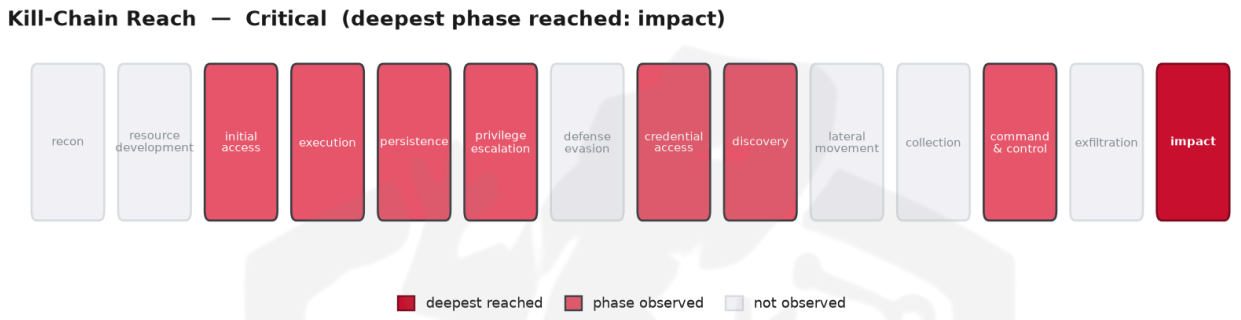
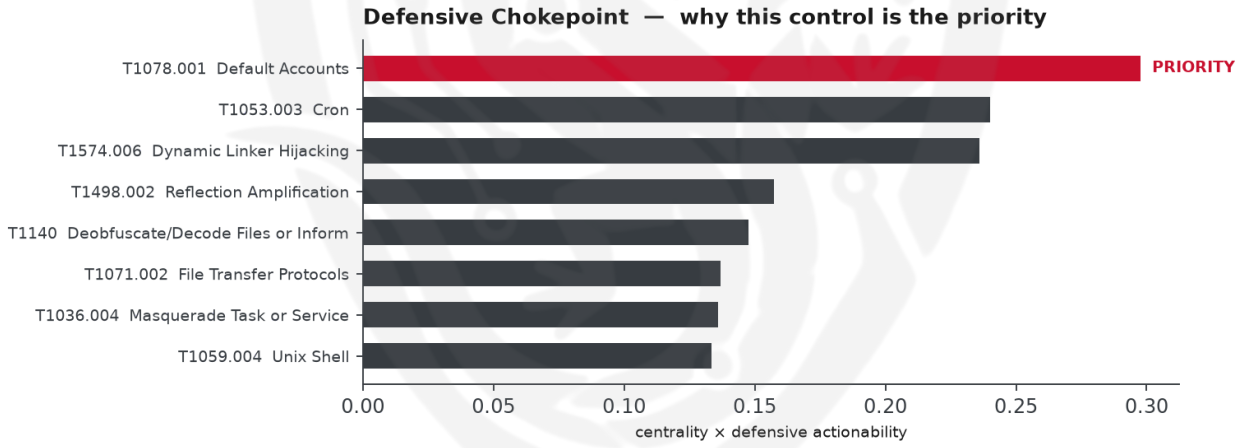
THREAT REPORT: UNKNOWN_ADVERSARY IOT BOTNET CAMPAIGN

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 has been linked to several malware families, including TuxBot v3 Evolution, AISURU, Kaitori, Tsunami, Mirai, Gafgyt, and MHDDoS. The threat actor is targeting IoT devices, and priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the risk. The campaign's impact is considered critical, and defensive actions should focus on securing accounts and monitoring for anomalous logons. The lack of specific targeting information makes it essential to prioritize general security measures.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, is utilizing a range of malware families to compromise IoT devices. The malware families involved include TuxBot v3 Evolution, AISURU, Kaitori,

Tsunami, Mirai, Gafgyt, and MHDDoS. The victimology of this campaign is not well-defined due to insufficient data, but the use of various techniques suggests a broad range of potential targets.

Attack Chain and Priority Control

The attack chain involves multiple techniques, including password guessing, network flooding, and system information discovery. The priority technique identified is T1078.001 Default Accounts, which is a critical chokepoint in the attack chain. To mitigate this risk, the priority 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 associated with this campaign is hosted on providers such as FlokiNET Ehf, Packet Star Networks Limited, and Boomerang Communications LLC. However, there are no malware families corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, with the highest confidence seen being 0%. These findings are based on third-party enrichment and do not override the primary source information.

