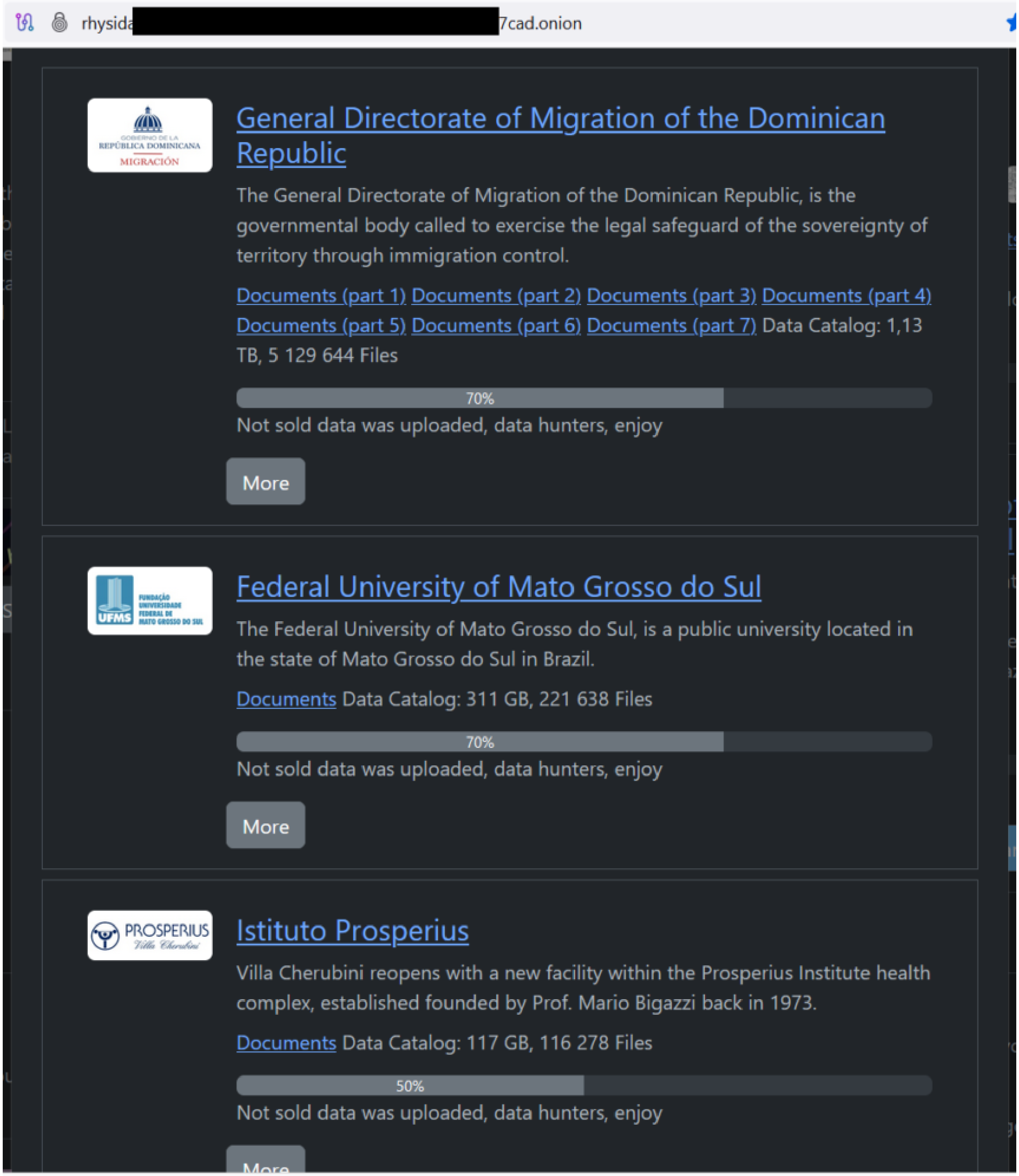
Rhysida Ransomware Technical Analysis

October 26, 2023

by Threat Research TeamOctober 26, 20236 min read

Rhysida is a new ransomware strain that emerged in the second quarter of 2023. The first mention of the Rhysida ransomware was in May 2023 by MalwareHunterTeam (sample's timestamp is May 16, 2023). As of Oct 12, the ransomware's leak site contains a list of over 50 attacked organizations of all types, including government, healthcare, and IT.


rhysida[redacted]7cad.onion
GOBIERNO DE LA REPÚBLICA DOMINICANA
MIGRACIÓN
UFMS
FUNDAÇÃO UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL
PROSPERIUS
Villa Cherubini

General Directorate of Migration of the Dominican Republic

The General Directorate of Migration of the Dominican Republic, is the governmental body called to exercise the legal safeguard of the sovereignty of territory through immigration control.

Documents (part 1) Documents (part 2) Documents (part 3) Documents (part 4) Documents (part 5) Documents (part 6) Documents (part 7) Data Catalog: 1,13 TB, 5 129 644 Files

70%

Not sold data was uploaded, data hunters, enjoy

More

Federal University of Mato Grosso do Sul

The Federal University of Mato Grosso do Sul, is a public university located in the state of Mato Grosso do Sul in Brazil.

Documents Data Catalog: 311 GB, 221 638 Files

70%

Not sold data was uploaded, data hunters, enjoy

More

Istituto Prosperius

Villa Cherubini reopens with a new facility within the Prosperius Institute health complex, established founded by Prof. Mario Bigazzi back in 1973.

Documents Data Catalog: 117 GB, 116 278 Files

50%

Not sold data was uploaded, data hunters, enjoy

More

Screenshot of the Rhysida data leak site as of Oct 16, 2023

Victims of the Rhysida ransomware can contact Avast experts directly at `decryptors-at-avast-dot-com` for a free consultation about how to mitigate damage caused by the attack.

Analysis of the Rhysida encryptor

The Rhysida encryptor comes as a 32-bit or 64-bit Windows PE file, compiled by MinGW GNU version 6.3.0 and linked by the GNU linker v 2.30. The first public version comes as a debug version, which makes its analysis easier.

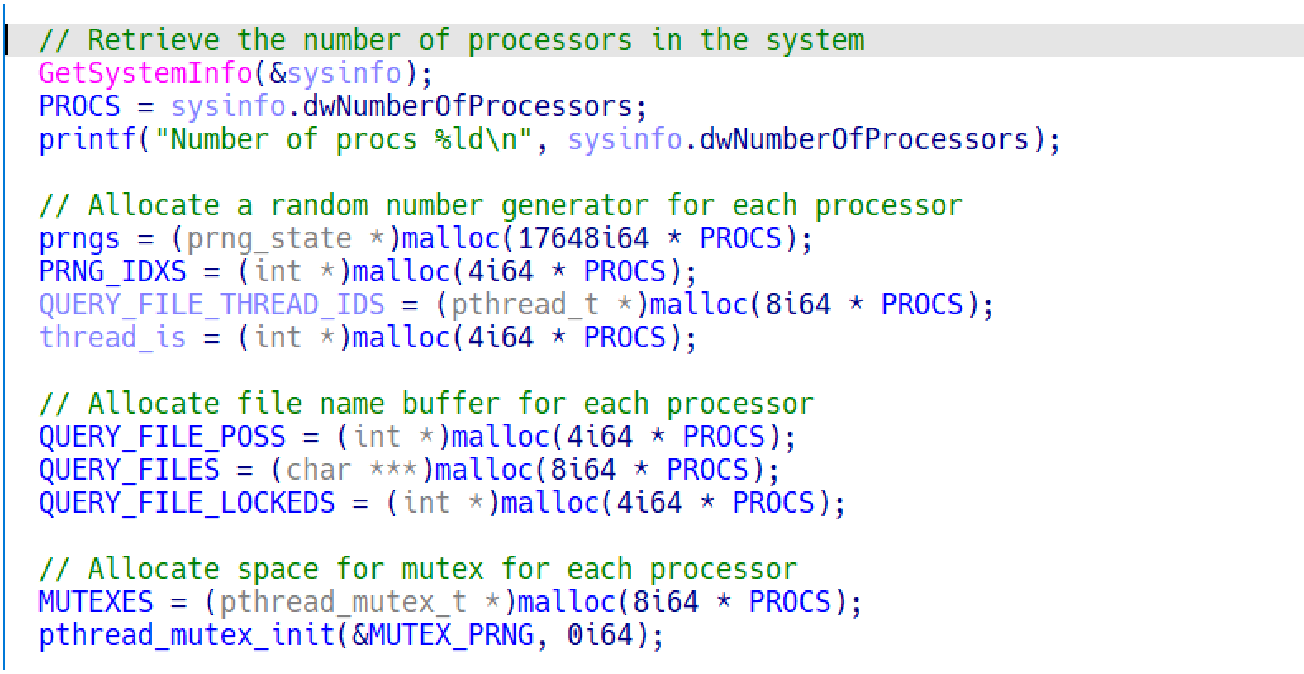
For cryptographic operations, Rhysida uses the LibTomCrypt library version 1.18.1. For multi-threaded and synchronization operations, Rhysida uses the winpthreads library. Chacha20 pseudo-random number generator is used for generating random numbers, such as AES encryption key, AES initialization vector and random padding for RSA-OAEP encryption. The public RSA key is hard-coded in the binary (ASN1-encoded) and loaded using the rsa_import function. Each sample has different embedded RSA key.

The encryptor executable supports the following command line arguments:

- `-d` Specifies a directory name to encrypt. If omitted, all drives (identified by letters) are encrypted
- `-sr` Enables self-remove after file encryption
- `-nobg` Disables setting desktop background
- `-S` When present, Rhysida will create a scheduled task, executing at OS startup under the System account
- `-md5` When present, Rhysida will calculate MD5 hash of each file before it is encrypted. However, this feature is not fully implemented yet – the MD5 is calculated, but it’s not used anywhere later.

When executed, the encryptor queries the number of processors in the system. This value serves for:

- Allocating random number generators (one per processor)
- Creating `Encryptor` threads (one per processor)



```
// Retrieve the number of processors in the system
GetSystemInfo(&sysinfo);
PROCS = sysinfo.dwNumberOfProcessors;
printf("Number of procs %ld\n", sysinfo.dwNumberOfProcessors);

// Allocate a random number generator for each processor
prngs = (prng_state *)malloc(17648i64 * PROCS);
PRNG_IDXS = (int *)malloc(4i64 * PROCS);
QUERY_FILE_THREAD_IDS = (pthread_t *)malloc(8i64 * PROCS);
thread_is = (int *)malloc(4i64 * PROCS);

// Allocate file name buffer for each processor
QUERY_FILE_POSS = (int *)malloc(4i64 * PROCS);
QUERY_FILES = (char ***)malloc(8i64 * PROCS);
QUERY_FILE_LOCKEDS = (int *)malloc(4i64 * PROCS);

// Allocate space for mutex for each processor
MUTEXES = (pthread_mutex_t *)malloc(8i64 * PROCS);
pthread_mutex_init(&MUTEX_PRNG, 0i64);
```

Initialization for multi-threaded encryption

Furthermore, Rhysida creates a `File Enumerator` thread, which searches all available disk drives by letter. Binaries prior July 2023 enumerate drives in normal order (from A: to Z:); binaries built after July 1st enumerate drives in reverse order (from Z: to A:).

The `File Enumerator` thread searches for files to encrypt and puts them into a synchronized list, ready to be picked by one of the `Encryptor` threads. Files in system critical folders, and files necessary to run operating systems and programs, are excluded from encryption.

List of skipped directories:

- /$Recycle.Bin
- /Boot
- /Documents and Settings
- /PerfLogs
- /Program Files
- /Program Files (x86)

- /ProgramData
- /Recovery
- /System Volume Information
- /Windows
- /$RECYCLE.BIN

List of skipped file types:

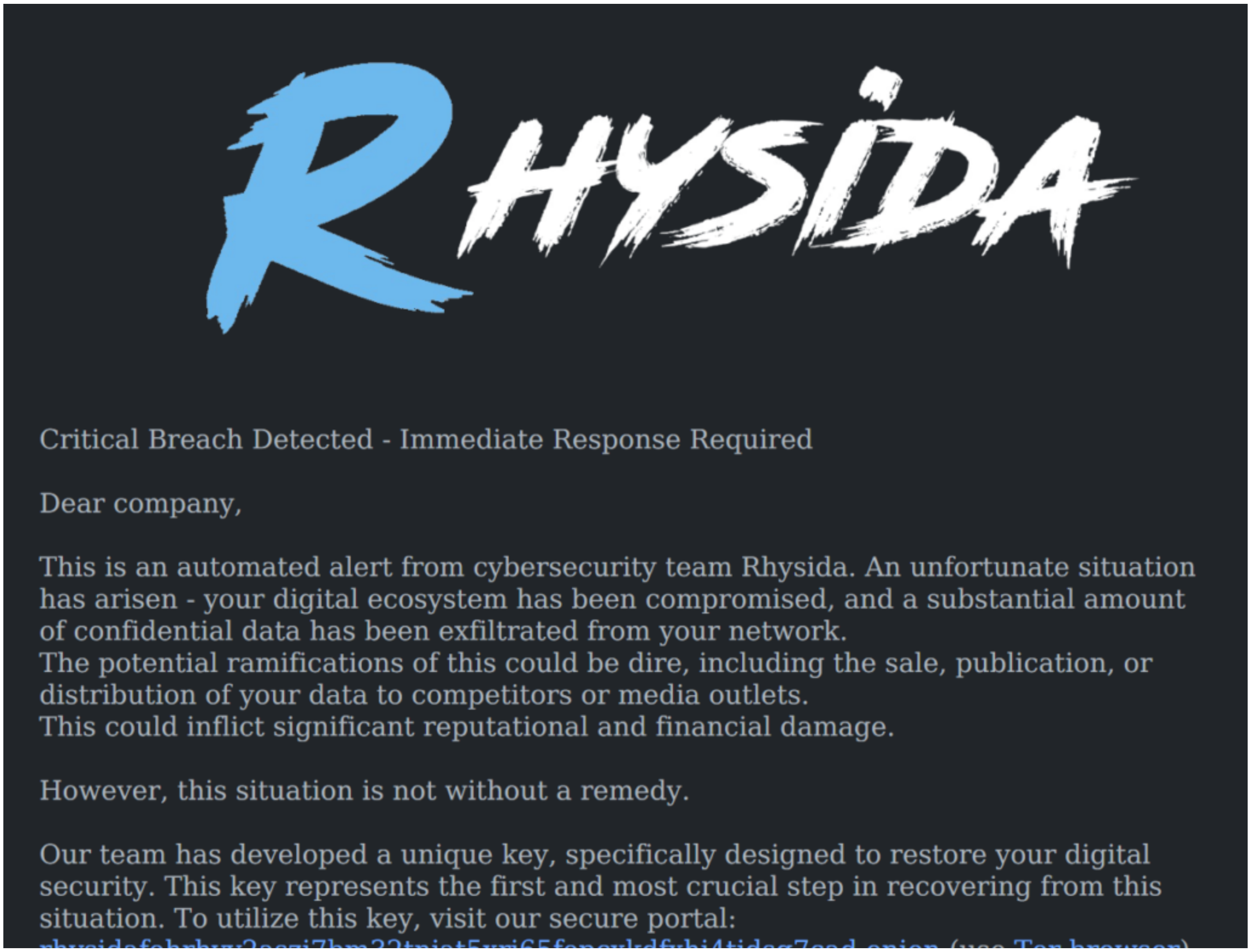
- .bat

- .bin
- .cab
- .cd
- .com
- .cur
- .dagaba
- .diagcfg
- .diagpkg

- .drv
- .dll
- .exe
- .hlp
- .hta
- .ico
- .lnk
- .msi
- .ocx

- .ps1
- .psm1
- .scr
- .sys
- .ini
- Thumbs.db
- .url
- .iso

Additionally, the ransom note file, usually named `CriticalBreachDetected.pdf`, is excluded from the list of encrypted files. The PDF content of the ransom note file is hard-coded in the binary and is dropped into each folder. The following picture shows an example of the ransom note from a September version of the ransomware:



Critical Breach Detected - Immediate Response Required

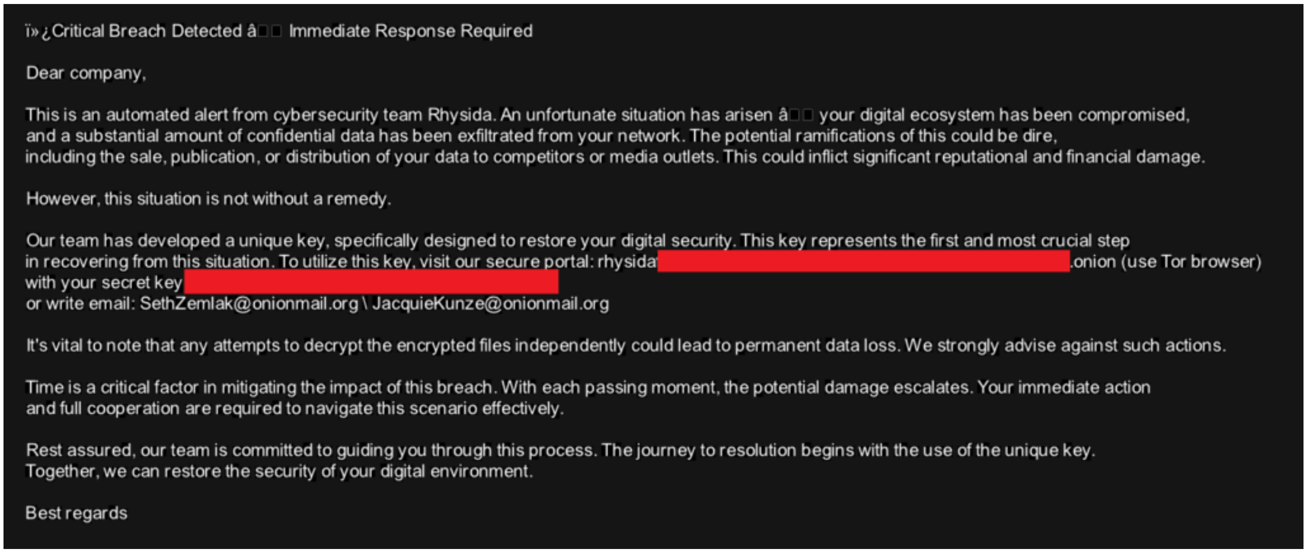
Dear company,

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:

In addition to dropping the ransom note, if enabled in the configuration, Rhysida generates a JPEG picture, which is stored into `C:/Users/Public/bg.jpg`. Earlier version of the ransomware generated the image with unwanted artifacts, which was fixed in later builds of Rhysida. The following picture shows an example of such JPEG pictures:



ï»¿Critical Breach Detected â□□ Immediate Response Required

Dear company,

This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen â□□ 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[redacted].onion (use Tor browser)
with your secret key [redacted]
or write email: SethZemlak@onionmail.org \ JacquieKunze@onionmail.org

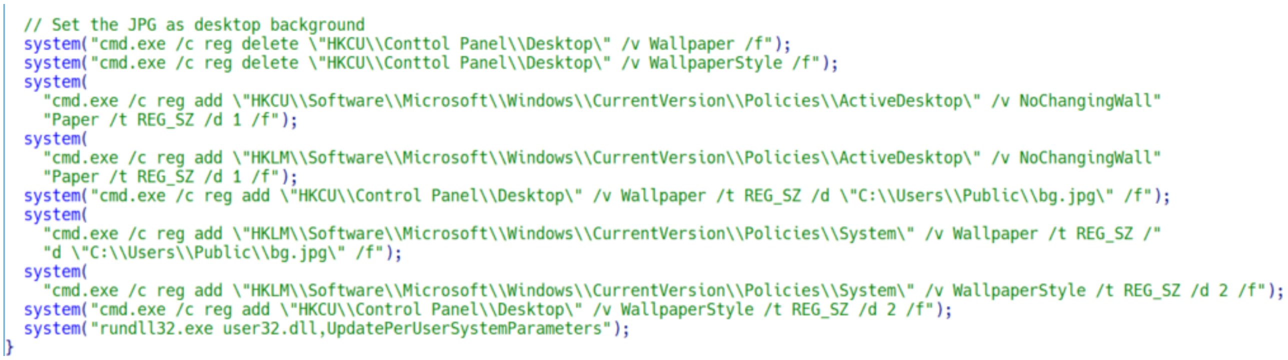
It's vital to note that any attempts to decrypt the encrypted files independently could lead to permanent data loss. We strongly advise against such actions.

