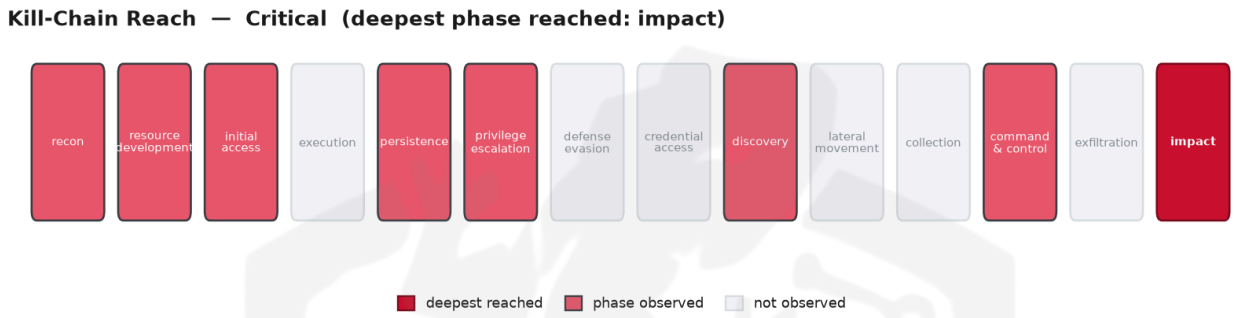
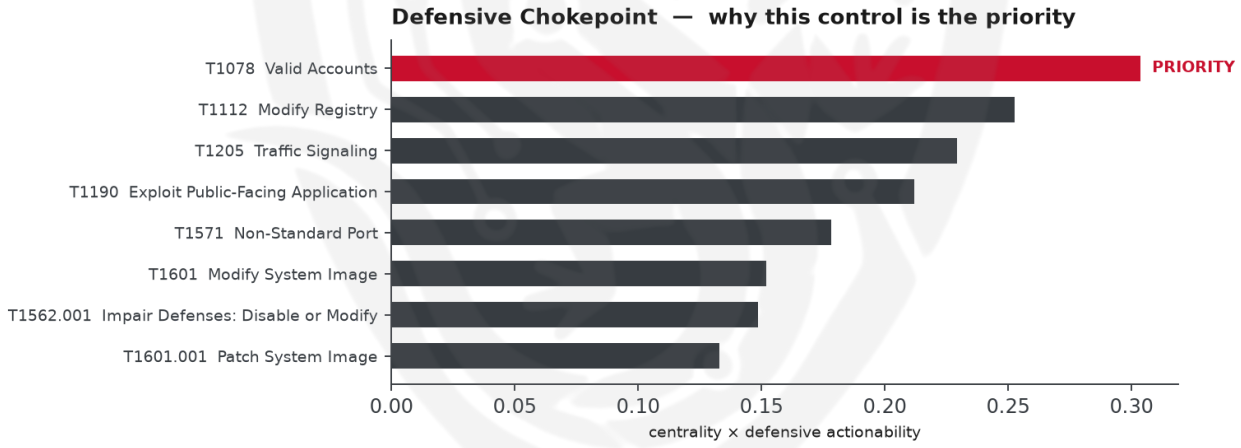
THREAT REPORT: CYBER AV3NGERS TARGET U.S. CRITICAL INFRASTRUCTURE

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 Cyber Av3ngers, who are exploiting vulnerabilities against critical infrastructure in the United States, specifically targeting government and energy sectors. The threat actor is utilizing various malware families, including IOCONTROL and MALPDB. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The ongoing exploitation poses a significant risk to national security and public safety.

Threat Overview

Cyber Av3ngers are employing a range of techniques, including network denial of service, external remote services, and stored data manipulation, to compromise U.S. critical infrastructure. The malware families

IOCONTROL and MALPDB are being used to carry out these attacks. The threat actor is targeting government and energy sectors, with the goal of disrupting critical operations.

Attack Chain and Priority Control

The observed techniques used by Cyber Av3ngers form a complex attack chain, with the priority technique being T1078 Valid Accounts, which serves as a chokepoint in the graph. To counter this, the lead control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

The malicious infrastructure is hosted on various providers, including Ultahost Inc., WorldStream B.V., BelCloud Ltd, and MivoCloud SRL. Although no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, the hosting providers and network infrastructure used by the threat actor provide valuable context for understanding the scope of the attack.

Technical Appendix

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

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

- T1498.001 Direct Network Flood
- T1133 External Remote Services
- T1565.001 Stored Data Manipulation
- T1584.003 Virtual Private Server
- T1190 Exploit Public-Facing Application
- T1205 Traffic Signaling
- T1112 Modify Registry
- T1583.003 Virtual Private Server
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1601 Modify System Image
- T1078 Valid Accounts
- T1571 Non-Standard Port
- T1589.001 Credentials
- T1601.001 Patch System Image
- T1070.004 File Deletion
- T1498 Network Denial of Service
- T1595.001 Scanning IP Blocks
- T1046 Network Service Discovery
- T1601.002 Downgrade System Image
- T1078.003 Local Accounts

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.3361).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3353; 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
Ember Bear	0.3353
Magic Hound	0.2508
Sea Turtle	0.2415
Dragonfly	0.241
Axiom	0.2326

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	Context
IP	79[.]133[.]46[.]209	AbuseIPDB 0% (DE) · AS214036 Ultahost Inc.
IP	185[.]82[.]73[.]162	AbuseIPDB 0% (NL) · AS214036 Ultahost Inc.
IP	185[.]82[.]73[.]164	AbuseIPDB 0% (NL) · AS214036 Ultahost Inc.
IP	185[.]82[.]73[.]171	AbuseIPDB 0% (NL) · AS214036 Ultahost Inc.
IP	135[.]136[.]1[.]133	AbuseIPDB 0% (RO) · AS9009 M247 Europe SRL
IP	185[.]82[.]73[.]165	AbuseIPDB 0% (NL) · AS214036 Ultahost Inc.

Type	Indicator	Context
IP	185[.]82[.]73[.]167	AbuseIPDB 0% (NL) · AS214036 Ultahost Inc.
IP	185[.]82[.]73[.]168	AbuseIPDB 0% (NL) · AS214036 Ultahost Inc.
IP	185[.]82[.]73[.]170	AbuseIPDB 0% (NL) · AS214036 Ultahost Inc.
IP	175[.]110[.]121[.]107	AbuseIPDB 0% (NL) · AS49981 WorldStream B.V.
IP	175[.]110[.]121[.]39	AbuseIPDB 0% (NL) · AS49981 WorldStream B.V.
IP	175[.]110[.]121[.]42	AbuseIPDB 0% (NL) · AS49981 WorldStream B.V.
IP	185[.]82[.]73[.]175	AbuseIPDB 0% (NL) · AS214036 Ultahost Inc.
IP	185[.]225[.]17[.]225	AbuseIPDB 0% (RO) · AS39798 MivoCloud SRL
IP	185[.]225[.]17[.]225	AbuseIPDB 0% (RO) · AS39798 MivoCloud SRL
IP	141[.]11[.]164[.]153	AbuseIPDB 0% (CH) · AS212238 DataCamp Limited
IP	192[.]142[.]54[.]79	AbuseIPDB 0% (NL) · AS214036 Ultahost Inc.
IP	84[.]200[.]205[.]165	AbuseIPDB 0% (DE) · AS214036 Ultahost Inc.
IP	88[.]80[.]150[.]199	AbuseIPDB 0% (BG) · AS44901 BelCloud Ltd
IP	88[.]80[.]150[.]200	AbuseIPDB 0% (BG) · AS44901 BelCloud Ltd
IP	88[.]80[.]150[.]202	AbuseIPDB 0% (BG) · AS44901 BelCloud Ltd
Domain	ocferda[.]com	
Domain	ocferda[.]com	
Domain	tylarion867mino[.]com	
Domain	tylarion867mino[.]com	
Domain	uuokhhfsdlk[.]tylarion867mino[.]com	
Domain	uuokhhfsdlk[.]tylarion867mino[.]com	

Type	Indicator	Context
Hash	95bd07b4400095acdafce05888da27228d7d07ca	
Hash	95bd07b4400095acdafce05888da27228d7d07ca	
Hash	366e435a1ea0f597deb6ebe7c0c5acdb6e8b33eb	
Hash	366e435a1ea0f597deb6ebe7c0c5acdb6e8b33eb	

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:** T1078 Valid Accounts (initial-access)
- **Observed here:** T1078 Valid Accounts 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 29+ groups that use Valid Accounts, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The Cyber Av3ngers could pivot to using Windows Management Instrumentation (T1047) as their next technique, as it would allow them to leverage the existing network infrastructure and management tools to gather information or execute actions on compromised systems, potentially evading detection by blending in with legitimate administrative activity. This technique may be particularly appealing to the Cyber Av3ngers because it enables them to interact with systems in a way that is often difficult to distinguish from normal system administration, making it harder for defenders to identify malicious activity. To counter this potential move, the mandated defensive control is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1053 Scheduled Task/Job (n=31, lift 1.4)

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