Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 09 - 15, 2024

Report Summary:

- **New Threat Detection Added** – 2 (BluStealer Malware and CHAOS RAT)
- **New Threat Protections - 200**

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

1. BluStealer Malware

BluStealer is a lurking information-stealing malware with a knack for customisation. First appearing in 2021, it's known for snatching login credentials, credit card info, and even cryptocurrency wallets. This stealer uses a two-part system: a Visual Basic core that loads separate payloads written in C#. This lets attackers tailor BluStealer's thievery for each victim. Devious yet not picky, BluStealer can target both personal and business devices. It hunts for browser passwords, FTP logins, and snatches crypto wallets, info most people wouldn't store on a work computer. Frighteningly, BluStealer can mask itself, evading detection by some security software.

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	System Information Discovery
Command-and-Control	T1071	Application Layer Protocol
	T1105	Ingress Tool Transfer
	T1095	Non-Application Layer Protocol
	T1571	Non-Standard Port

2. CHAOS RAT

CHAOS RAT, though dramatic in name, is a free, open-source tool with a double-edged sword. On the positive side, it functions as a legitimate Remote Administration Tool (RAT) for system administrators. It lets them remotely control computers, perform tasks like file transfers and screenshots, and gather basic system information. This can be useful for IT support or managing remote devices. However, the open-source nature means anyone can access and potentially misuse CHAOS RAT. In the wrong hands, it can turn malicious. Hackers could use it to establish remote connections to victims' machines, steal data, or launch further attacks.

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	T1106	Native API
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1027	Obfuscated Files or Information
	T1027.002	Software Packing
	T1036	Masquerading
	T1055	Process Injection
	T1497	Virtualization/Sandbox Evasion
Discovery	T1010	Application Window Discovery
	T1012	Query Registry
	T1018	Remote System Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Collection	T1005	Data from Local System
	T1114	Email Collection
Command-and-Control	T1071	Application Layer Protocol
	T1573	Encrypted Channel

Known exploited vulnerabilities (Week 2 July 2024):

Vulnerability	CVSS	Description
CVE-2024-23692	9.8 (Critical)	Rejetto HTTP File Server Improper Neutralization Vulnerability
CVE-2024-38080	7.8 (High)	Microsoft Windows Hyper-V Privilege Escalation Vulnerability
CVE-2024-38112	7.5 (High)	Microsoft Windows MSHTML Platform Spoofing Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-july-2024/487

Updated Malware Signatures (Week 2 July 2024)

Threat	Description
CoinMiner	This malicious software installs and runs cryptocurrency mining applications.
Trojan Miner	This malicious software installs and runs cryptocurrency mining applications.
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 17 industries spanning 20 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

Akira ransomware group stands out as the most prolific, having updated a significant number of victims (14%) distributed across multiple countries. In comparison, Inc. Ransom 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
Akira	14.04%
Black Suit	7.02%
Cactus	10.53%
Dragonforce	1.75%
Embargo	1.75%
Handala	1.75%
Hunters	1.75%
Inc. Ransom	12.28%
Lockbit3	7.02%
Medusa	5.26%
Monti	1.75%
Play	7.02%
Qilin	5.26%
Ransomcortex	3.51%
Ransomhouse	1.75%
Ransomhub	8.77%
Rhysida	1.75%
Stormous	1.75%
Vanir Group	5.26%

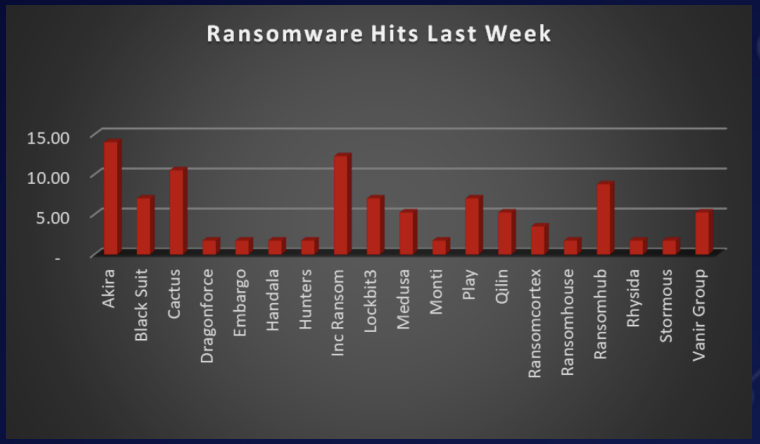


Figure 1: Ransomware Group Hits Last Week

Inc. Ransomware

Emerging in July 2023, Inc. Ransomware quickly carved a niche in the cybercrime landscape with its calculated approach. This malware employs a twist on the typical double extortion tactic, positioning itself as a "service" to its victims. While the exact origins of Inc. Ransomware remain unclear, security researchers suspect it may be linked to a Russian-speaking cybercriminal group.

Tactics, Techniques, and Procedures (TTPs):

Inc. Ransomware attempts to distinguish itself from its brutal counterparts by presenting a facade of offering "data recovery services" after encryption. However, this is a manipulative tactic designed to pressure victims into paying the ransom. Here's a closer look at Inc. Ransomware's tactics:

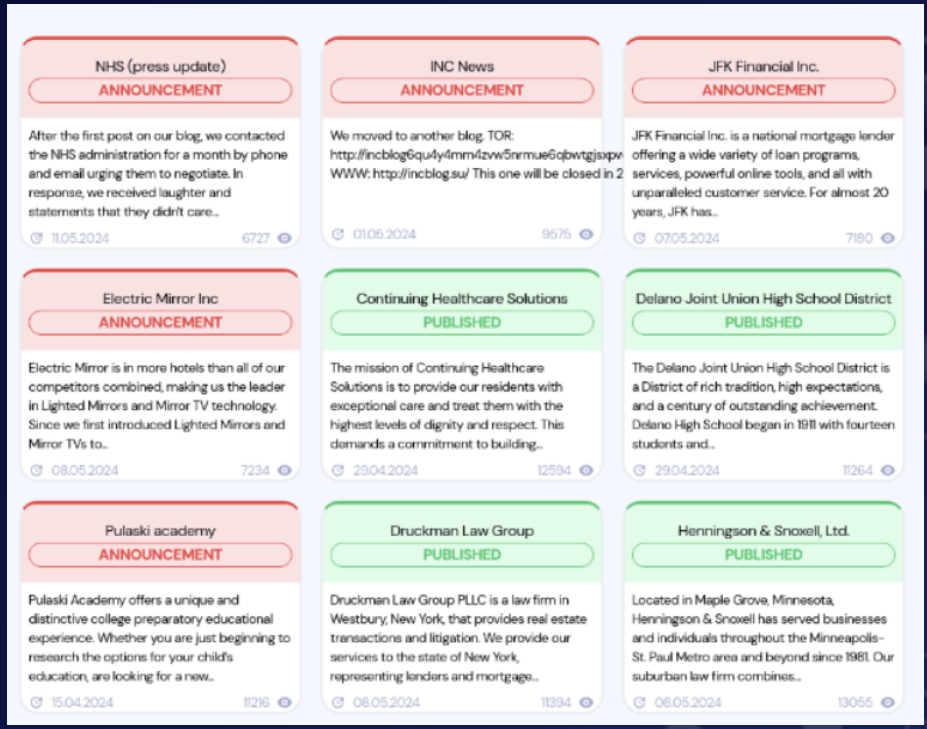
- Spear-Phishing Attacks: Unlike the ransomware strains that rely on mass phishing campaigns, Inc. targets victims with meticulously crafted spear-phishing emails. These emails appear to be from legitimate sources, such as business partners or service providers and often leverage social engineering tactics to trick recipients into clicking malicious links or downloading infected attachments.
- Exploiting Unpatched Vulnerabilities: Inc. actively seeks out unpatched vulnerabilities in software and operating systems to gain unauthorised access to networks. This reinforces the importance of keeping all software and systems updated with the latest security patches.
- Lateral Movement: Once a foothold is established on a single device, Inc. utilises various tools to move laterally across a network. This allows it to infect additional devices, escalate privileges, and potentially compromise critical systems.
- Living-off-the-Land Techniques: Similar to many malware strains, Inc. 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, Inc. often exfiltrates sensitive data like financial records, personal information, and intellectual property. This stolen data serves as a double-edged sword. Inc. threatens to not only encrypt but also leak this data on the dark web, escalating pressure on victims.
- Deceptive "Recovery Service": Following encryption, Inc. presents victims with a ransom note disguised as a "data recovery service agreement." This facade creates a false sense of negotiation and can manipulate victims into paying the ransom, believing they are regaining access to their data.
- Strong Encryption: Despite the deceptive tactics, Inc. 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.

A Global Reach with Focused Targets

While Inc. Ransomware exhibits a global reach, it also displays a preference for specific targets:

- Small and Medium-Sized Businesses (SMBs): SMBs are frequent targets due to their potentially less robust cybersecurity defences compared to larger enterprises. Inc.'s deceptive tactics can be particularly effective in these organisations.
- Supply Chain Attacks: There are concerns that Inc. 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.

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



Ransom Note

```
Greetings!
We inform you that the INC ransomware team hacked into your corporate network and downloaded more than a terabyte of confidential info
As proof, we have attached some of the downloaded files to the email.
We know the attitude of your country's legislation in the field of cybersecurity, and in order not to give the incident loud publicity
To find out how to solve the situation in which you find yourself, you need to log into the chat to communicate:

Paste this link - http://incpaysp74dphcbjyvg2eepxnl3tkgt5mq5vd4tnjusoissz342bdnad.onion
Use this ID - [snip] - to create chat account
Install TOR Browser to get access to our chat room - https://www.torproject.org/download/

If you do not get in touch within 48 hours, your information will be published on our blog - http://incapt.su/blog/leaks .
And we will inform the major media about the incident.
```

The emergence of Inc. Ransomware underscores the ever-evolving landscape of cyber threats. Its focus on social engineering tactics, combined with its deceptive "recovery service" facade, highlights the need for organisations to prioritise robust cybersecurity measures and employee awareness training. Here are some crucial steps organisations can take:

- 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.
- Phishing Simulations: Conduct simulated phishing attacks to identify vulnerabilities in employee awareness and response.
- 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.
- Endpoint Security Solutions: Deploy endpoint security solutions that can detect and prevent malware infections at the device level. These solutions can act as a first line of defence against Inc. 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.
- Incident Response Plan: Develop and regularly test an incident response plan to effectively respond.

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059	Command and Scripting Interpreter
Discovery	T1083	File and Directory Discovery
	T1016	System Network Configuration Discovery
	T1046	Network Service Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1135	Network Share Discovery
Impact	T1486	Data Encrypted for Impact
	T1489	Service Stop
	T1490	Inhibit System Recovery

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://incblog7vmuq7rktic73r4ha4j757m3ptym37tyvifzp2roedyyzzxid.onion hxxp://incapt.blog/ hxxp://incapt.su/blog/leaks hxxp://incblog6qu4y4mm4zvw5nrmue6qbwtgjsxpw6b7ixzssu36tsajldoad.onion/blog/disclosures	URLs (Onion)	Leak Site
fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced	Hash	Malicious File

In a comprehensive analysis of ransomware victims across 20 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 52% 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 (%)
Belgium	1.75%
Brazil	1.75%
Canada	7.02%
Chile	1.75%
China	1.75%
Denmark	1.75%
France	1.75%
Germany	3.51%
Guatemala	1.75%
India	1.75%
Indonesia	1.75%
Israel	1.75%
Italy	3.51%
Mexico	1.75%
Netherlands	3.51%
Peru	1.75%
Philippines	1.75%
South Africa	3.51%
UK	3.51%
USA	52.63%

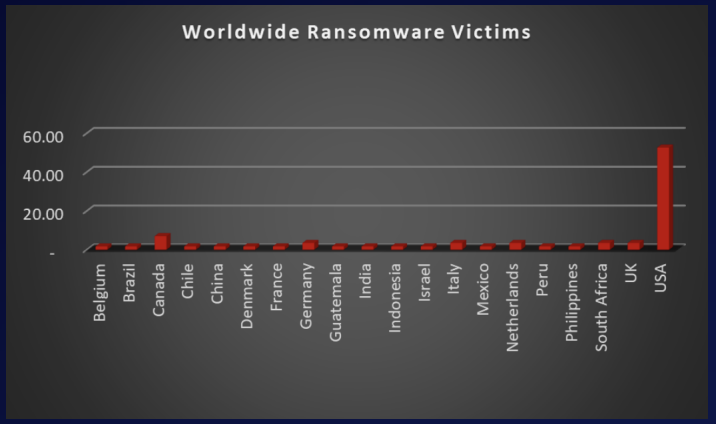


Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 17 different industries worldwide. Notably, Manufacturing bore the brunt of the attacks in the past week, accounting for 19% 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	7.02%
Cities, Towns & Municipalities	1.75%
Construction	10.53%
Consumer Services	3.51%
Education	3.51%
Energy, Utilities & Waste Treatment	5.26%
Finance	5.26%
Government	3.51%
Healthcare	5.26%
Legal Services	3.51%
Manufacturing	19.30%
Media & Internet	3.51%
Metals & Mining	3.51%
Organisation	5.26%
Retail	12.28%
Telecom	1.75%
Transportation	5.26%

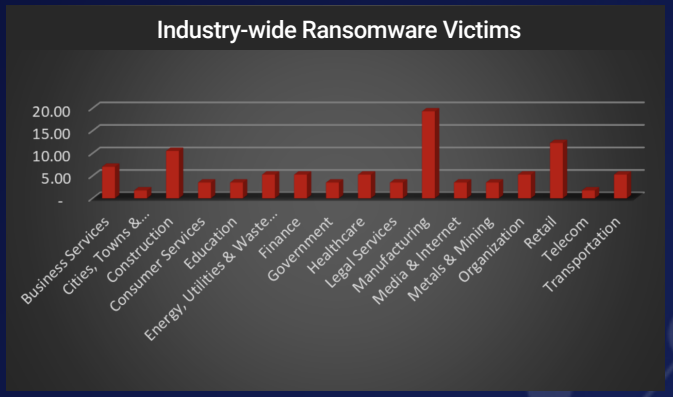


Figure 5: Industry-wide Ransomware Victims