Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 10 - 16, 2024

Report Summary:

- **New Threat Detection Added** – 2
  - Cleo Harmony, VLTrader, and LexiCom (CVE-2024-50623)
  - RevC2 and Venom Loader

- **New Threat Protections - 79**

The following threats were added to Crystal Eye XDR this week:

1. Cleo Harmony, VLTrader, and LexiCom (CVE-2024-50623)

A critical vulnerability, identified as CVE-2024-50623, has been discovered in Cleo's Managed File Transfer (MFT) software, specifically affecting Harmony, VLTrader, and LexiCom versions up to 5.8.0.21. This vulnerability allows remote attackers to execute arbitrary code on the affected systems by exploiting an arbitrary file write flaw through the /Synchronisation endpoint. The issue arises from improper path validation, enabling attackers to write malicious files to arbitrary locations, potentially leading to full system compromise. Although patches have been released, reports indicate that exploitation continues, suggesting that the initial fix may not have fully addressed the underlying issue.

Threats Protected: 02
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

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

2. RevC2 and Venom Loader

Deployed through Venom Spider's Malware-as-a-Service (MaaS) tools, RevC2 is a backdoor that utilises WebSockets for command-and-control (C2) communication, enabling capabilities such as credential theft, network traffic proxying, and remote code execution. Venom Loader is a customised malware loader that encodes its payload using the victim's computer name, enhancing its stealth and specificity. These malware families are distributed via malicious LNK files and exploit various obfuscation techniques to evade detection.

Threats Protected: 03
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	T1566.001	Spearphishing Attachment
Execution	T1059.001	Command and Scripting Interpreter
Defence Evasion	T1218.010	System Binary Proxy Execution: Regsvr32
Command-and-Control	T1071.001	Web Protocols

Known exploited vulnerabilities (Week 2 December 2024):

Vulnerability	CVSS	Description
CVE-2024-49138	7.8 (High)	Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability
CVE-2024-50623	8.8 (High)	Cleo Multiple Products Unrestricted File Upload Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-december-2024/531

Updated Malware Signatures (Week 2 December 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.
Remcos	Remcos functions as a remote access trojan (RAT), granting unauthorised individuals the ability to issue commands on the compromised host, record keystrokes, engage with the host's webcam, and take snapshots. Typically, this malicious software is distributed through Microsoft Office documents containing macros, which are often attached to malicious emails.

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, 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 Group	Overall Percentage of total attack coverage
Everest	1.58%
Inc ransom	1.58%
Rhysida	1.05%
Sarcoma	1.58%
Funksec	14.21%
Cicada3301	1.58%
Qilin	2.11%
Lynx	4.21%
RansomHub	4.74%
8base	0.53%
Killsec3	1.05%
Interlock	0.53%
Eraleign (APT73)	3.16%
BlackSuit	1.05%
Akira	12.11%
Blackout	0.53%
Cloak	2.11%
Bianlian	1.05%
Medusa	1.58%
Hunters	2.11%
Bluebox	1.05%
Nitrogen	2.11%
Stormous	4.21%
Argonauts group	2.11%
Fog	0.53%
RA group	0.53%
Termite	0.53%
SafePay	1.58%
Brain cipher	1.05%
Space bears	0.53%
Play	3.68%
Money message	0.53%
Kairos	1.58%
Leaked data	21.58%

