Rhysida ransomware group Report

By: Mohamed Galal Hashem

Source:

1- SentinelOne Report (Link to Report)

2- TrendMicro Report (Link to Report)

3- CISA.gov Page (Link to Page)

4- SOCRadar Report (Link to Page)

5- Cisco Talos Report (Link to Page)

6- FortiGuard Labs Threat Research Report (Link to Page)

7- Logpoint Report (Link to Page)

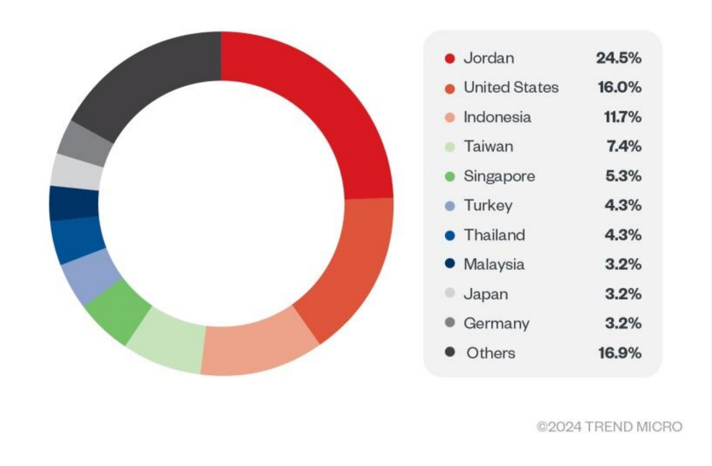
Information about Rhysida ransomware group

- The Rhysida ransomware group was first observed in May of 2023, following the emergence of their victim support chat portal hosted via TOR (.onion).
- A defining characteristic of Rhysida's operations is its double extortion technique. This method involves two primary phases: first, sensitive data is exfiltrated from the victim's network, and then the victim's systems are encrypted.
- The group positions themselves as a "cybersecurity team" who are doing their victims a favor by targeting their systems and highlighting the supposed potential ramifications of the involved security issues.
- Motivated by financial gain, Rhysida's operators have been known to use phishing attacks as a means of gaining initial access, after which Cobalt Strike is used for lateral movement in infected machines and using PsExec to deliver a script, detected as SILENTKILL, to terminate antivirus programs.
- the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory on Rhysida in November 2023 that pointed to similarities between the group's tactics, techniques, and procedures (TTPs) and those of another ransomware group called Vice Society
- The attackers deliver the ransom notice to victims through email and dark websites.
- The ransomware appends the .rhysida extension and turns off recovery tools.
- Open-source reporting has highlighted notable similarities between Rhysida's activity and that of the Vice Society (DEV-0832) ransomware group

Sectors and Regions have been targeted by Rhysida ransomware

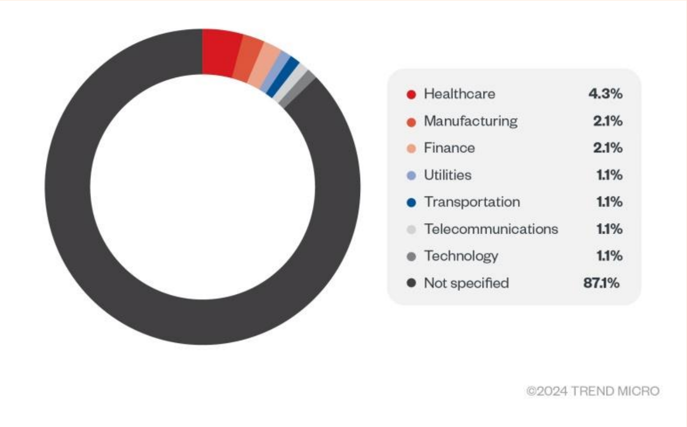
- Investigations and open-source reporting indicate a predominant deployment against organizations in the education, healthcare, manufacturing, information technology, and government sectors.
- Geographically, Rhysida's campaigns are global in scope, affecting organizations across Europe, North and South America, Asia, and Australia.
- Specific concentrations of victims have been observed in the United States, United Kingdom, and Italy.
- Rhysida will attack organisations that have weak email security.

Countries with the highest number of attack attempts in terms of infected machines for Rhysida ransomware (January 2023 – January 2024):



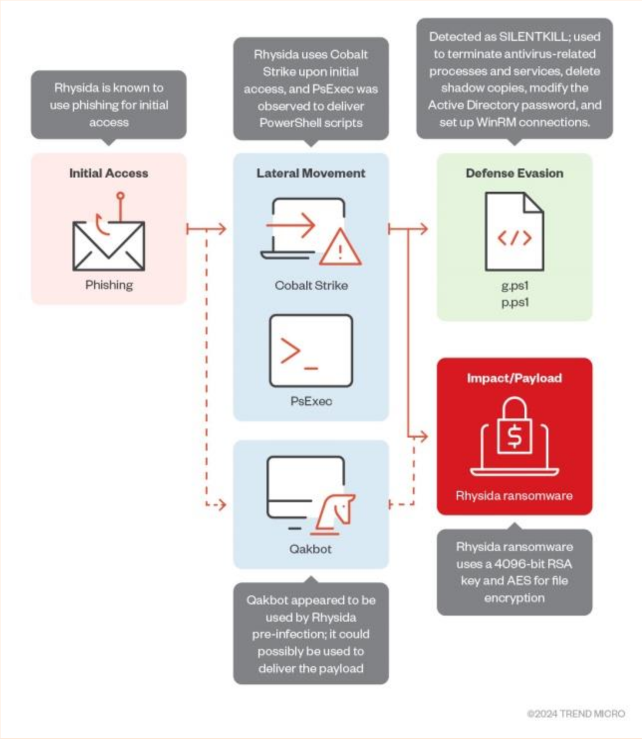
©2024 TREND MICRO

An industry breakdown of Rhysida ransomware attack attempts in terms of infected machines
(January 2023 – January 2024)**:**



The key stages of infection employed by Rhysida.

- **Initial Access:** Rhysida's threat actors allegedly use phishing for initial access.
- **Defense Evasion, Discovery:** The Rhysida ransomware drops PowerShell scripts (detected as SILENTKILL) to terminate antivirus-related processes and services, delete shadow copies, and modify Active Directory passwords. These scripts are also used to set up WinRM connections.
- **Lateral Movement:** Rhysida operators use Cobalt Strike beacons upon initial access. Additionally, they have been observed using PsExec to deploy the PowerShell scripts and the ransomware binary.
- **Impact:**
    - The Rhysida ransomware uses a 4096-bit RSA key and AES for file encryption.
    - Rhysida employs periodic encryption to evade detection, decrypting sections of files.
    - It appends the ".Rhysida" extension and removes backup catalogs.
    - The ransomware encrypts network shares first, then local drives.
    - Rhysida payloads have been observed using ChaCha20 for file encryption.
- Rhysida ransom notes are written as PDF documents to affected folders on targeted drives.
- Rhysida attempts to replace the desktop background via multiple commands.


Rhysida is known to use phishing for initial access
Rhysida uses Cobalt Strike upon initial access, and PsExec was observed to deliver PowerShell scripts
Detected as SILENTKILL; used to terminate antivirus-related processes and services, delete shadow copies, modify the Active Directory password, and set up WinRM connections.
Initial Access
Phishing
Lateral Movement
Cobalt Strike
PsExec
Defense Evasion
g.ps1
p.ps1
Impact/Payload
Rhysida ransomware
Qakbot
Rhysida ransomware uses a 4096-bit RSA key and AES for file encryption
Qakbot appeared to be used by Rhysida pre-infection; it could possibly be used to deliver the payload
©2024 TREND MICRO

Rhysida Activity Timeline

In Late 2022, Rhysida ransomware first observed on the cybercrime scene.

In March 2023, Rhysida's dedicated leak site (DLS) is established.

In May 2023, Group's activity first widely observed.
Debut high-profile attack against Chilean Army's website and email system

In June 15, 2023, Rhysida leaks files stolen from the Chilean Army.

In July 2023, Trend Micro detects Rhysida using PsExec to deliver "SILENTKILL" script to terminate AV.
Kuwaiti health ministry hacked, data encrypted and leaked.
ThreatDown reports initial activity of CleanUpLoader backdoor.

In August 2023, Trend Micro finds PowerShell versions of Rhysida ransomware.
Health Sector Cybersecurity Coordination Center (HC3) warns about Rhysida targeting healthcare.
Major attack impacts U.S. hospital group.

In November 2023, Joint advisory (AA23-319A) published detailing Rhysida IOCs and TTPs.
Linux version of Rhysida ransomware released.
Rhysida perpetrates notable cyberattack on the British Library.

