Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 28 - June 3, 2024

Report Summary:

- **New Threat Detection Added** – 3 (AsyncRAT Malware, Koi Stealer and Iluria Stealer)
- **New Threat Protections - 320**

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

1. AsyncRAT Malware

AsyncRAT, short for Asynchronous Remote Access Trojan, lurks as a double-edged sword. Publicly available as an open-source remote administration tool, its functionalities like keylogging and remote desktop control can be attractive for legitimate remote access. However, its stealthy nature and ease of customisation make it a favourite among cybercriminals. AsyncRAT silently infects systems through phishing emails and exploits, stealing credentials, and financial data, and even deploying ransomware. Its modular design allows attackers to tailor it for specific targets. Despite disclaimers on its source code, AsyncRAT's prevalence in malicious campaigns far outweighs its intended use.

Rules Created: 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
Defence Evasion	T1497 T1000	Virtualization/Sandbox Evasion Anti-Debugging
Persistence	T1053 T1547	Scheduled Task/Job Boot or Logon AutoStart Execution
Command-and-Control	T1056	Network File Transfer
Collection	T1056 T1083	Keylogging File System Discovery

2. Koi Stealer

Koi Stealer, a cunning cyber threat, operates in two parts: Koi Loader and Koi Stealer itself. This one-two punch infiltrates systems through phishing tactics. Once in, Koi Loader silently downloads the stealer component. Koi Stealer then works like a digital vacuum, snatching your browsing history, login credentials, cookies, and even information about your system like hardware specs and installed applications. This stolen data goldmine is then uploaded to a command-and-control server, potentially leaving you vulnerable to identity theft, hijacked accounts, and further malware infections. Koi Stealer's stealth and information-siphoning techniques make it a serious threat, underlining the importance of caution with suspicious emails and robust security measures to protect your data.

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: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1049	Phishing Email
Delivery	T1040	Malicious File
Execution	T1064	Scripting
Privilege Escalation	T1055	Process Injection
Discovery	T1082 T1087	System Information Discovery Account Discovery
Command-and-Control	T1071 T1095	Application Layer Protocol Non-Application Layer Protocol

3. Iluria Stealer

Iluria Stealer, a descendant of the notorious Nikki Stealer, lurks on the dark web, targeting Discord users. This malware masquerades as an innocuous file but harbours malicious intent. Once installed, it utilises its multi-stage attack to pilfer your Discord token, a key that unlocks your account. Iluria then injects itself into Discord's core, silently monitoring your activity. This digital eavesdropper can steal your login credentials, and messages, and even capture any two-factor authentication attempts. Armed with this stolen information, attackers can hijack your account, spam your contacts, or even target them with further scams. Iluria Stealer's ability to bypass initial detection makes it a sneaky threat. Staying vigilant against suspicious downloads and enabling two-factor authentication on Discord are crucial steps to defend yourself against this information-hungry malware.

Rules Created: 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	T1047	Windows Management Instrumentation
	T1059	Command and Scripting Interpreter
Persistence	T1547.001	Registry Run Key/ Startup Folder
	T1574.002	DLL Side-Loading
Privilege Escalation	T1055	Process Injection
	T1547.001	Registry Run Key/ Startup Folder
Defence Evasion	T1036	Masquerading
	T1055	Process Injection
Discovery	T1012	Query Registry
	T1057	Process Discovery
	T1018	Remote System Discovery
	T1082	System Information Discovery
Command-and-Control	T1073	Encrypted Channel
	T1071	Application Layer Protocol

Known exploited vulnerabilities (Week 5 May 2024):

Vulnerability	CVSS	Description
CVE-2024-5274	8.8 (High)	Google Chromium V8 Type Confusion Vulnerability
CVE-2024-4978	8.7 (High)	Justice AV Solutions (JAVS) Viewer Installer Embedded Malicious Code Vulnerability
CVE-2024-1086	7.8 (High)	Linux Kernel Use-After-Free Vulnerability
CVE-2024-24919	8.6 (High)	Check Point Quantum Security Gateways Information Disclosure Vulnerability

Updated Malware Signatures (Week 5 May 2024)

Threat	Description
Nanocore	The Nanocore trojan, built on the .NET framework, has been the subject of multiple source code leaks, resulting in its widespread accessibility. Similar to 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.
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.
QuasarRat	A remote access trojan that was made available to the public as an open-source project. Once installed on a victim's machine, it is capable of keylogging, data and screen capturing among other things. It is also known to be highly customisable depending on the threat actor's intended need.
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.

