Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

June 3 - 9, 2025

Report Summary:

- **New Threat Detection Added**
  - LandUpdate808
  - JanelaRAT
- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 130**
  - **Newly Detected Threats – 2**

The following threats were added to Crystal Eye this week:

1. LandUpdate808

LandUpdate808 is an exploit kit to make use of the ClickFix technique. The ClickFix technique tricks a user into thinking that their browsers aren't up to update, or they are running a vulnerable version that can be hacked and to fix it all the user has to do is copy the command given and paste it into PowerShell. This usually leads to a dropper being installed/executed that can deploy any number of malware and create a C2 backdoor on the system.

The exploit kit makes it easier for threat actors to deploy web pages utilising the ClickFix technique. It does this by imitating a browser update, and instead of copying a PowerShell command it gets the user to download the malicious payload directly from the website.

Rules Created: 02
Rule Set Type:

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

Class Type: Malware

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204.001	User Execution – Malicious Link
	T1204.002	User Execution – Malicious File

2. JanelaRAT

JanelaRat was first seen in June of 2023 and is expected to have originated from a Portuguese speaking country. JanelaRat appears to be targeting Banking and Financial institutions in Latin American areas. The threat actor distributes the malware via ZIP archives. These archives contain a heavily modified VBScript from a different malware called BX RAT. Once the VBScript is executed, it does two things; it downloads and extracts another ZIP Archive from the attacker-controlled server. This new archive contains the main payload in .dll format and a legit file called vmnat.exe. The initial VBScript also contained a .bat file that persistently runs the vmnat.exe which side loads the .dll payload, this is the whole infection chain. The user's system is now under control from this Remote Access Trojan.

The malware does contain several defence mechanisms to protect itself from reverse engineering and detection, such as string encryption, and it goes idle if it's inactive to avoid being picked up for the network

Rules Created: 03
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Resource Development	T1587.001	Develop Capabilities: Malware
Resource Development	T1608.001	Stage Capabilities: Upload Malware
Execution	T1059.005	Command and Scripting Interpreter: Visual Basic
Persistence	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder
	T1574.002	Hijack Execution Flow: DLL Side-Loading
Defence Evasion	T1027.002	Obfuscated Files or Information: Software Packing
Defence Evasion	T1140	Deobfuscate/Decode Files or Information
Defence Evasion	T1497.003	Virtualisation/Sandbox Evasion: Time Based Evasion
Command-and-Control	T1132.001	Data Encoding: Standard Encoding
Command-and-Control	T1573.001	Encrypted Channel: Symmetric Cryptography
Command-and-Control	T1095	Non-Application Layer Protocol
Exfiltration	T1041	Exfiltration Over C2 Channel

Known exploited vulnerabilities (Week 2 June 2025)

Vulnerability	CVSS	Description
CVE-2025-5419	8.8 (Critical)	Google Chromium V8 contains an out-of-bounds read and write vulnerability that could allow a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2025-21479 /CVE-2025-21480	8.6 (High)	Multiple Qualcomm chipsets contain an incorrect authorisation vulnerability. This vulnerability allows for memory corruption due to unauthorised command execution in GPU micronode while executing specific sequence of commands.
CVE-2025-27038	7.5 (High)	Multiple Qualcomm chipsets contain a use-after-free vulnerability. This vulnerability allows for memory corruption while rendering graphics using Adreno GPU drivers in Chrome.
CVE-2021-32030	9.8 (Critical)	ASUS Lyra Mini and ASUS GT-AC2900 devices contain an improper authentication vulnerability that allows an attacker to gain unauthorised access to the administrative interface. The impacted products could be end-of-life and/or end-of-service.
CVE-2025-3935	8.1 (High)	ConnectWise ScreenConnect contains an improper authentication vulnerability. This vulnerability could allow a ViewState code injection attack, which could allow remote code execution if machine keys are compromised.
CVE-2025-35939	5.3 (Medium)	Craft CMS contains an external control of assumed-immutable web parameter vulnerability. This vulnerability could allow an unauthenticated client to introduce arbitrary values, such as PHP code, to a known local file location on the server.
CVE-2024-56145	9.3 (Critical)	Craft CMS contains a code injection vulnerability. Users with affected versions are vulnerable to remote code execution if their php.ini configuration has register_argc_argv enabled.
CVE-2023-39780	8.8 (High)	ASUS RT-AX55 devices contain an OS command injection vulnerability that could allow a remote, authenticated attacker to execute arbitrary commands

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-june-2025/567

Updated Malware Signatures (Week 2 June 2025)

Threat	Description
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 Victims Worldwide

Qilin dominates this week's ransomware activity with 11.29% of total reported attacks. Its consistent appearance in top-tier rankings suggests operational maturity and sustained international reach, possibly driven by advanced tooling or active affiliate engagement.