Technical Appendix

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

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

- T1110.001 Password Guessing
- T1498.001 Direct Network Flood
- T1568.002 Domain Generation Algorithms
- T1071.004 DNS
- T1489 Service Stop
- T1497.001 System Checks
- T1053.003 Cron
- T1082 System Information Discovery
- T1498.002 Reflection Amplification
- T1140 Deobfuscate/Decode Files or Information
- T1078.001 Default Accounts
- T1574.006 Dynamic Linker Hijacking
- T1083 File and Directory Discovery
- T1036.004 Masquerade Task or Service
- T1057 Process Discovery
- T1071.002 File Transfer Protocols
- T1090.003 Multi-hop Proxy
- T1059.004 Unix Shell
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols

- T1543.002 Systemd Service

Analytical Scores

- Priority technique (graph chokepoint): T1078.001 Default Accounts (centrality 0.2977).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.381; 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
APT18	0.381
Rocke	0.381
Higaisa	0.3366
APT41	0.335
Tropic Trooper	0.312

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	185[.]10[.]68[.]127	AbuseIPDB 0% (RO) · AS200651 FlokiNET Ehf
IP	194[.]46[.]59[.]169	AbuseIPDB 0% (GB) · AS204044 Packet Star Networks Limited
IP	154[.]6[.]197[.]43	AbuseIPDB 0% (US) · AS395880 Boomerang Communications LLC

Type	Indicator	Context
Domain	jetross[.]com	
Domain	cfcybernews[.]eu	
Domain	digikalas[.]online	
Domain	newtuxdev[.]sevielw[.]digikalas[.]online	
Hash	71dfbb171eca4ef9d02ff630b56e5283bbef7b375d4dbe9e8c9531bef312fa8d	
Hash	50eadccdd0f2182bdc9f74aa7b3250b5	
Hash	12c167b69ad8089299fa342bdc22f99bebea7c01	
Hash	2774a5f5991657eb9b0062cd3da0391c9bad2643	
Hash	304e14a138b92135aad27bb37f4e9db440401ec2	
Hash	4cba585d9f208bd712b28f867f908e503ccc9cfe	
Hash	4e1483737f769e1cee80fa4d7a056a5d8e3b537e	
Hash	64af594c7f91793813e3d769e63816b143102396	
Hash	69dc276dde8efcb409411508da55d4cbe28d5600	
Hash	74fba0bad93bbb0e1eedb196b6efe6af1c0bf23d	
Hash	7ad840b1945cc346012987727ebcc062431965a4	
Hash	81670f250f4b3492fd3e00920f9fe7395ecbf85c	
Hash	877b804892ab218a53420b6dfbd0a2837368d0b5	
Hash	a70cea846442c18ad265f311b5ced29a4071771d	
Hash	a8fd13f6b1bdfa87c0f466df69b7e81325b5dd15	
Hash	adf267caab78a74c4b4dfabe7b578b0a4d639782	
Hash	b1cc41e2b9ddb11d0c9d03d319531fea9459cdae	
Hash	b21cdc5e1b96c640a1d553ed518c49729e367823	

Type	Indicator	Context
Hash	befb0e4d1cd7d2b4139b55f811993af2c8839e75	
Hash	cd540bb31909440fd2bf773e6f1480f5b6f12400	
Hash	e0f8dd23e4fb0086feb42ea0a5dcef70d7b4d17c	
Hash	0f8bcca3ed65e980da2a1f90a767b7d543be32eeea3e9 338d09d4d635a497988	
Hash	146f6010f6ee082aab13e0148d39baefa77eaba4ff6581 7b511b08c2092bdfd2	
Hash	15c17dce89deccd5172285b2650de957918aa1157cde 8e4633ae15dfe31f2711	
Hash	246c97957651de568e61eba1abe572f0b0f960456209995d43d53a0d7cc494a1	
Hash	2f2c3551762c03da126e45dca6fc2f997c63f0f1bfc21fd0 ceed680ac6f083ce	
Hash	3ec016d637e4c9cd331edd2580a229621ad638e924a4 aa29ac0342e9144ace19	
Hash	511d3ffb4091cbcc94571d9fb3102e8cb424c6e187d01d 53ff12078d54929bda	

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:** T1078.001 Default Accounts (initial-access)
- **Observed here:** T1078.001 Default Accounts was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1190 Exploit Public-Facing Application (initial-access)
- **Basis:** 32 of 170 documented groups that use Default Accounts also use Exploit Public-Facing Application (conditional 0.50, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

The actor could pivot to exploiting a public-facing application, as indicated by T1190, in an attempt to regain a foothold and continue their objective, potentially leveraging unpatched vulnerabilities to bypass the initial block. This shift may allow the actor to maintain access and move laterally within the network, exploiting weaknesses in external-facing systems. To counter this potential move, the mandated defensive

control is to patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Also plausible (same tactic): T1133 External Remote Services (n=25, lift 2.4), T1199 Trusted Relationship (n=10, lift 2.2)

Detection and hardening for the pivot (T1190 Exploit Public-Facing Application)

- **Telemetry:** WAF / reverse-proxy logs; Web server logs; EDR on the DMZ host
- **Detect:**
  - Exploit strings and anomalous request paths in access logs; 500s spikes
  - The web/app service account spawning shells or network tools
  - Outbound connections from a server that should never initiate them
- **Harden:**
  - Patch internet-facing software fast; virtual-patch at the WAF meanwhile
  - Egress filtering from DMZ hosts; least-privilege service accounts
- **MITRE:** M1051 Update Software, M1050 Exploit Protection, M1016 Vulnerability Scanning, M1030 Network Segmentation · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic