Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Feb 25 - Mar 03, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - implant.js: Modular Malware Using the V8 JavaScript Engine
  - Darcula Phishing-as-a-Service (PhaaS) Platform

- **New Threat Protections - 182**

The following threats were added to Crystal Eye this week:

1. implant.js: Modular Malware Using the V8 JavaScript Engine

At DistrictCon 2025, a security researcher introduced implant.js, a proof-of-concept modular malware framework written in C++ that leverages the V8 JavaScript Engine. This framework enables the development of operating system-agnostic modules, allowing code to be written once and executed across various architectures without the need for pre-compilation. implant.js provides operators with flexibility and usability, granting access to native code and system library functions for complex functionalities.

Threat Protected: 09
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
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

2. Darcula Phishing-as-a-Service (PhaaS) Platform

Darcula is a sophisticated phishing-as-a-service (PhaaS) platform that has been active since at least March 2024. It offers cybercriminals a comprehensive suite of tools to conduct large-scale phishing campaigns with minimal technical expertise. Initially, Darcula provided over 200 phishing templates targeting various brands and services. However, with the upcoming release of 'Darcula Suite' (version 3.0), the platform introduces a do-it-yourself (DIY) phishing kit generator. This feature allows users to create custom phishing kits by simply inputting the URL of the brand they wish to impersonate. The platform then automatically clones the legitimate site using tools like Puppeteer, replicating the HTML, CSS, images, and JavaScript to maintain the original design.

Threat Protected: 03
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204.001	User Execution: Malicious Link
Credential Access	T1557	Brute Force
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols

Known exploited vulnerabilities (Week 4 February 2024):

Vulnerability	CVSS	Description
CVE-2024-20953	8.8 (High)	Oracle Agile Product Lifecycle Management (PLM) Deserialization Vulnerability
CVE-2017-3066	9.8 (Critical)	Adobe ColdFusion Deserialisation Vulnerability
CVE-2023-34192	9.0 (Critical)	Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability
CVE-2024-49035	9.8 (Critical)	Microsoft Partner Center Improper Access Control Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-february-2025/551

Updated Malware Signatures (Week 4 February 2024)

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.

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
Hunters	1.53%
Akira	3.56%
Rhysida	0.25%
Wikileaksv2	1.27%
DragonForce	0.51%
Medusa	2.29%
Lynx	4.33%
Inc ransom	1.27%
Interlock	0.76%
RansomHub	7.89%
Cicada3301	2.04%
KillSec3	1.02%
Clop	56.23%
Qilin	2.04%
Cactus	3.82%
Kairos	0.25%
Eraleign (apt73)	0.25%
Morpheus	0.25%
Cloak	0.25%
Space Bears	0.25%
Stormous	0.25%
Lockbit3	0.76%
Embargo	0.25%
Anubis	1.02%
Play	2.54%
Termite	1.27%
RansomHouse	0.25%
Fog	0.25%
HellCat	0.25%
Run Some Wares	1.02%
Leaked Data	0.25%
FunkSec	1.02%
Ransomware Blog	0.25%
SafePay	0.25%