Inc Ransom and Sarcoma follow closely, each accounting for 8.87% of attacks. Their parallel rise could indicate coordinated campaigns or targeted attacks within specific industries or regions.

Lynx registered 8.06%, reinforcing its status as a growing mid-tier threat actor with a notable victim footprint. Meanwhile, Interlock posted 5.65%, continuing its trend of aggressive operations, often linked to data leak extortion.

Groups like DireWolf, El Dorado, and Play each contributed 4.84%, suggesting broad targeting across multiple sectors. WorldLeaks, Gunra, Medusa, and Global also appeared prominently at 4.03%, reflecting either opportunistic exploitation or scaled ransomware-as-a-service deployments.

Fsociety, J Group, and SafePay all recorded 3.23%, with Weyhro and Chaos at 2.42%, marking them as active but lower-volume operators this week.

A collection of groups—including Devman, Crypto24, BlackSuit, RansomHouse, Kairos, Everest, Bert, MetaEncryptor, Datacarry, Cloak, Arkana Security, and Stormous—each accounted for 0.81% of reported attacks. This reflects the fragmented and persistent nature of the ransomware ecosystem, where numerous actors operate below the radar but continue to pose substantial risks across industries.

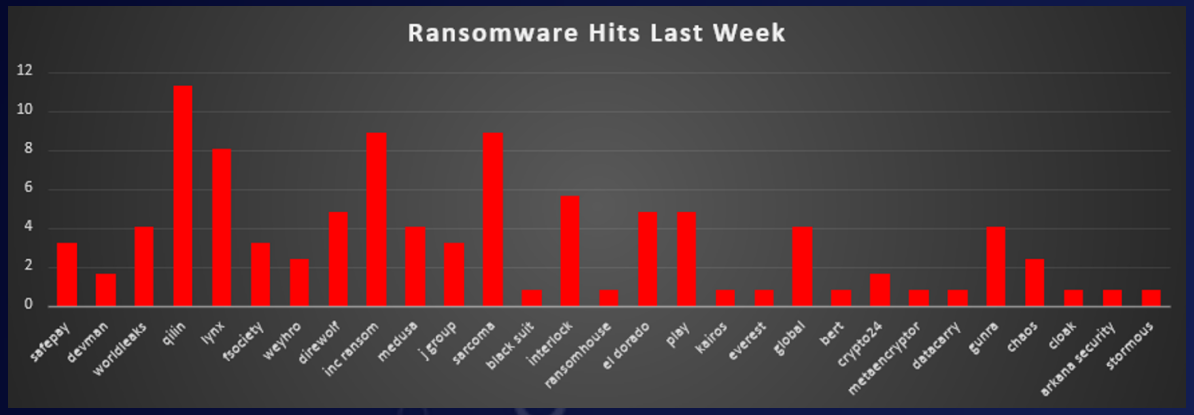

Figure 1: Ransomware Group Hits Last Week

Bert Ransomware

Bert is a double-extortion “Data Broker” ransomware family first observed in April 2025: after breaching a Windows host it encrypts data, appends “.encryptedbybert” (or a six-hex variant) to each filename, and plants a ransom note named “.note.txt” that directs victims to negotiate over the privacy-centric Session messenger. The note also threatens to release exfiltrated files on Bert’s Tor leak portal. Technical analyses show the malware uses native Win32 APIs, adds HKLM Run keys for persistence, injects into benign processes, timestomps PE headers to 2007, deletes Volume Shadow Copies, and employs ChaCha20 + Curve25519 for encryption. Initial access in early campaigns has come from phishing e-mails and at least one trojanised software-update distribution, underscoring Bert’s blend of low-friction delivery and aggressive data-leak extortion

TTP Summary

- Initial Access: phishing attachments/links and credential misuse remain the only publicly documented vectors.
- Execution & Persistence: binaries execute via native Win32 APIs or GLIBC calls and install Run-key/Startup entries that survive Safe-Mode boots.
- Privilege Escalation/Defence Evasion: process-injection into explorer.exe/WerFault.exe, timestomping, obfuscated strings, and path masquerading observed in JoeSandbox runs.
- Discovery & Collection: enumerates drives, mapped shares, and browser artefacts before staging data for exfil.
- C2 & Impact: encrypts with ChaCha20 + Curve25519 and communicates with Tor (.onion) services for negotiation.

TTP Chart

Tactic	Technique ID	Technique Name	Key Details / Sources
Initial Access	T1566	Phishing (malicious attachment)	ransom-note guidance & campaign lure
Execution	T1106	Native API	PE & ELF samples call Win32/glibc APIs directly
Persistence	T1547.001	Run Keys / Startup Folder	registry or .desktop AutoStart entries
Persistence	T1574	Hijack Execution Flow	service-replace variant in Windows build
Priv-Esc	T1055	Process Injection	reflective-load into svchost/systemd children
Defence Evasion	T1027	Obfuscated/Encrypted Code	PE resources & XOR-encoded strings
Defence Evasion	T1070.006	Timestomping	file dates reset to 2007-01-01 in samples
Discovery	T1083	File & Directory Discovery	scans mapped drives before encryption
Collection	T1074	Data Staged	temp archive before exfil
C2	T1071.001	Web Protocol (Tor)	traffic to leak site & negotiation onion
Impact	T1486	Data Encrypted for Impact	ChaCha20/ECC scheme
Impact	T1490	Shadow Copy Deletion	vssadmin delete shadows strings present

IOC

SHA256 (all first-seen 2025-06-06, 05:30-05:33 UTC)

c7efe9b84b8f48b71248d40143e759e6fc9c6b7177224eb69e0816cc2db393db
78eb838238dad971dcbc46b86491d95e297f3d47dc770de5c43af3163990d31c
5bba035c4cb3c2e09a355d9356b3397184af4bf1ac1ff1df99ae9c15edee9f2b
25c693808095f45d297171eba5196e9a5176281a2d248cb1a8cfa07a68bbe332
6182df9c60f9069094fb353c4b3294d13130a71f3e677566267d4419f281ef02
f2dc218ea8e2caa8668e54bae6561afd9fbf035a40b80ce9e847664ff0809799
ced4ed5e5ef7505dd008ed7dd28b8aff38df7febe073d990d6d74837408ea4be

MD5s

00fdc504be1788231aa7b7d2d1335893
71dc9540eb03f2ed4d1b6496b13fe839
d1013bbaa2f151195d563b2b65126fa3
3e581aad42a2a9e080a4a676de42f015
edec051ce461d62fbbd3abf09534b731
5cab4fabffeb5903f684c936a90e0b46
003291d904b89142bada57a9db732ae7
29a2cc59a9ebd334103ce146bca38522
38ce06bf89b28ccebf5a78404eb3818e

IPs

185.100.157.74
169.254.169.254

Domains / URLs

Onion services

Leak Site

bertblogsoqmm4ow7nqyh5ik7etsmefdbf25stauecytvwy7tkgizhad.onion

Negotiation Site

76yl7gfmz2kkjglcevxps4tleyeqnqhfcxh6rnstxj27oxhoxird3hyd.onion
yj3eozlkkxkcsprc2fug7tolgtnllruyavuyyar3yzsccjdgvu2bl2yd.onion
y6kyfs2unbfcyodzjrxadn4w5vyulhyotdi5dtiqulxbduujehupunqd.onion

File Server

4q5tsu5o3msmv4am4dfhupwhzlyg7wv3lpswbvbhcrknr4ega7xetxad.onion
5dw7bszmidrhpoltqbqmpixpz6mvgez3mr6xc7ktval2glrmbxkwopad.onion
ec6edgevw2lzqy4ipafpbvjuu7r6ugqbljqokl3pvecc6c3a5ix3wgyd.onion