In December 2023, Rhysida attack attempts, per Trend Micro telemetry, reach peak.
Data dump occurs, releasing Marvel's Wolverine game details and employee info.

In Early Feb 2024, South Korean researchers discover encryption vulnerability; public decryption tool released by KISA.
In July 2024, Rhysida uses new variant of Oyster backdoor (Broomstick) in private school attack.

In April 30, 2025, CISA advisory (AA23-319A) updated with new IOCs and TTPs.

An inferred country of origin for Rhysida

that the group may be based in Russia or the Commonwealth of Independent States (CIS) because their ransomware software has been found to contain Russian code snippets and comments and their ransom notes and dark web leak site often feature Russian words and phrases and The time zone observed in their communications with victims also aligns with this geographical region.

Rhysida tactics, techniques and procedures (TTPs)

Rhysida employs a methodical and multi-stage attack kill chain to infiltrate networks, exfiltrated data, and deploy ransomware. This process typically begins with initial access, followed by execution, persistence, privilege escalation, defense evasion, discovery, lateral movement, data collection and exfiltration, culminating in the encryption and impact phase.

Initial Access:

- Rhysida utilizes multiple vectors to gain initial access, making it challenging to pinpoint a single primary method.
- Rhysida employs sophisticated phishing emails containing malicious links or attachments designed to trick users into executing harmful payloads.
- Rhysida actors are known to exploit vulnerabilities in external-facing remote services such as Virtual Private Networks (VPNs) and Remote Desktop Protocols (RDP) to gain unauthorized access and maintain persistence.
- Rhysida actively targets and exploits known software flaws as Zerologon vulnerability (CVE-2020-1472).

Execution:

- Once inside a network, Rhysida executes malicious code and deploys additional tools to further its objectives.
- The group extensively uses PowerShell scripts, such as the one detected as "SILENTKILL," to carry out various malicious functions.
- Rhysida deploys various backdoors to maintain access and facilitate operations. This includes CleanUpLoader, a versatile backdoor delivered as fake software installers and often signed with valid digital certificates.

Persistence:

- To ensure continued access to compromised systems, Rhysida establishes persistence mechanisms.
- The group creates scheduled tasks to ensure the ransomware payload executes upon system startup, providing long-term access to compromised systems.
- Rhysida modifies registry entries to ensure its payload runs on system reboot.

Privilege Escalation:

- Rhysida operators use tools like `ntdsutil.exe` to copy the 'NTDS.dit' file, to a temporary folder
- These extracted credentials are then used to log into other hosts within the victim's domain.
- The group also employs `secretsdump` for credential extraction.

Defense Evasion:

- Rhysida appears to use fileless indicators, meaning its payload often resides in memory rather than on disk.
- Rhysida uses PowerShell and PsExec to clear event logs and delete forensic artifacts, such as recently accessed files and folders, RDP logs, and PowerShell command history.
- PowerShell scripts are specifically designed to terminate antivirus-related processes and services.

Discovery:

- Rhysida employs `net` commands and leverages tools like Advance IP/Port Scanner to enumerate victim environments and gather critical information about domains.

Lateral Movement:

- Rhysida makes extensive use of legitimate penetration testing and remote administration tools that are often misused by threat actors.
- Rhysida utilizes remote services such as Remote Desktop Protocol (RDP), Windows Remote Management (WinRM), and SSH via PuTTY to move laterally across victim networks.

Data Collection & Exfiltration:

- Rhysida targets a wide array of sensitive data, including personally identifiable information (PII), patient records, corporate documents, invoices, banking details, driver's licenses, passports, and Social Security Numbers (SSNs).
- Data is exfiltrated through diverse channels, including cloud storage services like MegaSync and custom PowerShell exfiltration scripts.

Impact & Encryption:

- After exfiltrating sensitive data, the group encrypts the victim's files and threatens to publicly release the stolen information on their dark web leak site if the ransom is not paid.
- Rhysida employs a hybrid encryption system using a two-layer scheme. Files are encrypted with the symmetric ChaCha20 algorithm.
- The ransomware is programmed to avoid encrypting certain system-critical files and directories (e.g., files with extensions like `.bat`, `.bin`, `.cmd`, `.dll`, `.exe`, `.sys`, and directories like `/boot`, `/dev`, `/etc`, `/proc`, `/sys` in Linux).

Rhysida Infrastructure

The infrastructure includes typosquatted domains, SEO poisoning, and C2 infrastructure for post-exfiltration activities. CleanUpLoader, commonly disguised as a software installer, aids Rhysida in data exfiltration and persistence. Notably, Rhysida targets sectors like healthcare and education, and focuses on both Windows and Linux-based systems. (source)

Notable patterns in the attacker's actions

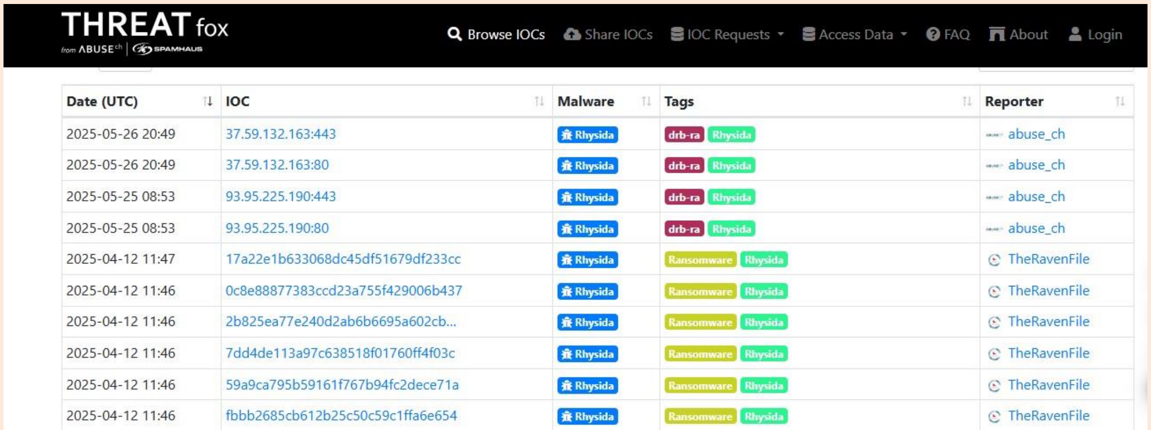
Rhysida Ransomware Indicators of Compromise:

SHA-256 HASH	DETECTION NAME
69b3d913a3967153d1e91ba1a31ebed839b297ed	Ransom.Win64.RHYSIDA.THEBBBC
338d4f4ec714359d589918cee1adad12ef231907	Ransom.Win64.RHYSIDA.THFOHBC
b07f6a5f61834a57304ad4d885bd37d8e1badba8	Ransom_Rhysida.R002C0DEV23 Ransom.Win64.RHYSIDA.SM
39649fa040a3c6894758016a65afec7b6acd4017	Ransom.Win64.RHYSIDA.SM
4947cf015875b169b6509a279941e854b022dd8e	Ransom.Win32.RHYSIDA.YXDGTT
c27a865b3ab1f0bd2ea1e8f7298b5ef9348c5ac	HZ_PSEXESVC
96dc78c00a622c3df5e038b8ed41b2de68e6c350	Trojan.PS1.SILENTKILL.A
df96143540d36edf1b9d9d25d91778855cafa8a6	Ransom.PS1.RHYSIDA.YXDHJ
a1034cdc499b4c551e43bc259d10928d75293214	Trojan.PS1.SILENTKILL.THHOIBC
de52c40ca449c7285660541c84ac5d6fe78a6bff	Trojan.PS1.SILENTKILL.YXDHHT
e14ee9ad241517ef72a4c6561fb848f6d659e764	Trojan.JS.QAKBOT.SFSJ

URL	DESCRIPTION
rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad[.]onion	Rhysida leak site
776c5589[.]schedule[.]newhomessection[.]com	URIs Used to Support Rhysida Operations
hxxps[:]//oij89jiiuguygh.blob.core.windows[.]net/	
776c5589[.]schedule[.]newhomessection[.]com	
hxxps[:]//e57thgdfge.blob.core.windows[.]net/	

Email Address	DESCRIPTION
rhysidaeverywhere@onionmail[.]org	Email Addresses Used to Support Rhysida Operations
rhysidaofficial@onionmail[.]org	

And for more IOCs, I used python script to collect them from Threat fox TIP.



Date (UTC)	IOC	Malware	Tags	Reporter
2025-05-26 20:49	37.59.132.163:443	Rhysida	drb-ra Rhysida	abuse_ch
2025-05-26 20:49	37.59.132.163:80	Rhysida	drb-ra Rhysida	abuse_ch
2025-05-25 08:53	93.95.225.190:443	Rhysida	drb-ra Rhysida	abuse_ch
2025-05-25 08:53	93.95.225.190:80	Rhysida	drb-ra Rhysida	abuse_ch
2025-04-12 11:47	17a22e1b633068dc45df51679df233cc	Rhysida	Ransomware Rhysida	TheRavenFile
2025-04-12 11:46	0c8e88877383ccd23a755f429006b437	Rhysida	Ransomware Rhysida	TheRavenFile
2025-04-12 11:46	2b825ea77e240d2ab6b6695a602cb...	Rhysida	Ransomware Rhysida	TheRavenFile
2025-04-12 11:46	7dd4de113a97c638518f01760ff4f03c	Rhysida	Ransomware Rhysida	TheRavenFile
2025-04-12 11:46	59a9ca795b59161f767b94fc2dece71a	Rhysida	Ransomware Rhysida	TheRavenFile
2025-04-12 11:46	fbbb2685cb612b25c50c59c1ffa6e654	Rhysida	Ransomware Rhysida	TheRavenFile

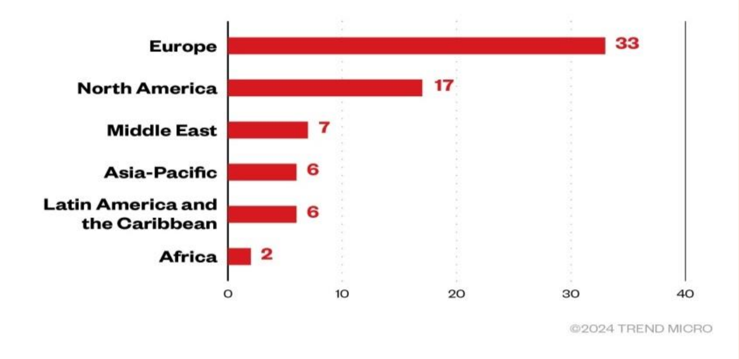
Rhysida's operational toolkit details

Rhysida's operational toolkit is not limited to its custom ransomware. It heavily integrates legitimate penetration testing tools (Cobalt Strike, PsExec, AnyDesk, WinSCP) with commodity malware and backdoors (PortStarter, SystemBC, Oyster/Broomstick, CleanUpLoader, Invicta Stealer).

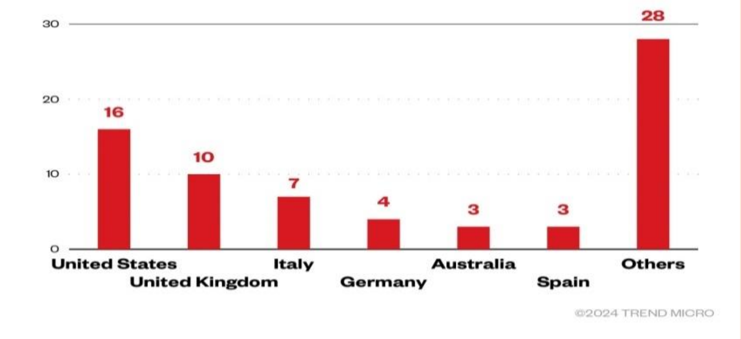
- The Rhysida ransomware payload itself is identified as a 64-bit Portable Executable (PE)
- payloads notably missing many commodity features common in modern ransomware, such as Volume Shadow Copy (VSS) removal.
- When executed, Rhysida typically displays a `cmd.exe` window as it traverses all files on local drives.
- The ransomware encrypts files using a hybrid encryption system, specifically employing the symmetric ChaCha20 algorithm.
- The ChaCha20 keys and Initialization Vectors (IVs) are then encrypted by a 4096-bit RSA public key.
- It appends the `.rhysida` extension to all encrypted files.
- Rhysida utilizes the open-source LibTomCrypt library for its encryption routine, including its pseudorandom number generator (PRNG) functionalities.
- To expedite data encryption, Rhysida employs parallel processing by creating sub-threads equivalent to the number of processors on the victim's PC and uses intermittent encryption, partially encrypting files to speed up the process.
- Rhysida’s operations are augmented by the use of several other malware families and legitimate tools, indicating a hybrid tooling strategy for efficiency and resilience.
- PortStarter and SystemBC malware families are utilized by Rhysida as a backdoor, facilitating command and control (C2) communications within compromised networks.
- A new variant of the Oyster backdoor, also known as Broomstick, was identified in Rhysida attacks in July 2024.
- CleanUpLoader is a versatile backdoor primarily linked to Rhysida threat actors.
- Invicta Stealer is coded in C++, has been observed being favored by Rhysida for data exfiltration.

