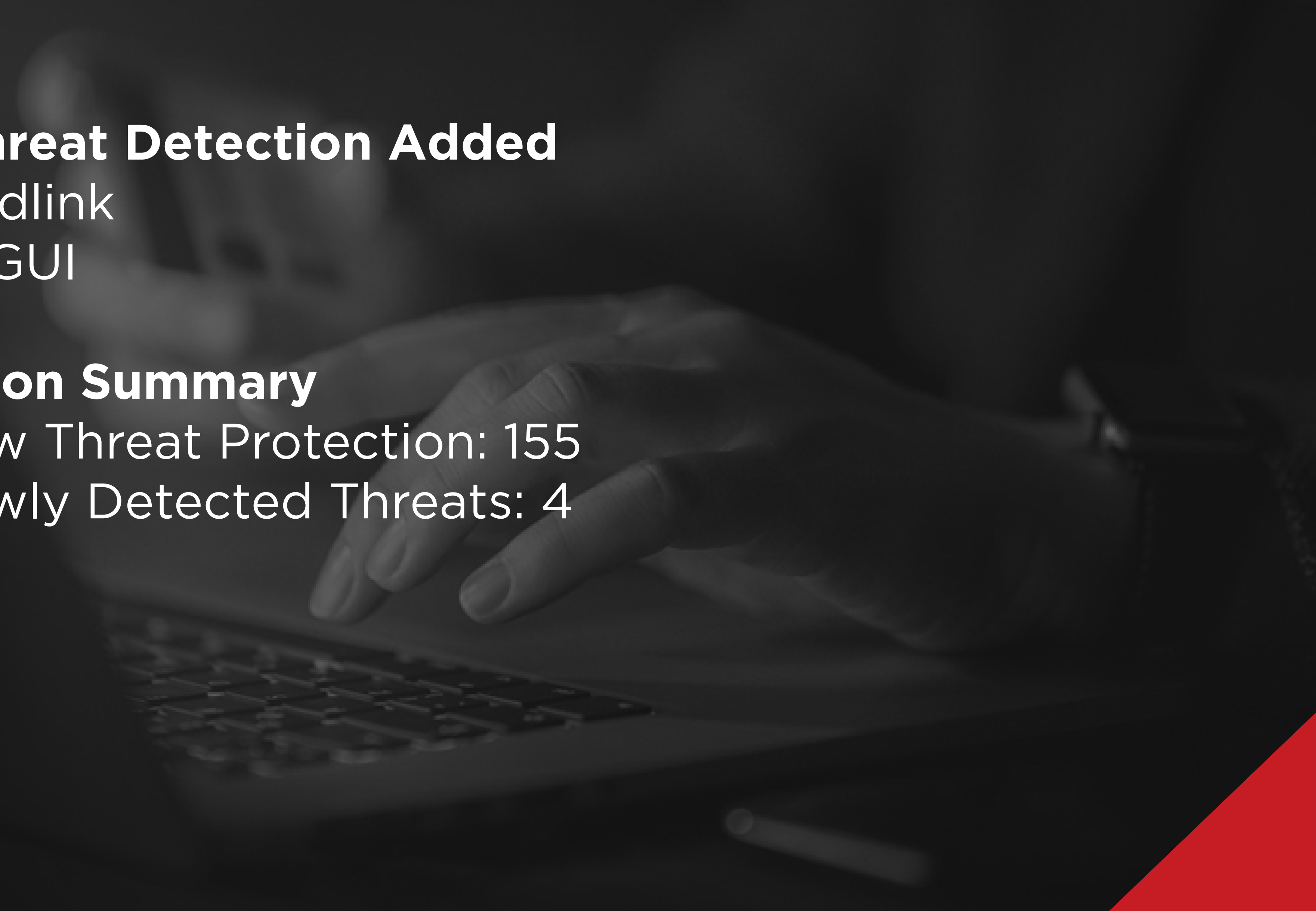
THREAT INTELLIGENCE REPORT

January 27 – February 02, 2026

Red Piranha
unified threat management

Report Summary:



New Threat Detection Added

- Voidlink
- CoGUI

Detection Summary

- New Threat Protection: 155
- Newly Detected Threats: 4

The following threats were added to Crystal Eye this week:

1. VoidLink

VoidLink is a recent malware that is designed for Linux systems as they make up the majority of cloud environments. The malware is written in Zig and uses a different evasion technique based on what Linux kernel the host is running; it automatically chooses to use eBPF or LKM (can do a Hybrid of both as well) depending on the kernel version, this information is sent to the C2 server, which then creates a complied module that is sent back to the infected host. The malware also has the capability to remove all evidence of itself from the infected system; this ranges from deleting logs, command history, artefacts.

