Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 18 - 24, 2025

Report Summary:

- **New Threat Detection Added**
  - SilentSync
  - OtterCookie
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 100**
  - **Newly Detected Threats - 7**

The following threats were added to Crystal Eye this week:

1. SilentSync

SilentSync is a RAT (Remote Access Tool) that is delivered via malicious python packages. SilentSync has the ability to steal credentials, capture the users' screens, and because it communicates with a C2 server, it can receive commands to execute and exfiltrate the data it's captured. It also maintains persistence on the user's device by registering a registry entry. SilentSync has the capabilities to affect Windows, Linux, and MacOS systems.

Threats Protected: 4
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
Initial Access	T1195	Supply Chain Compromise
Execution	T1059.006	Command and Scripting Interpreter: Python
Persistence	T1112	Modify Registry
Collection	T1119	Automated Collection
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

2. OtterCookie

OtterCookie is a trojan developed by North Korean threat actors. The malware is distributed via phishing targeting developers and people in the finance sector. People are tricked into running a chess program that downloads and executes the OtterCookie malware. The malware captures keystroke, clipboard, and captures the screen which is needed to steal financial and other information. The malware also maintains persistence via registry and connects to the C2 server.

Threats Protected: 2
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
Initial Access	T1566	Phishing
Execute	T1204	User Execution
Persistence	T1112	Modify Registry
Collection	T1119	Automated Collection
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

Current Threat Summary

Known exploited vulnerabilities (Week 3 November2025)

Vulnerability	CVSS	Description
CVE-2025-61757	9.8	Oracle Fusion Middleware contains an authentication bypass vulnerability that can allow a remote unauthenticated attacker to send HTTP requests to the REST API endpoints without authentication, exploitation of this vulnerability can result in an attacker executing code and gaining access to the system.
CVE-2025-12480	8.8	Google Chromium contains a type of confusion vulnerability in the V8 component of the browser that can result in heap corruption upon visiting specially crafted HTML page.
CVE-2025-58034	6.7	Fortinet FortiWeb contains a command injection vulnerability that can allow a remote authenticated attacker to execute operating system commands on the system. This vulnerability when combined with the recent authentication bypass via path traversal vulnerability (CVE-2025-64446) can result in an unauthenticated attacker gaining full access to the system.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-november-2025/619

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

Clop dominated this week's ransomware activity, responsible for 39.27% of all reported incidents. This overwhelming spike reflects a large-scale coordinated campaign or a mass dump of victim disclosures, placing Clop far ahead of every other active threat actor in the ecosystem.

Akira (13.09%) and Qilin (9.42%) followed as the next major contributors, forming a strong second tier. Both groups continued sustained, multi-industry targeting, leveraging high-volume data theft and opportunistic intrusions across multiple regions.

A mid-tier cluster included Inc Ransom (4.71%), Sinobi (4.71%), Medusa (3.66%), Play (3.14%), Everest (2.62%), RansomHouse (2.09%), DevMan2 (2.09%), and DragonForce (2.09%), each maintaining steady operational tempo and consistent victim disclosures. Additional notable actors such as Pear (1.57%), Coinbase Cartel (1.57%), Rhysida (1.05%), and Sarcoma (1.05%) contributed to diversified mid-level activity.

Smaller but active operators — Nova, Anubis, Morpheus, Nightspire, MyData, Crypto24, Ransomware Blog, Lynx (each 0.52–1.05%) — continued to appear in lower volumes but maintained presence across sectors, supporting the persistent background noise of ransomware operations.

A wide range of fringe groups each accounted for 0.52% of total incidents, including Brotherhood, KillSec3, Handala, 3AM, Datacarry, BlackShrantac, and others. While individually minor, their collective activity underscores the fragmentation, churn, and long-tail resilience of the ransomware ecosystem.

