Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

June 11 - 17, 2024

Report Summary:

- **New Threat Detection Added** – 2 (PCRat Malware and Earth Krahang APT)
- **New Threat Protections - 347**

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

1. PCRat Malware

PCRat is a malware known as a Remote Access Trojan (RAT). With its source code freely available online, it is a favourite among attackers for taking control of victim's computers. PCRat is a close relative to the Gh0st RAT family, sharing similar ways of communicating with its Command-and-Control centre. This malware allows attackers to do a bunch of harmful things like stealing files, spying on keystrokes, and even launching new attacks from the infected machine. Security researchers have seen PCRat being used by malware like BabyShark, further amplifying its reach. Since the source code is public, antivirus software is constantly updated to detect and remove PCRat.

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	T1059	Command and Scripting Interpreter
Persistence	T1547.001 T1574.002	Registry Run Key/ Startup Folder DLL Side-Loading
Privilege Escalation	T1055 T1547.001	Process Injection Registry Run Key/ Startup Folder
Defence Evasion	T1055	Process Injection
Discovery	T1057 T1082	Process Discovery System Information Discovery
Command-and-Control	T1073 T1071	Encrypted Channel Application Layer Protocol

2. Earth Krahang APT

Earth Krahang is a sneaky Advanced Persistent Threat (APT) group that has been around since at least 2022. They target governments around the world, aiming to steal sensitive information through spying. Their favourite tactic is spear phishing, where they send emails that look legitimate but actually contain malicious attachments or links. If you click on one of these, they can exploit weaknesses in your computer's software to install nasty tools like Cobalt Strike and XDealer. These tools give them remote access to your machine, letting them steal your data and potentially use your computer to launch attacks on others. Experts think Earth Krahang might be connected to Chinese actors, but they operate independently. There is no known easy way to stop them other than good security practices. Be super careful about the emails you open, and make sure your software is always up to date with the latest security patches.

Rules Created: 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
Initial Access	T1190	Exploit Public-Facing Application
	T1566.001	Phishing: Spear phishing Attachment
	T1199	Trusted Relationship
	T1078	Valid Accounts
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1203	Exploitation for Client Execution
	T1047	Windows Management Instrumentation
Persistence	T1543.003	Create or Modify System Process: Windows Service
	T1133	External Remote Services
	T1053.005	Scheduled Task/Job: Scheduled Task
	T1505.003	Server Software Component: Web Shell
Privilege Escalation	T1068	Exploitation for Privilege Escalation
	T1078.003	Valid Accounts: Local Accounts
Defence Evasion	T1140	Deobfuscate/Decode Files or Information
	T1656	Impersonation
	T1112	Modify Registry
Discovery	T1057	Process Discovery
	T1033	System Owner/User Discovery
	T1007	System Service Discovery
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols
	T1573	Encrypted Channel: Symmetric Cryptography
	T1105	Ingress Tool Transfer
	T1572	Protocol Tunnelling

Known exploited vulnerabilities (Week 2 June 2024):

Vulnerability	CVSS	Description
CVE-2024-4577	9.8 (Critical)	PHP-CGI OS Command Injection Vulnerability
CVE-2024-4610	5.5 (Medium)	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability
CVE-2024-4358	9.8 (Critical)	Progress Telerik Report Server Authentication Bypass by Spoofing Vulnerability
CVE-2024-26169	7.8 (High)	Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability
CVE-2024-32896	7.8 (High)	Android Pixel Privilege Escalation Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-june-2024/476

Updated Malware Signatures (Week 2 June 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.
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 18 industries spanning 19 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

