Russia hit by new wave of ransomware spam

welivesecurity.com/2019/01/28/russia-hit-new-wave-ransomware-spam/

January 28, 2019

Among the increased number of malicious JavaScript email attachments observed in January 2019, ESET researchers have spotted a large wave of ransomware-spreading spam targeting Russian users

Juraj Jánošík

28 Jan 2019 - 02:57PM

Among the increased number of malicious JavaScript email attachments observed in January 2019, ESET researchers have spotted a large wave of ransomware-spreading spam targeting Russian users

January 2019 has seen a dramatic uptick in detections of malicious JavaScript email attachments, an attack vector that mostly lay dormant throughout 2018. Among the “New Year edition” of malicious spam campaigns relying on this vector, we have detected a new wave of Russian-language spam that distributes ransomware known as Shade or Troldesh, and detected by ESET as Win32/Filecoder.Shade.

The campaign appears to be a follow-up to a malicious spam campaign that started distributing the Shade ransomware in October 2018.

The January 2019 campaign

Our telemetry shows the October 2018 campaign running at a consistent pace until the second half of December 2018, taking a break around Christmas, and then resuming in mid-January 2019 doubled in size, as seen in Figure 1. The drops in the graph are aligned with weekends, which suggests that the attackers favor company email addresses.

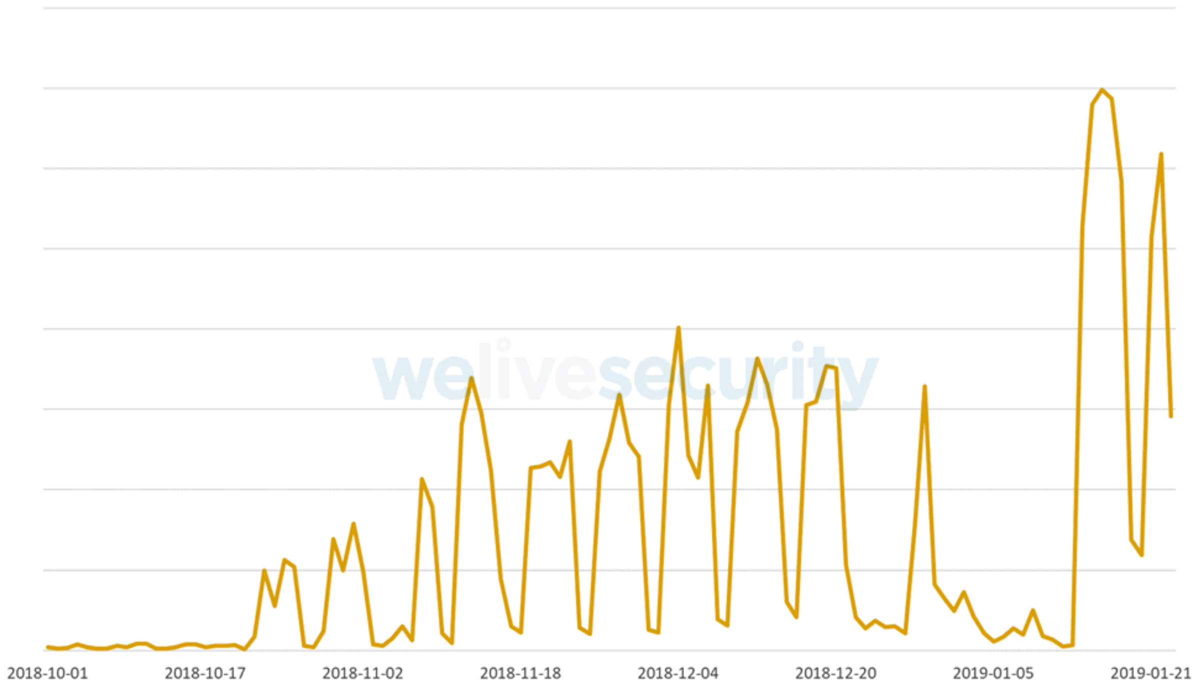


Figure 1 – Detections of malicious JavaScript attachments spreading Win32/Filecoder.Shade since October 2018

As previously mentioned, this campaign is a part of a larger trend we have observed from the beginning of 2019 – the comeback of malicious JavaScript attachments as a widely used attack vector. Figure 2 shows this development as seen in our telemetry.

