Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

April 1 - 7, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - Kentico Xperience CMS Authentication Bypass (CVE-2025-2747)
  - Ivanti Connect Secure Buffer Overflow (CVE-2025-22457)

- **New Threat Protections - 133**

The following threats were added to Crystal Eye this week:

1. Kentico Xperience CMS Authentication Bypass CVE-2025-2747

This authentication bypass vulnerability affects Kentico Xperience CMS versions up to 13.0.178. This vulnerability allows a threat actor to bypass account authentication for the Xperience CMS through the Staging Sync Server component. This allows the threat actor to control administrative objects.

Threat Protected: 04
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1106	Exploitation of Remote Services
Credential Access	T1212	Exploitation for Credential Access

2. Ivanti Connect Secure Buffer Overflow (CVE-2025-22457)

This vulnerability allows remote code execution via a buffer overflow on Ivanti Connect Secure, Pulse Connect Secure, Ivanti Policy Secure and ZTA Gateway. Threat actors can exploit this vulnerability to gain unauthorised access to the network and it has been observed that malware has been distributed through this vulnerability.

Threat Protected: 01
Rule Set Type:

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

Class Type: Web-application-attack

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application

Known exploited vulnerabilities (Week 1 April 2025):

Vulnerability	CVSS	Description
CVE-2025-22457	9.0 (Critical)	Ivanti Connect Secure, Policy Secure and ZTA Gateways Stack-Based Buffer Overflow Vulnerability
CVE-2025-24813	9.8 (Critical)	Apache Tomcat Path Equivalence Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-april-2025/559

Updated Malware Signatures (Week 1 April 2025)

Threat	Description
zgRAT	Is a trojan, usually deployed via USB devices or phishing emails that target browser information (Saved Login Details) and cryptowallets.
XWorm	A Remote Access Trojan (RAT) and malware loader commonly used in cyberattacks to give attackers complete 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
RansomHub	2.89%
Interlock	2.31%
Inc ransom	1.73%
Babuk-Bjorka	17.34%
Qilin	10.4%
Lynx	2.89%
Sarcoma	1.73%
Hellcat	0.58%
Rhysida	1.16%
CrazyHunter Team	0.58%
Ralord	2.89%
SafePay	17.34%
KillSec3	12.72%
Bianlian	2.31%
Lockbit3.0	0.58%
Nitrogen	0.58%
Chaos	2.31%
Kairos	0.58%
Morpheus	0.58%
VanHelsing	1.16%
Anubis	0.58%
Abyss-Data	0.58%
NightSpire	3.47%
Everest	0.58%
Medusa	2.89%
Play	4.62%
Leaked Data	2.31%
Hunters	1.16%
Frag	0.58%
BlackSuit	0.58%

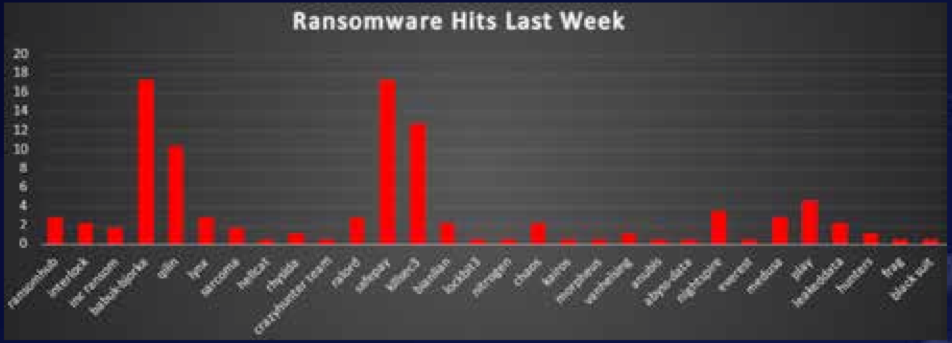


Figure 1: Ransomware Group Hits Last Week

LockBit3.0 Ransomware Group

LockBit3.0 continues to assert its dominance as one of the most prolific ransomware operations globally. Operating under the Ransomware-as-a-Service (RaaS) model, LockBit enables affiliates to launch attacks using the group's advanced encryption tools and infrastructure, allowing it to scale rapidly and efficiently. The group has been linked to nearly one-third of global ransomware attacks, with some estimates attributing 40% of all ransomware incidents to its affiliates.

A distinguishing feature of LockBit's ecosystem includes a professional dark web portal, a victim leak site, and the only known ransomware-affiliated bug bounty program. The threat actors behind LockBit have iterated their malware through multiple versions — LockBit Red (2.0), and LockBit Black (3.0), and are now testing encryptors for macOS, Linux, and even rare architectures like SPARC and MIPS.

