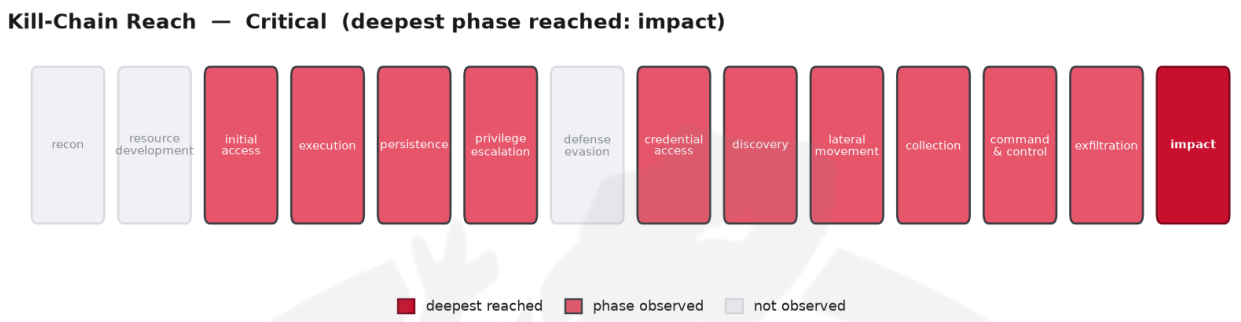
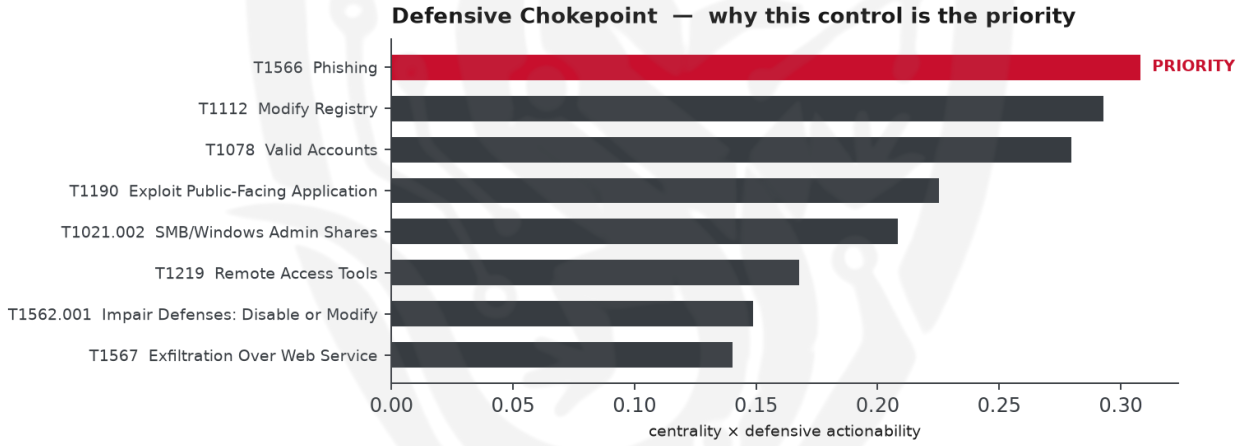
THREAT REPORT: INC RANSOMWARE CAMPAIGN

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 source attributes this activity to INC, a threat actor utilizing the Brave Prince, Lynx, Sinobi, and Cobalt Strike malware families to target various sectors, including legal, manufacturing, and healthcare. The actor is exploiting the CVE-2025-5777 vulnerability, among others, to gain access to systems. Priority should be given to patching the CVE-2025-5777 vulnerability on all affected systems to prevent further exploitation. The threat actor's use of phishing as a primary technique highlights the need for robust email security measures.

Threat Overview

The INC threat actor is utilizing a range of malware families, including Brave Prince, Lynx, Sinobi, and Cobalt Strike, to exploit vulnerabilities such as CVE-2025-5777. The actor is targeting multiple sectors, including legal, manufacturing, technology, healthcare, construction, and education. The exploited vulnerability and malware families are key components of the threat actor's attack chain.

Attack Chain and Priority Control

The observed techniques used by the INC threat actor form a complex attack chain, involving various tactics such as adversary-in-the-middle, OS credential dumping, and service stop. The priority technique is T1566 Phishing, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to: Patch CVE-2025-5777 on all affected systems as the top priority, then: Enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button.

