Rhysida ransomware behind recent attacks on healthcare

bleepingcomputer.com/news/security/rhysida-ransomware-behind-recent-attacks-on-healthcare/

Bill Toulas

By
Bill Toulas

- August 9, 2023
- 02:31 PM
- 1

The Rhysida ransomware operation is making a name for itself after a wave of attacks on healthcare organizations has forced government agencies and cybersecurity companies to pay closer attention to its operations.

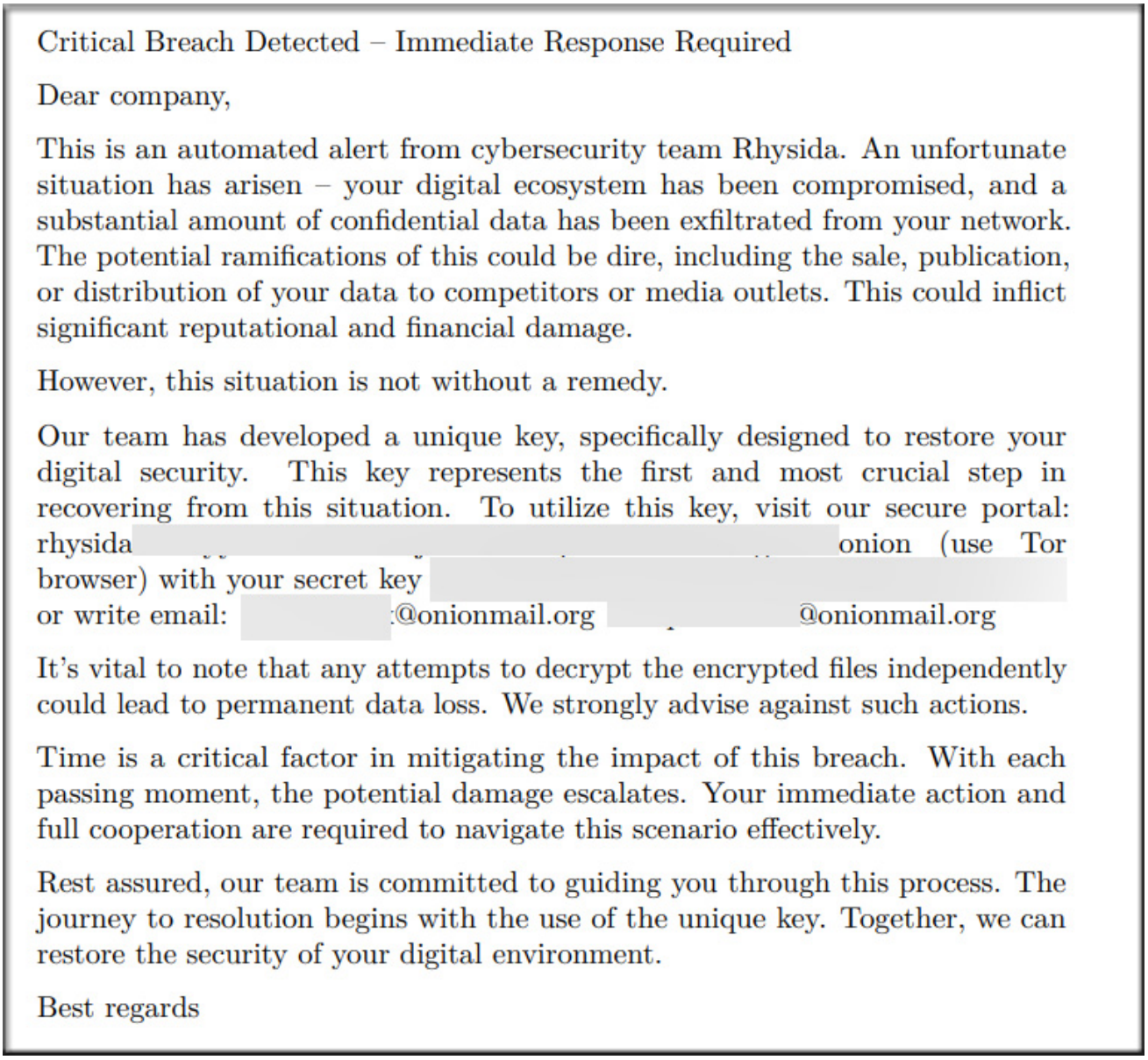
Following a security bulletin by the U.S. Department of Health and Human Services (HHS), CheckPoint, Cisco Talos, and Trend Micro have all released reports on Rhysida, focusing on different aspects of the threat actor's operations.

