Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 07- 13, 2024

Report Summary:

- **New Threat Detection Added** – 4 (GhostRAT, DarkRAT, AhMyth RAT and Borr Malware)
- **New Threat Protections - 169**

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

1. GhostRAT Malware

GhostRAT, also known as Gh0st RAT (Remote Access Tool), is a malicious program categorised as a Remote Access Trojan (RAT). First appearing in 2008, it grants unauthorised remote access to an infected Windows device. GhostRAT's source code is publicly available, allowing anyone with programming knowledge to modify it for their purposes. This adaptability has made it a popular tool among cybercriminals. Once installed, GhostRAT offers a variety of functionalities to the attacker, including:

a. Full remote control: View and control the victim's screen.
b. Keystroke logging: Capture everything typed on the keyboard.
c. Live feed access: View the webcam and microphone feed.
d. File manipulation: Download, upload, and execute files on the infected device.
e. System control: Reboot or shut down the device, disable user input.

Due to its ease of use and extensive features, GhostRAT remains a threat despite being around for over a decade. It's crucial to maintain up-to-date antivirus software and practice caution when downloading files or clicking on links to avoid infection.

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	T1059	Command and Scripting Interpreter
	T1129	Shared Modules
Persistence	T1543.003	Windows Service
	T1574.002	DLL Side-Loading
Privilege Escalation	T1543.003	Windows Service
	T1574.002	DLL Side-Loading
Defence Evasion	T1027	Obfuscated Files or Information
	T1064	Scripting
	T1070	Indicator Removal
	T1070.004	File Deletion
	T1222	File and Directory Permissions Modification
Credential Access	T1056	Input Capture
Discovery	T1010	Application Window Discovery
	T1082	System Information Discovery
Collection	T1056	Input Capture
Command-and-Control	T1071	Application Layer Protocol

2. DarkRAT

DarkRAT is a dangerous remote access tool (RAT) that grants unauthorised control to attackers. Once installed, it steals personal details, infects systems with malware, and runs hidden in the background. It automatically launches at startup and updates itself to evade detection. Attackers use various tricks to spread DarkRAT, including malicious attachments, fake software updates, untrustworthy download sources, and software cracks. Staying vigilant and cautious online can help you avoid falling victim to DarkRAT and similar threats.

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	T1059	Command and Scripting Interpreter
Persistence	T1574.002	DLL Side-Loading
Privilege Escalation	T1574.002	DLL Side-Loading
Defence Evasion	T1027 T1064	Obfuscated Files or Information Scripting
Credential Access	T1056	Input Capture
Discovery	T1010 T1082	Application Window Discovery System Information Discovery
Collection	T1056	Input Capture
Command-and-Control	T1071	Application Layer Protocol

3. AhMyth RAT

AhMyth RAT is a malicious program targeting Android devices. Disguised as legitimate apps like games or screen recorders, it tricks users into installing it. Once on the device, AhMyth steals sensitive information like banking credentials, two-factor codes, and even captures screenshots. It also functions as a remote control, allowing attackers to view the phone's camera feed, record audio, and access data like call logs and contacts. This versatility makes AhMyth a dangerous tool in the hands of cybercriminals.

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
Command-and-Control	T1071	Application Layer Protocol
	T1571	Non-Standard Port
	T1573	Encrypted Channel
Defence Evasion	T1406	Obfuscated Files or Information
	T1447	Delete Device Data
	T1523	Evade Analysis Environment
Credential Access	T1412	Capture SMS Messages
Discovery	T1421	System Network Connections Discovery
	T1426	System Information Discovery
	T1430	Location Tracking
Impact	T1447	Delete Device Data
	T1448	Carrier Billing Fraud
Collection	T1412	Capture SMS Messages
	T1429	Audio Capture
	T1430	Location Tracking
	T1432	Access Contact List
	T1433	Access Call Logs
	T1507	Network Information Discovery

4. Borr Malware

Borr malware is a sneaky threat lurking in the shadows of the internet. This malware family hides on Windows devices, granting remote access to attackers. The source code's public availability allows anyone with programming knowledge to modify it for their malicious purposes. Once infected, a device under Borr's control exposes sensitive information as attackers can download, upload, and manipulate files. Staying vigilant and using reliable antivirus software are crucial defences against Borr malware and its kin.

