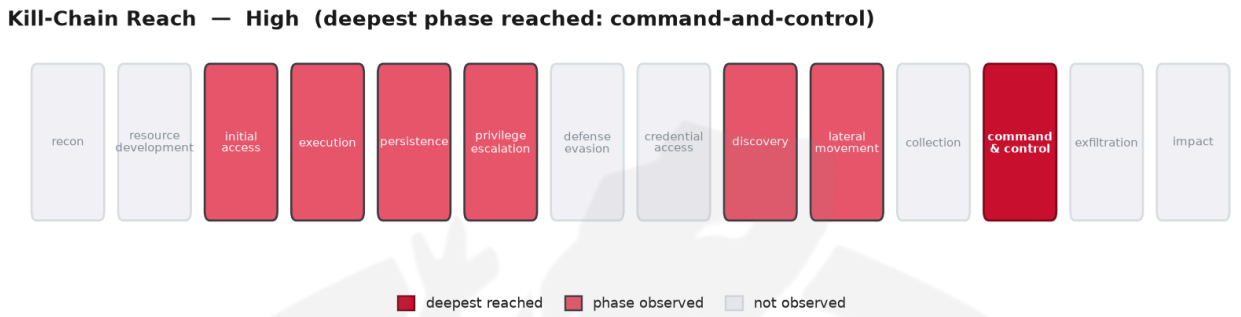
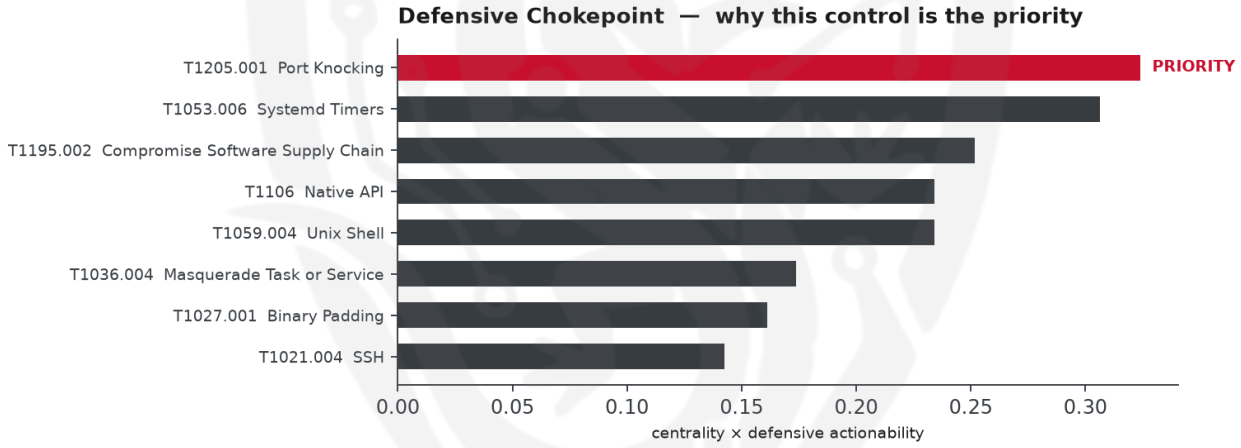
THREAT REPORT: ENDLESSDOORS CAMPAIGN

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 is associated with the ENDLESSDOORS and rctl malware families, which are exploiting the CVE-2026-66747 vulnerability. The targeted country and sectors are currently unknown. Priority should be given to patching the CVE-2026-66747 vulnerability on all affected systems and applying specific MITRE ATT&CK mitigations. The threat actor's activities have been observed to reach the command-and-control stage, posing a high operational risk.

Threat Overview

The observed cluster of activity is characterized by the use of the ENDLESSDOORS and rctl malware families, which exploit the CVE-2026-66747 vulnerability. The techniques used include a range of tactics such as bootkit, symmetric cryptography, and system information discovery. The victimology of this campaign is currently unknown.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including bootkit, symmetric cryptography, and system information discovery, ultimately leading to command-and-control. The priority technique is T1205.001 Port Knocking, which is the graph chokepoint. The priority control is to Apply the specific MITRE ATT&CK mitigation for this technique; add host/network detections and least-privilege controls around it. In parallel, patch CVE-2026-66747 on all affected systems.

Infrastructure and Corroboration

The malicious infrastructure is hosted on providers such as Hangzhou Alibaba Advertising Co. Ltd. and Hebei Sea Whale Technology Co. Ltd. Additionally, abuse.ch has corroborated the presence of the Aisuru malware family. However, no indicators have been flagged with high confidence 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, expert-tagged by source)

- T1542.003 Bootkit
- T1573.001 Symmetric Cryptography
- T1021.004 SSH
- T1082 System Information Discovery
- T1106 Native API
- T1027.001 Binary Padding
- T1083 File and Directory Discovery
- T1036.004 Masquerade Task or Service
- T1205.001 Port Knocking
- T1053.006 Systemd Timers
- T1059.004 Unix Shell
- T1195.002 Compromise Software Supply Chain
- T1573.002 Asymmetric Cryptography
- T1071.001 Web Protocols
- T1543.002 Systemd Service

Analytical Scores

- Priority technique (graph chokepoint): T1205.001 Port Knocking (centrality 0.3412).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3748; 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
Higaisa	0.3748
Rocke	0.3394
APT18	0.33
Stealth Falcon	0.3212
Cobalt Group	0.3051