Infrastructure and Corroboration

Although there is no observed hosting provider or ASN, the malware family INC has been corroborated by abuse.ch. However, no indicators have been flagged with an AbuseIPDB confidence of 80% or higher, with the highest confidence seen being 0%. These corroboration efforts provide additional context to the threat actor's activities, but 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)

- T1557 Adversary-in-the-Middle
- T1003 OS Credential Dumping
- T1489 Service Stop
- T1071 Application Layer Protocol
- T1190 Exploit Public-Facing Application
- T1567 Exfiltration Over Web Service
- T1219 Remote Access Tools
- T1021.002 SMB/Windows Admin Shares
- T1112 Modify Registry
- T1083 File and Directory Discovery
- T1566 Phishing
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1486 Data Encrypted for Impact
- T1027.002 Software Packing
- T1018 Remote System Discovery
- T1021.001 Remote Desktop Protocol
- T1569.002 Service Execution
- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.3082).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4338; 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
Medusa Group	0.4338
BlackByte	0.4029
INC Ransom	0.3742
Wizard Spider	0.364
APT39	0.36

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: INC.
- 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
Domain	incblog[.]su	
Domain	incblog6qu4y4mm4zvw5nrmue6qbwtgjsxpw6b7ixzssu36tsajldoad[.]onion	
Domain	incpaykabjqc2mtdxq6c23nqh4x6m5dkps5fr6vgdkgzp5njssx6qkid[.]onion	
Hash	6cd349eda0fa6c8b274a0920852c68f8b727afea1fdbc69ad183cef05d9cf141	INC
Hash	03dd0efa84d145d7d4ed8e240267e5c5	INC
Hash	265a8e89464e32b22553ef16edbab703da7176a7	INC

Type	Indicator	Context
Hash	dce9ad6317ce147f1f3f74bc93d9252a	
Hash	eb37c4fcfc00d3813ab94f4d59378b47	
Hash	16bad42a397db2e075e09b5b9dd53aaa67b495a4	
Hash	70331fdf528f4f5b75b5e30427e379bc88aa05b4	
Hash	31800380c359143ae82c4f9011eee653dd22443d03d6a499148203bbfc275502	
Hash	acce811c4fc2a6e3fddd4231e386f1648ca44f039d2d275316bc0a0fc96e0af4	
Hash	1898d056463284d849801cbdea6a3dec6c9f568f01569912c3868a5eea9a5449	
Hash	1d10d8f5a420d0e4683b4cb40bcf0c984d1e7ea1f3b4442a00a525584632ac11	
Hash	24f6c0ca39b2a5593086ff56d818ddfbde121f8e44d54faa762e510397dc9db7	
Hash	589d9480fbfec2d8e61638eb0b537183d0f9977411fd1d2c0f8eb611feebe880	
Hash	5cc212f84d2bf3fbab165aaf09b16e00fcf2f1ccd880d24b14404c53dcdbf241	
Hash	60aeb9f7bccf377ff02ed64783e66a62c0f976878d9729b067bc7e5b0b9da9d6	
Hash	6bf155b269d452f3c3b62832b27bbebe4da436e228dbf521155b1d5989e3743f	
Hash	765508aa2ec6a1b73a76a23f4fa559d32355622748c91a46ed7b315eae2ee60a	
Hash	7f37351979c249417cb180b4ede0ed17e5fe2a1f08add4d72606b589f8fdb245	
Hash	8d1a22c430252f29611766b8e4a82af0fba60d609246463466b384d6d4793df4	
Hash	90e46e89fec2108a1cb4850bb33e3563e92a14d04e1e613ac8c9311f152d294c	
Hash	97aebda5482899fef84a24e456bff055acaa47e5ab4029f768d9e0c62a660ce2	
Hash	bf8c45e5aa9551a17eefbd1d179422c32b4309c47ee9a3f315bb80ed6d4f7efc	
Hash	d26bfb0147f60dc6500a9298d521ee67b49daaf4b8f8be54e7cc8fd86a597570	
Hash	d65120291dee76c694f8bea54841f7f68329b499b28f4aee5ea5c9369a7432cb	
Hash	dc9938f51150d13a69fc25f3f19052eacb1bf0a086fd5cf39762501fb3ddd7da	
Hash	ea721240c14e3d14f8d88e0020880448c6c602f1180a1e5dbe40871cfeedcc22	
Hash	f6a01d0246ce31faf6938ea488086d4358505405a4ef5c5faa482e79e92cb347	
Hash	ff5da8f0330a4c581c37284c74aae2683c007dc6e406e1e2e6803e7bb398b77b	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.