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	T1047 T1053	Windows Management Instrumentation Scheduled Task/Job
Persistence	T1053 T1574.002	Scheduled Task/Job DLL Side Loading
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1027 T1027.002	Obfuscated File or Information Software Packing
Credential Access	T1003	OS Credential Dumping
Discovery	T1012 T1057 T1082 T1518.001	Query Registry Process Discovery System Information Discovery Security Software Discovery
Collection	T1005	Data from Local System
Command-and-Control	T1071	Application Layer Protocol

Known exploited vulnerabilities (Week 2 May 2024):

Vulnerability	CVSS	Description
CVE-2024-4671	Ongoing Analysis (High)	Use-After-Free Google Chrome vulnerability

Updated Malware Signatures (Week 2 May 2024)

Threat	Description
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.
CoinMiner	This malicious software installs and runs cryptocurrency mining applications.
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.
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.

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

LockBit3.0 ransomware stands out as the most prolific, having updated a significant number of victims (52%) distributed across multiple countries. In comparison, Stormous ransomware updated 7% 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	0.45%
Akira	0.45%
Bianlian	0.90%
Black Suit	2.71%
Blackbasta	4.52%
Clop	1.81%
Dan0N	1.81%
Darkvault	0.90%
Embargo	0.45%
Eraleign (Apt73)	0.45%
Everest	1.36%
Fsociety	1.81%
Hunters	1.81%
INC Ransom	3.62%
Lockbit3	52.49%
Medusa	3.62%
Metaencryptor	2.71%
Play	4.07%
Qilin	3.62%
Ransomhub	2.26%
Rhysida	0.45%
Stormous	7.24%
Team Underground	0.45%

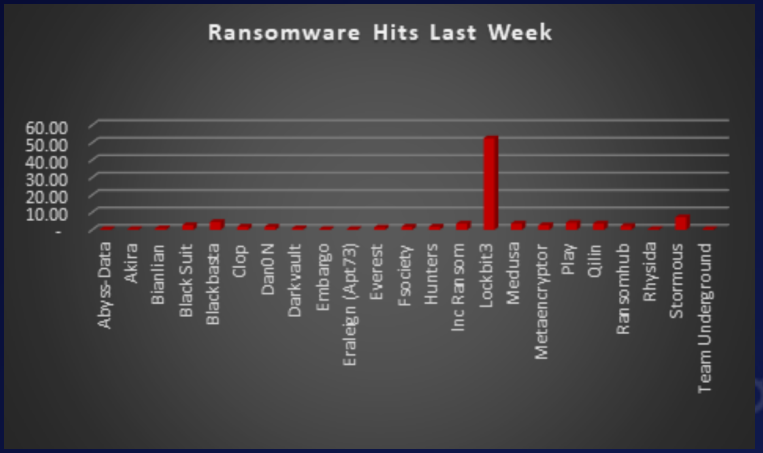


Figure 1: Ransomware Group Hits Last Week

Stormous Ransomware Group

Stormous is a ransomware group notorious for targeting a wide range of entities, including websites, companies, and organisations primarily in the United States and Ukraine. Their modus operandi involves encrypting victims' data and demanding payment for its release, posing significant threats to data security and integrity.

The group has garnered attention for claiming responsibility for cyber-attacks on major American brands such as Coca-Cola, Mattel, and Danaher. Additionally, they have targeted critical entities like the Ukraine Ministry of Foreign Affairs, acquiring sensitive information in the process.

One distinguishing aspect of Stormous is their proclaimed allegiance to Russia in its ongoing conflict with Ukraine. Exploiting the heightened tensions between the two nations, Stormous has used this allegiance to bolster their reputation. However, there exists a debate among experts regarding whether their actions are politically motivated or primarily driven by financial gain.

Tactics, Techniques, and Procedures (TTPs)

Phishing Email: Phishing emails represent one of the most prevalent infection vectors utilised by ransomware, Stormous included. These deceptive emails often contain malicious attachments or links. Upon interaction, such as clicking a link or opening an attachment, the ransomware is downloaded and executed on the victim's system. Stormous utilises phishing emails that masquerade as messages from organisations claiming to assist victims of the conflict in Ukraine.