The malware can target Docker Containers, Kubernetes, AWS, Alibaba, Tencent and GCP environments. The malware attempts to escape the containers and looks for sensitive files stored on the host system.

Threats Protected: 1
Class Type: Trojan-activity
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Reject	Drop

Kill Chain:

Tactic	Technique ID	Technique Name
Defence Evasion	T1622	Debugger Evasion
	T1678	Delay Execution
	T1140	Deobfuscate/Decode
	T1564	Files or Information
	T1070	Hide Artefacts
	T1014	Rootkit
Discovery	T1526	Cloud Service Discovery
Collection	T1119	Automated Collection
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

2. CoGUI

CoGUI is phishing kit that is primary targeting Japan. The phishing kit deploys a few evasion techniques to avoid detection and analysis. It deploys Geofencing, header fencing and fingerprinting to ensure it's only accessible but the intended victims. The phishing kit has been identified to be Dracula phishing kit which is link to China.
The campaign has impersonated Amazon, payment cards, transport card, Rakuten, Apple and Japan national tax (NTA). The campaign does not appear to have the ability to capture MFA credentials like similar platforms (evilginx).

Threats Protected: 2
Class Type: Credential-theft
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Reject	Drop

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Defence Evasion	T1672 T1070 T1036	Email Spoofing Indicator Removal Masquerading
Credential Capture	T1056	Input Capture

Current Threat Summary

Known Exploited Vulnerabilities (Week 5 - January 2026)

Vulnerability	CVSS	Description
CVE-2026-1281	9.8	Ivanti Endpoint Manager Mobile (EPMM) contains a vulnerability that can allow an unauthenticated remote attacker to execute operating system commands via HTTP request. Exploitation of this vulnerability can result in an attacker gaining complete access to the system.
CVE-2026-24858	9.4	Multiple Fortinet products contain an authentication bypass vulnerability that could allow an unauthenticated remote attacker to sign into the device via FortiCloud SSO. Exploitation of this vulnerability required an attacker to have a FortiCloud account along with a registered device and could allow authenticating to devices registered by an account they do not control.

For more information, please visit the Red Piranha Forum:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-5th-week-of-january-2026/635

Updated Malware Signatures (Week 5 - January 2026)

Threat	Description
Tycoon 2FA	This is a Phishing-as-a-Service (PhaaS) platform design to bypass/steal 2FA/MFA credentials. The platform uses reverse proxies to intercept traffic between the victim and web page (Man-in-the-Middle). This allows the credentials to be stolen by the hosting platform. The platform primarily targets Gmail and Microsoft accounts.

Ransomware Report

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. In the past week, our monitoring revealed multiple ransomware incidents across diverse threat groups, underscoring the persistent and widespread nature of these cyber risks. Presented below is a detailed breakdown of ransomware group activities during this period.

Ransomware Hits Last Week

0apt dominated this week's ransomware landscape, responsible for 23.75% of all reported incidents. This put it slightly ahead of Clop and made it the single most influential actor in the dataset, pointing to a concentrated campaign window or a bulk dump of victim disclosures that pushed 0apt to the top of the ecosystem.

Clop followed very closely at 22.74%, forming a powerful upper tier together with Qilin (8.7%). These three groups alone accounted for more than half of all observed activity, underscoring how a small set of high-volume operators continue to shape overall ransomware pressure through aggressive, multi-victim extortion operations.

A substantial mid-tier cluster included Nightspire, DevMan2, and Inc Ransom (each 4.68%), Akira and Tengu (each 3.68%), and Play and Sinobi (each 3.01%), with SafePay (2.34%) close behind. This band of actors maintained a steady operational tempo, regularly publishing new victims and contributing a significant secondary layer of risk across multiple regions and industries.

Smaller but still persistent operators, such as ShinyHunters (1.67%), RansomHouse, Genesis, and Pear (each 1%), along with Coinbase Cartel (1.34%), and low-mid volume crews like Worldleaks, DragonForce, Anubis, Rhysida, Orion, Nitrogen, Lynx (each 0.67%), added continuous background noise. While none of them rival the top-tier groups individually, together they meaningfully expand the breadth of active threats.

At the long tail, a wide range of fringe brands, The Gentlemen, Crypto24, Nova, Abyss-data, Kazu, Money Message, Interlock, Morpheus, Leaknet, Chaos, Beast, Benzona, Eraleign (APT73) and others (each 0.33%), appeared only sporadically but still contributed to overall fragmentation and churn. Individually minor but collectively resilient, this long-tail activity highlights how crowded and diversified the ransomware ecosystem remains even in weeks where a handful of families dominate the numbers.