Attack Chain Analysis

Initial Access
LockBit affiliates typically gain entry via compromised credentials from phishing, unpatched software, or brute-forcing RDP/VPN services. Reconnaissance and exploitation are automated using off-the-shelf tools or custom scripts.

Lateral Movement
After gaining a foothold, attackers use native Windows utilities like PsExec, WMI, and RDP to pivot across systems. Access tokens and credentials are harvested using tools such as Mimikatz.

Execution
The payload often includes PowerShell stagers or obfuscated binary droppers. Recent variants also utilise Safe Mode Boot execution and command-line parameters for stealth operations.

Defence Evasion
LockBit employs multiple evasion tactics:

- Encrypted payloads
- Process hollowing
- Use of signed binaries (LOLBAS)
- Environment-aware checks to avoid sandboxes

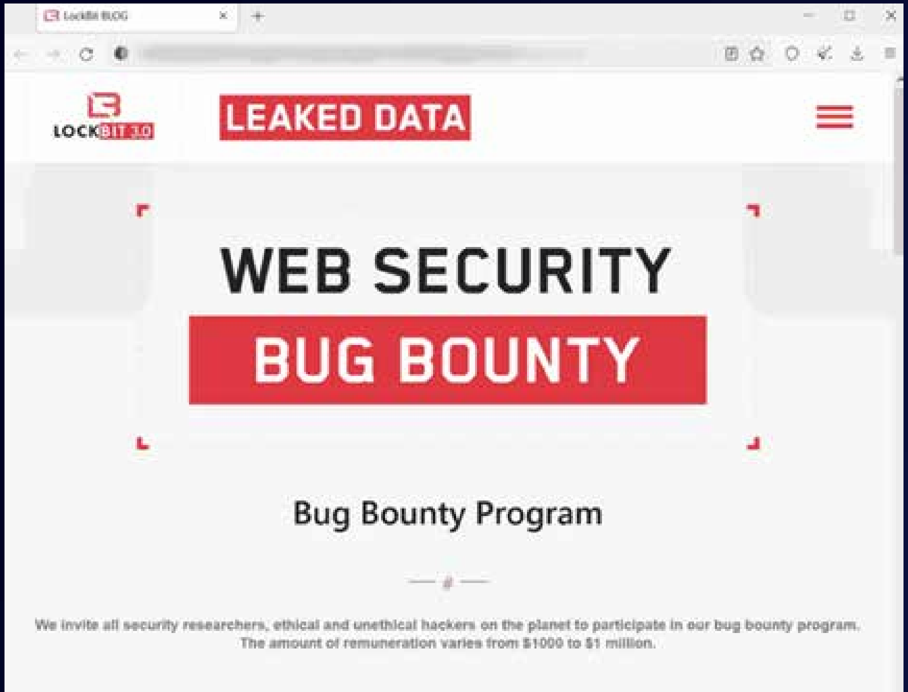
Data Exfiltration and Impact
Data is exfiltrated via C2 infrastructure or secure cloud storage before encryption. Upon failure to pay, victims' data is posted on LockBit's leak portals hosted on the Tor network.

Detailed TTPs

Stage	Tactic	Technique	Description
Initial Access	Valid Accounts (T1078)	Compromised VPN/RDP credentials	Gained access via brute-force or phishing credentials.
Execution	Command & Scripting (T1059)	PowerShell, Batch, WMI execution	Used for launching loaders, scripts, and ransomware binary.
Persistence	Boot or Logon AutoStart (T1547)	Safe Mode persistence	Reboots into Safe Mode to evade AVs before encryption.
Privilege Escalation	Exploitation for Privilege (T1068)	Custom exploits or LOLBins	Exploited system services or misconfigurations to elevate privileges.
Defence Evasion	Obfuscated Files/Info (T1027)	Encrypted & XOR payloads	Avoided detection by obfuscating code & using signed binaries.
Credential Access	Credential Dumping (T1003)	LSASS dumping via Mimikatz	Extracted hashes, tokens, and plaintext passwords.
Lateral Movement	Remote Services (T1021)	RDP, SMB, PsExec	Moved laterally using valid credentials and built-in tools.
Impact	Data Encrypted for Impact (T1486)	Ransomware payloads	Locked files using AES/RSA-based encryption.
Exfiltration	Exfiltration Over Web (T1041)	C2 channel or leak site staging	Uploaded data to attacker-controlled servers before encryption.

Mitigations Against LockBit Ransomware

- Harden External Interfaces
  Disable or strictly limit RDP and VPN exposure. Enforce strong passwords and MFA on all remote access points.
- Patch Management
  Regularly update software and operating systems to close known vulnerabilities, particularly those exploited in privilege escalation or lateral movement.
- Network Segmentation
  Implement VLANs or zero-trust architectures to limit lateral movement. Isolate backup systems entirely.
- Application Whitelisting & EDR/XDR
  Deploy next-gen AV/EDR solutions with behaviour-based detections. Use tools like AppLocker or WDAC to block unauthorised executables.
- Credential Protection
  Prevent credential theft by enforcing LSASS protections, disabling legacy protocols (e.g., SMBv1), and rotating domain admin passwords.



