# heimdall

security research

A DIVISION OF ISH

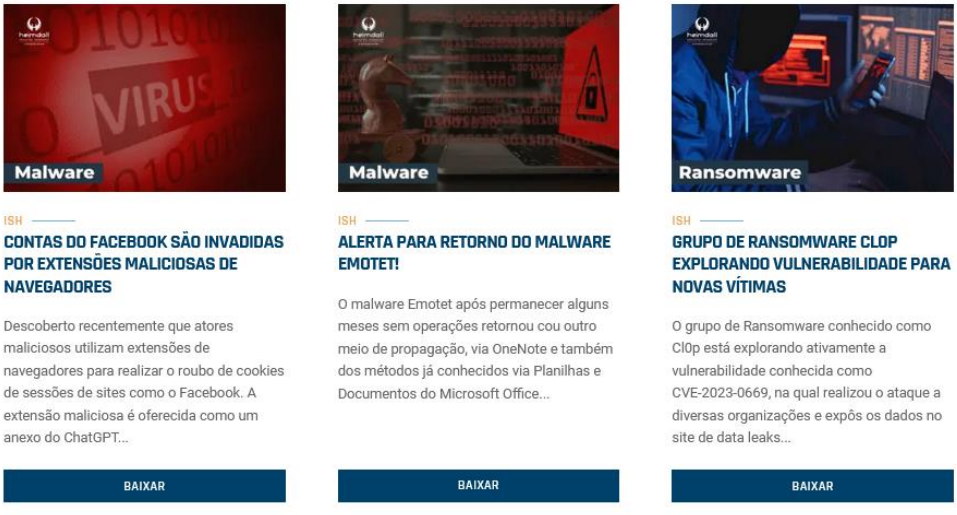
# Novo grupo de Ransomware: Rhysida

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

**Heimdall Security Research**


Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

**Boletins de Segurança – Heimdall**



## Sumário

1 Introdução ..... 7
2 Análise Técnica do Ransomware ..... 9
3 TTPs – MITRE ATT&CK ..... 14
4 Recomendações ..... 16
5 IoCs ..... 17
6 Referências ..... 18

# Lista de Tabelas

Tabela 1 – Pastas excluídas de criptografia. ..... 11
Tabela 2 – Arquivos excluídos de criptografia. ..... 12
Tabela 3 – Tabela Mitre Att&ck. ..... 15
Tabela 4 – IoC do ransomware. ..... 17

# Lista de Figuras

Figura 1 – Site de data leak do grupo Rhysida. ..... 7
Figura 2 – Publicação via twitter do ransomware Rhysida. ..... 7
Figura 3 – Informações do PE. ..... 9
Figura 4 – Strings identificadas no ransomware. ..... 9
Figura 5 – Argumentos do ransomware. ..... 10
Figura 6 – Prompt exibido durante a execução. ..... 11
Figura 7 – Algoritmo de criptografia. ..... 11
Figura 8 – Nota de resgate e comunicado via PDF. ..... 12
Figura 9 – Papel de parede alterado. ..... 13

# 1 INTRODUÇÃO

Um novo grupo de ransomwares foi identificado em maio de 2023, utilizando o nome de **Rhysida Ransomware**, o qual após realizar a criptografia dos arquivos, informa a organização vítima para que seja realizado o acesso via Rede Tor para iniciar as negociações.

A operação do Rhysida é similar aos demais grupos de ransomwares, adotando um site de data leak (vazamento de dados) para realizar a dupla extorsão da vítima.


*Figura 1 – Site de data leak do grupo Rhysida.*

O referido ransomware teria sido identificado por pesquisadores do perfil do twitter @malwhunterteam, publicado em 17 de maio de 2023 via twitter.

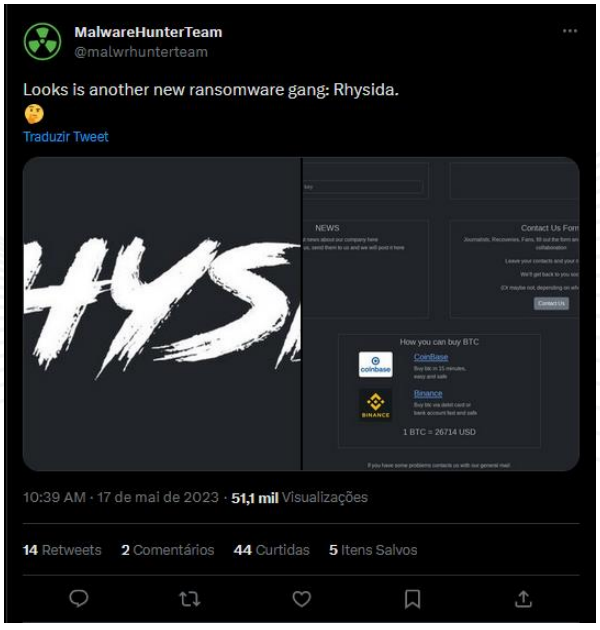



*Figura 2 – Publicação via twitter do ransomware Rhysida.*

Até o momento, através de pesquisas em fontes abertas foi possível obter apenas uma amostra do ransomware rhysida, bem como verificado que esta já foi analisada por pesquisadores, sendo apresentado os principais detalhes das análises na seção seguinte.

# 2 ANÁLISE TÉCNICA DO RANSOMWARE

Através da amostra de hashe: **a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6** correspondente ao arquivo malicioso do ransomware, é possível identificar que este fora analisado pela Secplicity e Cyble, obtendo os detalhes desta seção.

O ransomwares foi escrito na linguagem de programação **C++** e compilada utilizando o **MinGW,** com o tamanho de **1,2MB**.

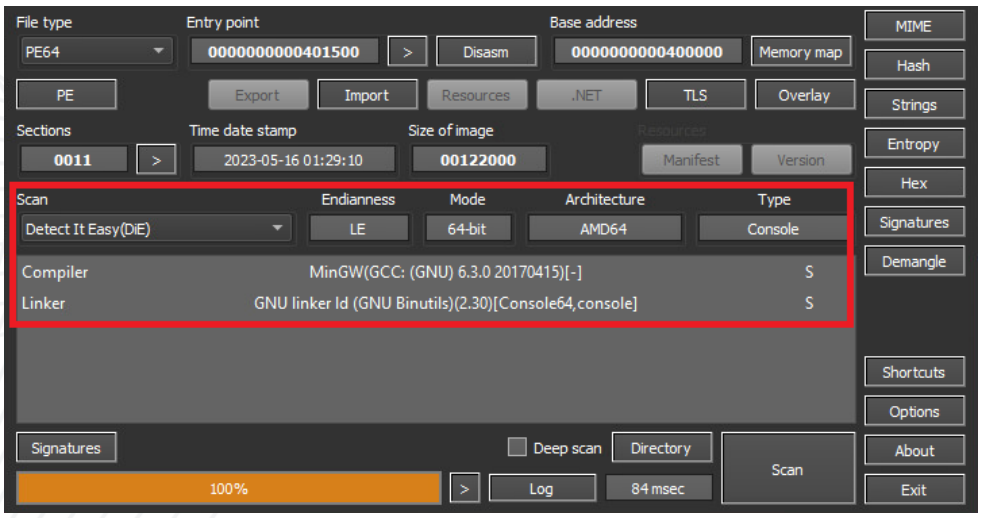



*Figura 3 – Informações do PE.*

Em análise de string, é possível verificar comandos via **"cmd.exe"** utilizados para realizar a troca de papel de parede após a criptografia, bem como a utilização do **PowerShell** do Windows.

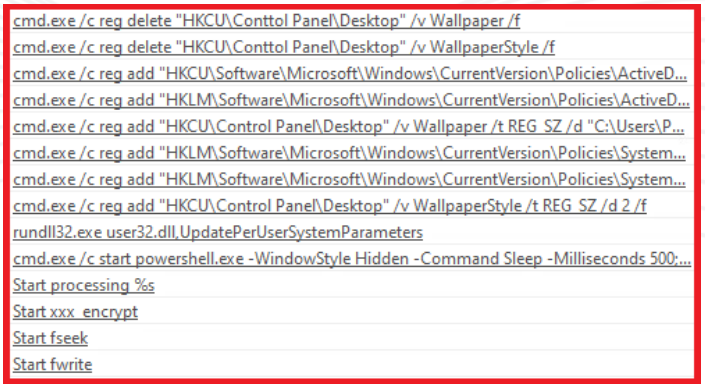



*Figura 4 – Strings identificadas no ransomware.*

Para sua execução, o ransomware aceita dois argumentos:

- **-d**: Selecione um diretório para criptografar
- **-sr**: O arquivo se exclui após a execução (“Eu serei removido”)

```
void __cdecl parseOptions(int argc, char **argv, Options *options)
{
  char _selfremoved[24]; // [rsp+20h] [rbp-60h] BYREF
  char self_remove_modifier[4]; // [rsp+41h] [rbp-3Fh] BYREF
  char directory_modifier[3]; // [rsp+45h] [rbp-3Bh] BYREF
  int dir_n; // [rsp+48h] [rbp-38h]
  int i; // [rsp+4Ch] [rbp-34h]

  options->program = (char *)malloc(0x1000ui64);
  options->directory = (char *)malloc(0x1000ui64);
  *options->directory = 0;
  options->is_self_remove = 1;
  strcpy(directory_modifier, "-d");
  strcpy(self_remove_modifier, "-sr");
  for ( i = 0; i < argc; ++i )
  {
    if ( i )
    {
      if ( !strcmp(argv[i], directory_modifier) )
      {
        if ( argv[++i] )
        {
          strcpy(options->directory, argv[i]);
          for ( dir_n = 0; dir_n < strlen(options->directory); ++dir_n )
          {
            if ( options->directory[dir_n] == 92 )
              options->directory[dir_n] = 47;
          }
        }
      }
      else if ( !strcmp(argv[i], self_remove_modifier) )
      {
        strcpy(_selfremoved, "I'm will be selfremoved");
        puts(_selfremoved);
        options->is_self_remove = 1;
      }
    }
    else
    {
      strcpy(options->program, *argv);
    }
  }
}
```

*Figura 5 – Argumentos do ransomware.*

Para que seja excluído, o ransomware utiliza o comando através do **powershell**:

- `"cmd.exe /c start powershell.exe -WindowStyle Hidden -Command Sleep -Milliseconds 500; Remove-Item -Force -Path \ ""`

O referido ransomwares utiliza vários segmentos para processar arquivos e diretórios, bem como abre diretórios e executa operações em arquivos. Realiza o rastreamento de estatísticas relacionadas aos arquivos processados, diretórios, erros, contagens de acessos e arquivos leia-me, sendo impresso na janela de prompt de comando após a sua execução.

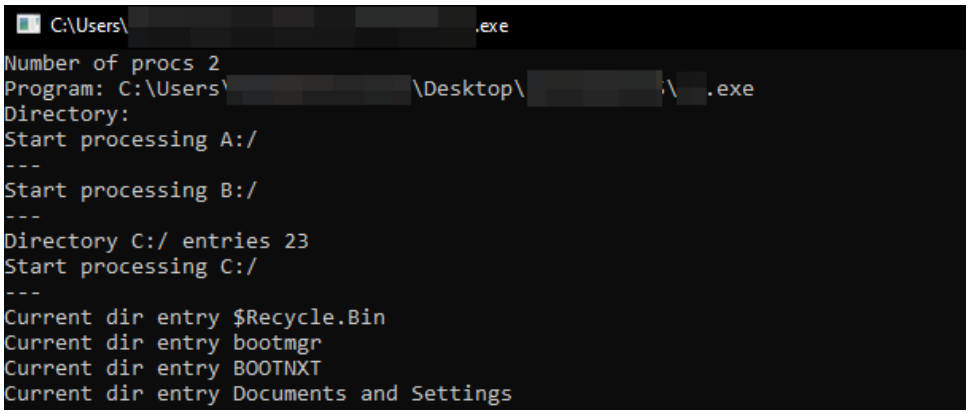



*Figura 6 – Prompt exibido durante a execução.*

Para a rotina de criptografia, o Ransomware Rhysida utiliza a **combinação de algoritmos** de criptografia **RSA** e **AES** para criptografar os arquivos.

```
for ( thread_i = 0; thread_i < PROCS; ++thread_i )
{
  if ( init_prng(&prngs[thread_i], &PRNG_IDXS[thread_i]) )
    goto LABEL_8;
}
if ( (unsigned int)rsa_import((__int64)_PUB_DER, _PUB_DER_LEN, (__int64)&key) )
{
  puts("ERROR rsa_import_key public");
}
else
{
  err = register_cipher(refptr_aes_enc_desc);
  if ( err )
  {
    v6 = (const char *)error_to_string((unsigned int)err);
    printf("ERROR Unable to register aes_enc_desc cipher %s\n", v6);
  }
  else
  {
    CIPHER = find_cipher("aes");
```

*Figura 7 – Algoritmo de criptografia.*

Para fins de criptogafia, o ransomware **não realiza a criptografia dos diretórios**:

| | | | |
|---|---|---|---|
| \$Recycle.bin | Documents and Settings | PerfLogs | Program Files |
| Program Files (x86) | ProgramData | Recovery | System Volume Information |

Tabela 1 – Pastas excluídas de criptografia.

Além dos diretórios, o ransomware **não realiza a criptografia de arquivos com as extensões**:

| | | | | |
|---|---|---|---|---|
| .bat | .bin | .cab | .cmd | .com |
| .cur | .diagcab | .diacfg | .diagpkg | .drv |
| .dll | .exe | .hlp | .hta | .ico |
| .lnk | .msi | .ocx | .ps1 | .psm1 |
| .scr | .sys | .ini | .db | .url. |
| .iso | .cab | | | |

Tabela 2 – Arquivos excluídos de criptografia.

E após a criptografia, o ransomware adiciona a extensão **“.rhysida”** para os arquivos que foram criptógrafos, bem como despeja um arquivo PDF chamado de **“CriticalBreachDetected.pdf”** contendo o link para a rede .onion (Tor).

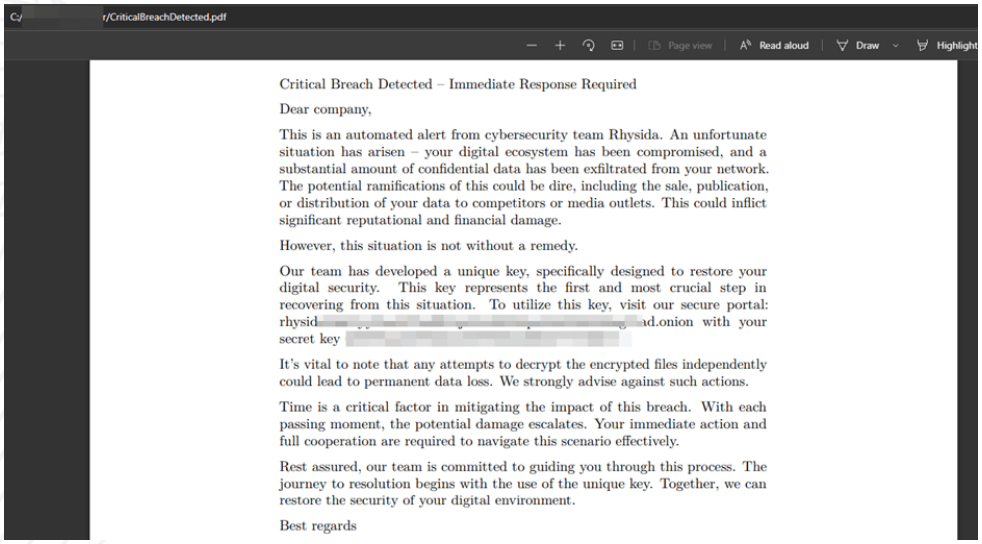



*Figura 8 – Nota de resgate e comunicado via PDF.*

Para fins de alteração de plano de fundo, o ransomware gera uma imagem de plano de fundo chamado **“bg.jpg”** contendo o conteúdo da nota de resgate no diretório **“C:\Users\Public”** e define como papel de parede. O ransomware utiliza os comandos:

- `system("cmd.exe /c reg delete \"HKCU\\Painel de controle\\Desktop\" /v Papel de parede /f");`
- `system("cmd.exe /c reg delete \"HKCU\\Painel de controle\\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");
```

Sendo alterado para o seguinte formato:

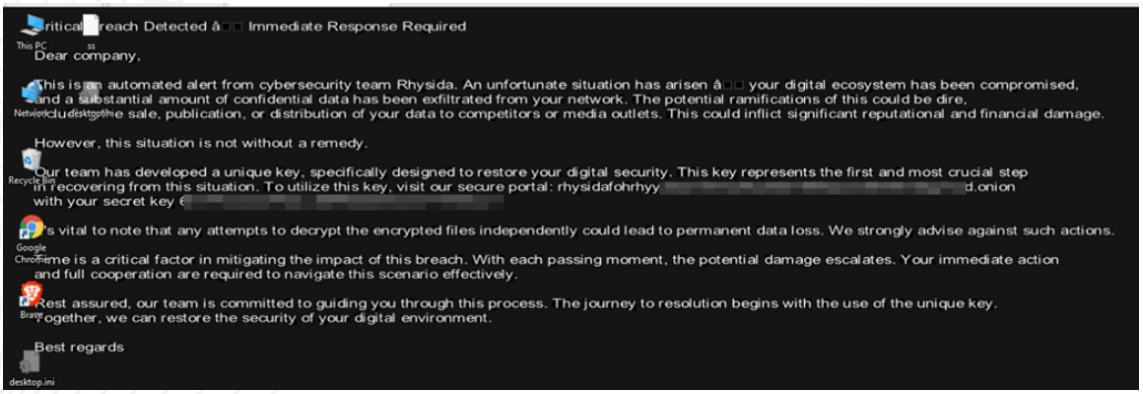



*Figura 9 – Papel de parede alterado.*

Portanto, com base na análise é possível verificar que a operação do ransomware está em sua **fase inicial de desenvolvimento**, bem como não há muitos recursos básicos que outros grupos utilizam como a remoção do VSS.

# 3 TTPs – MITRE ATT&CK

| Tática | Técnica | ID Técnica |
|---|---|---|
| Execution (TA0002) | Command and Scripting Interpreter | T1059 |
| | Shared Modules | T1129 |
| Persistence (TA0003) | Registry Run Keys/ Startup Folder | T1547.001 |
| Privilege Escalation (TA0004) | Process Injection | T1055 |
| | Thread Execution Hijacking | T1055.003 |
| Defense Evasion (TA0005) | Obfuscated Files or Information | T1027 |
| | Indicator Removal from Tools | T1027.005 |
| | Masquerading | T1036 |
| | Virtualization/Sandbox Evasion | T1497 |
| | Hide Artifacts | T1564 |
| | NTFS File Attributes | T1564.004 |
| | Reflective Code Loading | T1620 |
| Discovery (TA0007) | Application Windows Discovery | T1010 |
| | Process Discovery | T1057 |
| | System Information Discovery | T1082 |
| | File and Directory Discovery | T1083 |
| | Security Software Discovery | T1518.001 |
| Collection (TA0009) | Data from Local System | T1005 |
| | Automated Collection | T1119 |

| | | |
|---|---|---|
| Command and Control (TA0011) | Application Layer Protocol | T1071 |
| | Web Protocols | T1071.001 |
| Impact (TA0034) | Data Encrypted for Impact | T1486 |

Tabela 3 – Tabela Mitre Att&ck.

# 4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

- **Realização de *backups* regulares:** armazene cópias de segurança de todos os dados importantes em um local seguro e desconectado.
- **Realização de atualizações de *softwares*:** mantenha todos os *softwares* de ativos atualizados, incluindo sistemas operacionais e aplicativos.
- **Utilização de proteção de rede**, como *firewalls*, antivírus e outras medidas de segurança para proteger sua rede.
- **Realização do trabalho de conscientização** com os colaboradores, ensinando aos mesmos a reconhecer e evitar ameaças, como *phishing* e/ou clicar em *links* maliciosos.
- **Monitoração regular da sua rede e sistemas** para identificar e responder rapidamente a qualquer atividade suspeita.
- **Criação e aplicação de um plano de resposta de incidentes**, sendo que em caso de ataques de *ransomware* poderão ser utilizados e conterão informações como questões relacionadas a *backups* e recuperação de sistema.

# 5 IoCs

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

| Indicadores de compromisso de artefato malicioso/ analisado | |
|---|---|
| **md5:** | 0c8e88877383ccd23a755f429006b437 |
| **sha1:** | 69b3d913a3967153d1e91ba1a31ebed839b297ed |
| **sha256:** | a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6 |
| ***File name:*** | fury_ctm1042.bin |

Tabela 4 – IoC do ransomware.

# 6 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **MalwareHunterTeam - Twitter**
- **Ransomware Rhysida - SentinelOne**
- **Analise do Ransomware - Secplicity**
- **Identificação do Ransomware - Cyble**

heimdall
security research

A DIVISION OF ISH