given to patching the affected public-facing vulnerabilities and restricting management interfaces to mitigate the risk. The operational risk band is considered high due to the potential for command-and-control.

Threat Overview

The threat actor, whose identity is not determined, is associated with a campaign involving ClickFix Deno Abuse to CastleRAT. The central vulnerability and specific malware families used are not identified. The

actor's techniques, as inferred from the report, include exploiting public-facing applications and potentially using remote services, command and scripting interpreters, and other methods to gain access and control.

Attack Chain and Priority Control

The observed techniques form a chain that starts with initial access and moves through various stages, including remote services, command and scripting interpreters, and file and directory discovery. The priority technique identified is T1190 Exploit Public-Facing Application, which serves as a critical chokepoint. To mitigate this, the priority control is to "Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only."

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs used by the threat actor. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence of 80% or higher.

Technical Appendix

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

Observed Techniques (ATT&CK, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1021 Remote Services - T1059 Command and Scripting Interpreter - T1078 Valid Accounts - T1083 File and Directory Discovery - T1112 Modify Registry - T1190 Exploit Public-Facing Application - T1197 BITS Jobs - T1204 User Execution - T1219 Remote Access Tools - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.4118).
- Operational risk: High (score 0.594, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3651; 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
GOLD SOUTHFIELD	0.3651
Threat Group-1314	0.3586
TA459	0.3354
INC Ransom	0.3254
APT30	0.3162

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	lkczkqweca[.]com
Domain	smokeenew[.]com
Domain	ibewfszvehhb[.]lkczkqweca[.]com
Domain	webstizkgao[.]com
Domain	nicenicc[.]com
URL	hxxp://webstizkgao[.]com/v02c4fd90de22ee0677[.]js
URL	hxxp://webstizkgao[.]com/v2c4fd90de22ee0677[.]js
URL	hxxp://162[.]33[.]177[.]16/CFBatFIX/install[.]pyc
URL	hxxp://162[.]33[.]177[.]16/CFBatFIX/7sjVtn0zPVjMZzkxZ[.]MOa
Hash	f1ecb89facb7e31ee9c03278f4106113c0339ff9fc10b1aefe33aaab776e8540
Hash	f704a49c0cdaaae4515105bf937e26b5e39b1101c8a0cefaca3959fce7418e9d
Hash	82056127b671583deb500d931ecb893224c34d3b8de66c0959700d55a1bfbbfd
Hash	c9afa1e8ce84b3af50304b504519a587488658142137cf4bbf85f5780c06f682
Hash	b04bc0780b2cd11fde488372387f557a87fd473ba546295f5fca7771d5b8a394

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:** T1190 Exploit Public-Facing Application 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:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 22+ groups that use Exploit Public-Facing Application, this pairing runs 2.0x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain their objective by leveraging WMI's capabilities to execute commands and access sensitive information on the compromised system, potentially using WMI to query system details or execute malicious code. This technique may be particularly appealing to the actor as it allows for stealthy and targeted interactions with the system, potentially evading detection. To counter this, the mandated defensive control of monitoring wmiprvse.exe child-process creation, restricting remote WMI (DCOM) at the host firewall, and enabling WMI-Activity operational logging should be implemented.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=23, lift 1.5), T1569 System Services (n=8, lift 1.8)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command