Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jul 30 - Aug 5, 2024

Report Summary:

- **New Threat Detection Added** – 2 (Zloader Malware and CHM Stealer)
- **New Threat Protections - 115**

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

1. Zloader Malware

Zloader is a sophisticated banking trojan that has evolved from the infamous Zeus malware Known for its modular architecture and adaptability, Zloader targets financial institutions and individuals by stealing banking credentials, online payment information, and personal data. It employs various techniques to evade detection, including obfuscation, anti-analysis measures, and polymorphic capabilities. This malware has been linked to significant financial losses and has become a persistent threat to both individuals and organisations.

Threats Protected: 13
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
Execution	T1059	Command and Scripting Interpreter
Persistence	T1574 T1574.002	Hijack Execution Flow DLL Side Loading
Privilege Escalation	T1574 T1574.002	Hijack Execution Flow DLL Side Loading
Defence Evasion	T1027 T1112	Obfuscated Files or Information Modify Registry
Credential Access	T1056 T1056.001	Input Capture Keylogging
Discovery	T1010 T1082 T1083 T1497	Application Window Discovery System Information Discovery File and Directory Discovery Virtualization/Sandbox Evasion
Command-and-Control	T1071	Application Layer Protocol

2. CHM Stealer

CHM Stealer is a type of malware that leverages Compiled HTML Help (CHM) files as a delivery mechanism. These files, often used for documentation, can be weaponised to contain malicious scripts or payloads. Once executed, CHM Stealers can steal sensitive information such as login credentials, browser data, and personal files. These threats are typically distributed through phishing emails or malicious downloads, enticing victims to open the CHM file. Due to their common file format and potential to bypass security measures, CHM Stealers pose a significant risk to unsuspecting users.

Threats Protected: 01
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
Execution	T1059	Command and Scripting Interpreter
	T1059.001	PowerShell
	T1064	Scripting
Privilege Escalation	T1055	Spawns Processes
	T1134	Access Token Manipulation
Defence Evasion	T1036	Masquerading
	T1055	Process Injection
	T1564	Hide Artifacts
Discovery	T1010	Application Window Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Collection	T1114	Email Collection
Command-and-Control	T1071	Application Layer Protocol

Known exploited vulnerabilities (Week 1 August 2024):

Vulnerability	CVSS	Description
CVE-2023-45249	9.8 (Critical)	Acronis Cyber Infrastructure (ACI) Insecure Default Password Vulnerability
CVE-2024-5217	9.2 (Critical)	ServiceNow Incomplete List of Disallowed Inputs Vulnerability
CVE-2024-4879	9.8 (Critical)	ServiceNow Improper Input Validation Vulnerability
CVE-2024-37085	7.2 (High)	VMware ESXi Authentication Bypass Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-august-2024/493

Updated Malware Signatures (Week 1 August 2024)

Threat	Description
HawkEye	A trojan and keylogger used to steal various account credentials
Nanocore	The Nanocore trojan, built on the .NET framework, has been the subject of multiple source code leaks, resulting in its widespread accessibility. Like other remote access trojans (RATs), Nanocore empowers malicious actors with complete system control, enabling activities such as video and audio recording, password theft, file downloads, and keystroke logging.
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 actively collects information on organisations globally affected by ransomware attacks from various sources, including the Dark Web. In the past week alone, our team uncovered new ransomware victims and updates on previous victims across 19 industries spanning 12 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

Dispossessor ransomware group stands out as the most prolific, having updated a significant number of victims (26%) distributed across multiple countries. In comparison, Ransomhub ransomware updated 15% of victims, in the past week. The following list provides the victim counts in percentages for these ransomware groups and a selection of others.

Name of Ransomware Group	Percentage of new Victims last week
Abyss-Data	1.72%
Akira	8.62%
Bianlian	3.45%
Black Suit	5.17%
Cactus	10.34%
Cicada330	1.72%
Darkvault	1.72%
Dispossessor	25.86%
Fog	1.72%
Killsec	3.45%
Metaencryptor	1.72%
Qilin	5.17%
Ra Group	1.72%
Ransomhub	15.52%
Rhysida	5.17%
Space Bears	5.17%
Stormous	1.72%

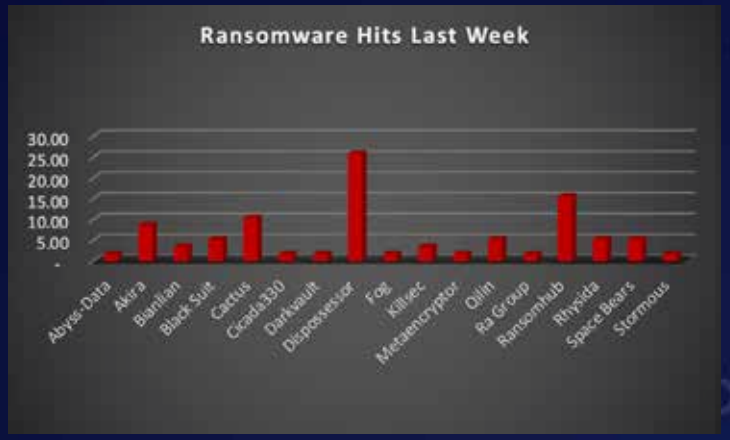


Figure 1: Ransomware Group Hits Last Week

Dispossessor Ransomware

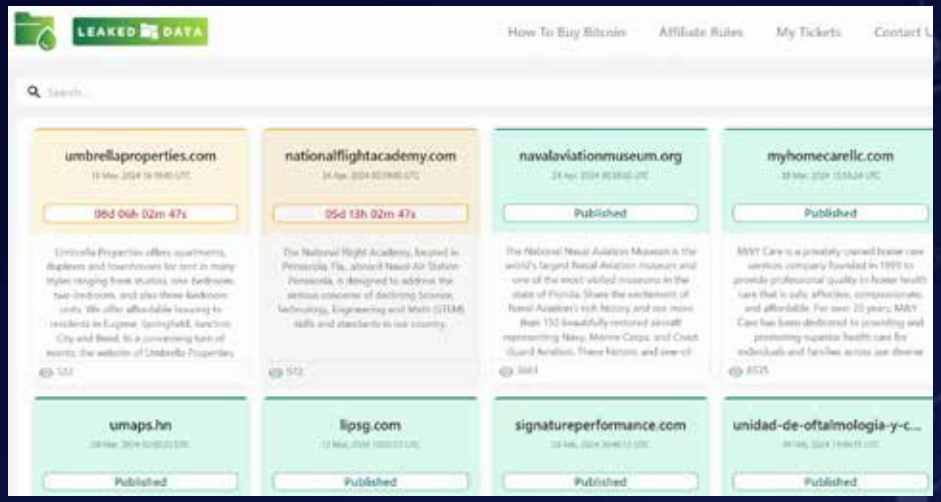
Emerging in late 2022, Dispossessor ransomware quickly made its mark as a formidable threat in the cybersecurity landscape. This malicious software employs a double extortion tactic, encrypting victims' data and threatening to leak it on the dark web unless a ransom is paid. While the exact origins of Dispossessor remain shrouded in mystery, security researchers believe it may be linked to a cybercriminal group operating out of Eastern Europe. This group's previous activities suggest a level of sophistication in malware development and deployment, making Dispossessor a particularly dangerous adversary.

TTPs:

Dispossessor ransomware doesn't rely solely on brute force. It possesses a diverse arsenal of tactics, techniques, and procedures (TTPs) to infiltrate and compromise systems stealthily. Here's a glimpse into its malicious toolkit:

- Phishing Attacks: Deceptive emails designed to trick users into clicking malicious links or downloading infected attachments are a common entry point. These emails often mimic egitimate business communications, making them more likely to be clicked.
- Exploiting Vulnerabilities: Dispossessor actively seeks out unpatched vulnerabilities in software and operating systems to gain unauthorised access to networks. This underscores the importance of keeping all software and systems updated with the latest security patches.
- Supply Chain Attacks: Dispossessor has shown a preference for targeting supply chains, compromising vendors and suppliers to gain access to a wider network of victims. This tactic allows attackers to reach a larger number of victims with a single intrusion.
- Living-off-the-Land Techniques: Like many malware strains, Dispossessor can utilise legitimate system administration tools for malicious purposes. This makes detection more challenging as these tools may appear as normal system activity.
- Data Exfiltration: Before encryption, Dispossessor often exfiltrates sensitive data like financial records, personal information, and intellectual property. This stolen data serves as additional leverage in extortion attempts, putting pressure on victims to pay the ransom.
- Strong Encryption: The malware utilises robust encryption algorithms to render files inaccessible. Decrypting them without the attacker's key is extremely difficult, if not impossible. This effectively cripples a victim's operations until a decision is made.

Data Leak Site: Dispossessor maintains a data leak site on the dark web where they list victims who haven't paid the ransom. This serves as a public shaming tactic and adds pressure on compromised organisations.



A Global Reach with Focused Targets

Dispossessor ransomware has demonstrated a global reach, targeting victims across various industries and geographies. While it has shown a preference for certain sectors, its impact can be felt worldwide.

