Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 14 - 20, 2024

Report Summary:

- **New Threat Detection Added** – 3 (Gh0stBins Malware, DarkComet RAT and DarkGate Malware)
- **New Threat Protections - 183**

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

1. Gh0stBins Malware

Gh0stBins is a nasty piece of malware classified as a Remote Access Trojan (RAT). This means it gives attackers full control over your device once infected. Launched in 2008, it's been a favourite tool for cybercriminals targeting governments and corporations. Be cautious of spam emails, as they're a common way Gh0stBins spreads. If infected, your privacy is at risk, you could suffer financial losses, and even have your identity stolen.

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
Discovery	T1082	System Information Discovery
Defence Evasion	T1027 T1140 T1574.001	Obfuscated Files or Information Deobfuscate/Decode Files or Information Hijack Execution Flow: DLL Search Order Hijacking
Command-and-Control	T1071.001 T1105 T1572	Application Layer Protocol Ingress Tool Transfer Protocol Tunnelling

2. DarkComet RAT

DarkComet RAT, short for Remote Access Trojan, is a malicious program that lurks in the shadows. Developed in 2008, it gives attackers remote control over your computer, allowing them to steal sensitive information, spy on your activity, and even manipulate your device. While its creator intended it as a legitimate tool, it gained notoriety for its use in cyberattacks, including the Syrian Civil War. Though development has ceased, DarkComet remains a threat.

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
Defence Evasion	T1036 T1055 T1064 T1070.004	Masquerading Process Injection Scripting File Deletion
Discovery	T1082 T1087	System Information Discovery Account Discovery
Command-and-Control	T1071 T1095 T1105	Application Layer Protocol Non-Application Layer Protocol Ingress Tool Transfer

3. DarkGate Malware

DarkGate malware lurks as a backdoor threat, silently granting remote access to your system. First appearing in 2017, it's become a favourite tool for cybercriminals sold as Malware-as-a-Service (MaaS). DarkGate empowers attackers with a buffet of malicious options, including stealing information, deploying cryptocurrency miners to steal your processing power for their gain, and even launching further attacks from your compromised device. Phishing emails and collaborative applications like Microsoft Teams are common ways DarkGate infiltrates systems.

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
Execution	T1059 T1059.001 T1064 T1106	Command and Scripting Interpreter Powershell Scripting Native API
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1036 T1055 T1064 T1070.004 T1497 T1564	Masquerading Process Injection Scripting File Deletion Virtualization/Sandbox Evasion Hide Artifacts
Discovery	T1082 T1087	System Information Discovery Account Discovery
Collection	T1005	Data from Local System
Command-and-Control	T1071 T1095 T1105	Application Layer Protocol Non-Application Layer Protocol Ingress Tool Transfer

Known exploited vulnerabilities (Week 3 May 2024):

Vulnerability	CVSS	Description
CVE-2024-30040	8.8 (High)	Microsoft Windows MSHTML Platform Security Feature Bypass Vulnerability
CVE-2024-30051	7.8 (High)	Microsoft DWM Core Library Privilege Escalation Vulnerability
CVE-2024-4761	Ongoing analysis	Google Chromium V8 Out-of-Bounds Memory Write Vulnerability
CVE-2021-40655	7.5 (High)	D-Link DIR-605 Router Information Disclosure Vulnerability
CVE-2014-100005	6.8 (Medium)	D-Link DIR-600 Router Cross-Site Request Forgery (CSRF) Vulnerability

Updated Malware Signatures (Week 3 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 21 different industries spanning 22 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 (18%) distributed across multiple countries. In comparison, DragonForce ransomware updated 12% 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
3AM	2.20%
8Base	8.79%
Akira	3.30%
Arcus Media	7.69%
Bianlian	2.20%
Black Suit	2.20%
Cactus	4.40%
DragonForce	12.09%
Everest	1.10%
Hunters	2.20%
Inc Ransom	8.79%
Killsec	2.20%
Lockbit3	18.68%
Money Message	1.10%
Monti	2.20%
Play	4.40%
Qilin	3.30%
Ransomhouse	2.20%
Ransomhub	7.69%
Rhysida	1.10%
Snatch	1.10%
Stormous	1.10%

