Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Apr 16 - 22, 2024

Report Summary:

- **New Threat Detection Added** – 3 (DoNot Group (APT-C-35), Colibri Loader Malware, and Gomorrah Stealer Malware)
- **New IDPS Rules Created - 149**

Newly Detected Threats Added

1. DoNot Group (APT-C-35)

DoNot, also known as APT-C-35, is a sophisticated cyber threat actor group, widely recognised for its advanced capabilities in espionage and cyber warfare. Operating since at least 2014, DoNot primarily targets governmental, diplomatic, and military entities across the Middle East and South Asia, with a focus on Pakistan. Their modus operandi includes spear-phishing, malware deployment, and social engineering tactics to gain unauthorised access to sensitive information and conduct espionage activities. DoNot's arsenal often includes custom-developed malware and exploits, showcasing their high level of technical expertise. Their activities highlight the persistent and evolving nature of cybersecurity threats in the modern digital landscape.

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
Persistence	T1624.001	Event Triggered Execution: Broadcast Receivers
Defence Evasion	T1407 T1629.001	Download New Code at Runtime Impair Defences: Prevent Application Removal
Discovery	T1426 T1422 T1418	System Information Discovery System Network Configuration Discovery Software Discovery
Collection	T1517 T1417.001 T1429 T1414	Access Notifications Input Capture: Keylogging Audio Capture Clipboard Data
Command-and-Control	T1437	Application Layer Protocol
Exfiltration	T1646	Exfiltration Over C2 Channel

2. Colibri Loader Malware

Colibri Loader is a potent malware loader utilised by cybercriminals to deploy various types of malicious payloads onto compromised systems. Emerging in recent years, it operates stealthily, evading detection by security software through encryption and obfuscation techniques. Colibri Loader's modular design allows it to adapt to different attack scenarios, facilitating the distribution of ransomware, banking Trojans, and other malware strains. It often spreads through phishing emails or exploit kits, leveraging social engineering tactics to trick users into executing it. Once installed, Colibri Loader acts as a gateway for further malicious activities, underscoring the persistent threat posed by sophisticated malware in cyberspace.

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
Initial Access	T1053.005	Scheduled Task
Execution	T1059.001	Command and Scripting Interpreter
Persistence	T1053.005	Scheduled Task
Defence Evasion	T1027	Obfuscated Files or Information
Exfiltration	T1020	Automated Exfiltration
Command-and-Control	T1071	Application Layer Protocol

3. Gomorrah Stealer Malware

Gomorrah Stealer initiates its operations by collecting data on the operating system, processor, memory (RAM), device name, and anti-virus/security software. This malicious software specialises in extracting information, primarily passwords, from browsers such as Google Chrome, Mozilla Firefox, Opera, Amigo, Brave, Comodo, Kometa, Orbitum, Torch, and Yandex. Additionally, it targets other applications like Mozilla Thunderbird (email client), FileZilla (FTP - File Transfer Protocol client), Pidgin (IM - Instant Messaging client), and Proxifier (proxy server support). Gomorrah aims to pilfer cryptocurrency wallet credentials and credit card details. It can download various files from desktops and document folders, including databases (MySQL, SQLite, SQL server backups, and Microsoft Access), documents/text files (.txt, .doc, .docx, .xlsx, and .pdf), images (.jpg, .png, .gif, and .jpge), and log files (.log). Another capability of Gomorrah is capturing screenshots.

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	T1047	Windows Management Instrumentation
Persistence	T1547.001	Registry Run Keys / Startup Folder
Privilege Escalation	T1055 T1055.003 T1547.001	Process Injection Thread Execution Hijacking Registry Run Keys / Startup Folder
Defence Evasion	T1027 T1055 T1497	Obfuscated Files or Information Process Injection Virtualization/Sandbox Evasion
Credential Access	T1003	OS Credential Dumping
Discovery	T1057 T1083	Process Discovery File and Directory Discovery
Command-and-Control	T1071	Application Layer Protocol

Known exploited vulnerabilities (Week 3 April 2024):

Vulnerability	CVSS	Description
CVE-2024-28253	9.4 (Critical)	OpenMetadata Code Injection vulnerability
CVE-2024-28254	8.8 (High)	OpenMetadata OS Command injection vulnerability
CVE-2024-28255	9.8 (Critical)	OpenMetadata Authentication Bypass vulnerability
CVE-2024-28847	8.8 (High)	OpenMetadata Code Injection vulnerability
CVE-2024-28848	8.8 (High)	OpenMetadata Code Injection vulnerability

Updated Malware Signatures (Week 3 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 20 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.

Akira and Lockbit3.0 ransomware stand out as the most prolific, having updated a significant number of victims (12%) each distributed across multiple countries. In comparison, Hunters International ransomware updated 10% 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
3Am	1.02%
8Base	8.16%
Akira	12.24%
Bianlian	4.08%
Black Suit	4.08%
Blackbasta	1.02%
Blackout	1.02%
Cactus	7.14%
Ciphbit	1.02%
Daixin	1.02%
Darkvault	4.08%
Dragonforce	2.04%
Hunters International	10.20%
INC Ransom	3.06%
Lockbit3	12.24%
Medusa	6.12%
Mydata	1.02%
Play	6.12%
Qilin	1.02%
Ra Group	3.06%
Ransomexx	1.02%
Ransomhouse	1.02%
Ransomhub	7.14%
Snatch	1.02%

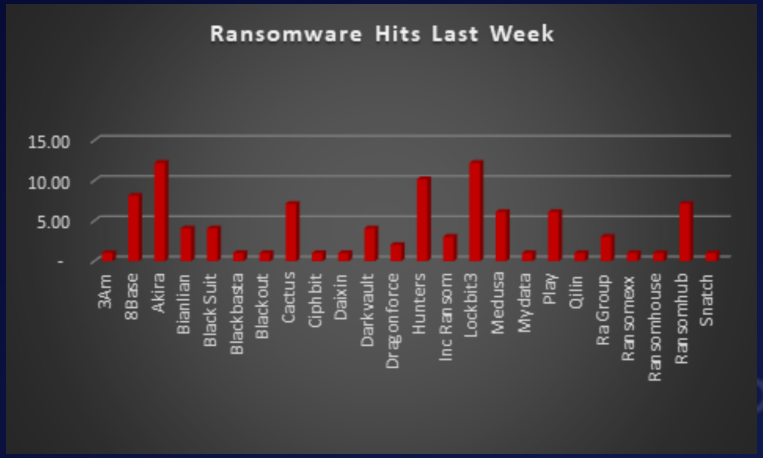


Figure 1: Ransomware Group Hits Last Week

Akira Ransomware Group

Relatively new, Akira first appeared in Q1 2023. By January 2024, they had impacted over 250 organisations globally, extorting a staggering $42 million. This rapid growth placed them among the top ransomware threats, particularly for critical infrastructure. Akira has targeted a wide range of businesses and government entities across North America, Europe, and Australia. Critical infrastructure hasn't been spared, making them a serious concern for national security.

Tactics, Techniques, and Procedures (TTPs)

Initial Access: They gain access through various means, including -

VPN Exploits: A favourite target is vulnerabilities in Virtual Private Networks (VPNs), particularly Cisco ASA SSL VPN and Cisco AnyConnect. These vulnerabilities (like CVE-2020-3259 and CVE-2023-20269) allow them to bypass security if Multi-Factor Authentication (MFA) isn't enabled on the VPN.

Lack of Multi-Factor Authentication (MFA): Akira heavily relies on exploiting systems where MFA is not enforced. MFA adds an extra layer of security beyond just usernames and passwords, making it significantly harder for unauthorised access.

Remote Desktop Protocol (RDP) Attacks: In some cases, Akira targets RDP (Remote Desktop Protocol) to gain initial access. This can involve brute-force attacks on weak passwords or exploiting known vulnerabilities in RDP software.

Stolen Credentials: The group may also take advantage of stolen usernames and passwords obtained through phishing campaigns or purchased on the dark web.

Lateral Movement: Once inside, they disable security software and employ techniques to move laterally across the network, granting them broader access to valuable data.

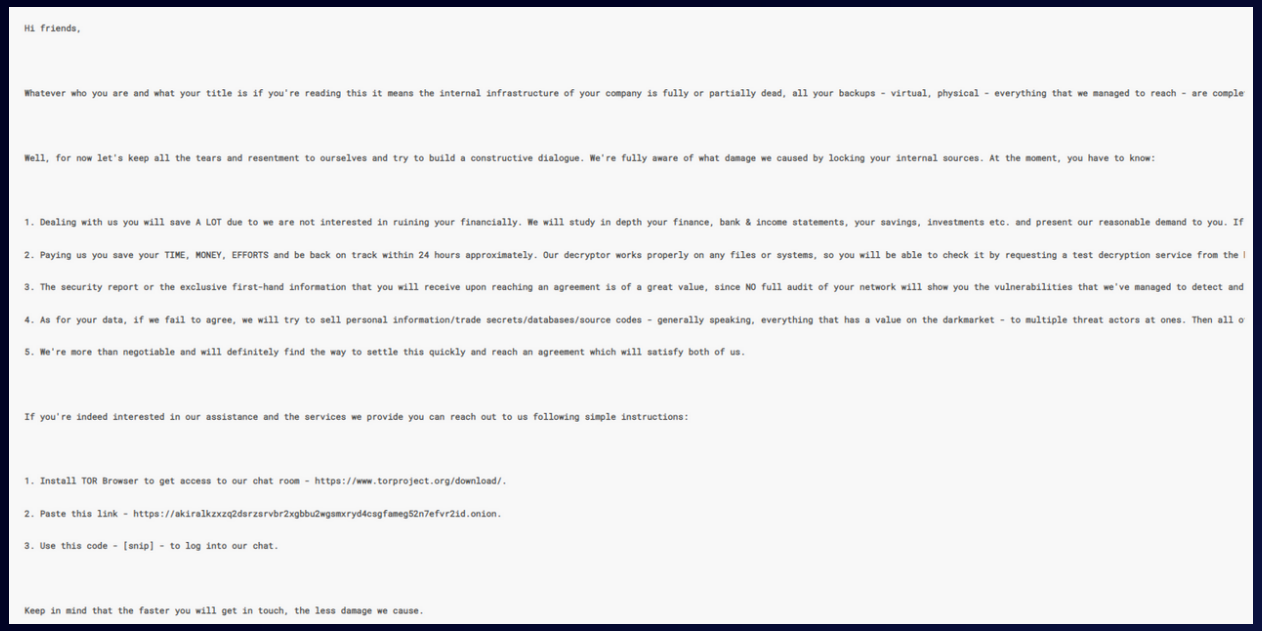
Encryption: Akira utilises a hybrid encryption combining Chacha20 and RSA algorithms, making decryption challenging. They also target shadow copies to prevent easy data recovery.

Variants: The group uses strains written in C++ and Rust, with file extensions like .akira and .powerranges. Their malware, Megazord, written in Rust, emerged in April 2023 targeting Linux servers.

Impact: Akira's success highlights the growing sophistication of ransomware attacks. Their focus on critical infrastructure raises concerns about potential disruption to essential services.

Data Leak Site: They maintain a dark web leak site (Akira) where they threaten to publish stolen data from unpaid victims.

Ransom Note:



Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are comple

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all o
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion.
3. Use this code - [snip] - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.

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
-08207409e1d789aea68419b04354184490ce46339be071c6c185c75ab9d08cba - 2727c73f3069457e9ad2197b3cda25aec864a2ab8da3c2790264d06e13d45c3d - 2db4a15475f382e34875b37d7b27c3935c7567622141bc203fde7fe602bc8643 - 56f1014eb2d145c957f9bc0843f4e506735d7821e16355bcfbb6150b1b5f39db - 58e9cd249d947f829a6021cf6ab16c2ca8e83317dbe07a294e2035bb904d0cf3 - 6270cef0c8cc45905556c40c9273391d71ef8d73c865d44d2254a8a4943ae5b4 - 77fe1619aa07d2ab169a2fa23feb22d7433bf07e856cda1402cf60205beddd7f - 78642603005f826a3b47effb852da980a6483ffb9461e30842020848305c9353 - 7d5da695e6f9a421e3d3a94e384ce00e8ec58fac5b895b4cba5b66a6de7fafd5 - 99c1cd740fa749a163ce8cdf93722191c4ba5d97de81576623a8bbcb622473d6 - b7bbfb66338a3413f981561115bd8ef8a4014479bcc320de563499cfc73a3de2 - c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddccd5bb37857e7bde6d2eb7 - ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d - d5558ec7979a96fe1ddcb1f33053a1ac3416a9b65d4f27b5cc9fd0a816296184 -e5c8888f51369c2105d47a4998ad9b4053471bd98b4fd73a854207da09206ee2 - ee0a27f3de6f21463f8125dbfc95268ff995ef8ea464660d67cf9f77e240e1ab - f1f82d3b62f92f4fe8af320afea6c346210bb51774bb1567149e308469d40c92 - ffcddd8544bca0acde69f49abd1ea9dbee5f4eb73df51dd456b401c045a0b6af	Hash	Akira ransomware binary
hxxps://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion/ hxxps://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion/n hxxps://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.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 60% 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	4.08%
Belgium	1.02%
Brazil	2.04%
Canada	6.12%
China	1.02%
Colombia	1.02%
Dâmbovița	1.02%
France	5.10%
Germany	1.02%
Holand	1.02%
Ireland	1.02%
Italy	3.06%
Netherlands	1.02%
South Africa	1.02%
Spain	2.04%
Taiwan	1.02%
UAE	1.02%
UK	6.12%
USA	60.20%

Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 20 different industries worldwide. Notably, Manufacturing 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	7.14%
Cities, Towns & Municipalities	2.04%
Construction	8.16%
Consumer Services	3.06%
Education	4.08%
Energy, Utilities & Waste Treatment	5.10%
Government	2.04%
Healthcare	3.06%
Hospitality	8.16%
Insurance	1.02%
IT	3.06%
Legal Services	3.06%
Manufacturing	23.47%
Media & Internet	2.04%
Organisations	3.06%
Real Estate	1.02%
Retail	10.20%
Telecom	1.02%
Transportation	8.16%
Finance	1.02%

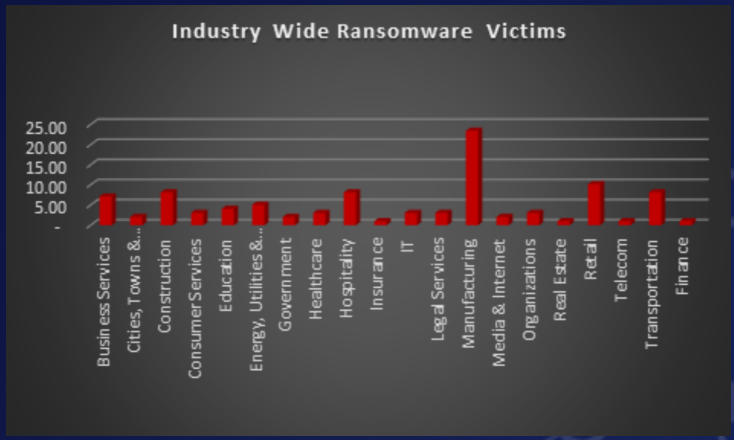


Figure 5: Industry-wise Ransomware Victims