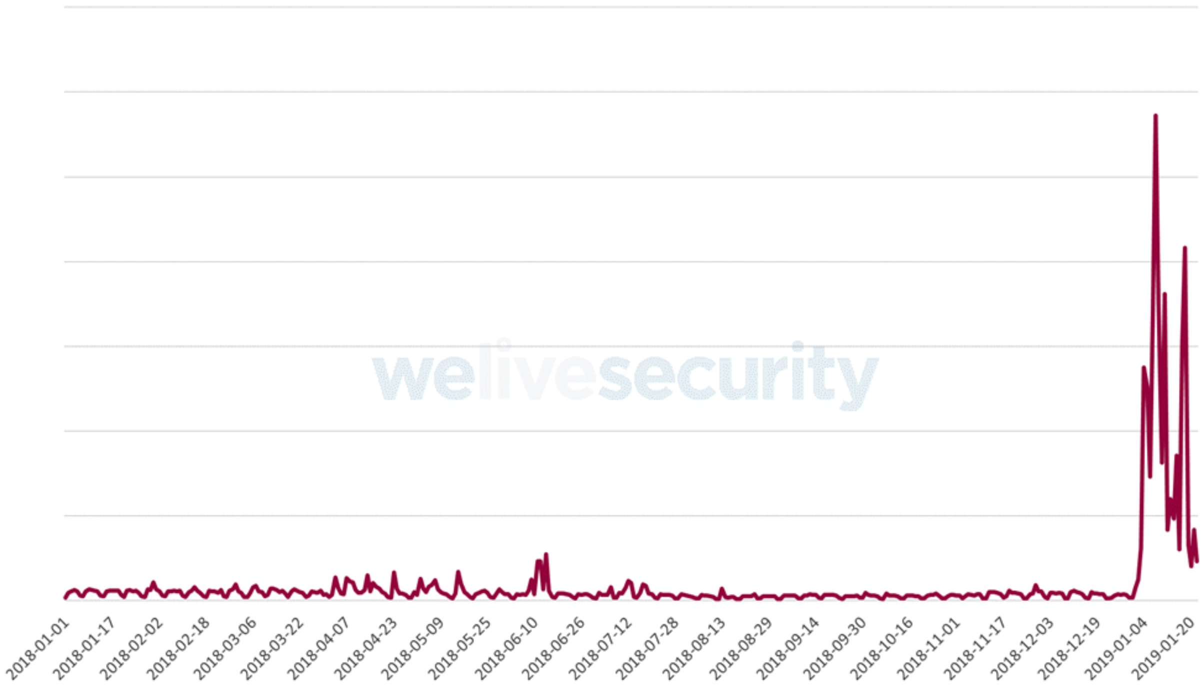


Figure 2 – Detections of malicious JavaScript distributed via email attachments, all of which are detected as JS/Danger.ScriptAttachment, in the last year

Of particular note, the campaign spreading the Shade ransomware in January 2019 has been most active in Russia, with 52% of the total detections of these malicious JavaScript attachments. Among other affected countries are Ukraine, France, Germany, and Japan, as seen in Figure 3.

