More Russian language malspam pushing Shade (Troldesh) ransomware

By SANS Internet Storm Center

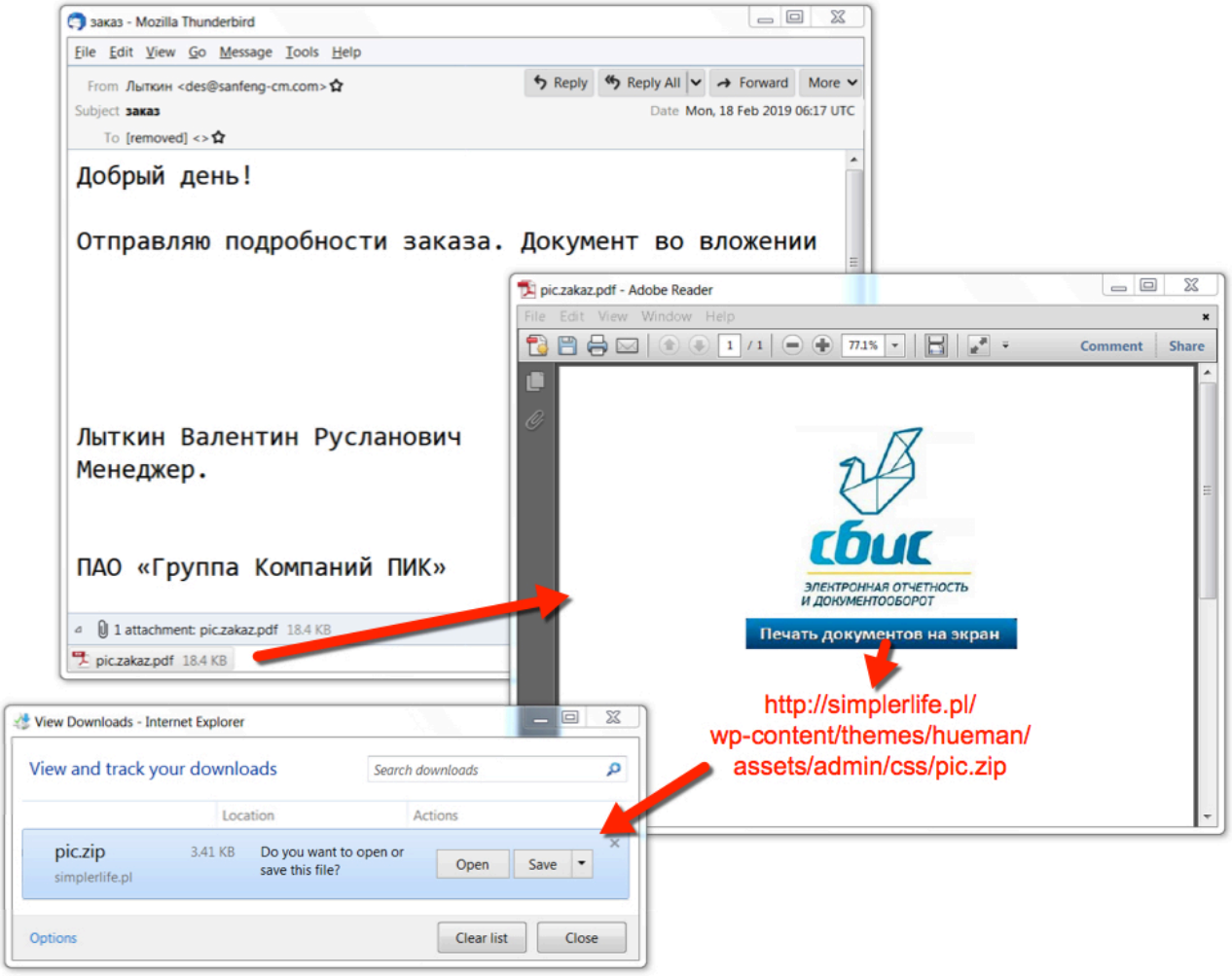
Archived: 2026-04-05 17:14:34 UTC

Introduction

Russian language spam pushing Shade ransomware (also known as Troldesh ransomware) has remained active since my previous ISC diary about it on 2018-11-29. However, sometime in February 2019, this malicious spam (malspam) has altered its tactics slightly. Instead of a zip archive directly attached to the malspam, recent emails have attached PDF files with links to download the zip archive. Otherwise, this infection activity remains relatively unchanged.

