Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Mar 18 - 24, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - TinyShell Backdoor
  - Land Update808 Fake Update
- **New Threat Protections - 174**

The following threats were added to Crystal Eye this week:

1. TinyShell Backdoor

UNC3886 is a sophisticated China-nexus cyber espionage group known for exploiting zero-day vulnerabilities to infiltrate network devices and virtualisation technologies. In mid-2024, they deployed custom backdoors on Juniper Networks' Junos OS routers, particularly targeting end-of-life hardware and software. The malware included TINYSHELL-based backdoors with both active and passive functionalities, along with scripts designed to disable logging mechanisms, facilitating stealthy and persistent access.

Threat Protected: 04
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
Persistence	T1505.003	Server Software Component: Web Shell
Defence Evasion	T1562.001	Impair Defences: Disable or Modify Tools
Credential Access	T1552.001	Unsecured Credentials: Credentials In Files
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

2. LandUpdate808 Fake Update

LandUpdate808 is a recently identified fake update malware variant that employs deceptive tactics to trick users into downloading malicious payloads. Unlike other fake update schemes, such as SocGholish, LandUpdate808 exhibits unique characteristics in its delivery chain and payload distribution. The malware operates through the following stages:

- Initial Compromise: Attackers inject malicious JavaScript into compromised legitimate websites.
- User Redirection: Visitors to these compromised sites are redirected to a fake update page designed to resemble legitimate software update prompts.
- Malicious Payload Delivery: Users are prompted to download an "update" file, which has been observed in various formats, including .js, .exe, and .msix. The naming convention typically follows the pattern: update_DD_MM_YYYY_#######.
- Payload Execution: Upon execution, the malicious payload establishes a foothold on the victim's system, potentially leading to further compromise or data exfiltration.

This variant's delivery chain has evolved over time, with changes in the endpoints and methods used to serve the fake update content. Notably, the initial stage previously utilised /p/land.php and has transitioned to using a remote js.php resource. Additionally, the final payload delivery path shifted from /wp-content/uploads/update.php to /wp-includes/pomo/update.php.

Threat Protected: 22
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.007	Command and Scripting Interpreter: JavaScript
Persistence	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder
Defence Evasion	T1027	Obfuscated Files or Information
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

Known exploited vulnerabilities (Week 3 March 2025):

Vulnerability	CVSS	Description
CVE-2025-30066	8.6 (High)	tj-actions/changed-files GitHub Action Embedded Malicious Code Vulnerability
CVE-2025-24472	9.8 (Critical)	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability
CVE-2017-12637	7.5 (High)	SAP NetWeaver Directory Traversal Vulnerability
CVE-2024-48248	8.6 (High)	NAKIVO Backup and Replication Absolute Path Traversal Vulnerability
CVE-2025-1316	9.3 (Critical)	Edimax IC-7100 IP Camera OS Command Injection Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-march-2025/556

Updated Malware Signatures (Week 3 March 2025)

Threat	Description
Lumma Stealer	A type of malware classified as an information stealer. Its primary purpose is to steal sensitive information from infected systems, including but not limited to credentials, financial information, browser data, and potentially other personal or confidential information.
AsyncRAT	A remote administration tool that was originally marketed as an open-source tool for legitimate remote system administration. However, it's often used for malicious purposes by cybercriminals due to its powerful features and stealthy behaviour.
XWorm	A Remote Access Trojan (RAT) and malware loader that's commonly used in cyberattacks to give attackers full remote control over a victim's system. It's part of a growing trend of commercialised malware sold or rented on dark web forums, often under the guise of a "legitimate tool."

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 Groups	Overall Percentage of total attack coverage
FunkSec	0.91%
Qilin	4.55%
Babuk-Bjorka	27.27%
Abyss-Data	0.45%
Stormous	6.36%
Leaked Data	8.64%
Hellcat	0.91%
RansomHub	12.27%
Crazy Hunter Team	0.45%
Orca	0.45%
Termite	0.45%
Trinity	0.91%
Hunters	1.82%
Inc ransom	3.18%
Sarcoma	0.45%
Nightspire	3.18%
Akira	5.45%
Fog	0.91%
VanHelsing	1.36%
Cactus	3.64%
Apos	0.45%
SafePay	0.91%
Lynx	0.91%
KillSec3	2.27%
Monti	0.91%
Arcus Media	1.36%
Rhysida	0.45%
Play	0.45%
Space Bears	0.91%
Cloak	2.27%
DragonForce	0.45%
Medusa	3.18%
Blackout	0.45%
Anubis	0.45%
BlackSuit	0.45%
Interlock	0.45%