Play ransomware group stands out as the most prolific, having updated 26% of victims across multiple countries. In comparison, Cactus, Dragonforce, Eraleign (APT73), and Ransomhub ransomware updated 6% of victims each, 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
Akira	3.85%
Arcus Media	1.28%
Bianlian	2.56%
Black Suit	2.56%
Blackbasta	2.56%
Cactus	6.41%
Clop	1.28%
Darkvault	2.56%
Dragonforce	6.41%
Eraleign (Apt73)	6.41%
Everest	5.13%
Handala	1.28%
Hunters	2.56%
Inc Ransom	5.13%
Lockbit3	2.56%
Monti	1.28%
Play	26.92%
Qilin	3.85%
Ransomhub	6.41%
Red Ransomware	1.28%
Rhysida	1.28%
Team Underground	2.56%
Trinity	3.85%

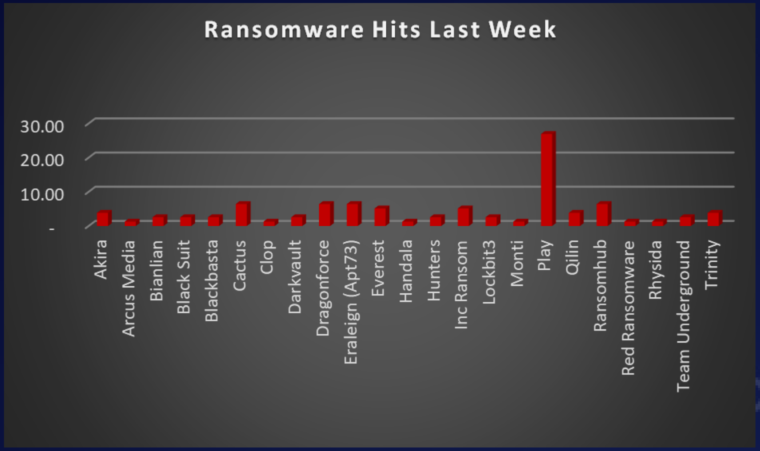


Figure 1: Ransomware Group Hits Last Week

Cactus Ransomware

First detected in the wild around March 2023, Cactus ransomware swiftly established itself as 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 are not met. While the exact origins of Cactus remain shrouded in some mystery, security researchers believe it may be linked to a Malaysian hacktivist group of the same name. However, the technical capabilities showcased by Cactus ransomware suggest that it leverages the leaked codebase of LockBit Black, a notorious ransomware group known for its effectiveness.

Tactics, Techniques, and Procedures (TTPs):

Cactus ransomware does not rely on brute force alone. It possesses a diverse arsenal of tactics, techniques, and procedures (TTPs) to infiltrate and compromise systems. Here are some of the most common methods employed:

1. Phishing Attacks
Deceptive emails designed to trick users into clicking malicious links or downloading infected attachments are a frequent entry point. These emails may appear to be from legitimate sources such as banks, logistics companies, or even colleagues.

2. Exploiting Unpatched Vulnerabilities
Cactus 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. Here are some recently exploited vulnerabilities by the Cactus Ransomware group, based on credible security sources:

- VPN vulnerabilities: A key element of Cactus' attack strategy seems to be targeting vulnerabilities in Virtual Private Network (VPN) appliances. Reports suggest they may have exploited flaws in Fortinet VPN devices, but other VPN vendors could potentially be vulnerable as well.
- Qlik Sense vulnerabilities: Security researchers have observed Cactus exploiting vulnerabilities within Qlik Sense, a popular data analytics platform. These vulnerabilities might grant attackers initial access to a system.
- Lateral Movement: Once a foothold is established on a single device, Cactus can utilise various tools to move laterally across a network. This allows it to infect additional devices and escalate privileges, potentially compromising critical systems.

3. Living-off-the-Land Techniques
Like other malware strains, Cactus can utilise legitimate system administration tools for malicious purposes. This makes detection more challenging as these tools may appear as normal system activity.

4. Data Exfiltration
Before encryption, Cactus 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.

5. 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.

