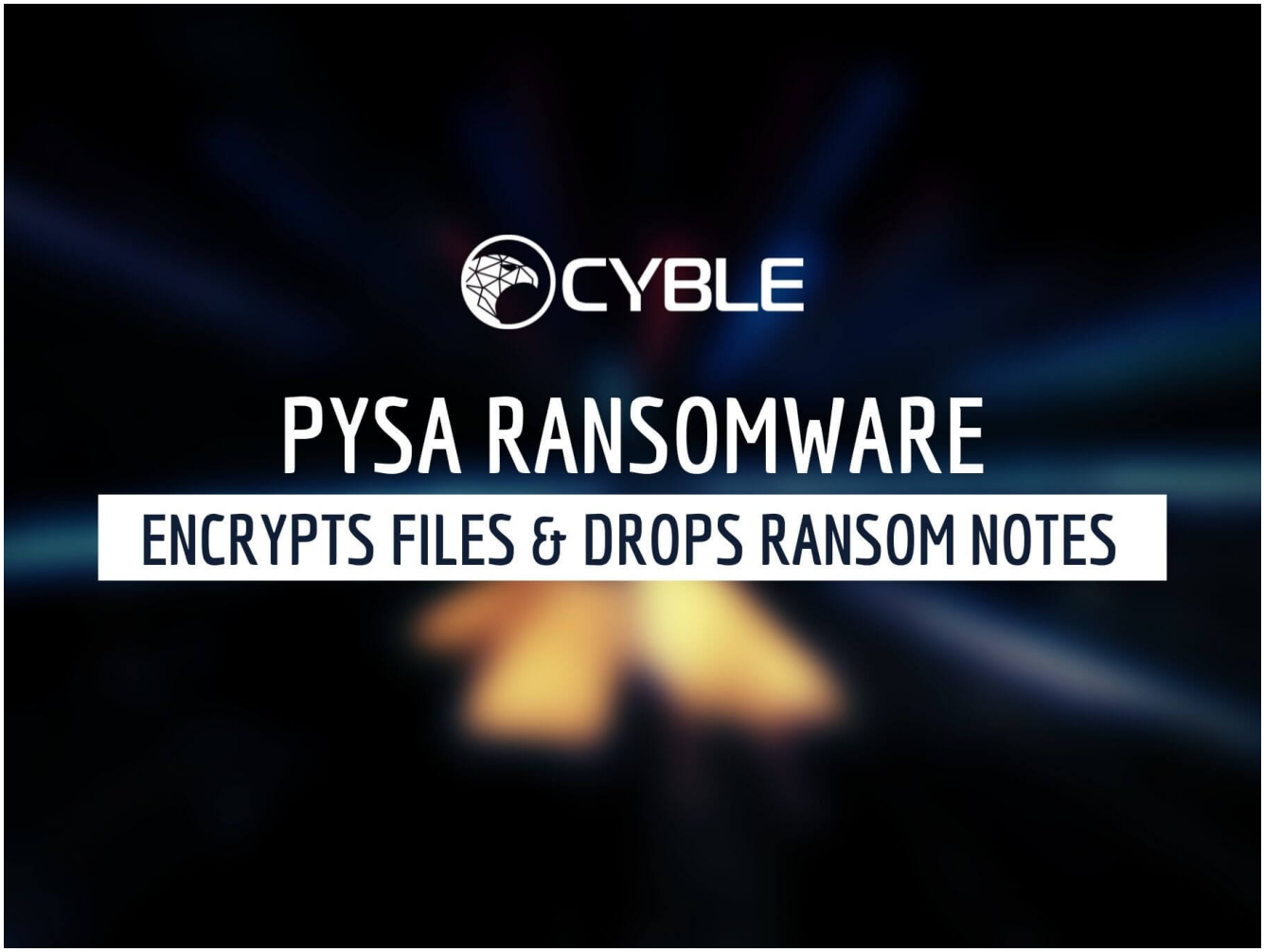
Pysa Ransomware Under the Lens: A Deep-Dive Analysis

blog.cyble.com/2021/11/29/pysa-ransomware-under-the-lens-a-deep-dive-analysis/

November 29, 2021



Initially observed in 2019, Pysa ransomware has actively targeted organizations in many countries. Once executed on the victim machine, Pysa encrypts the victim files and drops ransom notes to instruct users on how to recover the files in exchange for the ransom amount. It is human-operated ransomware and does not have self-propagation capability. Once the Threat Actor (TA) is done with the data exfiltration from the victim machine or organization, they execute Pysa for the encryption. The Pysa ransomware group is also known for double extortion.

Presently there are 190+ victims of the Pysa ransomware across the world, and the image below shows the Heat Map of countries impacted by the Pysa ransomware.