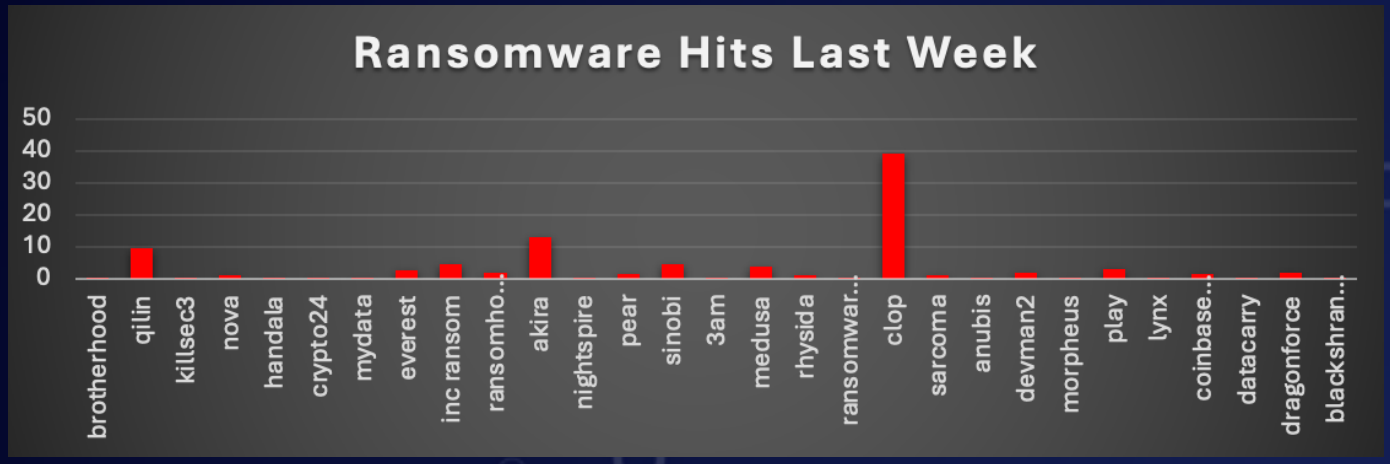

Figure 1: Ransomware Group Hits Last Week

Crypto24 Ransomware

The Red Piranha threat intelligence team continues to track ransomware operators across leak sites, dark-web forums, and open-source feeds. During recent weeks, Crypto24 has emerged as a technically sophisticated double-extortion operator targeting large enterprises across Asia, Europe, and North America.

Crypto24 primarily goes after financial services, manufacturing, entertainment, technology and healthcare organisations with substantial data assets and low tolerance for downtime. Attacks are typically staged during nights/weekends and combine "living off the land" with custom EDR-bypass malware, stealthy data theft and then wide-scale encryption using the ".crypto24" extension and "Decryption.txt" ransom note.

Detailed TTPs (Narrative View)
Below is a compact, operator-centric view of Crypto24's attack flow:

1. External Footprinting & Target Selection
   - Scan for exposed RDP/VPN and other remote admin services.
   - Prioritise enterprises with large data footprint and visible OT/ERP/backup infrastructure.
2. Initial Access – Valid Accounts & Remote Services
   - Use compromised, purchased or recycled credentials to log into RDP/VPN.
   - Reactivate default or dormant admin accounts to avoid noisy brute-force.
3. Foothold Stabilisation & Persistence
   - Create/enable local admin users with innocuous names and add them to Administrators/Remote Desktop Users.
   - Deploy malicious services (e.g. WinMainSvc, MSRuntime) running under svchost.exe to load keylogger and loaders on boot.
   - Set scheduled tasks pointing to scripts in %ProgramData%\Update\ to guarantee execution even after partial cleanup.
4. Privilege Escalation & Lateral Movement
   - Escalate via UAC bypass (CMSTPLUA interface), runas.exe, and PsExec with stolen admin credentials.
   - Enable and harden RDP for operator use (patch termsrv.dll for multiple sessions, add RDP users, relax restrictions).
5. Defence Evasion & EDR Bypass
   - Run RealBlindingEDR to kill/cripple AV/EDR drivers and tamper with hooks.
   - Abuse gpscript.exe (signed binary) to invoke vendor uninstallers (e.g. Trend Micro agent remover) and remove endpoint protection.
   - Masquerade malware as "Microsoft Runtime Manager" or similar benign-sounding services; aggressively delete logs and self-remove payloads post-encryption.
6. Credential Access & Monitoring
   - Load WinMainSvc.dll as a service to record keystrokes (including control keys).
   - Harvest credentials for domain admins, backup systems, and critical line-of-business apps, enabling further lateral movement and future re-entry.
7. Discovery & Environment Mapping
   - Use WMIC and batch scripts (e.g. 1.bat) to dump OS version, hardware, disks, processes, and services.
   - Enumerate users and groups via net user / net localgroup.
   - Probe reachable hosts and shares to identify file servers, databases, backup targets and high-value data.
8. Data Collection & Exfiltration (Double-Extortion Setup)
   - Aggregate sensitive data (DB dumps, file shares, documentation) into staging paths.
   - Use Google Drive API or similar cloud services for exfiltration, hiding in normal HTTPS SaaS traffic.
   - In some cases, hundreds of GB of data are uploaded before any encryption begins.
9. Pre-Encryption Kill Chain & Tool Removal
   - Kill database, backup and high-lock processes to ensure maximum encryption coverage.
   - Stop or uninstall security agents and scheduled backups where possible.
10. Ransomware Deployment & Impact
    - Launch the Crypto24 encryptor across key systems, typically from already-persistent services or PsExec.
    - Append ".crypto24" to encrypted files and drop "Decryption.txt" ransom notes across directories.
    - Direct victims to contact addresses and a Tor leak site; threaten data dumps if payment is refused.