List of victims from their Data Leak Sites (DLS)

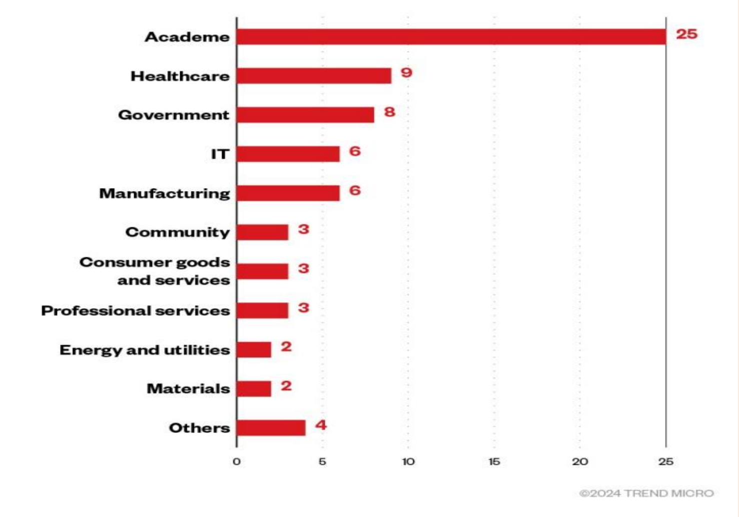
The distribution by region of Rhysida ransomware's victim organizations (June 7, 2023 – Jan. 13, 2024):



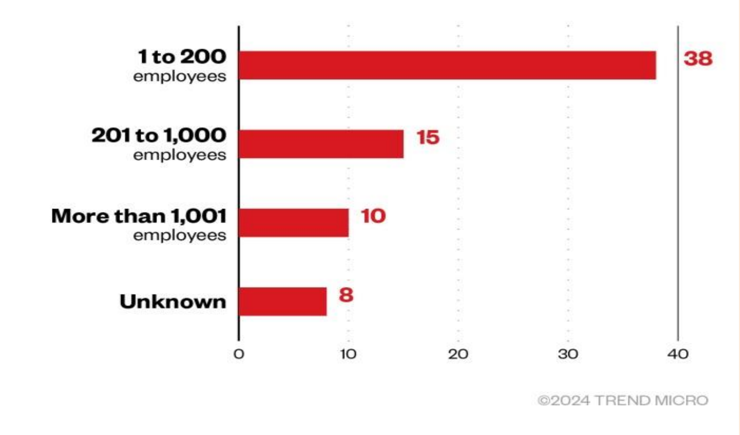
The distribution by country of Rhysida ransomware's victim organizations
(June 7, 2023 – Jan. 13, 2024):



The distribution by industry of Rhysida ransomware's victim organizations
(June 7, 2023 – Jan. 13, 2024):