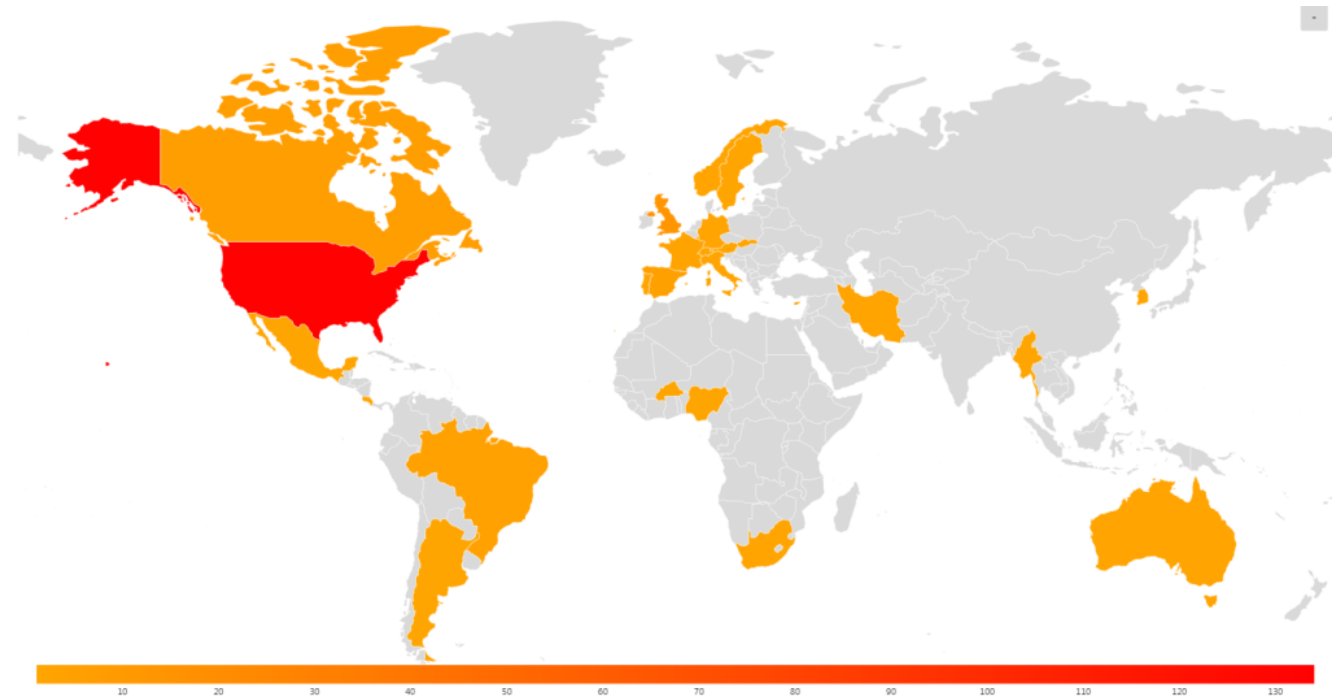


Figure 1 Pysa Ransomware Heat Map

The top 5 Countries affected by Pysa are the US, UK, Canada, Spain, and Brazil. Pysa has impacted industries like Education, Utilities, Transportation, Construction, Healthcare, and Business Services, etc. The Pysa ransomware group operates from the dark web site *pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqieywad[.]onion,* as shown below.