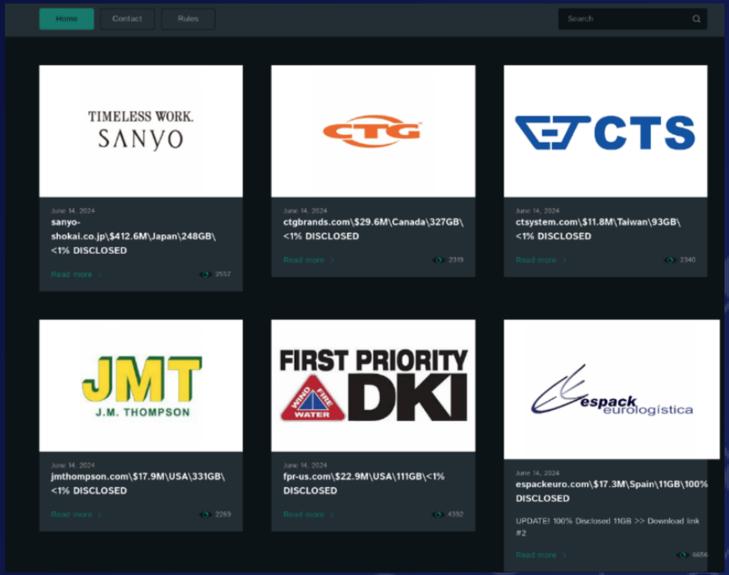
A Global Reach with Focused Targets:

Cactus ransomware demonstrates a lack of geographical bias, targeting victims worldwide. Here are some examples of its reach and the damage it has caused:

- Government Entities in Latin America: Early reports in July 2022 indicated widespread Cactus ransomware attacks targeting government entities in Latin America. These attacks can disrupt critical services and cause significant delays in government operations.
- Manufacturing Disruptions: Manufacturing companies across the globe have fallen victim to Cactus, experiencing data breaches, operational disruptions, and potential production delays.
- Critical Infrastructure Concerns: The increasing sophistication of Cactus raises concerns about potential attacks on critical infrastructure, such as power grids or transportation systems. A successful attack on such infrastructure could have catastrophic consequences.

Leak Site

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



June 14, 2024
sanyo-shokai.co.jp\$412.6M\Japan\248GB\<1% DISCLOSED
Read more
2557

June 14, 2024
ctgbrands.com\$29.6M\Canada\327GB\<1% DISCLOSED
Read more
2319

June 14, 2024
ctsystem.com\$11.8M\Taiwan\93GB\<1% DISCLOSED
Read more
2340

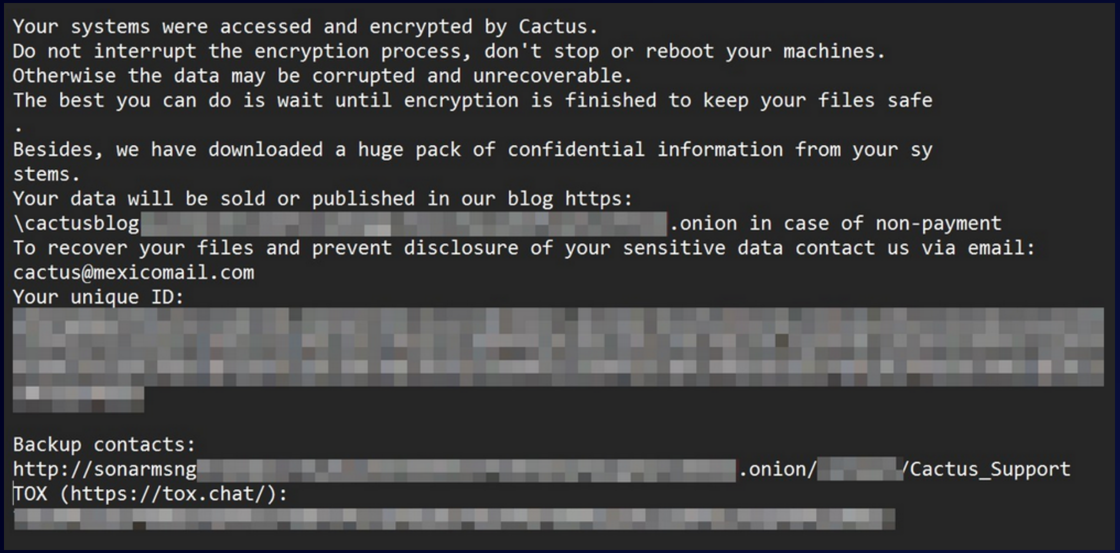
June 14, 2024
jmthompson.com\$17.9M\USA\331GB\<1% DISCLOSED
Read more
2269

