Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 6 - 12, 2024

Report Summary:

- **New Threat Detection Added** – 2 (DeerStealer and Moonstone Sleet APT)
- **New Threat Protections - 367**

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

1. DeerStealer

DeerStealer is a relatively new information-stealing malware that has gained notoriety for its deceptive distribution methods. Often disguised as legitimate applications like Google Authenticator, it targets unsuspecting users through fake ads and malicious downloads. Once installed, DeerStealer harvests sensitive data including login credentials, credit card information, and personal details. Its ability to mimic trusted software and its rapid spread underscores the evolving tactics employed by cybercriminals to compromise systems and steal valuable information.

Threats Protected: 17
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	Link function
Persistence	T1574	Hijack Execution Flow
	T1574.002	DLL Side Loading
Privilege Escalation	T1574	Hijack Execution Flow
	T1574.002	DLL Side Loading
Defence Evasion	T1027	Obfuscated Files or Information
	T1562	Impair Defences
	T1562.001	Disable or Modify Tools
Credential Access	T1003	OS Credentials Dumping
	T1539	Steal Web Session Cookie
	T1552	Unsecured Credentials
	T1552.002	Credentials in Files
Discovery	T1010	Application Window Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1497	Virtualisation/Sandbox Evasion
Collection	T1005	Data from the Local System
Command-and-Control	T1071	Application Layer Protocol
	T1573	Encrypted Channel

2. Moonstone Sleet APT

Moonstone Sleet is a North Korean-linked advanced persistent threat (APT) group targeting a broad spectrum of sectors, including aerospace, education, and software development. Differentiating itself from other North Korean APTs, Moonstone Sleet uniquely combines espionage and financial gain objectives. Employing a mix of traditional and innovative techniques, this group leverages social engineering, trojanised software, and even a malicious game to infiltrate target systems. Their recent deployment of custom ransomware demonstrates their evolving tactics and increasing financial motivation.

Threats Protected: 03
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
	T1129	Shared Modules
Persistence	T1547	Boot or Logon AutoStart Execution
	T1547.009	Shortcut Modification
	T1574.002	DLL Side Loading
Privilege Escalation	T1547	Boot or Logon AutoStart Execution
	T1547.009	Shortcut Modification
Defence Evasion	T1027	Obfuscated Files or Information
	T1112	Modify Registry
Discovery	T1010	Application Window Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Collection	T1056	Input Capture
	T1056.001	Keylogging
	T1115	Clipboard Data
Command-and-Control	T1071	Application Layer Protocol

Known exploited vulnerabilities (Week 2 August 2024):

Vulnerability	CVSS	Description
CVE-2018-0824	8.8 (High)	Microsoft COM for Windows Deserialisation of Untrusted Data Vulnerability
CVE-2024-32113	9.8 (Critical)	Apache OFBiz Path Traversal Vulnerability
CVE-2024-36971	7.8 (High)	Android Kernel Remote Code Execution Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-august-2024/494

Updated Malware Signatures (Week 2 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 26 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

RansomHub ransomware group stands out as the most prolific, having updated a significant number of victims (15%) distributed across multiple countries. In comparison, Meow ransomware updated 13% 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
3Am	2.33%
Abyss-Data	1.16%
Black Suit	2.33%
Cactus	9.30%
Cicada3301	2.33%
Darkvault	1.16%
Dispossessor	2.33%
Dragonforce	2.33%
Embargo	1.16%
Everest	3.49%
Fog	3.49%
Inc Ransom	1.16%
Killsec	2.33%
Lockbit3	9.30%
Lynx	2.33%
Mad Liberator	2.33%
Medusa	4.65%
Meow	13.95%
Play	4.65%
Ransomexx	1.16%
RansomHouse	5.81%
RansomHub	15.12%
Rhysida	3.49%
Space Bears	2.33%