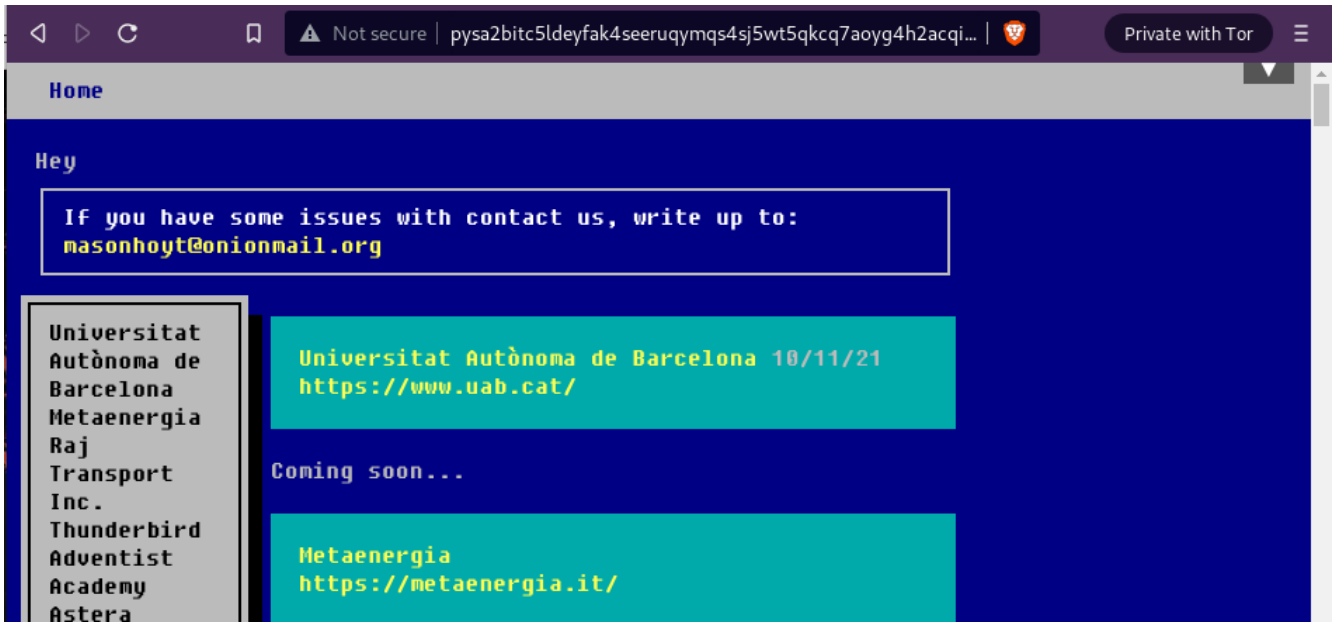


Figure 2 TOR Website of Pysa Ransomware group

The image below shows the high-level execution diagram of the Pysa ransomware. Initially, the ransomware creates a mutex with the name of Pysa, and later it enumerates drives in the victim's system. Additionally, it goes through files and directories to search for targeted files having specific extensions that are hardcoded in the malware. Once found, the ransomware appends the '*.pysa'* extension to the victim files and encrypts the content as a priority, followed by the encryption of the rest of the files. Later it carries out the registry modification and finally creates a file called *update.bat* for self-deletion.

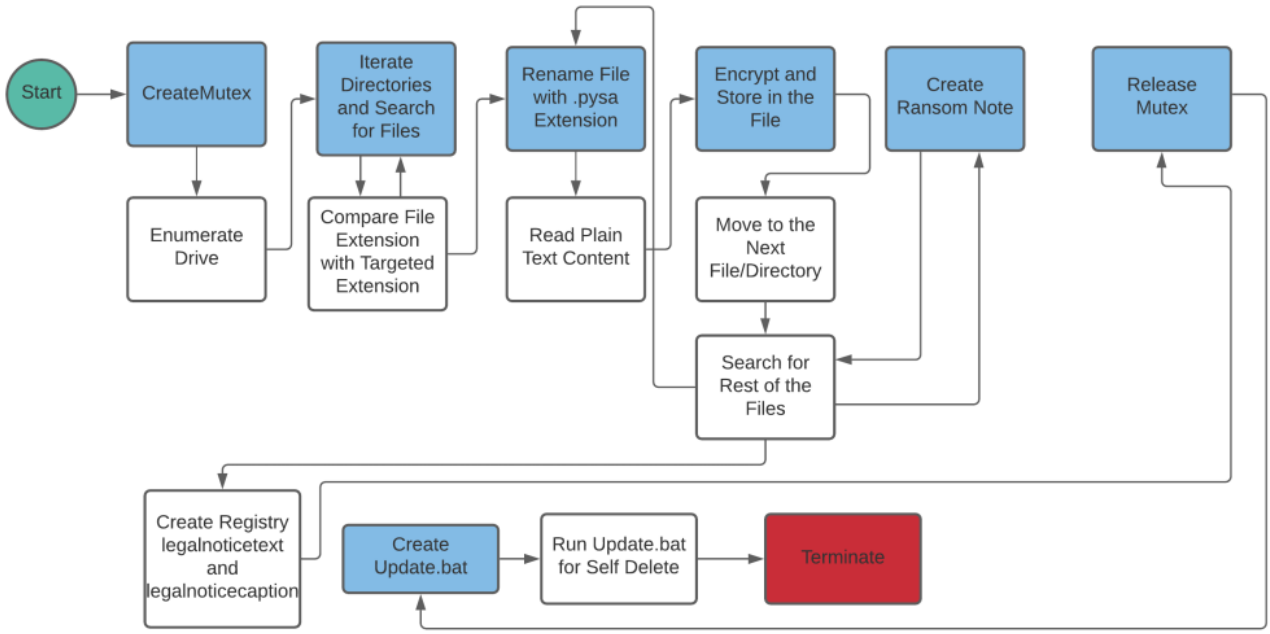


Figure 3 High-level Execution Flow of Pysa Ransomware

In this report, Cyble Research Labs has covered the deep-dive analysis of the Pysa ransomware to understand the behaviour and infection mechanism.

Technical Analysis

The Static properties of Pysa ransomware tell us that the ransomware is an x86 Windows Portable Executable (PE) written in the C/C++ language and compiled on 2021-10-11 10:21:04, as shown below.

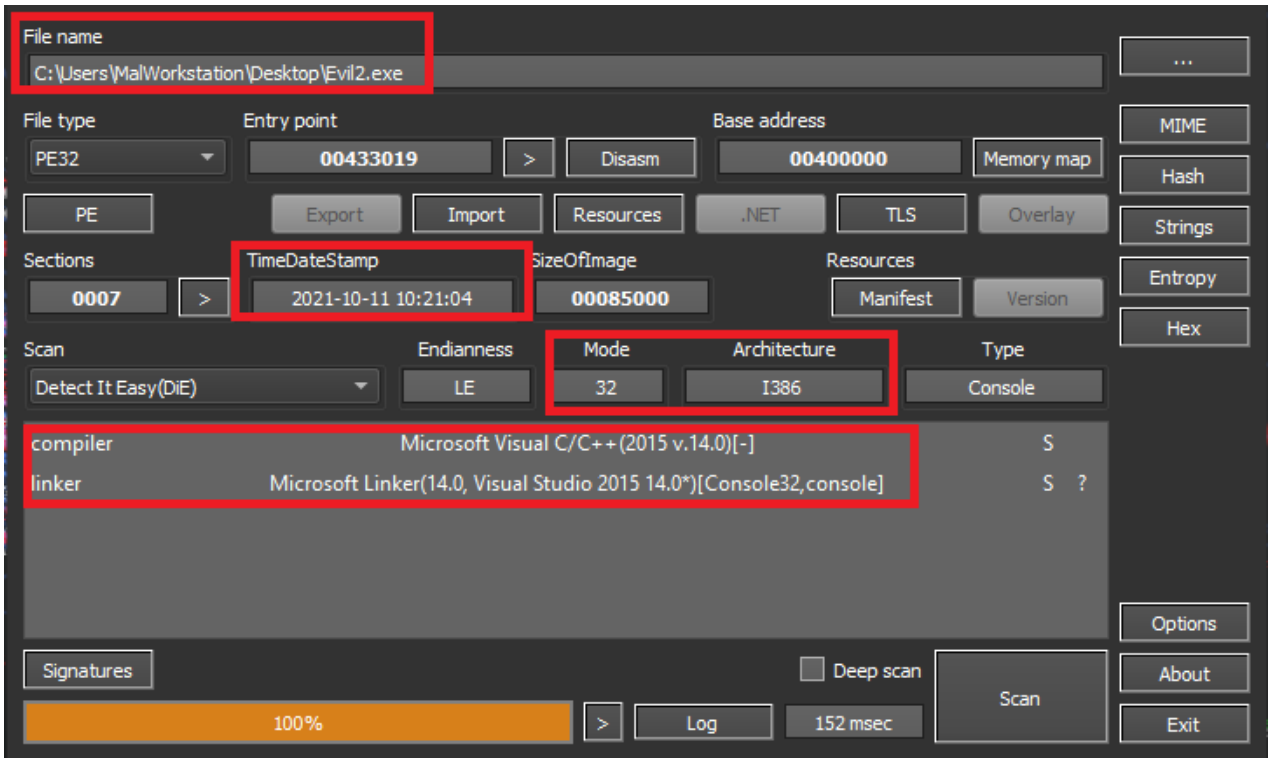


Figure 4 Static Information of Pysa

Upon execution of the ransomware, it creates a process tree, as shown below.

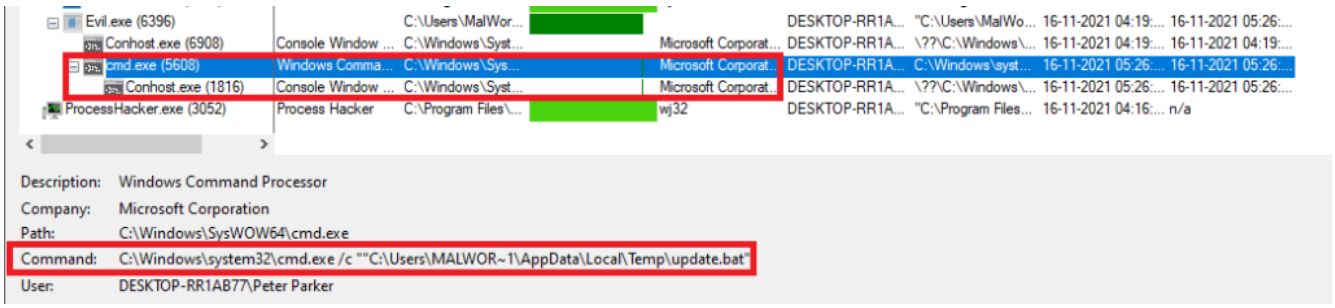


Figure 5 Process Tree

After successful execution, the malware infects the victim's files and appends the extension, '*.pysa'*, as shown below.

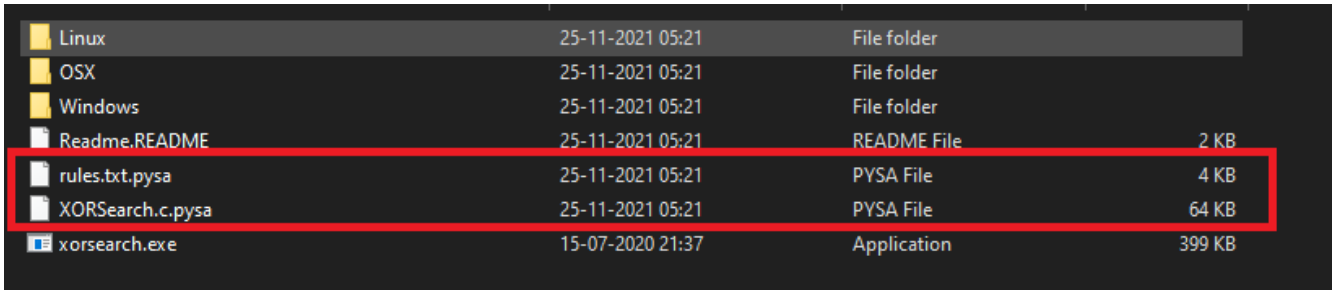


Figure 6 Ransomware appends .pysa extension

The image below showcases the content of the ransom note in which the TA instructs victims to pay the ransom amount. In case the victim fails to pay the demanded ransom, the TA threatens to upload the data on their leake website or sell it to cybercriminals in the darknet.

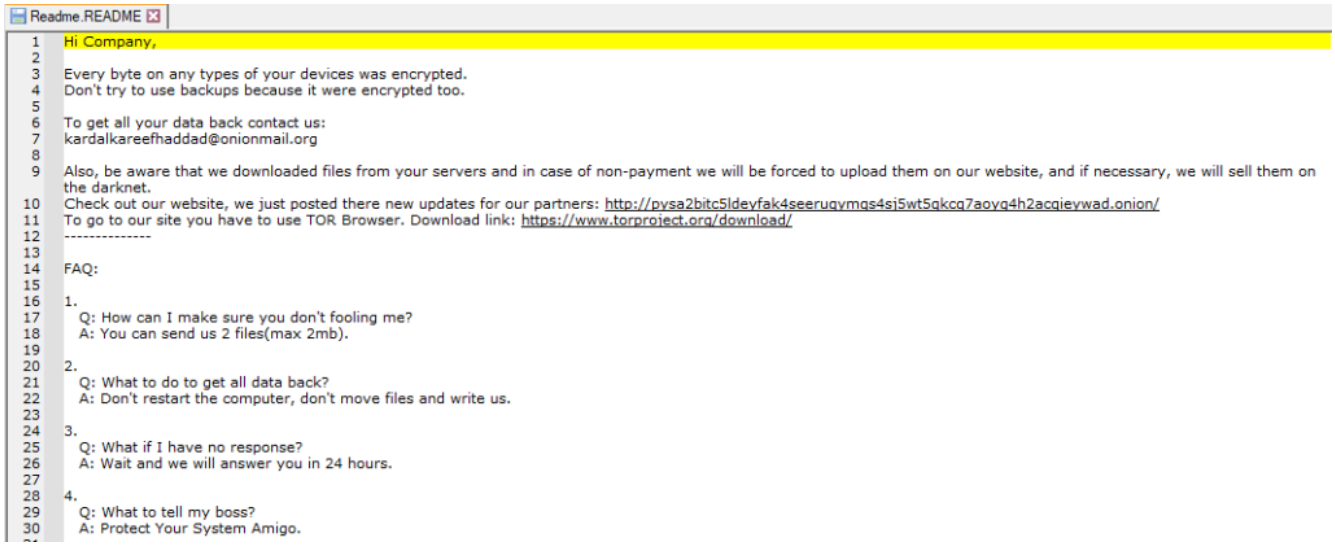


Figure 7 Ransom Note Created by P

Code Analysis

As shown in the below code, the ransomware first creates a mutex with the name "pysa". The mutex has been designed to ensure that only one instance of the ransomware is running in the victim system at a time.

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  HANDLE MutexA; // esi

  FreeConsole();
  if ( !OpenMutexA(0x1F0001u, 0, "Pysa") )
  {
    MutexA = CreateMutexA(0, 0, "Pysa");
    sub_40A234(0);
    sub_40A234(1);
    sub_40A13D();
    ReleaseMutex(MutexA);
    sub_409EF2();
  }
  return 0;
}
```

Figure 8 Code for creating Mutex

Later, the ransomware enumerates the victim's drives using the Application Program Interface (API) *GetLogicalDriveStringsW* and uses the *GetDriveTypeW* API to ensure that the drive is a fixed drive (0x03), such as a hard disk.

```
if ( GetLogicalDriveStringsW(0x104u, v3) )
{
  for ( i = 0; i < 100; i += 4 )
  {
    if ( v3[i] )
    {
      v9[0] = v3[i];
      v9[1] = v3[i + 1];
      v9[2] = v3[i + 2];
      v5 = sub_408A3B(lpRootPathName, (int)v9, (int)v10, (int)&v11);
      LOBYTE(v16) = 2;
      sub_4098FD(&v13, (unsigned int)v5);
      LOBYTE(v16) = 1;
      std::wstring::_Tidy(1, 0);
    }
  }
  for ( j = v13; j != v14; j += 24 )
  {
    std::wstring::wstring(j);
    v7 = (const WCHAR *)lpRootPathName;
    LOBYTE(v16) = 3;
    if ( lpRootPathName[5] >= (LPCWSTR)8 )
      v7 = lpRootPathName[0];
    if ( GetDriveTypeW(v7) == 3 )
      sub_40996A(a1, (int)v3, (unsigned int)lpRootPathName);
    LOBYTE(v16) = 1;
    std::wstring::_Tidy(1, 0);
  }
```

Figure 9 Enumerates Drives and Checks if the Drive is a Fixed drive

Once the list of drives is found, the ransomware creates a Thread using the *CreateThread* API and passes the Drive letter as a parameter for the infection, as shown below.

```
std::wstring::wstring(v4);
LOBYTE(v26) = 1;
ProcessHeap = GetProcessHeap();
v8 = (void **)HeapAlloc(ProcessHeap, 8u, 0x1Cu);
*v2 = v8;
if ( !v8 )
  ExitProcess(2u);
if ( v8 != v22 )
  sub_408E20(v8, v22, 0, 0xFFFFFFFF);
*((_WORD *)*v2 + 12) = a1;
Thread = CreateThread(0, 0, StartAddress, *v2, 0, (LPDWORD)((char *)v2 + v17));
*(LPVOID *)((char *)v2 + v16) = Thread;
if ( !Thread )
  ExitProcess(3u);
LOBYTE(v26) = 0;
```

Figure 10 Creates Thread for Infection

Each directory that is found by the ransomware is compared with the list below, as the ransomware does not infect files present in the directory list shown below.

```
SubStr[0] = L":\\Windows\\";
SubStr[1] = L"\\Boot\\";
SubStr[2] = L"\\BOOTSECT";
SubStr[3] = L"\\pagefile";
SubStr[4] = L"\\System Volume Information\\";
SubStr[5] = L"bootmgr";
SubStr[6] = L"\\Recovery";
SubStr[7] = L"\\Microsoft";
```

Figure 11 Whitelisted Directories

Once the malware has found the files present in the victim machine, the ransomware compares the files extension with the list below.

.doc	.myd	.bkf	.pbf	.zip
.xls	.ndf	.bkup	.qic	.rar
.docx	.sdf	.bup	.sqb	.cad
.xlsx	.trc	.fbk	.tis	.dsd
.pdf	.wrk	.mig	.vbk	.dwg
.db	.001	.spf	.vbm	.pla
.db3	.acr	.vhdx	.vrb	.pln
.frm	.bac	.vfd	.win	
.ib	.bak	.avhdx	.pst	
.mdf	.backupdb	.vmcx	.mdb	
.mwb	.bck	.vmrs	.7z	

Table 1 Targeted File Extension

Once the victim's file extension matches with the above list, the ransomware Call *MoveFileW* API to append the *.pysa* extension as shown in the below figure.

```
004068D3    50          PUSH EAX                    eax:L"C:\\iDefense\\MAP\\DiE\\SDK\\Form1.frm.pysa"
004068D4    56          PUSH ESI                    esi:L"C:\\iDefense\\MAP\\DiE\\SDK\\Form1.frm"
004068D5    E8 43830300 CALL evil2.43EC1D
```

Figure 12 Appends .pysa Extension

As shown in the below code, the ransomware reads the content from the files.

```
if ( !ReadFile(hConsoleHandle, lpBuffer, nNumberOfBytesToRead, &NumberOfCharsRead, 0)
  || (v24 = a3, NumberOfCharsRead > a3) )
{
  LastError = GetLastError();
  if ( LastError == 5 )
  {
    *_errno() = 9;
    *__doserrno() = 5;
    goto LABEL_39;
  }
```

Figure 13

Reads Plain Text Content

Once the plain text content has been read, it encrypts it using Advanced Encryption Standard (AES) 256 and then writes the encrypted content into the file.

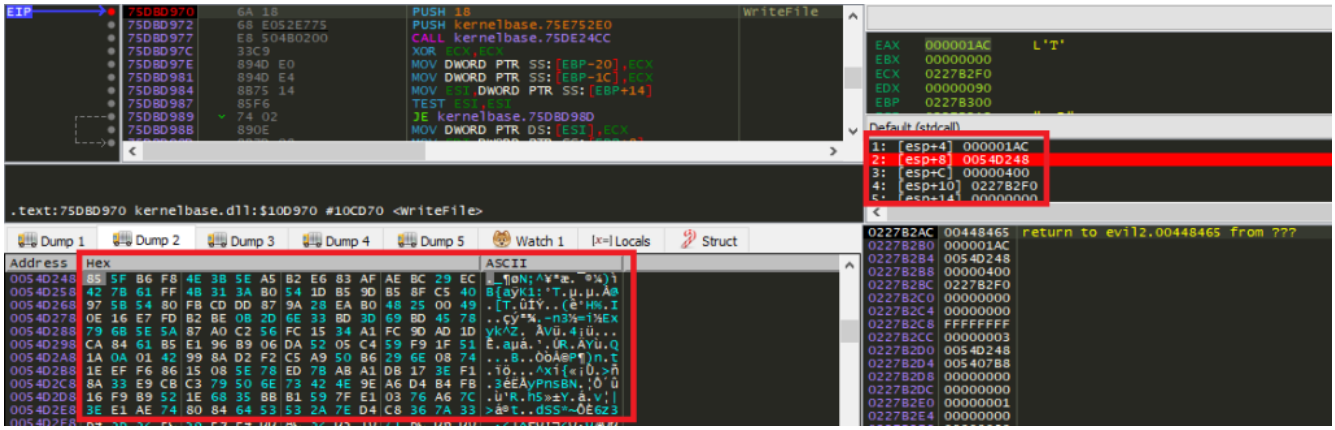


Figure 14 Write Encrypted Content into the File

Once the above process is done, the ransomware creates ransom notes and encrypts the remaining files in the victim machine.

Furthermore, the Pysa ransomware creates two registry keys under *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System*, with the name *legalnoticetext* having value as *Ransom note content* and *legalnoticecaption* having values as *PYSA,* as shown in the below code.

```
LSTATUS sub_40A13D()
{
  HKEY phkResult; // [esp+4h] [ebp-8h] BYREF

  RegOpenKeyExA(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", 0, 2u, &phkResult);
  RegSetValueExA(phkResult, "legalnoticetext", 0, 7u, lpData, strlen((const char *)lpData) + 1);
  RegSetValueExA(phkResult, "legalnoticecaption", 0, 7u, "PYSA", 5u);
  return RegCloseKey(phkResult);
}
```

Figure 15 Create registry entry legalnoticetext and legalnoticecaption

Ransomware created entry *legalnoticetext* and inserted content *ransom note*.

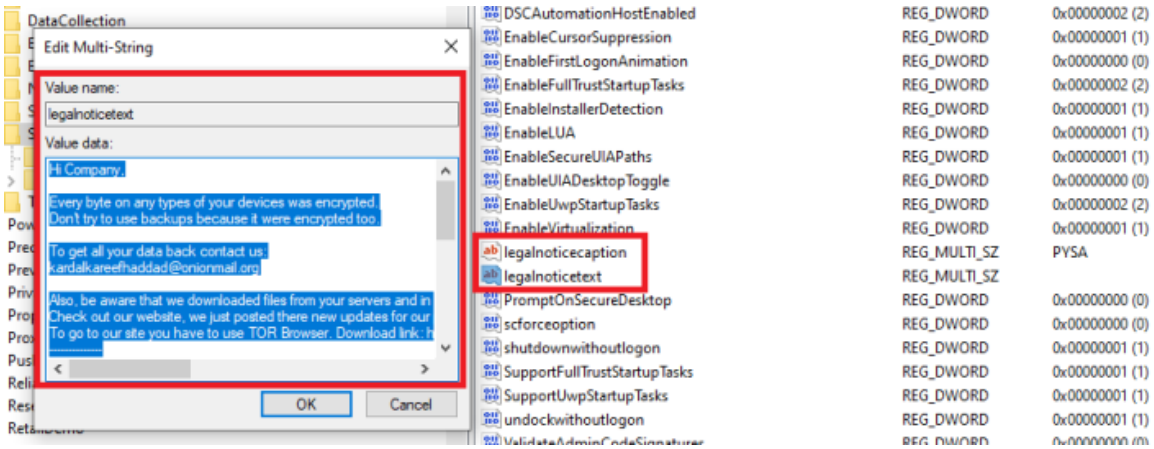


Figure 16 Creates registry legalnoticetext

Another entry is created with the name of *legalnoticetext* and having content *PYSA*.

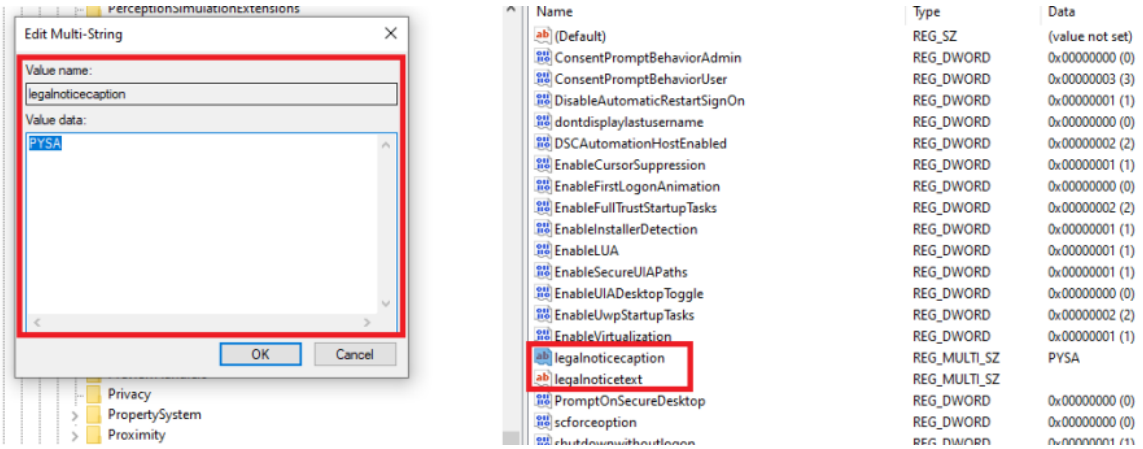


Figure 17 Creates registry legalnoticecaption

Finally, the ransomware releases the mutex and a update.bat file under the Temp folder of the currently logged-in user containing the content below.

```
:Repeat
del “C:\\Users\\MalWorkstation\\Desktop\\Evil2.exe”
if exist “C:\\Users\\MalWorkstation\\Desktop\\Evil2.exe” goto Repeat
rmdir “C:\\Users\\MalWorkstation\\Desktop”
del “C:\\Users\\MALWOR~1\\AppData\\Local\\Temp\\update.bat””
```

Table 2 Content of update.bat

Using the above code, the malware performs the self-Delete operation to delete its traces.

Conclusion

The Pysa ransomware has multiple victims around the world, and the initial execution is manual after the TA exfiltrates the data from the victim’s machine. The Pysa ransomware is one of the many ransomware presented on the surface web that can encrypt user files using a strong encryption algorithm and leave ransom notes for instructing users on how to recover the files.

Cyble Research Labs is continuously monitoring Pysa’s activities, and we keep informing our clients with recent updates about this campaign.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the suggestions given below:

- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Conduct regular backup practices and keep those backups offline or in a separate network.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial access	T1566	Phishing
Execution	T1204	User Execution
Discovery	T1082	System Information Discovery
Defense Evasion	T1112	Modify Registry
Impact	T1490 T1489 T1486	Inhibit System Recovery Service Stop Data Encrypted for Impact

Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
7c774062bc55e2d0e869d5d69820aa6e3b759454dbc926475b4db6f7f2b6cb14	SHA-256	Pysa Ransomware
pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqieywad[.]onion	TOR-URL	TAs Website
kardalkareefhaddad@onionmail.org	Email	TAs Email

Generic signatures and Rules:

Yara Rules:

```
rule win32_pysaransomware
{
meta:
        author= "Cyble Research"
        date= "2021-11-25"
        description= "Coverage for Pysa Ransomware"
        hash= "7c774062bc55e2d0e869d5d69820aa6e3b759454dbc926475b4db6f7f2b6cb14"
        strings:
                $header= "MZ"
                $sig1 = "Readme.README" wide ascii
                $sig2 = "n.pysa" wide ascii
                $sig3 = "pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqieywad.onion" wide ascii
                $sig4 = "kardalkareefhaddad@onionmail.org" wide ascii
                $sig5 = "Every byte on any types of your devices was encrypted." wide ascii
                $sig6 = "To get all your data back contact us" wide ascii
        condition:
                $header at 0 and (4 of ($sig*))
}
```