Breaking Petya - Solving Malware Using a Poor Implementation of Salsa20

Peixian Wang

May 6, 2016

Abstract

Ransomware has become a relatively profitable development in recent years with the surge in popularity of Bitcoin and other untracable forms of money transactions. In this paper we detail Petya, a recent form of ransomware targeting Windows platforms and NTFS drives. We describe the construction of Petya and the underlying encryption algorithm, Salsa20, and also present one possible solution utilizing Z3, an efficient satisfiabliity modulo theory solver, to defeat Petya.

1 Introduction

Online transactions through Tor (?) using anonomyous cryptocurrencies allow for a certain level of privacy when it comes to payments, but also allow themselves to be used in a malicious fashion. Since Bitcoin, the most popular form of cryptocurrency, makes it extremely hard to track the transactions, Bitcoin has become the de facto standard for ransomware, malware which infects the victim's computer, holds files hostage through encryption, and extorts the victims for money in return for the files. Petya is one such ransomware, except rather than targeting the files of the victim, it targets the master boot record (MBR) and master file table (MFT) (9).

2 Petya

2.1 Overview

Petya is a relatively new ransomware variant, only starting to appear within the early months of 2016. In order to bypass the lengthy process of encrypting each file on the victim's hard drive, Petya simply seeks to write malicious code to the start of the disk. This code overwrites the MBR of the hard drive with a small kernel that then encrypts the MFT.

2.2 Behavioral Analysis

Petya is usually destributed through a zip file (3), containing two other files: 1. a photo of a young man, puporting to be an applicant and 2. an executable, disguised as a csv file, shown in figure 1. After opening the executable, Petya calls an undocumented API called NtRaiseHardError. The computer then promptly crashes and boots into a fake CHKDSK scan, shown in figure 2, which starts

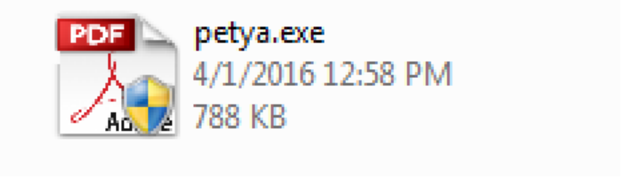
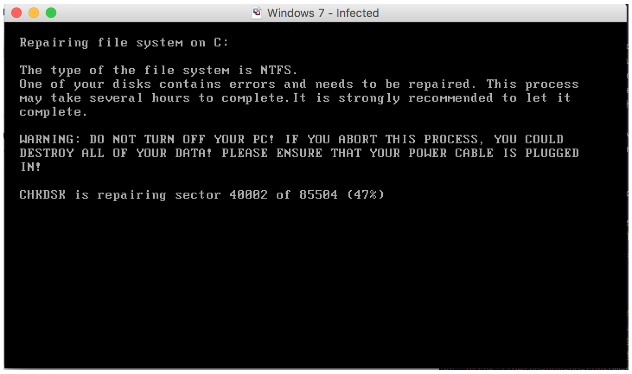
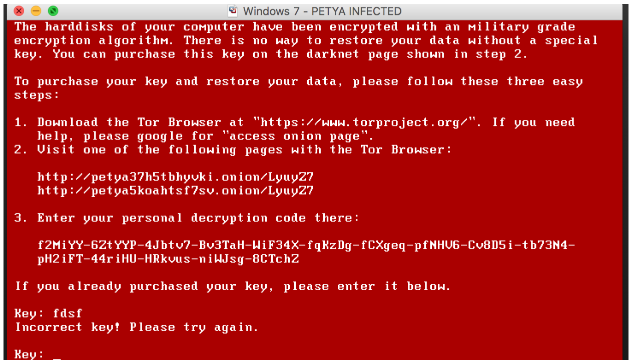

petya.exe
4/1/2016 12:58 PM
788 KB

Figure 1: The petya executable disguised as a .pdf file.



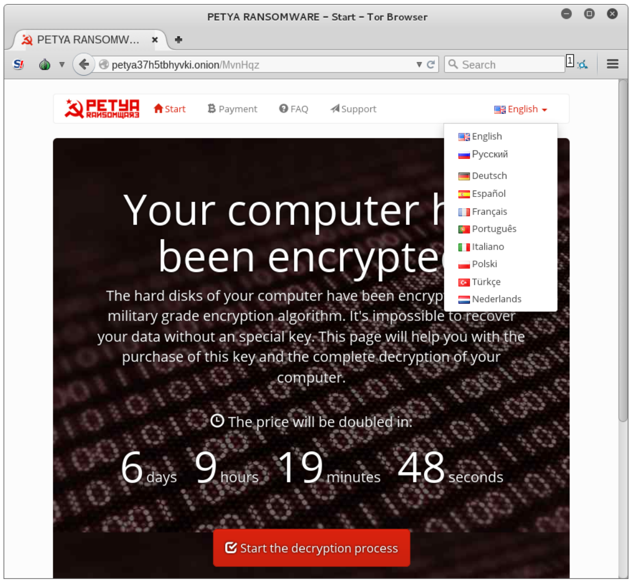
```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 40002 of 85504 (47%)
```

Figure 2: The fake CHKDSK scan made by Petya while it encrypts the MFT.



```
The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/LyuyZ7
   http://petya5koahtsf7sv.onion/LyuyZ7

3. Enter your personal decryption code there:

   f2MiYY-6ZtYYP-4Jbtv7-Bv3TaH-WiF34X-fqKzDg-fCXgeq-pfNHV6-Cv8D5i-tb73N4-
   pH2iFT-44riHU-HRkvus-niWJsg-8CTchZ

If you already purchased your key, please enter it below.

Key: fdsf
Incorrect key! Please try again.

Key: _
```

Figure 3: The ransom note by Petya.



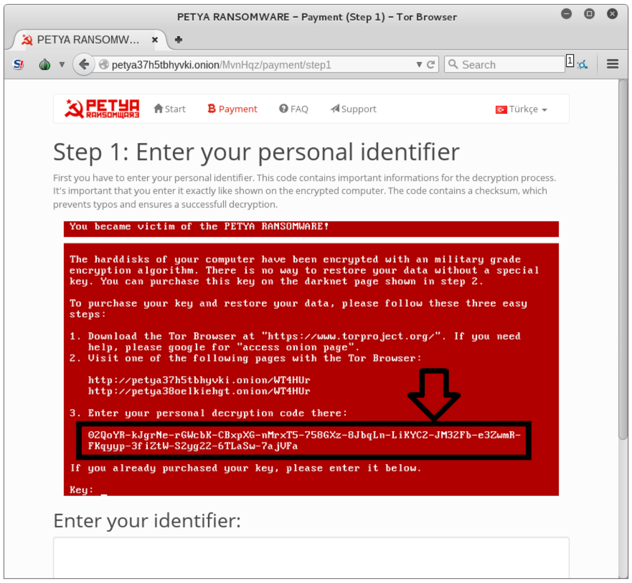
Your computer h
been encrypte

The hard disks of your computer have been encryp military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

The price will be doubled in:

6 days 9 hours 19 minutes 48 seconds

Figure 4: Accessibility is important, even for malware. From (3).


PETYA RANSOMWARE – Payment (Step 1) – Tor Browser
PETYA RANSOMW...
petya37h5tbhyvki.onion/MvnHqz/payment/step1
Search
PETYA RANSOMWARE
Start
Payment
FAQ
Support
Türkçe

Step 1: Enter your personal identifier

First you have to enter your personal identifier. This code contains important informations for the decryption process. It's important that you enter it exactly like shown on the encrypted computer. The code contains a checksum, which prevents typos and ensures a successfull decryption.

```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/WT4HUr
   http://petya38oelkiehgt.onion/WT4HUr

3. Enter your personal decryption code there:

   02QoYR-kJgrNe-rGWcbK-CBxpXG-nMrxT5-758GXz-8JbqLn-LiKYC2-JM32Fb-e3ZwmR-
   FKqyyp-3fiZtW-S2yg22-6TLaSw-7ajVFa

If you already purchased your key, please enter it below.

Key: _
```

Enter your identifier:

Figure 5: Petya Tutorial on purchasing bitcoins and performing a transaction.

the encryption on the MFT. When the encryption completes, the user is shown a ransom note screen, shown in figure 3. After visiting the website, the user is presented with a relatively upscale website, featuring multiple languages (figure 4) and a tutorial on how victims can perform a bitcoin transaction (figure 5).

2.3 Code Analysis

3 Salsa20

3.1 Overview

3.2 Implementation

3.3 Implementation Within Petya

4 Infestor

4.1 Code Walkthrough

As online transcations through Tor (?) and cryptocurrencies become more commonplace,

References

[1] Bernstein, D. J. Salsa20 specification. `https://cr.yp.to/snuffle/spec.pdf`.

[2] de Moura, L., and Bjørner, N. Z3: An efficient smt solver. `http://research.microsoft.com/en-us/um/redmond/projects/z3/z3.pdf`.

[3] hasherezade. Petya – taking ransomware to the low level. `https://blog.malwarebytes.org/threat-analysis/2016/04/petya-ransomware/`, 2016.

[4] Research, M. z3. `https://z3prover.github.io/api/html/z3.html`.

[5] Stone, L. hack-petya mission accomplished!!! `https://github.com/leo-stone/hack-petya`, 2016.

[6] tisf Nativ, Y., and Shalev, S. thezoo. `https://github.com/ytisf/theZoo`, 2016.

[7] Tonello, G. Breaking petya ransomware! `http://www.tgsoft.it/english/news_archivio_eng.asp?id=718`, 2016.

[8] Tonello, G. Petya ransomware x-rayed !!! `http://www.tgsoft.it/english/news_archivio_eng.asp?id=712718`, 2016.

[9] Trafimchuk, A. Decrypting the petya ransomware. `http://blog.checkpoint.com/2016/04/11/decrypting-the-petya-ransomware/`, 2016.

[10] Weber, A. Salsa20. `https://github.com/alexwebr/salsa20/blob/master/salsa20.c`, 2015.