Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

May 21 - 27, 2024

Report Summary:

- **New Threat Detection Added** – 2 (DoraRAT Malware and pcTattletale Spyware)
- **New Threat Protections - 161**

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

1. DoraRAT Malware

DoraRAT is a Remote Access Trojan (RAT) used by the Andariel threat group to target organisations like manufacturers, educational institutions, and construction companies. DoraRAT grants remote access to attackers, allowing them to steal information, control systems, and potentially escalate privileges within the network. It utilises tactics like phishing campaigns to gain initial access and often works alongside other tools like keyloggers and information stealers for comprehensive data theft. Identified in 2024, DoraRAT highlights the evolving methods of cybercriminals.

Rules Created: 04
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	T1059.001 T1064	Powershell Scripting
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1055 T1070.004 T1497	Process Injection File Deletion Virtualization/Sandbox Evasion
Discovery	T1082 T1087	System Information Discovery Account Discovery
Command-and-Control	T1071 T1095	Application Layer Protocol Non-Application Layer Protocol

2. pcTattletale Spyware

pcTattletale is a commercially available spyware program marketed as a parental control or employee monitoring tool. Despite its legitimacy claims, it raises significant privacy concerns. This consumer-grade spyware operates on Windows and Android devices, capturing screenshots, potentially every few seconds, to monitor a target's activity. A critical security flaw exposed these screenshots on pcTattletale's servers, making them accessible to anyone on the internet, not just the authorised user. This incident, where the spyware was found on hotel check-in systems, compromising guest data, highlights the potential dangers of such software in the wrong hands. While pcTattletale may seem convenient for monitoring purposes, its security risks and ethical implications make it a questionable choice for legitimate use.

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
Execution	T1064	Scripting
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1036 T1070.004	Masquerading 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

Known exploited vulnerabilities (Week 4 May 2024):

Vulnerability	CVSS	Description
CVE-2024-4947	8.8 (High)	Google Chromium V8 Type Confusion Vulnerability
CVE-2023-43208	9.8 (Critical)	NextGen Healthcare Mirth Connect Deserialization of Untrusted Data Vulnerability
CVE-2020-17519	7.5 (High)	Apache Flink Improper Access Control Vulnerability

Updated Malware Signatures (Week 4 May 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.
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.
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 18 different industries spanning 19 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

Play and INC Ransom ransomware groups stand out as the most prolific, having updated a significant number of victims (13%) each 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
8Base	4.76%
Akira	4.76%
Bianlian	5.95%
Black Suit	4.76%
Blackbasta	7.14%
Cactus	5.95%
Daixin	1.19%
Donutleaks	1.19%
Embargo	2.38%
Eraleign (APT-73)	1.19%
Hunters	1.19%
INC Ransom	13.10%
Lockbit3	9.52%
Meow	1.19%
Play	13.10%
Qilin	2.38%
Ransomhouse	10.71%
Ransomhub	5.95%
Red Ransomware	1.19%
Rhysida	1.19%
Team Underground	1.19%

