Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 17 - 23, 2024

Report Summary:

- **New Threat Detection Added** – 4 (RAZR Ransomware, XWorm Malware, Cthulu Stealer and Konni RAT)
- **New Threat Protections - 228**

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

1. RAZR Ransomware

RAZR Ransomware is a highly destructive malware that encrypts files on infected systems, rendering them inaccessible until a ransom is paid. This ransomware is known for its aggressive tactics and rapid spread, often targeting businesses and organisations of all sizes. RAZR employs various techniques to infiltrate systems, including phishing emails, exploit kits, and remote desktop protocol (RDP) brute-forcing. Once inside, it quickly scans the network for valuable data and encrypts it using a strong encryption algorithm. To mitigate the risk of RAZR Ransomware infections, organisations should implement robust cybersecurity measures, such as regular backups, strong password policies, and network segmentation. Additionally, staying updated with the latest security patches and educating employees about phishing threats can help prevent successful attacks.

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	T1129	Shared Module
Persistence	T1547 T1574 T1574.002	Boot or Logon AutoStart Execution Hijack Execution Flow DLL Side Loading
Privilege Escalation	T1574 T1574.002	Hijack Execution Flow DLL Side Loading
Defence Evasion	T1027 T1497	Obfuscated Files or Information Virtualization/Sandbox Evasion
Discovery	T1082 T1083	System Information Discovery Files and Directory Discovery
Collection	T1005 T1114	Data from Local System Email Collection
Command-and-Control	T1071 T1095	Application Layer Protocol Non-Application Layer Protocol

2. XWorm Malware

XWorm is a sophisticated worm malware known for its rapid propagation and ability to spread through various network protocols. This worm exploits vulnerabilities in network devices, such as routers and servers, to gain unauthorised access and infect other systems. Once on a network, XWorm can disrupt operations, steal data, and launch further attacks. Its ability to self-propagate and evade detection makes it a significant threat to individuals and organisations. To protect against XWorm and other worm threats, it is essential to keep network devices updated with the latest security patches, implement strong network segmentation, and monitor network traffic for suspicious activity.

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
Initial Access	T1091	Replication Through Removable Media
Execution	T1129	Shared Modules
Persistence	T1547.001	Registry Run Keys / Startup Folder
Privilege Escalation	T1055 T1134	Process Injection Access Token Manipulation
Defence Evasion	T1027	Obfuscated Files or Information

3. Cthulu Stealer

Cthulu Stealer is a potent information-stealing malware that has emerged as a significant threat in the cyber landscape. This malware targets sensitive data, which includes login credentials, credit card information, cryptocurrency wallet details, and personal files. Cthulu Stealer's advanced capabilities, such as keylogging, screen capturing, and file exfiltration, make it a formidable tool for cybercriminals. Often distributed through phishing emails or malicious downloads, Cthulu Stealer poses a significant risk to individuals and organisations. Effective cybersecurity measures, including vigilant email practices, strong password management, and regular software updates, are essential to protect against this and other malware threats.

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 T1059.002	Command and Scripting Interpreter AppleScript
Defence Evasion	T1070 T1070.004 T1564 T1564.001	Indicator Removal File Deletion Hide Artifacts Hidden Files and Directories
Discovery	T1082	System Information Discovery
Command-and-Control	T1071 T1095	Application Layer Protocol Non-Application Layer Protocol

4. Konni RAT

Konni RAT is a sophisticated Remote Access Trojan (RAT) that has emerged as a significant threat in the cyber landscape. This malware grants attackers extensive control over compromised systems, enabling them to steal data, execute commands, and establish persistent backdoors. Konni RAT's modular architecture allows for customisation, making it a versatile tool for cybercriminals. The malware's ability to evade detection, combined with its affiliation with a well-resourced threat actor, makes Konni RAT a significant concern for organisations worldwide. Effective cybersecurity measures, including vigilant email practices, strong password management, and regular software updates, are essential to protect against this and other malware threats.

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
Initial Access	T1566	Phishing
	T1566.001	Spear Phishing
Execution	T1059	Command and Scripting Interpreter
	T1204.002	Malicious File
	T1064	Scripting
Defence Evasion	T1027	Obfuscated Files or Information
Discovery	T1082	System Information Discovery
	T1083	Files and Directory Discovery
Collection	T1113	Screen Capture
	T1005	Data from Local System
	T1048	Exfiltration on Alternative Protocol
Command-and-Control	T1071	Application Layer Protocol
	T1095	Non-Application Layer Protocol
	T1573	Encrypted Channel

Known exploited vulnerabilities (Week 3 September 2024):

