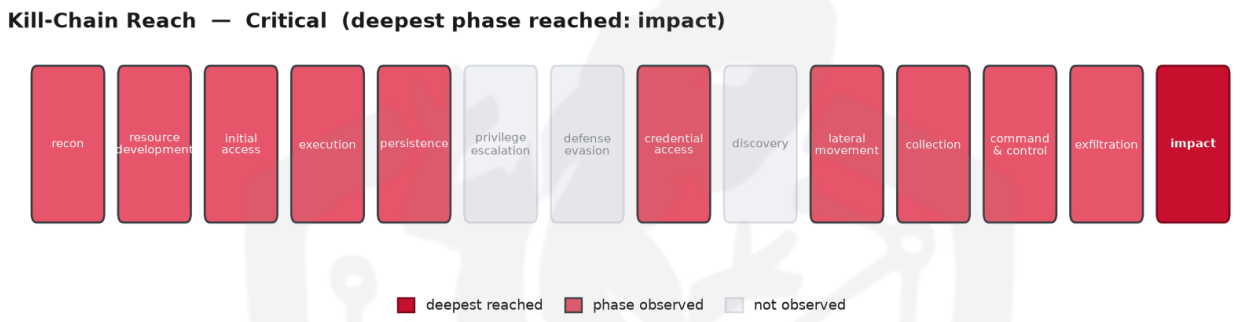
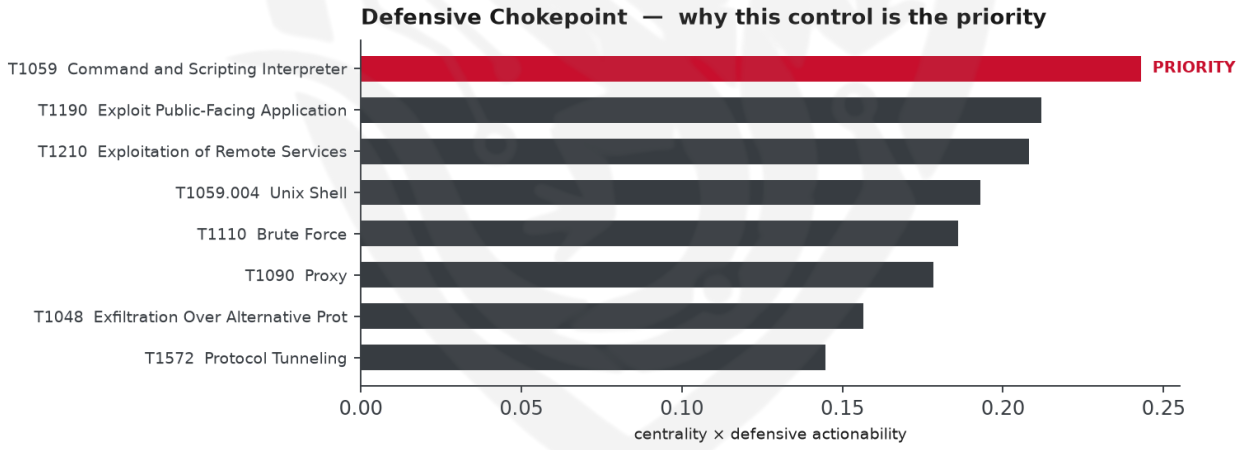
THREAT REPORT: MIRAI-BASED EVOOO1BOT BOTNET TURNS COMPROMISED LINUX HOSTS INTO PROXIES

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 leverages the Mirai-derived Evooo1Bot malware to compromise Linux systems and repurpose them as network proxies. Exploitation centers on CVE-2007-3010, among other listed vulnerabilities, though the primary focus is the 2007 flaw. Victim geography and sectors are not disclosed in the source. Defensive priority should be to constrain PowerShell for unprivileged users (Constrained Language Mode + AppLocker), enable script-block logging, block wscript/cscript where unnecessary, and promptly patch CVE-2007-3010 on all affected hosts.

Threat Overview

The source does not identify a specific adversary, describing the threat actor as “Data Insufficient.” The campaign employs the Evooo1Bot and Mirai malware families, exploiting the public-facing vulnerability CVE-2007-3010 to gain footholds on Linux devices. No concrete information on targeted countries or industry sectors is provided.

Attack Chain and Priority Control

The activity follows a multi-stage chain:

1. **Acquire Infrastructure** (T1583) – the operators obtain hosting resources.
2. **External Remote Services** (T1133) and **Exploit Public-Facing Application** (T1190) – they reach vulnerable internet-exposed services.
3. **Exploitation of Remote Services** (T1210) and **Brute Force** (T1110) – credential-guessing and service abuse are used to gain initial access.
4. **Command and Scripting Interpreter** (T1059) – the priority chokepoint where malicious scripts are executed on compromised hosts.
5. **Unix Shell** (T1059.004) and **Application Layer Protocol** (T1071) – facilitate command execution and data movement.
6. **Proxy** (T1090) and **Protocol Tunneling** (T1572) – compromised machines are turned into proxies for further traffic.
7. **Stage Capabilities** (T1608) and **Ingress Tool Transfer** (T1105) – additional tools are delivered.
8. **Exfiltration Over Alternative Protocol** (T1048) and **Network Denial of Service** (T1498) – enable data theft and disruptive actions.

Priority technique: T1059 Command and Scripting Interpreter.
Concrete control: *Constrain PowerShell for unprivileged users (Constrained Language Mode + AppLocker); enable script-block logging; block wscript/cscript where unneeded. In parallel, patch CVE-2007-3010 on all affected systems.*

Infrastructure and Corroboration

Third-party enrichment indicates that the malicious command-and-control nodes are hosted by TechTies Inc., as observed in the associated ASN data. AbuseIPDB reports no indicators with confidence ≥ 80 % (the highest confidence observed is 17 %). Abuse.ch does not corroborate any additional malware families for this activity.

Technical Appendix

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

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

- T1557 Adversary-in-the-Middle
- T1583 Acquire Infrastructure
- T1133 External Remote Services

- T1071 Application Layer Protocol
- T1190 Exploit Public-Facing Application
- T1572 Protocol Tunneling
- T1589 Gather Victim Identity Information
- T1595 Active Scanning
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1608 Stage Capabilities
- T1210 Exploitation of Remote Services
- T1048 Exfiltration Over Alternative Protocol
- T1110 Brute Force
- T1059.004 Unix Shell
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1498 Network Denial of Service
- T1105 Ingress Tool Transfer
- T1556 Modify Authentication Process

Analytical Scores

- Priority technique (graph chokepoint): T1059 Command and Scripting Interpreter (centrality 0.3254).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3182; 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
Sea Turtle	0.3182
APT28	0.315
Ember Bear	0.2863
Contagious Interview	0.2654
OilRig	0.2644

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 17%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	91[.]92[.]40[.]118	AbuseIPDB 17% (NL) · AS197170 TechTies Inc.

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:** T1059 Command and Scripting Interpreter (execution)
- **Observed here:** T1059 Command and Scripting Interpreter was the only execution technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (execution)
- **Basis:** of the 54+ groups that use Command and Scripting Interpreter, this pairing runs 1.3x above base rate, a disproportionately-coupled move rather than the obvious one.

With T1059 Command and Scripting Interpreter blocked, the threat actor could preserve the same objective by pivoting to T1053 Scheduled Task/Job, a technique disproportionately paired with it across tracked groups. Defensive countermeasure: Alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1574 Hijack Execution Flow (n=32, lift 1.2), T1106 Native API (n=19, lift 1.3)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File