Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 03 - 09, 2024

Report Summary:

- **New Threat Detection Added** – 2 (Angry Stealer and Diamotrix Clipper)
- **New Threat Protections - 120**

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

1. Angry Stealer

Angry Stealer is a potent information-stealing malware that has emerged as a significant threat in the cyber landscape. This malware targets a wide range of sensitive data, including login credentials, credit card information, cryptocurrency wallet details, and personal files. Angry 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, Angry Stealer poses a significant risk to both 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
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

2. Diamotrix Clipper

Diamotrix Clipper is a sophisticated malware known for its ability to intercept and modify financial transactions. This clipper, often associated with organised crime groups, targets online banking and cryptocurrency platforms. By modifying transaction details, Diamotrix can redirect funds to unauthorised accounts, resulting in significant financial losses for victims. The malware's advanced evasion techniques and persistence make it a challenging threat to detect and mitigate. Effective cybersecurity measures, including vigilant online banking practices, strong password management, and regular software updates, are essential to protect against Diamotrix Clipper and other financial malware.

Threats Protected: 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	T1566	This malware reaches users via phishing sites.
Execution	T1204	The user needs to execute the file downloaded from the phishing site manually.
Execution	T1059.001	Uses PowerShell Script to load the Clipper binary from the Registry.
Persistence	T1053	Creates a Task Scheduler entry.
Defence Evasion	T1036.008 T1112 T1027.011	Downloads file disguised as a legitimate application. Files are obfuscated using a Pure crypter. The loader binary is stored in the registry.
Collection	T1115 T1113	Monitors clipboard data and replaces crypto address with their address. Takes a screenshot of the victim's screen and Exfiltrates it.
Exfiltration	T1567	Uses discord webhook to exfiltrate data.

Known exploited vulnerabilities (Week 1 September 2024):

Vulnerability	CVSS	Description
CVE-2024-7262	9.3 (Critical)	Kingsoft WPS Office Path Traversal Vulnerability
CVE-2021-20124	7.5 (High)	Draytek VigorConnect Path Traversal Vulnerability
CVE-2021-20123	7.5 (High)	Draytek VigorConnect Path Traversal Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-september-2024/502

Updated Malware Signatures (Week 1 September 2024)

Threat	Description
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.
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.
BlankGrabber Stealer	BlankGrabber stealer malware is a type of malicious software designed to steal sensitive information from an infected system. This information can include login credentials, passwords, browser cookies, stored credit card information, and other personal data. The malware typically operates by extracting this data from web browsers, applications, and system files where such information is commonly stored.

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 19 industries in 27 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 this week, claiming a 31% increase in victims compared to the previous week (11%). It stands out as the most prolific ransomware group, with victims distributed across multiple countries. Monti ransomware updated its victim count by 10% 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	0.94%
Bianlian	5.66%
Black Suit	6.60%
Cactus	5.66%
Cicada3301	2.83%
Dispossessor	0.94%
El Dorado	1.89%
Everest	0.94%
Hunters	4.72%
Inc Ransom	1.89%
Killsec	2.83%
Lockbit3	5.66%
Lynx	2.83%
Mad Liberator	0.94%
Meow	4.72%
Monti	9.43%
Play	3.77%
Qilin	0.94%
RansomHouse	1.89%
RansomHub	31.13%
Rhysida	2.83%
Trinity	0.94%

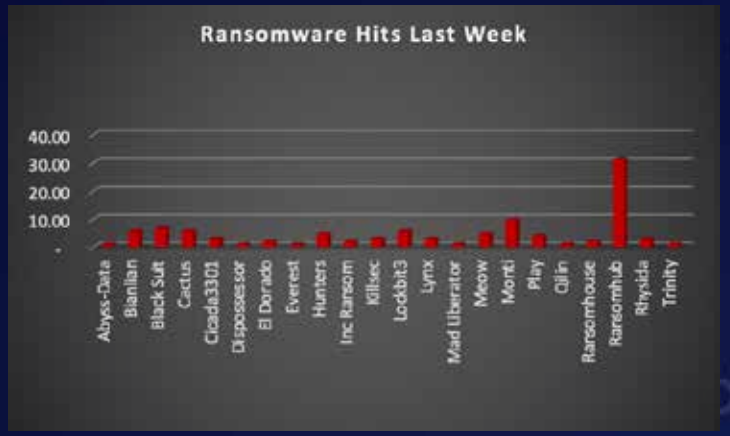

Figure 1: Ransomware Group Hits Last Week

Monti Ransomware

Monti ransomware, a formidable threat in the cybercrime landscape, first emerged in late 2021. This malicious software 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 Monti 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 Monti a particularly dangerous adversary.

TTPs:
Monti 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 legitimate business communications, making them more likely to be clicked.
- Exploiting Unpatched Vulnerabilities: Monti 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, Monti 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: Monti 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, Monti 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, Monti 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: Monti 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.