Previously, in June, Rhysida drew attention for the first time after leaking documents stolen from the Chilean Army (Ejército de Chile) on its data leak site.

At the time, a preliminary analysis of the Rhysida encryptor by SentinelOne showed that the ransomware was in early development, missing standard features seen in most strains like persistence mechanisms, Volume Shadow Copy wiping, process termination, etc.

"This is an automated alert from cybersecurity team Rhysida," reads the Rhysida ransom note.

"An unfortunate situation has arisen – your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network."



Critical Breach Detected – Immediate Response Required

Dear company,

This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen – your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network. The potential ramifications of this could be dire, including the sale, publication, or distribution of your data to competitors or media outlets. This could inflict significant reputational and financial damage.

However, this situation is not without a remedy.

Our team has developed a unique key, specifically designed to restore your digital security. This key represents the first and most crucial step in recovering from this situation. To utilize this key, visit our secure portal: rhysida onion (use Tor browser) with your secret key
or write email: @onionmail.org @onionmail.org

It's vital to note that any attempts to decrypt the encrypted files independently could lead to permanent data loss. We strongly advise against such actions.

Time is a critical factor in mitigating the impact of this breach. With each passing moment, the potential damage escalates. Your immediate action and full cooperation are required to navigate this scenario effectively.

Rest assured, our team is committed to guiding you through this process. The journey to resolution begins with the use of the unique key. Together, we can restore the security of your digital environment.

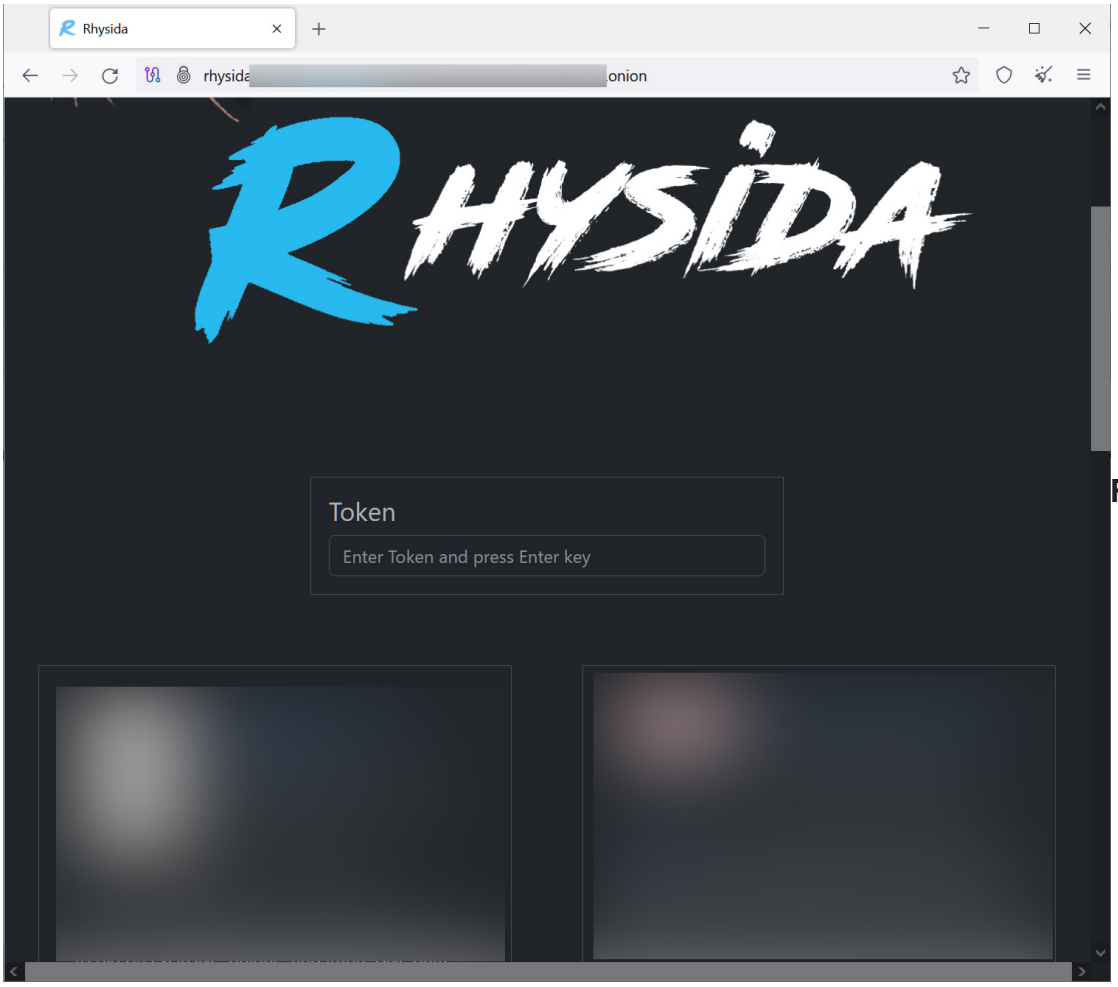
Best regards

Rhysida ransom note
Source: BleepingComputer

Rhysida targets healthcare orgs

While some ransomware operations claim not to intentionally target healthcare organizations and even provide free decryption keys if done by mistake, Rhysida does not appear to follow the same policy.

The Rhysida dark web data leak site lists a healthcare organization in Australia, giving them a week to pay a ransom before the stolen data is leaked.



Rhysida dark web data leak site

Source: BleepingComputer

A bulletin published by the U.S. Department of Health and Human Services (HHS) last week warned that while Rhysida still uses an elementary locker, the scale of its activities has grown to dangerous proportions, and recently, the threat actors demonstrated a focus on the healthcare and public sector.

"Its victims are distributed throughout several countries across Western Europe, North, South America, and Australia," reads HHS's bulletin.

"They primarily attack education, government, manufacturing, and technology and managed service provider sectors; however, there has been recent attacks against the Healthcare and Public Health (HPH) sector."

Sources have told BleepingComputer that Rhysida is behind a recent cyberattack on Prospect Medical Holdings, which still experiences a system-wide outage impacting 17 hospitals and 166 clinics across the United States.