- Healthcare Organisations: Hospitals and other healthcare providers have been frequent targets due to the sensitive nature of patient data and the potential disruption to critical services.
- Manufacturing Disruptions: Manufacturing companies across the globe have fallen victim to Dan0n, experiencing data breaches, operational disruptions, and potential production delays.
- Financial Institutions: The financial sector has also been targeted, with banks and credit unions facing potential data breaches and financial losses.

The emergence of Dan0n ransomware underscores the ever-evolving threat landscape of cybercrime. Its focus on supply chain attacks and the potential for significant disruptions highlights the need for organisations to prioritise robust cybersecurity measures. Here are some crucial steps organisations can take to mitigate the risk of Dan0n ransomware and similar threats:

- Third-Party Risk Management: Implement a comprehensive third-party risk management program to assess and monitor the security posture of vendors and suppliers.
- Supply Chain Visibility: Maintain visibility into your supply chain to identify potential risks and vulnerabilities.
- Regular Backups: Maintain secure, offline backups of critical data to facilitate recovery in case of a ransomware attack.
- Patch Management: Implement a rigorous patch management system to ensure all software and operating systems are updated with the latest security patches.
- Security Awareness Training: Educate employees on identifying phishing attempts and other social engineering tactics used by attackers. Regular training can significantly reduce the risk of human error leading to breaches.
- Endpoint Security Solutions: Deploy endpoint security solutions that can detect and prevent malware infections at the device level. These solutions can act as a first line of defence against Dan0n and other malware threats.
- Network Segmentation: Segmenting your network can limit the lateral movement of ransomware, potentially preventing it from spreading throughout your entire infrastructure.
- Incident Response Planning: Develop and regularly test an incident response plan to effectively respond to a ransomware attack and minimise damage. Having a plan in place ensures a more coordinated and efficient response during a crisis.

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
http://e27z5kd2rjsern2gpgukhcioysqlfquxgf7rxpvcwepxl4lfc736piyd.onion http://cybertube.video/web/index.html#!/details?id=0c3b52f6e73709725dc6e12b30b139d9&serverId=2be5e68176ff4f8fbb930fe66321ab72 http://e27z5kd2rjsern2gpgukhcioysqlfquxgf7rxpvcwepxl4lfc736piyd.onion/back/getallblogs	URLs (Onion)	Leak Site
https://dispossessor.com	URL (Clear Net)	Leak Site

In a comprehensive analysis of ransomware victims across 12 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 69% of victim updates in the past week. The following list provides a breakdown of the number and percentage of new ransomware victims per country, underscoring the persistent and concerning prevalence of ransomware attacks, with the USA particularly susceptible to these cybersecurity threats.

Industry	Victims Count (%)
Australia	1.72%
Belgium	1.72%
Brazil	1.72%
Bulgaria	1.72%
Canada	5.17%
France	1.72%
Mexico	1.72%
Peru	1.72%
Portugal	1.72%
Romania	1.72%
UK	10.34%
USA	68.97%

Figure 3: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 19 different industries worldwide. Notably, Manufacturing bore the brunt of the attacks in the past week, accounting for 17% of victims each.

Industry	Victims Count (%)
Agriculture	1.72%
Business Services	12.07%
Cities, Towns & Municipalities	1.72%
Construction	12.07%
Consumer Services	1.72%
Education	8.62%
Energy, Utilities & Waste Treatment	1.72%
Finance	1.72%
Healthcare	10.34%
IT	5.17%
Legal Services	5.17%
Manufacturing	17.24%
Media & Internet	3.45%
Metals & Mining	1.72%
Organisations	3.45%
Real Estate	1.72%
Retail	6.90%
Telecom	1.72%
Transportation	1.72%

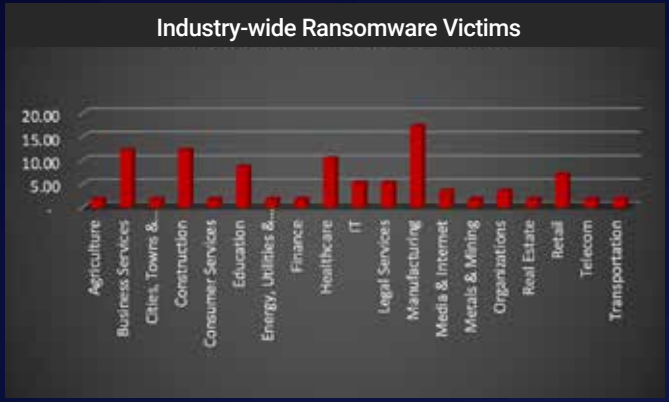


Figure 4: Industry-wide Ransomware Victims