Petya and Mischa For All Part II: They’re Here…

blogs.blackberry.com/en/2016/07/petya-and-mischa-for-all-part-ii-theyre-here

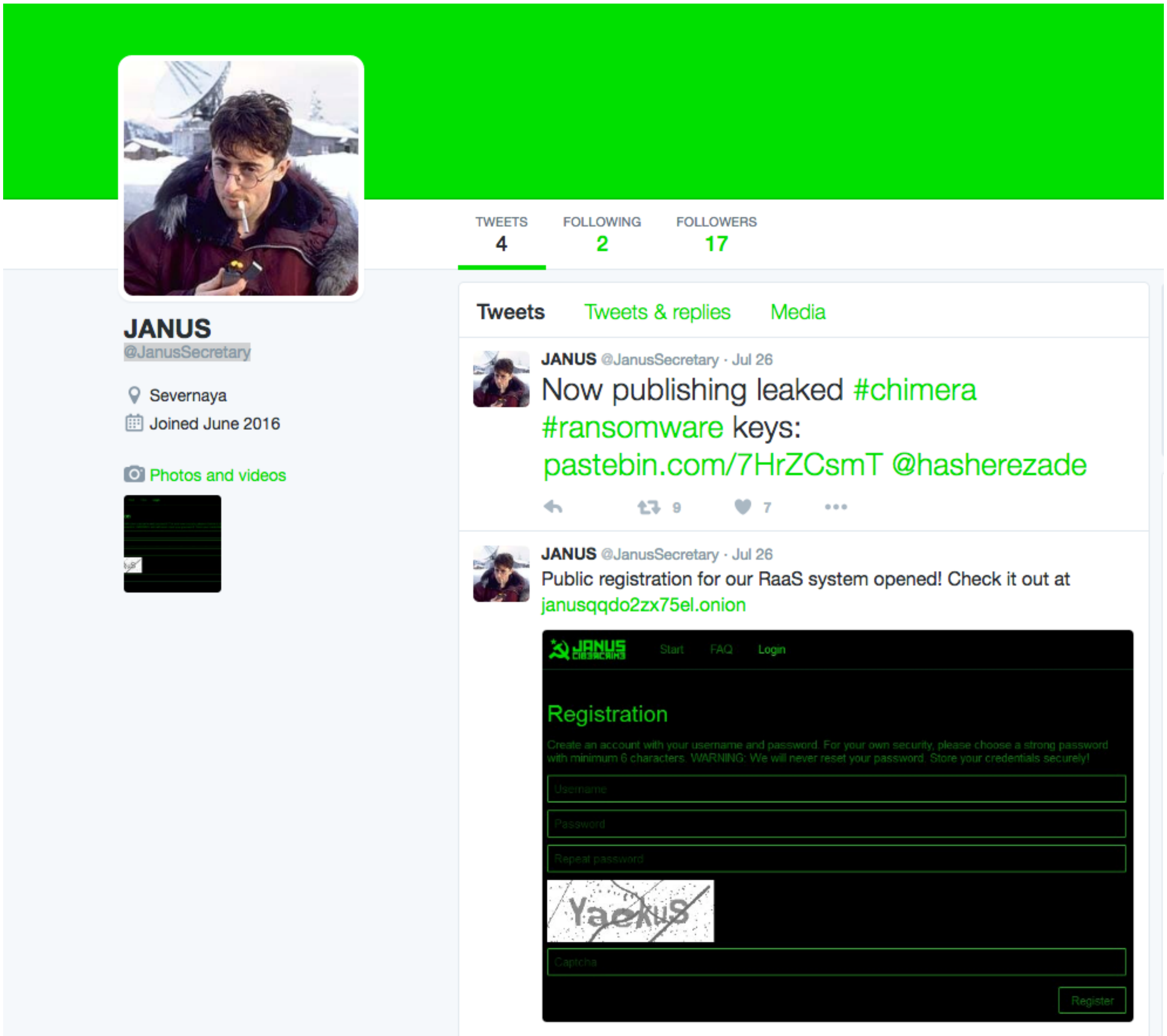
Jim Walter

/ 07.28.16 / Jim Walter

The time has come to follow up on our previous analysis of the Petya and Mischa ransomware family. When we last left off, private ransomware distributor Janus Cybercrime Solutions had started opening up the platform by offering private stubs and support, in line with most ransomware as a service (RaaS) offerings.

Now, the day security experts around the world have both expected and feared has finally come: the Petya and Mischa bundle is open and available to all!

The update was quietly announced on July 26, 2016, on a little-known Twitter account run by Janus Cybercrime Solutions. It is important to note here that this Twitter alias changed between updates as well. Prior to July, the account username was '@janussec,' whereas now, Janus is operating as '@janussecretary'.



JANUS
@JanusSecretary

Severnaya
Joined June 2016

JANUS @JanusSecretary · Jul 26
Now publishing leaked #chimera #ransomware keys: pastebin.com/7HrZCsmT @hasherezade

9 7

JANUS @JanusSecretary · Jul 26
Public registration for our RaaS system opened! Check it out at janusqqdo2zx75el.onion

JANUS CIB3RCRIM3

Registration

Create an account with your username and password. For your own security, please choose a strong password with minimum 6 characters. WARNING: We will never reset your password. Store your credentials securely!