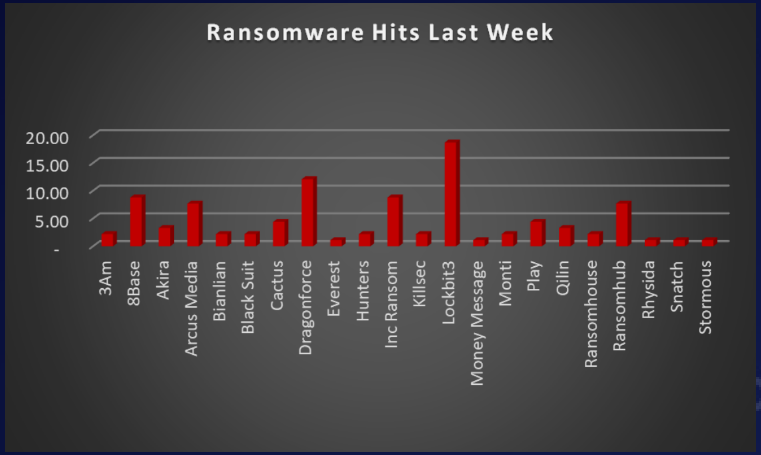


Figure 1: Ransomware Group Hits Last Week

DragonForce Ransomware

Emerging in late 2023, DragonForce ransomware has quickly become a force to be reckoned with 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 aren't met.

The origins of DragonForce remain shrouded in some mystery. While a Malaysian hacktivist group of the same name announced plans to launch ransomware in 2022, the connection to the current DragonForce ransomware is unclear. Security researchers believe the ransomware itself is built upon the leaked codebase of LockBit Black, a notorious ransomware group. This shared lineage suggests a certain level of sophistication, as LockBit Black was known for its effectiveness.

Tactics, Techniques, and Procedures (TTPs)

DragonForce leverages a range of tactics, techniques, and procedures (TTPs) to infiltrate and compromise systems. These include:

- Phishing Attacks: Deceptive emails designed to trick users into clicking malicious links or downloading infected attachments are a common entry point.
- Exploiting Vulnerabilities: DragonForce actively seeks out unpatched vulnerabilities in software and operating systems to gain unauthorised access to networks.
- Lateral Movement: Once a foothold is established, the malware can spread laterally across a network, infecting additional devices and escalating privileges.
- Data Exfiltration: Before encryption, DragonForce exfiltrates sensitive data like financial records, personal information, and intellectual property. This stolen data serves as leverage in extortion attempts.
- Strong Encryption: DragonForce utilises robust encryption algorithms to render files inaccessible, making decryption without the attacker's key extremely difficult, if not impossible.

Famous Fallouts:

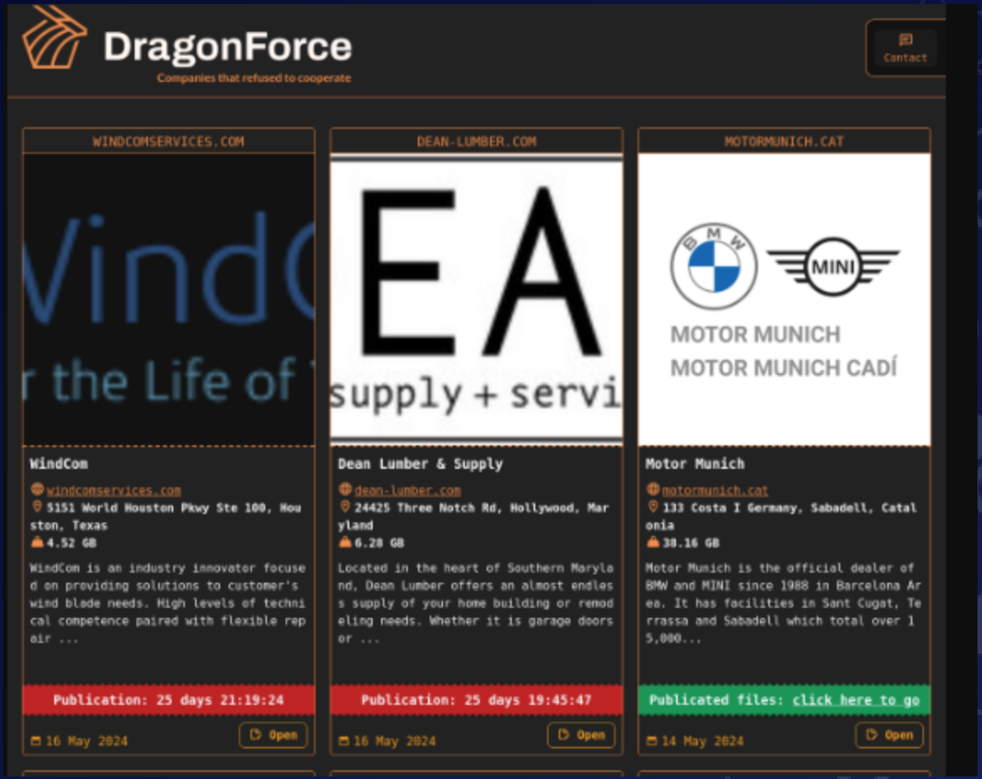
DragonForce has targeted a diverse range of victims worldwide, demonstrating its opportunistic nature. Some notable examples include:

- The Ohio Lottery: In a high-profile attack, DragonForce breached the Ohio Lottery's systems and claimed to have stolen over 600 GB of data, potentially compromising millions of records.
- Yakult Australia: DragonForce ransomware claimed to have attacked this beverage company, boasting about stealing nearly 100 GB of sensitive company data.
- Coca-Cola Singapore: DragonForce ransomware claimed to have attacked the Singapore branch of Coca-Cola, stealing data exceeding 400 GB.

Global Targets: Its reach extends beyond these specific cases. Reports indicate that DragonForce has targeted organisations in manufacturing, technology, healthcare, finance, and other critical sectors across various countries.

DragonForce's emergence highlights the ever-evolving threat landscape of ransomware. Its use of readily available tools like LockBit Black's codebase and its focus on double extortion tactics underscore the need for organisations to prioritise cybersecurity measures.

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



DragonForce

Companies that refused to cooperate

WINDCOMSERVICES.COM

WindCom

windcomservices.com
5151 World Houston Pkwy Ste 100, Houston, Texas
4.52 GB

WindCom is an industry innovator focused on providing solutions to customer's wind blade needs. High levels of technical competence paired with flexible repair ...

Publication: 25 days 21:19:24

16 May 2024

DEAN-LUMBER.COM

Dean Lumber & Supply

dean-lumber.com
24425 Three Notch Rd, Hollywood, Maryland
6.28 GB

Located in the heart of Southern Maryland, Dean Lumber offers an almost endless supply of your home building or remodeling needs. Whether it is garage doors or ...

Publication: 25 days 19:45:47

16 May 2024

MOTORMUNICH.CAT

Motor Munich

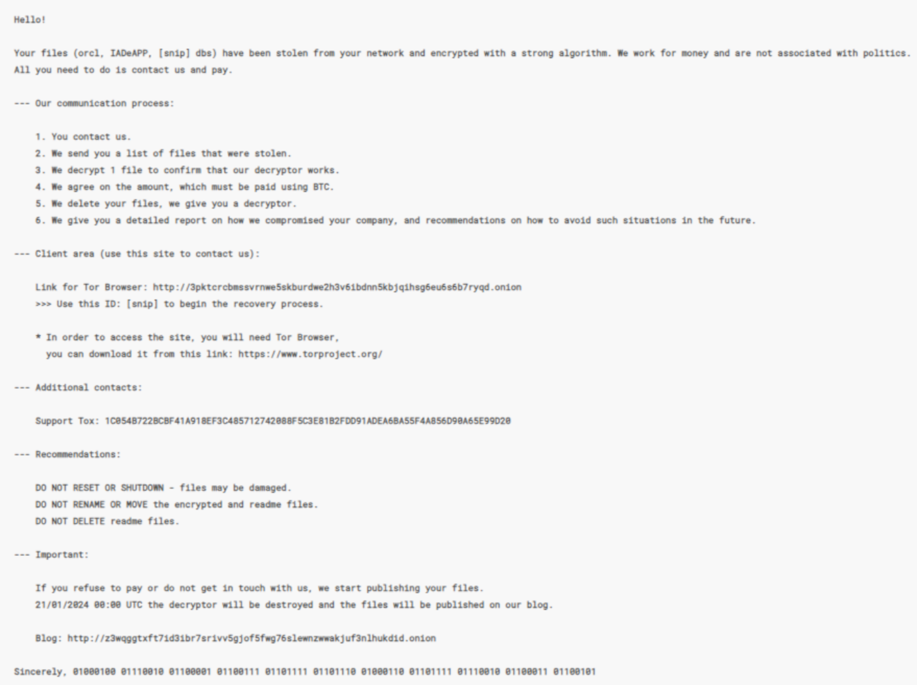
motormunich.cat
133 Costa I Germany, Sabadell, Catalonia
38.16 GB

Motor Munich is the official dealer of BMW and MINI since 1988 in Barcelona Area. It has facilities in Sant Cugat, Terrassa and Sabadell which total over 15,000...

