Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

June 4 - 10, 2024

Report Summary:

- **New Threat Detection Added** – 3 (PikaBot Malware, RubySleet APT and MageCart Malware)
- **New Threat Protections - 112**

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

1. PikaBot Malware

PikaBot is not a benign electric mouse this time. The PikaBot Java Loader is a malicious program designed to infiltrate systems and deploy the more dangerous PikaBot core module. This two-part attacker reassembles itself upon entry. The loader, written in Java, fetches chunks of encrypted data hidden within itself and decrypts them to form the core module. This core is the real troublemaker, a backdoor allowing remote attackers to control the system, steal data, and potentially deploy ransomware. PikaBot's distribution methods are as sly as its namesake. Phishing emails with malicious attachments or links are a common tactic. Once downloaded, the Java Loader silently executes in the background, giving attackers a foothold within your system.

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
Discovery	T1082 T1518.001	System Information Discovery Security Software Discovery
Command-and-Control	T1071 T1095 T1105	Application Layer Protocol Non-Application Layer Protocol Ingress Tool Transfer

2. RubySleet APT

RubySleet APT, also known as APT37, Reaper, and Ricochet Chollima, is a North Korean state-sponsored threat group, active since at least 2012. They primarily target organisations in South Korea but have also been linked to attacks in Japan, Vietnam, and the Middle East. Their objectives lie in information theft and espionage. RubySleet utilises social engineering tactics and exploits vulnerabilities in software like Hangul Word Processor and Adobe Flash to gain initial access. Once inside, they deploy a diverse arsenal of custom malware for espionage purposes, including tools for stealing data and maintaining persistence on the system. The group is known for its increasing sophistication, improving operational security over time.

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
Initial Access	T1049	Phishing Email
Delivery	T1040	Malicious File
Execution	T1047 T1059	Windows Management Instrumentation Command and Scripting Interpreter
Persistence	T1547.001 T1574.002	Registry Run Key/ Startup Folder DLL Side-Loading
Privilege Escalation	T1055 T1547.001	Process Injection Registry Run Key/ Startup Folder
Defence Evasion	T1036 T1055	Masquerading Process Injection
Discovery	T1012 T1057 T1082	Query Registry Process Discovery System Information Discovery
Command-and-Control	T1073 T1071	Encrypted Channel Application Layer Protocol

3. MageCart Malware

MageCart is not a single malware but refers to a group or a collection of groups specialising in web skimming attacks targeting e-commerce platforms. These digital thieves inject malicious code, often Javascript, into vulnerable parts of a website's checkout process. This hidden code lurks silently, capturing sensitive payment information like credit card details as unsuspecting customers enter them. MageCart attacks are notorious for their stealth and the variety of tactics employed. They can target vulnerabilities in e-commerce platforms, third-party plugins, or even compromise supply chains to inject their skimmers. The stolen data is then exfiltrated to the attacker's servers and potentially sold on the dark web.

Rules Created: 30
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	T1055	Process Injection
Defence Evasion	T1055	Process Injection
Discovery	T1012 T1018	Query Registry Remote System Discovery
Command-and-Control	T1071	Application Layer Protocol

Known exploited vulnerabilities (Week 1 June 2024):

Vulnerability	CVSS	Description
CVE-2017-3506	7.4 (High)	Oracle WebLogic Server OS Command Injection Vulnerability

For more information, please visit the **Red Piranha Forum**.

Updated Malware Signatures (Week 1 June 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.
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 23 industries spanning 29 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 stand out as the most prolific, having updated a significant number of victims (45%) distributed across multiple countries. In comparison, El Dorado 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	1.67%
Akira	3.33%
Arcus Media	3.33%
Bianlian	0.83%
Blackbasta	4.17%
Cactus	2.50%
Daixin	0.83%
Dragonforce	0.83%
El Dorado	10.83%
Embargo	0.83%
Everest	2.50%
Handala	1.67%
Hunters	1.67%
Inc Ransom	0.83%
Lockbit3	4.17%
Mallox	2.50%
Medusa	8.33%
Qilin	1.67%
Ransomhub	45.83%
Sensayq	1.67%

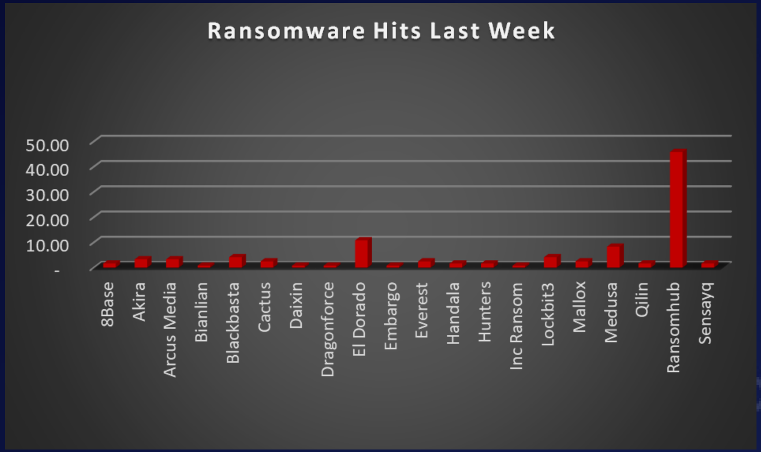


Figure 1: Ransomware Group Hits Last Week

El Dorado Ransomware

Surfacing in mid-2022, El Dorado ransomware quickly carved a niche in the cybercrime landscape. This malware strain employs a ruthless double extortion tactic, encrypting a victim's data and threatening to leak it on the dark web if ransom demands aren't met. While the exact origins of El Dorado remain unclear, security researchers suspect a connection to a Russian-speaking cybercriminal group. This group's past activities suggest a proficiency in developing and deploying malware, making El Dorado a potentially sophisticated threat.

Tactics, Techniques, and Procedures (TTPs):

El Dorado doesn't rely solely on brute force attacks. It wields a diverse arsenal of tactics, techniques, and procedures (TTPs) to infiltrate and compromise systems. Here's a glimpse into its malicious toolkit:

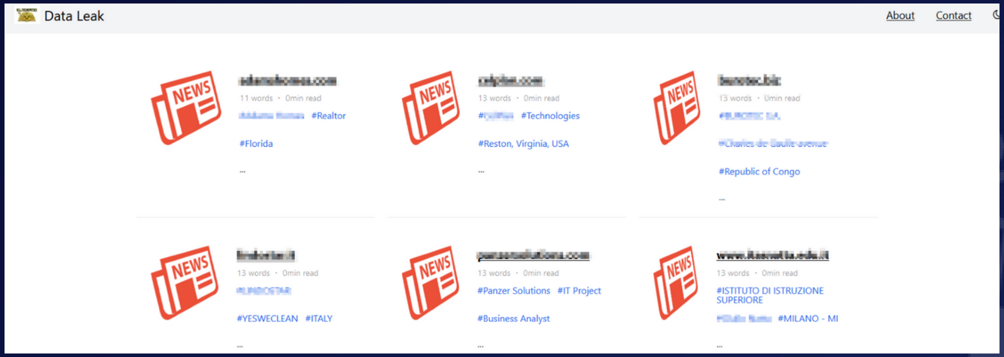
- **Phishing Attacks**
  Deceptive emails that trick users into clicking malicious links or downloading infected attachments are a common entry point. These emails may appear to be from legitimate sources, such as banks, logistics companies, or even colleagues.
- **Exploiting Unpatched Vulnerabilities**
  El Dorado actively seeks out unpatched vulnerabilities in software and operating systems to gain unauthorised access to networks. This highlights the importance of keeping all systems and software updated with the latest security patches.
- **Remote Desktop Protocol (RDP) Exploitation**
  Like Medusa ransomware, El Dorado 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.
- **Supply Chain Attacks**
  El Dorado might target vulnerabilities in software suppliers or third-party vendors to gain access to a wider network. By compromising a trusted vendor, attackers can infiltrate a larger number of victims through a single point of entry.
- **Living-off-the-Land Techniques**
  Like many malware strains, El Dorado 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, El Dorado 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.
- **Strong Encryption**
  The malware utilises robust 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:

El Dorado ransomware exhibits a mix of global reach and targeted attacks. Here are some examples:

- Small and Medium-Sized Businesses (SMBs): SMBs are a frequent target for El Dorado attacks due to their potentially less robust cybersecurity defences compared to larger enterprises.
- Critical Infrastructure: There have been concerns about El Dorado targeting critical infrastructure sectors like power grids and transportation systems. A successful attack on such infrastructure could have devastating consequences.
- Supply Chain Disruptions: El Dorado's use of supply chain attacks raises concerns about large-scale disruptions across multiple industries.

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



[redacted]
11 words · 0min read
[redacted] #Realtor
#Florida
...

[redacted]
13 words · 0min read
#[redacted] #Technologies
#Reston, Virginia, USA
...

[redacted]
13 words · 0min read
#[redacted]
#[redacted]
#Republic of Congo
...

[redacted]
13 words · 0min read
#[redacted]
#YESWECLEAN #ITALY
...

[redacted]
13 words · 0min read
#Panzer Solutions #IT Project
#Business Analyst
...

[redacted]
13 words · 0min read
#ISTITUTO DI ISTRUZIONE SUPERIORE
#[redacted] #MILANO - MI
...

The emergence of El Dorado ransomware underscores the constantly evolving threat landscape of cybercrime. Its focus on a mix of exploit types and its ruthless double extortion tactics highlights the need for organisations to prioritise robust cybersecurity measures.

Here are some crucial steps organisations can take to mitigate the risk of El Dorado 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.
- Multi-Factor Authentication (MFA): Enable MFA for all user accounts wherever possible. MFA adds an extra layer of security by requiring a second verification factor beyond just a username and password.
- 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 the first line of defence against El Dorado and other malware threats.
- Network Segmentation: Segmenting your network can limit the lateral movement of ransomware, potentially preventing it from spreading throughout your entire infrastructure.
- Supply Chain Risk Management: Organisations should evaluate the security of their supply chain.

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
hxxp://dataleakypypu7uwblm5kttv726l3iripago6p336xjnbstkjwrlnlid.onion	URLs (Onion)	Leak Site
russoschwartz@onionmail.org	Email	Contact

In a comprehensive analysis of ransomware victims across 29 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 45% 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	0.83%
Argentina	0.83%
Australia	2.50%
Brazil	5.83%
Canada	0.83%
Colombia	0.83%
Congo	0.83%
Croatia	2.50%
Egypt	0.83%
France	0.83%
Germany	0.83%
India	0.83%
Israel	1.67%
Italy	5.00%
Japan	1.67%
Lebanon	0.83%
Malaysia	0.83%
Mexico	0.83%
New Zealand	0.83%
Norway	0.83%
South Africa	1.67%
Spain	1.67%
Sri Lanka	0.83%
Sweden	0.83%
Taiwan	1.67%
Turkey	0.83%
UAE	1.67%
UK	5.83%
USA	54.17%

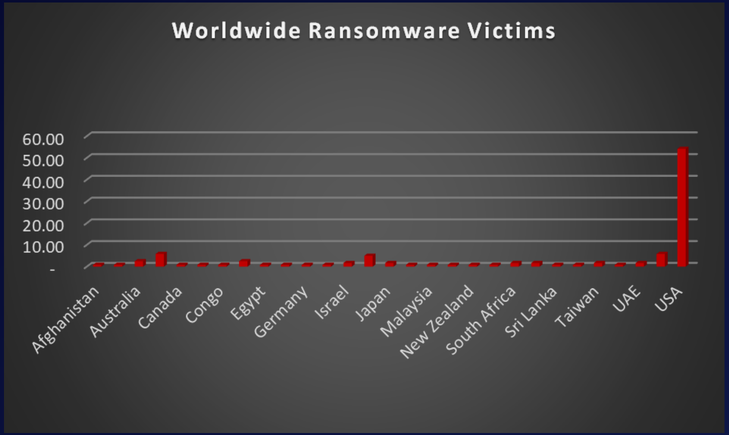


Figure 3: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 23 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	0.83%
Business Services	15.00%
Cities, Towns & Municipalities	0.83%
Construction	7.50%
Consumer Services	2.50%
Education	4.17%
Electricity, Oil & Gas	0.83%
Energy, Utilities & Waste Treatment	1.67%
Finance	4.17%
Government	5.00%
Healthcare	3.33%
Hospitality	5.00%
Insurance	0.83%
IT	4.17%
Legal Services	2.50%
Manufacturing	17.50%
Media & Internet	0.83%
Metals & Mining	1.67%
Organisations	3.33%
Real Estate	0.83%
Retail	9.17%
Telecom	4.17%
Transportation	4.17%

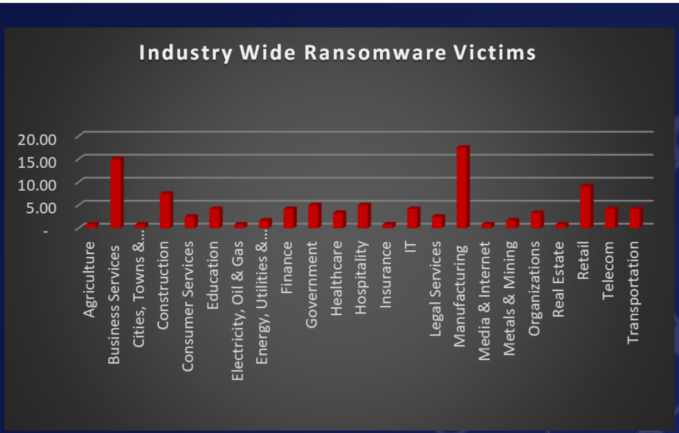


Figure 4: Industry-wise Ransomware Victims