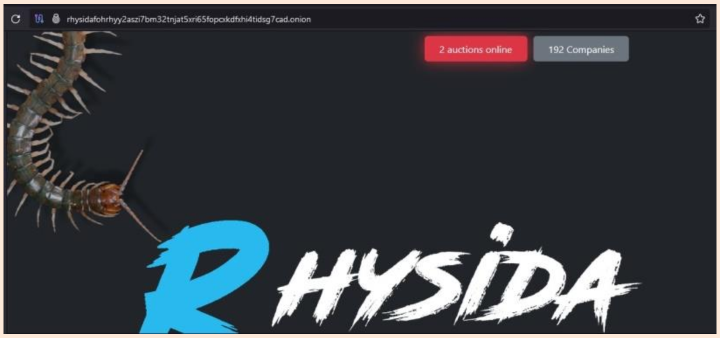


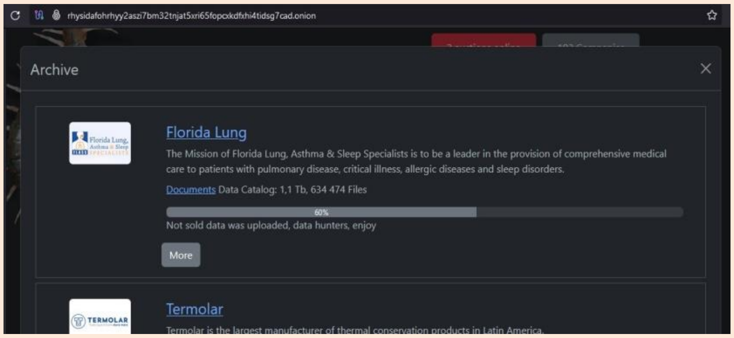
The distribution by organization size of Rhysida ransomware's victim organizations
(June 7, 2023 – Jan. 13, 2024):



How did I get the List of victims from Rhysida Data Leak Site?

1- From Rhysida site, I opened achieved companies


rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad.onion
2 auctions online
192 Companies
RHYSIDA


rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad.onion
Archive
×

Florida Lung

The Mission of Florida Lung, Asthma & Sleep Specialists is to be a leader in the provision of comprehensive medical care to patients with pulmonary disease, critical illness, allergic diseases and sleep disorders.