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Aisuru.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	43[.]248[.]136[.]125	AbuseIPDB 0% (CN) · AS151302 Hebei Sea Whale Technology Co. Ltd.
IP	47[.]100[.]190[.]96	AbuseIPDB 0% (CN) · AS37963 Hangzhou Alibaba Advertising Co. Ltd.
IP	47[.]107[.]224[.]89	AbuseIPDB 0% (CN) · Aisuru · AS37963 Hangzhou Alibaba Advertising Co. Ltd.
Domain	zbtlink[.]com	
Domain	zbtwifi[.]com	

Type	Indicator	Context
Domain	rbdg4nzqadui[.]wikaba[.]com	
Domain	zbtctl[.]epplink[.]net	
Hash	00a1228648fffa7338076970037b89f679a166a08c4d9573f1f27973ec6ed497	
Hash	09ed9ad3ac886f5aaf8357127b6dd5926bd4af1e2cc687a6a4856bcaedee2667	
Hash	1545169fa8a3ae182d8e39aca8ec6cb6849b864e38646f29017232813e397e77	
Hash	2d558bc9a6c7e7480e946f1c0524a651554887a1c563d7633f1903d06ff493fb	
Hash	31ee58a134b766f6ed4424a22cc2cb08cfabbc9a5f35e0ae11a250c81ccc7f5e	
Hash	33f8c0532100eeb10213d167e5eb483394a7e43bf6d276441a1573360622011a	
Hash	37efadf0f4a110be0145139a43ebd032abb5b27b79b1eb2ab3578dcd31655a9e	
Hash	47d8ffb3a9a3fe0337e3c1e355fab4847dd61952fbe9aad98aadede489ca31fd	
Hash	4f5d8319b4bad5d9243496c1358fda4783ea9a0865c32881b3f57ecedb879570	
Hash	6926f919da7f4447229f49842266d884369e1587df655149673e46f1d8787e47	
Hash	71b20ebff0630b33c96bef320adc75901b34f1fd2cc9af974cf93ff37d102ec8	
Hash	73a0d95b8e23c7780cd91e978238c6db519665b05481fb228b4db9a9ec99c8ae	
Hash	76a17581bbde4c0550e8f4abfd903923aceeb50dc69dae4dd904628c273b90ee	
Hash	7791de11cd27cb596deff089904a6eab3a7e0aa391f867c2389582d5c78fef4c	

Type	Indicator	Context
Hash	ab8467e1495479693f4de8e838a5aeb61a65f3682d68f5b2d7c856cbfc91a247	
Hash	b3956cfbebf9c8d0b2c7a2ecbe59e71c31a5802f2084d25d93a984c0f811e2c7	
Hash	b3e667235e9b41b8fc3594edaa64879750e7f75d7518fff7514d55837430411a	
Hash	b4fda77e082fbf961db02273999e92e715e1824140ea92b2ab30163338b6622b	
Hash	dc1f4056af20677bdc7294ae4707f0c7bdfc85d8b57db212b622b9dc09c92731	
Hash	dcdaa1fe80707b8d8fde8ad36c3e62a53623aff09bf5ccc544d4c1a1a54208b8	
Hash	dee3908280b91cb7ad60c69c1d34c599ceed7c8c66c025851e5831482815b271	
Hash	e85104fce4061d52d47f4528df9aaf656edc49f05c0f026c5bc6b65d57eb7f22	
Hash	efc8a8ead69c63ecfffd883cfbe6bd131082aa13c0d3b324c00d79f4c149bd92	
Hash	f019d03c2489b2bc486d71e355e07f8f2862dff078574a8662a5a45932e7e453	
Hash	f5a94e536a1cac8552fb9c327c4bac6017e034786be98cc402a149cb51250d8f	
Hash	f961e4243e759453294340bc7d1b145016d70b97ab328caf47c64ea3cd818148	
Hash	df1ae1a109b329689a1eb3d1bd9bd1e9ed247cfd	

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:** T1205.001 Port Knocking (persistence)

- **Observed here:** T1205.001 Port Knocking was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1505 Server Software Component (persistence)
- **Basis:** of the 3+ groups that use Port Knocking, this pairing runs 4.0x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1505 Server Software Component by exploiting vulnerabilities in server software to gain access to sensitive areas, potentially leveraging the existing network knowledge gained from the initial port knocking attempt to identify vulnerable server components. This technique may be particularly appealing as it allows the actor to blend in with normal server activity, making it harder to detect, and could enable them to install web shells or backdoors. The defender would likely counter this by implementing the mandated defensive control: Integrity-monitor web-server directories for web shells; restrict server module/plugin installation.

Also plausible (same tactic): T1547 Boot or Logon Autostart Execution (n=3, lift 2.2), T1078 Valid Accounts (n=3, lift 2.0)

Detection and hardening for the pivot (T1505 Server Software Component)

- **Telemetry:** Web server logs; File integrity monitoring on web roots; EDR
- **Detect:**
  - New/modified files in web-accessible directories (aspx/php/jsp)
  - w3wp.exe / httpd spawning cmd.exe, powershell.exe or whoami
  - Anomalous POSTs to newly created endpoints in web access logs
- **Harden:**
  - File integrity monitoring on web roots; least-privilege service accounts
  - Remove dev tooling from production web servers; WAF in front
- **MITRE:** M1047 Audit, M1018 User Account Management, M1042 Disable or Remove Feature · DS0022 File, DS0009 Process, DS0015 Application Log