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

The picture is set as the desktop background on the infected device. For that purpose, a set of calls to an external process via `system` (a C equivalent of CreateProcess) is used:



```
  // Set the JPG as desktop background
  system("cmd.exe /c reg delete \"HKCU\\Conttol Panel\\Desktop\" /v Wallpaper /f");
  system("cmd.exe /c reg delete \"HKCU\\Conttol Panel\\Desktop\" /v WallpaperStyle /f");
  system(
    "cmd.exe /c reg add \"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\ActiveDesktop\" /v NoChangingWall"
    "Paper /t REG_SZ /d 1 /f");
  system(
    "cmd.exe /c reg add \"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\ActiveDesktop\" /v NoChangingWall"
    "Paper /t REG_SZ /d 1 /f");
  system("cmd.exe /c reg add \"HKCU\\Control Panel\\Desktop\" /v Wallpaper /t REG_SZ /d \"C:\\Users\\Public\\bg.jpg\" /f");
  system(
    "cmd.exe /c reg add \"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\" /v Wallpaper /t REG_SZ /"
    "d \"C:\\Users\\Public\\bg.jpg\" /f");
  system(
    "cmd.exe /c reg add \"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\" /v WallpaperStyle /t REG_SZ /d 2 /f");
  system("cmd.exe /c reg add \"HKCU\\Control Panel\\Desktop\" /v WallpaperStyle /t REG_SZ /d 2 /f");
  system("rundll32.exe user32.dll,UpdatePerUserSystemParameters");
}
```

Rhysida may or may not (depending on the configuration and binary version) execute additional actions, including:

- Delete shadow copies using:

  ```
  cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet
  ```

- Delete the event logs with this command:

  ```
  cmd.exe /c for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
  ```

- Delete itself via Powershell command

  ```
  cmd.exe /c start powershell.exe -WindowStyle Hidden -Command Sleep -Milliseconds 500; Remove-Item -Force -Path "%BINARY_NAME%” -ErrorAction SilentlyContinue;
  ```

- (Re-)create scheduled task on Windows startup:

  ```
  cmd.exe /c start powershell.exe -WindowStyle Hidden -Command “Sleep -Milliseconds 1000; schtasks /end /tn Rhsd; schtasks /delete /tn Rhsd /f; schtasks /create /sc ONSTART /tn Rhsd /tr \”
  ```

- Remove scheduled task using:

  ```
  cmd.exe /c start powershell.exe -WindowStyle Hidden -Command "Sleep -Milliseconds 1000; schtasks /delete /tn Rhsd /f;"
  ```