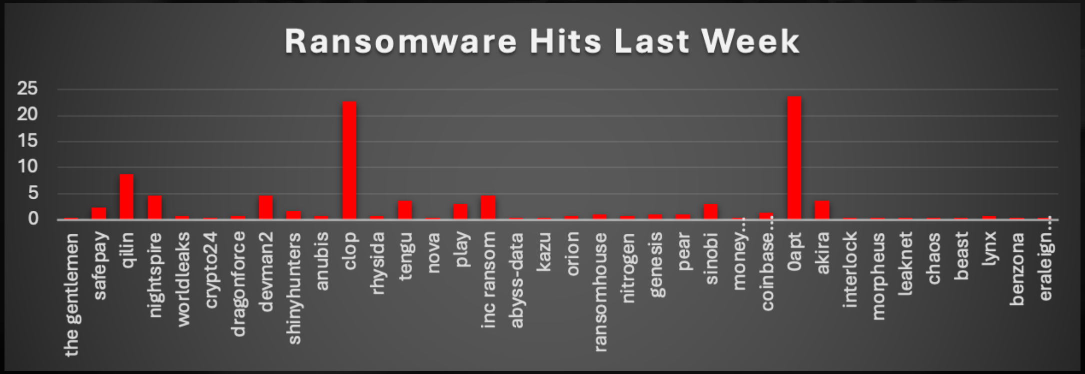


Figure 1: Ransomware Group Hits Last Week

0APT Ransomware

0APT is a newly identified Ransomware-as-a-Service (RaaS) syndicate that emerged on January 28, 2026, with an unprecedented campaign compromising 71 organisations across multiple sectors within 48 hours. The group employs double extortion tactics, combining AES-256/Salsa20 file encryption with data exfiltration and public leak threats.

Threat Actor Description

0APT (pronounced "Zero-APT") is a financially motivated ransomware syndicate that explicitly distances itself from nation-state Advanced Persistent Threat actors. The group brands itself as a "politically neutral underground syndicate" focused purely on financial gain. Their ransom notes frame attacks as a "tax on security negligence" - psychological tactics designed to normalise payment and discourage victim resistance.

Group Characteristics

Attribute	Details
Group Name	0APT (Zero-APT)
First Observed	January 28, 2026
Operational Model	Ransomware-as-a-Service (RaaS)
Extortion Method	Double Extortion (Encryption + Data Leak)
Motivation	Financial - Explicitly non-political
Attribution	Unknown - Possible links to Haron ransomware (2021)
Victim Count (Jan 28-30)	71 confirmed organisations

Malware Characteristics

The 0APT "locker" malware is a crypto-ransomware strain written in C# targeting Windows environments with cross-platform capabilities. Analysis reveals the malware uses a hybrid encryption scheme combining Salsa20 stream cipher for file encryption with RSA-1024 for key protection. This differs from the AES-256 claim in ransom notes - a simplification for victims. The code shares technical fingerprints with Haron ransomware (2021), including the unusual trait of not appending extensions to encrypted files.

Technical Attribute	Value
Programming Language	C# (.NET)
Target Platform	Windows (primary), Linux/ESXi (reported)
File Encryption	Salsa20 stream cipher
Key Protection	RSA-1024
File Extension	None (files retain original names)
Ransom Note	HOW TO RESTORE YOUR FILES.TXT
Obfuscation	SmartAssembly (suspected), string encryption
Lineage	Technical similarities to Haron ransomware (2021)

Detailed Tactics, Techniques, and Procedures (TTPs)

Initial Access

0APT affiliates leverage multiple intrusion vectors through the RaaS model:

Credential Phishing: Sophisticated spear-phishing campaigns using phishing kits that mimic Okta/SSO login portals. Identified domains include myadyensso.com (Adyen), weworksso.com (WeWork), cnainsurancesso.com (CNA Insurance), and others. These pages hijack active sessions, bypassing MFA and providing administrative access.

Exposed Remote Services: Exploitation of RDP, VPNs, and other remote access services using stolen credentials from phishing or dark web purchases. Unpatched VPN appliances may also be targeted.

Pre-positioning: The rapid 48-hour campaign timing suggests victims may have been compromised earlier and simultaneously "detonated" at launch.