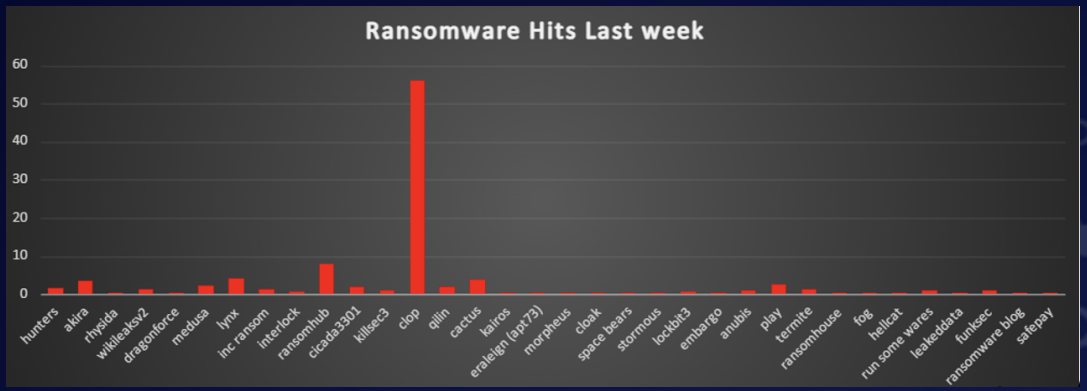

Figure 1: Ransomware Group Hits Last Week

Lynx Ransomware

1.Group Emergence & Characteristics

- Windows & Linux Availability: Lynx Ransomware is distributed in both Windows and Linux flavours. Although the Linux variant is built for ESXi servers, it has not been observed in active attacks yet.
- Mode-Based Encryption: Later versions of Lynx introduced fast/medium/slow/entire encryption modes, allowing attackers to define how much of each file is encrypted - striking different balances between speed and thoroughness. Earlier variants lacked this feature, defaulting to a roughly 16% file encryption scheme.
- Targeted Systems & Extension: Upon encrypting files, Lynx appends the ".LYNX" extension.

Option	Platform(s)	Description
file	Windows, Linux	Encrypt only specified file(s).
dir	Windows, Linux	Encrypt only specified directory(ies).
mode	Windows, Linux	Defines encryption thoroughness: slow (25%), medium (15%), fast (5%), or entire (100%).
verbose	Windows, Linux	Prints logging messages to the console.
help	Windows, Linux	Displays a help menu.
silent	Windows only	Executes encryption without adding extension or notes.
stop-processes	Windows only	Terminates active processes using RestartManager.
encrypt-network	Windows only	Encrypts network shares.
load-drives	Windows only	Enumerates & mounts hidden or unmounted volumes.
hide-cmd	Windows only	Hides the console window during execution.
no-background	Windows only	Prevents changing the desktop wallpaper.
no-print	Windows only	Disables printing of ransom notes.
kill	Windows only	Kills specified processes/services.
safe-mode	Windows only	Reboots into Safe Mode and starts encryption.
esxi	Linux only	Force-stops running ESXi VMs via their World IDs.
delay	Linux only	Delays the encryption process by N minutes.
fork	Linux only	Forks the current process.
motd	Linux only	Inserts the ransom note into the system's Message of the Day.

2.Environment Preparation & Privilege Escalation (Windows)

- Privilege Escalation: If the ransomware detects insufficient file access, it automatically enables SeTakeOwnershipPrivilege, takes ownership of target files, and modifies their Discretionary Access Control List (DACL).
- Windows Restart Manager: Processes using targeted files are terminated to ensure uninterrupted encryption.
- Drive Mounting: When load-drives is enabled, Lynx identifies unmounted volumes and assigns them drive letters, expanding its attack surface.

3.Whitelisted & Blacklisted Entities

- Whitelisted File Extensions: .exe, .dll, .msi, .lynx
- Blacklisted Services (Windows): sql, veeam, backup, exchange
- Blacklisted Processes (Windows): sql, veeam, backup, exchange, java, notepad

4.Encryption Scheme

- Multi-Threading:
  - Windows: Spawns 4× the number of CPU cores for maximum concurrency.
  - Linux: Spawns 2× CPU cores (optimised for ESXi targeting).
- Algorithm Combination: Uses Curve25519 Donna for key exchange, while file data is encrypted with AES-128 in CTR mode.
- File Extension: Once encrypted, files are renamed with the .LYNX suffix (unless silent mode is specified).