WEB SECURITY

BUG BOUNTY

Bug Bounty Program

We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program. The amount of remuneration varies from $1000 to $1 million.

IOCs

IP addresses

72.167.106.35
52.60.114.31
198.244.187.248
184.168.221.18
50.63.202.55
91.219.236.192
3.33.152.147
198.71.232.3
72.167.191.69
50.63.202.33
93.115.26.127
46.21.250.52
193.233.132.177
38.180.61.247
142.91.170.6
142.91.170.175
193.143.1.65
45.156.21.148
94.154.35.208
170.130.55.164

Domains

aapu.xyz
rinryesop.one
360nvidia.com
lockbitaptxxx.onion
user.group
accessservicesonline.com
retailadvertisingservices.com
user.compdatasystems.com
compdatasystems.com
lockbit.tac-tic.info
viviendas8.com

lockbitsptqsmaf56cmo7bieqwh5htlsfkodpahsaurxlquoz67zwrad.onion
lockbit7z5ehshj6gzpetw5kso3onts6ty7wrnneya5u4aj3vzkeoaqd.onion
ll7wsjnsv23csjgaeyqjzoo6s2mhswo7ezzwyqrqbtqz6zzv4lykovqd.onion
lbbov7weoojwnqytnjqygmglkwtim5dvyw3xvoluk5ostz75ofd6enqd.onion
lockbitfss2w7co3ij6am6wox4xcurtgwukunx3yubcoe5cbxiqakxqd.onion
lly4dbpmlg4lgsua37sqn3mdocstjuqnvdtzv7fkz7sfsfu56xahd7yd.onion
lockbitapiahy43zttdhslabjvx4q6k24xx7r33qtcvwqehmnnqxy3yd.onion
lockbit7z6qinyhhmibvycu5kwmcvgrbpvtztkvvmdce5zwtucaeyrqd.onion
llhsnvqxz5i5jkvebb2nt4l77l5cu4hd5jhpjlkj5n7ramr2z6g4kzyd.onion

Ransomware Victims Worldwide

A recent ransomware threat landscape analysis reveals that the United States remains the most significantly impacted nation, accounting for a substantial 48.85% of global incidents. This highlights the persistent targeting of US-based organisations by increasingly sophisticated ransomware operations.

Germany emerges as the second-most affected country, reporting 10.34% of global incidents, followed by Canada at 6.9%, and the United Kingdom at 4.6%. These figures signal an intensifying focus on key Western economies. Meanwhile, India reports 3.45% of global cases, demonstrating the spread of ransomware campaigns into South Asia.

Several other countries have experienced moderate levels of ransomware activity, including Italy (2.3%), Bangladesh (1.72%), France (1.72%), Australia (1.72%), Spain (1.72%), and the United Arab Emirates (1.72%), reflecting a broader geographic distribution of ransomware attacks across Europe, Asia, and the Middle East.

Nations reporting 1.15% of incidents each include Brazil, Saudi Arabia, Taiwan, and Singapore — suggesting that even technologically advanced or geographically distant countries are not immune to these threats.

Several countries recorded lower yet notable percentages of ransomware activity, each contributing 0.57% of global incidents. These include the Netherlands, Austria, China, Israel, Colombia, Indonesia, Argentina, Japan, Ireland, Switzerland, Sweden, Egypt, Iran, Ukraine, New Zealand, Greece, and Turkey.

This global distribution of ransomware incidents underscores the widening scope and international scale of cybercriminal operations. The findings highlight the urgent need for coordinated cybersecurity efforts, including cross-border intelligence sharing, robust threat detection capabilities, and resilient incident response plans to mitigate the escalating risk posed by ransomware threats.