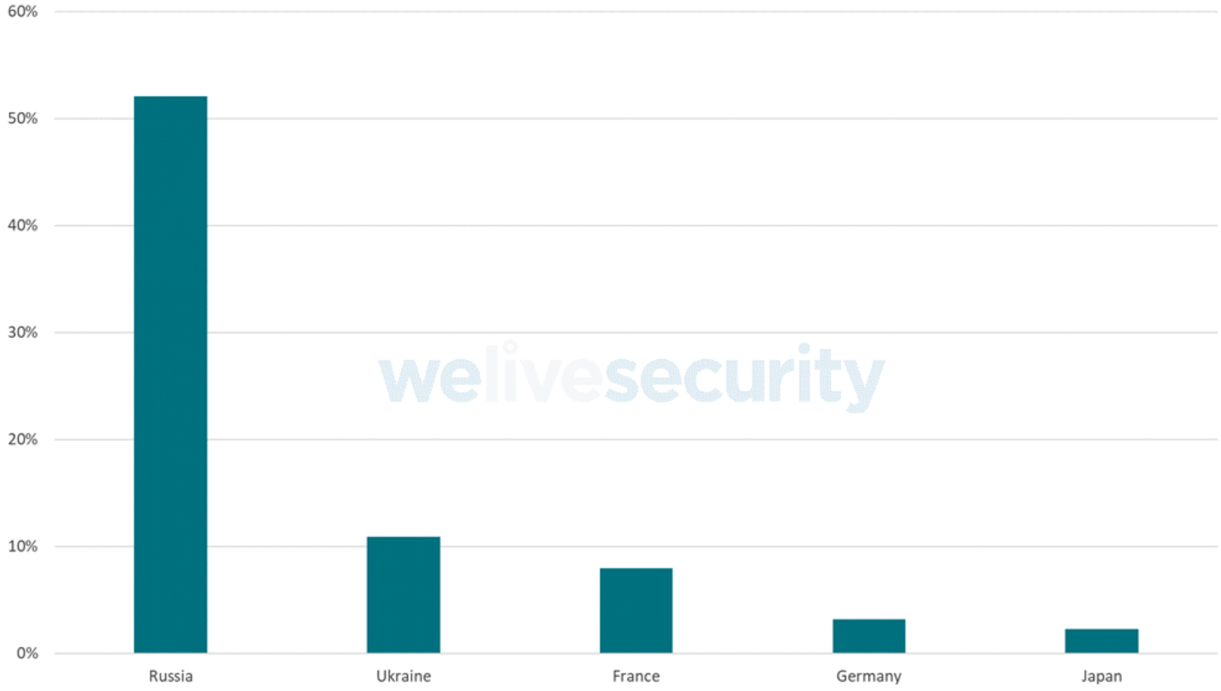


Figure 3 – Distribution of ESET detections of malicious JavaScript attachments spreading Win32/Filecoder.Shade between January 1, 2019 and January 24, 2019

Based on our analysis, a typical attack in the January 2019 campaign starts with the delivery of an email written in Russian, with an attached ZIP archive named “info.zip” or “inf.zip”.