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 21 different industries spanning 22 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

Medusa ransomware group stand out as the most prolific, having updated a significant number of victims (21%) distributed across multiple countries. In comparison, LockBit3.0 ransomware updated 18% 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
8Base	6.58%
Akira	10.53%
Bianlian	3.95%
Black Suit	1.32%
Blackout	1.32%
Clop	3.95%
Dragonforce	1.32%
Handala	3.95%
Hunters	2.63%
Inc Ransom	2.63%
Lockbit3	18.42%
Mallox	1.32%
Medusa	21.05%
Monti	2.63%
Play	6.58%
Qilin	1.32%
Qiulong	1.32%
Ransomhub	5.26%
Red ransomware	1.32%
Rhysida	1.32%
Space Bears	1.32%

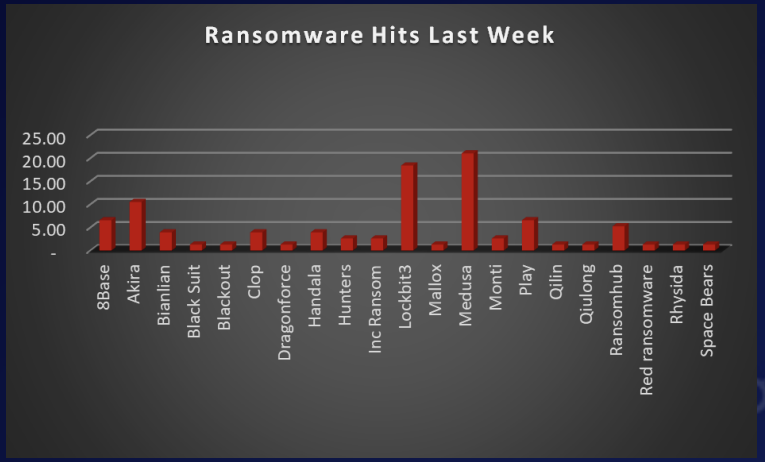


Figure 1: Ransomware Group Hits Last Week

Medusa Ransomware

Emerging in late 2021, Medusa ransomware has swiftly become a formidable foe in the cybersecurity landscape. This ruthless malware employs a double extortion tactic, crippling victims by encrypting their data and threatening to leak it on the dark web if ransom demands aren't met. While the exact origins of Medusa remain shrouded in mystery, security researchers believe it may be linked to a cybercriminal group known as UNC7885. This group has a history of utilising ransomware and other malware strains, suggesting a level of experience behind the development and deployment of Medusa.

Tactics, Techniques, and Procedures (TTPs):

Medusa isn't a one-trick pony. It possesses a diverse arsenal of tactics, techniques, and procedures (TTPs) to infiltrate and compromise systems. Here's a glimpse into its malicious toolkit:

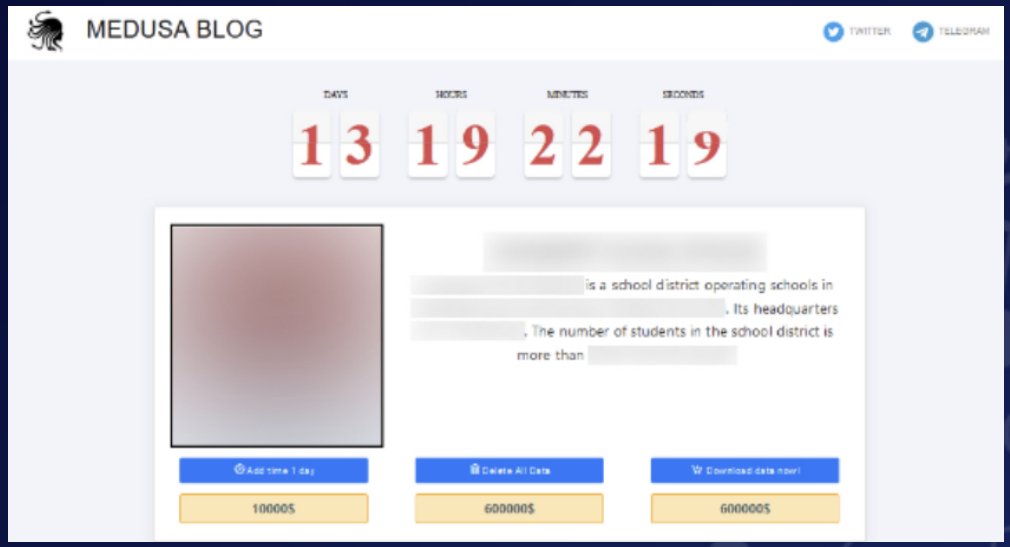
- Phishing Attacks: Deceptive emails designed to trick users into clicking malicious links or downloading infected attachments are a common entry point. These emails may appear to be from legitimate sources, such as trusted colleagues, delivery companies, or even financial institutions.
- Exploiting Vulnerabilities: Medusa actively seeks out unpatched vulnerabilities in software and operating systems to gain unauthorised access to networks. This underscores the importance of keeping all systems and software updated with the latest security patches.
- Remote Desktop Protocol (RDP) Exploitation: Medusa can exploit weaknesses in RDP configurations to gain access to a system. RDP allows remote access to a computer, and misconfigured settings can create a vulnerability for attackers.
- Brute-Force Attacks: In some instances, Medusa may attempt to gain access through brute-force attacks, where it systematically tries different combinations of usernames and passwords until it cracks the login credentials.
- Lateral Movement: Once a foothold is established on a single system, Medusa can leverage various tools to move laterally across a network. This allows it to infect additional devices and escalate privileges, potentially compromising critical systems.
- Living-off-the-Land Techniques: Similar to other malware, Medusa 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, Medusa 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.
- Robust Encryption: The malware utilises strong 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.

Famous Fallouts:

Medusa demonstrates a lack of geographical bias, targeting victims worldwide. Here are some examples of its reach:

- Critical Infrastructure: Security researchers have observed Medusa targeting critical infrastructure sectors like power grids and transportation systems. A successful attack on such infrastructure could have devastating consequences.
- Healthcare Organisations: Hospitals and other healthcare providers have also fallen victim to Medusa attacks. The disruption caused by encrypted medical records and operational systems can severely impact patient care.
- Educational Institutions: Schools and universities haven't been spared either. Data breaches involving student information or disruption of educational services can have serious consequences.

Leak Site: Medusa ransomware maintains a leak site on the dark web where they threaten to publish stolen data if the ransom is not paid.



Medusa's Ransom notes

The emergence of Medusa ransomware underscores the ever-evolving threat landscape of cybercrime. Its use of readily available tools, combined with its focus on double extortion tactics, highlights the need for organisations to prioritise robust cybersecurity measures.

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1204.002	User Execution
Defence Evasion	T1562.001 T1070.004	Impair Defences: Disable or Modify Tools Indicator Removal: File Deletion
Discovery	T1083	File and Directory Discovery
Impact	T1486	Data Encrypted for Impact

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
2919a13b964c8b006f144e3c8cc6563740d3d242f44822c8c44dc0db38137ccb 85ebf6330039de69dbef1a4860274f21d8b980adb9c3d8385873c5d697c61685 e514935ab07b29ca1ee9eedaf699de202ada70e29b4fc4618908b8ca8b3f83ef 290eb4666848172a03c9c5123c004278647e8f5445a7d4e9c29a9ecc58c1b329 4654f4cbd9e3910f4901493b9774d978060f1c9a9489612b66d66ee61667f60f 4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270	Hash	Medusa Ransomware
Medusakxxtp3uo7vusntvubnytaph4d3amxivbggl3hnhpk2nmus34yd[.]onion medusaxko7jxtrojdkxo66j7ck4q5tgktf7uqsqyfry4ebnxlcbkccyd[.]onion	URLs (Onion)	Leak Site
Disability[.]su Franchessko[.]top Ircnews[.]wang Kjnsfiosgjnlorgiko[.]ru Mhforum[.]biz Missyiurfound[.]bid scam-financial[.]org sgsdgsdger[.]ru troyamylove[.]gdn wooow1[.]ru youframegood[.]ru	URLs	Command-and-Controls

In a comprehensive analysis of ransomware victims across 22 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 47% 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 (%)
Argentina	1.32%
Australia	2.63%
Bangladesh	1.32%
Belgium	1.32%
Canada	7.89%
France	3.95%
Germany	1.32%
Kuwait	1.32%
India	1.32%
Ireland	1.32%
Israel	3.95%
Italy	2.63%
Japan	2.63%
Mexico	1.32%
Russia	1.32%
Senegal	1.32%
Singapore	1.32%
Spain	2.63%
Sweden	1.32%
UAE	1.32%
UK	9.21%
USA	47.37%

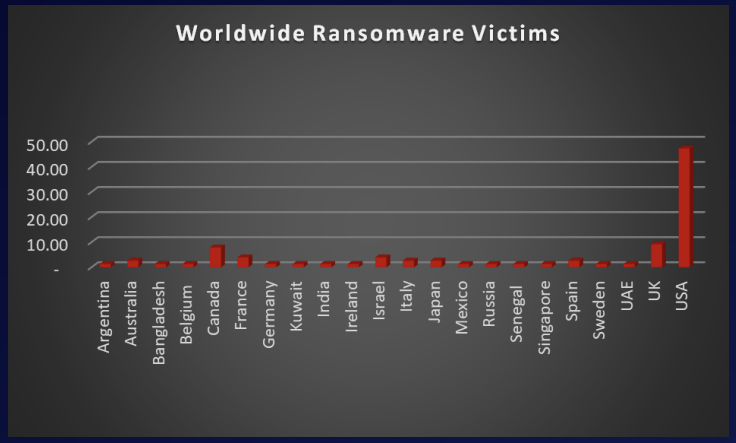


Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 21 different industries worldwide. Notably, Manufacturing bore the brunt of the attacks in the past week, accounting for 20% of victims. There are a few key reasons why the manufacturing sector is a prime target for ransomware groups:

- High Disruption Potential: Manufacturing relies heavily on interconnected systems and just-in-time production. A ransomware attack can grind operations to a halt, causing significant financial losses due to production delays and lost revenue. This pressure to get back online quickly can make manufacturers more willing to pay the ransom.

- Vulnerable Legacy Systems: Many manufacturers use legacy control systems (OT) that haven't been updated for security. These older systems often lack robust security features, making them easier targets for attackers to exploit.

- Limited Cybersecurity Investment: Traditionally, cybersecurity might not have been a top priority for some manufacturers compared to production efficiency. This lack of investment in security awareness training and robust security protocols leaves them exposed.

- Valuable Data: Manufacturing facilities often hold valuable intellectual property (IP) and trade secrets. Ransomware groups may not only disrupt operations but also threaten to leak this sensitive data if the ransom isn't paid.

- Success Breeds Success: The high payout potential from past attacks on manufacturers incentivises ransomware groups to continue targeting them.

The table below delineates the most recent ransomware victims, organised by industry, shedding light on the sectors grappling with the significant impact of these cyber threats.

Industry	Victims Count (%)
Agriculture	1.35%
Business Services	10.81%
Cities, Town & Municipalities	1.35%
Construction	4.05%
Consumer Services	4.05%
Education	6.76%
Energy, Utilities & Waste Treatment	4.05%
Finance	1.35%
Government	1.35%
Healthcare	5.41%
Hospitality	4.05%
Insurance	1.35%
IT	6.76%
Legal Services	2.70%
Manufacturing	20.27%
Media & Internet	2.70%
Organisation	4.05%
Real Estate	4.05%
Retail	9.46%
Telecom	4.05%
Transportation	2.70%

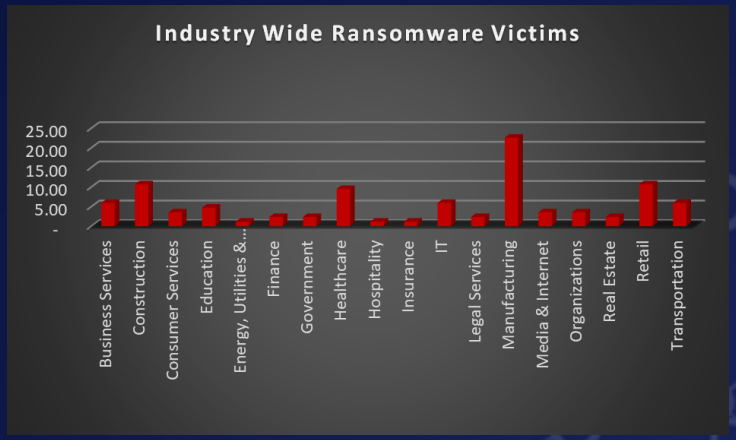


Figure 5: Industry-wise Ransomware Victims