Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

June 25 - July 01, 2024

Report Summary:

- **New Threat Detection Added** – 2 (Bmanager APT and Mint Stealer)
- **New Threat Protections - 321**

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

1. Bmanager APT

Bmanager APT, discovered in January 2024, is a modular Trojan designed to steal banking information, login credentials, and conduct phishing attacks. Targeting vulnerable websites, it injects malicious scripts to steal user data entered on those sites. This Trojan's strength lies in its modularity. Hackers can customise its functionality to bypass security measures and adapt to new situations. Boolka, the group behind Bmanager, has been active since 2022, employing opportunistic tactics to exploit website weaknesses.

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. Mint Stealer

Mint Stealer is a malicious software program designed to steal cryptocurrency credentials from infected devices. Disguised as legitimate applications or spread through phishing campaigns, it infiltrates your system and searches for private keys, seed phrases, and login details for popular crypto wallets. Once it locates this information, Mint Stealer transmits it to the attackers, allowing them to steal your cryptocurrency holdings. This malware can also steal browser cookies and other sensitive data, increasing the potential financial loss.

Rules Created: 05
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	T1566.001	Phishing: Spear phishing Attachment
Execution	T1059.001 T1059.003	Command and Scripting Interpreter: PowerShell
Persistence	T1543.003 T1505.003	Create or Modify System Process: Windows Scheduled Task/Job: Scheduled Task
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defence Evasion	T1140	Deobfuscate/Decode Files or Information
Discovery	T1057	Process Discovery
Command-and-Control	T1071.001 T1573	Application Layer Protocol: Web Protocols Encrypted Channel: Symmetric Cryptography

Known exploited vulnerabilities (Week 4 June 2024):

Vulnerability	CVSS	Description
CVE-2020-13965	6.1 (Medium)	Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability
CVE-2022-2586	7.8 (High)	Linux Kernel Use-After-Free Vulnerability
CVE-2022-24816	9.8 (Critical)	GeoSolutionsGroup JAI-EXT Code Injection Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-june-2024/482

Updated Malware Signatures (Week 4 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.
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.

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 21 industries spanning 18 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

BlackSuit ransomware group stands out as the most prolific, having updated a significant number of victims (15%) distributed across multiple countries. In comparison, Ransomhouse 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	3.61%
Akira	7.23%
Arcus Media	2.41%
Bianlian	4.82%
BlackSuit	15.66%
Blackbasta	2.41%
Blackbyte	1.20%
Cactus	10.84%
Darkvault	3.61%
Everest	1.20%
Handala	1.20%
Inc Ransom	3.61%
Lockbit3	6.02%
Meow	2.41%
Monti	1.20%
Play	12.05%
Qilin	3.61%
Qiulong	1.20%
Ransomhouse	1.20%
Ransomhub	10.84%
Rhysida	1.20%
Space Bears	2.41%

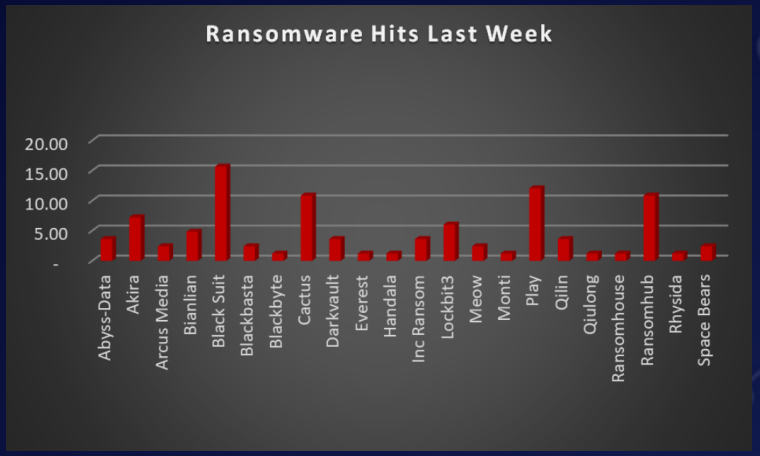


Figure 1: Ransomware Group Hits Last Week

BlackSuit Ransomware

Emerging in early 2023, BlackSuit ransomware swiftly carved a niche in the cybercrime 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 aren't met. While BlackSuit's origins remain shrouded in some mystery, security researchers believe it's a rebrand of the notorious Royal ransomware operation. Royal ransomware, itself suspected to be the successor of the Conti cybercrime syndicate, had a significant presence in the cybercriminal underworld. BlackSuit's connection to these groups suggests a level of experience and expertise behind its development and deployment.