Contact

Session ID: 05149ef8a65c342bc76bad335ad3a314ec1321b18cdb6092667083b4e56a4dcb42

Mitigation (Guidance with subtle CE 5.0 context)

- Block Tor & Onion Domains: Add all BERT onion addresses and Tor relay 185.100.157.74 to DNS / web-proxy deny lists. CE 5.0's Advanced Firewall lets administrators create object-based rules tied to these indicators without touching core routing tables.
- Registry & Safe-Boot Monitoring: Detect unexpected HKLM\...\Run keys or Safe-Mode boots—early signs of BERT's persistence. CE 5.0's Intrusion Protection & Detection profile can be bound to the workstation VLAN to raise SOC tickets automatically when such events occur.
- Driver & Script Control: Enforce Microsoft's vulnerable-driver block list and Attack-Surface-Reduction rules. Where CE is deployed as a gateway, its Network Detection & Response module surfaces BYOVD or process-injection traffic anomalies before encryption starts.
- Immutable Backups & Segmentation: Keep offline/WORM snapshots and separate backup networks; CE's interface zoning and VLAN support make micro-segmentation straightforward.
- Endpoint Integration: Pair CE with Microsoft Defender for Endpoint to stream ransomware telemetry into the same dashboard, improving mean-time-to-detect without extra consoles.
- Threat-Hunt & Incident Response: Use CE's built-in Threat Hunt Dashboard for continuous correlation and enable the Incident Response Services plug-in so that critical BERT alerts auto-escalate to Red Piranha's SOC for 24×7 containment. See here for details.
- Unified Platform Advantage: Because CE 5.0 delivers firewall, IDPS, NDR, DLP and MDR in one appliance, defenders avoid the integration gaps BERT exploits—while keeping licensing overhead low.cyberdefensemagazine.com

Worldwide Ransomware Victim

The United States continues to dominate the global ransomware landscape, accounting for 50.81% of all reported victims this week. Its expansive digital ecosystem, critical infrastructure, and deep enterprise networks make it a primary target for ransomware actors.

Australia emerges as a significant second with 10.48%, reflecting heightened threat actor attention on the Asia-Pacific region—likely due to its growing role in global tech and finance sectors.

Canada reports 7.26%, showing persistent threat activity against North American enterprises. The United Kingdom follows at 4.84%, with continued targeting of financial, legal, and service-based organisations.

Countries like Brazil (3.23%), United Arab Emirates, and Vietnam (2.42% each) represent active zones of exploitation, often tied to strategic industries or emerging markets.

A wide array of nations—including Germany, Venezuela (1.61% each), and Monaco, Barbados, Bahrain, Hungary, Norway, Italy, Ecuador, China, Thailand, Turkey, Colombia, Chile, Jordan, India, Argentina, Croatia, Ireland, and Netherlands (0.81% each)—illustrate the global distribution of ransomware threats. This “long-tail” of impacted countries reinforces the notion that ransomware is a worldwide risk, indiscriminately targeting vulnerable entities regardless of geography.