MITRE ATT&CK TTPs:

Tactic	Technique (ID)	Notes / Crypto24 Use
Initial Access	External Remote Services (T1133)	RDP/VPN access with stolen/dormant credentials to directly enter internal network.
	Valid Accounts (T1078)	Reactivates default admin accounts; creates new admins for stealthy, persistent access.
Execution	Command & Scripting Interpreter – Windows CMD (T1059.003)	Batch scripts (*.bat) used for recon, tooling deployment and task automation.
Persistence	Create Account (T1136) / Account Manipulation (T1098)	New local/domain accounts added to privileged groups.
	Windows Service (T1543.003)	Services like WinMainSvc and MSRuntime under svchost.exe to load keylogger/ransomware.
	Scheduled Task/Job (T1053)	Recurring tasks in %ProgramData%\Update\ executing scripts and loaders.
Privilege Escalation	Bypass UAC (T1548.002)	CMSTPLUA COM UAC bypass to silently elevate processes.
	Valid Accounts (T1078)	Elevated access via stolen domain admin credentials and created admin users.
Defence Evasion	Impair Defences – Disable Security Tools (T1562.001)	RealBlindingEDR disables AV/EDR and Defender drivers.
	Masquerading – Valid Service Name (T1036.004)	Pseudo-legit names like “Microsoft Runtime Manager” and services bound to svchost.exe.
	Signed Binary Proxy Execution (T1218)	gpscript.exe abused to run uninstaller for security agents.
	Indicator Removal on Host (T1070)	Cleans logs, removes artifacts, and self-deletes ransomware binaries post-impact.
Credential Access	Keylogging (T1056.001)	WinMainSvc.dll records keystrokes and credential input.
Discovery	System Information Discovery (T1082)	WMIC and scripts gather OS/hardware/process info.
	Account Discovery (T1087)	net user and net localgroup to map users and groups.
Lateral Movement	Remote Services – RDP (T1021.001)	Enables and abuses RDP for lateral admin sessions.
	Remote Services – SMB/Admin Shares (T1021.002)	PsExec over admin$ shares for remote command execution.
Collection	Input Capture (T1056) / Data from Local System (T1005)	Keylogging and file staging prior to exfiltration.
Exfiltration	Exfiltration Over Web Service – Cloud Storage (T1567.002)	Google Drive API leveraged to upload stolen archives and logs.
Command-and-Control	Encrypted/Remote Access Tools (T1573/T1572)	AnyDesk/VNC-style remote control for interactive operations.
Impact	Data Encrypted for Impact (T1486)	.crypto24 encryption at scale; critical services killed first.
	Data Theft & Leak (TA0040 / T1485)	Double-extortion via Tor leak site and direct leak threats.

Indicators of Compromise (IoCs)

File extension: crypto24 on encrypted files.
crypto24support@pm.me
noreply@crypto24lab.com
Historical / earlier variant: haowieo2839@proton.me
http://j5o5y2feotmhvr7cbcp2j2ewayv5mn5zenl3joqwx67gtfchhezjznad.onion/
http://j5o5y2feotmhvr7cbcp2j2ewayv5mn5zenl3joqwx67gtfchhezjznad.onion:5050/data

Domains Linked to Campaigns
palmgold-mgmt[.]com
cms[.]law/en/int/
karndean[.]com
soubeiranchobet[.]com[.]ar
larimart[.]it
arianadx[.]com
NOTE: Some are victim websites. Use them primarily as pivot points for historical investigation.