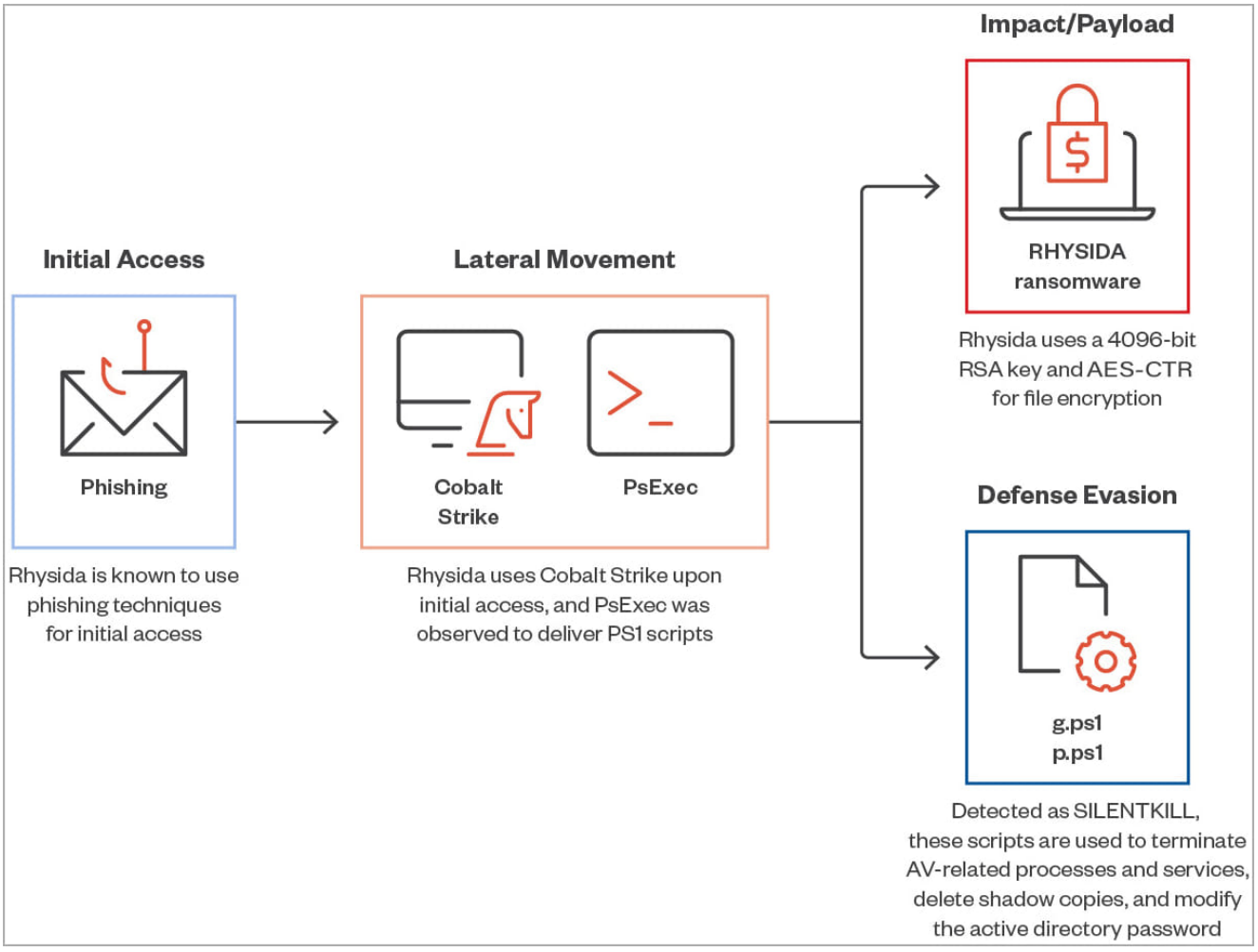
However, Rhysida has not taken responsibility for the attack yet, and PMH has not responded to emails on whether the ransomware gang is behind the attack.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731.

A Trend Micro report released today focuses on the most commonly observed Rhysida attack chain, explaining that the threat group uses phishing emails to achieve initial access, then deploys Cobalt Strike and PowerShell scripts, and eventually drops the locker.

An interesting observation from Trend Micro's analysts is that the PowerShell scripts used by Rhysida operators terminate AV processes, delete shadow copies, and modify RDP configurations, indicating the locker's active development.

A ransomware encryptor itself usually handles these tasks, but for the Rhysida operation, they use external scripts to achieve the same purposes.



Rhysida's latest attack chain *(Trend Micro)*

Cisco Talos' report confirms that the most recent Rhysida locker uses a 4096-bit RSA key with the ChaCha20 algorithm for file encryption and now excludes several directories as well as the following filetypes:

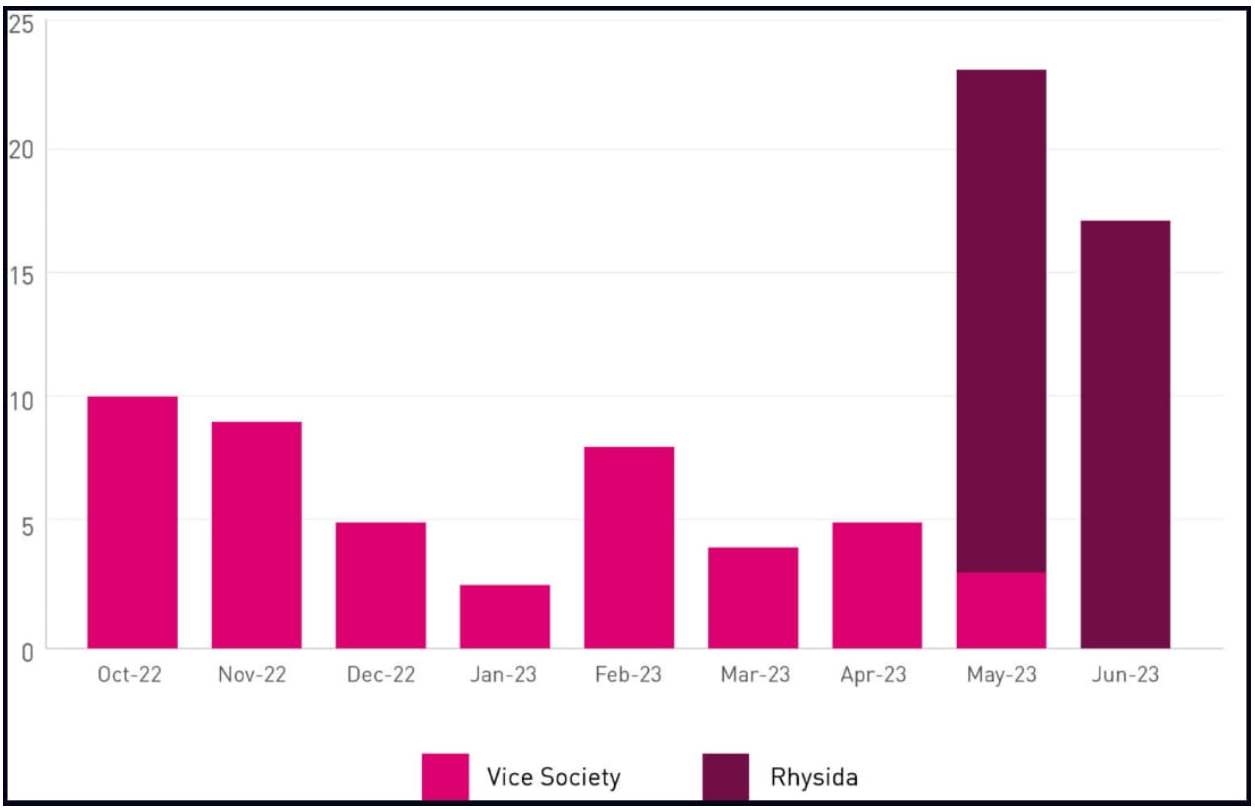
```
.bat .bin .cab .cmd .com .cur .diagcab .diagcfg, .diagpkg .drv .dll .exe .hlp .hta
.ico .lnk .msi .ocx .ps1 .psm1 .scr .sys .ini thumbs .db .url .iso and .cab
```

```
exclude_directories:                    ; DATA XREF: isDirectoryExcluded+65↑o
                                        ; isDirectoryExcluded+AE↑o
                text "UTF-32LE", '/$Recycle.Bin',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,'/Boot',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,'/Documents and Settings',0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,'/PerfLogs',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,'/Program Files',0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,'/Program Files (x86)',0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,'/ProgramData',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,'/Recovery',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,0,0,0,'/System Volume Information',0,0,0
                text "UTF-32LE", 0,0,0,0,'/Windows',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,0,0,'/$RECYCLE.BIN',0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,0,0,0
                align 20h
```

Directories excluded from encryption

Source: Cisco

CheckPoint's report goes a step further, linking Rhysida to the now-defunct Vice Society ransomware operation, based on the victim publishing times on the two extortion sites and their similar victim targeting patterns..



Comparison of activity change in Vice Society and Rhysida *(CheckPoint)*

In conclusion, Rhysida has established itself in the ransomware space quickly, targeting organizations in various sectors and showing no hesitation in attacking hospitals.

Although the RaaS appeared to move too quickly in terms of operations while the technical aspect lagged behind, developments on that front show that the locker is catching up.

Related Articles:

Rhysida claims ransomware attack on Prospect Medical, threatens to sell data

The Week in Ransomware - August 11th 2023 - Targeting Healthcare

Mom’s Meals discloses data breach impacting 1.2 million people

Japanese watchmaker Seiko breached by BlackCat ransomware gang

Hawai'i Community College pays ransomware gang to prevent data leak