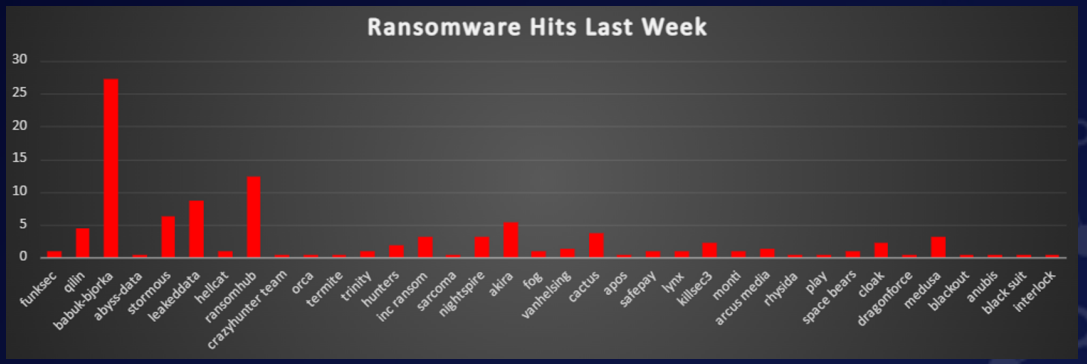
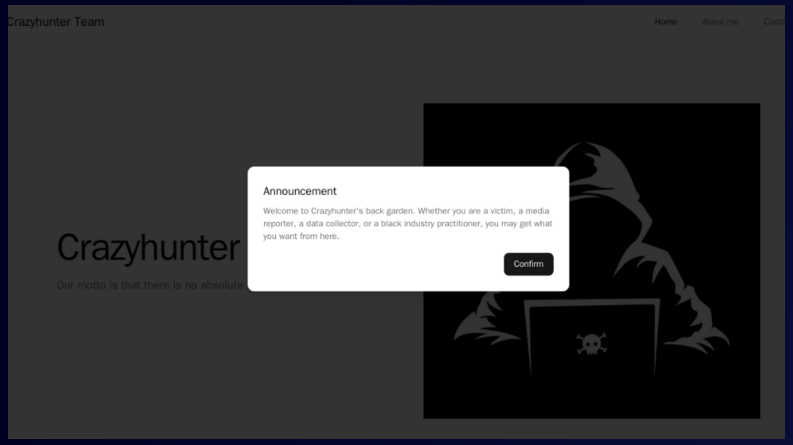


Figure 1: Ransomware Group Hits Last Week

Crazy Hunter Ransomware

Attackers infiltrated the target's network via Active Directory (AD) misconfigurations, leveraging Bring-Your-Own-Vulnerable-Driver (BYOVD) techniques to escalate privileges and ultimately distribute ransomware through Group Policy Objects (GPOs). This resulted in significant operational disruption and triggered an emergency response from relevant authorities.

Red Piranha has been tracking Crazy Hunter, monitoring domains associated with this campaign—such as tianyinsoft[.]top—to detect and block malicious activities. Our proactive threat intelligence enabled early identification of the infrastructure used by the attackers, demonstrating the importance of real-time intelligence to thwart ransomware before it spreads.



Detailed TTPs

Attack Progression:

- Initial Access: Exploitation of weak passwords and AD misconfigurations allowed attackers to gain entry.
- Privilege Escalation: BYOVD techniques, including the use of a modified Zemana driver, bypassed security measures.
- Lateral Movement & Encryption: Malware was deployed via GPOs, encrypting critical target systems.
- Extortion: Despite claims of data exfiltration, forensic analysis found no evidence to support these assertions.

Below is a summary of the tactics, techniques, and procedures (TTPs) used by the attackers, aligned with the MITRE ATT&CK framework:

Tactic (ID)	Technique	Technique ID	Description
Initial Access (TA0001)	Valid Accounts - Domain Accounts	T1078.002	Exploited weak passwords to compromise AD accounts.
	Phishing	T1566	Potential initial access vector, though not definitively confirmed in this instance.
Execution (TA0002)	User Execution - Malicious File	T1204.002	Executed the ransomware payload after gaining initial access.
Persistence (TA0003)	Domain Policy Modification	T1484.001	Leveraged SharpGPOAbuse to deploy malware via Group Policy Objects (GPOs).
Privilege Escalation (TA0004)	Exploitation for Privilege Escalation	T1068	Utilised BYOVD with a modified Zemana driver to bypass security controls.
Defence Evasion (TA0005)	Code Signing	T1553.002	Signed malicious drivers to avoid detection.
	Masquerading	T1036	Disguised ransomware as a legitimate process.
Credential Access (TA0006)	Credential Dumping	T1003	Likely extracted credentials to facilitate lateral movement within the network.
Discovery (TA0007)	Remote System Discovery	T1018	Identified accessible systems to expand the attack.
Lateral Movement (TA0008)	Remote Services	T1021	Propagated the ransomware using compromised AD credentials and GPOs.
Impact (TA0040)	Data Encrypted for Impact	T1486	Encrypted over 600 target systems, severely disrupting operations.
	Data Destruction	T1485	Possibly deleted backups or logs to complicate recovery efforts.
	Network Denial of Service	T1498	Disrupted operations by causing network service outages over several days.
Command-and-Control (TA0011)	Application Layer Protocol	T1071	Connected to tianyinsoft[.]top for C2 communication.