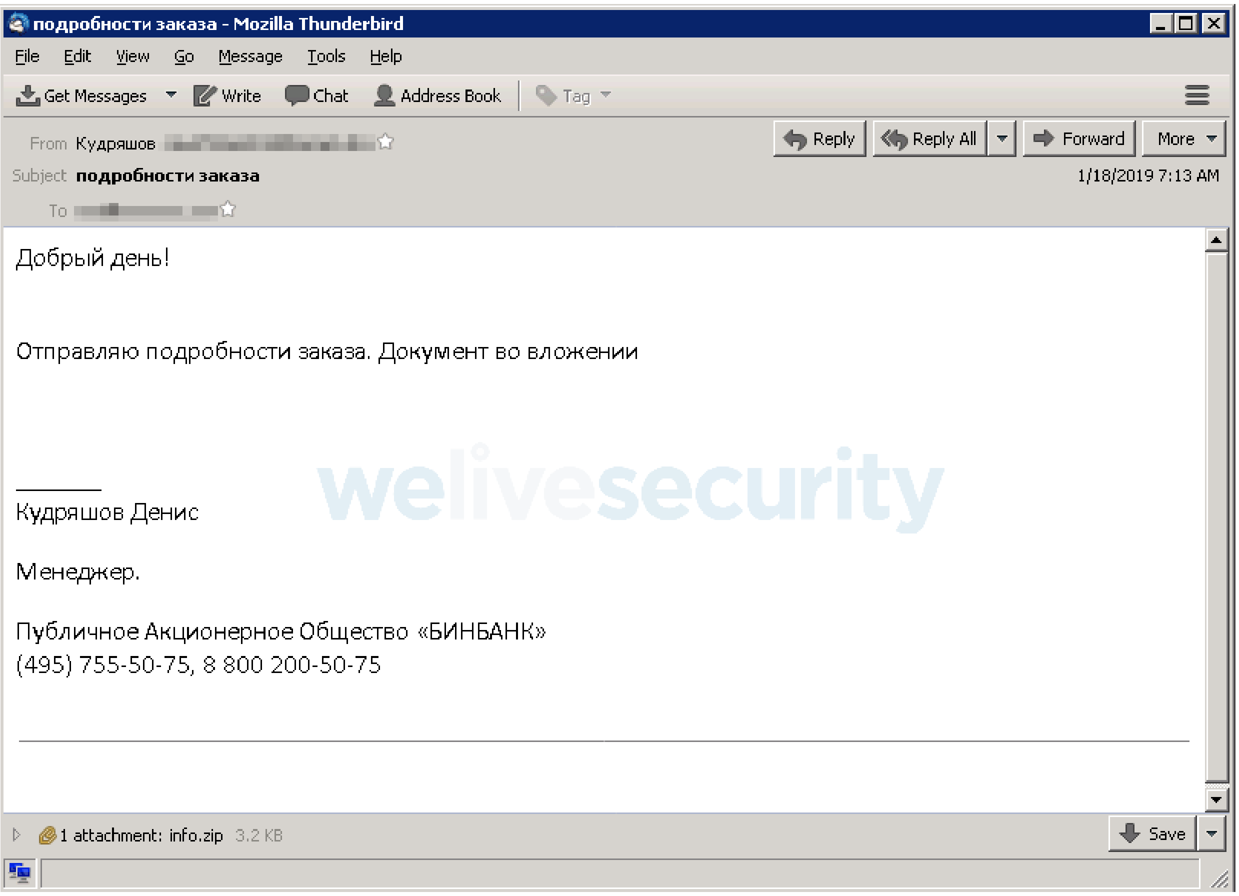
These malicious emails pose as order updates, seemingly coming from legitimate Russian organizations. The emails we have seen impersonate the Russian bank B&N Bank (note: recently merged with Otkritie Bank), and the retail chain Magnit. In one of the emails detected by ESET systems, the English translation is:

Subject: Details of the order

Hello!

I’m sending to you the details of the order. The document is enclosed.

Denis Kudrashev, manager



From Кудряшов [redacted]
Subject **подробности заказа**
To [redacted]
1/18/2019 7:13 AM

Добрый день!

Отправляю подробности заказа. Документ во вложении

____

Кудряшов Денис

Менеджер.

Публичное Акционерное Общество «БИНБАНК»
(495) 755-50-75, 8 800 200-50-75

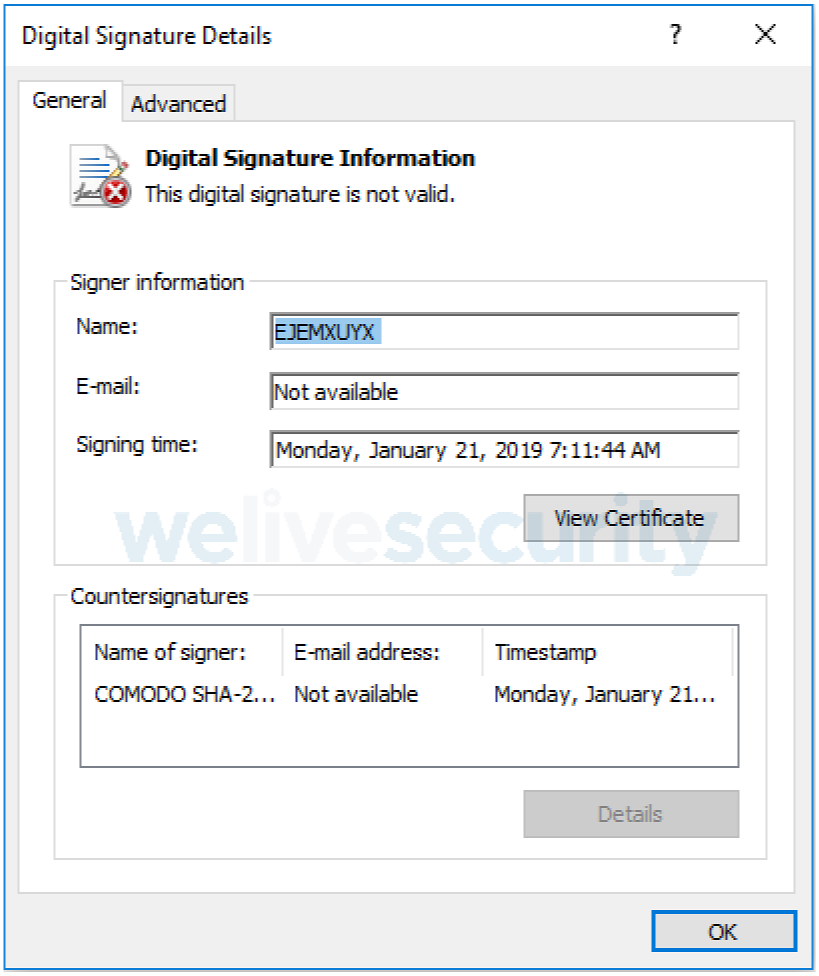
1 attachment: info.zip 3.2 KB

Figure 4 – Example of a spam email used in the January 2019 campaign

The ZIP archive contains a JavaScript file named “Информация.js“ (which translates to “Information” in English). Once extracted and launched, the JavaScript file downloads a malicious loader, detected by ESET products as Win32/Injector. The malicious loader decrypts and launches the final payload – the Shade ransomware.

The malicious loader is downloaded from URLs at compromised, legitimate WordPress sites, where it is disguised as an image file. To compromise the WordPress pages, attackers used mass-scale password brute-force attacks carried out via automated bots. Our telemetry data shows hundreds of such URLs, all ending with the string “ssj.jpg”, hosting the malicious loader file.

The loader is signed using an invalid digital signature that claims to be issued by Comodo, as seen in Figure 5. The name in “Signer information” and the timestamp are unique for each sample.



Digital Signature Information

This digital signature is not valid.

Signer information

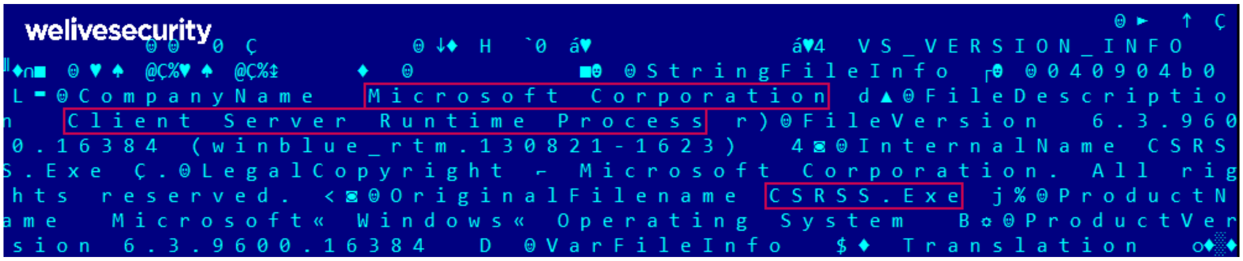
Name:	EJEMXUYX
E-mail:	Not available
Signing time:	Monday, January 21, 2019 7:11:44 AM

Countersignatures

Name of signer:	E-mail address:	Timestamp
COMODO SHA-2...	Not available	Monday, January 21...

Figure 5 – Fake digital signature used by the malicious loader

Besides this, the loader attempts to disguise itself further by posing as the legitimate system process Client Server Runtime Process (csrss.exe). It copies itself into C:\ProgramData\Windows\csrss.exe, where “Windows” is a hidden folder created by the malware, and is not normally located in ProgramData.