Execution & Lateral Movement

Post-exploitation follows standard ransomware playbooks:

- Internal reconnaissance to map networks, identify critical servers and backups
- Credential dumping from LSASS memory (likely Mimikatz or similar tools)

- Lateral movement via Microsoft Sysinternals PsExec and WMI
- Domain Group Policy abuse for enterprise-wide ransomware deployment
- Targeting of VMware ESXi and network storage for maximum impact

Defence Evasion

The malware employs multiple evasion techniques:

- Heavy obfuscation using SmartAssembly for C# binaries with string encryption
- Security software termination via taskkill/net stop commands
- Shadow copy deletion using vssadmin delete shadows /all /quiet
- Backup system targeting and destruction prior to encryption
- Process naming mimicking legitimate system files (e.g., svcHost.exe)

Command-and-Control

C2 infrastructure utilises:

- Dedicated C2 domains: approvalmechanism.com, commerceapprove.com, technicalposition.com
- Tor network for leak site operations and encrypted communications
- HTTPS/TLS encrypted channels for data exfiltration

Data Exfiltration

Pre-encryption data theft involves:

- Volumes ranging from 50GB to 3TB per victim
- Standard exfiltration tools (likely Rclone, FTP, cloud storage)
- Data archived and compressed before transfer
- Multi-day quiet exfiltration before ransomware detonation

Final impact phase includes:

- Salsa20 encryption deployed enterprise-wide simultaneously
- Ransom notes dropped with Tor site address and unique victim ID
- Countdown timers on leak site threatening data publication
- Cryptocurrency payment demands with short deadlines

Impact

MITRE ATT&CK Matrix

The following matrix maps observed and inferred 0APT techniques to the MITRE ATT&CK framework. Confidence levels: CONFIRMED (directly observed), HIGH (industry-standard for RaaS), MEDIUM (inferred from operational model).

Tactic	Technique ID	Description	Confidence
Initial Access	T1566.001	Spearphishing Attachment/Link - Okta SSO phishing kits	CONFIRMED
Initial Access	T1078	Valid Accounts - Stolen credentials for VPN/RDP	CONFIRMED
Initial Access	T1133	External Remote Services - RDP/VPN exploitation	HIGH
Execution	T1204.002	User Execution: Malicious File	CONFIRMED
Execution	T1059.001	PowerShell - Obfuscated script execution	HIGH
Execution	T1047	WMI - Remote execution	CONFIRMED
Persistence	T1547.001	Registry Run Keys/Startup Folder	MEDIUM
Persistence	T1053.005	Scheduled Task/Job	MEDIUM
Privilege Escalation	T1003	OS Credential Dumping - LSASS/Mimikatz	HIGH
Privilege Escalation	T1055	Process Injection	HIGH
Defence Evasion	T1027	Obfuscated Files - SmartAssembly, string encryption	CONFIRMED
Defence Evasion	T1562.001	Disable/Modify Tools - AV/EDR termination	HIGH
Defence Evasion	T1070	Indicator Removal - Log deletion	MEDIUM
Credential Access	T1003.001	LSASS Memory Dumping	HIGH
Credential Access	T1555	Credentials from Password Stores	MEDIUM
Discovery	T1135	Network Share Discovery	CONFIRMED
Discovery	T1083	File and Directory Discovery	CONFIRMED
Discovery	T1082	System Information Discovery	HIGH
Lateral Movement	T1021.002	SMB/Windows Admin Shares - PsExec	CONFIRMED
Lateral Movement	T1021.001	Remote Desktop Protocol	HIGH
Lateral Movement	T1570	Lateral Tool Transfer	HIGH
Collection	T1560	Archive Collected Data - ZIP/RAR	CONFIRMED
Collection	T1005	Data from Local System	CONFIRMED
Collection	T1039	Data from Network Shared Drive	CONFIRMED
Exfiltration	T1041	Exfiltration Over C2 Channel	CONFIRMED
Exfiltration	T1567	Exfiltration Over Web Service	HIGH
Command & Control	T1573	Encrypted Channel - HTTPS/Tor	CONFIRMED
Command & Control	T1071.001	Web Protocols	HIGH
Impact	T1486	Data Encrypted for Impact - Salsa20	CONFIRMED
Impact	T1490	Inhibit System Recovery - Shadow copy deletion	CONFIRMED
Impact	T1489	Service Stop - Security/database services	HIGH
Impact	T1485	Data Destruction (backup deletion)	CONFIRMED

Indicators of Compromise (IOCs)

The following IOCs have been validated and combined from multiple intelligence sources. Status indicates validation level.