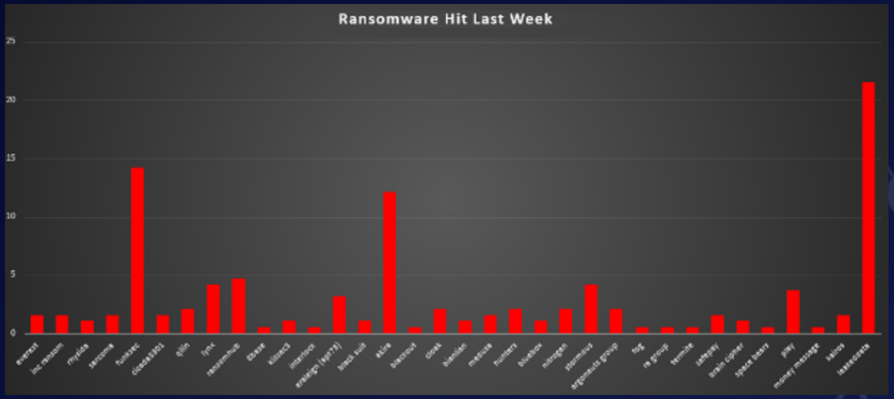


Figure 1: Ransomware Group Hits Last Week

Akira Ransomware Group

Akira ransomware operations began in March 2023, quickly gaining attention due to the unique "retro aesthetic" applied to their Data Leak Site (DLS) and overall branding. The group employs multi-extortion tactics, leveraging a TOR-based (.onion) portal to host victim details and negotiate ransom demands. Victims are given a unique identifier via ransom notes to initiate contact through this portal. Akira ransomware is notorious for demanding exorbitant ransom payments, often reaching hundreds of millions of dollars.

Detailed TTPs (Tactics, Techniques, and Procedures)

- Initial Payload Execution:
  - Upon execution, Akira ransomware removes Volume Shadow Copies (VSS) via PowerShell commands to inhibit data recovery.
  - Hard-coded file extensions are processed for encryption while excluded extensions ensure encryption stability.
- Encryption Techniques:
  - Encrypted files are appended with the .akira extension.
  - If files are locked by the operating system, the ransomware uses the Windows Restart Manager (WRM) API to handle the locked files and continue encryption.
- Communication and Negotiation:
  - Victims are instructed to connect to Akira's TOR-based portal to begin ransom negotiations.

Indicators of Compromise (IOCs)

File Hashes

FileHash-MD5:

- 08bd63480cd313d2e219448ac28f72cd
- 436c014614477e79696e838d6b605f4e
- 4b807353dfbeadaddb392627e27470f9
- 56f673b1d3d65dce3ef3c8754098df04
- 5eadd67bec799465fa27a17d6bf93e2d
- 7486f1a88d6a3ae96fa08f882d452399
- 7bf5cbca413b327c655e2270645955d9
- a1f4931992bf05e9bff4b173c15cab15
- b163803130f466db74f68a19f9cee11e
- e57340a208ac9d95a1f015a5d6d98b94
- e8139b0bc60a930586cf3af6fa5ea573
- f59d26d27cbab79fe84ef2e7e3b718f9
- fc5be86c846e93b0a65dd18849205514
- feb81a8d7e0f91d6f74b440cdd3c2f28

FileHash-SHA1:

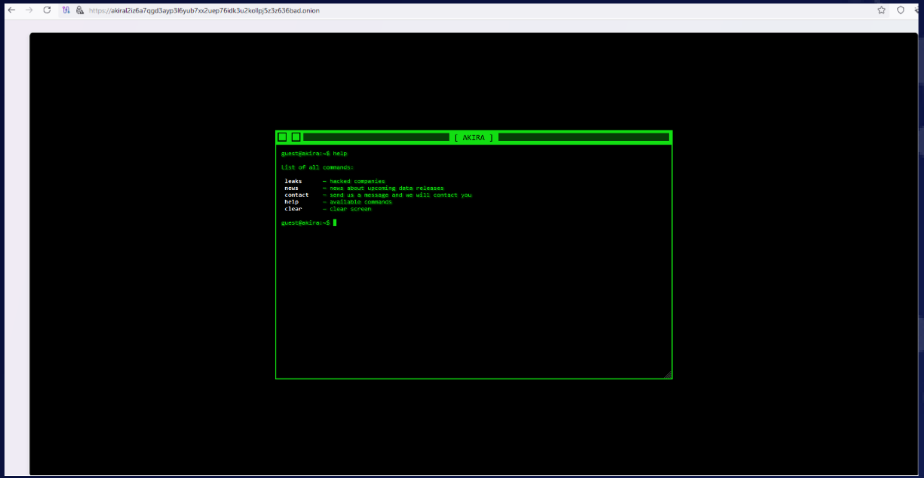
- 41323075a7dc590f20a154f503e089d2dac2fd12
- 4549f715bfeab0477c816dc7629b3d50963c4d23
- 7144371d00217533f49e03d40f650f3349fd04d1
- 810d0bcfcb83cb1a23ed3abd53c867bf260f239a
- 86f46189ea993c35fd029ca2308870c069f921e0
- 8951e54fabdd4d8e424573e53a51e309203f6f41
- c0aafc8c63d0bf316722968d1fe8f1d7637271cd

FileHash-SHA256:

- 0c662d28268514fabc7129fd14d6e3e9d7df29261a861bcf8aab1f318bb8e7d0
- 1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218
- 566ef5484da0a93c87dd0cb0a950a7cff4ab013175289cd5fccf9dd7ea430739
- 58e685695afc3a85d2632777a2b54967dc53d6a6fa1b7e2c110b2023b561bfe9
- 78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0
- 87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d
- 88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2
- ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5

Known Akira TOR-based Links:

- https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion/
- https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion/l



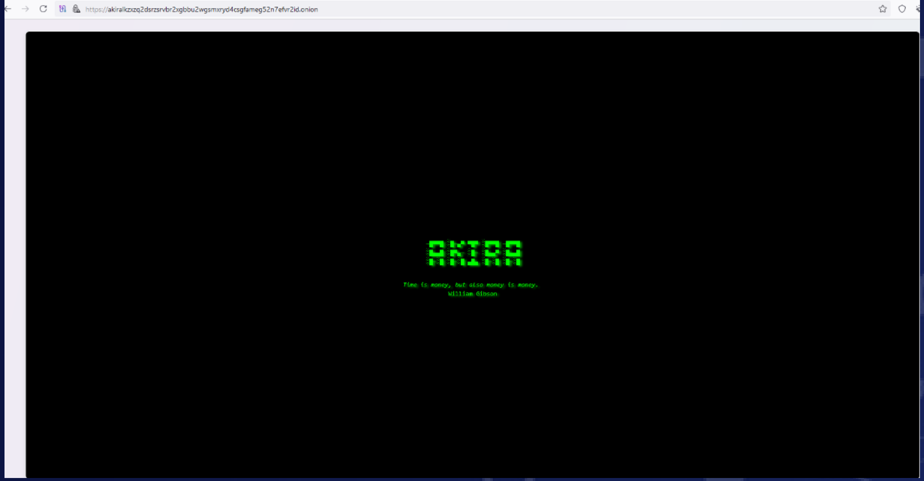
```
guest@akira:~$ help

List of all commands:

 leaks      - hacked companies
 news       - news about upcoming data releases
 contact    - send us a message and we will contact you
 help       - available commands
 clear      - clear screen

guest@akira:~$
```

- Chat Server: https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion



Time is money, but also money is money.
William Gibson

Threat Assessment

- Akira ransomware represents a significant threat due to its multi-extortion model, highly targeted victimology, and reliance on robust encryption techniques. The use of PowerShell for shadow copy removal and its ability to overcome file locks using the WRM API showcase a sophisticated approach designed to maximise damage. The high ransom demands indicate a focus on financially capable enterprises, likely identified through pre-attack reconnaissance.

Mitigations

1. Educate Employees
   - Train employees to identify and avoid phishing emails and malicious attachments. Encourage reporting of suspicious activities.
2. Implement Strong Password Policies
   - Enforce complex passwords and regular rotation, ensuring passwords are at least 12 characters long with a mix of uppercase, lowercase, numbers, and special characters.
3. Enable Multi-Factor Authentication (MFA)
   - Require MFA for all accounts using mobile apps (e.g., Google Authenticator) or hardware tokens.
4. Regular Updates and Patching
   - Continuously patch operating systems, applications, and firmware to close known vulnerabilities. Disable unused services or protocols.
5. Backup and Disaster Recovery (BDR)
   - Maintain regular offline backups in a secure, offsite location. Test backup integrity frequently to ensure seamless restoration in case of an attack.

Ransomware Victims Industry-wise

Based on the analysis of ransomware attacks across various industries, the data highlights notable trends in attack distribution:

- Manufacturing (14.21%) emerged as the most targeted sector. This indicates the criticality of the manufacturing industry and the potential impact of disruptions in supply chains.
- Business Services (12.63%) experienced a substantial share of attacks, emphasising the persistent threat to organisations offering a broad range of professional services.
- Retail (8.95%) and Construction (7.89%) were heavily impacted, highlighting the vulnerability of industries with significant operational dependencies and customer-facing services.
- Insurance (7.37%), Healthcare (4.74%), and Finance (5.26%) also faced significant risks, underscoring the expansive reach of ransomware threats across industries that manage sensitive data or financial transactions.
- Telecommunications (2.63%), Government (3.16%), Hospitals (1.05%), and Real Estate (1.58%) further illustrate the diversity of sectors targeted, showing the critical need for cybersecurity resilience even in traditionally less digital industries.
- Smaller but critical sectors such as Industrial Machinery (1.05%), Agriculture (1.05%), Media & Internet (1.58%), Hospitality (2.11%), and Education (1.05%) were not spared, reflecting the pervasive nature of these attacks.
- Niche sectors like Law Firms (7.89%), Minerals & Mining (1.58%), Consumer Services (1.58%), and Energy (1.05%) highlight the broad targeting patterns that ransomware campaigns employ.
- Very small but notable percentages were observed in Membership Organisations (0.53%), Architecture (0.53%), Logistics Services (0.53%), and Electricity (0.53%), demonstrating that no sector is immune.

This analysis underscores the extensive reach of ransomware across industries, emphasising the urgent need for cross-sector collaboration, enhanced threat detection, and robust incident response plans. The broad targeting patterns demonstrate that all industries, regardless of size or digital reliance, must prioritise cybersecurity to mitigate risks effectively.

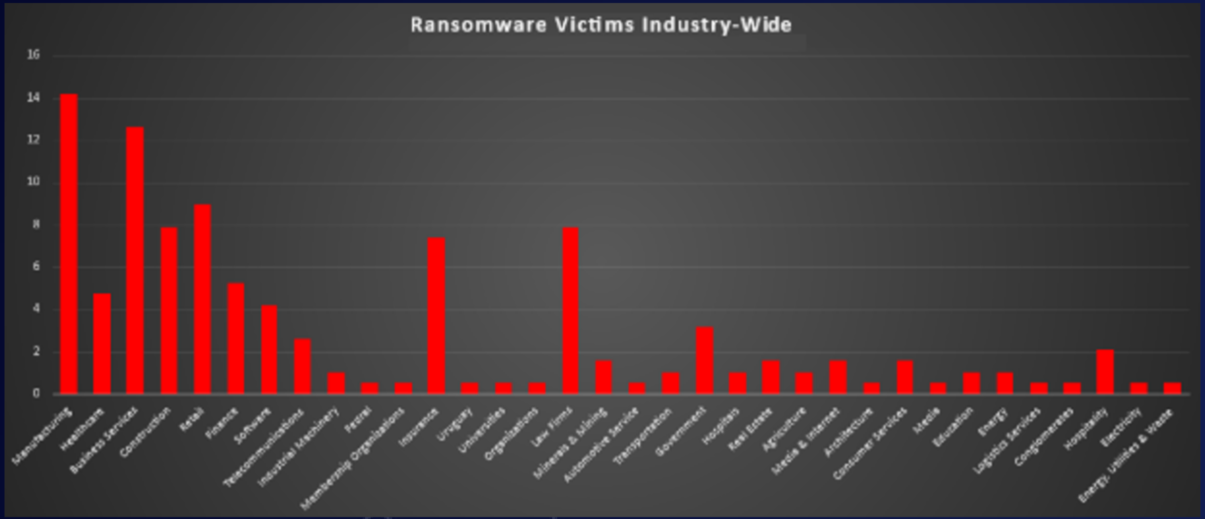


Figure 4: Industry-wise Ransomware Victims

Ransomware Victims Worldwide

A recent ransomware analysis reveals a striking 61.58% of global incidents targeted the United States, making it the hardest-hit country by far. Trailing behind, Canada and Australia each experienced 4.74% of attacks, reflecting notable vulnerabilities in these regions.

United Kingdom (3.16%), Brazil (2.11%), and Germany (2.11%) saw significant percentages of incidents, underscoring their exposure to ransomware threats. Meanwhile, countries such as Italy, India, and Spain contributed 1.58% each to the total, further illustrating the widespread geographical reach of ransomware attacks.

Other countries, including Saudi Arabia (1.05%), Sweden (1.05%), and Bolivia (1.05%), reported smaller shares of attacks. Even less frequently targeted nations like Paraguay (1.05%), Zambia (1.05%), and Namibia (0.53%) were not spared, highlighting the far-reaching nature of ransomware.

This analysis demonstrates the pervasive nature of ransomware, with North America bearing the brunt of these persistent threats. The high numbers in the United States emphasise the urgent need for enhanced cybersecurity measures in heavily targeted regions. Additionally, the data shows that no country, regardless of size or economic status, is immune to the risks posed by ransomware.

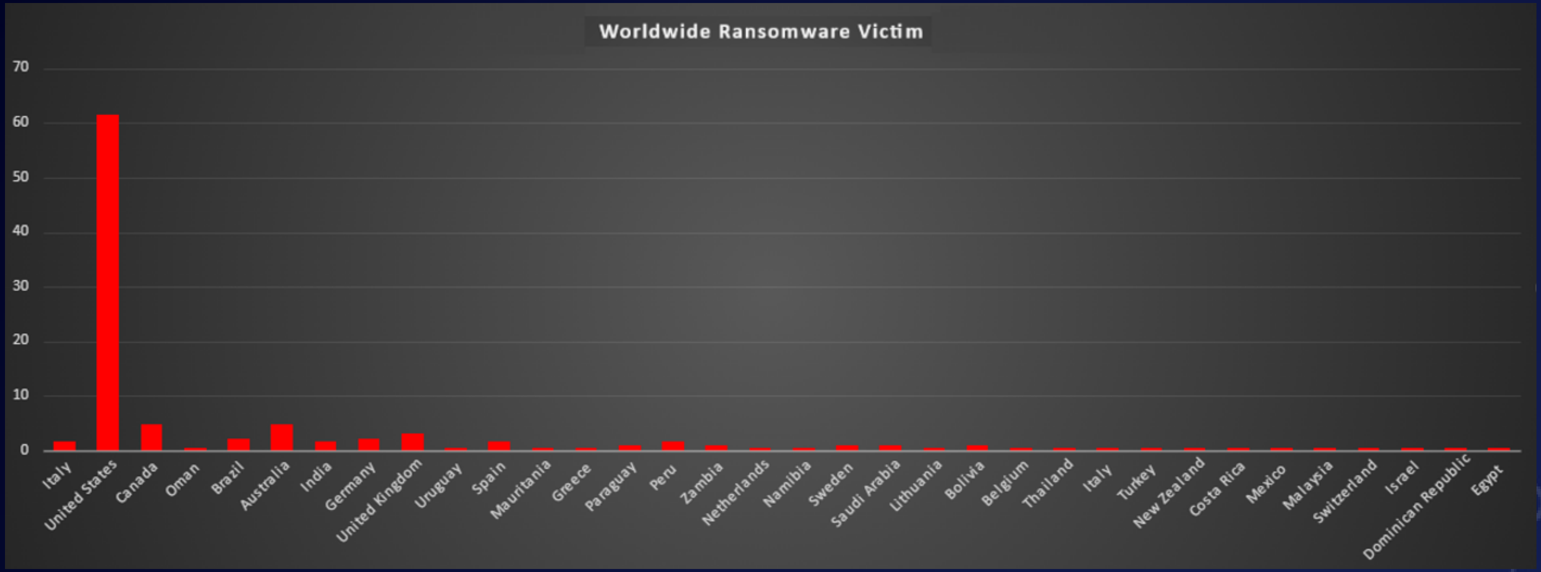


Figure 5: Ransomware Victims Worldwide