Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 02 - 08, 2024

Report Summary:

- **New Threat Detection Added** – 2 (Phorpiex Malware and Cerber Ransomware)
- **New Threat Protections - 245**

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

1. Phorpiex Malware

Phorpiex is not your average malware. It's a well-established botnet, a network of compromised devices controlled by attackers. First appearing in 2019, Phorpiex has adapted over time to stay relevant. This botnet acts as a delivery system for various malicious payloads. It can unleash phishing attacks to steal your credentials, spam your inbox with unwanted messages, or even deploy ransomware to lock your files and demand payment. Phorpiex spreads through removable drives and infects network shares, making it crucial to be cautious with external devices.

Rules Created: 20
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	T1047 T1053 T1064 T1129	Windows Management Instrumentation Scheduled Task/Job Command and Scripting Interpreter Shared Modules
Persistence	T1053 T1543.003 T1547.001	Scheduled Task/Job Windows Service Registry Run Keys / Startup Folder
Privilege Escalation	T1055 T1547.001	Process Injection Registry Run Key/ Startup Folder
Defence Evasion	T1055 T1027	Process Injection Obfuscated Files or Information
Discovery	T1057 T1082	Process Discovery System Information Discovery
Command-and-Control	T1073 T1071 T1105	Encrypted Channel Application Layer Protocol Ingress Tool Transfer

2. Cerber Ransomware

Cerber ransomware takes a unique approach by utilising Ransomware-as-a-Service (RaaS). Unlike traditional ransomware where attackers develop, deploy, and profit alone, Cerber functions as a business model. Developers license the ransomware for a fee, typically 40% of the ransom collected. This allows anyone, even those without technical expertise, to become a Cerber affiliate by simply launching attacks and splitting the profits. This RaaS approach benefits both parties. Developers can cast a wider net with minimal effort, while affiliates gain access to a powerful tool without needing coding skills. Cerber exemplifies the evolution of ransomware, shifting the burden of victim acquisition and infection to affiliates, maximising attack distribution while minimising developer workload. Additionally, the use of Bitcoin facilitates anonymous transactions, further complicating law enforcement efforts.

Rules Created: 10
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	T1078 T1091	Valid Accounts Replication Through removable media
Execution	T1047 T1129	Windows Management Instrumentation Shared Module
Persistence	T11078	Valid Accounts
Privilege Escalation	T1548	Abuse Elevation Control Mechanism
Defence Evasion	T1027	Obfuscated Files or Information
Discovery	T1057 T1027	Process Discovery Query Registry
Command-and-Control	T1071 T1573	Application Layer Protocol Encrypted Channel
Impact	T1486	Data Encryption

Known exploited vulnerabilities (Week 1 July 2024):

Vulnerability	CVSS	Description
CVE-2024-20399	6.7 (Medium)	Cisco NX-OS Command Injection Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-july-2024/486

Updated Malware Signatures (Week 1 July 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 19 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.

Ransomhub ransomware group stands out as the most prolific, having updated a significant number of victims (15%) distributed across multiple countries. In comparison, Akira 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
Akira	10.39%
Arcus Media	3.90%
Bianlian	5.19%
Blackbasta	1.30%
Blackout	1.30%
Brain Cipher	1.30%
Cloak	1.30%
Darkvault	2.60%
Donutleaks	1.30%
Dragonforce	9.09%
Embargo	2.60%
Hunters	5.19%
Inc Ransom	5.19%
Killsec	1.30%
Lockbit3	5.19%
Medusa	5.19%
Monti	1.30%
Play	7.79%
Pyrx	1.30%
Ransomexx	1.30%
Ransomhouse	2.60%
Ransomhub	15.58%
Rhysida	1.30%
Space Bears	3.90%
Team Underground	2.60%

