What Cisco Talos knows about the Rhysida ransomware

blog.talosintelligence.com/rhysida-ransomware/

Cisco Talos August 8, 2023

By Cisco Talos

Tuesday, August 8, 2023 15:08

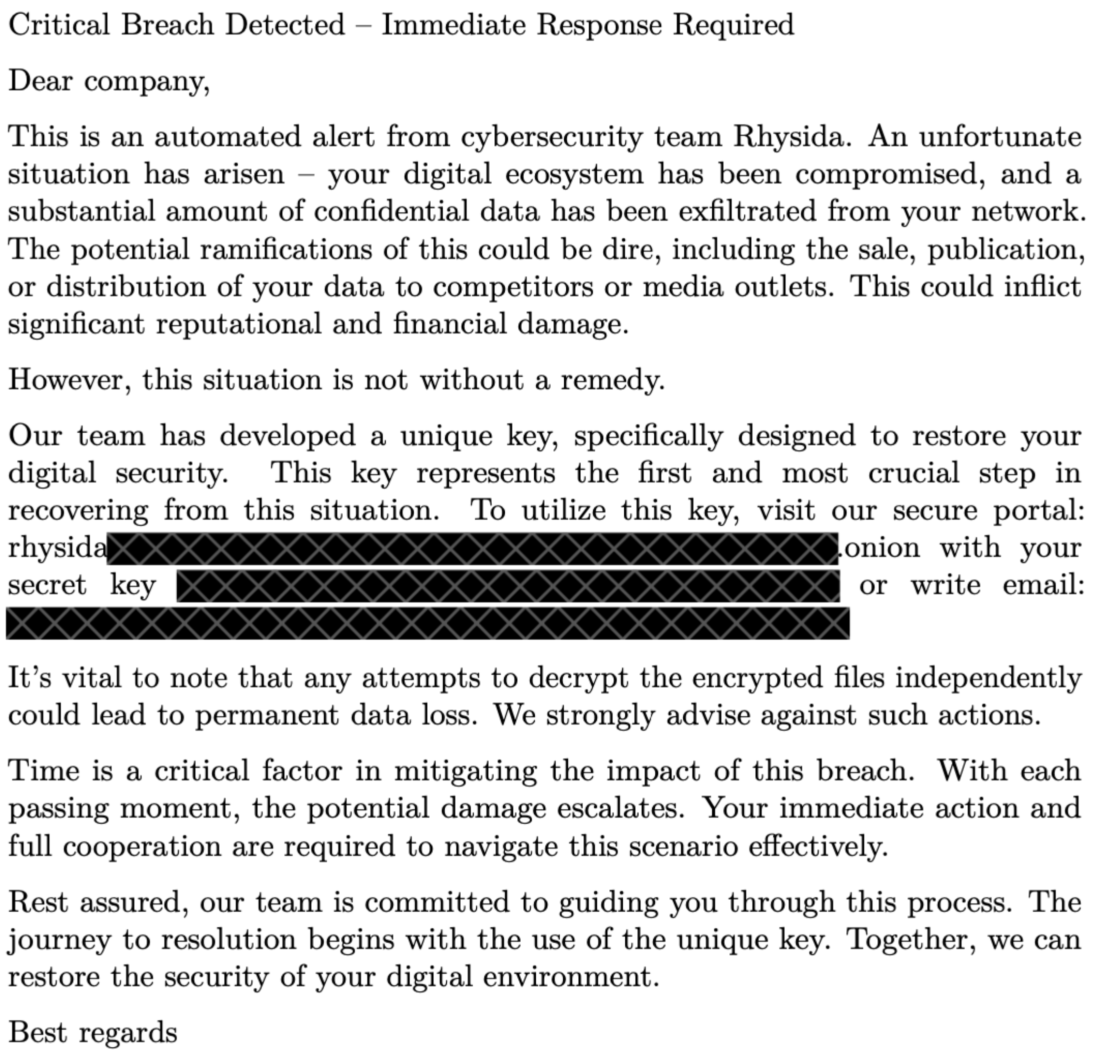
Cisco Talos is aware of the recent advisory published by the U.S. Department of Health and Human Services (HHS) warning the healthcare industry about Rhysida ransomware activity.

As we've discussed recently, there has been huge growth in the ransomware and extortion space, potentially linked to the plethora of leaked builders and source code related to various ransomware cartels. This is just another example of how these groups can now quickly develop their own ransomware variants by standing on the shoulders of those criminals who had their previous work exposed publicly. Rhysida appears to have first popped up back in May, with several high-profile compromises posted on their leak site.

Rhysida ransomware details

As we commonly see in the ransomware space, this threat is delivered through a variety of mechanisms which can include phishing and being dropped as secondary payloads from command and control (C2) frameworks like Cobalt Strike. These frameworks are commonly delivered as part of traditional commodity malware, so infection chains can vary widely.

The group itself likes to pretend to be a cybersecurity organization as shown in the ransom note below. They claim to have compromised the company and are willing to help resolve the issue. These types of approaches are not uncommon — historically, groups have done things like provide "security reports" to compromised organizations to help them "resolve the issue."



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[redacted].onion with your secret key [redacted] or write email: [redacted]

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.

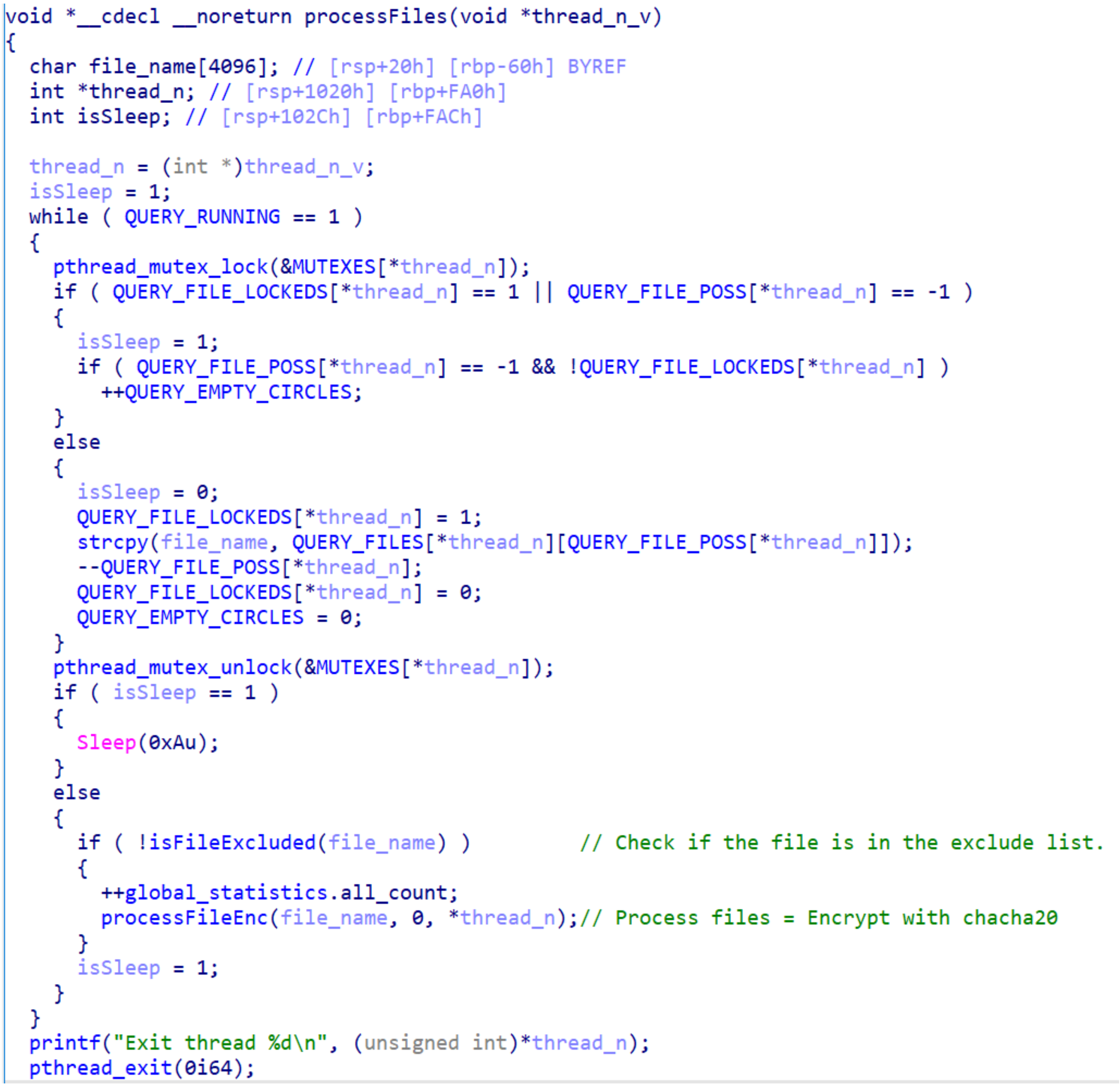
Best regards

Sample ransom note.

The group appears to commonly deploy double extortion — of the victims that have been listed on the leak site, several of them have had some portion of their exfiltrated data exposed.

Encryption algorithm

Rhysida's encryption algorithm is relatively straightforward and uses the ChaCha20 encryption algorithm. We have seen this algorithm deployed by other groups before, either as a standalone encryption algorithm or as part of a more custom approach. Rhysida will enumerate through directories and files in directories starting from "A:" to "Z:" drives, ensure they're missing from the "exclude list" and then "process," i.e., encrypt the files. Once encrypted, the file is then renamed to "<filename>.rhysida".

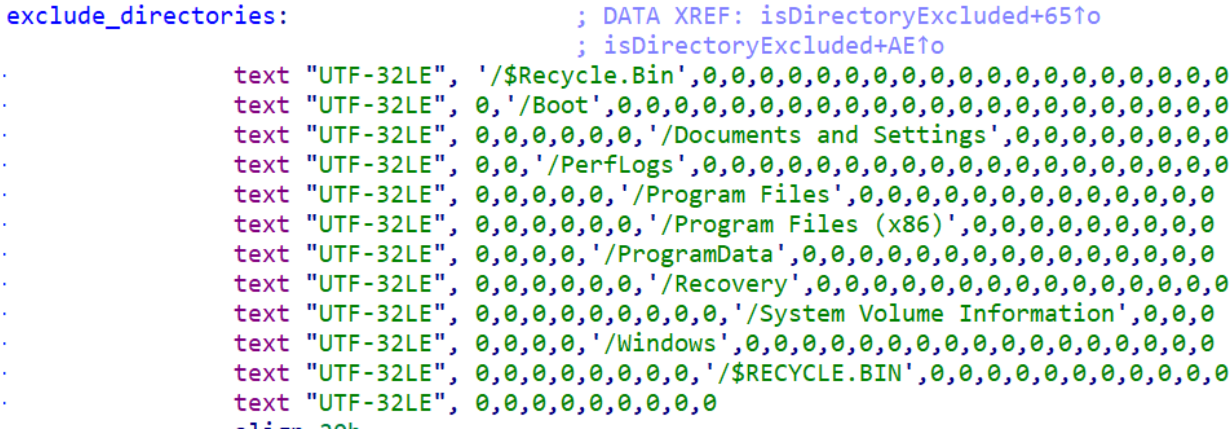


```
void *__cdecl __noreturn processFiles(void *thread_n_v)
{
  char file_name[4096]; // [rsp+20h] [rbp-60h] BYREF
  int *thread_n; // [rsp+1020h] [rbp+FA0h]
  int isSleep; // [rsp+102Ch] [rbp+FACh]

  thread_n = (int *)thread_n_v;
  isSleep = 1;
  while ( QUERY_RUNNING == 1 )
  {
    pthread_mutex_lock(&MUTEXES[*thread_n]);
    if ( QUERY_FILE_LOCKEDS[*thread_n] == 1 || QUERY_FILE_POSS[*thread_n] == -1 )
    {
      isSleep = 1;
      if ( QUERY_FILE_POSS[*thread_n] == -1 && !QUERY_FILE_LOCKEDS[*thread_n] )
        ++QUERY_EMPTY_CIRCLES;
    }
    else
    {
      isSleep = 0;
      QUERY_FILE_LOCKEDS[*thread_n] = 1;
      strcpy(file_name, QUERY_FILES[*thread_n][QUERY_FILE_POSS[*thread_n]]);
      --QUERY_FILE_POSS[*thread_n];
      QUERY_FILE_LOCKEDS[*thread_n] = 0;
      QUERY_EMPTY_CIRCLES = 0;
    }
    pthread_mutex_unlock(&MUTEXES[*thread_n]);
    if ( isSleep == 1 )
    {
      Sleep(0xAu);
    }
    else
    {
      if ( !isFileExcluded(file_name) )         // Check if the file is in the exclude list.
      {
        ++global_statistics.all_count;
        processFileEnc(file_name, 0, *thread_n);// Process files = Encrypt with chacha20
      }
      isSleep = 1;
    }
  }
  printf("Exit thread %d\n", (unsigned int)*thread_n);
  pthread_exit(0i64);
```

Rhysida’s algorithm for “processing” files.