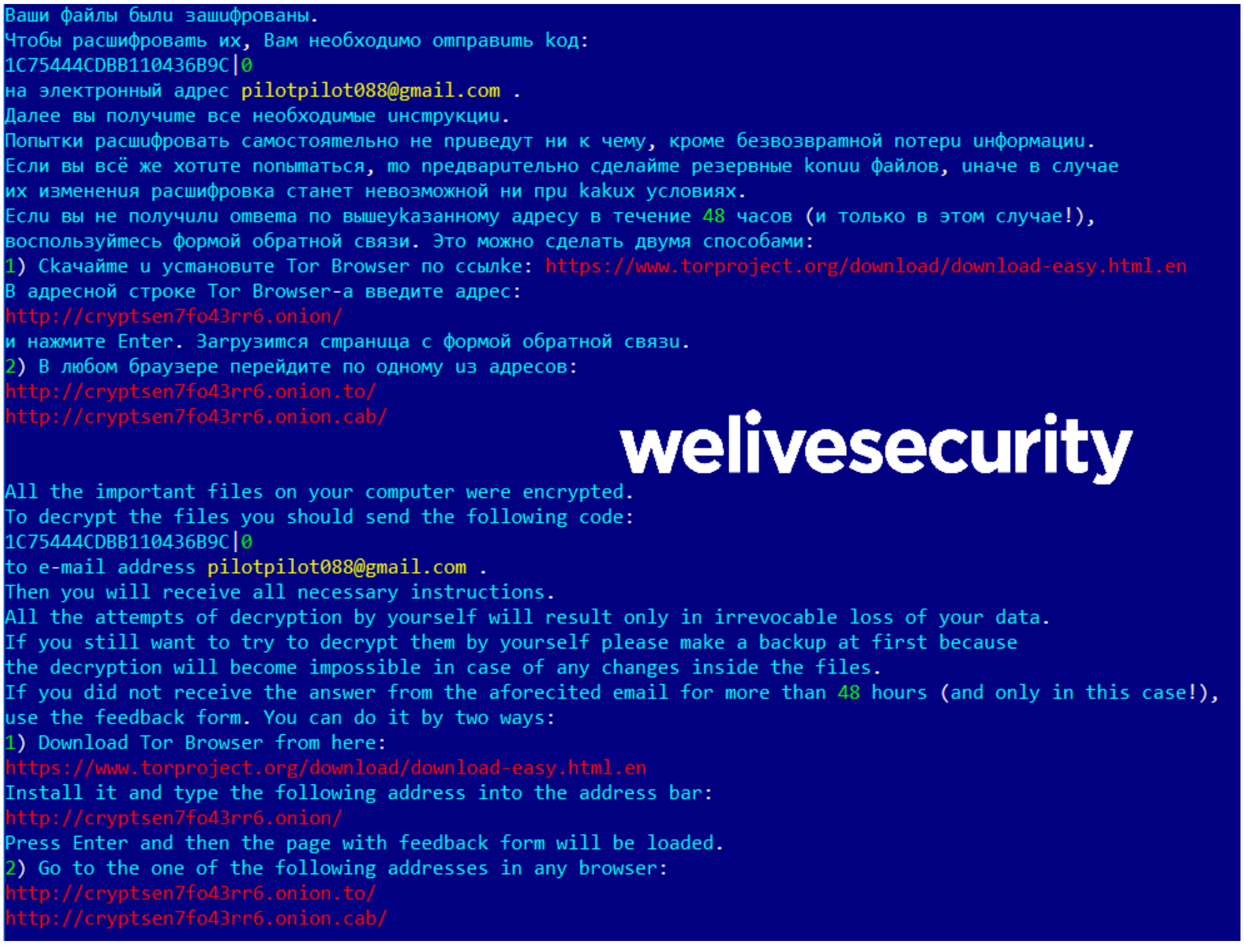
```
                                                                          ☻►  ↑ Ç
welivesecurity☻☻ 0 Ç        ☻↓♦ H  `0 á♥          á♥4  VS_VERSION_INFO
♦n■ ☻♥♠ @Ç%♥♠ @Ç%‡    ♦  ☻         ■☻ ☻StringFileInfo  ┌☻ ☻040904b0
L▬☻CompanyName   Microsoft Corporation   d▲☻FileDescriptio
n  Client Server Runtime Process   r)☻FileVersion   6.3.960
0.16384 (winblue_rtm.130821-1623)   4◙☻InternalName CSRS
S.Exe Ç.☻LegalCopyright ← Microsoft Corporation. All rig
hts reserved. <◙☻OriginalFilename CSRSS.Exe  j%☻ProductN
ame  Microsoft« Windows« Operating System   B☼☻ProductVer
sion 6.3.9600.16384   D ☻VarFileInfo   $♦ Translation  o♦▒♦
```

Figure 6 – The malware posing as a system process and using version details copied from a legitimate Windows Server 2012 R2 binary

The Shade ransomware

The final payload of this malicious campaign is crypto-ransomware dubbed Shade or Troldesh. First seen in the wild in late 2014, but frequently resurfacing since, the ransomware encrypts a wide range of file types on local drives. In the recent campaign, the ransomware appends the extension .crypted000007 to the encrypted files.

