Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 23 - 29, 2024

Report Summary:

- **New Threat Detection Added** – 2 (AsyncRAT and Daolpu Stealer)
- **New Threat Protections - 85**

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

1. AsyncRAT

AsyncRAT, a Remote Access Trojan (RAT), is a versatile and dangerous malware tool that has gained significant notoriety. Originally released as an open-source project, it has evolved into a potent weapon for cybercriminals. With its ability to steal credentials, download additional malware, and provide remote control over infected systems, AsyncRAT poses a serious threat. Its modular architecture and open-source availability have contributed to its rapid spread and adaptation by various threat actors. From financially motivated cybercriminals to state-sponsored hacking groups, AsyncRAT has been employed in a wide range of malicious campaigns, making it a persistent challenge for cybersecurity professionals.

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
Persistence	T1547	Boot or Logon Autostart Execution
Privilege Escalation	T1547.009	Shortcut Modification
Defence Evasion	T1027 T1112	Obfuscated Files or Information Modify Registry
Credential Access	T1056 T1056.001	Input Capture Keylogging
Discovery	T1010 T1012 T1082 T1083	Application Window Discovery Query Registry System Information Discovery File and Directory Discovery
Collection	T1056 T1056.001 T1115 T1125	Input Capture Keylogging Clipboard Data Video Capture

2. Daolpu Stealer

Daolpu Stealer is a relatively new information-stealing malware that emerged in 2024. Initially spread through phishing campaigns disguised as a Microsoft recovery tool, Daolpu targets web browsers to steal credentials and cookies. It's known for its aggressive behaviour, forcibly terminating Chrome processes before collecting data. This malware is particularly concerning due to its potential to compromise a wide range of online accounts, from social media to banking. While still under investigation, Daolpu's rapid emergence highlights the persistent threat of information-stealing malware and the importance of robust cybersecurity measures.

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	T1204	User Execution
Credential Access	T1555	Credentials from Password Stores
Command-and-Control	T1071.001	Application Layer Protocol: WEB Protocols
Exfiltration	T1041	Exfiltration of C2 Channel

Known exploited vulnerabilities (Week 4 July 2024):

Vulnerability	CVSS	Description
CVE-2024-39891	5.3 (Medium)	Twilio Authy Information Disclosure Vulnerability
CVE-2012-4792	9.3 (Critical)	Microsoft Internet Explorer Use-After-Free Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-july-2024/489

Updated Malware Signatures (Week 4 July 2024)

Threat	Description
CoinMiner	This malicious software installs and runs cryptocurrency mining applications.
Trojan Miner	This malicious software installs and runs cryptocurrency mining applications.
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.

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.

Dan0n ransomware group stands out as the most prolific, having updated a significant number of victims (13%) distributed across multiple countries. In comparison, Medusa ransomware updated 10% 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	0.83%
Akira	7.44%
Arcus Media	0.83%
Bianlian	3.31%
Black Suit	1.65%
Blackbasta	0.83%
Brain Cipher	4.13%
Cactus	1.65%
Cicada3301	4.13%
Cloak	0.83%
Clop	0.83%
Daixin	0.83%
Dan0N	13.22%
Darkvault	0.83%
Dispossessor	7.44%
Dragonforce	3.31%
Everest	1.65%
Fog	1.65%
Handala	2.48%
Inc Ransom	3.31%
Lockbit3	1.65%
Mad Liberator	1.65%
Medusa	8.26%
Monti	1.65%
Play	6.61%
Qilin	2.48%
Ra Group	2.48%
Ransomhouse	4.13%
Ransomhub	7.44%
Rhysida	1.65%
Space Bears	0.83%