The file exclusion list maintained in Rhysida samples is most of the usual system directories required for the operating system to function:



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

Excluded folders.

Excluded extensions include:

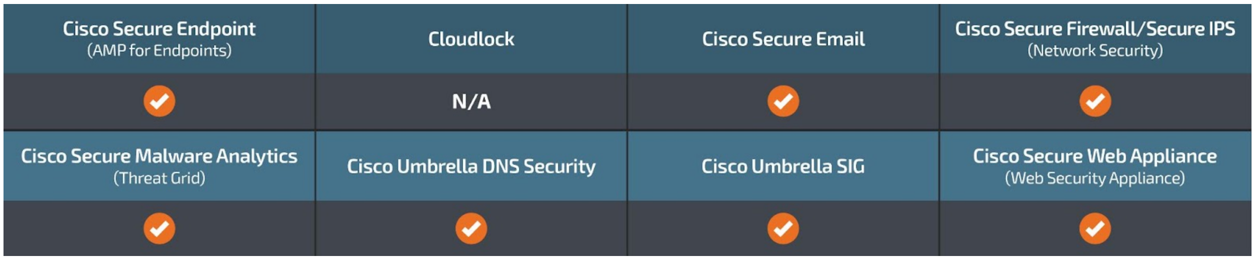
.bat .bin .cab .cmd .com .cur .diagcab .diagcfg, .diagpkg .drv .dll .exe .hlp .hta .ico .lnk .msi .ocx .ps1 .psm1 .scr .sys .ini Thumbs.db .url .iso .cab

After encryption, the ransomware will display the ransom note by creating and opening it as a PDF and the background wallpaper. The PDF usually named "CriticalBreachDetected.pdf" is generated using content embedded in the ransomware binary, including the skeleton PDF and the ransom note (shown above). The ransom note is also used to generate a message in the form of the background wallpaper typically located at "C:/Users/Public/bg.jpg".

This new ransomware variant doesn't have any novel features or functionality and points to the challenges organizations are facing as the landscape continues to shift and a plethora of new actors join their ranks. This isn't even the only new ransomware group we've written about this week.

Coverage

Ways our customers can detect and block this threat are listed below.



Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	Cisco Umbrella DNS Security	Cisco Umbrella SIG	Cisco Secure Web Appliance (Web Security Appliance)
✓	✓	✓	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.
Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Cisco Talos is releasing the following Snort SIDs to protect against this threat: 62220 - 62229, 300653 - 300657.

Indicators of compromise

D5C2F87033A5BAEEB1B5B681F2C4A156FF1C05CCD1BFDAF6EAE019FC4D5320EE

1A9C27E5BE8C58DA1C02FC4245A07831D5D431CDD1A91CD35D2DD0AD62DA71CD

258DDD78655AC0587F64D7146E52549115B67465302C0CBD15A0CBA746F05595

0BB0E1FCFF8CCF54C6F9ECFD4BBB6757F6A25CB0E7A173D12CF0F402A3AE706F

F6F74E05E24DD2E4E60E5FB50F73FC720EE826A43F2F0056E5B88724FA06FBAB

250E81EEB4DF4649CCB13E271AE3F80D44995B2F8FFCA7A2C5E1C738546C2AB1

A864282FEA5A536510AE86C77CE46F7827687783628E4F2CEB5BF2C41B8CD3C6

6903B00A15EFF9B494947896F222BD5B093A63AA1F340815823645FD57BD61DE

3BC0340007F3A9831CB35766F2EB42DE81D13AEB99B3A8C07DEE0BB8B000CB96

2A3942D213548573AF8CB07C13547C0D52D1C3D72365276D6623B3951BD6D1B2