Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Apr 30 - May 06, 2024

Report Summary:

- **New Threat Detection Added** – 5 (DinodasRAT, Firebird RAT, Matsnu Malware, DarkGate RAT and Ducktail Malware)
- **New Threat Protections - 96**

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

1. DinodasRAT

DinodasRAT, also known as XDealer, is a sneaky malware that gives attackers full control of your computer. This multi-platform threat can spy on you, steal data, and even run programs remotely. DinodasRAT has versions for Windows and Linux, and it's especially dangerous because it can hide its tracks. Developed from a legitimate remote access tool, it's been linked to cyberespionage campaigns targeting governments.

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
Execution	T1053.001 T1059 T1064	AT (Linux): Sample Persists itself using system V run levels. Command and Scripting Interpreter Scripting
Persistence	T1053.001	Sample persists itself using System V run levels
Defence Evasion	T1027 T1064 T1070 T1070.004 T1222	Obfuscated Files or Information Scripting Indicator Removal File Deletion File and Directory Permissions Modification
Discovery	T1016 T1033	System Network Configuration Discovery System Owner/User Discovery
Collection	T1105	Ingress Tool Transfer
Command-and-Control	T1071.001 T1095 T1573	Application Layer Protocol Non-Application Layer Protocol Encrypted Channel

2. Firebird RAT

Firebird RAT, also known as Hive RAT, was a malicious remote access tool that masquerades as a legitimate administration tool and grants attackers full control of infected devices. Firebird boasted stealthy features and could steal passwords, spy on victims, and even turn their machines into parts of large botnets. Thankfully, in April 2024, authorities arrested those believed to be behind Firebird's creation and distribution.

Rules Created: 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	T1566.001	Spear phishing Attachment
Execution	T1059.003 T1059.005	Command and Scripting Interpreter: Windows Command Shell Command and Scripting Interpreter: Visual Basic
Persistence	T1053.001	Registry Run Keys / Startup Folder
Defence Evasion	T1036 T1027	Masquerading Obfuscated Files or Information
Discovery	T1057	Process Discovery
Collection	T1114	Email Collection
Command-and-Control	T1071	Application Layer Protocol

3. Matsnu Malware

Matsnu is a sneaky Windows Trojan that acts as a backdoor for attackers. It infects your system and hides, impersonating other software to avoid detection. Once in, it can download and run malicious programs on your machine. This malware uses clever tricks like domain generation algorithms to connect with its command centre, making it harder to block. Matsnu is a serious threat that can steal data or encrypt your files.

Rules Created: 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
Defence Evasion	T1027 T027.002	Obfuscated Files or Information Software Packing
Credential Access	T1003	OS Credential Dumping
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Collection	T1005 T1560	Data from Local System Archive Collected Data
Command-and-Control	T1071	Application Layer Protocol

4. DarkGate RAT

DarkGate, lurking since 2018, is a Remote Access Trojan (RAT) for hire. Sold on cybercrime forums, it grants attackers full control of infected devices. Disguised as harmless files, DarkGate can steal your data, spy on your keystrokes, and even take control of your webcam. This RAT is known for evading detection and has exploited Windows vulnerabilities in the past. Stay vigilant, keep your software updated, and be cautious of suspicious links or attachments to avoid DarkGate's grasp.

Rules Created: 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	T1566.002	Spear phishing Link
Execution	T1204	User Execution
Defence Evasion	T1036	Masquerading
Credential Access	T1003 T1056 T1552	OS Credential Dumping Input Capture Unsecured Credentials
Discovery	T1012	Query Registry
Collection	T1005	Data from Local System
Command-and-Control	T1071	Application Layer Protocol

5. Ducktail Malware

Ducktail malware, active since 2021, targets Facebook Business accounts. This Vietnamese cybercrime operation spreads through fake job postings, often on LinkedIn. Luring marketing professionals, they send archives with malware disguised as PDFs containing fashion industry content. Ducktail steals Facebook session cookies to hijack ad accounts, potentially causing financial losses and privacy issues for businesses.

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
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1055 T1497	Process Injection VM Evasion
Discovery	T1018 T1082	Remote System Discovery System Information Discovery
Command-and-Control	T1071	Application Layer Protocol

Known exploited vulnerabilities (Week 1 May 2024):

Vulnerability	CVSS	Description
CVE-2024-29988	8.8 (High)	Microsoft SmartScreen Prompt Security Feature Bypass Vulnerability
CVE-2023-7028	7.5 (High)	GitLab Community and Enterprise Editions Improper Access Control Vulnerability

Updated Malware Signatures (Week 1 May 2024)

Threat	Description
Upatre	Upatre is also a malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.
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.
QuasarRat	A remote access trojan that was made available to the public as an open-source project. Once installed on a victim's machine, it is capable of keylogging, data and screen capturing among other things. It is also known to be highly customisable depending on the threat actor's intended need.
Bifrost	A remote access trojan that enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.

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 20 different 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.

Play ransomware stands out as the most prolific, having updated a significant number of victims (15%) distributed across multiple countries. In comparison, LockBit3.0 ransomware updated 14% 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
8Base	3.30%
Akira	1.10%
Apos	4.40%
Bianlian	2.20%
Black Suit	1.10%
Blackbasta	3.30%
Cactus	1.10%
Cloak	2.20%
Dan0N	1.10%
Darkvault	1.10%
Embargo	1.10%
Eraleign (Apt73)	3.30%
Everest	3.30%
Hunters	3.30%
INC Ransom	5.49%
Lockbit3.0	14.29%
Medusa	5.49%
Play	15.38%
Qilin	2.20%
RA Group	2.20%
Ransomhub	3.30%
Ransomware Blog	1.10%
Rhysida	1.10%
Space Bears	5.49%
Team Underground	12.09%

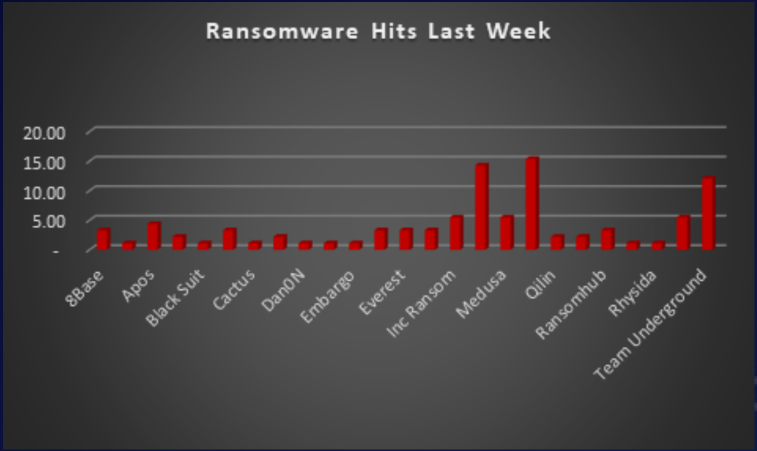


Figure 1: Ransomware Group Hits Last Week

Team Underground Ransomware

Team Underground is a relatively new ransomware group that emerged in 2023. While not as notorious as some established actors, they have garnered attention for their tactics and the information they offer alongside their typical extortion attempts.

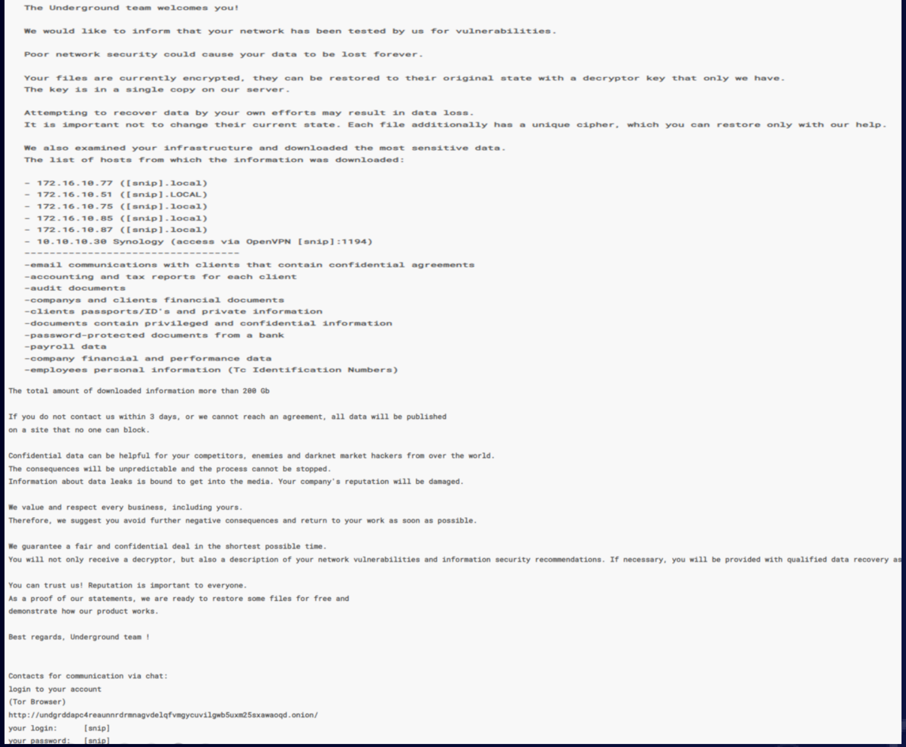
Tactics, Techniques, and Procedures (TTPs)

Delivery: The exact infection vector used by Team Underground is still under investigation. However, some reports suggest they might leverage spam campaigns with malicious attachments or exploit unpatched vulnerabilities in software to gain initial access.

Encryption: Team Underground utilises a custom-made ransomware executable built with Microsoft Visual C/C++ and designed for 64-bit systems. The ransomware encrypts victim files and unlike many strains, doesn't alter filenames or extensions.

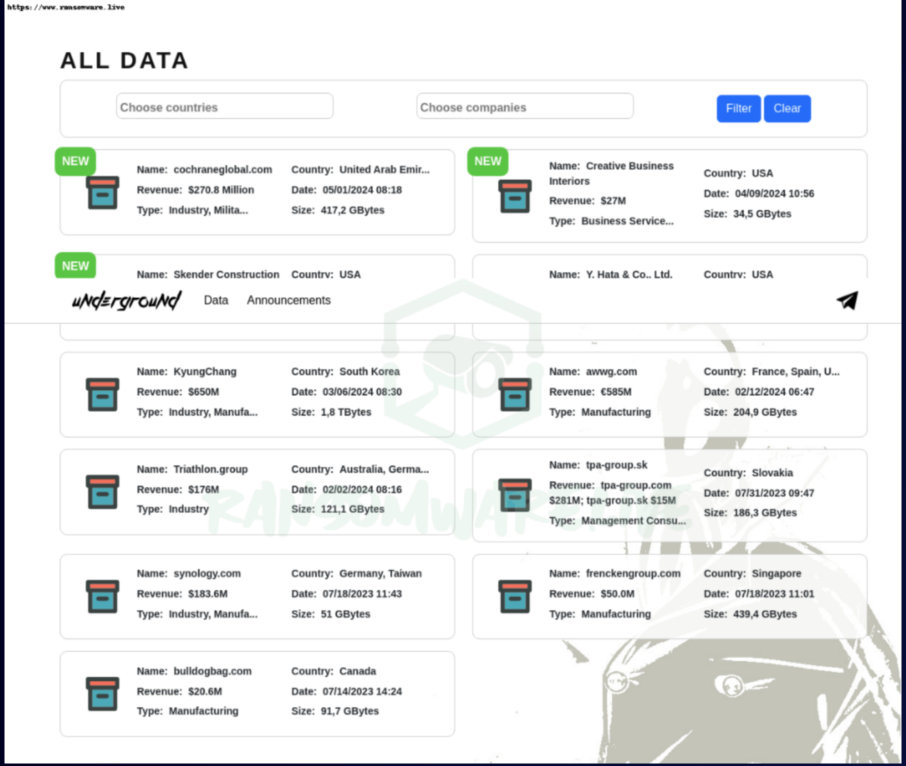
Exfiltration: In a unique twist, Team Underground claims to steal data during the attack process. Their ransom note mentions exfiltrating sensitive information like financial records, employee data, and confidential agreements. This adds another layer of pressure on victims, as leaking such information could be disastrous.