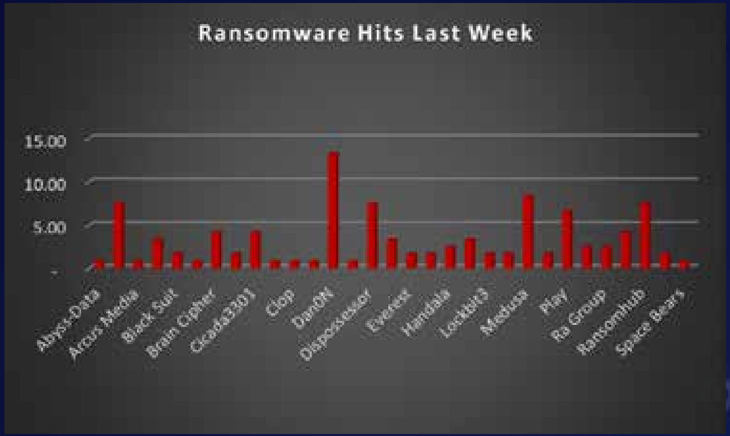


Figure 1: Ransomware Group Hits Last Week

Dan0n Ransomware

Emerging in the latter half of 2022, Dan0n ransomware, with its seemingly innocuous name, belies its malicious intent. This cyber threat 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 Dan0n remain shrouded in mystery, security researchers believe it may be linked to a cybercriminal group operating out of Eastern Europe. The group's previous activities suggest a level of sophistication in malware development and deployment, making Dan0n a formidable adversary.

Tactics, Techniques, and Procedures (TTPs):

Dan0n ransomware doesn't rely solely on brute force. It possesses a diverse arsenal of 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 banks, logistics companies, or even colleagues.

- Exploiting Vulnerabilities: Dan0n 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: Similar to other ransomware strains, Dan0n 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.

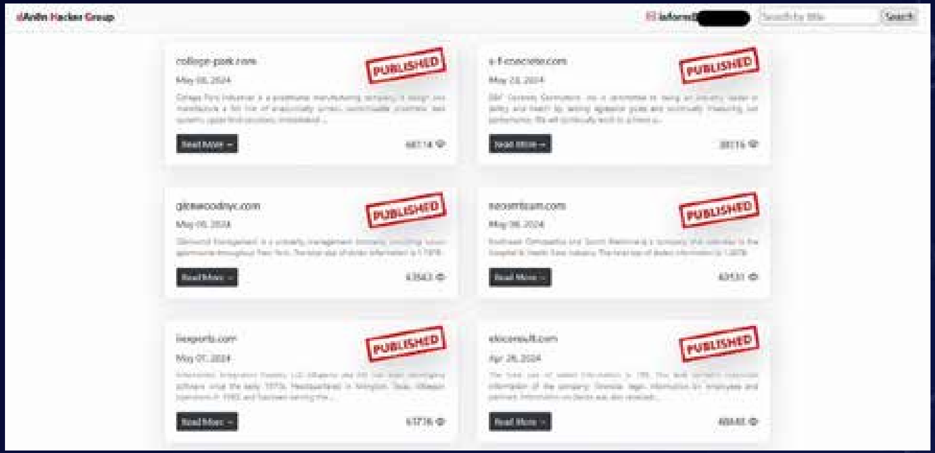
- Supply Chain Attacks: Dan0n has demonstrated a preference for targeting supply chains, compromising vendors and suppliers to gain access to their customers' networks. This tactic allows attackers to reach a wider range of victims with a single intrusion.

- Living-off-the-Land Techniques: Like many malware strains, Dan0n can utilise legitimate system administration tools for malicious purposes. This makes detection more challenging as these tools may appear as normal system activity. Learn more on LOTL Techniques.

- Data Exfiltration: Before encryption, Dan0n 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: Dan0n 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.



dAn0n Hacker Group

informa[redacted] Search by title Search

college-park.com
May 08, 2024
[illegible]
Read More →
68714

a-f-concrete.com
May 23, 2024
[illegible]
Read More →
38116

glenwoodnyc.com
May 09, 2024
[illegible]
Read More →
43543

neoortteam.com
May 08, 2024
[illegible]
Read More →
43131

liexports.com
May 07, 2024
[illegible]
Read More →
63776

ebiconsult.com
Apr 28, 2024
[illegible]
Read More →
40848

A Global Reach with Focused Targets

Dan0n 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 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.