The payment instructions are presented to victims in a TXT file, in Russian and English, which is dropped to all drives on the affected computer. The wording of the ransom note is identical to that from the previously-reported October 2018 campaign.



```
Ваши файлы были зашифрованы.
Чтобы расшифровать их, Вам необходимо отправить код:
1C75444CDBB110436B9C|0
на электронный адрес pilotpilot088@gmail.com .
Далее вы получите все необходимые инструкции.
Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.
Если вы всё же хотите попытаться, то предварительно сделайте резервные копии файлов, иначе в случае
их изменения расшифровка станет невозможной ни при каких условиях.
Если вы не получили ответа по вышеуказанному адресу в течение 48 часов (и только в этом случае!),
воспользуйтесь формой обратной связи. Это можно сделать двумя способами:
1) Скачайте и установите Tor Browser по ссылке: https://www.torproject.org/download/download-easy.html.en
В адресной строке Tor Browser-а введите адрес:
http://cryptsen7fo43rr6.onion/
и нажмите Enter. Загрузится страница с формой обратной связи.
2) В любом браузере перейдите по одному из адресов:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/


All the important files on your computer were encrypted.
To decrypt the files you should send the following code:
1C75444CDBB110436B9C|0
to e-mail address pilotpilot088@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.
If you still want to try to decrypt them by yourself please make a backup at first because
the decryption will become impossible in case of any changes inside the files.
If you did not receive the answer from the aforecited email for more than 48 hours (and only in this case!),
use the feedback form. You can do it by two ways:
1) Download Tor Browser from here:
https://www.torproject.org/download/download-easy.html.en
Install it and type the following address into the address bar:
http://cryptsen7fo43rr6.onion/
Press Enter and then the page with feedback form will be loaded.
2) Go to the one of the following addresses in any browser:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/
```

Figure 7 – The Shade ransomware ransom note from January 2019

How to stay safe

To avoid falling victim to malicious spam, always verify the authenticity of emails before opening any attachments or clicking on links. If necessary, check with the organization seemingly sending the email using contact details provided on their official website.

For Gmail users, it may be useful to know that Gmail has been blocking JavaScript attachments in both received and sent emails for almost two years now.

Users of other email services, including company mail servers, must rely on their awareness – unless they use some security solution capable of detecting and blocking malicious JavaScript files.

Several different modules in ESET security products independently detect and block malicious JavaScript files.

To avoid having your WordPress website compromised, use a strong password and two-factor authentication and make sure to regularly update WordPress itself, as well as WordPress plugins and themes.

Indicators of Compromise (IoCs)

Example hashes of the malicious ZIP attachments

0A76B1761EFB5AE9B70AF7850EFB77C740C26F82
D072C6C25FEDB2DDF5582FA705255834D9BC9955
80FDB89B5293C4426AD4D6C32CDC7E5AE32E969A
5DD83A36DDA8C12AE77F8F65A1BEA804A1DF8E8B
6EA6A1F6CA1B0573C139239C41B8820AED24F6AC
43FD3999FB78C1C3ED9DE4BD41BCF206B74D2C76

Example hashes of JavaScript downloaders

37A70B19934A71DC3E44201A451C89E8FF485009
08C8649E0B7ED2F393A3A9E3ECED89581E0F9C9E
E6A7DAF3B1348AB376A6840FF12F36A137D74202

ESET detection name: Win32/Injector

1F1D2EEC68BBEC77AFAE4631419E900C30E09C2F

CC4BD14B5C6085CFF623A6244E0CAEE2F0EBAF8C

ESET detection name: Win32/Injector

Example hashes of the Shade ransomware

FEB458152108F81B3525B9AED2F6EB0F22AF0866

7AB40CD49B54427C607327FFF7AD879F926F685F

441CFA1600E771AA8A78482963EBF278C297F81A

9023B108989B61223C9DC23A8FB1EF7CD82EA66B

D8418DF846E93DA657312ACD64A671887E8D0FA7

ESET detection name: Win32/Filecoder.Shade

Campaign-specific string in URLs hosting the Shade ransomware

hxxp://[redacted]/ssj.jpg

28 Jan 2019 - 02:57PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion