Shade Ransomware Hits High-Tech, Wholesale, Education Sectors in U.S, Japan, India, Thailand, Canada

unit42.paloaltonetworks.com/shade-ransomware-hits-high-tech-wholesale-education-sectors-in-u-s-japan-india-thailand-canada/

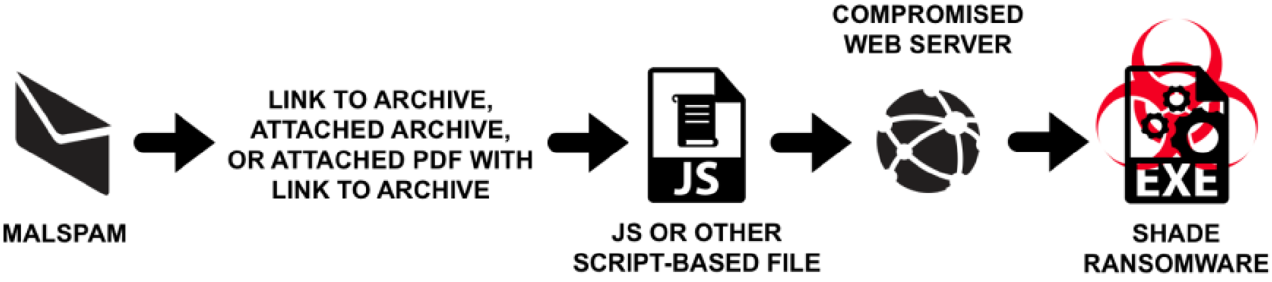
Brad Duncan May 22, 2019

By Brad Duncan

May 22, 2019 at 9:00 AM

Category: Ransomware, Unit 42

Tags: Malspam, Shade Ransomware


MALSPAM
LINK TO ARCHIVE, ATTACHED ARCHIVE, OR ATTACHED PDF WITH LINK TO ARCHIVE
JS
JS OR OTHER SCRIPT-BASED FILE
COMPROMISED WEB SERVER
EXE
SHADE RANSOMWARE

This post is also available in: 日本語 (Japanese)

Shade ransomware is a long-established family of ransomware first spotted in late 2014 targeting hosts running Microsoft Windows. It is also known as Troldesh. Shade has been distributed through malicious spam (malspam) and exploit kits. A recent report focused on Russian language emails that deliver Shade, but this ransomware is also distributed through English-language malspam.

Where is Shade currently appearing? To answer this question, we reviewed recent trends in Shade ransomware among our customer base. Our results indicate the majority of recent Shade ransomware executables have also targeted users outside of Russia.

In fact, our research shows that the top five countries affected by Shade ransomware are not Russia or nations of the former Soviet Union, they are the United States, Japan, India, Thailand, and Canada, Russia only occurs at number seven and the only other country we found in the top ten where Russian is an official language is Kazakhstan at number ten. The top industries attacked in these countries were High-Tech, Wholesale, and Education.

Very Little Change Since 2016

The Shade ransomware executable (EXE) has been remarkably consistent. All EXE samples we have analyzed since 2016 use the same Tor address at ***cryptsen7f043rr6.onion*** as a decryptor page. The desktop background that appears during an infection has been the same since Shade was first reported as Troldesh in late 2014.