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
	T1566	Phishing
Execution	T1129	Shared Modules
Defence Evasion	T1027	Obfuscated Files or Information
	T1497	Virtualization/Sandbox Evasion
Discovery	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1497	Virtualization/Sandbox Evasion
	T1518.001	Security Software Discovery
Lateral Movement	T1080	Taint Shared Content
Collection	T1056	Input Capture
Command-and-Control	T1071	Application Layer Protocol
	T1573	Encrypted Channel
Impact	T1486	Data Encrypted for Impact

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://2c7nd54guzi6xhjyqrj5kdkrq2ngm2u3e6oy4nfhn3wm3r54ul2utiqd.onion/	URLs (Onion)	Leak Site
hxxps://dan0n.com	URL (Clear Net)	Leak Site
inform@dan0n.com	Email	
Blackmail	Extortion Types	
Direct Extortion		
Double Extortion		
Elicit Cyber Insurance		
Extortion Timeout		
Free Data Leaks		
Regulator Complaint		
Victim Client Communication		
Victim Employee Communication		

In a comprehensive analysis of ransomware victims across 26 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 64% 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	1.65%
Belgium	0.83%
Brazil	1.65%
Canada	5.79%
China	2.48%
Croatia	0.83%
Czech Republic	0.83%
Denmark	0.83%
Germany	1.65%
Hungary	0.83%
Indonesia	0.83%
Ireland	0.83%
Isreal	1.65%
Italy	1.65%
Japan	0.83%
Malta	0.83%
Netherlands	3.31%
Pakistan	0.83%
Romania	0.83%
Saudi Arabia	0.83%
Singapore	1.65%
South Africa	0.83%
Sweden	1.65%
UK	0.83%
Ukraine	0.83%
USA	64.46%

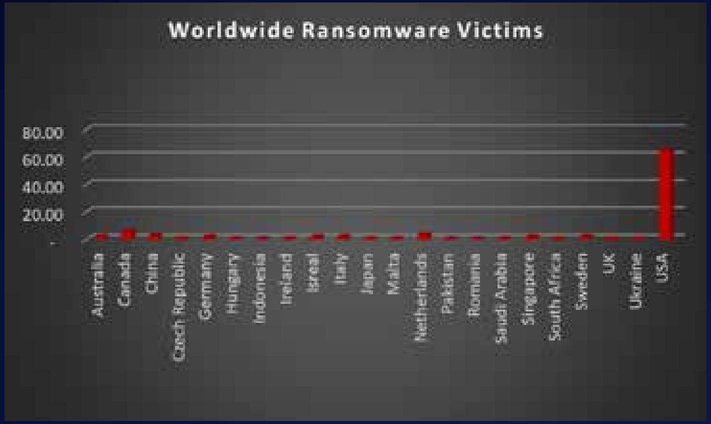


Figure 3: Ransomware Victims Worldwide

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 19% of victims each.

Industry	Victims Count (%)
Business Services	14.05%
Construction	11.57%
Consumer Services	3.31%
Energy, Utilities & Waste Treatment	3.31%
Finance	3.31%
Government	3.31%
Healthcare	2.48%
Hospitality	4.96%
Insurance	4.13%
IT	7.44%
Legal Service	3.31%
Manufacturing	19.83%
Media & Internet	3.31%
Metals & Mining	1.65%
Organisation	2.48%
Real Estate	2.48%
Reta	0.83%
Retail	5.79%
Transportation	2.48%

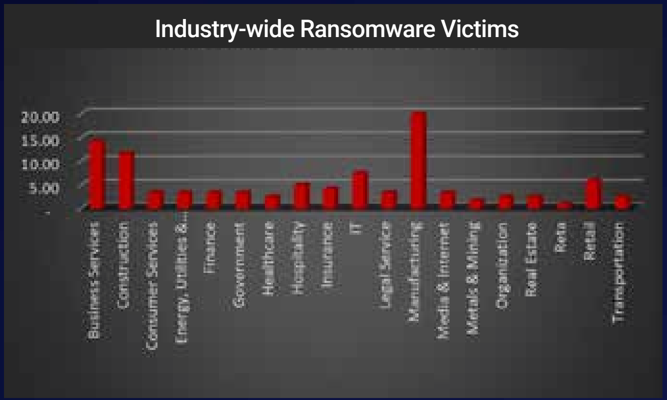


Figure 4: Industry-wide Ransomware Victims