Ransom Note: Team Underground's ransom note, titled "!readme!!!.txt", stands out for offering more than just a decryption key in exchange for a ransom payment (which can be as high as $3 million!). They promise to provide details on exploited network vulnerabilities and even offer recommendations for improved information security. It is unclear if these are genuine offers or simply a ploy to build trust with victims.



```
  The Underground team welcomes you!

  We would like to inform that your network has been tested by us for vulnerabilities.

  Poor network security could cause your data to be lost forever.

  Your files are currently encrypted, they can be restored to their original state with a decryptor key that only we have.
  The key is in a single copy on our server.

  Attempting to recover data by your own efforts may result in data loss.
  It is important not to change their current state. Each file additionally has a unique cipher, which you can restore only with our help.

  We also examined your infrastructure and downloaded the most sensitive data.
  The list of hosts from which the information was downloaded:

  - 172.16.10.77 ([snip].local)
  - 172.16.10.51 ([snip].LOCAL)
  - 172.16.10.75 ([snip].local)
  - 172.16.10.85 ([snip].local)
  - 172.16.10.87 ([snip].local)
  - 10.10.10.30 Synology (access via OpenVPN [snip]:1194)
  ---------------------------------
  -email communications with clients that contain confidential agreements
  -accounting and tax reports for each client
  -audit documents
  -companys and clients financial documents
  -clients passports/ID's and private information
  -documents contain privileged and confidential information
  -password-protected documents from a bank
  -payroll data
  -company financial and performance data
  -employees personal information (Tc Identification Numbers)
The total amount of downloaded information more than 200 Gb

If you do not contact us within 3 days, or we cannot reach an agreement, all data will be published
on a site that no one can block.

Confidential data can be helpful for your competitors, enemies and darknet market hackers from over the world.
The consequences will be unpredictable and the process cannot be stopped.
Information about data leaks is bound to get into the media. Your company's reputation will be damaged.

We value and respect every business, including yours.
Therefore, we suggest you avoid further negative consequences and return to your work as soon as possible.

We guarantee a fair and confidential deal in the shortest possible time.
You will not only receive a decryptor, but also a description of your network vulnerabilities and information security recommendations. If necessary, you will be provided with qualified data recovery as

You can trust us! Reputation is important to everyone.
As a proof of our statements, we are ready to restore some files for free and
demonstrate how our product works.

Best regards, Underground team !


Contacts for communication via chat:
login to your account
(Tor Browser)
http://undgrddapc4reaunnrdrmnagvdelqfvmgycuvilgwb5uxm25sxawaoqd.onion/
your login:     [snip]
your password:  [snip]
```

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



https://www.ransomware.live

ALL DATA

NEW
Name: cochraneglobal.com
Revenue: $270.8 Million
Type: Industry, Milita...
Country: United Arab Emir...
Date: 05/01/2024 08:18
Size: 417,2 GBytes

NEW
Name: Creative Business Interiors
Revenue: $27M
Type: Business Service...
Country: USA
Date: 04/09/2024 10:56
Size: 34,5 GBytes

NEW
Name: Skender Construction
Countrv: USA

Name: Y. Hata & Co.. Ltd.
Countrv: USA

Name: KyungChang
Revenue: $650M
Type: Industry, Manufa...
Country: South Korea
Date: 03/06/2024 08:30
Size: 1,8 TBytes

Name: awwg.com
Revenue: €585M
Type: Manufacturing
Country: France, Spain, U...
Date: 02/12/2024 06:47
Size: 204,9 GBytes

Name: Triathlon.group
Revenue: $176M
Type: Industry
Country: Australia, Germa...
Date: 02/02/2024 08:16
Size: 121,1 GBytes

Name: tpa-group.sk
Revenue: tpa-group.com $281M; tpa-group.sk $15M
Type: Management Consu...
Country: Slovakia
Date: 07/31/2023 09:47
Size: 186,3 GBytes

Name: synology.com
Revenue: $183.6M
Type: Industry, Manufa...
Country: Germany, Taiwan
Date: 07/18/2023 11:43
Size: 51 GBytes

Name: frenckengroup.com
Revenue: $50.0M
Type: Manufacturing
Country: Singapore
Date: 07/18/2023 11:01
Size: 439,4 GBytes

Name: bulldogbag.com
Revenue: $20.6M
Type: Manufacturing
Country: Canada
Date: 07/14/2023 14:24
Size: 91,7 GBytes

Exploited Vulnerabilities

Specific vulnerabilities exploited by Team Underground have not been publicly disclosed yet. However, their ability to gain access to systems suggests they target unpatched software vulnerabilities or weaknesses in network security.

Recommendations:

- Stay Updated: Regularly update your software and operating systems to patch known vulnerabilities.
- Educate Staff: Train employees on cybersecurity best practices, including phishing awareness, to avoid falling victim to social engineering attacks.
- Strong Backups: Maintain robust backup procedures and store backups securely, ideally offline. This allows for data recovery in case of an attack.
- Security Measures: Implement strong security measures like firewalls and endpoint detection and response (XDR/EDR) solutions to deter and identify threats.
- Remember: Paying the ransom does not guarantee data recovery and fuels the cybercrime ecosystem. Report any ransomware attack to the relevant authorities, such as the Australian Cyber Security Centre (ACSC).