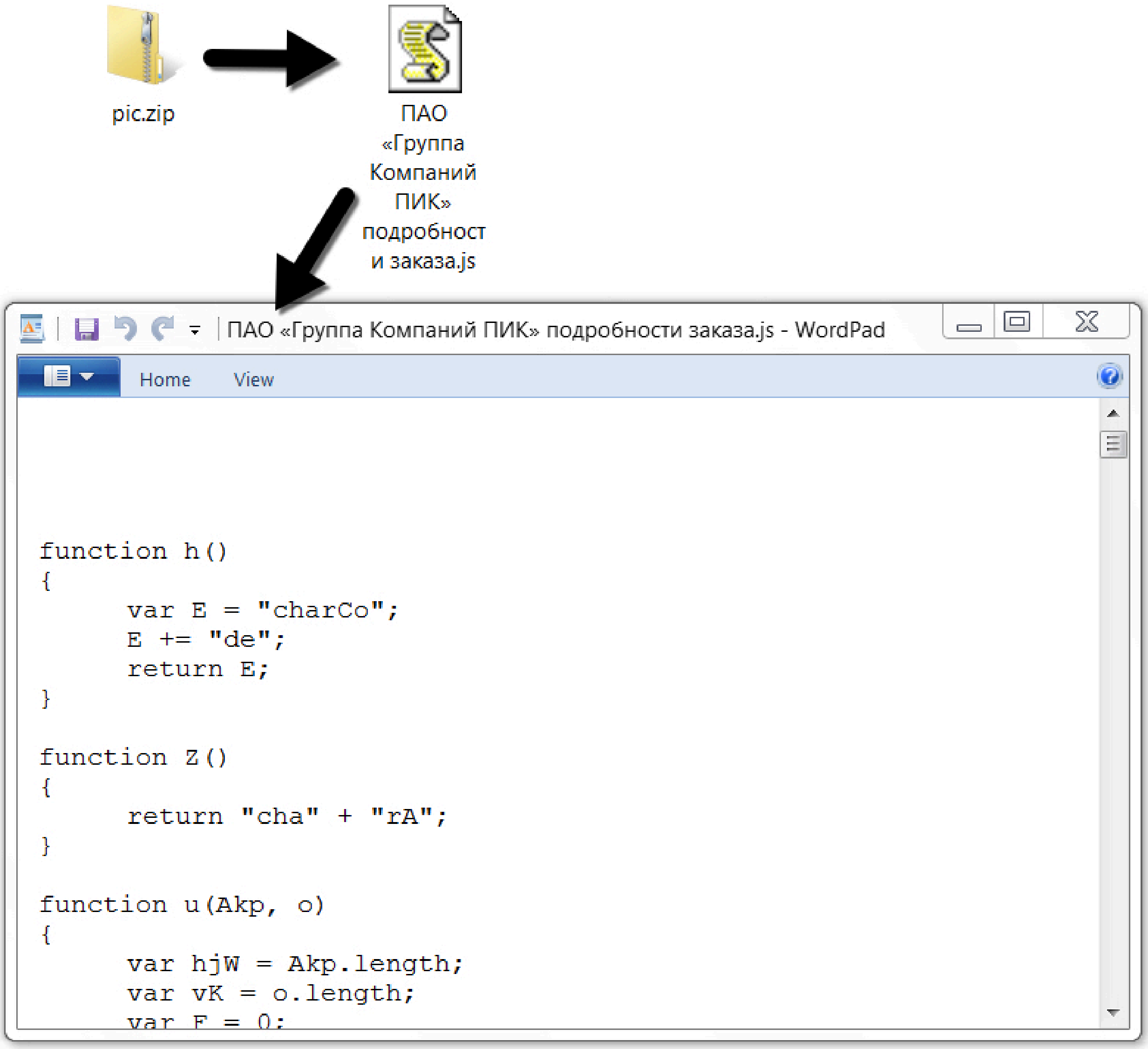
Details

Malspam pushing Shade has a variety of subjects, spoofed sending addresses, and message text. The common theme is some sort of order or invoice. The attached PDF files have links to download an alleged invoice, which was saved as ***pic.zip*** when I checked.