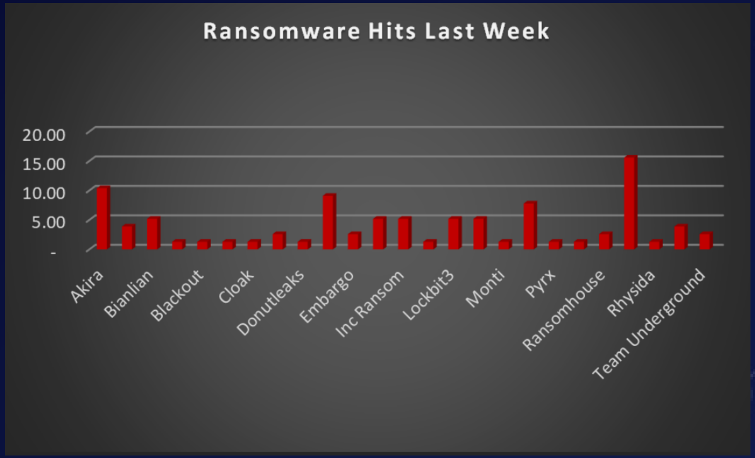


Figure 1: Ransomware Group Hits Last Week

Bianlian Ransomware

First detected in the wild around late 2021, Bianlian ransomware has undergone a fascinating evolution in the cybercrime landscape. Initially emerging as an Android banking trojan, it quickly pivoted its focus to become a formidable ransomware threat by July 2022. 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 the exact origins of Bianlian remain unclear, security researchers suspect a connection to a cybercriminal group known as UNC7885. This group has a history of utilising various malware strains, suggesting a level of adaptability and expertise behind Bianlian's development.

Tactics, Techniques, and Procedures (TTPs):

Bianlian doesn't rely on a single method of attack. It possesses a diverse arsenal of tactics, techniques, and procedures (TTPs) that evolve over time, reflecting its name's inspiration – the traditional Chinese art of face-changing. Here's a glimpse into its ever-expanding toolkit:

- Phishing Attacks: Deceptive emails 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 trusted colleagues, delivery companies, or even financial institutions.

- Exploiting Unpatched Vulnerabilities: Bianlian 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, Bianlian 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, Bianlian 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 emphasises the importance of strong passwords and enabling Multi-Factor Authentication (MFA) wherever possible.

- Living-off-the-Land Techniques: Like many malware strains, Bianlian 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, Bianlian 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.

- Shifting Focus: One of Bianlian's distinguishing features is its adaptability. Recent reports by Unit 42, a cybersecurity firm, suggest a shift away from data encryption and towards a pure extortion model. This highlights the need for organisations to stay vigilant against evolving tactics.

A Global Reach with Focused Targets

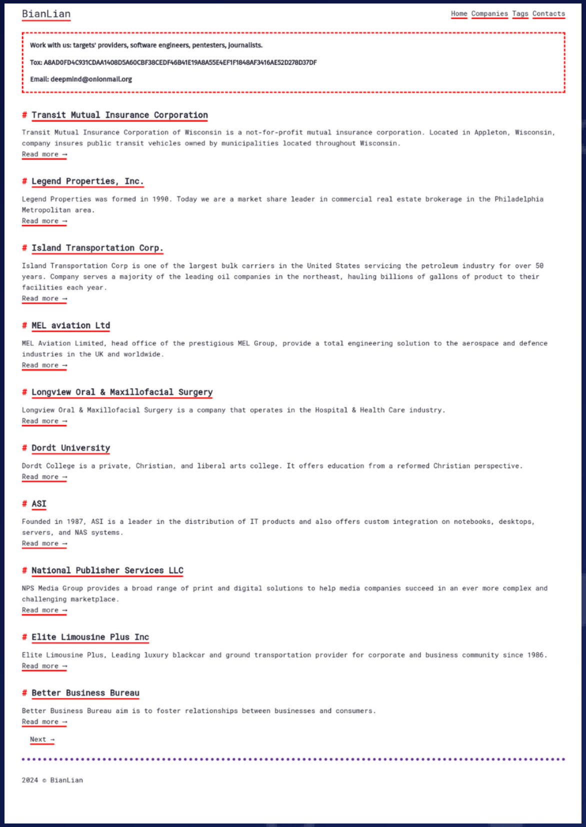
Bianlian ransomware demonstrates a lack of geographical bias, targeting victims worldwide. Here are some examples of its reach and the impact it has caused:

- 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 Bianlian, experiencing data breaches, operational disruptions, and potential production delays.

- Professional Services: Targets have also included companies in the professional and legal services sectors, highlighting the versatility of Bianlian's attacks.

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



Work with us: targets' providers, software engineers, pentesters, journalists.

Tox: A8AD0FD4C931CDAA1408D5A60CBF38CEDF46B41E19A8A55E4EF1F1848AF3416AE52D278D37DF

Email: deepmind@onionmail.org

Transit Mutual Insurance Corporation

Transit Mutual Insurance Corporation of Wisconsin is a not-for-profit mutual insurance corporation. Located in Appleton, Wisconsin, company insures public transit vehicles owned by municipalities located throughout Wisconsin.
Read more →

Legend Properties, Inc.

