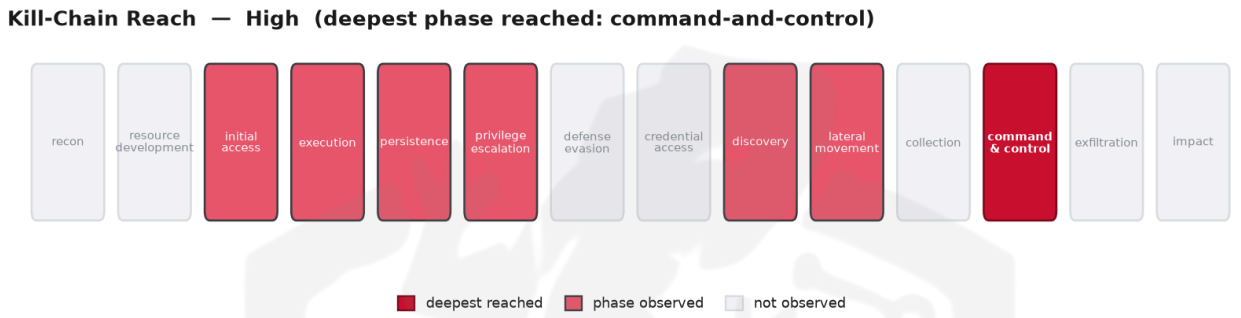
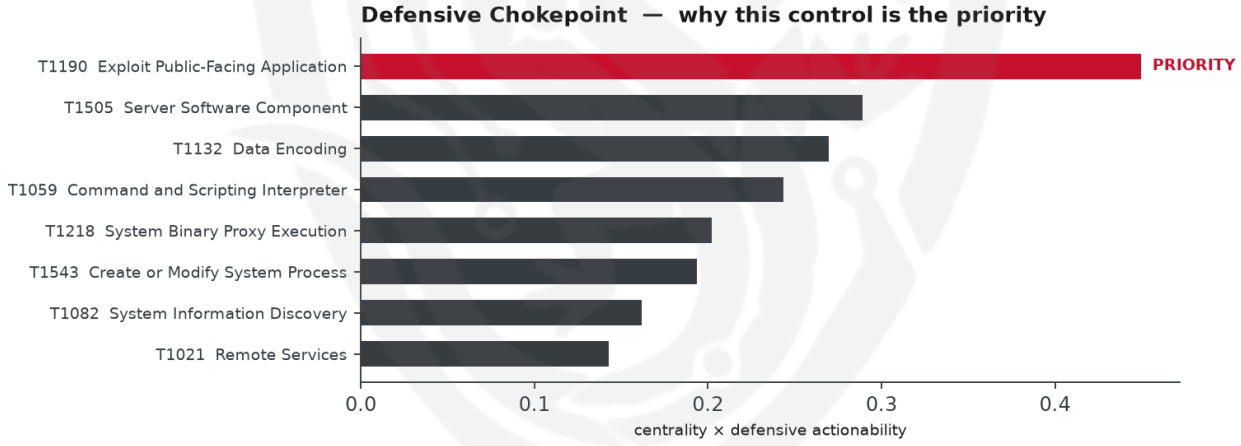
THREAT REPORT: BADIIS AND XMRIG MALWARE CAMPAIGN TARGETS TECHNOLOGY SECTOR

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 deployment of BadIIS, XMRig, and CnCrypt Protect malware families, targeting the technology sector. The threat actor's identity and targeted country remain unknown. Priority should be given to patching public-facing vulnerabilities and applying a web application firewall (WAF) virtual patch to mitigate the threat. The operational risk band is considered high due to the potential for command-and-control capabilities.

Threat Overview

The threat actor, whose identity is unknown, is associated with the BadIIS, XMRig, and CnCrypt Protect malware families. The central vulnerability exploited is unknown, but the techniques inferred from the

report include remote services, command and scripting interpreter, and system information discovery, among others. The technology sector is the primary target of this campaign.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including remote services, command and scripting interpreter, and system information discovery, ultimately leading to the exploitation of public-facing applications. The priority technique is T1190 Exploit Public-Facing Application, which serves as a chokepoint in the attack chain. To mitigate this threat, 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 available information on the hosting providers or ASNs observed, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with a confidence level of 80% or higher by AbuseIPDB, 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, 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 - T1082 System Information Discovery - T1132 Data Encoding - T1190 Exploit Public-Facing Application - T1218 System Binary Proxy Execution - T1505 Server Software Component - T1543 Create or Modify System Process

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.4495).
- Operational risk: High (score 0.552, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3586; 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
Blue Mockingbird	0.3586
Deep Panda	0.343
Agrius	0.3227
Moses Staff	0.3162
APT19	0.3125

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	334thribetlhkyo977gqrcht1k7bvdj2[.]oastify[.]com
Hash	c4c8e8c336c3429d97195076bf3bb6eb

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 native capabilities to execute commands and access sensitive information, potentially exploiting the lack of monitoring and control over WMI activity. This technique may be particularly appealing as it allows the actor to interact with the system in a way that blends in with legitimate administrative activity, making it harder to detect. To counter this potential pivot, 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