Tactics, Techniques, and Procedures (TTPs):

BlackSuit doesn't rely on a one-size-fits-all approach. It possesses a diverse arsenal of tactics, techniques, and procedures (TTPs) to target specific victims and maximise impact. Here are some key elements in its malicious toolkit:

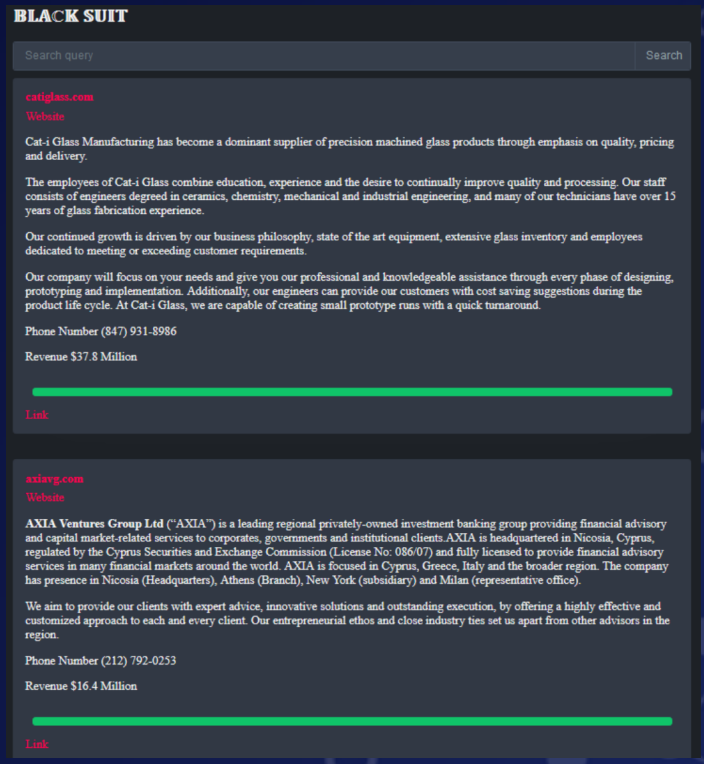
- Phishing Attacks: Deceptive emails designed to trick users into clicking malicious links or downloading infected attachments are a common entry point. These emails may appear to be from trusted sources such as delivery companies, financial institutions, or even colleagues.
- Exploiting Unpatched Vulnerabilities: Qilin 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, Qilin 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.
- Brute-Force Attacks: In some instances, Qilin may attempt to gain access through brute-force attacks, where it systematically tries different combinations of usernames and passwords until it cracks the login credentials. This highlights the importance of using strong passwords and enabling multi-factor authentication (MFA) where possible.
- Living-off-the-Land Techniques: Like many malware strains, Qilin can utilise legitimate system administration tools for malicious purposes. This makes detection more challenging as these tools may appear as normal system activity.
- Data Exfiltration: Before encryption, Qilin 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.

A Global Reach with Focused Targets:

BlackSuit ransomware demonstrates a mix of global reach and targeted attacks. Here are some examples of its operations:

- Healthcare and Education Sectors: Hospitals, universities, and other educational institutions have been frequent targets due to the potentially sensitive data they hold and the disruption a ransomware attack can cause.
- Critical Infrastructure Concerns: There have been concerns about BlackSuit targeting critical infrastructure sectors like power grids and transportation systems. A successful attack on such infrastructure could have devastating consequences.
- Supply Chain Attacks: BlackSuit's potential use of IABs raises concerns about large-scale supply chain attacks where a single compromised vendor can provide access to a wider network of victims.

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



Ransom Note

One of the BlackSuit ransom notes is given below:

```
Good whatever time of day it is!

Your safety service did a really poor job of protecting your files against our professionals.
Extortioner named  BlackSuit has attacked your system.

As a result all your essential files were encrypted and saved at a secure serverfor further useand publishing on the Web into the publ
Now we have all your files like: financial reports, intellectual property, accounting, law actionsand complaints, personal filesand so

We are able to solve this problem in one touch.
We (BlackSuit) are ready to give you an opportunity to get all the things back if you agree to makea deal with us.
You have a chance to get rid of all possible financial, legal, insurance and many others risks and problems for a quite small compensa
You can have a safety review of your systems.
All your files will be decrypted, your data will be reset, your systems will stay in safe.
Contact us through TOR browser using the link:
    http://weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz637f2yd.onion/?id=[snip]
```

The emergence of BlackSuit ransomware underscores the constantly evolving cybercrime landscape. Its rebranding strategy, focus on exploiting vulnerabilities, and ruthless 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 BlackSuit 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.
- Multi-Factor Authentication (MFA): Enable MFA for all user accounts wherever possible. MFA adds an extra layer of security by requiring a second verification factor beyond just a username and password.
- 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 such attacks.