Exploiting vulnerabilities: Stormous may exploit vulnerabilities within software or operating systems to infiltrate systems. This encompasses unpatched systems, vulnerable websites, and compromised VPN servers.

Remote Desktop Protocol (RDP): RDP facilitates remote access to computers or servers. If RDP configurations are inadequately secured, they can serve as entry points for ransomware attacks, including those carried out by Stormous.

Ads and pop-ups: Ransomware, including Stormous, can leverage advertisements and pop-ups on websites as a means of infiltration.

Credential abuse: This involves the illicit use of stolen or weak login credentials to gain unauthorised access to systems.

Stormous ransomware operates according to a typical ransomware attack pattern. While specific details about Stormous ransomware may be limited, we can deduce its operational method based on general knowledge about ransomware attacks.

Initial infection

Stormous ransomware gains entry to a computer or network through various means, including exploiting software vulnerabilities, phishing emails, or Remote Desktop Protocol (RDP) attacks.

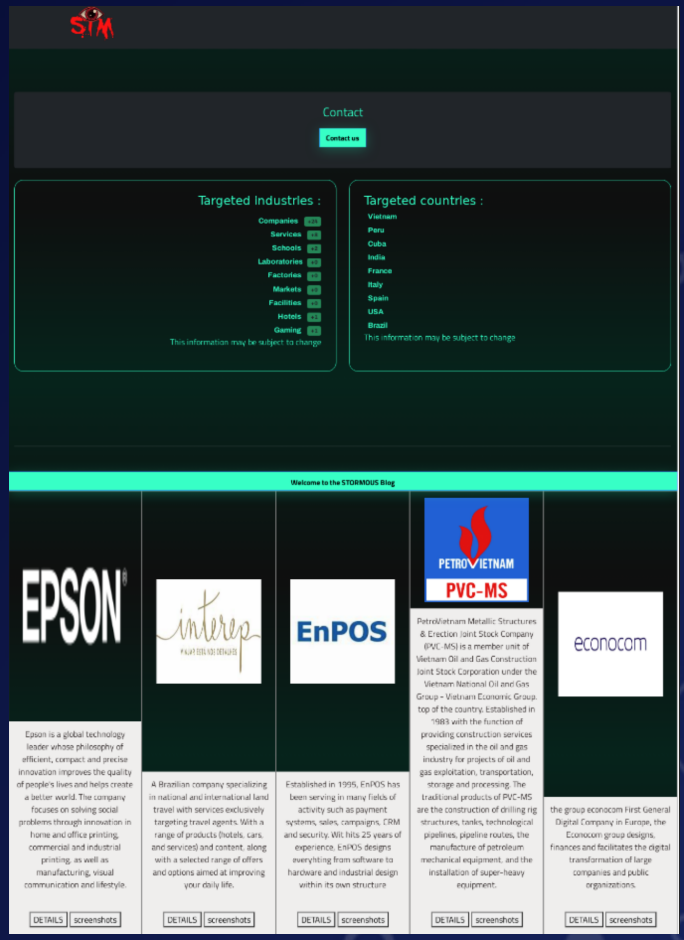
File Encryption

Once infiltrated, Stormous ransomware initiates the encryption process, locking files on the infected device and potentially extending to connected network drives.

Ransom Demand

Following file encryption, a ransom note is typically delivered, demanding payment in exchange for the decryption key and a pledge not to leak the stolen data. Attackers commonly demand payment in cryptocurrencies like Bitcoin to obscure transaction tracing.

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



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
96ba3ba94db07e895090cdaca701a922523649cf6d6801b358c5ff62416be9fa b7863120606168b3731395d9850bbf25661d05c6e094c032fc486e15daeb5666	Hash	Stormous Ransomware
3slz4povugieoi3tw7sblxoowxhbzxeju427cffsst5fo2tizepwatid.onion h3reihqb2y7woqdary2g3bmk3apgtxuyhx4j2ftovbhe3l5svev7bdyd.onion ransekgbpijp56bflufgxptwn5hej2rztx423v6sim2zrzz7xetnr2qd.onion pdcizqzjitsgfcgqeyhuee5u6uki6zy5slzioinlhx6xjnsw25irdgqd.onion stmxylixiz4atpmkspvhkym4xccjvpcv3v67uh3dze7xwwhtnz4faxid.onion	URLs	Leak Site