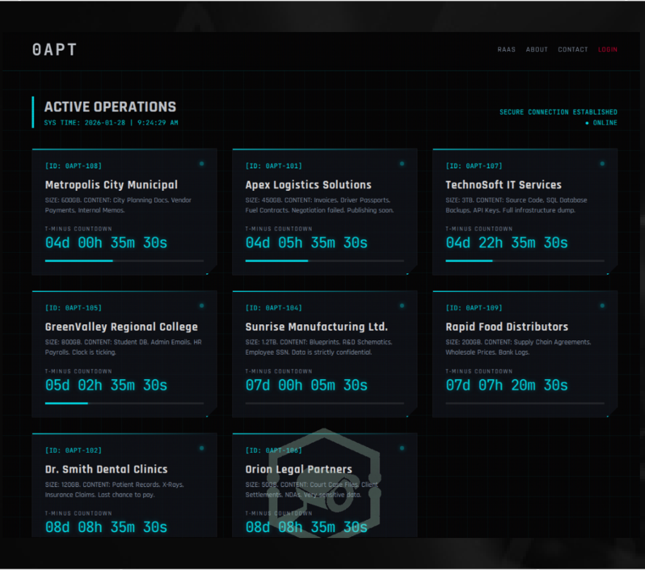
Malware File Hash

Type	Value	Status
SHA-256	a28771c1e89c474cad0dcd22d8e5bd92e42d55-fa99a8d8eb961525e75ebcd766	VALIDATED

Network Infrastructure

Tor Leak Site

Type	Value	Status
Onion Address	oaptxiyisljt2kv3we2we34kuudmqda7f2geffoylz-peo7ourhtz4dad.onion	CONFIRMED
Site Title	0APT | Command Ops	CONFIRMED
Web Server	NGINX 1.22.1	CONFIRMED



ACTIVE OPERATIONS

SYS TIME: 2026-01-28 | 9:24:29 AM

SECURE CONNECTION ESTABLISHED

• ONLINE

[ID: 0APT-108]
Metropolis City Municipal
SIZE: 600GB. CONTENT: City Planning Docs, Vendor Payments, Internal Memos.
T-MINUS COUNTDOWN
04d 00h 35m 30s

[ID: 0APT-101]
Apex Logistics Solutions
SIZE: 450GB. CONTENT: Invoices, Driver Passports, Fuel Contracts. Negotiation failed. Publishing soon.
T-MINUS COUNTDOWN
04d 05h 35m 30s

[ID: 0APT-107]
TechnoSoft IT Services
SIZE: 3TB. CONTENT: Source Code, SQL Database Backups, API Keys. Full infrastructure dump.
T-MINUS COUNTDOWN
04d 22h 35m 30s

[ID: 0APT-105]
GreenValley Regional College
SIZE: 800GB. CONTENT: Student DB, Admin Emails, HR Payrolls. Clock is ticking.
T-MINUS COUNTDOWN
05d 02h 35m 30s

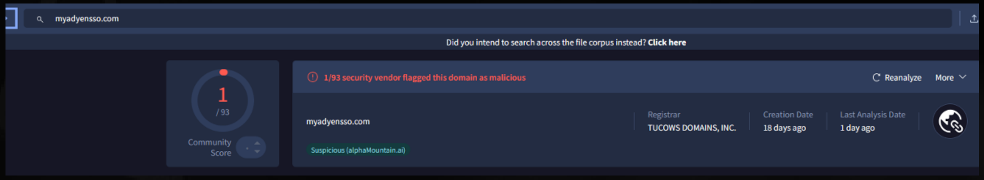
[ID: 0APT-104]
Sunrise Manufacturing Ltd.
SIZE: 1.2TB. CONTENT: Blueprints, R&D Schematics, Employee SSN. Data is strictly confidential.
T-MINUS COUNTDOWN
07d 00h 05m 30s

[ID: 0APT-109]
Rapid Food Distributors
SIZE: 200GB. CONTENT: Supply Chain Agreements, Wholesale Prices, Bank Logs.
T-MINUS COUNTDOWN
07d 07h 20m 30s

[ID: 0APT-102]
Dr. Smith Dental Clinics
SIZE: 120GB. CONTENT: Patient Records, X-Rays, Insurance Claims. Last chance to pay.
T-MINUS COUNTDOWN
08d 08h 35m 30s

[ID: 0APT-106]
Orion Legal Partners
SIZE: 500GB. CONTENT: Court Case Files, Client Settlements, NDAs. Very sensitive data.
T-MINUS COUNTDOWN
08d 08h 35m 30s