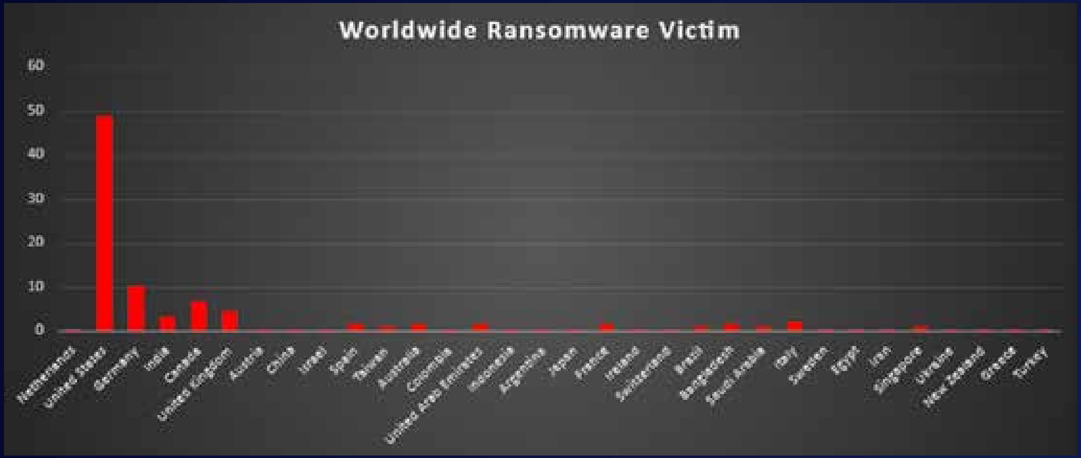


Figure 3: Ransomware Victims Worldwide

Ransomware Victims by Industry

In the most recent industry-specific analysis of ransomware activity, the Manufacturing sector has emerged as the most targeted, accounting for 18.97% of global incidents. This continues to highlight the pressing vulnerabilities in industrial control systems, production infrastructure, and interconnected supply chains.

Business Services followed with 12.07%, signalling a sustained ransomware focus on service-based and consulting organisations that handle large volumes of client data. The Construction industry ranked third, with 11.49% of incidents, reflecting ongoing exposure among engineering, infrastructure, and development firms.

Other heavily impacted sectors include Healthcare (7.47%) and Retail (6.9%), underscoring the targeting of sensitive patient records and consumer data. Notably, the Federal sector reported 5.17% of incidents, emphasising the growing threat to governmental and public agencies.

Finance (4.02%) and Law Firms (4.02%) remain high-value targets due to their concentration of confidential financial and legal data. Sectors such as Education (3.45%), Transportation (3.45%), and Hospitality (2.87%) also saw considerable ransomware activity, revealing attackers' interest in institutions providing essential services.

Emerging concerns were observed in industries like Telecommunications (2.3%), Consumer Services (2.87%), Organisations (2.3%), Insurance (2.3%), and IT (2.3%), indicating a shift toward digital service providers and policy-driven data holders.

Lower but still notable targeting was seen in Real Estate (1.15%), Energy (1.72%), Media & Internet (1.72%), and Minerals & Mining (1.72%), as threat actors diversify across operationally critical sectors. Agriculture (0.57%) and Electricity (0.57%) were also affected, proving that even traditionally offline industries are not immune.

This analysis affirms that ransomware attacks remain indiscriminate and opportunistic, affecting both critical infrastructure and commercial enterprises. The growing breadth of targeted sectors reinforces the necessity for industry-specific cybersecurity frameworks, enhanced intrusion detection mechanisms, and robust incident response plans to combat these evolving threats.

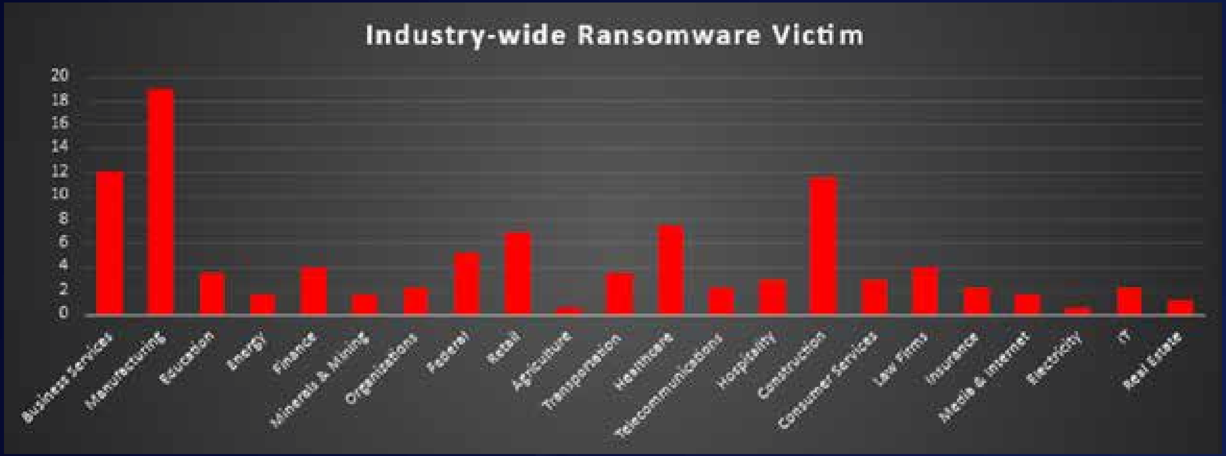


Figure 4: Industry-wide Ransomware Victims