Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Apr 23 - 29, 2024

Report Summary:

- **New Threat Detection Added** – 2 (PlugX RAT and Carbon Paper Malware)
- **New Threat Protections - 105**

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

1. PlugX RAT

RATs aim to remotely control devices with various functions. PlugX, for instance, utilises DLL sideloading to infiltrate devices, hiding malicious payloads within benign executables. Recently, a variant emerged, spreading across multiple countries, monitoring USB devices for further infection. It hides files on the Windows OS, visible only on Unix-like systems. This variant also creates a concealed directory, possibly for stolen data. Since December 2022, PlugX has used HTML smuggling to deliver malware, bypassing traditional security measures. Darktrace observed PlugX activity, detecting C2 communications within customer networks, enabling swift response to mitigate threats. Suspicious connections to rare endpoints on ports like 110, 443, 5938, and 80 were noted.

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	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Persistence and Privilege Escalation	T1547.001	Boot or Logon AutoStart Execution
	T1574.001	DLL Search Order Hijacking
	T1574.002	DLL Side-Loading
	T1140	Deobfuscate / Decode Files or Information
	T1083	File and Directory Discovery
Defence Evasion	T1564.001	Hide Artifacts
	T1036.005	Masquerading
Credential Access	T1056.001	Input Capture
Collection	T1105	Ingress Tool Transfer
Command-and-Control	T1573.001	Encrypted Channel
	T1070.003	Mail Protocols
	T1071.001	Web Protocol

2. Carbon Paper Malware

The Turla espionage group has long targeted various institutions. Recently, we discovered new versions of Carbon, a backdoor in their arsenal. Swiss GovCERT.ch analysed this component last year after an attack on RUAG, a Swiss government-owned defence firm. Our blog post highlights technical innovations in the latest Carbon versions. The group continuously develops Carbon, as evidenced by the internal version changes. They alter tools once exposed. Carbon is deployed after reconnaissance, often initiated through spearphishing or watering hole attacks. It's a sophisticated backdoor aimed at stealing sensitive data. Sharing similarities with "Uroburos," Carbon serves as a communication channel between malware components, offering fewer features than its predecessor. It's deployed after a reconnaissance tool confirms the target's significance.

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
Execution	T1059	Command and Scripting Interpreter
	T1129	Shared Modules
Defence Evasion	T1027	Obfuscated Files or Information
	T1218.011	Rundll32
	T1497	Virtualization/Sandbox Evasion
Discovery	T1012	Query Registry
	T1016	System Network Configuration Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1518	Software Discovery

Known exploited vulnerabilities (Week 4 April 2024):

Vulnerability	CVSS	Description
CVE-2022-38028	7.8 (High)	Microsoft Windows Print Spooler Privilege Escalation Vulnerability
CVE-2024-4040	10.0 (Critical)	CrushFTP VFS Sandbox Escape Vulnerability
CVE-2024-20359	6.0 (Medium)	Cisco ASA and FTD Privilege Escalation Vulnerability
CVE-2024-20353	8.6 (High)	Cisco ASA and FTD Denial of Service Vulnerability

Updated Malware Signatures (Week 4 April 2024)

Threat	Description
Upatre	Upatre is also a malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.
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.
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.

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 16 different 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.

RansomHub ransomware stands out as the most prolific, having updated a significant number of victims (10%) distributed across multiple countries. In comparison, Blackbasta, Cactus and Dan0n ransomware updated 9% victims each, 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	7.69%
Abyss-Data	1.54%
Bianlian	6.15%
Black Suit	3.08%
Blackbasta	9.23%
Cactus	9.23%
Dan0n	9.23%
Eraleign	1.54%
Everest	1.54%
Hellogookie	1.54%
Hunters	3.08%
Inc Ransom	3.08%
Lockbit3	7.69%
Mydata	1.54%
Qilin	4.62%
Qiulong	3.08%
Ra Group	3.08%
Ransomhouse	7.69%
RansomHub	10.77%
Ransomware blog	1.54%
Red Ransomware	1.54%
Rhysida	1.54%