Documents Data Catalog: 1,1 Tb, 634 474 Files

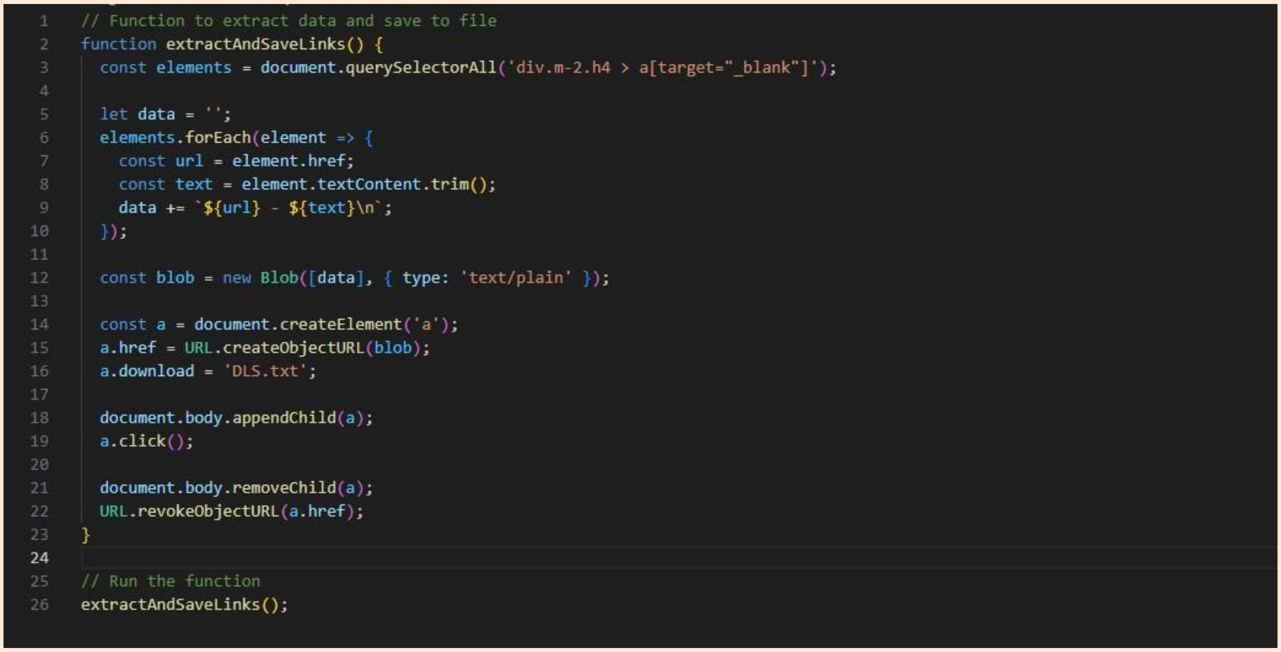
60%

Not sold data was uploaded, data hunters, enjoy

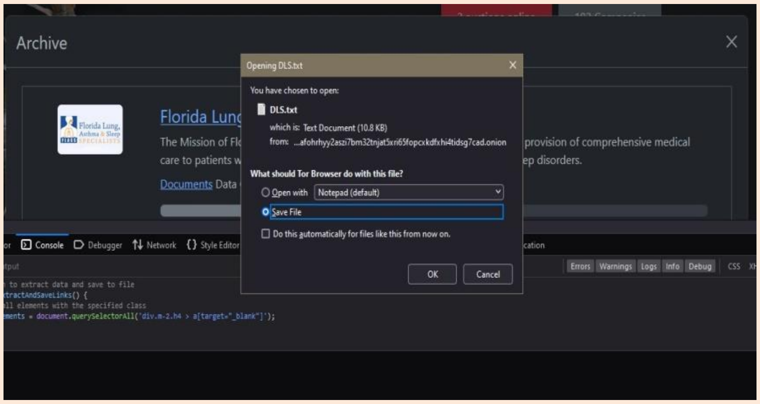
Termolar

Termolar is the largest manufacturer of thermal conservation products in Latin America.

2- I write simple Dom JS to extract all victims' names and links



```
// Function to extract data and save to file
function extractAndSaveLinks() {
  const elements = document.querySelectorAll('div.m-2.h4 > a[target="_blank"]');

  let data = '';
  elements.forEach(element => {
    const url = element.href;
    const text = element.textContent.trim();
    data += `${url} - ${text}\n`;
  });

  const blob = new Blob([data], { type: 'text/plain' });

  const a = document.createElement('a');
  a.href = URL.createObjectURL(blob);
  a.download = 'DLS.txt';

  document.body.appendChild(a);
  a.click();

  document.body.removeChild(a);
  URL.revokeObjectURL(a.href);
}

// Run the function
extractAndSaveLinks();
```



You have chosen to open:

DLS.txt

which is: Text Document (10.8 KB)

from: ...afohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad.onion

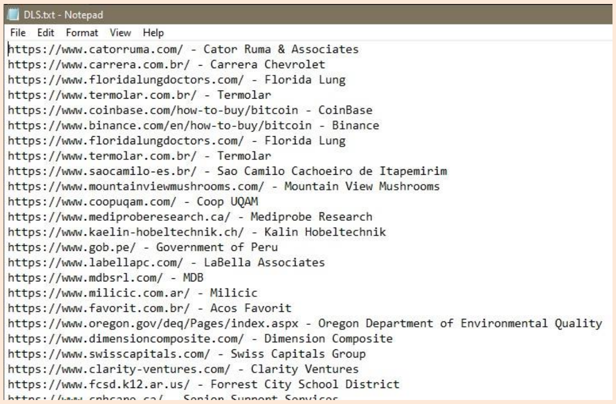
What should Tor Browser do with this file?

○ Open with Notepad (default)

● Save File

□ Do this automatically for files like this from now on.

```
 to extract data and save to file
tractAndSaveLinks() {
ll elements with the specified class
ments = document.querySelectorAll('div.m-2.h4 > a[target="_blank"]');
```



```
https://www.catorruma.com/ - Cator Ruma & Associates
https://www.carrera.com.br/ - Carrera Chevrolet
https://www.floridalungdoctors.com/ - Florida Lung
https://www.termolar.com.br/ - Termolar
https://www.coinbase.com/how-to-buy/bitcoin - CoinBase
https://www.binance.com/en/how-to-buy/bitcoin - Binance
https://www.floridalungdoctors.com/ - Florida Lung
https://www.termolar.com.br/ - Termolar
https://www.saocamilo-es.br/ - Sao Camilo Cachoeiro de Itapemirim
https://www.mountainviewmushrooms.com/ - Mountain View Mushrooms
https://www.coopuqam.com/ - Coop UQAM
https://www.mediproberesearch.ca/ - Mediprobe Research
https://www.kaelin-hobeltechnik.ch/ - Kalin Hobeltechnik
https://www.gob.pe/ - Government of Peru
https://www.labellapc.com/ - LaBella Associates
https://www.mdbsrl.com/ - MDB
https://www.milicic.com.ar/ - Milicic
https://www.favorit.com.br/ - Acos Favorit
https://www.oregon.gov/deq/Pages/index.aspx - Oregon Department of Environmental Quality
https://www.dimensioncomposite.com/ - Dimension Composite
https://www.swisscapitals.com/ - Swiss Capitals Group
https://www.clarity-ventures.com/ - Clarity Ventures
https://www.fcsd.k12.ar.us/ - Forrest City School District
```