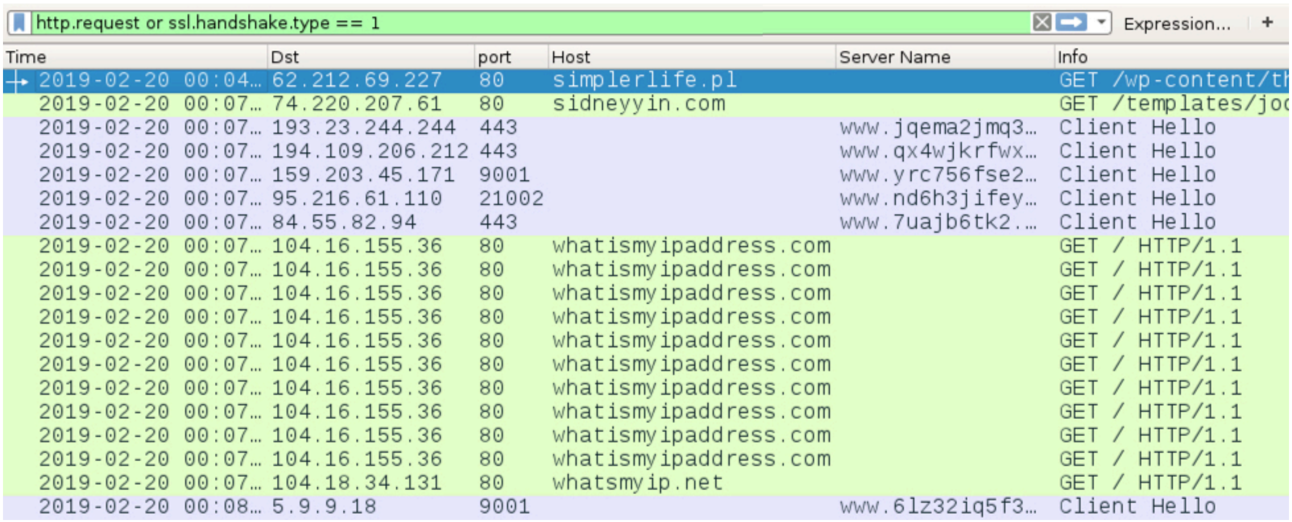


Shown above: From malspam to PDF to downloaded zip archive.

Pic.zip contained a JavaScript (.js) file designed to infect a vulnerable Windows host when double-clicked. Infection traffic remained similar to previous examples of Shade ransomware, and my infected Windows host exhibited the expected behavior.