5.Post-Encryption Actions

- Wallpaper & Print Jobs: Lynx changes the victim's desktop background to a ransom note and attempts to print the note on connected printers (excluding "Microsoft Print to PDF" and "Microsoft XPS Document Writer").
- ESXi-Specific Scripts (Linux):
  - Killing VMs: Writes a script named kill, which force-terminates all virtual machines on an ESXi host by enumerating their "World IDs":

```
for i in $(esxcli vm process list | grep 'World' | grep -Eo '[0-9]{1,8}'); do esxcli vm process kill -t=force -w=$i; done
```

  - Removing Snapshots: Writes a script named delete to remove all snapshots on each ESXi VM

```
for i in $(vim-cmd vmsvc/getallvms | awk '{print $1}' | grep -Eo '[0-9]{1,8}'); do vim-cmd vmsvc/snapshot.removeall $i; done
```

Detailed TTPs

The table below maps Lynx Ransomware tactics to MITRE ATT&CK techniques:

TTP ID	Tactic	Technique	Description
T1059	Execution	Command and Scripting Interpreter (Windows)	Supports command-line encryption options, process termination, and parameterised attacks.
T1059.004	Execution	Command and Scripting Interpreter (Linux/Unix)	Allows specifying encryption scope, targeting ESXi with esxi argument.
T1134	Privilege Escalation	Access Token Manipulation	Sets SeTakeOwnershipPrivilege and edits file DACLs to gain control over restricted files.
T1490	Impact	Inhibit System Recovery	Deletes Volume Shadow Copies on Windows; removes ESXi snapshots to cripple backup/restore efforts.
T1005	Collection	Data from Local System	Enumerates files, including those on newly mounted volumes, to maximise encryption.
T1486	Impact	Data Encrypted for Impact	Core functionality: encrypt files (Windows/Linux) and demand ransom, often accompanied by a ransom note.

IOCs

b1d81e8bbecccc547645d17395538a2d
a20886a5b378624d16972db66bd4e7e1
f16238836909d07f86154c5ccbade96a
30656c737338818bee8cc3591e3f3dcc
571684f28ce1cf4d8236dbd46ef6f7f0
65c0c7c9fe6bc1d5296447aae6c6c14c
d972bbbb3edb0e5ab5751b911f3dda17
146d350fd6271b4411714c630d8cda87
ff458208c49836cdec92f0a4a7ba6afd
67a44a38cc36becd6e2e9c20c27fd9ad
3a39bcd9fc840b4e13042f916d9eb39a
b47cdcdc179c5949ce18f4d161603901
2348b069647af0a714ae1e005f73b522
14a0ecf45aa72adb2b1f2ccca99f6faa
57f45c0738af9cd49c61984ea99f83ca
31a77e0d1c1b91eebec1f7cdcc1ab8b8
74ae58a716aaa834949388ee1574788e0
0e521e0452f113cdf8b5c2fa6580db1f
7e851829ee37bc0cf65a268d1d1baa7a

- File Hash

svhost.exe.bin	80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441
Frantic_Setup.exe	80fd105d0685b85c1be5d5d3af63608d2ec91b186d4c591416934fe454770ca1
build.exe	3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eaed044e
	97c8f54d70e300c7d7e973c4b211da3c64c0f1c95770f663e04e35421dfb2ba0
windows.exe	468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a
	432f549e9a2a76237133e9fe9b11fbb3d1a7e09904db5ccace29918e948529c6
win.exe	4e5b9ab271a1409be300e5f3fd90f934f317116f30b40eddc82a4dfd18366412

- Lynx URLs

http://lynxblog.net/
http://lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd.onion/leaks
http://lynxblog.net/leaks
http://lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd.onion/leaks
http://lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd.onion/leaks
http://lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd.onion/leaks
http://lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad.onion/leaks
http://lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad.onion/leaks
http://lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad.onion/leaks
http://lynxblogxutufossaeawlij3j3uikaloll5ko6grzhkwdclrjngrfoid.onion/leaks

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States continues to be the most heavily impacted nation, accounting for an extraordinary 71.5% of all documented ransomware incidents—underscoring its pronounced vulnerability to such cyber threats. Following this, Canada emerges as the second most targeted region with 6.36% of reported attacks, followed by the United Kingdom at 4.33%.

