By Victor Alyusnin, Fedor Sinitsyn on April 8, 2015. 10:00 am

In the middle of last year, my colleagues published a blogpost about a new generation of ransomware programs based on encryptor Trojans, and used the example of the Onion family (also known as CTB-Locker) to analyze how these programs work.

Last autumn, we discovered the first sample of an interesting new encryptor, TorLocker (this is the original name given by the creator); later on, TorLocker was used to launch an attack on Japanese users. When it was discovered on 24 October, 2014, the proactive components in Kaspersky Lab's products already detected this piece of malware; later on, it was assigned the verdict 'Trojan-Ransom.Win32.Scraper'.

> Trojan-Ransom.Win32.Scraper encrypts the victim's documents and demands a ransom ($300 or greater) to decrypt them

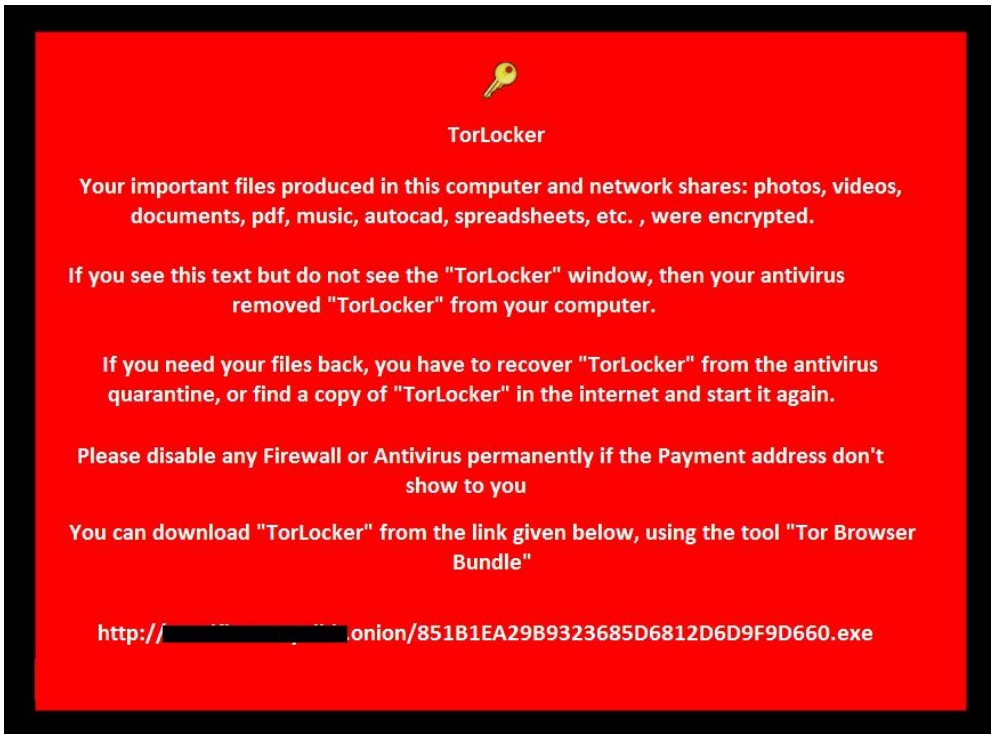
All the TorLocker samples that we have obtained belong to one of two versions: 1.0.1 (in English) or 2.0 (in English and Japanese.) There are only slight differences between them: 1) in the method employed to obfuscate code, and 2) in the sources used for additional modules: in the first version, the additional modules are extracted from the data section, while in the second version, they are downloaded from the Internet (from file hosting services or from compromised sites). Also in the second version, some strings were relocated from the data section into the code section, and dangling (redundant, not used) bytes emerged. The file encryption algorithm is the same in both versions.

Common features and peculiarities of this malware family

Our analysis has shown that Trojan-Ransom.Win32.Scraper was presumably written in assembler, which is unusual for this type of malware. The Trojan uses the Tor network to contact its "owners" – something that is apparently

becoming a norm for the new generation of ransomware – and the proxy server polipo. This piece of malware often lands on users' computers via the Andromeda botnet.

Trojan-Ransom.Win32.Scraper encrypts the victim's documents and demands a ransom ($300 or greater) to decrypt them. If the malware gets deleted by a security product after the files are encrypted, the Trojan installs bright red wallpaper on the Desktop, containing a link to its executable file. Thus, users have a chance to re-install the Trojan and report to its owners that they have paid the ransom: to do so, users need to enter payment details in a dedicated TorLocker window. This data will be sent to the C&C server which will either reply with a private RSA key or notify that there was no payment.



This typical representative of the Scraper family is packed with UPX. The data section is additionally encrypted with AES with a 256-bit key. In the code section, between the assembler instructions, there are a large number of redundant bytes that are not used in any way.

```
.text:0040612D                 push    eax             ; lpOverlapped
.text:0040612E                 push    offset NumberOfBytesRead ; lpNumberOfBytesRead
.text:00406133                 push    1E0h            ; nNumberOfBytesToRead
.text:00406138                 push    offset Sample_id_in_file ; lpBuffer
.text:0040613D                 push    hFile           ; hFile
.text:00406143                 call    ReadFile
.text:00406148                 test    eax, eax
.text:0040614A                 jnz     short loc_406153
.text:0040614C                 sub     esi, esi
.text:0040614E                 jmp     loc_4065CE
.text:00406153 ; ---------------------------------------------------------------------------
.text:00406153
.text:00406153 loc_406153:                             ; CODE XREF: file_crypt+293↑j
.text:00406153                 jmp     short loc_406163
.text:00406153 ; ---------------------------------------------------------------------------
.text:00406155                 db 0D9h, 0D3h, 4Dh, 67h, 49h, 11h, 0A9h, 4Ah, 0A0h, 0ACh, 1Ah, 0D1h, 0B5h, 0E1h
.text:00406163 ; ---------------------------------------------------------------------------
.text:00406163
.text:00406163 loc_406163:                             ; CODE XREF: file_crypt:loc_406153↑j
.text:00406163                 mov     eax, Sample_id
.text:00406168                 jmp     short loc_406175
.text:00406168 ; ---------------------------------------------------------------------------
.text:0040616A                 db 0B6h, 0DFh, 4Ah, 8Dh, 50h, 7Ch, 0ECh, 28h, 2Fh, 41h, 52h
.text:00406175 ; ---------------------------------------------------------------------------
.text:00406175
.text:00406175 loc_406175:                             ; CODE XREF: file_crypt+2B1↑j
.text:00406175                 cmp     eax, Sample_id_in_file
.text:0040617B                 jnz     short loc_406184
.text:0040617D                 sub     esi, esi
.text:0040617F                 jmp     loc_4065CE
.text:00406184 ; ---------------------------------------------------------------------------
.text:00406184
.text:00406184 loc_406184:                             ; CODE XREF: file_crypt+2C4↑j
.text:00406184                 push    hFile           ; hObject
.text:0040618A                 call    CloseHandle
.text:0040618F                 push    esi             ; a6
.text:00406190                 push    80h             ; a5
.text:00406195                 push    3               ; a4
.text:00406197                 push    GENERIC_WRITE or GENERIC_READ ; a3
.text:0040619C                 call    CreateFile
.text:004061A1                 jmp     short loc_4061A5
.text:004061A1 ; ---------------------------------------------------------------------------
.text:004061A3                 db 2Bh, 0FEh
.text:004061A5 ; ---------------------------------------------------------------------------
.text:004061A5
.text:004061A5 loc_4061A5:                             ; CODE XREF: file_crypt+2EA↑j
.text:004061A5                 mov     hFile, eax
.text:004061AA                 inc     eax
```

The redundant bytes in the encryptor's body

The method of submitting string arguments to functions is just as unusual. The strings are located directly in the code section; in order to submit a string as an argument to a function, the pointer to that string is placed into the stack by way of calling (using the '**call**' instruction) the instruction following the string. As a result, the return address (which is identical to the pointer to the string) is placed into the stack:

```
.text:00401121
.text:00401121 loc_401121:                             ; CODE XREF: .text:0040102D↑j
.text:00401121                 call    loc_401144
.text:00401121 ; ---------------------------------------------------------------------------
.text:00401126 aHttpWhatismyip db 'http://whatismyipaddress.com/',0
.text:00401144 ; ---------------------------------------------------------------------------
.text:00401144
.text:00401144 loc_401144:                             ; CODE XREF: .text:loc_401121↑p
.text:00401144                 call    file_get_contents
.text:00401149                 test    eax, eax
.text:0040114B                 jnz     short loc_401154
.text:0040114D                 sub     esi, esi
.text:0040114F                 jmp     loc_4011FE
```

Handling string constants as arguments to functions

Operating principles

Once launched, the Trojan starts by decrypting its data section with a 256-bit AES key. The first 4 bytes of this key are used as a sample ID, added to the end of the encrypted files. Then the Trojan is copied to a temporary

folder, and a registry key for that copy's autorun is created in the following registry section:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
```

Next the Trojan creates several threads to do the following:

- Search for and terminate the taskmgr.exe, regedit.exe, procexp.exe, procexp64.exe processes.
- Delete all system recovery points.
- Encrypt the user's office documents, video and audio files, images, archives, databases, backup copies, virtual machines encryption keys, certificates and other files on all hard and network drives, except files located in the folders %windir%, %temp%. The names and extensions of encrypted files remain unchanged.
  Here is the complete list of file extensions that are encrypted:
  .3gp .7z .accdb .ai .aiff .arw .avi .backup .bay .bin .blend .cdr .cer .cr2 .crt .crw .dat .dbf .dcr .der .dit .dng .doc .docm .docx .dwg .dxf .dxg .edb .eps .erf .flac .gif .hdd .indd .jpe .jpg .jpeg .kdc .kwm .log .m2ts .m4p .mdb .mdf .mef .mkv .mov .mp3 .mp4 .mpg .mpeg .mrw .ndf .nef .nrw .nvram .odb .odm .odp .ods .odt .ogg .orf .p12 .p7b .p7c .pdd .pdf .pef .pem .pfx .pif .png .ppt .pptm .pptx .psd .pst .ptx .pwm .qcow .qcow2 .qed .r3d .raf .rar .raw .rtf .rvt .rw2 .rwl .sav .sql .srf .srw .stm .txt .vbox .vdi .vhd .vhdx .vmdk .vmsd .vmx .vmxf .vob .wav .wb2 .wma .wmv .wpd .wps .xlk .xls .xlsb .xlsm .xlsx .zip
- Extract a BMP image, save it to a temporary folder and then set it as desktop wallpaper:
- Download tor.exe and polipo.exe, the files required to communicate with C&C servers, from the links specified in the Trojan's configuration (in the case of TorLocker 2.0) or extract them from the data section (in case of TorLocker 1.0). Then tor.exe is launched with the following arguments:

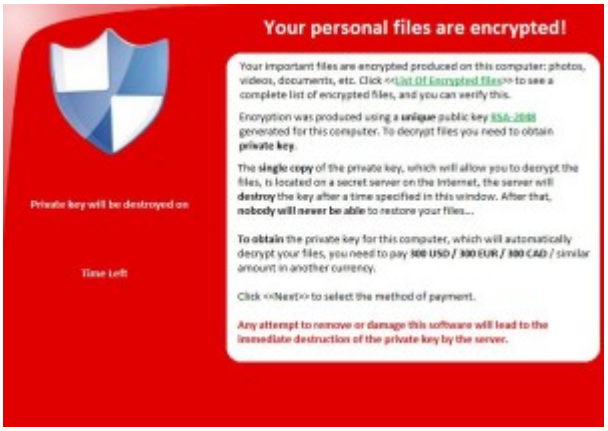
  ```
  tor.exe -SOCKSPort 9150 -AvoidDiskWrites 1 -ExcludeSingleHopRelays 0 -FascistFirewall 1 -DirReqStatistics 0
  ```

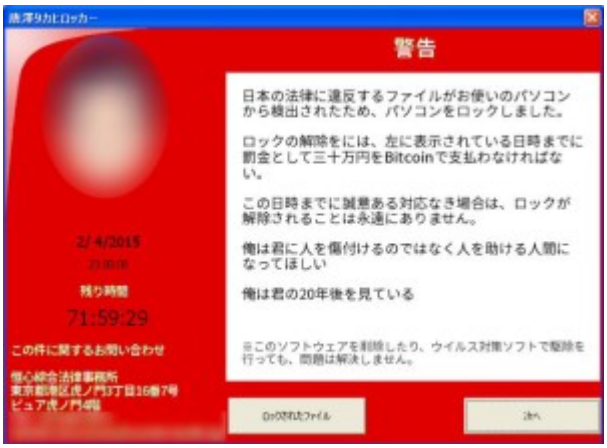
  polipo.exe is launched in the following configuration:

  ```
  127.0.0.1:57223 proxyPort = 57223 socksParentProxy = 127.0.0.1:9150 socksProxyType = socks5
  ```

- Create a GUI window demanding that the victim pays the creators of Trojan-Ransom.Win32.Scraper and display the window in the top left

corner of the screen. It supports payment via BitCoin, UKash and PaySafeCard.





To encourage the user to pay the ransom to the Trojan's owners faster, the Trojan threatens to delete the private key required to decrypt the files if the user fails to send the money within a certain time period. In reality, the RSA keys are not deleted. They are associated with the malware sample rather than with a specific user, so the same RSA key is used for several users at the same time.

- The IP address of the victim computer is determined using www.iplocation.net, www.seuip.com.br, whatismyipaddress.com, or checkip.dyndns.org.
- Establish a connection to the C&C server in the onion domain via the proxy server polipo 127.0.0.1:57223. If the victim user has paid the ransom to the extorters, then, after contacting the C&C server and sending the information about the client (the selected RSA key, the number of encrypted files, the client's IP address and ID, the selected method of payment and the number of the bank card), the Trojan then receives the private RSA key with which to decrypt the files – in this case, a file decryption thread is created. Otherwise, a message is sent that the payment has not been effected yet. In each sample of Trojan-

Ransom.Win32.Scraper?, a few dozens C&C domain names are hardcoded; they are not updated and may lead to the same C&C server.

Encryption

When launching, Trojan-Ransom.Win32.Scraper chooses one of the 128 public RSA keys hardcoded in it, depending on the victim computer's name and the serial number of the logical drive. The number (n) of the public RSA key is calculated as following:

> **n = (VolumeSerialNumber * strlen(ComputerName)) mod 128,** where **strlen(ComputerName)** is the length of the computer's name, and **VolumeSerialNumber** is the serial number of the logical drive on which Winsow is installed.

Each sample contains its own set of public keys.

The user's files are encrypted with AES-256 with a randomly generated one-time key; an individual encryption key is created for each file. Then, a 512-byte service section is added to the end of each file, which consists of 32 bytes of padding, 4 bytes of the Trojan's identifier, and 476 bytes of the employed AES key encrypted with RSA-2048.

If the file size is greater than 512 MB + 1 byte, then of the first 512 MB of the file get encrypted. The encrypted data is written on top of the original, non-encrypted data; no new file is created, and the old file is not deleted.

The Structure of an encrypted file

The Trojan does not need Internet access to encrypt the files.

Packing

In order to obstruct the analysis, some of the detected samples of Trojan-Ransom.Win32.Scraper were additionally packed with the KazyLoader and KazyRootkit protectors along with UPX.

KazyLoader is a two-stage protector of executable files, written in .NET Framework. The protected executable is encrypted with AES, and then placed into the protector's assets section as a color palette of a BMP image.

The image decryption module is encrypted by XORing with one byte, then divided into parts and also placed into the protector assets section in the form of strings LOADER0, LOADER1, ... LOADER272.

The KazyRootkit protector is also written in .NET Framework and has a feature that can conceal processes in the Task Manager (taskmgr.exe) and conceal registry keys in the Registry Editor (regedit.exe) by deleting strings from ListView GUI elements with the help of WinAPI. Depending on its configuration, the protector may shut down without unpacking the file embedded in it, if it detects any of Sandboxie, Wireshark, WPE PRO or a code emulator.

> Although Scraper (TorLocker) encrypts all files with AES-256 + RSA-2048, in 70%+ cases they can be decrypted

The file to be protected is encrypted by XORing with a certain key, and then injected into the protector's process. A large array of random bytes is stored in the protector's overlay.

Partnership program

Trojan-Ransom.Win32.Scraper's builder (i.e. the program with which to create new samples of the Trojan with specified configuration) is distributed via a partnership program and sold for a few bitcoins. We found two posts about selling the builder for TorLocker 2.0 in the 'Evolution' (now taken down) underground online store:

The published screenshot of the builder suggests that the cybercriminal can change some of the encryptor's settings, as follows:

- Allow or block the launch of Task Manager or Process Explorer after infection;
- Allow or block the use of payment systems like BitCoin, PaySafeCard and Ukash to pay the ransom;
- Allow or block the removal of Windows recovery points;

- Modify the links from which to download tor.exe and polipo.exe; modify the names of these files after they are downloaded.

A screenshot of the builder's window

On the underground e-store's website, there are 11 reviews of the vendor of the Trojan-Ransom.Win32.Scraper builder, posted between 8 May 2014 and 17 January 2015.

By way of advertisement, news links are published about successful attacks performed using Trojan-Ransom.Win32.Scraper.

A brief description of TorLocker's operating principles and a comparison with CryptoLocker is also provided.

Decryption

At the decryption stage, when the ransom payment is received, Trojan-Ransom.Win32.Scraper contacts the cybercriminals' C&C servers via the Tor network and the polipo proxy server, to receive a private RSA key. With this key, the Trojan decrypts the AES key for each encrypted file, and then decrypts the files.

Although Trojan-Ransom.Win32.Scraper encrypts all files with AES-256 + RSA-2048, in 70%+ cases they can be decrypted because of the errors made during the implementation of cryptography algorithms. To restore the original files, Kaspersky Lab has developed the ScraperDecryptor utility, which can be downloaded from Kaspersky Lab's technical support website.

FINANCIAL MALWARE MALWARE TECHNOLOGIES RANSOMWARE TOR TROJAN

Share post on:

Related Posts

IT threat evolution Q3

IT threat evolution Q3

IT threat evolution Q3

2020. Non-mobile statistics

2020 Mobile statistics

2020

THERE IS 1 COMMENT

mr x

Posted on April 14, 2015. 12:04 am

so would just the fact of having sandboxie installed be enough to protect from this (as it norm runs as a service in the taskbar) as in normal world sandboxie would be extremely rare to be on a system (but it would be if you was playing around on unsafe sites)

REPLY