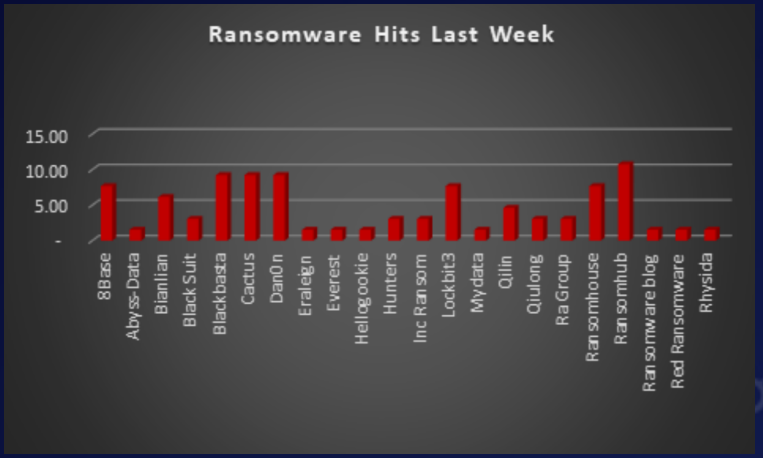


Figure 1: Ransomware Group Hits Last Week

RansomHub Ransomware Group

RansomHub is a relatively new ransomware group that emerged in late 2020. They distinguish themselves from other ransomware groups by offering a supposedly better deal to affiliates and having stricter controls in place. Notably, they also claim to avoid targeting non-profit organisations. However, there's some evidence suggesting a potential link between RansomHub and ALPHV, a previous ransomware group. Given RansomHub's recent emergence, its future operations and attack patterns remain unclear. Here's a comprehensive overview of RansomHub ransomware:

Tactics, Techniques, and Procedures (TTPs)

Initial Access Vectors: RansomHub employs various methods to gain initial access into a victim's network, including:

- Phishing Attacks: Deceptive emails containing malicious attachments or links are a common tactic.
- Exploiting Unpatched Vulnerabilities: Exploited Vulnerabilities (CVEs): RansomHub has been known to exploit a wide range of vulnerabilities, including some older, unpatched ones. Here are a few examples:
- EternalBlue (CVE-2017-0144): This critical vulnerability in Windows SMB implementation allowed remote code execution. While a patch is available, it's crucial to ensure all systems are updated.
- PetitPotam (CVE-2020-1472): This vulnerability in the Windows RPC service could be exploited for privilege escalation. A patch is available, so ensuring systems are up to date is essential.
- Fax Server vulnerabilities (CVE-2020-0787 & CVE-2020-0788): These vulnerabilities in Windows Fax Server allowed remote code execution. Patches are available, so update accordingly.
- RansomHub may also exploit newer, unpatched vulnerabilities. Security researchers are constantly discovering new vulnerabilities, and attackers are quick to incorporate them into their exploits.

Additional Exploits:

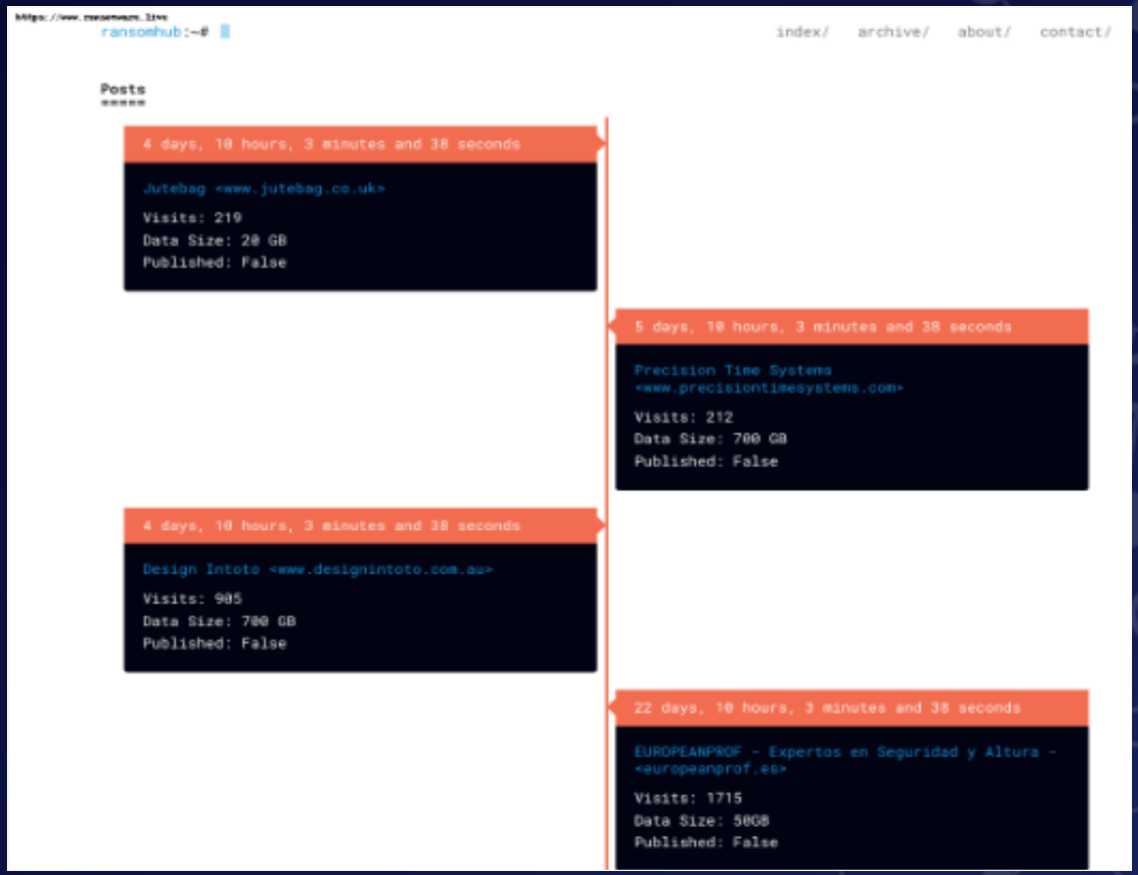
- Brute-Force Attacks: RansomHub may attempt to crack weak passwords through brute-force attacks, particularly for RDP or VPN access. RansomHub may exploit vulnerabilities in operating systems, software, or remote desktop protocols (RDP) to gain access.
- RDP Brute-Force Attacks: They may attempt to crack weak RDP passwords through brute-force attacks.

Lateral Movement & Privilege Escalation: Once inside, RansomHub uses various tools to move laterally across the network and escalate privileges to access critical systems.

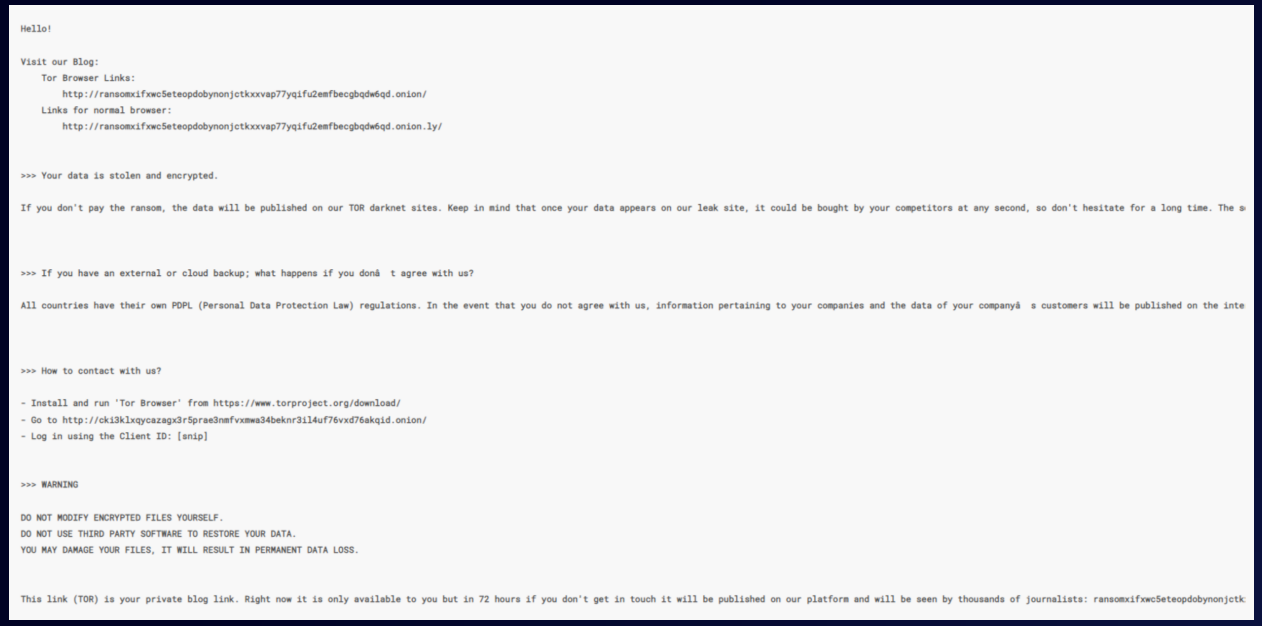
Data Exfiltration: RansomHub exfiltrates sensitive data from compromised systems, potentially including financial records, personal information, and intellectual property.

Encryption: RansomHub encrypts files on infected devices, rendering them inaccessible and demanding a ransom payment for decryption.

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



Ransom Note:



```
Hello!

Visit our Blog:
    Tor Browser Links:
        http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/
    Links for normal browser:
        http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/


>>> Your data is stolen and encrypted.

If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The s


>>> If you have an external or cloud backup; what happens if you donâ  t agree with us?

All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree with us, information pertaining to your companies and the data of your companyâ  s customers will be published on the inte


>>> How to contact with us?

- Install and run 'Tor Browser' from https://www.torproject.org/download/
- Go to http://cki3klxqycazagx3r5prae3nmfvxmwa34beknr3il4uf76vxd76akqid.onion/
- Log in using the Client ID: [snip]


>>> WARNING

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.


This link (TOR) is your private blog link. Right now it is only available to you but in 72 hours if you don't get in touch it will be published on our platform and will be seen by thousands of journalists: ransomxifxwc5eteopdobynonjctk
```

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
	T1047	Windows Management Instrumentation
	T1059	PowerShell
Defence Evasion	T1497	Virtualization/Sandbox Evasion
	T1027	Obfuscated Files or Information
Discovery	T1057	Process Discovery
	T1012	Query Registry
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Impact	T1486	Data Encrypted for Impact
	T1490	Inhibit System Recovery

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion	URLs	Leak Site
5596A55062A4232F5AA55C2F7C4DF0AC1EAD10B78D4055A3328AD142A42B555E	ID	Tox
koley	ID	RAMP

In a comprehensive analysis of ransomware victims across 20 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 50% 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 (%)
Australia	4.62%
Brazil	1.54%
Canada	6.15%
Czech Republic	1.54%
France	3.08%
Germany	9.23%
Holland	1.54%
Hungary	1.54%
Indonesia	1.54%
Italy	3.08%
Myanmar	1.54%
Norway	1.54%
Pakistan	1.54%
Poland	1.54%
Portugal	1.54%
Spain	1.54%
Switzerland	1.54%
Taiwan	1.54%
UK	3.08%
USA	50.77%

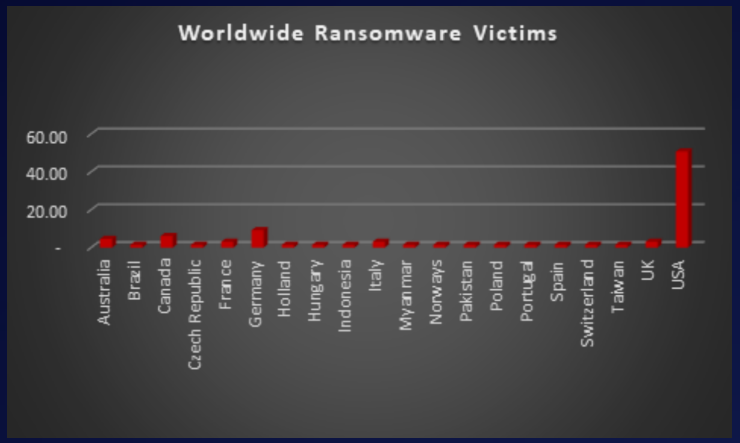


Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 16 different industries worldwide. Notably, the Manufacturing industry bore the brunt of the attacks in the past week, accounting for 23% 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	7.69%
Construction	7.69%
Consumer Services	1.54%
Cultural	1.54%
Education	1.54%
Finance	4.62%
Government	1.54%
Healthcare	13.85%
Hospitality	4.62%
Insurance	1.54%
IT	6.15%
Legal Services	9.23%
Manufacturing	23.08%
Organisations	1.54%
Retail	12.31%
Transportation	1.54%

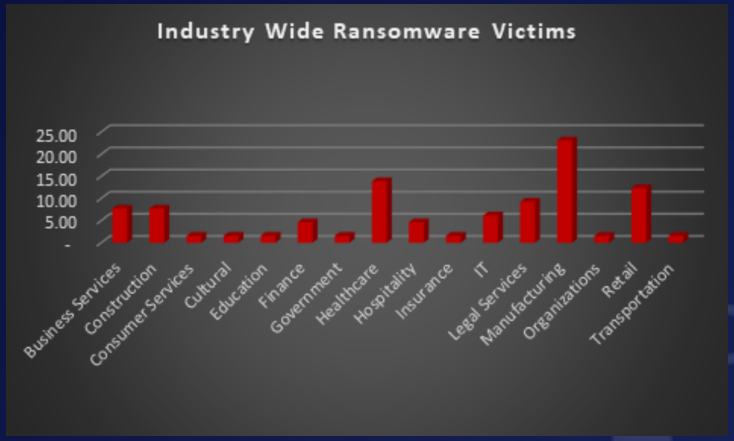


Figure 5: Industry-wise Ransomware Victims