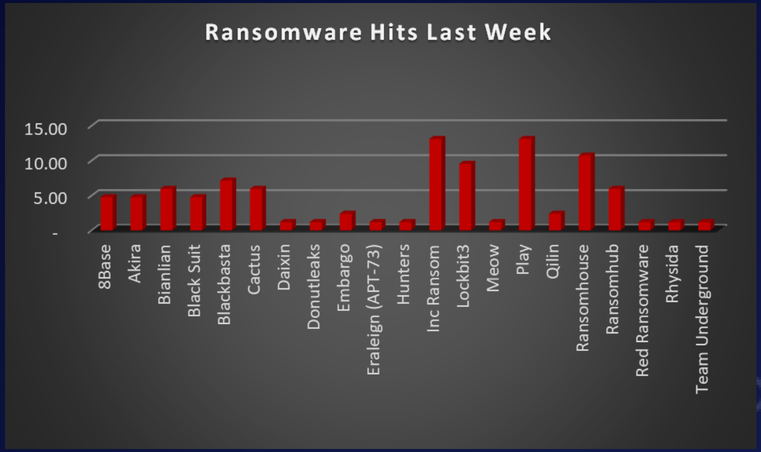


Figure 1: Ransomware Group Hits Last Week

Play Ransomware

Emerging in mid-2022, Play ransomware has swiftly established itself as a formidable foe 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. While the exact origins of Play remain shrouded in some mystery, security researchers believe it may be linked to a Malaysian hacktivist group of the same name. However, the technical prowess exhibited by the Play ransomware itself suggests it leverages the leaked codebase of LockBit Black, a notorious ransomware group known for its effectiveness

Tactics, Techniques, and Procedures (TTPs):

Play ransomware doesn't rely on brute force alone. It possesses a diverse arsenal of tactics, techniques, and procedures (TTPs) to infiltrate and compromise systems. Here are some of the most common:

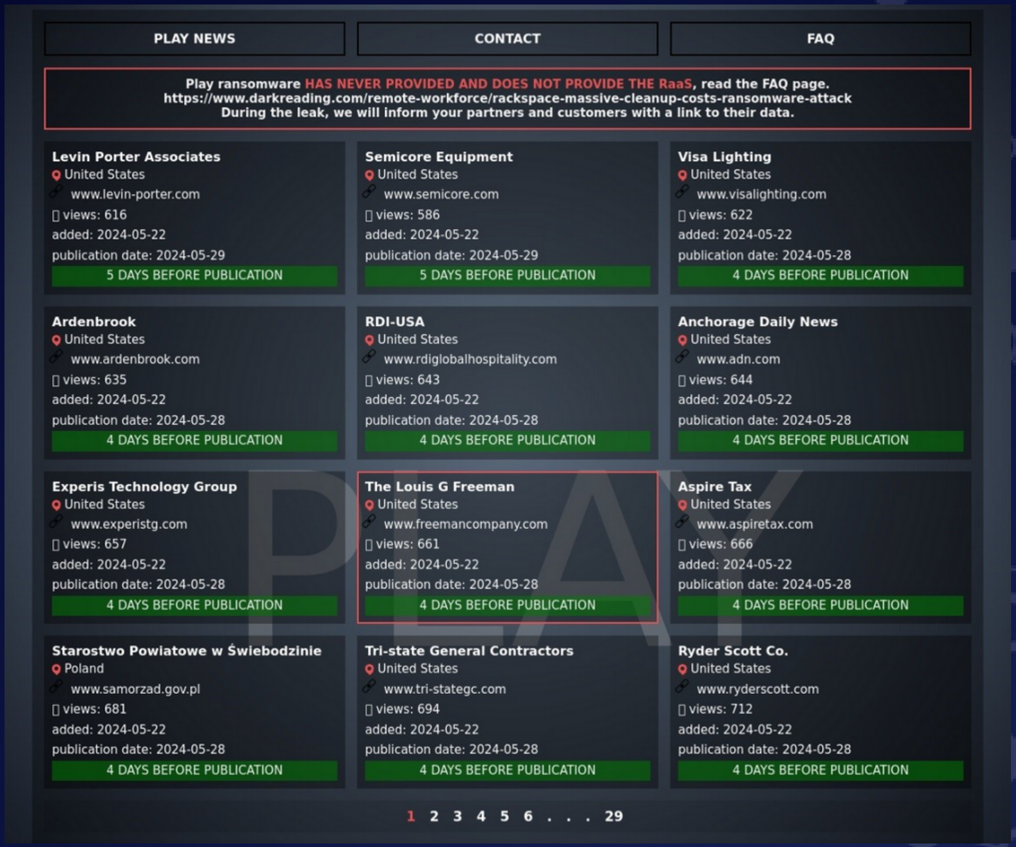
- Phishing Attacks: Deceptive emails designed to trick users into clicking malicious links or downloading infected attachments are a frequent entry point. These emails may appear to be from legitimate sources, such as banks, logistics companies, or even colleagues.
- Exploiting Vulnerabilities: Play actively seeks out unpatched vulnerabilities in software and operating systems to gain unauthorised access to networks. This highlights the importance of keeping software and systems updated with the latest security patches.
- Lateral Movement: Once a foothold is established on a single device, Play can utilise various tools to move laterally across a network. This allows it to infect additional devices and escalate privileges, potentially compromising critical systems.
- Living-off-the-Land Techniques: Play can employ 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, Play 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.
- Robust Encryption: Play utilises strong 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.

Famous Fallouts:

Play ransomware doesn't discriminate. It has targeted a wide range of victims worldwide, demonstrating its opportunistic nature. Here are some notable examples:

- Government Entities in Latin America: Early reports in July 2022 indicated Play ransomware attacks targeting government entities in Latin America.
- Global Manufacturing: Manufacturing companies across the globe have fallen victim to Play, experiencing data breaches and operational disruptions.
- Critical Infrastructure: The increasing sophistication of Play raises concerns about potential attacks on critical infrastructure, such as power grids or transportation systems.

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



Play ransomware HAS NEVER PROVIDED AND DOES NOT PROVIDE THE RaaS, read the FAQ page.
https://www.darkreading.com/remote-workforce/rackspace-massive-cleanup-costs-ransomware-attack
During the leak, we will inform your partners and customers with a link to their data.

Levin Porter Associates
United States
www.levin-porter.com
□ views: 616
added: 2024-05-22
publication date: 2024-05-29
5 DAYS BEFORE PUBLICATION

Semicore Equipment
United States
www.semicore.com
□ views: 586
added: 2024-05-22
publication date: 2024-05-29
5 DAYS BEFORE PUBLICATION

Visa Lighting
United States
www.visalighting.com
□ views: 622
added: 2024-05-22
publication date: 2024-05-28
4 DAYS BEFORE PUBLICATION

Ardenbrook
United States
www.ardenbrook.com
□ views: 635
added: 2024-05-22
publication date: 2024-05-28
4 DAYS BEFORE PUBLICATION

RDI-USA
United States
www.rdiglobalhospitality.com
□ views: 643
added: 2024-05-22
publication date: 2024-05-28
4 DAYS BEFORE PUBLICATION

Anchorage Daily News
United States
www.adn.com
□ views: 644
added: 2024-05-22
publication date: 2024-05-28
4 DAYS BEFORE PUBLICATION

Experis Technology Group
United States
www.experistg.com
□ views: 657
added: 2024-05-22
publication date: 2024-05-28
4 DAYS BEFORE PUBLICATION

The Louis G Freeman
United States
www.freemancompany.com
□ views: 661
added: 2024-05-22
publication date: 2024-05-28
4 DAYS BEFORE PUBLICATION

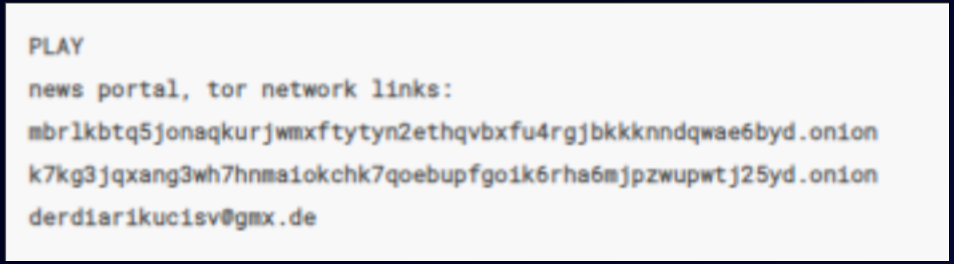
Aspire Tax
United States
www.aspiretax.com
□ views: 666
added: 2024-05-22
publication date: 2024-05-28
4 DAYS BEFORE PUBLICATION

Starostwo Powiatowe w Świebodzinie
Poland
www.samorzad.gov.pl
□ views: 681
added: 2024-05-22
publication date: 2024-05-28
4 DAYS BEFORE PUBLICATION

Tri-state General Contractors
United States
www.tri-stategc.com
□ views: 694
added: 2024-05-22
publication date: 2024-05-28
4 DAYS BEFORE PUBLICATION

Ryder Scott Co.
United States
www.ryderscott.com
□ views: 712
added: 2024-05-22
publication date: 2024-05-28
4 DAYS BEFORE PUBLICATION

Play Ransomware Ransom notes



```
PLAY
news portal, tor network links:
mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion
derdiarikucisv@gmx.de
```

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
762bb8a7209da29afb89f7941ae1c00a04cf45a144c6c5dddcfa78ff0d941539	Hash	Play Ransomware
hxxp://mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion hxxp://k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion	URLs	Leak Site

In a comprehensive analysis of ransomware victims across 19 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 63% 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	1.19%
Australia	1.19%
Bermuda	1.19%
Canada	4.76%
Chian	1.19%
Chile	1.19%
Czech Republic	1.19%
France	1.19%
Germany	2.38%
India	1.19%
Italy	2.38%
Japan	1.19%
Mexico	1.19%
Philippines	1.19%
Portugal	1.19%
Taiwan	1.19%
UK	10.71%
USA	63.10%
Vietnam	1.19%

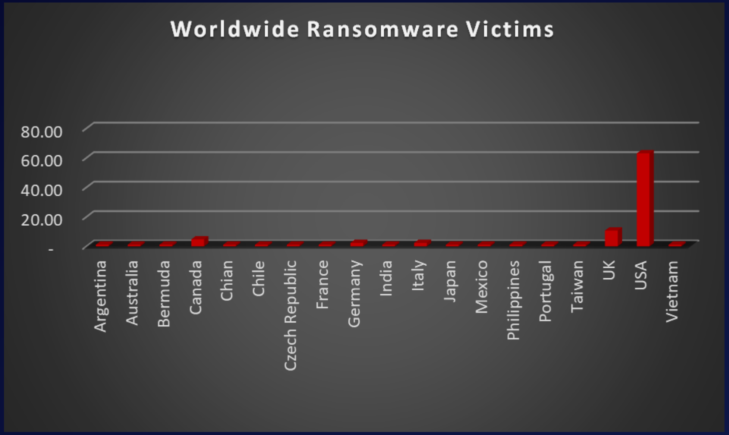


Figure 4: Ransomware Victims Worldwide

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 22% 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	5.95%
Construction	10.71%
Consumer Services	3.57%
Education	4.76%
Energy, Utilities & Waste Treatment	1.19%
Finance	2.38%
Government	2.38%
Healthcare	9.52%
Hospitality	1.19%
Insurance	1.19%
IT	5.95%
Legal Services	2.38%
Manufacturing	22.62%
Media & Internet	3.57%
Organisations	3.57%
Real Estate	2.38%
Retail	10.71%
Transportation	5.95%

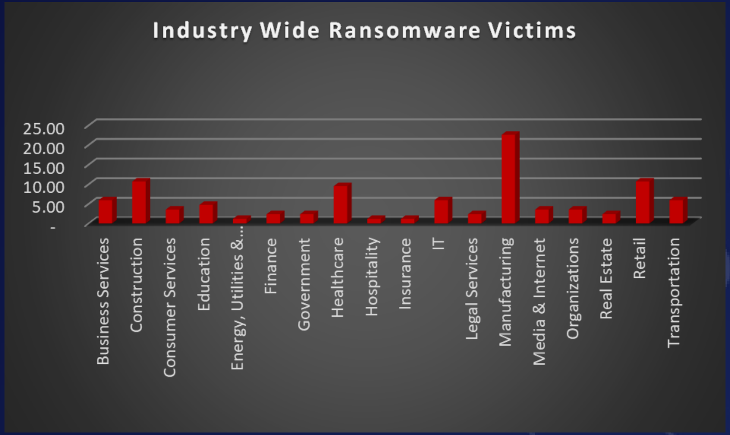


Figure 5: Industry-wise Ransomware Victims