Publicated files: click here to go

14 May 2024

DragonForce Ransom Notes:



```
Hello!

Your files (orcl, IADeAPP, [snip] dbs) have been stolen from your network and encrypted with a strong algorithm. We work for money and are not associated with politics.
All you need to do is contact us and pay.

--- Our communication process:

    1. You contact us.
    2. We send you a list of files that were stolen.
    3. We decrypt 1 file to confirm that our decryptor works.
    4. We agree on the amount, which must be paid using BTC.
    5. We delete your files, we give you a decryptor.
    6. We give you a detailed report on how we compromised your company, and recommendations on how to avoid such situations in the future.

--- Client area (use this site to contact us):

    Link for Tor Browser: http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion
    >>> Use this ID: [snip] to begin the recovery process.

    * In order to access the site, you will need Tor Browser,
      you can download it from this link: https://www.torproject.org/

--- Additional contacts:

    Support Tox: 1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

--- Recommendations:

    DO NOT RESET OR SHUTDOWN - files may be damaged.
    DO NOT RENAME OR MOVE the encrypted and readme files.
    DO NOT DELETE readme files.

--- Important:

    If you refuse to pay or do not get in touch with us, we start publishing your files.
    21/01/2024 00:00 UTC the decryptor will be destroyed and the files will be published on our blog.

    Blog: http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion

Sincerely, 01000100 01110010 01100001 01100111 01101111 01101110 01000110 01101111 01110010 01100011 01100101
```

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1204.002	User Execution
Defence Evasion	T1562.001 T1070.004	Impair Defences: Disable or Modify Tools Indicator Removal: File Deletion
Discovery	T1083	File and Directory Discovery
Impact	T1486	Data Encrypted for Impact

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
d54bae930b038950c2947f5397c13f84	Hash	DragonForce Ransomware
hxxp://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion/blog	URLs	Leak Site

In a comprehensive analysis of ransomware victims across 22 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 48% 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 (%)
Austria	1.10%
Bangladesh	1.10%
Belgium	1.10%
Brazil	6.59%
Canada	5.49%
Chile	1.10%
Colombia	2.20%
Finland	1.10%
France	2.20%
Germany	1.10%
India	2.20%
Iran	1.10%
Italy	3.30%
Japan	1.10%
Mexico	1.10%
Nepal	1.10%
Netherlands	1.10%
Philippines	1.10%
Spain	4.40%
Sudan	1.10%
UK	10.99%
USA	48.35%

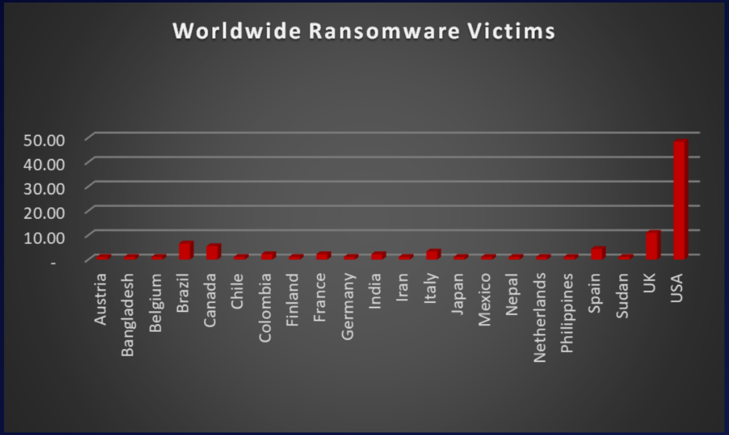


Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 21 different industries worldwide. Notably, Manufacturing bore the brunt of the attacks in the past week, accounting for 17% 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	1.10%
Business Services	15.38%
Cities, Towns & Municipalities	1.10%
Construction	5.49%
Consumer Services	3.30%
Education	8.79%
Energy, Utilities & Waste	3.30%
Finance	7.69%
Government	1.10%
Healthcare	5.49%
Hospitality	5.49%
Insurance	2.20%
IT	2.20%
Legal Services	5.49%
Manufacturing	17.58%
Media & Internet	1.10%
Metals & Mining	1.10%
Real Estate	1.10%
Retail	5.49%
Telecom	1.10%
Transportation	4.40%

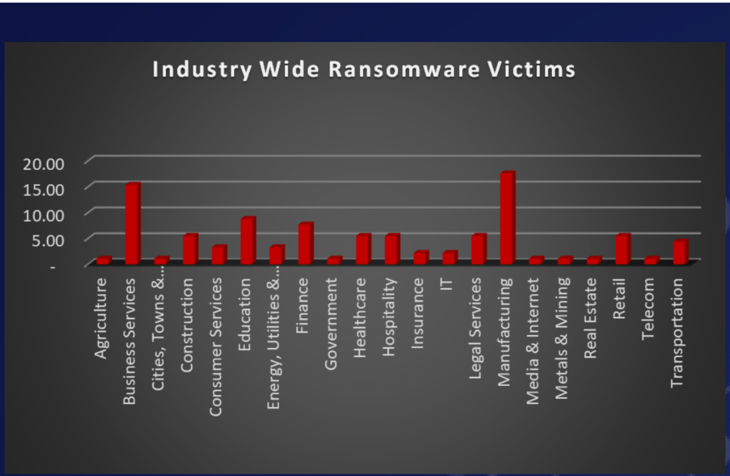


Figure 5: Industry-wise Ransomware Victims