Vulnerability	CVSS	Description
CVE-2024-6670	9.8 (Critical)	Progress WhatsUp Gold SQL Injection Vulnerability
CVE-2024-43461	8.8 (High)	Microsoft Windows MSHTML Platform Spoofing Vulnerability:
CVE-2014-0502	8.8 (High)	Adobe Flash Player Double Free Vulnerability
CVE-2013-0648	8.8 (High)	Adobe Flash Player Code Execution Vulnerability
CVE-2013-0643	8.8 (High)	Adobe Flash Player Incorrect Default Permissions Vulnerability
CVE-2014-0497	9.8 (Critical)	Adobe Flash Player Integer Underflow Vulnerability
CVE-2020-14644	9.8 (Critical)	Oracle WebLogic Server Remote Code Execution Vulnerability
CVE-2022-21445	9.8 (Critical)	Oracle ADF Faces Deserialisation of Untrusted Data Vulnerability
CVE-2020-0618	8.8 (High)	Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability
CVE-2024-27348	9.8 (Critical)	Apache HugeGraph-Server Improper Access Control Vulnerability
CVE-2024-8963	9.1 (Critical)	Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-september-2024/507

Updated Malware Signatures (Week 3 September 2024)

Threat	Description
Zeus	Also known as Zbot, this malware is primarily designed to steal banking credentials.
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.
Vidar	A stealer designed to collect sensitive data from infected machines. It usually targets Windows-based machines and is spread through email attachments or downloads from compromised websites.

Ransomware Report

The Red Piranha Team actively monitors the dark web and other sources to identify organisations globally affected by ransomware attacks. In the past week alone, we have uncovered new ransomware victims and updates on existing cases across 22 industries in 28 countries. This highlights the pervasive nature of ransomware, demonstrating its ability to target organisations of all sizes and sectors worldwide.

RansomHub ransomware group significantly increased its attacks in the past three weeks, claiming a 21% decrease in victims compared to the previous week (15%). It is the most prolific ransomware group, with victims distributed across multiple countries. Play and Medusa ransomware updated their victim count by 10% each in the past. 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
3AM	1.94%
Abyss-Data	1.94%
Arcus Media	4.85%
Bianlian	2.91%
Black Suit	1.94%
Cactus	6.80%
Cicada3301	0.97%
Clop	0.97%
Dispossessor	0.97%
Everest	1.94%
Fog	1.94%
Handala	1.94%
Hunters	5.83%
Inc Ransom	1.94%
Killsec	1.94%
Lockbit3	1.94%
Lynx	0.97%
Medusa	9.71%
Meow	2.91%
Orca	1.94%
Play	9.71%
Qilin	2.91%
Ransomexx	0.97%
RansomHub	21.36%
Rhysida	1.94%
Stormous	0.97%
Trinity	0.97%
Valencia Leaks	4.85%

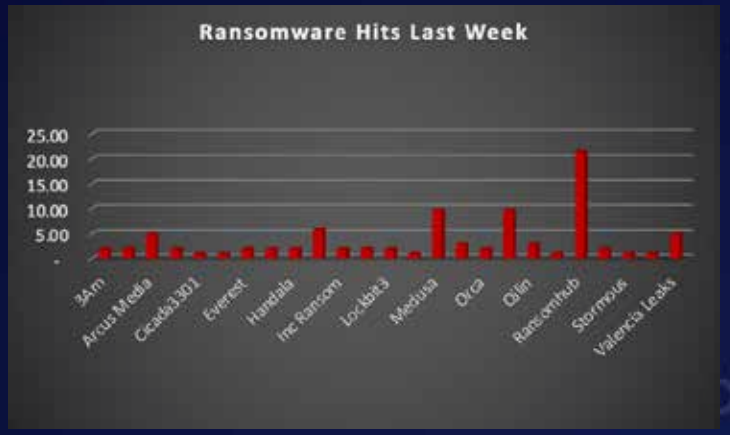

Figure 1: Ransomware Group Hits Last Week

Fog Ransomware

Emerging in the latter half of 2022, Fog Ransomware quickly established itself as a formidable threat in the cybercrime landscape. This stealthy malware employs a double extortion tactic, encrypting victims' data and threatening to leak it on the dark web if ransom demands aren't met. While the exact origins of Fog remain shrouded in some 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 Fog a particularly dangerous adversary.

TTPs:

Fog ransomware doesn't rely solely on brute force. 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 often mimic legitimate business communications, making them more likely to be clicked.
- Exploiting Unpatched Vulnerabilities: Fog 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.
- Remote Desktop Protocol (RDP) Exploitation: Like other ransomware strains, Fog 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.
- Supply Chain Attacks: Fog 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.
- Lateral Movement: Once a foothold is established on a single system, Fog can utilise various tools to move laterally across a network. This allows it to infect additional devices, escalate privileges, and potentially compromise critical systems.
- Data Exfiltration: Before encryption, Fog 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: Fog ransomware 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.

Figure 2: Screenshot of Leak Site used by Fog Ransomware

Ransom Note

Fog ransomware, a notorious cyber threat, employs a deceptive tactic in its ransom notes. Rather than demanding a ransom outright, it presents itself as a "bidon_readme.txt" or "readme.txt". This facade aims to manipulate victims into believing they have a chance to recover their encrypted data for a fee.