Legend Properties was formed in 1990. Today we are a market share leader in commercial real estate brokerage in the Philadelphia Metropolitan area.
Read more →

Island Transportation Corp.

Island Transportation Corp is one of the largest bulk carriers in the United States servicing the petroleum industry for over 50 years. Company serves a majority of the leading oil companies in the northeast, hauling billions of gallons of product to their facilities each year.
Read more →

MEL aviation Ltd

MEL Aviation Limited, head office of the prestigious MEL Group, provide a total engineering solution to the aerospace and defence industries in the UK and worldwide.
Read more →

Longview Oral & Maxillofacial Surgery

Longview Oral & Maxillofacial Surgery is a company that operates in the Hospital & Health Care industry.
Read more →

Dordt University

Dordt College is a private, Christian, and liberal arts college. It offers education from a reformed Christian perspective.
Read more →

ASI

Founded in 1987, ASI is a leader in the distribution of IT products and also offers custom integration on notebooks, desktops, servers, and NAS systems.
Read more →

National Publisher Services LLC

NPS Media Group provides a broad range of print and digital solutions to help media companies succeed in an ever more complex and challenging marketplace.
Read more →

Elite Limousine Plus Inc

Elite Limousine Plus, Leading luxury blackcar and ground transportation provider for corporate and business community since 1986.
Read more →

Better Business Bureau

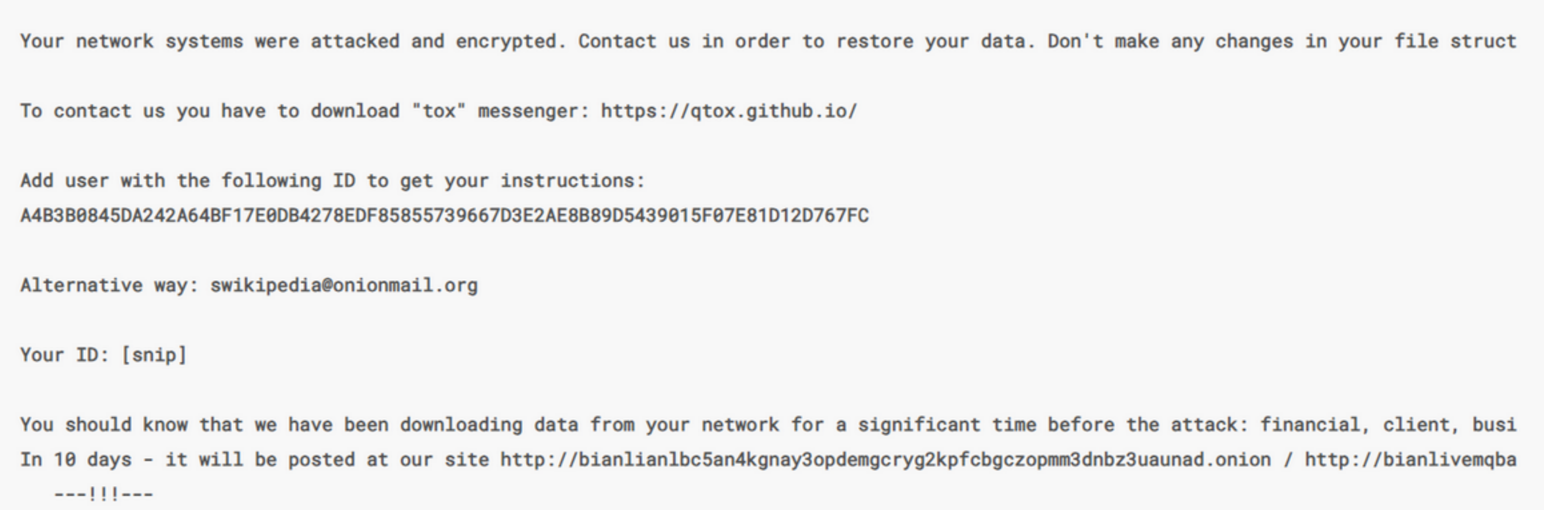
Better Business Bureau aim is to foster relationships between businesses and consumers.
Read more →

Next →

2024 © BianLian

Ransom Note

One of the Bianlian ransom notes is given below:



```
Your network systems were attacked and encrypted. Contact us in order to restore your data. Don't make any changes in your file struct

To contact us you have to download "tox" messenger: https://qtox.github.io/

Add user with the following ID to get your instructions:
A4B3B0845DA242A64BF17E0DB4278EDF85855739667D3E2AE8B89D5439015F07E81D12D767FC

Alternative way: swikipedia@onionmail.org

Your ID: [snip]

You should know that we have been downloading data from your network for a significant time before the attack: financial, client, busi
In 10 days - it will be posted at our site http://bianlianlbc5an4kgnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad.onion / http://bianlivemqba
   ---!!!---
```