Notably, Germany experiences 2.29% of observed attacks, while Mexico registers 2.04%. Further highlighting the global scope of ransomware threats, Australia and France each account for 1.53% of incidents. Spain, cumulatively at 1.52% (combining two reported entries), and Brazil with 1.02% also show considerable impact.

Other countries collectively reporting under 1% include New Zealand, Italy, and India at 0.76%, alongside Egypt, Sweden, Saudi Arabia, Singapore, Peru, and Japan at 0.51%. A broader group of nations—such as Taiwan, Netherlands, Ireland, Indonesia, China, Chile, Austria, Thailand, Palau, Colombia, and more—each report 0.25% of global ransomware cases, indicating that no single region remains untouched by these attacks.

This analysis highlights the persistent, worldwide reach of ransomware operations, with North America once again facing disproportionately high risks. As threats proliferate, the need for robust cybersecurity measures, proactive defence strategies, and cross-sector vigilance has never been more critical to mitigate potential impacts on government agencies, businesses, and individuals alike.

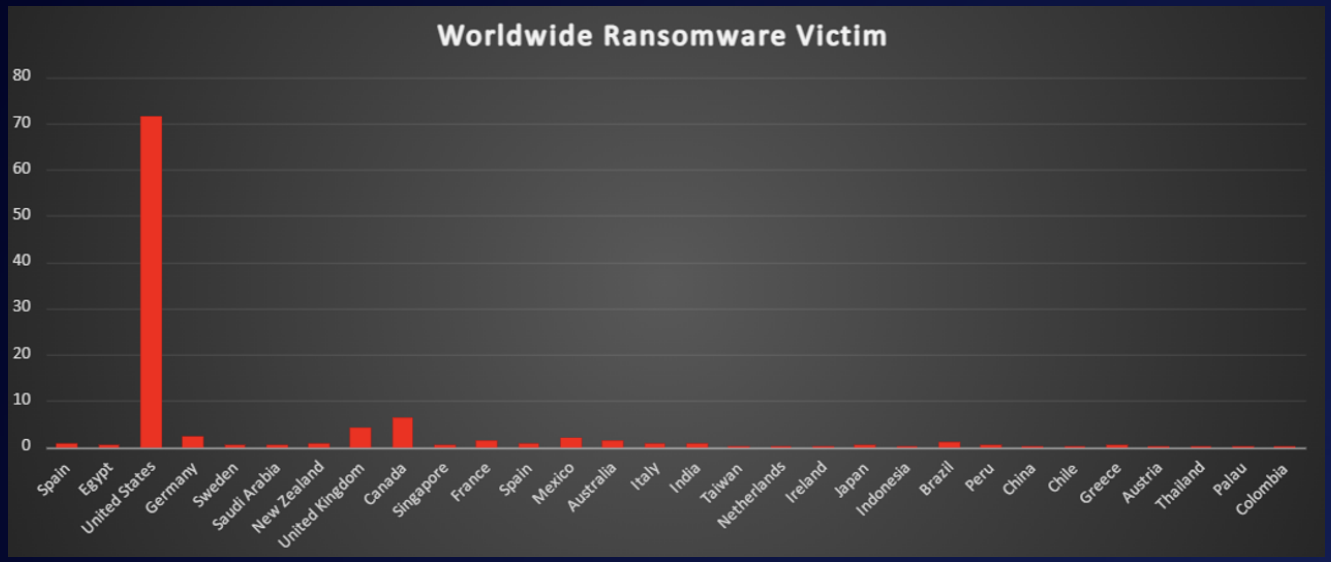

Figure 3: Ransomware Victims Worldwide

Ransomware Victims by Industry

A recent ransomware analysis reveals that the Manufacturing sector remains the single most targeted industry, accounting for 24.43% of total reported incidents—underscoring the high stakes involved when production lines and supply chains are compromised. Trailing closely behind, the Retail sector stands at 20.36%, highlighting its persistent vulnerability, especially in consumer-facing operations.