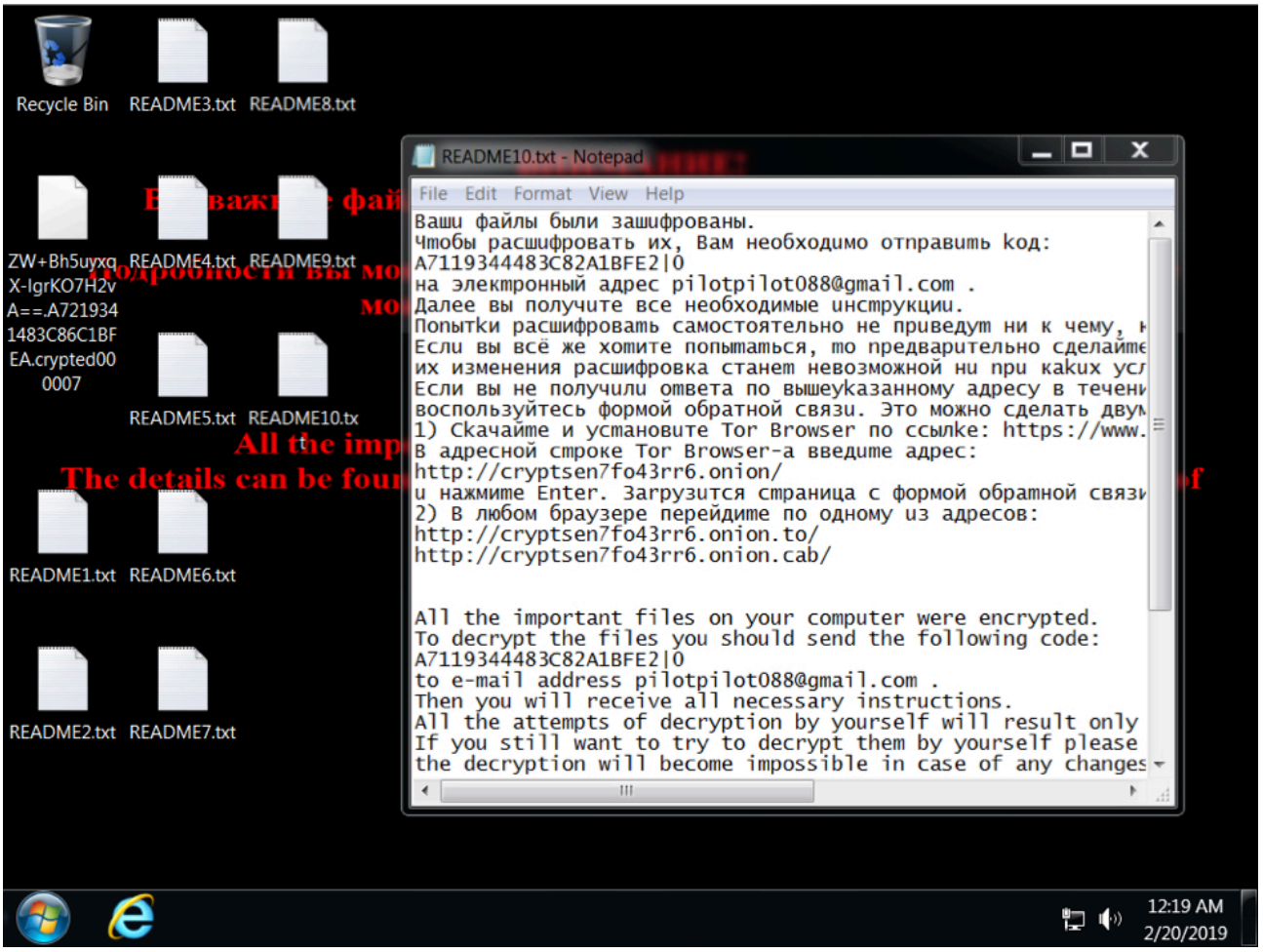


Shown above: Downloaded zip archive and extracted .js file.