In a comprehensive analysis of ransomware victims across 45 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 46% 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 (%)
Afghanistan	0.45%
Belgium	0.90%
Brazil	1.36%
Canada	4.98%
Chile	0.45%
China	0.90%
Colombia	0.45%
Croatia	0.45%
Czech Republic	0.45%
Denmark	0.45%
Egypt	0.90%
France	4.07%
Germany	5.43%
India	4.07%
Indonesia	0.45%
Ireland	0.45%
Island	0.45%
Israel	0.45%
Italy	3.17%
Japan	0.45%
Lebanon	0.45%
Malaysia	0.45%
Mexico	1.81%
Mozambique	0.45%
Namibia	0.45%
Netherlands	0.90%

Industry	Victims Count (%)
Nigeria	0.45%
Peru	0.45%
Poland	0.45%
Singapore	0.45%
Slovakia	0.45%
South Africa	0.45%
South Korea	0.45%
Spain	3.17%
Sri Lanka	0.45%
Sweden	0.90%
Switzerland	0.90%
Taiwan	0.90%
Thailand	0.90%
Turkey	0.90%
UAE	0.90%
UK	4.98%
Ukraine	0.45%
USA	46.15%
Vietnam	0.90%

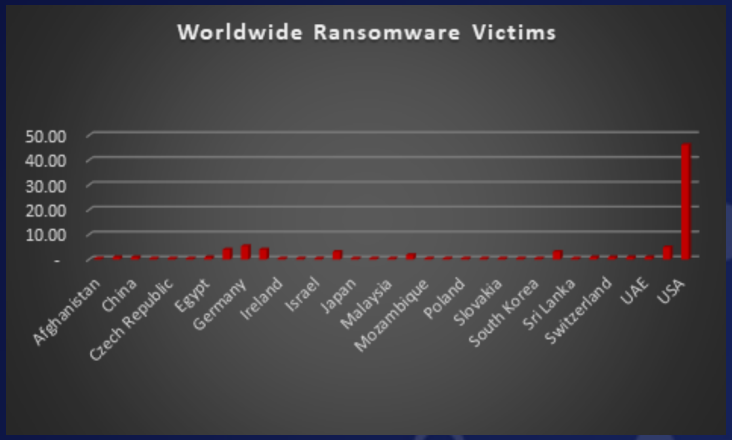


Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 20 different industries worldwide. Notably, Manufacturing bore the brunt of the attacks in the past week, accounting for 20% 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	12.67
Construction	6.79
Consumer Services	3.62
Education	4.98
Energy, Utilities & Waste Treatment	0.45
Finance	4.07
Government	3.17
Healthcare	8.14
Hospitality	4.07
IT	6.33
Legal Services	3.17
Manufacturing	20.36
Media & Internet	0.90
Metals & Mining	0.45
Organisations	3.17
Real Estate	0.45
Retail	9.95
Telecom	2.71
Transportation	4.07
Agriculture	0.45

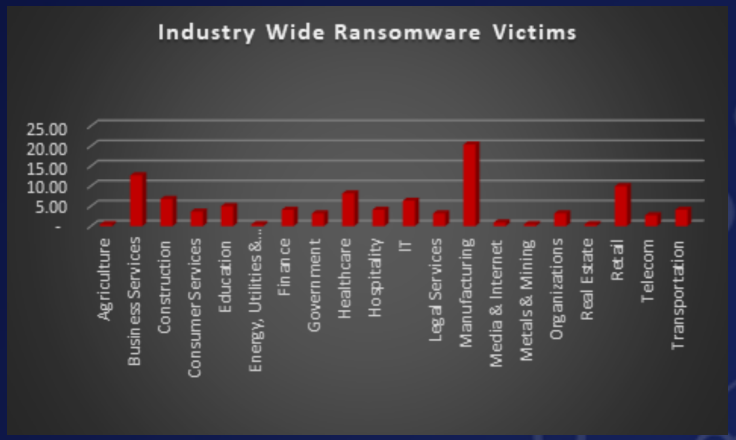


Figure 5: Industry-wise Ransomware Victims