

THREAT INTELLIGENCE REPORT

Apr 09 - 15, 2024

Report Summary:

- **New Threat Detection Added** – 3 (RomCom RAT, Erbium Stealer and Parallax RAT)
- **New IDPS Rules Created** - 79



Newly Detected Threats Added

1. RomCom RAT

Storm-0978, also known as RomCom, is a cybercriminal group from Russia. They use sneaky tactics like ransomware and extortion to make money. They also steal login details for spying. Storm-0978 creates and spreads a sneaky program called RomCom. They also use a ransomware called Underground, linked to another called Industrial Spy. They recently used a computer bug called CVE-2023-36884 to sneak RomCom onto computers. Storm-0978 tricks people by hiding their bad software in popular good ones. They often target government and military groups in Ukraine, plus other organisations in Europe and North America, especially those connected to Ukraine. They have hit telecom and finance companies.

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	T1204	User Execution
Defence Evasion	T1027	Obfuscated Files or Information
Credential Access	T1003	OS Credential Dumping
Collection	T1005	Data from Local System
	T1560	Archive Collected Data
Command-and-Control	T1071	Application Layer Protocol



2. Erbium Stealer

Erbium is a new type of malicious software that is becoming popular among cybercriminals. It is like a service - people pay to use it. Erbium steals information from computers and is getting attention because it does various things, has good customer service, and is cheap. It was first talked about in July 2022, but it is not clear if it is being used yet. At first, it cost \$9 a week, but now it is \$100 a month or \$1000 a year. Compared to another similar program called RedLine, Erbium is cheaper. It steals passwords, credit card details, and cryptocurrency info from web browsers.

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	T1566.001	Spear phishing Attachment
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Persistence	T1547	Registry Run Keys / Startup Folder
Defence	T1036	Masquerading
Discovery	T1057	Process Discovery
Command-and-Control	T1071	Application Layer Protocol



3. Parallax RAT

Parallax RAT infiltrated systems through a drive-by download disguised as a Fortinet VPN client distributed via popular search engines. The threat actor behind it utilised PsExec for lateral movement from the initial infection point to the Domain Controller within a tight 2-hour window. The RAT ensured persistence by integrating itself into the Startup folder and renaming its executable. It also deployed NetSupportRAT on the Domain Controller. Offering various functionalities like remote control, data exfiltration, keylogging, and more, Parallax RAT's cracked version persists despite the project's closure, utilising evasion tactics like anti-disassembly measures and RC4 encryption for configuration concealment.

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	T1189	Drive-By Compromise
Execution	T1059	Command and Scripting Interpreter
Persistence	T1547	Registry Run Keys / Startup Folder
Defence Evasion	T1027	Obfuscated Files or Information
Exfiltration	T1020	Automated Exfiltration
Command-and-Control	T1071	Application Layer Protocol



Known exploited vulnerabilities (Week 2 April 2024):

Vulnerability	CVSS	Description
CVE-2024-3272	9.8 (Critical)	D-Link Multiple NAS Devices Use of Hard-Coded Credentials Vulnerability
CVE-2024-3273	9.8 (Critical)	D-Link Multiple NAS Devices Command Injection Vulnerability
CVE-2024-3400	10.0 (Critical)	Palo Alto Networks PAN-OS Command Injection Vulnerability

Updated Malware Signatures (Week 2 April 2024)

Threat	Description
Cerber	Another type of ransomware but instead of the usual ransom text files, it plays audio on the victim's infected machine.
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.
Gh0stRAT	Gh0stRAT is a widely recognised group of remote access trojans strategically crafted to grant an assailant full authority over a compromised system. Its functionalities encompass monitoring keystrokes, capturing video via the webcam, and deploying subsequent malware. The source code of Gh0stRAT has been openly accessible on the internet for an extended period, substantially reducing the hurdle for malicious actors to adapt and employ the code in fresh attack endeavours.
MacStealer	A remote access trojan 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 21 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.