IOCs (Indicators of Compromise)

- Domains:
  - tianyinsoft[.]top (Confirmed C2 domain)
  - ncmep[.]org (Observed DNS lookup, likely a connectivity check)

- IP Addresses:
  - 163.181.22.245
  - 139.9.248.128
  - 163.181.22.246
  - 82.157.38.90
  - 8.130.41.80
  - 139.9.248.128
  - 47.246.44.248

MD5: 34afc7a3496ba4c9b6080a24c0db88ac
SHA1: 98ce84bebe5551e3d79d2e8cd4a19bed4535a060
SHA256: 2e835677929cb3bc3334e530c08e528858502c02585e7763db502f01190bc84b
IMPHASH: 2d18cdf9c43ac1ee575cac6663a8fb17
PEHASH: 60db50efc129f75eeb0ec1a0316a465f8a54d37e

Onion URL:
http://7i6sfmfvmqfaabjksckwrttu3nsbopl3xev2vbxbkghsivs5lqp4yeqd.onion/

Mitigations

1. Harden Active Directory
   - Implement strong password policies and multi-factor authentication (MFA).
   - Conduct regular audits of GPO configurations and monitor for unusual modifications.
   - Minimise unnecessary permissions within AD to reduce the attack surface.
2. Implement Network Segmentation
   - Isolate critical target systems from general and administrative networks.
   - Use micro-segmentation to contain lateral movement within the network.
3. Prevent BYOVD Exploits
   - Maintain a rigorous patching schedule for operating systems and drivers.
   - Deploy endpoint detection solutions capable of identifying and blocking known vulnerable drivers.

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States remains the most heavily impacted nation, accounting for approximately 45.4% of global incidents. This dominant share underscores its persistent vulnerability to ransomware threats.

Following the United States, Canada emerges as the second most targeted region with about 8.8% of reported cases. The United Kingdom and China also face significant exposure, contributing roughly 5.6% and 4.2% of global incidents respectively.

Other nations have also experienced considerable ransomware activity. France accounts for around 3.7%, while India represents about 3.2% of total cases. Both Spain and Germany contribute approximately 2.8% each, and Australia registers close to 2.3%.

Smaller yet noteworthy percentages are observed in countries like Thailand (1.9%), along with several nations—including Chile, Italy, Brazil, Indonesia, Iraq, and Malaysia—all hovering between 1.4% and 1.9% of global incidents. Numerous other countries contribute marginally, reinforcing the widespread and global nature of ransomware threats.

This analysis highlights that while North America continues to bear the brunt of ransomware attacks, significant activity is also occurring in other regions. The findings call for robust cybersecurity frameworks, proactive defences, and heightened vigilance across all nations to combat this evolving threat.