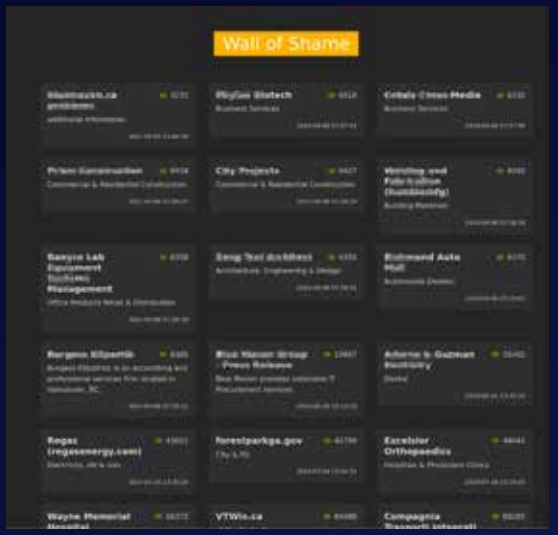

Figure 2: Screenshot of Leak Site used by Monti Ransomware

Ransom Note

Monti 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 Monti Ransomware

A Global Reach with Focused Targets

Monti 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 worldwide have fallen victim to Monti, 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 economic losses.

The emergence of Monti 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
Execution	T1059.001	PowerShell
	T1569.002	Service Execution
Persistence	T1547.001	Registry Run Keys / Startup Folder
Privilege Escalation	T1548	Abuse Elevation Control Mechanism
Defence Evasion	T1112	Modify Registry
	T1055	Process Injection
Credential Access	T1558.004	AS-REP Roasting
	T103.001	LSASS Memory
Discovery	T1069.002	Domain Groups
	T1482	Domain Trust Discovery
	T1018	Remote System Discovery
	T1518.001	Security Software Discovery
	T1518	Software Discovery
	T1082	System Information Discovery
Collection	T1560	Archive Collected Data
Command-and-Control	T1090	Proxy
Impact	T1486	Data Encrypted for Impact
	T1490	Inhibit System Recovery

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid.onion/	URLs (Onion)	Leak Site
9aa1f37517458d635eae4f9b43cb4770880ea0ee171e7e4ad155bbdee0cbe732 df492b4cc7f644ad3e795155926d1fc8ece7327c0c5c8ea45561f24f5110ce54 78517fb07ee5292da627c234b26b555413a459f8d7a9641e4a9fcc1099f06a3d b45fe91d2e2340939781d39daf606622e6d0b9ddacd8425cb8e49c56124c1d56 158dcb26239a5db7a0eb67826178f1eaa0852d9d86e59afb86f04e88096a19bc 702099b63cb2384e11f088d6bc33afbd43a4c91848f393581242a6a17f1b30a0 f1c0054bc76e8753d4331a881cdf9156dd8b812a a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbc74ef	Hash	Malicious Files

A recent analysis of ransomware victims across 27 countries reveals the United States as the most heavily impacted nation, with a staggering 50% increase in victim reports over the past week. Notably, Canada has also experienced a significant rise, with victim reports jumping from 5% to over 12% in the same period. 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	2.83%
Belgium	2.83%
Canada	12.26%
Czech Republic	0.94%
Dominican Republic	0.94%
East Timor	0.94%
Fiji	0.94%
France	0.94%
Germany	0.94%
Guatemala	0.94%
India	0.94%
Italy	2.83%
Jamaica	0.94%
Japan	2.83%
Luxembourg	0.94%
Mexico	1.89%
Netherlands	0.94%
New Zealand	0.94%
Oman	0.94%
Romania	0.94%
Singapore	0.94%
South Korea	0.94%
Spain	1.89%
Switzerland	0.94%
UAE	0.94%
UK	4.72%
USA	50.94%

Figure 4: Ransomware Victims Worldwide

Further analysis reveals that ransomware has impacted 19 industries worldwide. The manufacturing sector remains a significant target, accounting for 20% of victims in the past week, despite a slight increase in attacks on business services (16%), construction (16%), and retail (13%).

Industry	Victims Count (%)
Business Services	16.04%
Construction	16.04 %
Consumer Services	1.89%
Education	4.72%
Energy, Utilities & Waste Treatment	0.94%
Finance	1.89%
Government	2.83%
Healthcare	4.72%
Hospitality	3.77%
Insurance	1.89%
IT	2.83%
Legal Service	0.94%
Manufacturing	19.81%
Media & Internet	0.94%
Organisations	1.89%
Real Estate	2.83%
Retail	13.21%
Telecom	1.89%
Transportation	0.94%

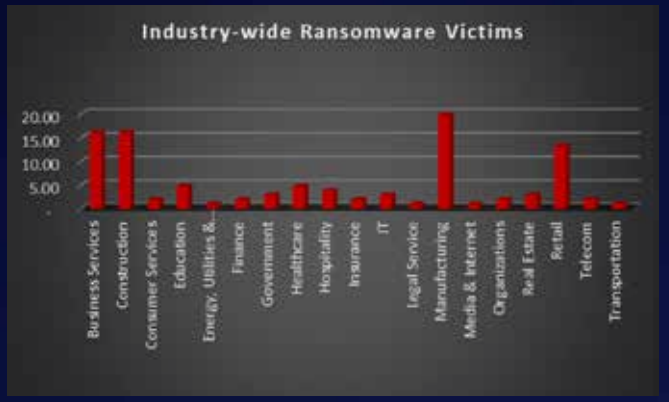

Figure 5: Industry-wide Ransomware Victims

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.