Domain	Impersonating	Status
myadyensso.com	Adyen SSO/Okta Portal	CONFIRMED
weworksso.com	WeWork SSO Portal	CONFIRMED
centerspacesso.com	CenterSpace SSO Portal	CONFIRMED
cnainsurancesso.com	CNA Insurance SSO Portal	CONFIRMED
mycoldwellsso.com	Coldwell Banker SSO Portal	CONFIRMED



myadyensso.com

Did you intend to search across the file corpus instead? **Click here**

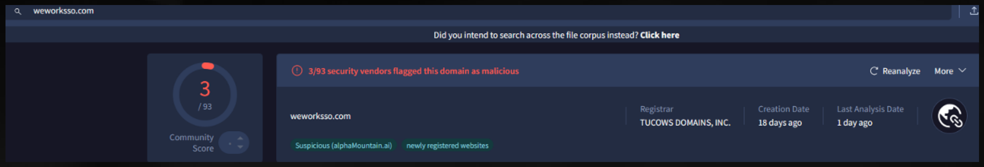
1 / 93

1/93 security vendor flagged this domain as malicious

myadyensso.com

Suspicious (alphaMountain.ai)

Registrar: TUCOWS DOMAINS, INC.
Creation Date: 18 days ago
Last Analysis Date: 1 day ago



weworksso.com

Did you intend to search across the file corpus instead? **Click here**

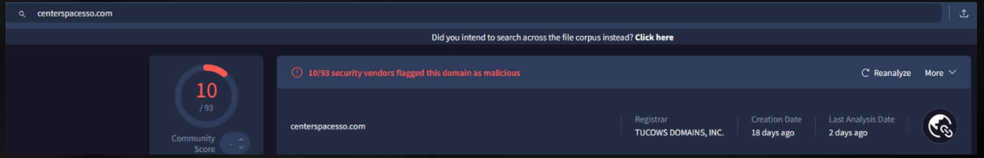
3 / 93

3/93 security vendors flagged this domain as malicious

weworksso.com

Suspicious (alphaMountain.ai)
newly registered websites

Registrar: TUCOWS DOMAINS, INC.
Creation Date: 18 days ago
Last Analysis Date: 1 day ago



centerspacesso.com

Did you intend to search across the file corpus instead? **Click here**

10 / 93

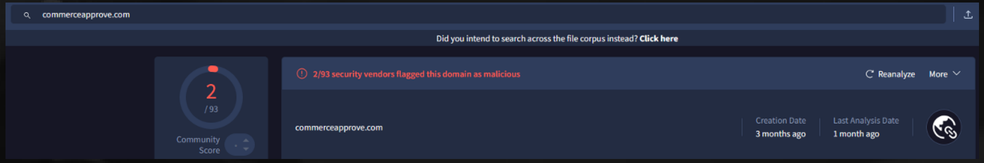
10/93 security vendors flagged this domain as malicious

centerspacesso.com

Registrar: TUCOWS DOMAINS, INC.
Creation Date: 18 days ago
Last Analysis Date: 2 days ago

C2 Domains

Domain	Purpose	Status
approvalmechanism.com	Second-stage payload / C2	CONFIRMED
commerceapprove.com	C2 / Exfiltration endpoint	CONFIRMED
technicalposition.com	Second-stage / C2	CONFIRMED



commerceapprove.com

Did you intend to search across the file corpus instead? **Click here**

2 / 93

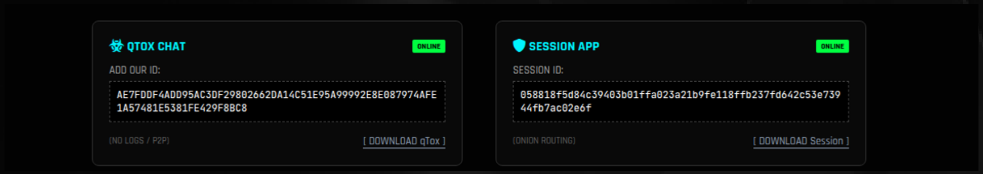
2/93 security vendors flagged this domain as malicious

commerceapprove.com

Creation Date: 3 months ago
Last Analysis Date: 1 month ago

Threat Actor Communication Channels

Platform	Identifier	Status
Tox Messenger	AE7FDDF4ADD95AC3DF29802662DA14C51E95A99992E8E087974AFE1A57481E5381FE429F8BC8	CONFIRMED
Session Messenger	058818f5d84c39403b01ffa023a21b9fe118ffb237fd642c53e73944fb7ac02e6f	CONFIRMED



ADD OUR ID:

```
AE7FDDF4ADD95AC3DF29802662DA14C51E95A99992E8E087974AFE
1A57481E5381FE429F8BC8
```

(NO LOGS / P2P)

SESSION ID:

```
058818f5d84c39403b01ffa023a21b9fe118ffb237fd642c53e739
44fb7ac02e6f
```

(ONION ROUTING)

Artifact Type	Value	Status
Ransom Note Filename	HOW TO RESTORE YOUR FILES.TXT	CONFIRMED
Suspicious Process Name	svcHost.exe (unusual path)	OBSERVED
File Extension	None (files retain original names)	CONFIRMED
Shadow Copy Deletion	vssadmin delete shadows /all /quiet	CONFIRMED