June 14, 2024
fpr-us.com\$22.9M\USA\111GB\<1% DISCLOSED
Read more
4392

June 14, 2024
espackeuro.com\$17.3M\Spain\11GB\100% DISCLOSED
UPDATE! 100% Disclosed 11GB >> Download link #2
Read more
6656

Ransom Note

The Cactus ransomware has a different ransom note for every victim. One of the Cactus ransom note is given below:



```
Your systems were accessed and encrypted by Cactus.
Do not interrupt the encryption process, don't stop or reboot your machines.
Otherwise the data may be corrupted and unrecoverable.
The best you can do is wait until encryption is finished to keep your files safe
.
Besides, we have downloaded a huge pack of confidential information from your sy
stems.
Your data will be sold or published in our blog https:
\cactusblog[redacted].onion in case of non-payment
To recover your files and prevent disclosure of your sensitive data contact us via email:
cactus@mexicomail.com
Your unique ID:
[redacted]

Backup contacts:
http://sonarmsng[redacted].onion/[redacted]/Cactus_Support
TOX (https://tox.chat/):
[redacted]
```

The emergence of Cactus ransomware underscores the ever-evolving landscape of cyber threats. Its use of readily available tools like LockBit Black's codebase and its focus on double extortion tactics highlight the need for organisations to prioritise robust cybersecurity measures. Here are some crucial steps organisations can take to mitigate the risk of Cactus ransomware and similar threats:

- 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 Cactus 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
Execution	T1059	Command and Scripting Interpreter
	T1053	Scheduled Task/Job
	T1072	Software Deployment Tools
Persistence	T1136	Create Account
Defence Evasion	T1562	Impair Defences
	T1027	Obfuscated Files or Information
	T1070	Indicator Removal
Credential Access	T1555	Credentials from Password Stores
	T1003	OS Credential Dumping
Discovery	T1049	System Network Connections Discovery
	T1083	File and Directory Discovery
Lateral Movement	T1072	Software Deployment Tools
	T1570	Lateral Tool Transfer
Collection	T1119	Automated Collection
Exfiltration	T1567	Exfiltration Over Web Service
Command-and-Control	T1219	Remote Access Software
	T1090	Proxy

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxps://cactusbloguuodvqjmnzlwetjlpj6aggc6iocwhuupb47laukux7ckid.onion hxxps://cactus5dqnqkppa5ayckiyk6dttpqwczdqphv5mxh4dkk5ct544q5aad.onion	URLs (Onion)	Leak Site
163.123.142.213 64.52.80.252 162.33.177.56 45.61.138.99 206.188.196.20 45.61.136.79 45.61.136.127	IP	C2
cactus787835@proton[.]me	Email	Contact
eba1596272ff695a1219b1380468293a e28db6a65da2ebcf304873c9a5ed086d de6ce47e28337d28b6d29ff61980b2e9 949d9523269604db26065f002feef9ae 5737cb3a9a6d22e957cf747986eeb1b3 2611833c12aa97d3b14d2ed541df06b2 1add9766eb649496bc2fa516902a596 d5e5980feb1906d85fbd2a5f2165baf7 78aea93137be5f10e9281dd578a3ba73 26f3a62d205004fbc9c76330c1c71536 be7b13aee7b510b052d023dd936dc32f 39fe99d2250954a0d5ed0e9ff9c41d81 0e4ee38fe320cfb573a30820198ff442 8d2e4bef47e3f2ee0195926bbf4a25d5 f7a6d1e6e5436bd3c10f3a26f3e9b9b9 fb467a07f44e8d58e93e3567fd7ff016 be139fc480984eb31de025f25a191035 08d2c800c93015092e14738c941ac492 02e4da16377fc85e71a8c8378b2a8a96 8b37df9d295bbc2906961f72b7cdc5fb 8af259ad55c3746926e992c82bc7e850 55e42014424c0d120ff17f11e207e4f0 5f7c3cda7759ef6e577552ad322c1f64	Hash	File