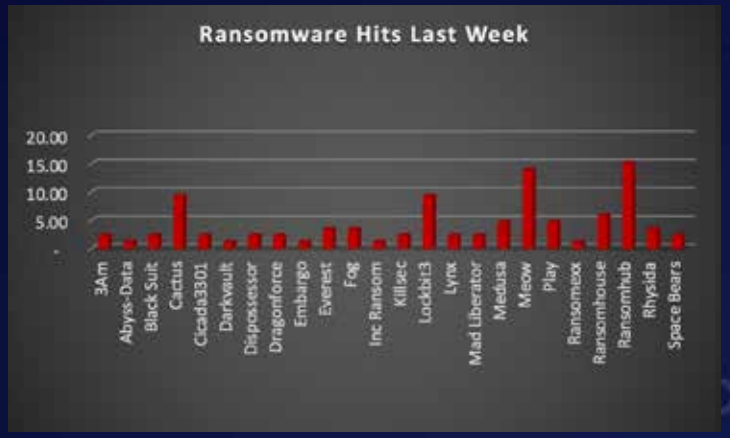


Figure 1: Ransomware Group Hits Last Week

RansomHouse Ransomware

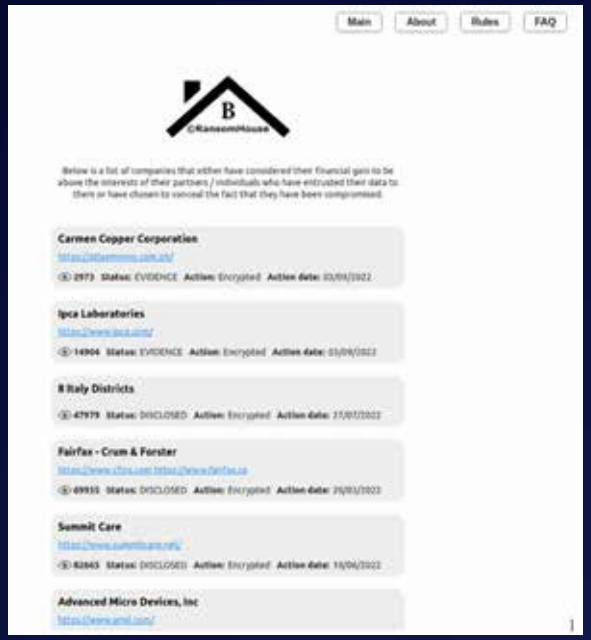
Emerging in the latter half of 2023, RansomHouse ransomware quickly gained notoriety for its aggressive tactics and the significant impact it inflicted on its victims. This malware strain employs a double extortion model, encrypting victims' data and threatening to leak it on the dark web unless a ransom is paid. While the exact origins of RansomHouse 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 RansomHouse a formidable adversary.

TTPs:

RansomHouse doesn't operate like a random act of theft. It employs a calculated approach, utilising 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 Vulnerabilities: RansomHouse 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, RansomHouse 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: RansomHouse 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, RansomHouse 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, RansomHouse 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: RansomHouse 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

RansomHouse 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 RansomHouse, 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 RansomHouse 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 RansomHouse 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 RansomHouse 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.

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://xw7au5pnwtl6lozbsudkmyd32n6gnqdngitjdppybudan3x3pjgpmpid.onion hxxp://zohlm7ahjwegcedoz7lrdrti7bvpofymcayotp744qhx6gjmxbuo2yid.onion	URLs (Onion)	Leak Site
https://t.me/Rhouse_News	Telegram Channel	
https://twitter.com/RHouseNews	X- Handle	
188.126.89.20:23762 89.208.107.158	Domains	C2

In a comprehensive analysis of ransomware victims across 26 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 56% 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	2.33%
Bahrain	1.16%
Brazil	2.33%
Canada	3.49%
China	1.16%
France	4.65%
Germany	2.33%
India	2.33%
Italy	1.16%
Japan	1.16%
Kuwait	1.16%
Malaysia	1.16%
Mexico	1.16%
Netherlands	1.16%
New Zealand	1.16%
Pakistan	3.49%
Peru	1.16%
Philippines	1.16%
Portugal	1.16%
Seychelles	1.16%
Singapore	1.16%
Spain	1.16%
Sweden	1.16%
Taiwan	1.16%
UK	3.49%
USA	55.81%

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 26% of victims each.

Industry	Victims Count (%)
Agriculture	1.16%
Business Services	3.49%
Construction	8.14%
Consumer Services	2.33%
Education	8.14%
Energy, Utilities & Waste Treatment	2.33%
Finance	4.65%
Government	4.65%
Healthcare	4.65%
Hospitality	3.49%
IT	3.49%
Legal Services	3.49%
Manufacturing	25.58%
Media & Internet	3.49%
Metals & Mining	1.16%
Real Estate	2.33%
Retail	6.98%
Telecom	3.49%
Transportation	6.98%

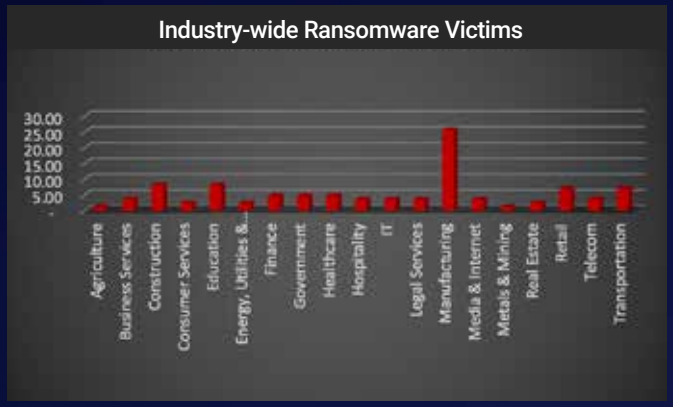


Figure 4: Industry-wide Ransomware Victims