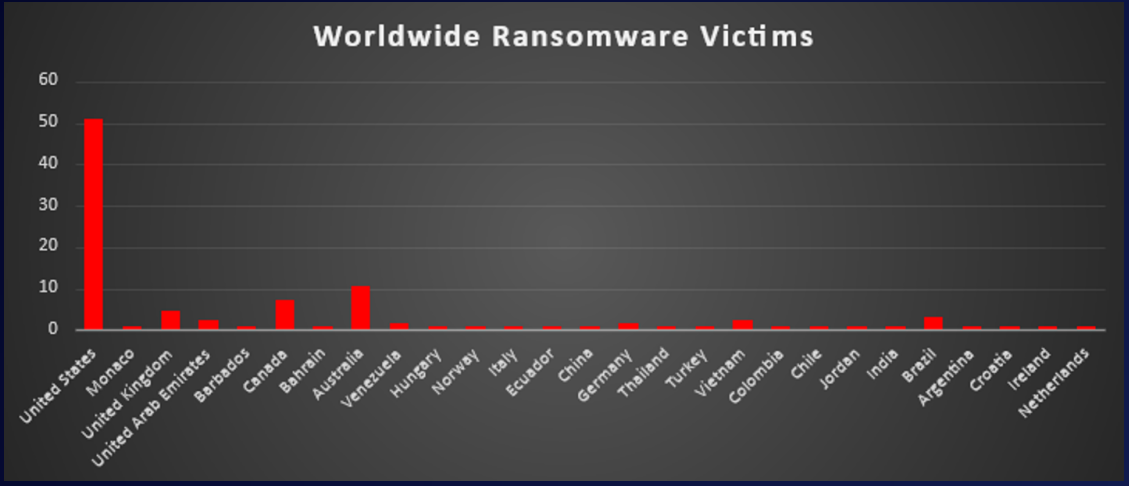

Figure 2: Ransomware Victims Worldwide

Ransomware Victims by Industry

Manufacturing remains the most heavily impacted sector this week, accounting for 20.97% of reported ransomware incidents. Its large operational surface, reliance on legacy systems, and critical role in supply chains make it a persistent target.

Business Services follows with 10.48%, highlighting the vulnerability of consultancy, logistics, and outsourced IT sectors often serving multiple high-value clients. Both Retail and Construction reported 8.87%, indicating continued targeting of sectors with distributed endpoints, seasonal workflows, and high transaction volume. Real Estate and Hospitality each saw 7.26% of incidents, reflecting threat actors' interest in sectors rich with personal and financial data but often lacking mature cybersecurity defences.

Finance registered 6.45%, driven by its high-value digital assets and regulatory pressures. Meanwhile, Law Firms saw 4.84%, consistent with ongoing interest in sensitive legal data.

Federal and IT sectors reported 4.03% each, underscoring the risk to public sector agencies and digital infrastructure providers.

Sectors such as Education, Organisations, Transportation, and Electricity each accounted for 2.42%, suggesting moderate but noteworthy threat activity. Smaller shares were observed in Insurance, Media & Internet, Agriculture, and Consumer Services (all at 1.61%), demonstrating the ransomware ecosystem's broad reach across nearly every industry.

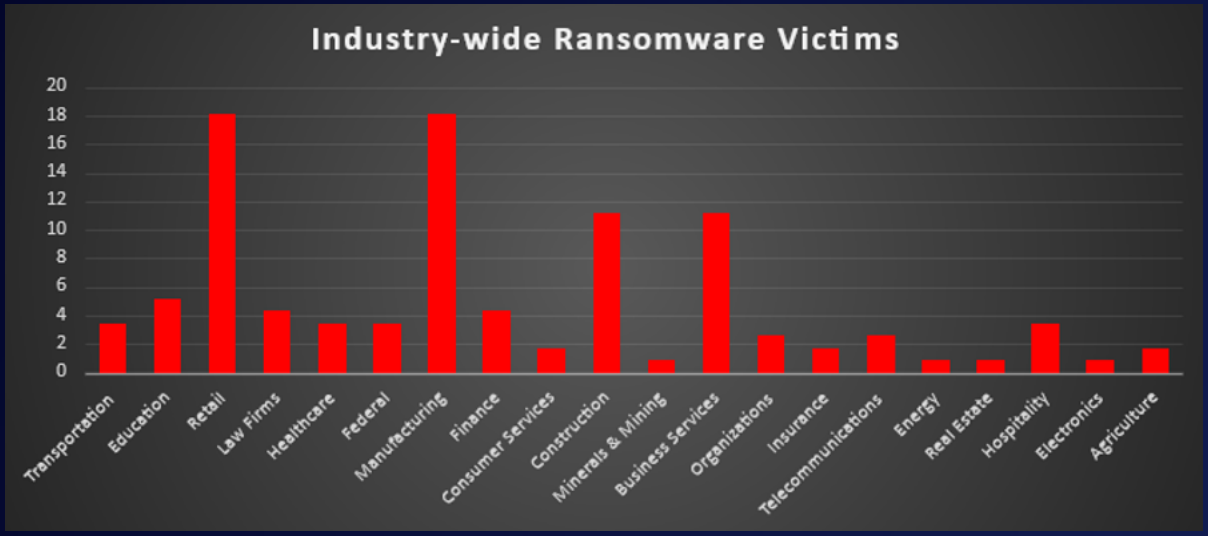

Figure 3: Industry-wide Ransomware Victims