Mitigations – Crystal Eye XDR 5.5

- Lock down RDP/VPN
  Only allow RDP over VPN, enforce MFA on all admin/VPN accounts, and geo-block/ACL access to known management IPs.
- Control admin accounts hard
  Disable default/dormant admins, review local/domain admin groups regularly, and alert on any new privileged account creation.
- Block EDR tampering and LOLBins
  Use CEASR / app-control to block gpscript.exe, PsExec and unknown binaries from %ProgramData% and temp paths; alert on AV/EDR service stops/uninstalls.
- Segment and isolate critical assets
  Put DCs, file servers, DBs and backup servers in separate zones; restrict SMB/RDP laterals between segments to only what's absolutely required.
- Protect backups from ransomware
  Keep backups in isolated networks or immutable storage; no interactive logon, no direct RDP/SMB from user LAN; regularly test restores.
- Monitor exfil and Tor/cloud abuse
  Use SWG/SIEM to detect large HTTPS uploads (Google Drive, etc.) from servers; block Tor traffic and alert on any attempt to reach .onion gateways.
- Harden endpoints and logging
  Enforce Defender/EDR tamper protection, block shadow copy deletion (vssadmin, wmic patterns), and enable forensic logging/PCAP on key servers.
- Have a Crypto24-style IR playbook ready
  On detection: isolate hosts via CE, push IoC blocklists (hashes, IPs, emails), rotate privileged creds, and restore only after re-hardening and clean verification.

Worldwide Ransomware Victims

The United States accounted for 55.5% of all reported ransomware victims this week, maintaining an overwhelming lead as the most targeted nation globally. This reflects sustained large-scale campaigns against U.S. enterprises, critical services, and high-value sectors that continue to offer attackers strong financial leverage.

Canada (5.24%) and Mexico (2.62%) followed as significant regional hotspots, highlighting an extended concentration of activity across North America. Japan (2.62%) and the United Kingdom (2.09%) also registered elevated targeting, reinforcing continued adversary pressure on major G7 economies.

A broad mid-tier cluster included India (3.14%), Australia (1.57%), Thailand (1.57%), Sweden (1.57%), Brazil (1.57%), Switzerland (1.57%), and Saudi Arabia (1.57%)—each showing consistent victimisation across critical and commercial sectors. Additional nations such as France (1.05%), Italy (1.05%), Germany (1.05%), South Korea (1.05%), Malaysia (1.05%), United Arab Emirates (1.05%), Sri Lanka (1.05%), Kuwait (1.05%), and Pakistan (1.05%) reflected distributed targeting across Europe, the Middle East, and Asia.

Smaller but meaningful single-incident activity appeared across Barbados, Bolivia, Ireland, China, Netherlands, Oman, Peru, Portugal, Singapore, Slovenia, Uruguay, Colombia, Trinidad & Tobago, Réunion, IGT, and others. Though individually limited, these events underscore the wide geographic scatter of modern ransomware operations.