Detection & Mitigation Recommendations

Crystal Eye 5.5 (Red Piranha)

1. Secure external access (RDP/VPN + apps): Enforce MFA on RDP/VPN, patch exposed apps, block legacy protocols, and apply WAF rules to catch auth bypass / API abuse / injection attempts.
2. Privilege management: Rotate admin/MSP credentials, disable unused accounts, enforce least privilege for service accounts (web apps + DB), and monitor privilege escalation inside CE SIEM.
3. Execution control + kill-chain correlation: Use CEASR to block unknown binaries executing from %TEMP% / %APPDATA%, restrict PsExec/WMI remoting, and correlate ransomware chains like bcdedit + vssadmin + PsExec, including alerts for AV/service stops.
4. Network controls + segmentation: Block known C2/IP/domain indicators, restrict outbound HTTPS to unknown IPs, limit SMB/WinRM east-west movement, isolate admin workstations, and segment AD / file servers / DB servers / critical infra from general user networks.
5. Backup hardening + IR playbook automation: Use offline/immutable backups, restrict backup server access, detect shadow-copy deletion attempts, validate restores periodically, and trigger rapid SOAR actions (isolate hosts, block hashes/onion/IOCs, rotate credentials, notify SOC).

Worldwide Ransomware Victims

The United States remained the primary hotspot for ransomware activity, accounting for 42.65% of all identified victims. That means well over two out of every five known cases this period hit U.S. based organisations, keeping it far ahead of any other single country in terms of observable exposure.

A strong second tier consisted of the United Kingdom (8.06%) and Canada (5.69%), followed by Italy and India (each 3.32%), Brazil (2.84%), and Spain and Germany (each 2.37%). Together, this bloc of mature and large economies forms the bulk of non-U.S. activity, reflecting big digital footprints, consistent incident disclosure, and attractive victim profiles for extortion operators.

A broader mid-band followed, led by Malaysia (1.9%), and a cluster of countries at 1.42% each - Switzerland, Taiwan, Netherlands, Czech Republic, South Africa, Japan, New Zealand, Mexico, France. These figures show that ransomware is firmly entrenched across Europe, Asia-Pacific, and the Americas, not just in North America.

Below that, a long tail of lower-volume geographies - including Vietnam, China, Israel, Bulgaria, Thailand (each 0.95%), and a wide spread of Morocco, Tanzania, Peru, Slovenia, Colombia, Kenya, Philippines, Finland, Senegal, United Arab Emirates, Singapore, Bahamas, Mauritius, Australia, Argentina, Paraguay, Belgium, Chile, Slovakia, Indonesia, Greece (each 0.47%) appeared only sporadically. Individually they contribute small fractions, but collectively they reinforce the pattern: ransomware remains a global problem, touching dozens of countries rather than being confined to a handful of headline markets.

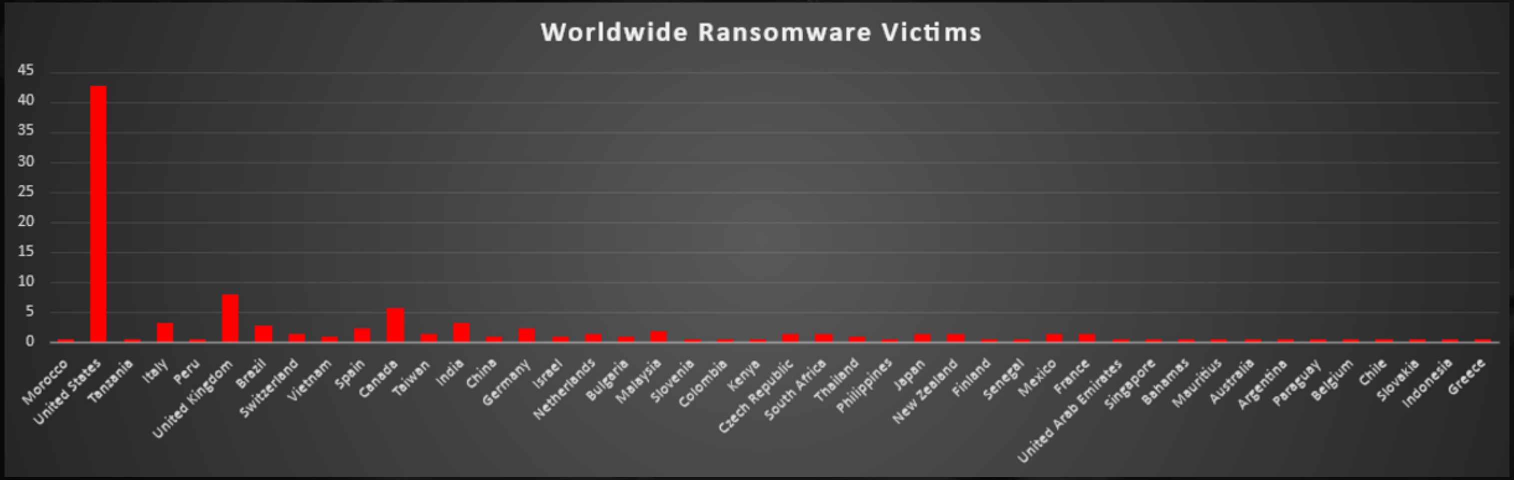


Figure 8: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing was once again the most heavily targeted sector, accounting for 21.33% of all identified ransomware victims. That puts production environments and supply-chain–critical operations clearly at the top of the risk ladder, where even short outages immediately translate into lost revenue and strong leverage for extortion.

A strong second tier consisted of Construction (11.85%), Business Services (11.37%), and Retail (10.9%). Together, these project-driven, service-oriented and customer-facing industries form a large concentration of cases, reflecting their reliance on time-sensitive projects, logistics, and payment flows that attackers routinely weaponise to force quick decisions under pressure.

A broad mid-band followed, led by Healthcare and Hospitality (each 4.74%), Finance (4.27%), Law Firms and Media & Internet (each 3.79%), along with Education (3.32%), and IT, Transportation (each 2.84%). Supporting this layer, Federal entities and Insurance (each 2.37%), plus Organisations, Consumer Services, and Electronics (each 1.9%), show that both public-sector bodies and information-rich commercial verticals are now routine fixtures in leak-site data rather than exceptions.

Lower-volume but still active categories included Real Estate, Agriculture, and Energy (each 0.95%), with Telecommunications and Minerals & Mining (each 0.47%) forming the long tail. Individually small but collectively meaningful, this spread underlines the same pattern seen across previous weeks: ransomware pressure is highly diversified across industries, and any organisation with digitised operations and monetisable data sits somewhere inside this threat surface.

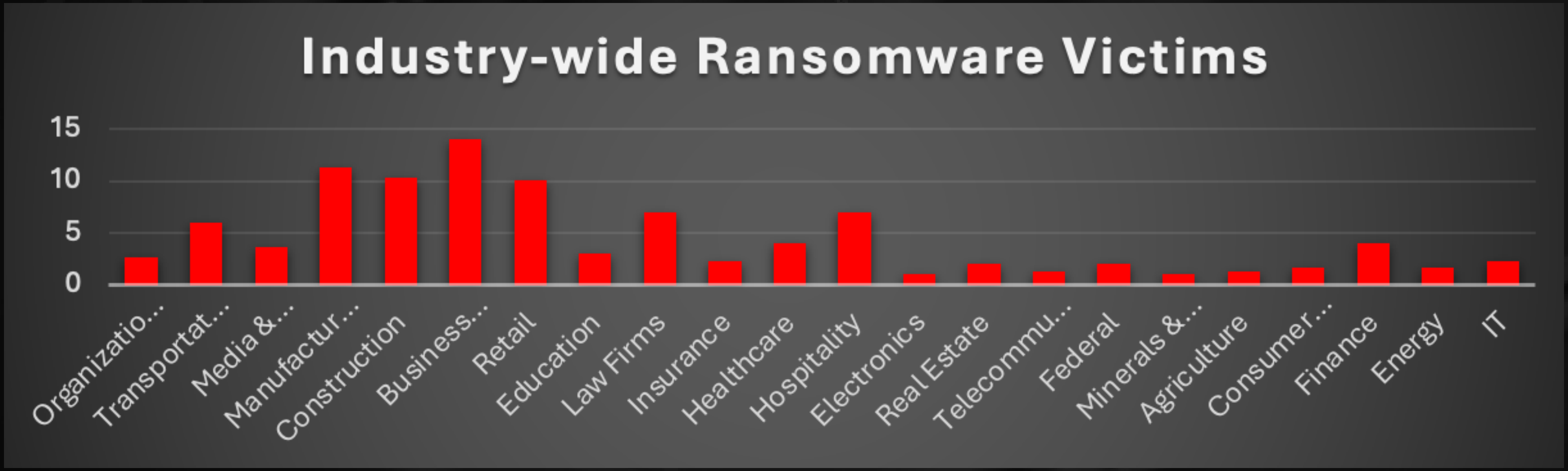


Figure 9: Industry-wide Ransomware Victims