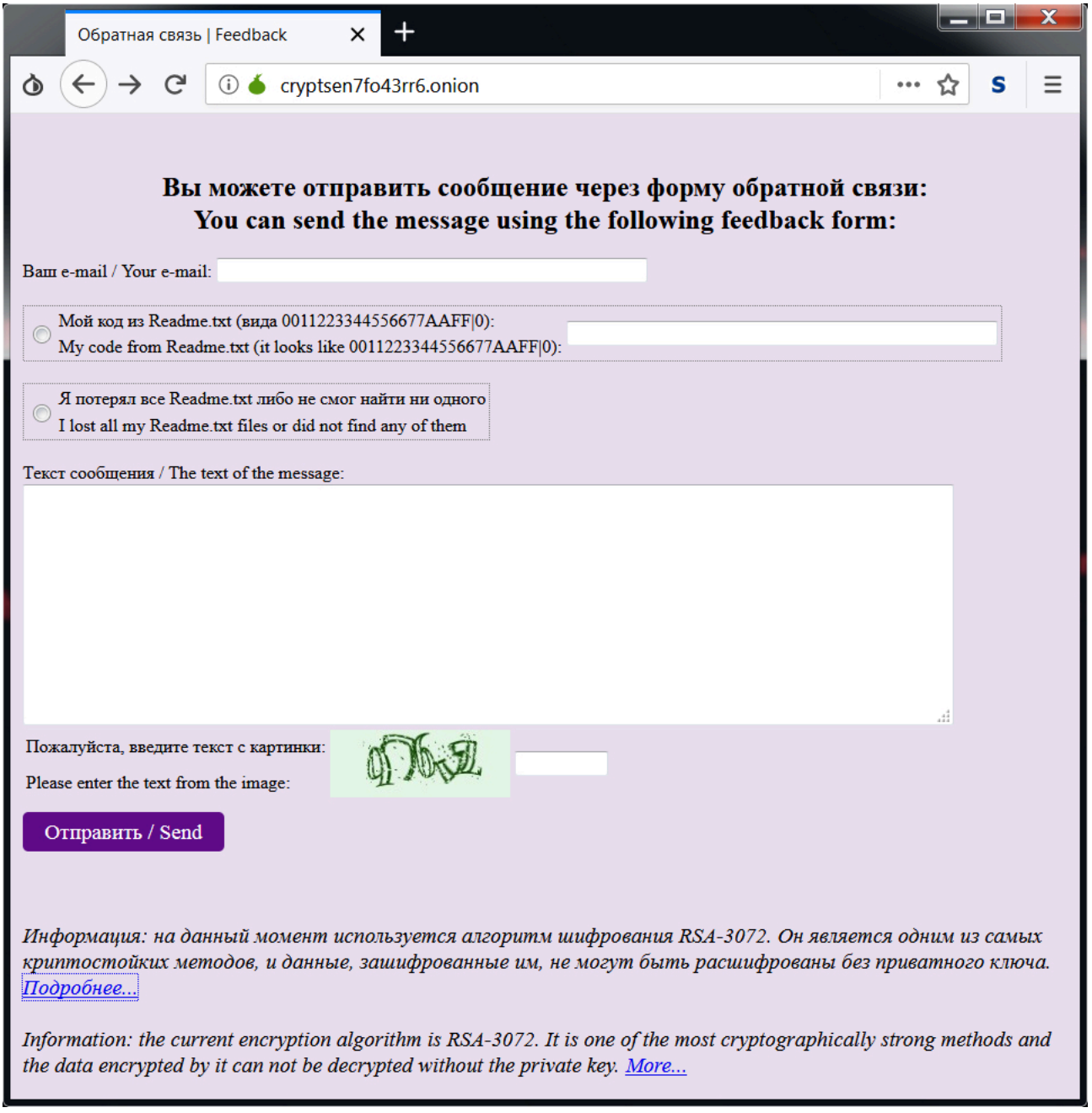

http.request or ssl.handshake.type == 1

Time	Dst	port	Host	Server Name	Info
2019-02-20 00:04…	62.212.69.227	80	simplerlife.pl		GET /wp-content/th
2019-02-20 00:07…	74.220.207.61	80	sidneyyin.com		GET /templates/jo(
2019-02-20 00:07…	193.23.244.244	443		www.jqema2jmq3…	Client Hello
2019-02-20 00:07…	194.109.206.212	443		www.qx4wjkrfwx…	Client Hello
2019-02-20 00:07…	159.203.45.171	9001		www.yrc756fse2…	Client Hello
2019-02-20 00:07…	95.216.61.110	21002		www.nd6h3jifey…	Client Hello
2019-02-20 00:07…	84.55.82.94	443		www.7uajb6tk2.…	Client Hello
2019-02-20 00:07…	104.16.155.36	80	whatismyipaddress.com		GET / HTTP/1.1
2019-02-20 00:07…	104.16.155.36	80	whatismyipaddress.com		GET / HTTP/1.1
2019-02-20 00:07…	104.16.155.36	80	whatismyipaddress.com		GET / HTTP/1.1
2019-02-20 00:07…	104.16.155.36	80	whatismyipaddress.com		GET / HTTP/1.1
2019-02-20 00:07…	104.16.155.36	80	whatismyipaddress.com		GET / HTTP/1.1
2019-02-20 00:07…	104.16.155.36	80	whatismyipaddress.com		GET / HTTP/1.1
2019-02-20 00:07…	104.16.155.36	80	whatismyipaddress.com		GET / HTTP/1.1
2019-02-20 00:07…	104.16.155.36	80	whatismyipaddress.com		GET / HTTP/1.1
2019-02-20 00:07…	104.16.155.36	80	whatismyipaddress.com		GET / HTTP/1.1
2019-02-20 00:07…	104.16.155.36	80	whatismyipaddress.com		GET / HTTP/1.1
2019-02-20 00:07…	104.18.34.131	80	whatsmyip.net		GET / HTTP/1.1
2019-02-20 00:08…	5.9.9.18	9001		www.6lz32iq5f3…	Client Hello

Shown above: Traffic from the infection filtered in Wireshark.



Shown above: Desktop of an infected Windows host.



Shown above: Decryption instructions from the Tor page.

Indicators of compromise (IoCs)

The following are indicators associated with today's infection:

SHA256 hash: 6950efbd9d6d10fdd8f644a71b30e53a8d1dbd64976279d8a192a0c9459d06e1

- File name: ***pic.zakaz.pdf***
- File size: 18,831 bytes
- File description: PDF attachment from malspam pushing Shade/Troldesh ransomware