BlackBasta and Medusa ransomware groups stand out as the most prolific, having updated a significant number of victims (10%) each distributed across multiple countries. In comparison, Black Suit, Darkvault and Dragonforce ransomware groups updated 9% of 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	3.96%
Akira	4.95%
Bianlian	3.96%
Black Suit	9.90%
BlackBasta	10.89%
Ciphbit	1.98%
Darkvault	9.90%
Dragonforce	9.90%
Dunghill	0.99%
Hunters	3.96%
Inc Ransom	1.98%
Lockbit3	1.98%
Malek Team	0.99%
Mallox	2.97%
Medusa	10.89%
Play	5.94%
Qilin	2.97%
Ra Group	1.98%
Ransomhub	6.93%
Rhysida	2.97%

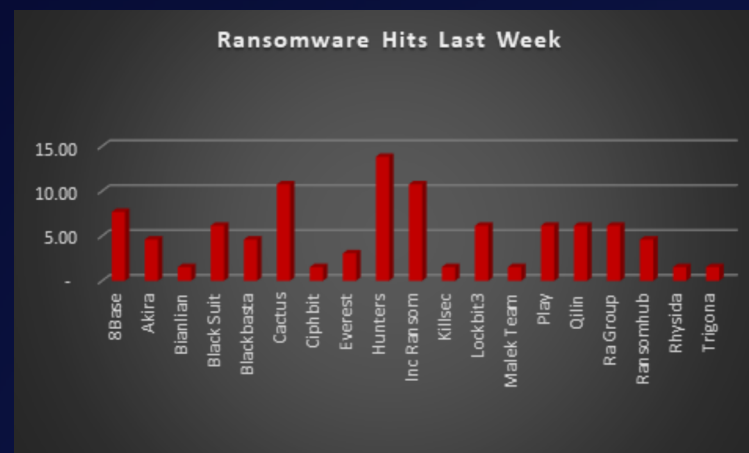


Figure 1: Ransomware Group Hits Last Week



Black Basta Ransomware Group

Black Basta, discovered in early 2022, is known for its tricky double extortion tactic. This group, speaking Russian, doesn't just lock up computers with ransomware; they also sneak out private information and threaten to publish it if the victim doesn't pay up. The way they work is similar to other cyber gangs like Conti and BlackMatter, leading some to think they might be connected. Although they're not big on recruiting or advertising online, they're still a big threat. It's important for people to know about them and take steps to stay safe.

Tactics, Techniques, and Procedures (TTPs):

Double Extortion: Black Basta employs the double extortion tactic. They encrypt victim data and demand a ransom for decryption. Additionally, they steal sensitive information and threaten to leak it publicly if the ransom is unpaid.

Targeted Attacks: Black Basta appears to target specific victims rather than using a widespread approach.

Exploited Vulnerabilities (CVEs):

Recent ScreenConnect Vulnerabilities (CVE-2024-1708 & CVE-2024-1709): These recently discovered vulnerabilities (February 2024) in ConnectWise ScreenConnect software (versions 23.9.7 and earlier) allow attackers to bypass authentication and potentially gain complete control of the system. Black Basta, along with other ransomware groups, have been actively exploiting these vulnerabilities.

ZeroLogon (CVE-2020-1472): This critical vulnerability in the Netlogon protocol (used for domain authentication in Windows) allows attackers to gain domain administrator privileges. While a patch is available, it's crucial to ensure all systems are updated.

PrintNightmare (CVE-2021-34527): This vulnerability in the Windows Print Spooler service allows privilege escalation. Black Basta has been known to leverage this vulnerability to elevate privileges and deploy additional payloads like Cobalt Strike.

NoPac vulnerabilities (CVE-2021-42278 & CVE-2021-42287): These vulnerabilities in the Microsoft Server Message Block (SMB) protocol can be exploited for privilege escalation.

MSDT Remote Code Execution (CVE-2022-30190): Black Basta variants have been observed exploiting this vulnerability in Microsoft Office documents to achieve remote code execution.

Initial Intrusion Vectors: They gain initial access through various methods, including:

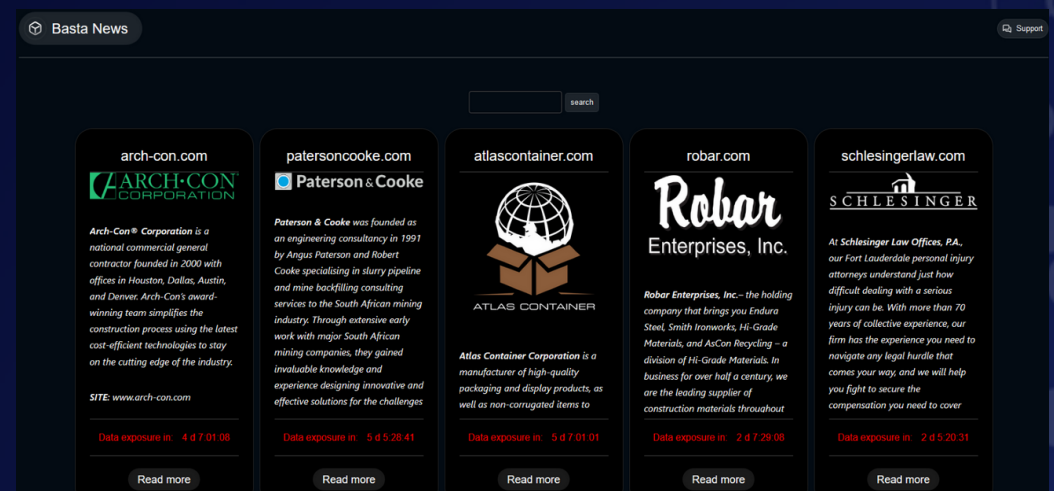
Qakbot Trojan: This malware can steal credentials, download additional payloads, and move laterally within a network.

Brute Force Attacks: They may attempt to crack weak passwords to gain access.

Cobalt Strike: This tool allows for post-exploitation activities like privilege escalation and lateral movement.

Data Exfiltration: Once inside, Black Basta exfiltrates sensitive data to their servers.

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



The screenshot shows the Basta News website interface. At the top, there is a search bar and a 'Support' link. Below the search bar, there is a grid of five article cards. Each card features a company logo, a brief description of the company, and a 'Data exposure in' timestamp. The cards are for arch-con.com, patersoncooke.com, atlascontainer.com, robar.com, and schlesingerlaw.com. Each card has a 'Read more' button at the bottom.

Company	Data Exposure In
arch-con.com	4 d 7 01 08
patersoncooke.com	5 d 5 28 41
atlascontainer.com	5 d 7 01 01
robar.com	2 d 7 29 08
schlesingerlaw.com	2 d 5 20 31



Ransom Note:

```
ATTENTION!
Your network has been breached and all data was encrypted. Please contact us at:
https://bastadshuzwepdixedg2gekq7jk22ato24zy1lp6ljx7wdtyctgyvd.onion/

Login ID: [snip]

** To access .onion websites download and install Tor Browser at:

https://www.torproject.org/ (Tor Browser is not related to us)

** To restore all your PCs and get your network working again, follow these instructions:

- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.

Please follow these simple rules to avoid data corruption:

- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption.

- Do not hire a recovery company. They can't decrypt without the key.
They also don't care about your business. They believe that they are
good negotiators, but it is not. They usually fail. So speak for yourself.

Waiting you in a chat.
```

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059	Command and Scripting Interpreter
Defence Evasion	T1112	Modify Registry
	T1027	Obfuscated Files or Information
	T1562.001	Impair Defences: Disable or Modify Tools
Discovery	T1082	System Information Discovery
	T1083	File and Directory Discovery
Impact	T1490	Inhibit System Recovery
	T1489	Service Stop
	T1486	Data Encrypted for Impact



Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
01fafd51bb42f032b08b1c30130b963843fea0493500e871d6a6a87e555c7bac c9df12fbfcae3ac0894c1234e376945bc8268acdc20de72c8dd16bf1fab6bb70 94428d7620fff816cb3f65595978c6abb812589861c38052d30fa3c566e32256 1cad451cedeb9967c790c1671cd2e3482de87e3e802953f28e426642894ceb7b 81a6c44682b981172cd85ee4a150ac49f838a65c3a0ed822cb07a1c19dab4af5 17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6c6ba6b094b0a52b0aa ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6	Hash	Black Basta's ransomware binary
8882186bace198be59147bcabae6643d2a7a490ad08298a4428a8e64e24907ad 72a48f8592d89eb53a18821a54fd791298fcc0b3fc6bf9397fd71498527e7c0e c7eb0facf612dbf76f5e3fe665fe0c4bfed48d94edc872952a065139720e3166 130af6a91aa9ecbf70456a0bee87f947bf4ddc2d2775459e3feac563007e1aed c4683097a2615252eeddab06c54872efb14c2ee2da8997b1c73844e582081a79 ac49c114ef137cc198786ad8daefa9cfcc01f0c0a827b0e2b927a7edd0fca8b0 580ce8b7f5a373d5d7fbfbfef5204d18b8f9407b0c2cbf3bcae808f4d642076a	Hash	Black Basta's tools
24.178.196.44:2222 37.186.54.185:995 39.44.144.182:995 45.63.1.88:443 46.176.222.241:995 47.23.89.126:995 72.12.115.15:22 72.76.94.52:443 72.252.157.37:995 72.252.157.212:990	URLs	Qakbot C&C
http://stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd.onion/ Screen https://bastad5huzwkepdixedg2gek7jk22ato24zylp6lnjx7wdtyctgvvd.onion	URLs	Leak Site



Tools used by Blackbasta Ransomware for hacking

Indicators	Indicator Type
Initial access	Spear phishing
Discovery	Netcat
Privilege escalation	PrintNightmare vulnerability (CVE-2021-34527)
Credential access	Mimikatz
Lateral movement	BITSAAdmin Coroxy PsExec RDP WMI
Execution	PowerShell Windows command shell WMI
Exfiltration	Cobeacon Rclone
Command-and-Control	Command-and-Control
Impact	Black Basta ransomware



In a comprehensive analysis of ransomware victims across 20 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 57% 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	2.97%
Brazil	0.99%
Canada	9.90%
China	0.99%
Curacao	0.99%
Egypt	0.99%
France	0.99%
Germany	1.98%
India	2.97%
Italy	3.96%
Lalau	0.99%
Malaysia	1.98%
Netherlands	0.99%
Oman	0.99%
Spain	1.98%
Sri Lanka	0.99%
Sweden	0.99%
Thailand	1.98%
UK	4.95%
USA	57.43%

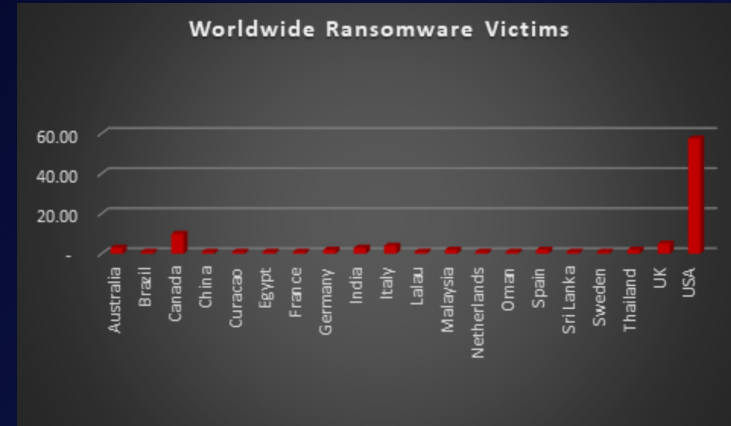


Figure 4: Ransomware Victims Worldwide



Upon further investigation, it has been identified that ransomware has left its mark on 21 different industries worldwide. Notably, the Manufacturing bore the brunt of the attacks in the past week, accounting for 29% of victims. 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	8.91%
Cities, Towns & Municipalities	0.99%
Construction	7.92%
Consumer Services	0.99%
Education	2.97%
Energy, Utilities & Waste Treatment	1.98%
Finance	1.98%
Government	3.96%
Healthcare	1.98%
Hospitality	2.97%
Insurance	1.98%
IT	2.97%
Legal Services	2.97%
Manufacturing	29.70 %
Media & Internet	0.99 %
Organisations	3.96%
Real Estate	2.97%
Retail	8.91%
Telecom	6.93%
Transportation	3.96%

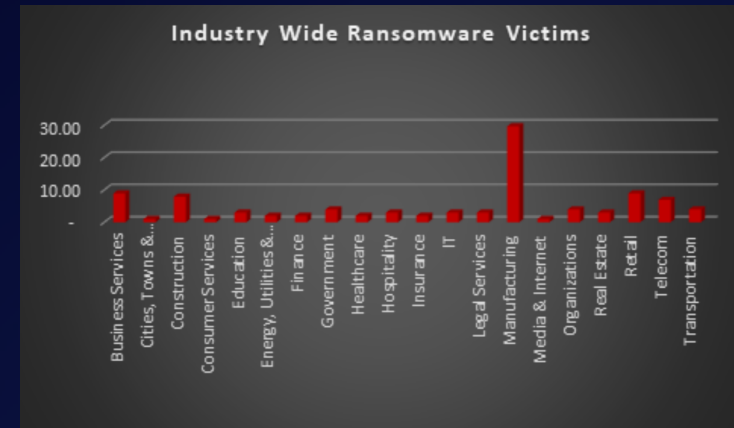


Figure 5: Industry-wise Ransomware Victims