Business Services ranks next with 13.49% of the attacks, reflecting the vital role of outsourced services and consultancies in modern economies. The Transportation industry follows at 9.16%, pointing to the growing risk in logistical infrastructures. Meanwhile, Construction records 5.09% of ransomware incidents, signifying cybercriminals' continued interest in critical development and building projects.

Several industries register moderate exposure, including both Healthcare and Hospitality at 2.8%, as well as Law Firms and IT each reporting 2.29%. Real Estate, Education, and Federal sectors all stand at 2.04%, illustrating the diversity of targets spanning both private and public domains.

Further down the list, Finance and Consumer Services each account for 1.78%, while Telecommunications and Media & Internet follow at 1.27%. Organisations (1.02%) and Agriculture (1.02%) also face ongoing risk. Rounding out the lower percentages are Electricity (0.76%), Insurance (0.76%), Energy (0.76%), and Minerals & Mining (0.51%), each still notable given the often-critical nature of their operations.

This analysis reinforces the broad and indiscriminate reach of ransomware threats. Cybercriminals continue to target high-value or critical infrastructure sectors—such as Manufacturing and Retail—while also casting a wide net across services, technology, and other essential industries. The findings highlight the urgent need for sector-specific security strategies, robust risk management, and proactive cybersecurity measures to combat an evolving ransomware landscape.

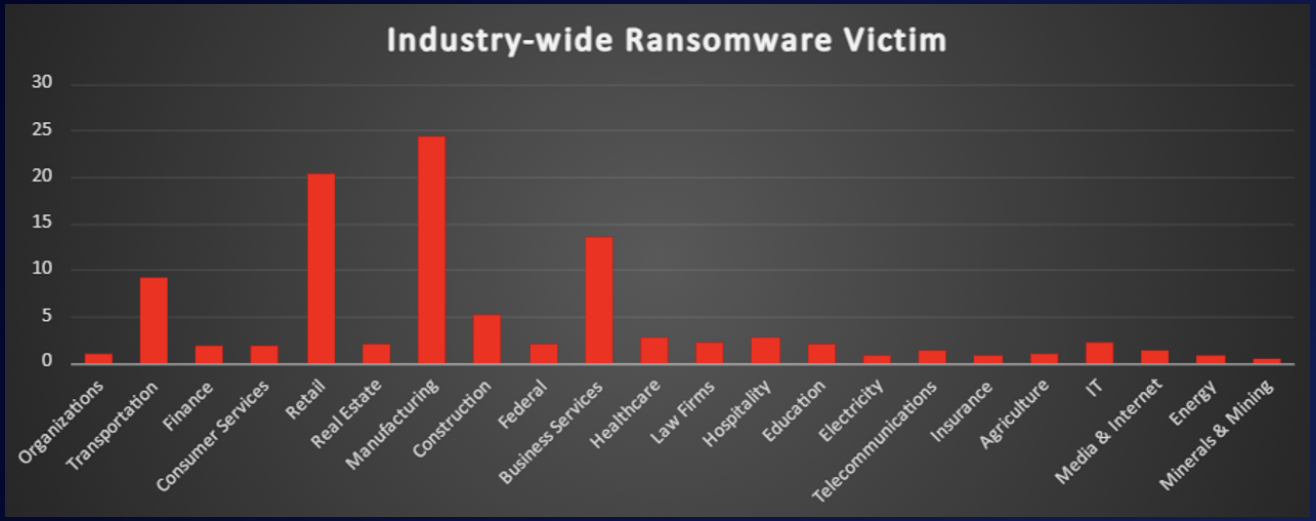

Figure 3: Industry-wide Ransomware Victims