In a comprehensive analysis of ransomware victims across 19 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 61% 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	1.28%
Austria	1.28%
Belgium	1.28%
Brazil	1.28%
Canada	8.97%
Denmark	1.28%
Egypt	1.28%
France	1.28%
Germany	3.85%
Hong Kong	1.28%
India	1.28%
Japan	1.28%
Netherlands	1.28%
Philippines	1.28%
Switzerland	1.28%
Taiwan	2.56%
Turkey	1.28%
UK	5.13%
USA	61.54%

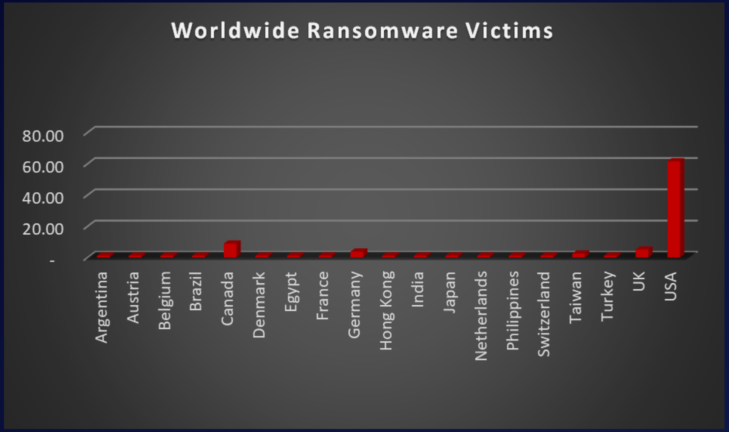


Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 18 different industries worldwide. Notably, Manufacturing bore the brunt of the attacks in the past week, accounting for 21% 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 (%)
Business Services	14.10%
Construction	8.97%
Consumer Services	5.13%
Education	5.13%
Energy, Utilities & Waste Treatment	1.28%
Finance	5.13%
Government	2.56%
Healthcare	7.69%
Hospitality	2.56%
IT	5.13%
Legal Services	2.56%
Manufacturing	21.79%
Metals & Mining	1.28%
Retail	1.28%
Real Estate	1.28%
Retail	7.69%
Telecom	2.56%
Transportation	3.85%

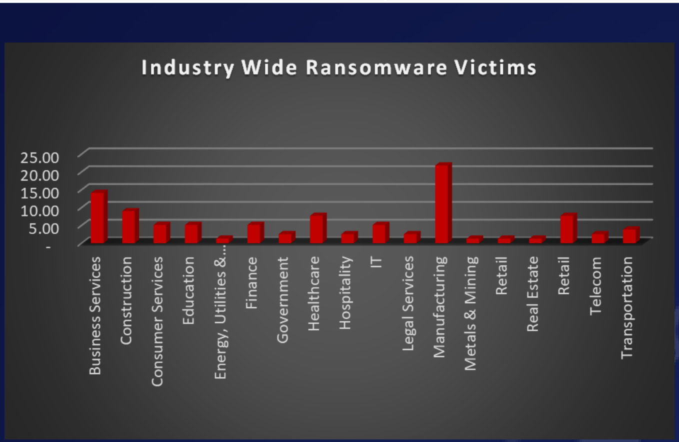


Figure 5: Industry-wise Ransomware Victims