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
	T1190	Exploit Public-Facing Application
Execution	T1059	Command and Scripting Interpreter
	T1053	Scheduled Task/Job
Persistence	T1136	Boot or Logon Initialisation Scripts
Privilege Escalation	T1068	Exploitation of Vulnerabilities
	T1548	Abuse Elevation Control Mechanism
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
Impact	T1486	Data Encrypted for Impact
	T1485	Data Destruction
	T1490	Inhibit System Recovery

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz637f2yd.onion	URLs (Onion)	Leak Site
2902e12f00a185471b619233ee8631f3 4f813698141cb7144786cdc6f629a92b 748de52961d2f182d47e88d736f6c835 9656cd12e3a85b869ad90a0528ca026e 748de52961d2f182d47e88d736f6c835 9656cd12e3a85b869ad90a0528ca026e 90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c 1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e 6ac8e7384767d1cb6792e62e09efc31a07398ca2043652ab11c090e6a585b310 4d7f6c6a051ecb1f8410243cd6941b339570165ebcfd3cc7db48d2a924874e99 b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08687796be30e2093286c	Hash	Malicious File

In a comprehensive analysis of ransomware victims across 18 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 57% 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 (%)
Argentina	1.20%
Brazil	3.61%
Canada	7.23%
China	1.20%
Denmark	1.20%
France	3.61%
Germany	2.41%
India	2.41%
Italy	2.41%
Japan	1.20%
Myanmar	1.20%
New Zealand	1.20%
Norway	1.20%
South Africa	1.20%
Spain	1.20%
Turkey	1.20%
UK	8.43%
USA	57.83%

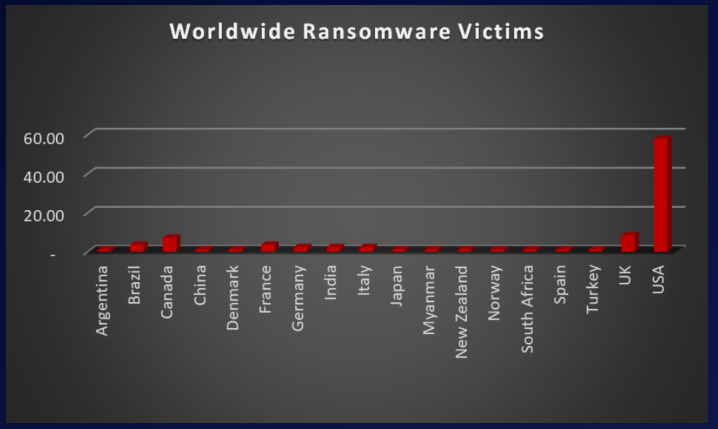


Figure 4: Ransomware Victims Worldwide

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 16% 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 (%)
Agriculture	1.20%
Business Services	9.64%
Cities, Town & Municipalities	1.20%
Construction	9.64%
Consumer Services	2.41%
Education	2.41%
Energy, Utilities & Waste Treatment	2.41%
Finance	4.82%
Government	1.20%
Healthcare	4.82%
Hospitality	2.41%
Insurance	2.41%
IT	6.02%
Legal Services	6.02%
Manufacturing	15.66%
Media & Internet	3.61%
Organisations	6.02%
Real Estate	2.41%
Retail	9.64%
Telecom	1.20%
Transport	4.82%

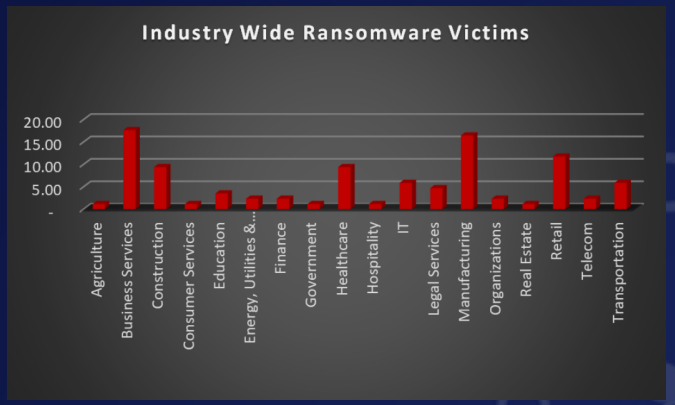


Figure 5: Industry-wise Ransomware Victims