SHA256 hash: e76b93f6ab032e16f5f1d600cb061db49a10538b10a063561df95be94156ac0b

- File name: ***pic.zip***

- File size: 3,493 bytes
- File location: hxxp://simplerlife[.]pl/wp-content/themes/hueman/assets/admin/css/pic.zip
- File description: Downloaded zip archive from link in PDF attachment

SHA256 hash: 17539e1a0c33fe2f98fa1b8fa282f9f3786ba15419e30ae6c4171ccff65338c9

- File size: 6,932 bytes
- File description: .js file extracted from pic.zip

SHA256 hash: 33dde2eed8ccb2b74c9d0feaf19c341354e54cb5d2c9e475507ff3fe22240381

- File size: 1,254,664 bytes
- File location: hxxp://sidneyyin[.]com/templates/joomlage0084-aravnik/css/msg.jpg
- File location: C:\Users*[username]*\AppData\Local\Temp\rad8EEC7.tmp
- File location: C:\ProgramData\Windows\csrss.exe
- File description: Downloaded zip archive from link in PDF attachment

Traffic from an infected Windows host:

- 62.212.69[.]227 port 80 - ***simplerlife[.]pl*** - GET /wp-content/themes/hueman/assets/admin/css/pic.zip
- 74.220.207[.]61 port 80 - ***sidneyyin[.]com*** - GET /templates/joomlage0084-aravnik/css/msg.jpg
- Various IP addresses over various TCP ports - Tor traffic
- port 80 - ***whatismyipaddress.com*** - GET /
- port 80 - ***whatsmyip.net*** - GET /

Email address and URLs from the decryption instructions:

- pilotpilot088@gmail.com
- hxxp://cryptsen7fo43rr6[.]onion/
- hxxp://cryptsen7fo43rr6[.]onion.to/
- hxxp://cryptsen7fo43rr6[.]onion.cab/

Final words

As I stated last time, Russian language malspam pushing Shade/Troldesh ransomware is nothing new. Since I first posted a diary about it back in 2016, it's never disappeared for long. Nor is this malspam limited to Russian language. An example I documented in 2017 was from English malspam. This diary is yet another reminder the criminals behind this malware remain active.

Brad Duncan
brad [at] malware-traffic-analysis.net