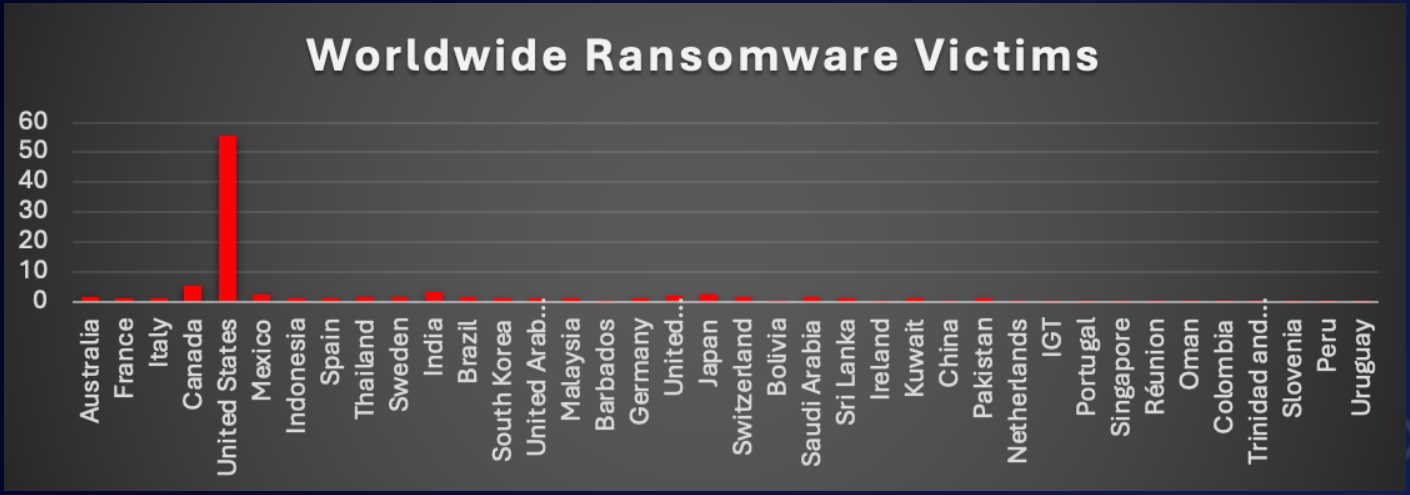

Figure 5: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing remained the most heavily targeted sector this week, accounting for 19.37% of all reported ransomware incidents. Its dependency on legacy systems, operational technology, and continuous uptime makes it one of the most profitable and easily disrupted verticals for attackers.

Business Services (13.09%) and Retail (9.95%) followed as major hotspots, reflecting ongoing exploitation of service-driven enterprises and customer-facing infrastructures. Construction (8.9%) and Energy (7.85%) also endured sustained pressure, with their complex supply chains and critical operations providing strong leverage for extortion.

A solid mid-tier cluster included Education (5.24%), Hospitality (3.66%), Finance (3.66%), IT (3.66%), Consumer Services (3.14%), Real Estate (3.14%), and Federal entities (3.14%)—each showing consistent targeting across diverse geographies and operational models.

Lower-volume but active sectors such as Transportation (2.62%), Electronics (2.62%), Law Firms (2.09%), Insurance (2.09%), Agriculture (1.57%), Telecommunications (1.57%), and Minerals & Mining (1.05%) continued to appear across the mid-lower tier, reflecting ransomware's wide operational reach.

A small set of fringe-activity industries—including Healthcare, Media & Internet, and Organisations (each 0.52%)—rounded out the dataset. While individually limited, these incidents reinforce ransomware's opportunistic nature, where even less-targeted verticals are not immune from exploitation.

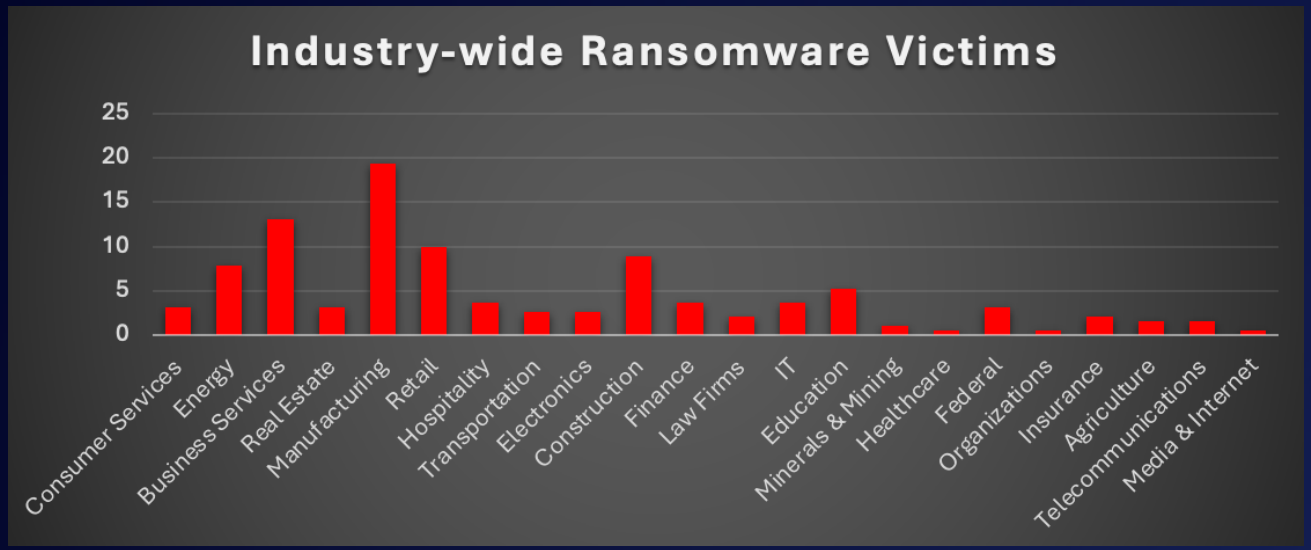

Figure 6: Industry-wide Ransomware Victims