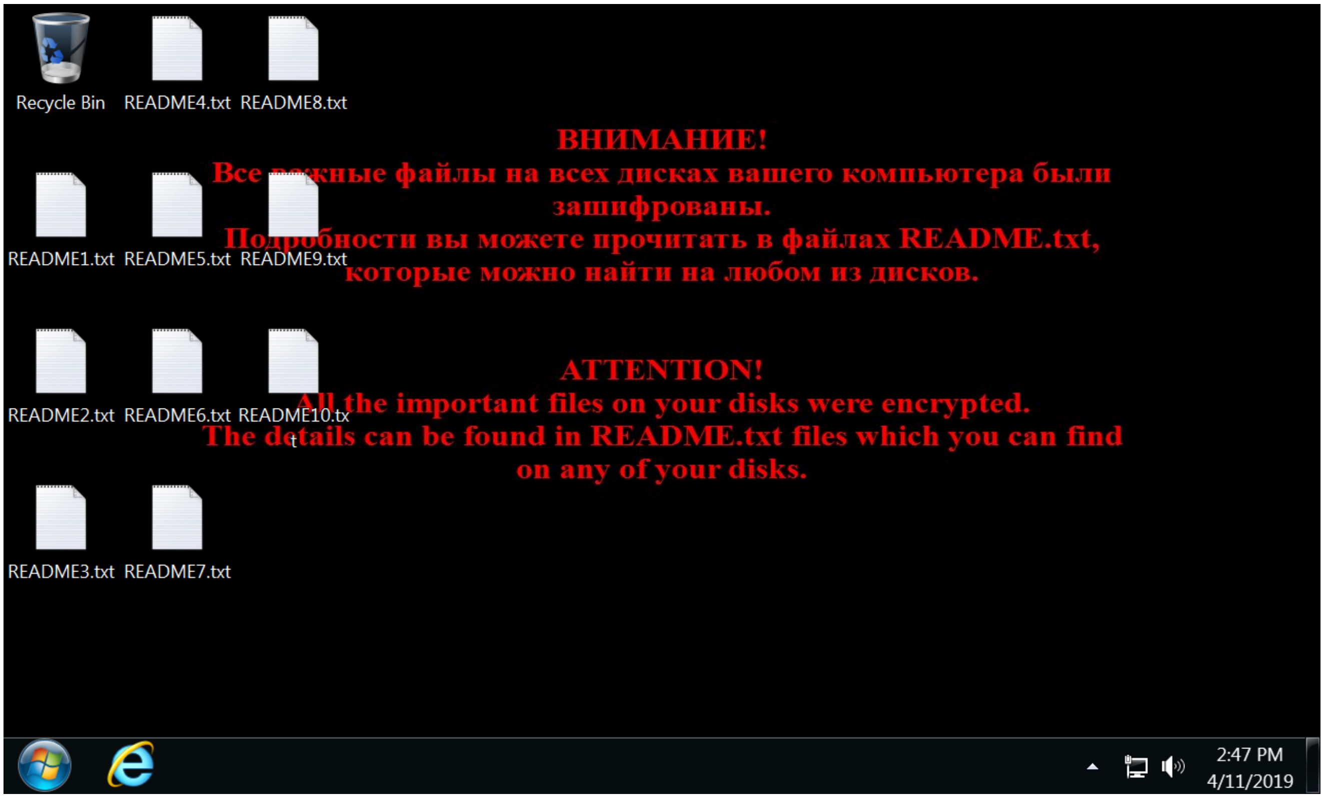
Shade ransomware infections may include other activity like click fraud traffic as noted here.

Russian and English Language Distribution

Recent reports of malspam pushing Shade ransomware have focused on distribution through Russian language emails. However, Shade decryption instructions have always included English as well as Russian text. English language waves of malspam have been noted pushing Shade ransomware, like this wave of IRS notifications targeting recipients in the United States in 2017.

What does a Shade infection look like?

When a Windows host is infected with Shade ransomware, its desktop background announces the infection, and ten text files appear on the desktop named README1.txt through README10.txt as shown in Figure 1.

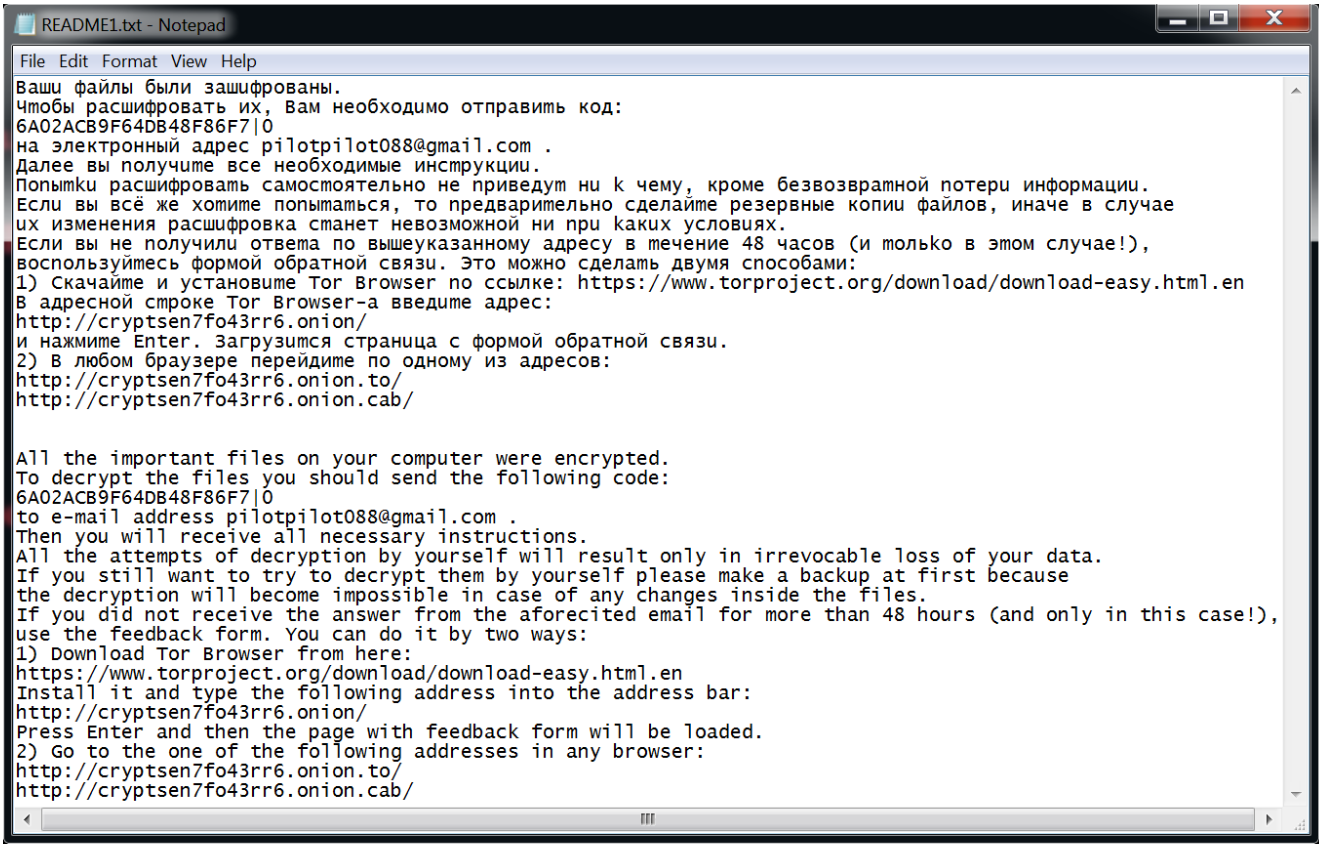


ВНИМАНИЕ!
Все важные файлы на всех дисках вашего компьютера были зашифрованы.
Подробности вы можете прочитать в файлах README.txt, которые можно найти на любом из дисков.

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.

Figure 1. Desktop of a Windows host infected with Shade ransomware.

The ten README files all contain the same instructions as shown in Figure 2.



```
Ваши файлы были зашифрованы.
Чтобы расшифровать их, Вам необходимо отправить код:
6A02ACB9F64DB48F86F7|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:
6A02ACB9F64DB48F86F7|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 2. Decryption instructions from a recent Shade ransomware infection.

Since June 2016, file extensions for any encrypted files are ***.crypted000007*** as shown in Figure 3.

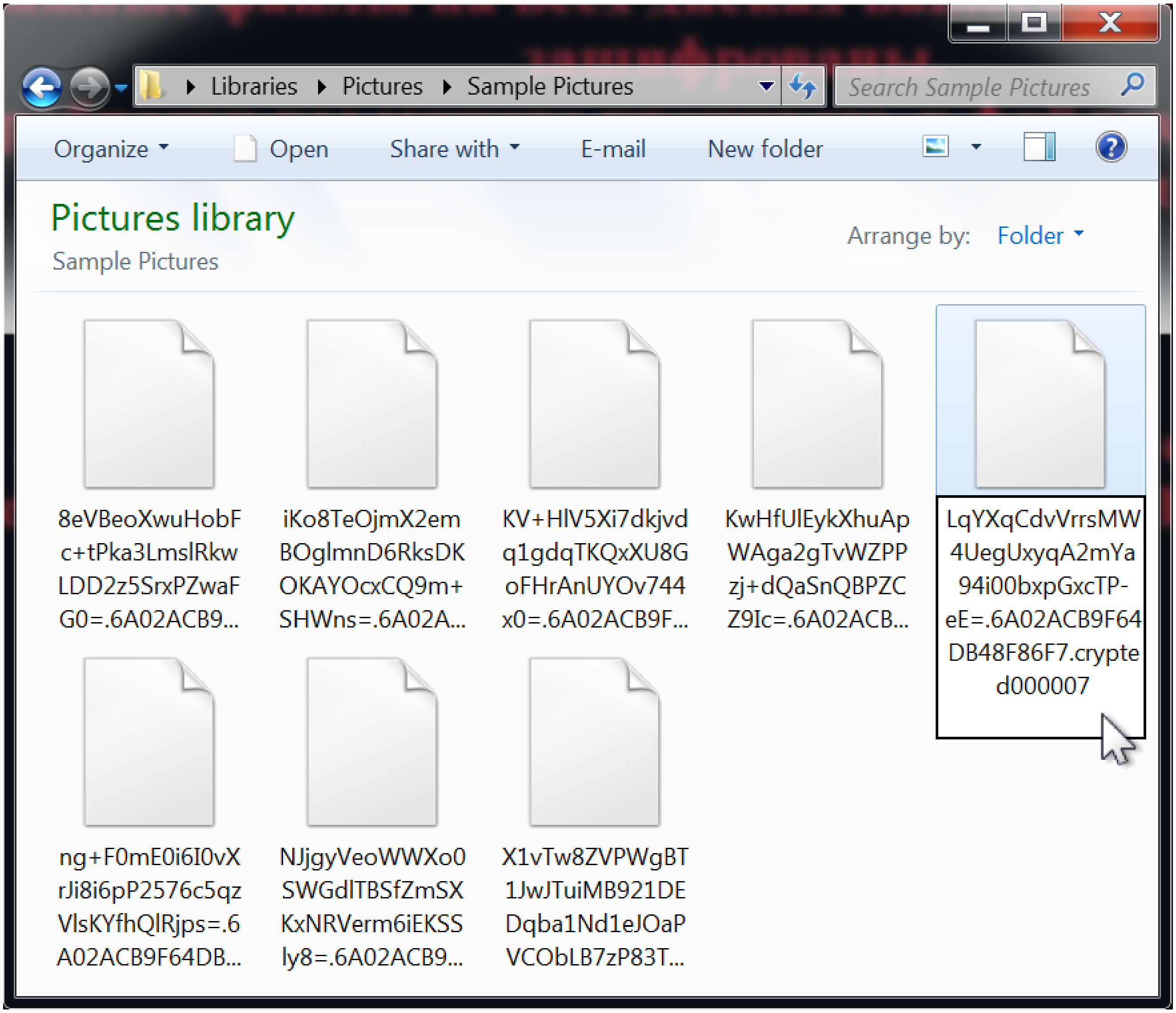

Libraries
Pictures
Sample Pictures
Search Sample Pictures
Organize
Open
Share with
E-mail
New folder
Pictures library
Sample Pictures
Arrange by:
Folder
8eVBeoXwuHobFc+tPka3LmslRkwLDD2z5SrxPZwaFG0=.6A02ACB9...
iKo8TeOjmX2emBOglmnD6RksDKOKAYOcxCQ9m+SHWns=.6A02A...
KV+HlV5Xi7dkjvdq1gdqTKQxXU8GoFHrAnUYOv744x0=.6A02ACB9F...
KwHfUlEykXhuApWAga2gTvWZPPzj+dQaSnQBPZCZ9Ic=.6A02ACB...
LqYXqCdvVrrsMW4UegUxyqA2mYa94i00bxpGxcTP-eE=.6A02ACB9F64DB48F86F7.crypted000007
ng+F0mE0i6I0vXrJi8i6pP2576c5qzVlsKYfhQlRjps=.6A02ACB9F64DB...
NJjgyVeoWWXo0SWGdlTBSfZmSXKxNRVerm6iEKSSly8=.6A02ACB9...
X1vTw8ZVPWgBT1JwJTuiMB921DEDqba1Nd1eJOaPVCObLB7zP83T...

Figure 3. Examples of encrypted files from a Shade ransomware infection.

Shade Distribution through Malspam

Malspam-based infections for Shade ransomware involve a JavaScript (.js) or other type of script-based file disguised as an invoice or bill. In some cases, Shade malspam has links for these script-based files. In other cases, the files are directly attached to the emails within a zip file or other type of archive. In February 2019, waves of Russian-language malspam used attached PDF files with links to download zip archives containing these script-based files.

In all cases we have reviewed, a .js or other script-based file was involved as indicated in Figure 4. These script-based files are designed to retrieve executable files for Shade ransomware.

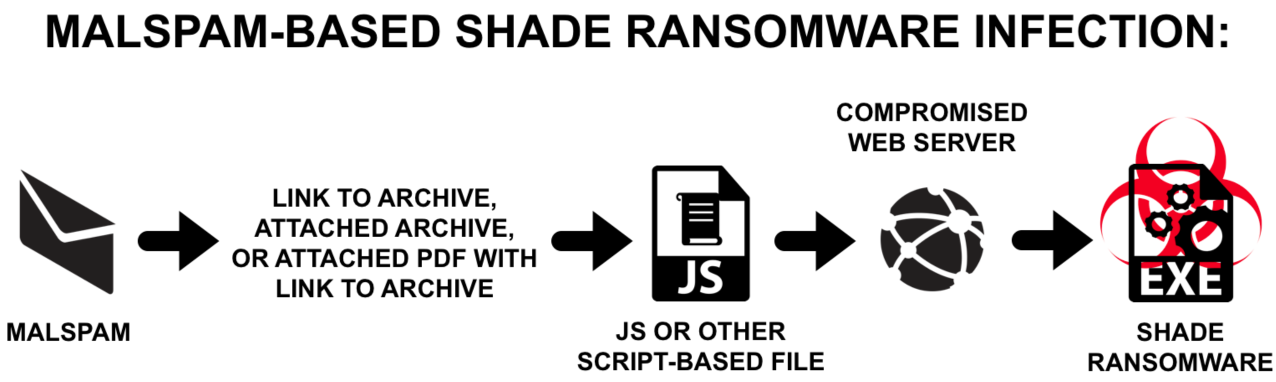

MALSPAM-BASED SHADE RANSOMWARE INFECTION:
MALSPAM
LINK TO ARCHIVE, ATTACHED ARCHIVE, OR ATTACHED PDF WITH LINK TO ARCHIVE
JS
JS OR OTHER SCRIPT-BASED FILE
COMPROMISED WEB SERVER
EXE
SHADE RANSOMWARE

Figure 4. Flow chart for malspam-based Shade ransomware infections.

Executable delivery during the infection chain

Malspam-based Shade infection chains have one thing in common. They all involve retrieving an executable file from a compromised server. By focusing on the executable in this chain of events, we can determine where Shade ransomware infection attempts have occurred.

AutoFocus search parameters

AutoFocus has a Shade ransomware tag that identifies any items associated with Shade ransomware. We searched on attempted deliveries of a Shade ransomware executable during an infection chain, and we focused our search on packed executable (PE) files sent through a URL over TCP port 80.

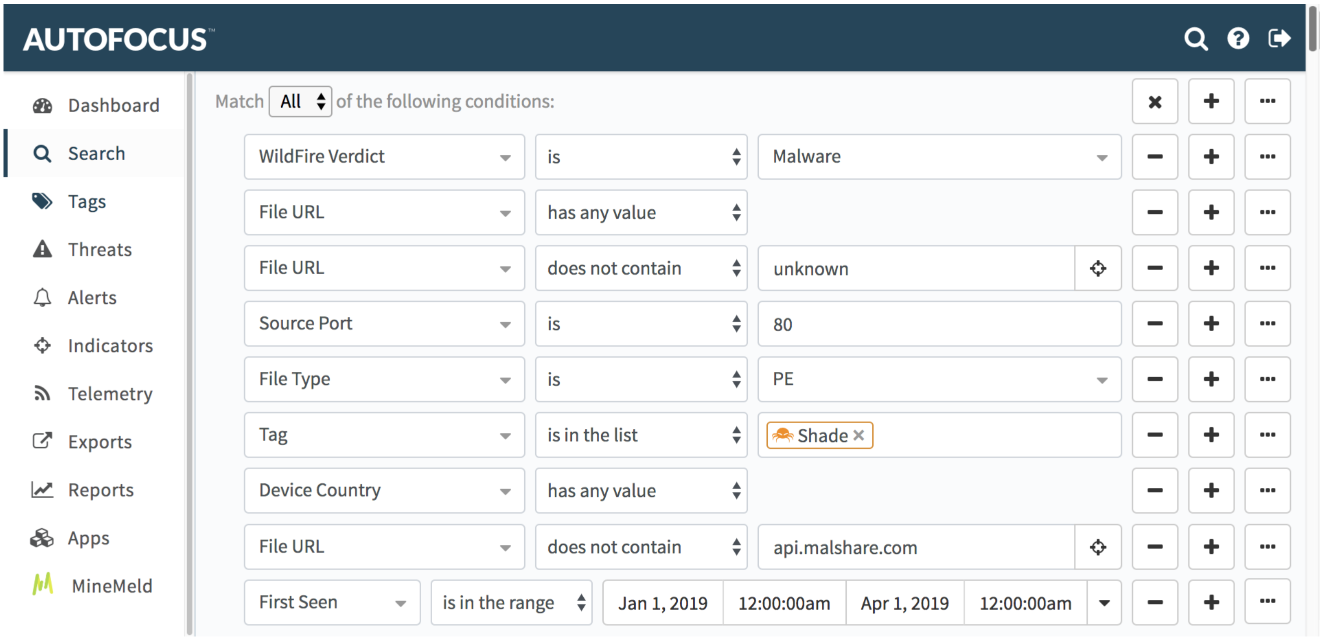
Since we're trying to determine geographic locations among our customer base where Shade ransomware attempts have happened, we looked for the country of Palo Alto Networks devices that discovered these attempts.

This search is for the first quarter of 2019.

Finally, our query eliminated any obvious malware submissions to online sandboxes and online sharing services. Our search parameters from the AutoFocus database were:

- Date is in the range from January 1st through March 31st
- Unit 42 tag is for Shade ransomware
- File type is PE
- File URL has any value but is not unknown
- Source port (the TCP port the file came from) is 80
- Device Country has any value (is not blank or unidentified)
- File URL does not contain the string ***/malware/***
- File URL does not contain the string ***malshare.com***
- File URL does not contain the string ***paloaltonetworks***

- File URL does not contain the string ***local***



Match All of the following conditions:

WildFire Verdict	is	Malware		
File URL	has any value			
File URL	does not contain	unknown		
Source Port	is	80		
File Type	is	PE		
Tag	is in the list	Shade		
Device Country	has any value			
File URL	does not contain	api.malshare.com		
First Seen	is in the range	Jan 1, 2019 12:00:00am	Apr 1, 2019 12:00:00am	

Figure 5. An AutoFocus query for Shade ransomware executables in the first quarter of 2019.

Results from January through March 2019

Our search results from January through March 2019 revealed 307 Shade ransomware samples over 6,536 sessions. Each session represents an HTTP request for a URL hosting a Shade ransomware executable. Many of these URLs were seen multiple times in separate sessions. Locations of our top ten results were:

- United States - 2,010 sessions
- Japan - 1,677 sessions
- India - 989 sessions
- Thailand - 723 sessions
- Canada - 712 sessions
- Spain - 505 sessions
- Russian Federation - 86 sessions
- France - 71 sessions
- United Kingdom - 67 sessions
- Kazakhstan - 21 sessions

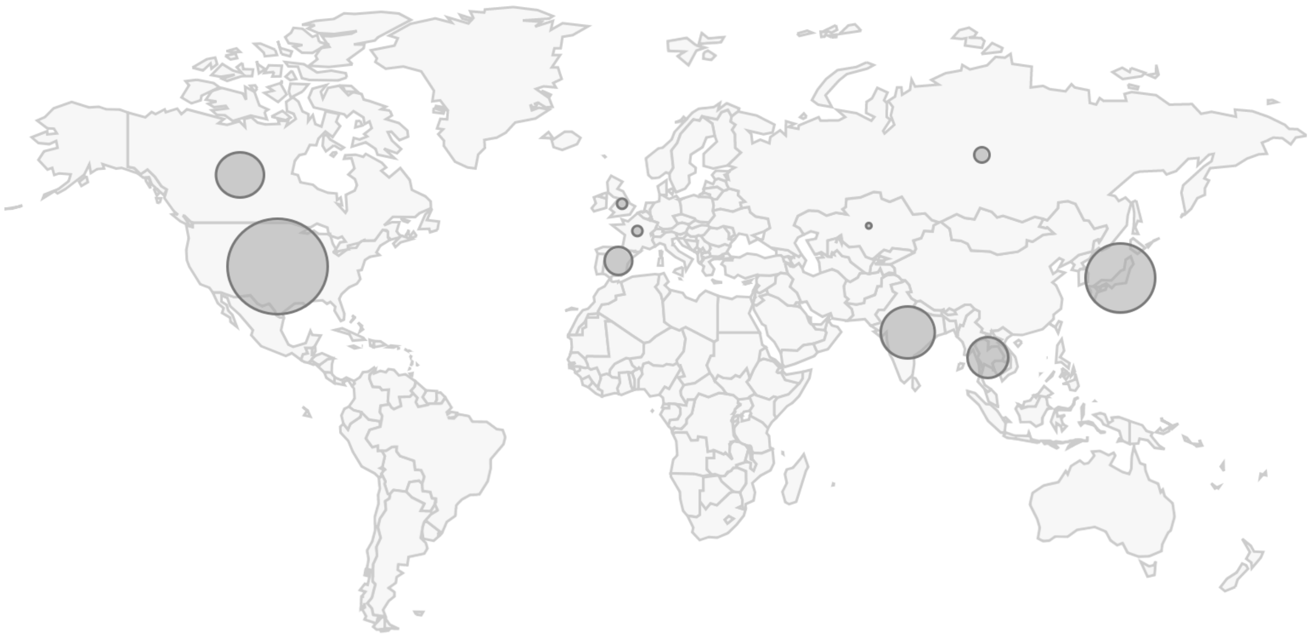


Figure 6. Top ten countries from our AutoFocus search results as shown on a world map.

The top country with Shade ransomware infection attempts among our customer base was the United States. The vast majority of these for URLs hosting Shade ransomware executables were reported from customer devices outside of Russia and Russian language countries.

The top 10 verticals for this period were:

- High Tech: 5,009 sessions
- Wholesale and Retail: 722 sessions
- Education: 720 sessions
- Telecommunications: 311 sessions
- Finance: 51 sessions
- Transportation and Logistics: 24 sessions
- Manufacturing: 32 sessions
- Professional and Legal Services: 8 sessions
- Utilities and Energy: 4 sessions
- State and Local Government: 1 session

Conclusion

The top country with Shade ransomware infection attempts among our customer base was the United States. The vast majority of these for URLs hosting Shade ransomware executables were reported from customer devices outside of Russia and Russian language countries.

The most common target for Shade ransomware infection attempts were organizations that fell under the High Tech category.

These results are likely skewed towards English due to our customer base. However, they indicate Shade ransomware is very active outside of Russia and possibly targeting more English-speaking victims than Russian.

Palo Alto Networks customers are protected from Shade ransomware by our threat prevention platform which easily detects these executables. AutoFocus users can track Shade ransomware attempts by using the Shade tag. See the appendices below for details on recent Shade ransomware samples we discovered in March and April 2019.

Appendix A

73 recent SHA256 file hashes for Shade ransomware executable files found in March and April 2019. Information is available at: https://github.com/pan-unit42/iocs/blob/master/Shade_ransomware/Shade-ransomware-SHA256-hashes-March-and-April-2019.txt

Appendix B

203 recent URLs that returned Shade ransomware executable files in March and April 2019. Information is available at: https://github.com/pan-unit42/iocs/blob/master/Shade_ransomware/Shade-ransomware-URLs-March-and-April-2019.txt

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.