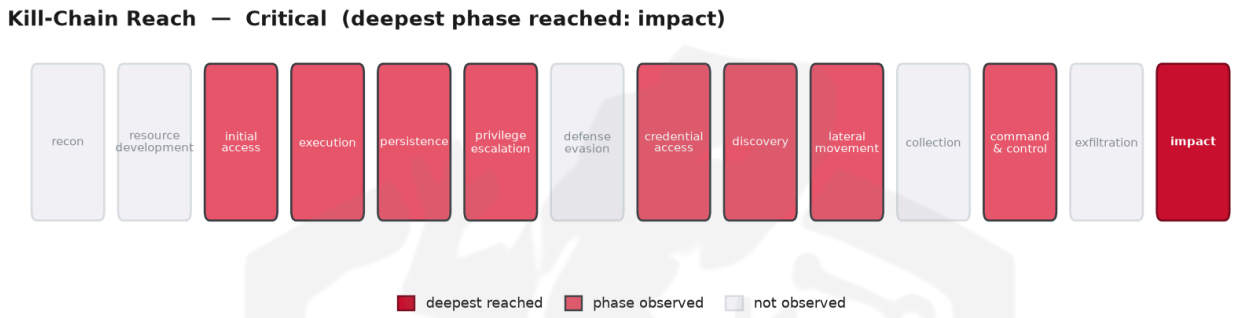
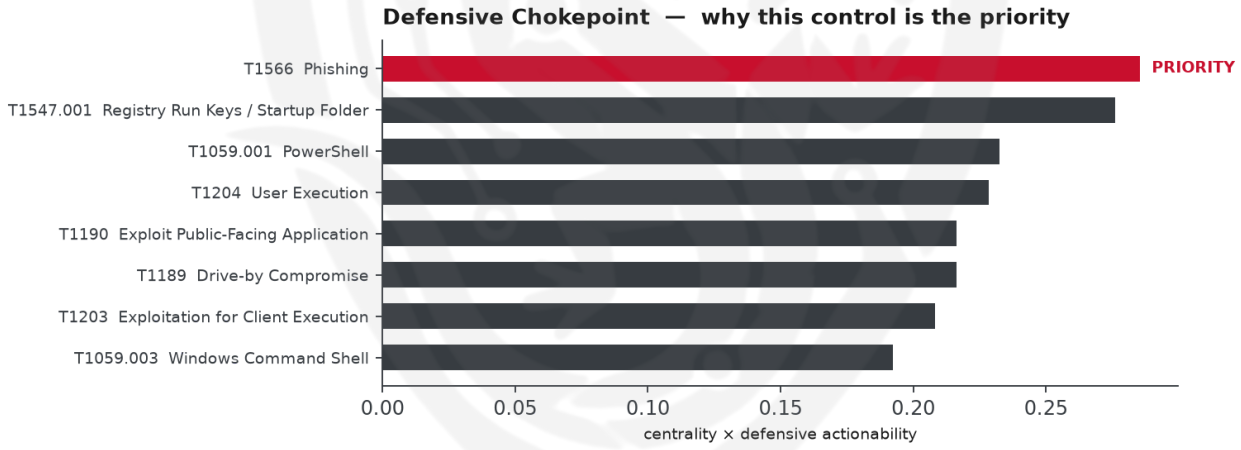
THREAT REPORT: HIVE0163, RHYSIDA, VANILLA TEMPEST, TAG-124, ITG23

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 threat actors Hive0163, Rhysida, Vanilla Tempest, TAG-124, and ITG23 have been observed targeting various sectors in the United States of America, utilizing a range of malware families including NodeSnake, InterlockRAT, and Rhysida. The primary vulnerability exploited is CVE-2026-20131. Priority should be given to patching this vulnerability on all affected systems to prevent further exploitation. The actors' campaign has significant implications, affecting multiple industries.

Threat Overview

The observed cluster of activity, attributed to Hive0163, Rhysida, Vanilla Tempest, TAG-124, and ITG23 by the source, involves the use of multiple malware families, including NodeSnake, InterlockRAT, and Rhysida, to exploit the CVE-2026-20131 vulnerability. The threat actors are targeting a broad range of

sectors, including aerospace, agriculture, and finance, among others. The malware families utilized are diverse, indicating a complex and adaptable campaign.

Attack Chain and Priority Control

The attack chain involves various techniques, including phishing, process injection, and domain account discovery, ultimately leading to data encryption for impact. The priority technique identified is T1566 Phishing, which serves as a critical entry point for the threat actors. To mitigate this threat, the priority control is to: Patch CVE-2026-20131 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 specific hosting providers or ASNs are not identified, abuse.ch has corroborated the presence of the INTERLOCK malware family. There are no indicators with an AbuseIPDB confidence level of 80% or higher, with the highest confidence seen being 0%. This lack of specific infrastructure details highlights the need for vigilance and proactive measures to prevent exploitation.

Technical Appendix

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

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

- T1053.005 Scheduled Task
- T1218.011 Rundll32
- T1003 OS Credential Dumping
- T1087.002 Domain Account
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1055 Process Injection
- T1482 Domain Trust Discovery
- T1083 File and Directory Discovery
- T1204 User Execution
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1566 Phishing
- T1486 Data Encrypted for Impact
- T1203 Exploitation for Client Execution
- T1059.003 Windows Command Shell
- T1189 Drive-by Compromise
- T1027.002 Software Packing
- T1018 Remote System Discovery

- T1105 Ingress Tool Transfer
- T1021.001 Remote Desktop Protocol
- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2855).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4814; 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
Silence	0.4814
APT3	0.4695
Dark Caracal	0.4686
BRONZE BUTLER	0.4633
menuPass	0.4607

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: INTERLOCK.
- 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	185[.]196[.]9[.]234	AbuseIPDB 0%
IP	157[.]250[.]195[.]229	

Type	Indicator	Context
IP	213[.]139[.]77[.]167	
IP	170[.]168[.]103[.]208	
IP	216[.]219[.]95[.]234	
Domain	leadslaw[.]com	
Domain	registrywave[.]com	
Domain	coretether[.]com	
Domain	nucleusgate[.]com	
Domain	scs-techresources[.]com	
Domain	microsoft-teams[.]icu	
Domain	typically-performer-builds-increasing[.]trycloudflare[.]com	
Domain	repair-provision-supplies-folder[.]trycloudflare[.]com	
Domain	confident-accounts-ban-damaged[.]trycloudflare[.]com	
URL	hxxps://apple-online[.]shop/ChromeSetup[.]exe	
URL	hxxps://apple-online[.]shop/MSTeamsSetup[.]exe	
Hash	f0b3e112ce4807a28e2b5d66a840ed7f	
Hash	54a6743781fd4ceb720331fce92f16186931192d	
Hash	333903c7d22a27098e45fc64b77a264aa220605cfbd3e329c200d7e4b42c881c	
Hash	edbf152ed9ac79e5d9e0111d1071af48	
Hash	b0cfa2089802634ffb8c77962cdb18317a6332d4	
Hash	64a0ab00d90682b1807c5d7da1a4ae67cde4c5757fc7d995d8f126f0ec8ae983	
Hash	c9920e995fbc98cd3883ef4c4520300d5e82bab5d2a5c781e9e9fe694a43e82f	INTERLOCK
Hash	43f4ca1c7474c0476a42d937dc4af01c8ccfc20331baa0465ac0f3408f52b2e2	
Hash	7890b116d13a52efe696ce1e2c0ed83029775cf4bea836ce551e71d222ee116f	
Hash	f962e15c6efebb3c29fe399bb168066042b616affddd83f72570c979184ec55c	
Hash	28a9982cf2b4fc53a1545b6ed0d0c1788ca9369a847750f5652ffa0ca7f7b7d3	

Type	Indicator	Context
Hash	2b2e657ae1bc2fdcdfe5201a8e0e5224	
Hash	8bd16897409ae5d5667c345276d2532f493c0f98	
Hash	259fd28f9e66159d5a30b86688fec184	
Hash	42a99a5effdc1d02f6b622537de881e1	
Hash	3e62797fd746ce9bd5d49cb833b7d9ac62d6b7a2	
Hash	442af2726e22f512b49f67bcdbf7c0d1e806aa8b	
Hash	16474e9e4773fbc1e0b48a5025fad31b7f084b1beffb9a42687b4d01979885fe	
Hash	2528df60e55f210a6396dd7740d76afe30d5e9e8684a5b8a02a63bdcb5041bfc	
Hash	4e4a3751581252e210f6f45881d778d1f482146f92dc790504bfbcd2bdfa0129	
Hash	6190923b28679eb8230010aff9b1d1a4184e8697540cc021a5be38126f3f6d99	
Hash	72bed9b26a7747252156b65d24a9a737d70b9bf6aca069c514c1c7b9e04ef9b6	
Hash	b659389cde06f5e01e592dca458fe1be07a302c40dc2a820c7f76d4ee788bad3	
Hash	16afa928cd820a572bd47e798f481c46	

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