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
Defence Evasion	T1070	Delete Shadow drive data
Discovery	T1217 T1082 T1083	Browser Information Discovery System Information Discovery File and Directory Discovery
Impact	T1486 T1490	Data Encrypted for Impact Inhibit System Recovery

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
059175be5681a633190cd9631e2975f6 0a08d9b027457da99725968eb4566eb836a7d503219ad5690f851caecabce93d	Hash	Underground Team Ransomware
hxxp://47glxkuxyayqrvugfumgsblrdagvrah7gttfscgzn56eyss5wg3uvmqd.onion hxxp://undgrddapc4reaunnrdrmnagvdelqfvmgycuvilgwb5uxm25sxawaoqd.onion hxxp://ehehqyhw3iev2vfso4vqs7kcrzltfebe5vbimq62p2ja7pslczs3q6qd.onion/auth/login	URLs	Leak Site

In a comprehensive analysis of ransomware victims across 26 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 59% 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	3.30%
Australia	3.30%
Brazil	2.20%
Canada	3.30%
Czech Republic	1.10%
France	1.10%
Georgia	1.10%
Germany	4.40%
India	2.20%
Libya	1.10%
Malaysia	1.10%
Mexico	1.10%
Netherlands	1.10%
New Zealand	1.10%
Norway	1.10%
Puerto Rico	1.10%
Slovakia	1.10%
Sobieski	1.10%
South Korea	1.10%
Spain	1.10%
Sweden	1.10%
Switzerland	1.10%
Taiwan	1.10%
UAE	1.10%
UK	2.20%
USA	59.34%

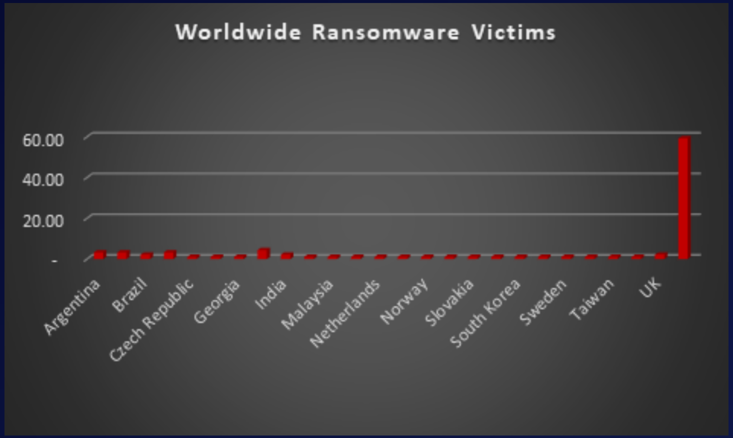


Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 20 different industries worldwide. Notably, the Manufacturing industry bore the brunt of the attacks in the past week, accounting for 15% 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	15.38%
Construction	16.48%
Consumer Services	2.20%
Education	1.10%
Energy, Utilities & Waste Treatment	3.30%
Finance	6.59%
Government	1.10%
Healthcare	4.40%
Hospitality	2.20%
Insurance	3.30%
IT	3.30%
Legal Services	1.10%
Manufacturing	15.38%
Media & Internet	3.30%
Metals & Mining	1.10%
Organisations	2.20%
Real Estate	2.20%
Retail	10.99%
Telecom	2.20%
Transportation	2.20%

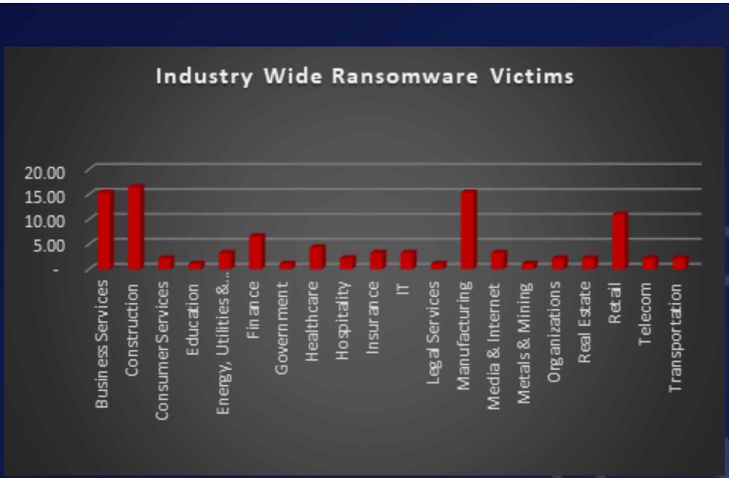


Figure 5: Industry-wise Ransomware Victims