The emergence and evolution of Bianlian ransomware underscore the constantly evolving cybercrime landscape. Its ability to adapt its tactics and the recent shift towards pure extortion highlight the need for organisations to prioritise comprehensive cybersecurity measures. Here are some crucial steps organisations can take to mitigate the risk of Bianlian 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 Bianlian and other malware threats.

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1195	Supply Chain Compromise
	T1566.002	Spearphishing Link
	T1190	Exploit Public-Facing Application
	T1566.001	Spearphishing Attachment
	T1078	Valid Accounts
Execution	T1059.001	PowerShell
	T1569.002	Service Execution
	T1059.003	Windows Command Shell
Persistence	T1547.009	Shortcut Modification
	T1547.001	Registry Run Keys / Startup Folder
	T1078	Valid Accounts
Privilege Escalation	T1078	Valid Accounts
	T1547.001	Registry Run Keys / Startup Folder
	T1547.009	Shortcut Modification
Defence Evasion	T1027.001	Binary Padding
	T1036.005	Match Legitimate Name or Location
	T1078	Valid Accounts
Discovery	T1016.001	Internet Connection Discovery
Collection	T1114.001	Local Email Collection
Exfiltration	T1537	Transfer Data to Cloud Account
	T1567	Exfiltration Over Web Service
Impact	T1486	Data Encrypted for Impact

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://bianlianlbc5an4kgnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad.onion/ hxxp://bianlivemqbawcco4cx4a672k2fip3guyxudzurfqvdszafam3ofqgqd.onion/	URLs (Onion)	Leak Site
7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893 1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43 0c1eb11de3a533689267ba075e49d93d55308525c04d6aff0d2c54d1f52f5500 40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce af46356eb70f0fbb0799f8a8d5c0f7513d2f6ade4f16d4869f2690029b511d4f 1fd42d07b4be99e0e503c0ed5af2274312be1b03e01b54a6d89c0eef04257d6e 3a2f6e614ff030804aa18cb03fcc3bc357f6226786efb4a734cbe2a3a1984b6f 46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b 1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43 eaf5e26c5e73f3db82cd07ea45e4d244ccb3ec3397ab5263a1a74add7bbcb6e2 c775e6d87a3bcc5e94cd055fee859bdb6350af033114fe8588d2d4d4f6d2a3ae c57ca631b069745027d0b4f4d717821ca9bd095e28de2eafe4723eeaf4b062cf c592194cea0acf3d3e181d2ba3108f0f86d74bcd8e49457981423f5f902d054b df51b7b031ecc7c7fa899e17cce98b005576a20a199be670569d5e408d21048c 2ed448721f4e92c7970972f029290ee6269689c840a922982ac2f39c9a6a838f 264af7e7aa17422eb4299df640c1aa199b4778509697b6b296efa5ae7e957b40 73d095abf2f31358c8b1fb0d5a0dc9807e88d44282c896b5033c1b270d44111f 8b65c9437445e9bcb8164d8557ecb9e3585c8bebf37099a3ec1437884efbdd24 4ca84be5b6ab91694a0f81350cefe8379efcad692872a383671ce4209295edc7 93fb7f0c2cf10fb5885e03c737ee8508816c1102e9e3d358160b78e91fa1ebdb afb7f11da27439a2e223e6b651f96eb16a7e35b34918e501886d25439015bf78 53095e2ad802072e97dbb8a7ccea03a36d1536fce921c80a7a2f160c83366999 16cbfd155fb44c6fd0f9375376f62a90ac09f8b7689c1afb5b9b4d3e76e28bdf 60b1394f3afee27701e2008f46d766ef466caa7711c45ddfd443a71efc39a407 ba3c4bc99b67038b42b75a206d7ef04f6d8abaf87a76c373d4dec85e73859ce2 e7e097723d00f58eab785baf30365c1495e99aa6ead6fe1b86109558838d294e 96e02ea8b1c508f1ee3c1535547f9b89396f557011e61478644ae5876cdaaca5 ac1d42360c45e0e908d07e784ceb15faf8987e4ba1744d56313de6524d2687f7 1cba58f73221b5bb7930bfeab0106ae5415e70f49a595727022dcf6fda1126e9 487f0d748a13570a46b20b6687eb7b7fc70a1a55e676fb5ff2599096a1ca888c f84edc07b23423f2c2cad47c0600133cab3cf2bd6072ad45649d6faf3b70ec30 93953eef3fe8405d563560dc332135bfe5874ddeb373d714862f72ee62bef518 f3f3c692f728b9c8fd2e1c090b60223ac6c6e88bf186c98ed9842408b78b9f3c f6669de3baa1bca649afa55a14e30279026e59a033522877b70b74bfc000e276 228ef7e0a080de70652e3e0d1eab44f92f6280494c6ba98455111053701d3759 0e4246409cdad59e57c159c7cc4d75319edf7d197bc010174c76fe1257c3a68e 90f50d723bf38a267f5196e22ba22584a1c84d719b501237f43d10117d972843	Hash	Malicious File
208.123.119[.]123 13.215.228[.]73 54.193.91[.]232 172.96.137[.]159 204.152.203[.]90 144.208.127[.]119 192.161.48[.]43 146.70.87[.]197 45.86.230[.]64 45.56.165[.]17 23.163.0[.]168 172.96.137[.]249 173.254.204[.]78 185.56.137[.]117 52.87.206[.]242 45.66.249[.]118 96.44.157[.]203 103.20.235[.]122 44.212.9[.]14	IPs	C2