However, this is a deceptive ploy. Once a victim pays the ransom, there's no guarantee that their data will be decrypted. In many cases, victims are left with no option but to rebuild their systems and data from backups.

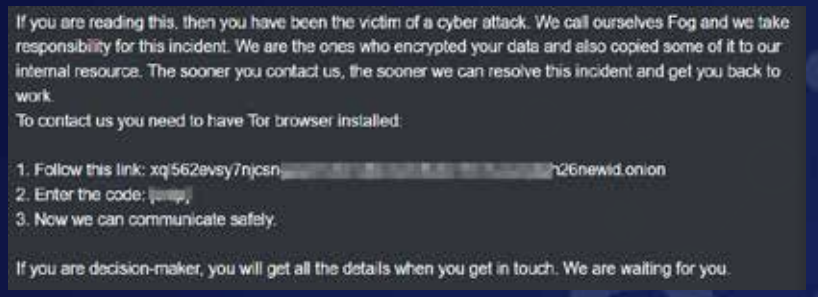

Figure 3: Screenshot of Ransom Note used by Fog Ransomware

A Global Reach with Focused Targets

Fog ransomware has demonstrated a global reach, targeting victims across various industries and geographies. Here are some examples of its operations and the impact it has caused:

- 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 Fog, 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 Fog 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.

Tactic	Technique ID	Technique Name
Initial Access	T1133	External Remote Services
	T1078	Valid Accounts
Discovery	T1046	Network Service Discovery
	T1135	Network Share Discovery
Lateral Movement	T1021	Remote Services
	T1570	Lateral Tool Transfer
Credential Access	T1003	OS Credential Dumping
	T1555	Credentials from Password Stores
	T1110	Brute Force
Persistence	T1136	Create Account
Execution	T1059	Command and Scripting Interpreter
	T1569	System Services
Defence Evasion	T1562	Impair Defences
	T1550	Use Alternate Authentication Material
	T1078	Valid Accounts
Impact	T1486	Data Encrypted for Impact
	T1490	Inhibit System Recovery
	T1489	Service Stop

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxps://xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid.onion/ hxxp://xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd.onion hxxp://xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd.onion/posts	URLs (Onion)	Leak Site
f7c8c60172f9ae4dab9f61c28ccae7084da90a06 507b26054319ff31f275ba44ddc9d2b5037bd295 e1fb7d15408988df39a80b8939972f7843f0e785 83f00af43df650fda2c5b4a04a7b31790a8ad4cf 44a76b9546427627a8d88a650c1bed3f1cc0278c eeafa71946e81d8fe5ebf6be53e83a84dcca50ba 763499b37aacd317e7d2f512872f9ed719aacae1 3477a173e2c1005a81d042802ab0f22cc12a4d55 90be89524b72f330e49017a11e7b8a257f975e9a	Hash	Malicious Files

A recent analysis of ransomware victims across 28 countries reveals the United States as the most heavily impacted nation, with a staggering 58% increase in victim reports over the past week. Notably, Canada has also experienced a significant rise once again, with victim reports of 7% last week. The following list details the number and percentage of new ransomware victims per country, highlighting the pervasive and concerning nature of ransomware attacks, particularly in the United States.

Industry	Victims Count (%)
Australia	0.97%
Bangladesh	0.97%
Belgium	0.97%
Brazil	2.91%
Canada	6.80%
China	0.97%
Colombia	0.97%
Denmark	0.97%
France	0.97%
Georgia	0.97%
Germany	0.97%
India	0.97%
Israel	1.94%
Italy	1.94%
Japan	0.97%
Luxembourg	0.97%
Malaysia	0.97%
Mauritius	0.97%
Mexico	0.97%
Paraguay	0.97%
Philippines	0.97%
Spain	4.85%
Taiwan	0.97%
Tunisia	0.97%
Turkey	2.91%
UAE	0.97%
UK	0.97%
USA	58.25%

Figure 4: Ransomware Victims Worldwide

Further analysis reveals that ransomware has impacted 22 industries worldwide. The manufacturing sector remains a significant target, accounting for 20% of victims in the past week Retail and Construction sectors got 12% of victims each in the past week.

Industry	Victims Count (%)
Agriculture	1.94%
Business Services	8.74%
Cities, Towns & Municipalities	0.97%
Construction	11.65%
Consumer Services	3.88%
Education	1.94%
Energy, Utilities & Waste Treatment	1.94%
Finance	8.74%
Government	0.97%
Healthcare	4.85%
Hospitality	2.91%
Insurance	0.97%
IT	0.97%
Legal Services	3.88%
Manufacturing	20.39%
Media & Internet	1.94%
Metals & Mining	1.94%
Organisations	1.94%
Real Estate	1.94%
Retail	11.65%
Telecom	2.91%
Transportation	2.91%

Figure 5: Industry-wide Ransomware Victims

Here are some crucial steps organisations can take to mitigate the risk of 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 Cloak 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.