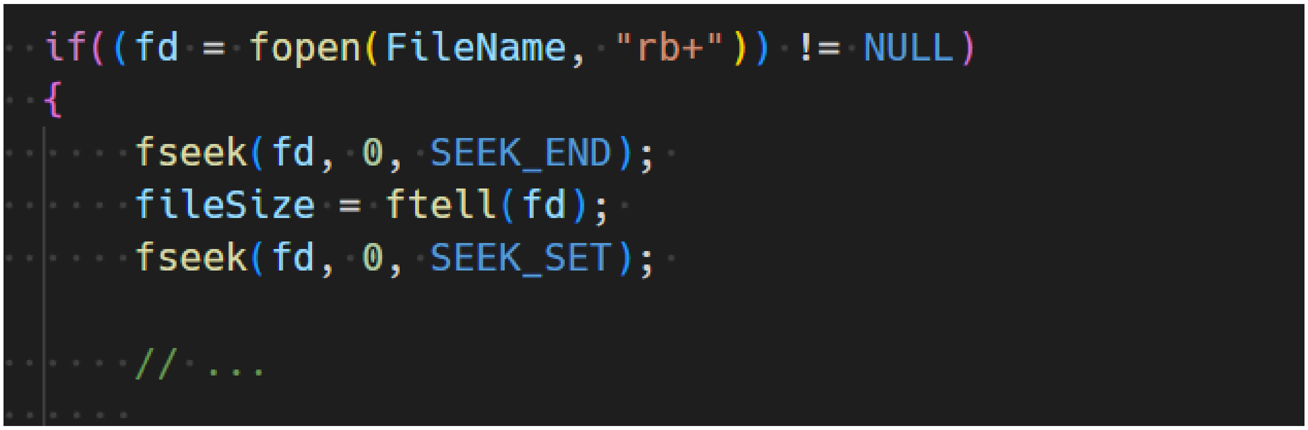
How Rhysida encrypts files

To achieve the highest possible encryption speed, Rhysida's encryption is performed by multiple `Encryptor` threads. Files bigger than 1 MB (1048576 bytes) are divided to 2-4 blocks and only 1 MB of data is encrypted from each block. The following table shows an overview of the number of blocks, size of one block and length of the encrypted part:

File Size	Block Count	Block Size	Encrypted Length
0 – 1 MB	1	(whole file)	(whole block)
1 – 2 MB	1	(whole file)	1048576
2 – 3 MB	2	File Size / 2	1048576
3 – 4 MB	3	File Size / 3	1048576
> 4MB	4	File Size / 4	1048576

Table 1: File sizes, block counts, block lengths and encrypted lengths.
Multiple steps are performed to encrypt a file:

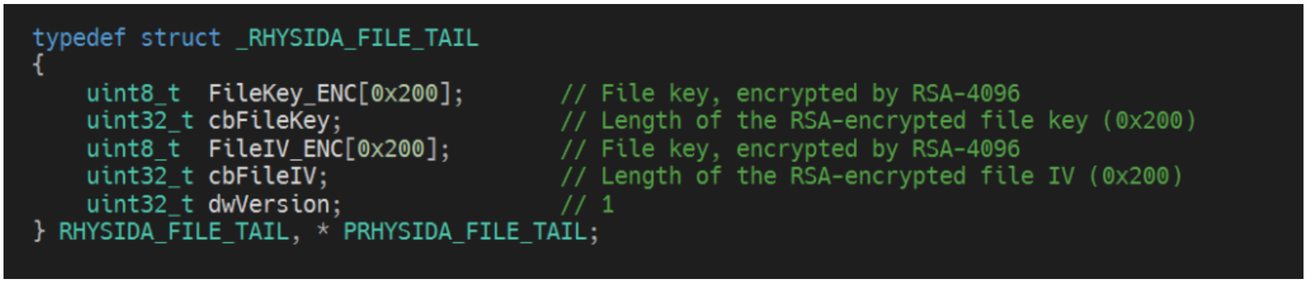
- The file is renamed to have the ".rhysida" extension.
- The file size is obtained by the sequence below. Note that earlier versions of the ransomware contain a bug, which causes the upper 32 bits of the file size to be ignored. In later versions of Rhysida, this bug is fixed.



```
  if((fd = fopen(FileName, "rb+")) != NULL)
  {
      fseek(fd, 0, SEEK_END);
      fileSize = ftell(fd);
      fseek(fd, 0, SEEK_SET);

      // ...
```

- Based on the file size, Rhysida calculates counts and length shown in Table 1.
- 32-byte file encryption key and 16-byte initialization vector for AES-256 stream cipher is generated using the random number generator associated with the `Encryptor` thread.
- Files are encrypted using AES-256 in CTR mode.
- Both file encryption key and the IV are encrypted by RSA-4096 with OAEP padding and stored to the file tail structure.
- This file tail is appended to the end of the encrypted file:



```
typedef struct _RHYSIDA_FILE_TAIL
{
    uint8_t  FileKey_ENC[0x200];       // File key, encrypted by RSA-4096
    uint32_t cbFileKey;                // Length of the RSA-encrypted file key (0x200)
    uint8_t  FileIV_ENC[0x200];        // File key, encrypted by RSA-4096
    uint32_t cbFileIV;                 // Length of the RSA-encrypted file IV (0x200)
    uint32_t dwVersion;                // 1
} RHYSIDA_FILE_TAIL, * PRHYSIDA_FILE_TAIL;
```

Conclusion

Rhysida is a relatively new ransomware, but already has a long list of attacked organizations. As of October 2023, it is still in an active development.

Victims of the Rhysida ransomware may contact us at `decryptors-at-avast-dot-com` for a consultation about how to mitigate damage caused by the attack.

Tagged asdecryptor, decryptors, ransomware
Share:XFacebook