In a comprehensive analysis of ransomware victims across 18 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 55% 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	3.90%
Austria	1.30%
Brazil	3.90%
Canada	5.19%
China	1.30%
Croatia	2.60%
Dominican Republic	1.30%
France	3.90%
Germany	3.90%
India	1.30%
Indonesia	2.60%
Italy	1.30%
Japan	1.30%
Peru	1.30%
Switzerland	2.60%
Taiwan	1.30%
UK	5.19%
USA	55.84%

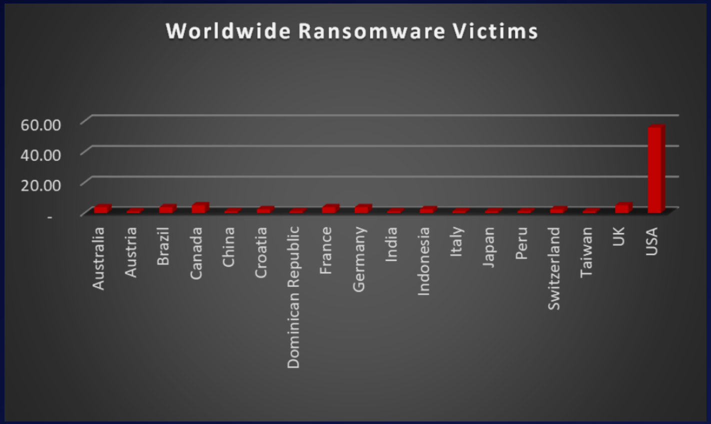


Figure 4: Ransomware Victims Worldwide

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 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	1.30%
Business Services	11.69%
Construction	5.19%
Consumer Services	2.60%
Education	6.49%
Energy, Utilities & Waste Treatment	2.60%
Finance	3.90%
Government	3.90%
Healthcare	5.19%
Hospitality	3.90%
Insurance	2.60%
IT	3.90%
Legal Services	1.30%
Manufacturing	16.88%
Metals & Mining	3.90%
Organisations	5.19%
Real Estate	3.90%
Retail	10.39%
Transportation	5.19%

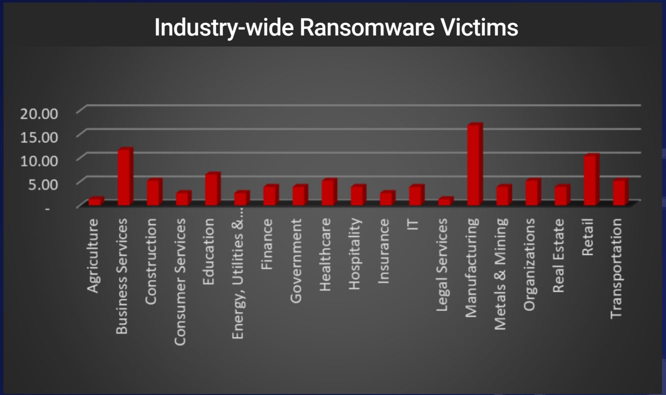


Figure 5: Industry-wise Ransomware Victims