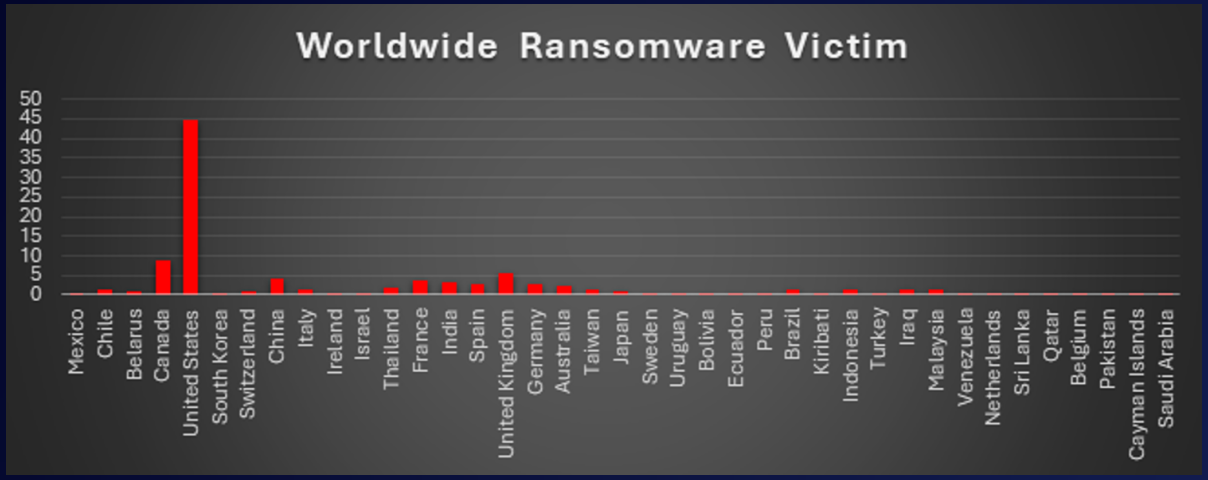


Figure 3: Ransomware Victims Worldwide

Ransomware Victims by Industry

A recent ransomware analysis reveals that the Business Services sector is the most targeted industry, accounting for approximately 16.5% of all reported incidents. This alarming figure emphasises the severe risks facing service-oriented organisations in today's threat landscape.

Close behind is the Manufacturing sector, representing about 15.1% of global ransomware cases. This highlights vulnerabilities within production processes and the broader supply chain, which cybercriminals continue to exploit.

The Retail industry accounts for roughly 8.3% of incidents, while Federal entities contribute around 7.3%, reflecting the heightened risk in governmental infrastructures. In addition, sectors such as Education, Telecommunications, and Law Firms each report about 5.5% of total incidents, indicating substantial exposure across these critical fields.

Both the Healthcare and Finance industries follow closely, each with nearly 4.6% of incidents, underscoring the ongoing challenges in safeguarding sensitive information. Other sectors, including Construction (4.1%), Real Estate (3.7%), and both IT and general Organisations (each at 3.2%), have also seen notable ransomware activity.

Moderate targeting is evident in Consumer Services (2.3%) and Transportation (1.4%). Meanwhile, sectors such as Insurance, Energy, Hospitality, and Media & Internet each account for about 1.8% of incidents, and both Building Materials and Minerals & Mining contribute around 0.9%.

This detailed industry analysis underscores the pervasive and indiscriminate nature of ransomware attacks. It highlights the urgent need for tailored cybersecurity strategies, proactive defence measures, and continuous risk assessments across all industry sectors to mitigate the evolving threat landscape.

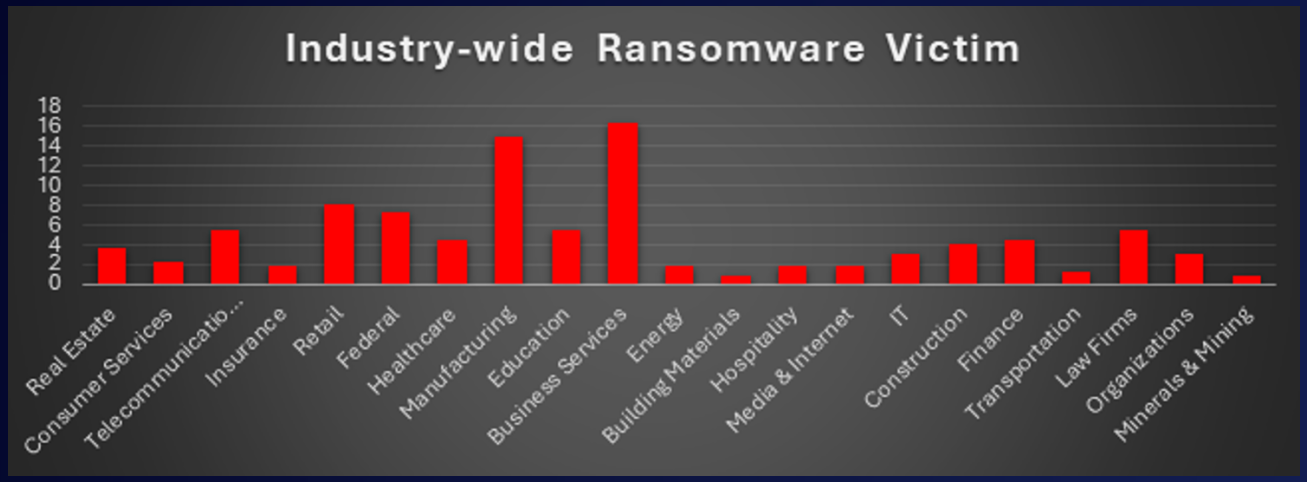


Figure 4: Industry-wide Ransomware Victims