Username

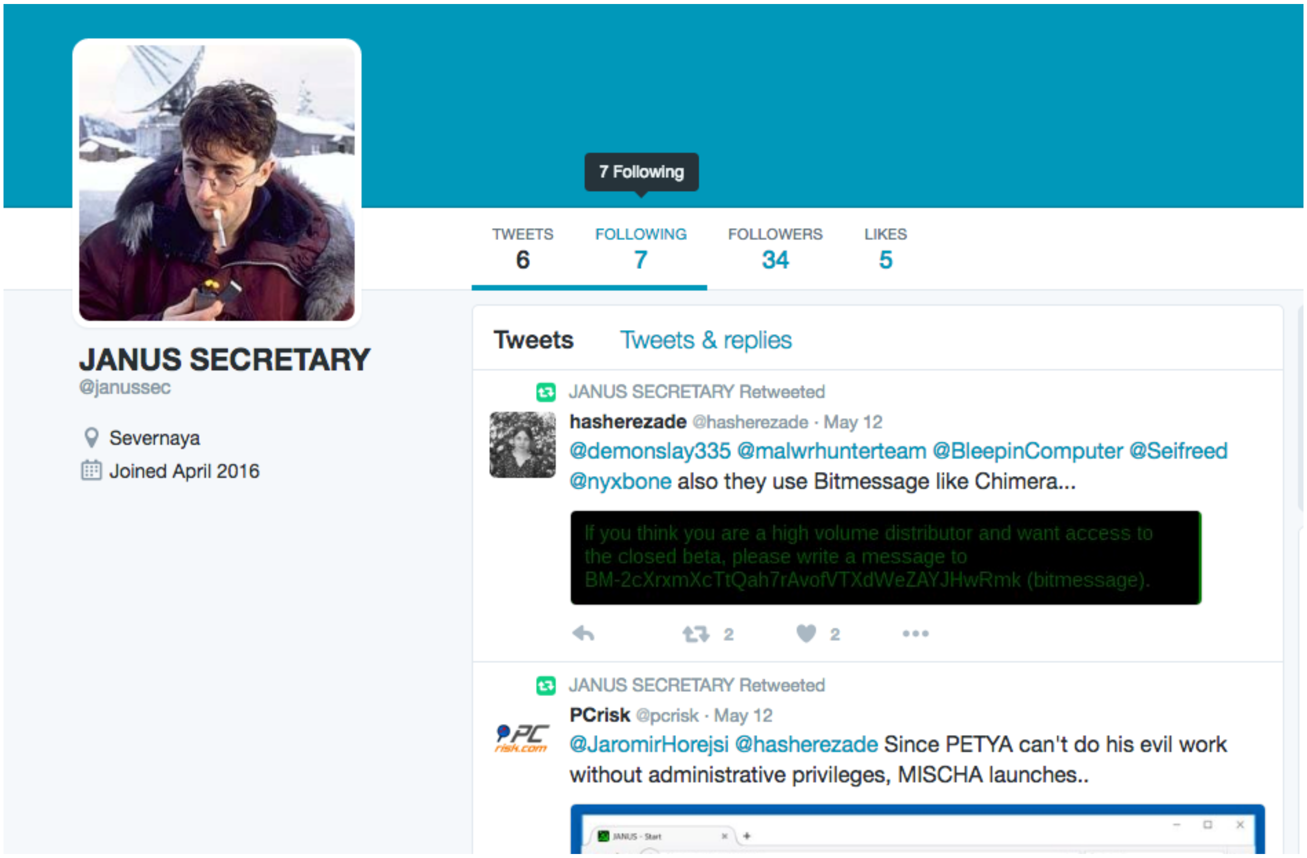
Password

Repeat password

YaekuS

Captcha

Figure 1: Janus Cybercrime Solutions Twitter Page - July 26th, 2016



7 Following

TWEETS 6 FOLLOWING 7 FOLLOWERS 34 LIKES 5

JANUS SECRETARY
@janussec

Severnaya
Joined April 2016

Tweets Tweets & replies

JANUS SECRETARY Retweeted
hasherezade @hasherezade · May 12
@demonslay335 @malwrhunterteam @BleepinComputer @Seifreed @nyxbone also they use Bitmessage like Chimera...

If you think you are a high volume distributor and want access to the closed beta, please write a message to BM-2cXrxmXcTtQah7rAvofVTXdWeZAYJHwRmk (bitmessage).

2 2

JANUS SECRETARY Retweeted
PCrisk @pcrisk · May 12
@JaromirHorejsi @hasherezade Since PETYA can't do his evil work without administrative privileges, MISCHA launches..

Figure 2: Previous Twitter Page for Janus Cybercrime Solutions - May 12th, 2016

Petya: Coming Soon to a Computer Near You

In short, the platform is now fully open to anyone who wants to create, spread, and manage their own Petya infections. The danger here of course is that the Petya ransomware generated by this service is every bit as destructive as previous generations.

This is how a typical Petya infection goes: upon execution of the malware, the infected host computer will shut down and reboot. Following the restart, the victim (as was the case prior) will be presented with a false CHKDSK screen. Interrupting that screen, or forcing a reboot in an attempt to stop the fake process, leads to the familiar skull and crossbones animation. Pressing any key during the skull display leads the victim to instructions on how to pay the ransom, along with their personal decryption code.

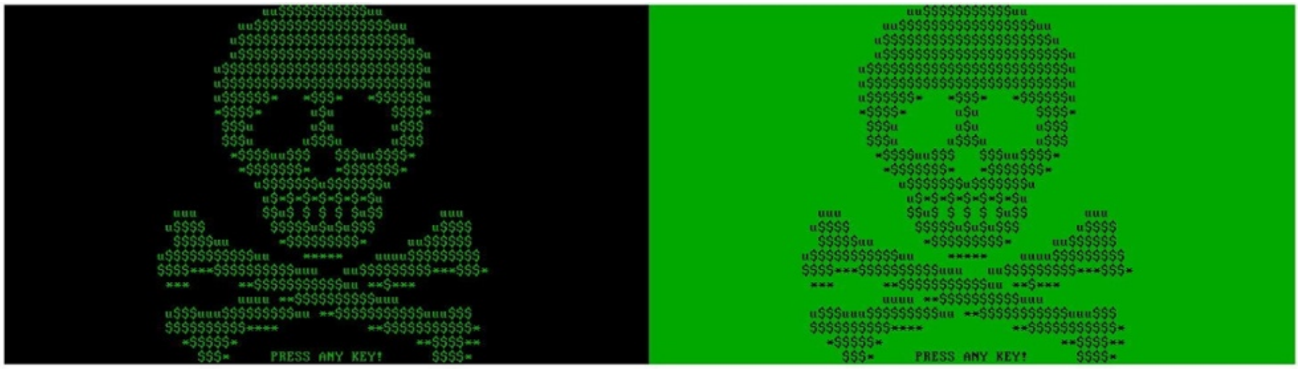
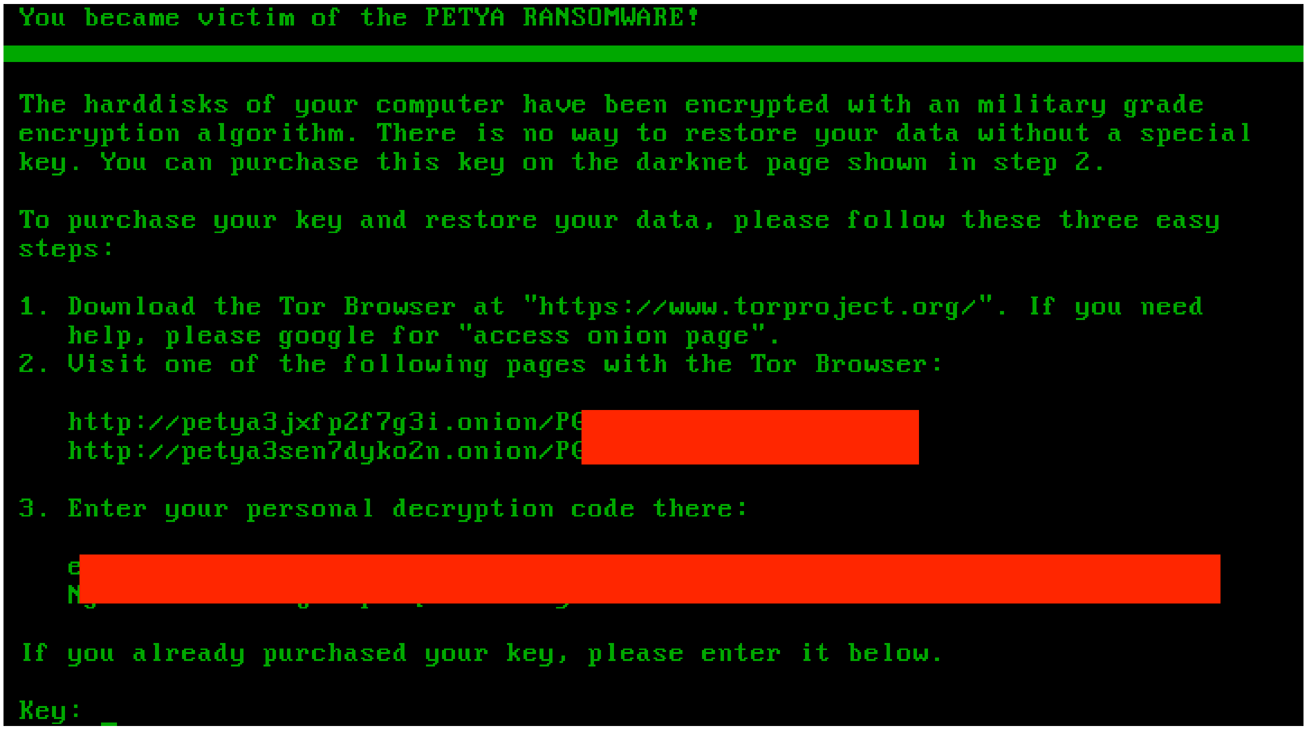
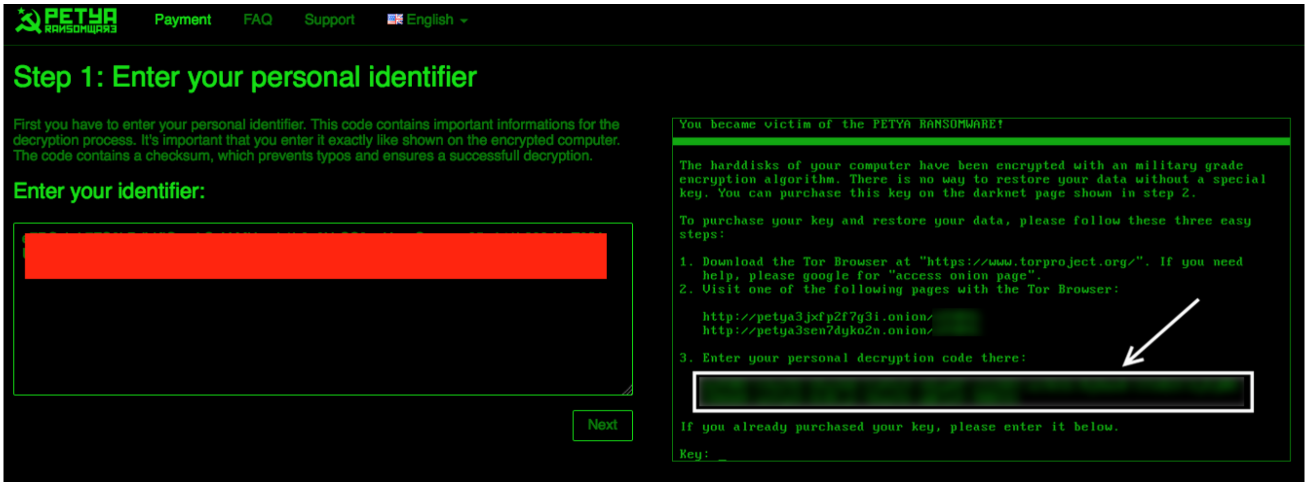


Figure 3: Skull and Crossbones Display – the Hallmark of a Petya Ransomware Infection



```
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://petya3jxfp2f7g3i.onion/P[redacted]
   http://petya3sen7dyko2n.onion/P

3. Enter your personal decryption code there:

   [redacted]

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

Key: _
```

Figure 4: Petya Ransom Note



Step 1: Enter your personal identifier

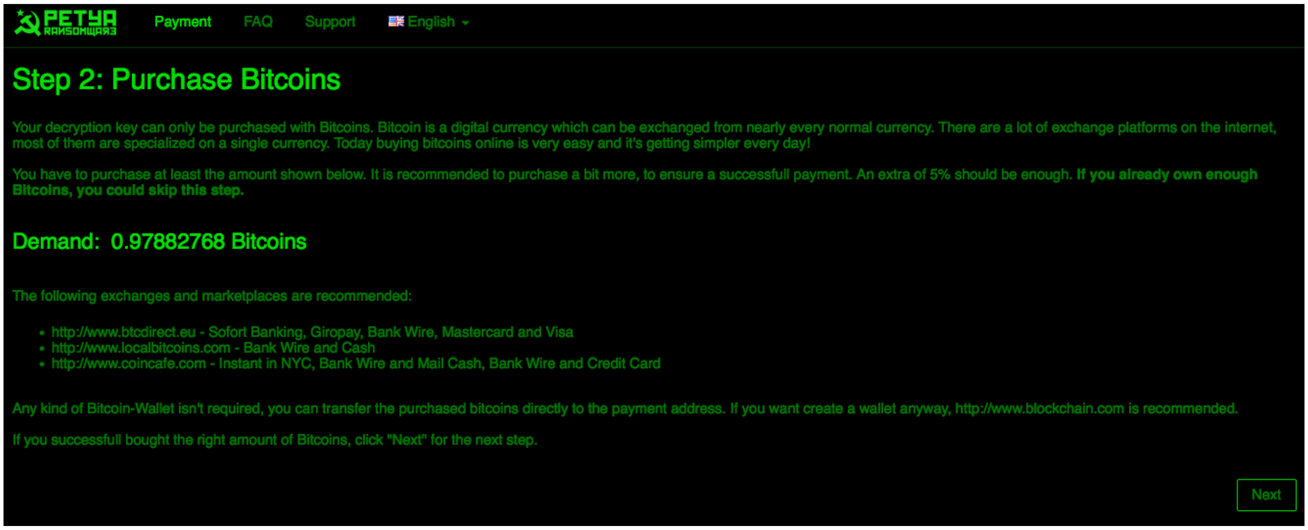
First you have to enter your personal identifier. This code contains important informations for the decryption process. It's important that you enter it exactly like shown on the encrypted computer. The code contains a checksum, which prevents typos and ensures a successfull decryption.

Enter your identifier:

[redacted]

```
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://petya3jxfp2f7g3i.onion/[redacted]
   http://petya3sen7dyko2n.onion/

3. Enter your personal decryption code there:

   [redacted]

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

Key: _
```

Figure 5: Petya Payment Screen



Step 2: Purchase Bitcoins

Your decryption key can only be purchased with Bitcoins. Bitcoin is a digital currency which can be exchanged from nearly every normal currency. There are a lot of exchange platforms on the internet, most of them are specialized on a single currency. Today buying bitcoins online is very easy and it's getting simpler every day!

You have to purchase at least the amount shown below. It is recommended to purchase a bit more, to ensure a successfull payment. An extra of 5% should be enough. **If you already own enough Bitcoins, you could skip this step.**

Demand: 0.97882768 Bitcoins

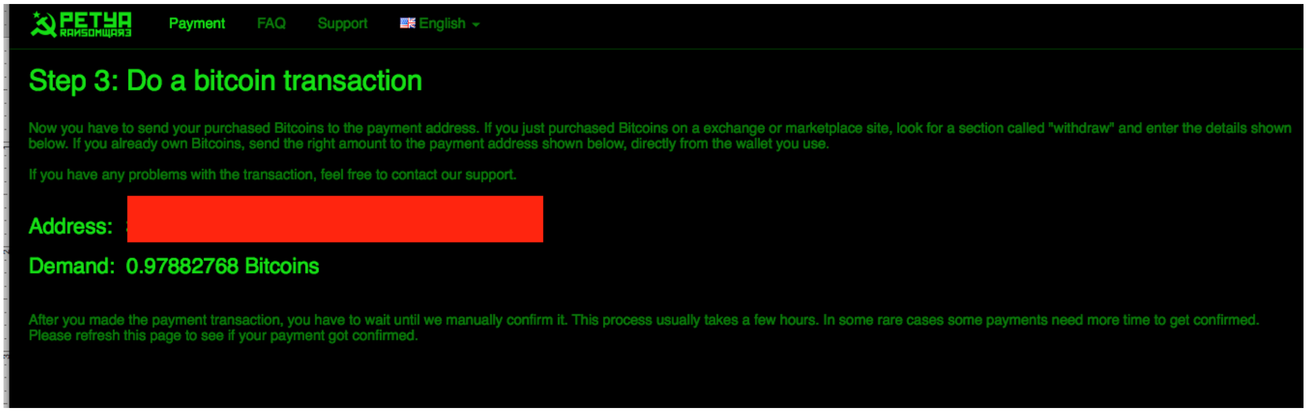
The following exchanges and marketplaces are recommended:

- http://www.btcdirect.eu - Sofort Banking, Giropay, Bank Wire, Mastercard and Visa
- http://www.localbitcoins.com - Bank Wire and Cash
- http://www.coincafe.com - Instant in NYC, Bank Wire and Mail Cash, Bank Wire and Credit Card

Any kind of Bitcoin-Wallet isn't required, you can transfer the purchased bitcoins directly to the payment address. If you want create a wallet anyway, http://www.blockchain.com is recommended.

If you successfull bought the right amount of Bitcoins, click "Next" for the next step.

Figure 6: Purchasing Bitcoin to Pay the Petya Ransom



Step 3: Do a bitcoin transaction

Now you have to send your purchased Bitcoins to the payment address. If you just purchased Bitcoins on a exchange or marketplace site, look for a section called "withdraw" and enter the details shown below. If you already own Bitcoins, send the right amount to the payment address shown below, directly from the wallet you use.

If you have any problems with the transaction, feel free to contact our support.

Address: [redacted]

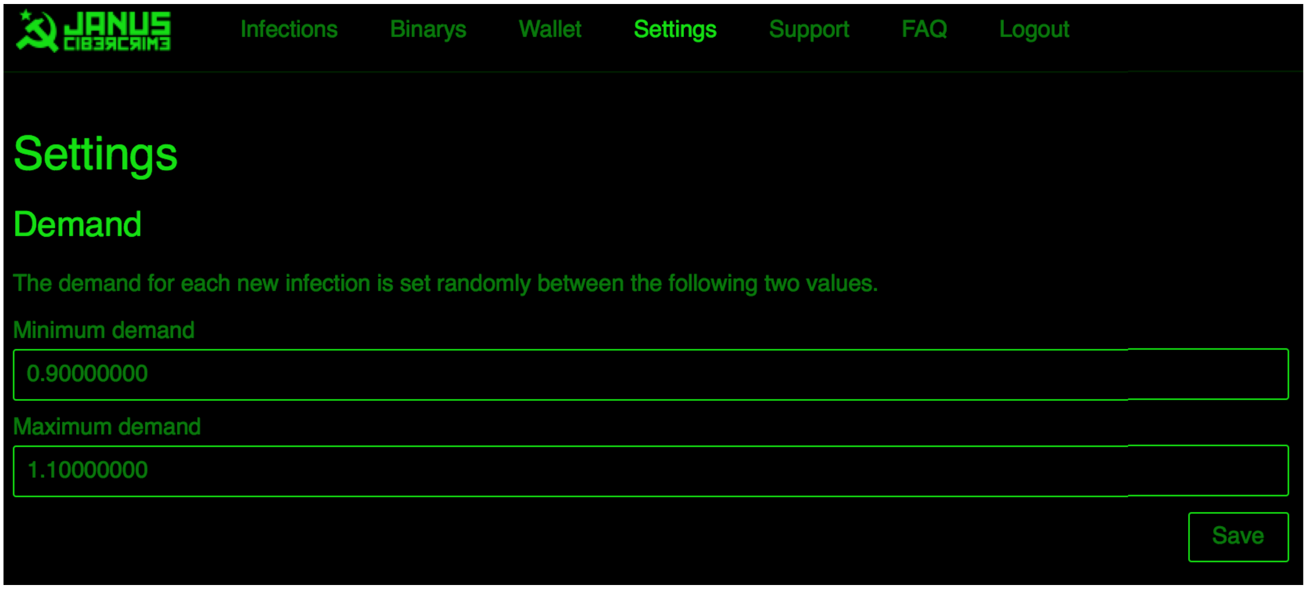
Demand: 0.97882768 Bitcoins

After you made the payment transaction, you have to wait until we manually confirm it. This process usually takes a few hours. In some rare cases some payments need more time to get confirmed. Please refresh this page to see if your payment got confirmed.

Figure 7: Ransom Demand for 0.97 Bitcoin - Worth Approximately $637.00 in July 2016

What’s in it For Them?

As is the case with other similar ransomware offerings (TOX, Ransom32, Encryptor RaaS[1]), the authors or facilitators get a ‘cut’ of the payment. Payment is dictated by a random range set by the user of the portal. The victims will be charged a random amount within this range.



Settings

Demand

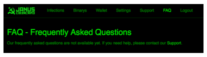
The demand for each new infection is set randomly between the following two values.

Minimum demand: 0.90000000

Maximum demand: 1.10000000

Figure 8: Janus Cybercrime Solutions Payment Settings Screen

The amount of the 'cut' is unclear at the time of writing this, as the FAQ for Petya RaaS is not yet live. In the absence of the FAQ, users are instructed to message support via a form on the Janus Cybercrime portal.



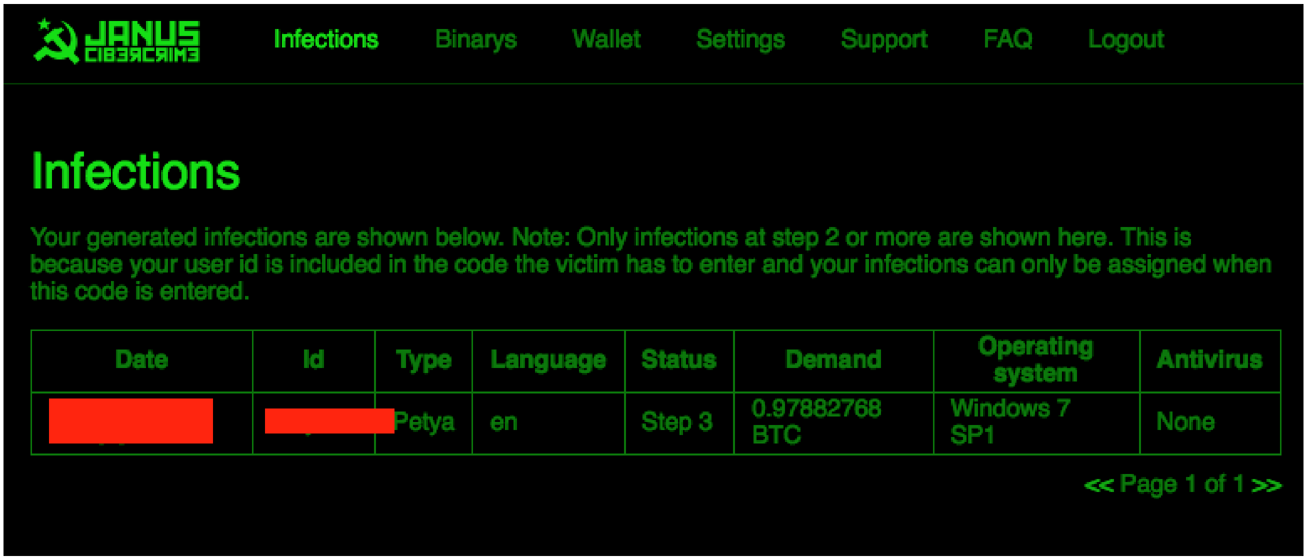
FAQ - Frequently Asked Questions

Our frequently asked questions are not available yet. If you need help, please contact our Support.

Figure 9: Missing 'FAQ' Section for the Petya RaaS Offering

Petya RaaS Administrative Portal

The administrative portal for Petya is very straightforward and 'Tox-like'. The same site page used for registration serves as the management portal and panel for subsequent infections.



Infections

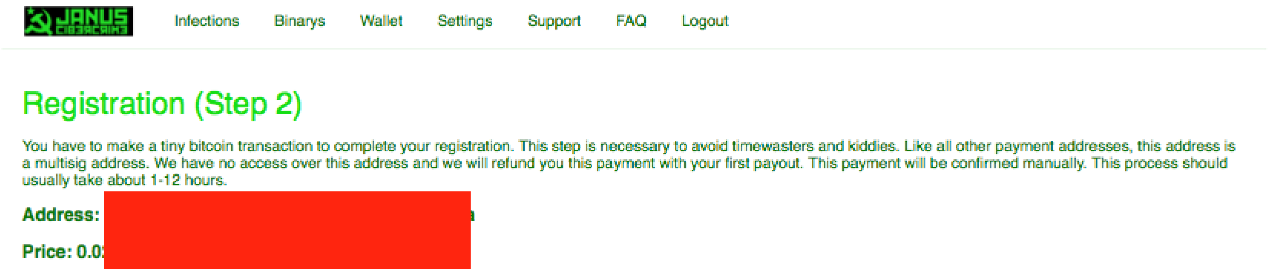
Your generated infections are shown below. Note: Only infections at step 2 or more are shown here. This is because your user id is included in the code the victim has to enter and your infections can only be assigned when this code is entered.

Date	Id	Type	Language	Status	Demand	Operating system	Antivirus
[redacted]	[redacted]	Petya	en	Step 3	0.97882768 BTC	Windows 7 SP1	None

<< Page 1 of 1 >>

Figure 10: Behind the Scenes at Petya RaaS

Registration, however, is not as immediate as the past offerings from Janus. For starters, it is not 100% free. The authors require a small fee which is paid upfront. On their registration page, they position this as a way to weed out the "timewasters and kiddies".



Registration (Step 2)

You have to make a tiny bitcoin transaction to complete your registration. This step is necessary to avoid timewasters and kiddies. Like all other payment addresses, this address is a multisig address. We have no access over this address and we will refund you this payment with your first payout. This payment will be confirmed manually. This process should usually take about 1-12 hours.

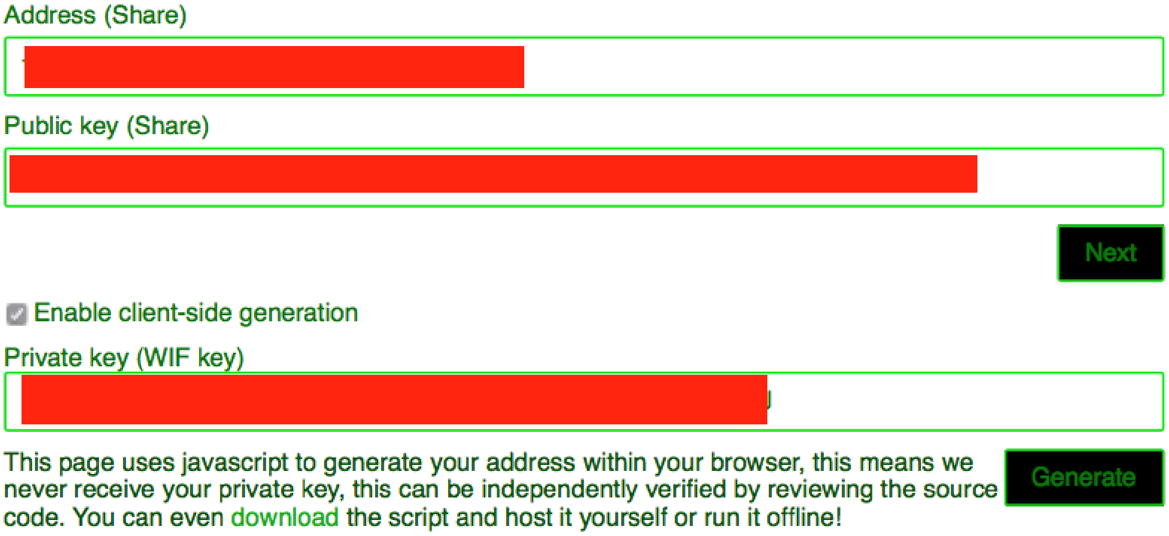
Address: [redacted]

Price: 0.0

Figure 11: Fine Print on Janus Registration Page

The price of the upfront fee fluctuates, as it is based on bitcoin (BTC). That being said, it appears to hover around the $8.00 to $18.00 USD range – a low price which is (in my opinion) certainly well within the reach of the aforementioned "kiddies and timewasters."

In order to register and make payment, you must provide the authors with a valid bitcoin address for payment collection, along with the public key for that address. The system then runs a script to generate your private key for the ransomware.



Address (Share)

[redacted]

Public key (Share)

[redacted]

Next

☑ Enable client-side generation

Private key (WIF key)

[redacted]

This page uses javascript to generate your address within your browser, this means we never receive your private key, this can be independently verified by reviewing the source code. You can even download the script and host it yourself or run it offline!

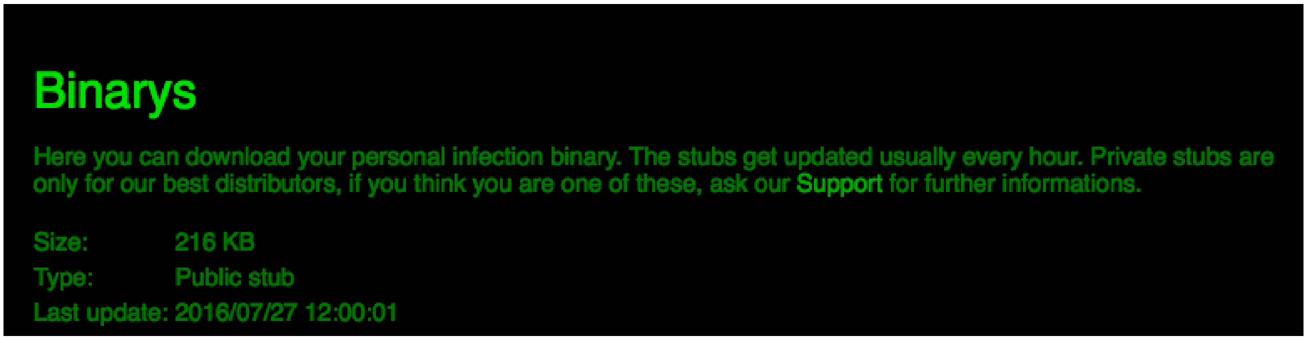
Generate

Figure 12: Entering Registration Information Into the System

Once you are 'in' - a process that takes between one and twelve hours due to manual verification of the bitcoin transfers - you are then able to download binaries, update wallet settings, track infections, contact support and more.

An important note on the binaries themselves: most registrants will be offered the 'public' stub. The private stubs, which are more rare, are reserved for their most active distributors.

The stubs (binaries) are updated daily, possibly multiple times per day, to ensure detection evasion. Even the 'public' stubs vary per user, and as stated, over time.



Binarys

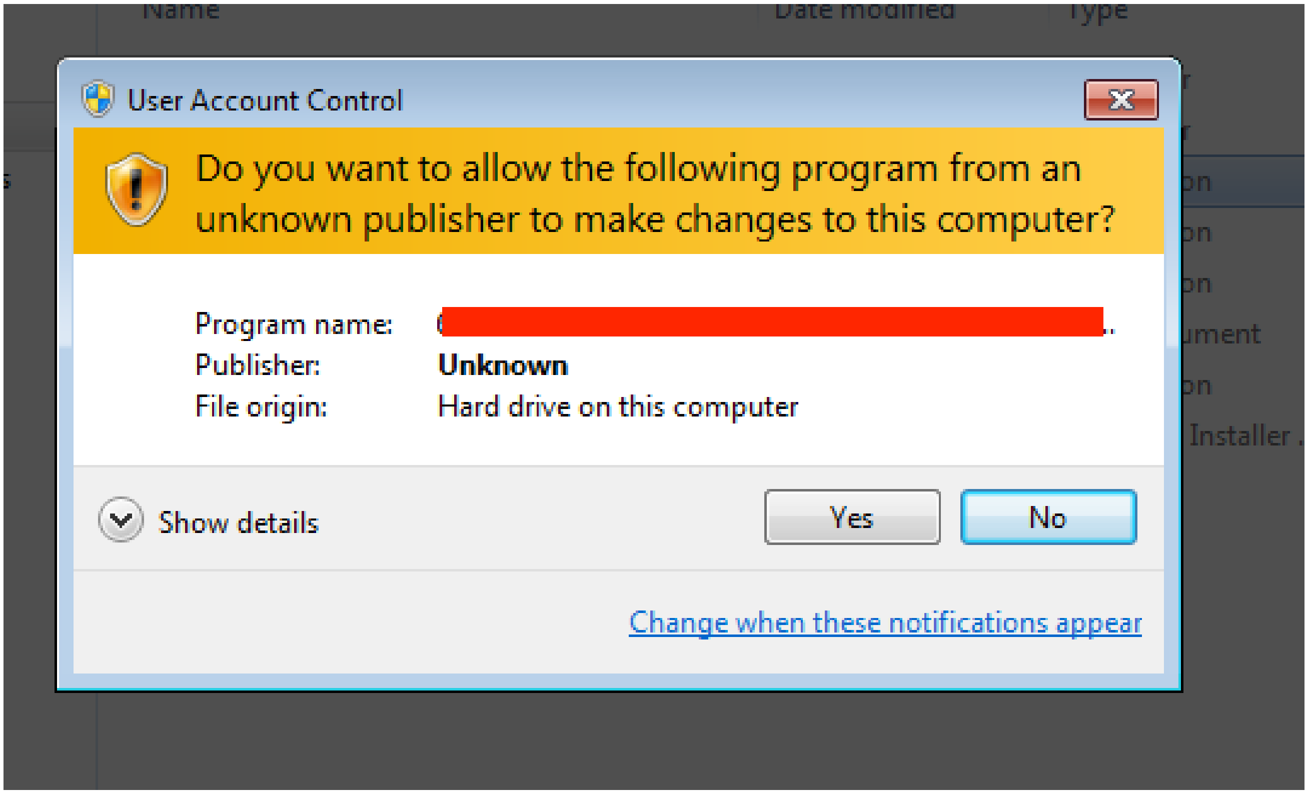
Here you can download your personal infection binary. The stubs get updated usually every hour. Private stubs are only for our best distributors, if you think you are one of these, ask our Support for further informations.

Size:	216 KB
Type:	Public stub
Last update:	2016/07/27 12:00:01

Figure 13: Download Screen for Binaries

Petya vs. Mischa: Stages of Infection

Mischa and Petya infections are handled via the same binary and portal as per previous generations. When Petya is denied administrative privileges by way of UAC controls or otherwise, the Mischa-specific payload is executed. Rather than overwrite the master boot record (MBR), Mischa behaves more like ‘traditional’ ransomware. It will encrypt the local files and then inform the victim how to recover them, in a style mimicking the Petya instructions.

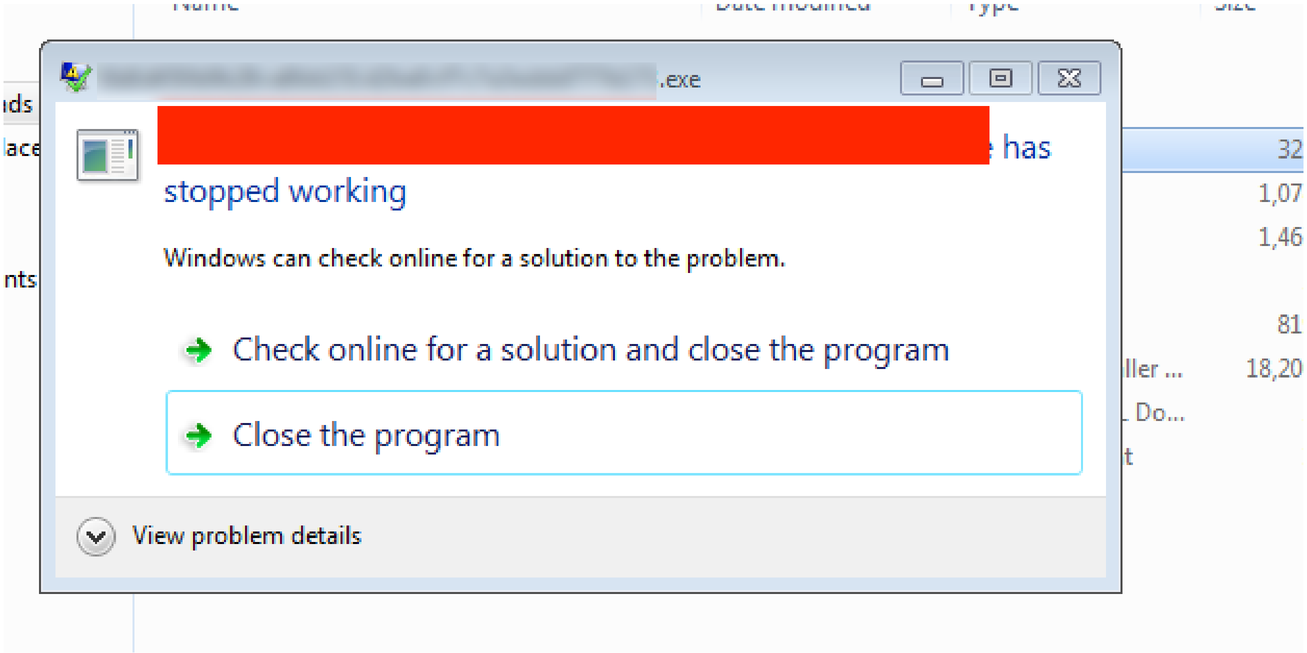


User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: [redacted]
Publisher: **Unknown**
File origin: Hard drive on this computer

Figure 14: User Account Control Notification – Clicking "No" May Earn You a Mischa Infection

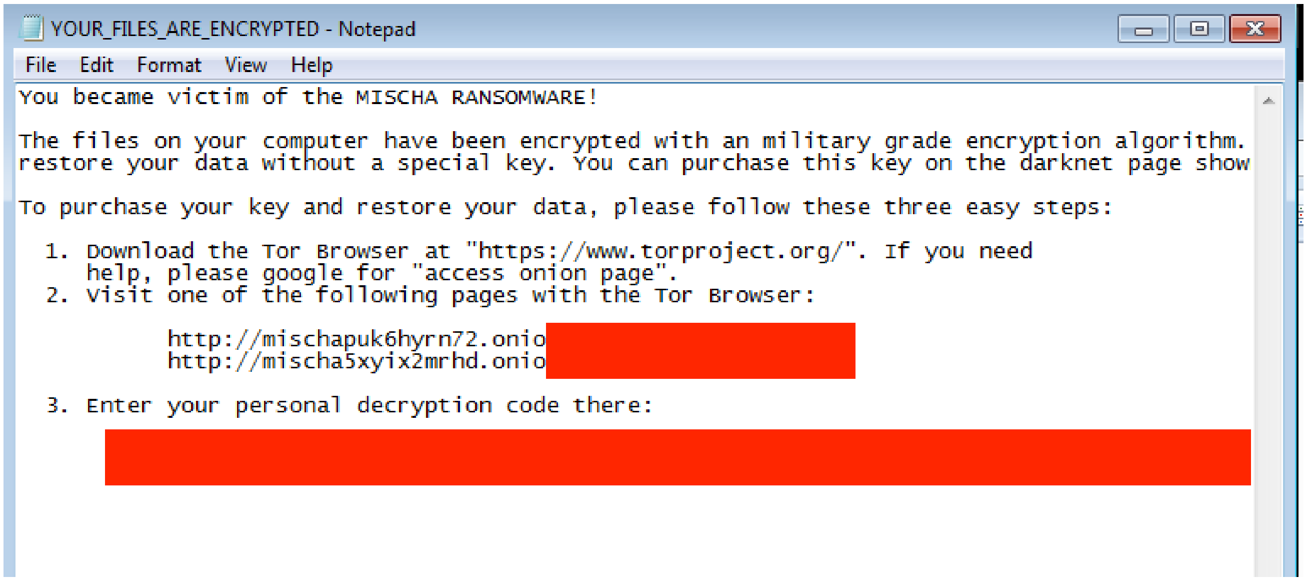


[redacted].exe

[redacted] has stopped working

Windows can check online for a solution to the problem.

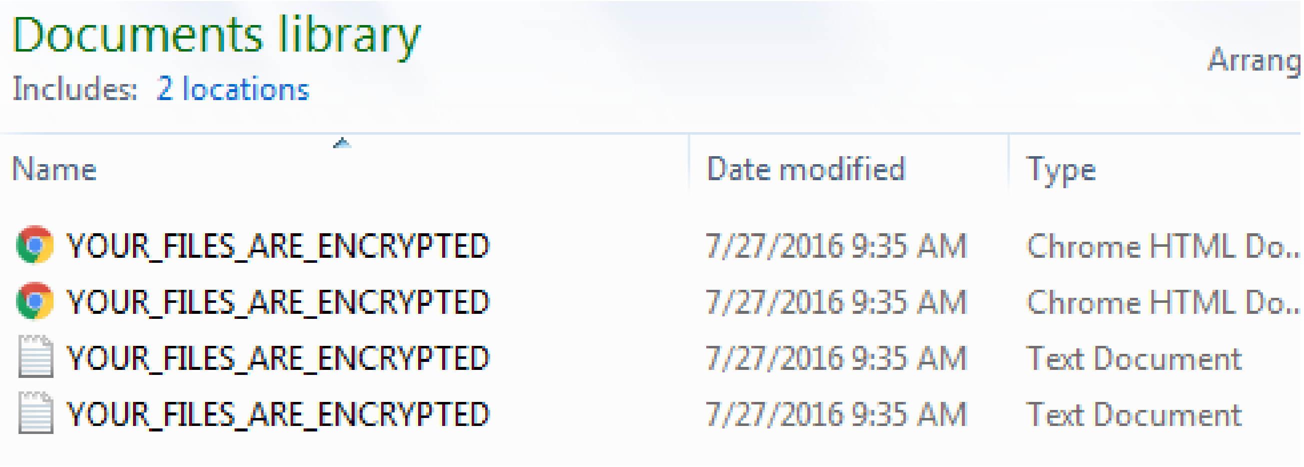
Figure 15: Mischa Malware Detonation In Progress



YOUR_FILES_ARE_ENCRYPTED - Notepad

```
You became victim of the MISCHA RANSOMWARE!

The files on your computer have been encrypted with an military grade encryption algorithm.
restore your data without a special key. You can purchase this key on the darknet page show

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://mischapuk6hyrn72.onio[redacted]
           http://mischa5xyix2mrhd.onio

  3. Enter your personal decryption code there:

       [redacted]
```

Figure 16: Stage 2 of the Mischa Infection



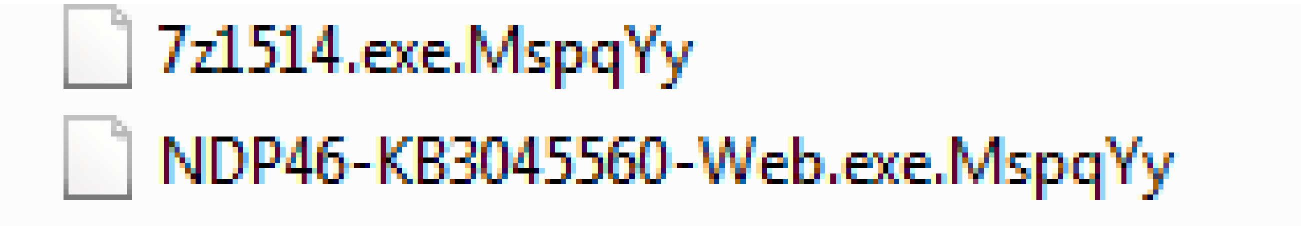
Documents library

Includes: 2 locations

Name	Date modified	Type
YOUR_FILES_ARE_ENCRYPTED	7/27/2016 9:35 AM	Chrome HTML Do..
YOUR_FILES_ARE_ENCRYPTED	7/27/2016 9:35 AM	Chrome HTML Do..
YOUR_FILES_ARE_ENCRYPTED	7/27/2016 9:35 AM	Text Document
YOUR_FILES_ARE_ENCRYPTED	7/27/2016 9:35 AM	Text Document

Figure 17: Victim Document Library, Showing Mischa Ransom Notes

In our analysis, Mischa-encrypted files are given a 'MspqYy' extension.

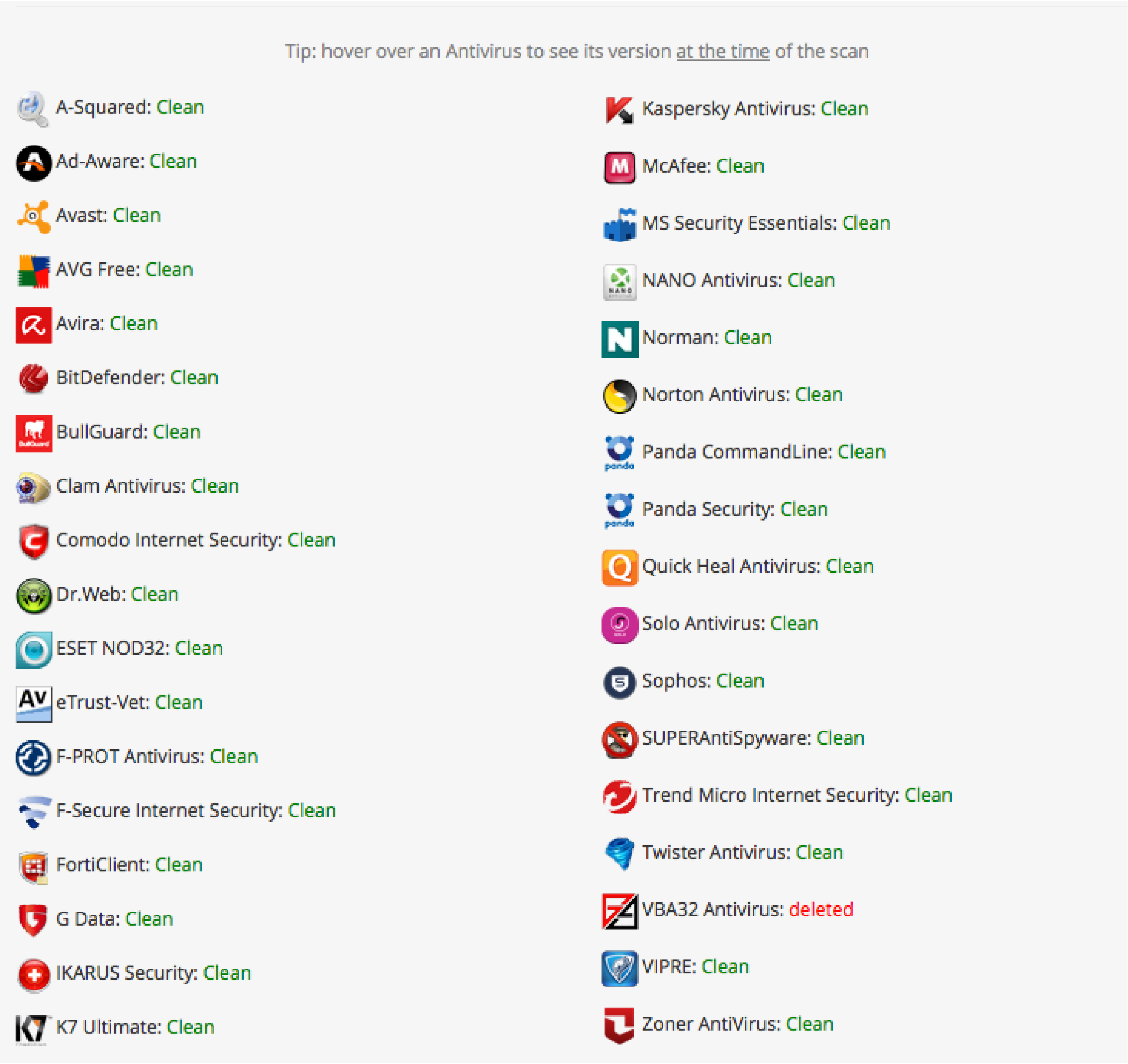


7z1514.exe.MspqYy

NDP46-KB3045560-Web.exe.MspqYy

The Test: CylancePROTECT® vs. Petya and Mischa RaaS Bundle

Even the public stubs are very effective at evading legacy signature-based endpoint products, as you can see in the image below. The fact that the binaries are updated daily, if not more often, further compounds this problem. Casual testing with a popular multi-engine scanning site shows that only one vendor picked up the Petya/ Mischa sample!



Tip: hover over an Antivirus to see its version at the time of the scan

A-Squared: Clean

Ad-Aware: Clean

Avast: Clean

AVG Free: Clean

Avira: Clean

BitDefender: Clean

BullGuard: Clean

Clam Antivirus: Clean

Comodo Internet Security: Clean

Dr.Web: Clean

ESET NOD32: Clean

eTrust-Vet: Clean

F-PROT Antivirus: Clean

F-Secure Internet Security: Clean

FortiClient: Clean

G Data: Clean

IKARUS Security: Clean

K7 Ultimate: Clean

Kaspersky Antivirus: Clean

McAfee: Clean

MS Security Essentials: Clean

NANO Antivirus: Clean

Norman: Clean

Norton Antivirus: Clean

Panda CommandLine: Clean

Panda Security: Clean

Quick Heal Antivirus: Clean

Solo Antivirus: Clean

Sophos: Clean

SUPERAntiSpyware: Clean

Trend Micro Internet Security: Clean

Twister Antivirus: Clean

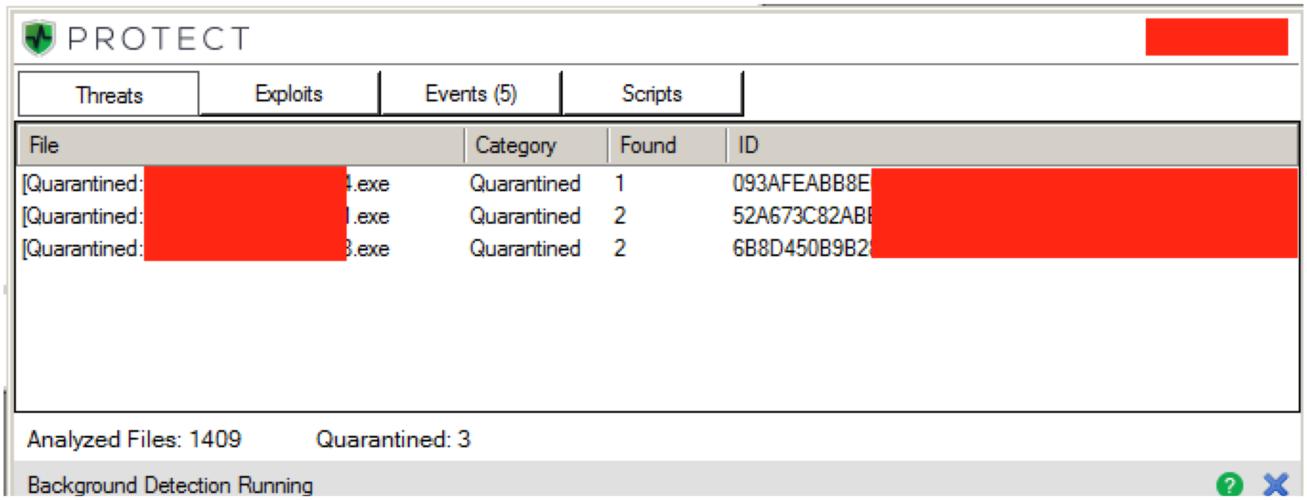
VBA32 Antivirus: deleted

VIPRE: Clean

Zoner AntiVirus: Clean

Figure 18: Multi-Engine Scanning Site Encountering a Malicious Petya/ Mischa Binary

It’s a different story with CylancePROTECT. Our artificial intelligence-based mathematical model was able to prevent the execution of Petya and Mischa right out of the gate, stopping it dead pre-execution. We tested multiple binaries over the course of 48 hours and the Petya/ Mischa bundle was no match for our math-based technology.



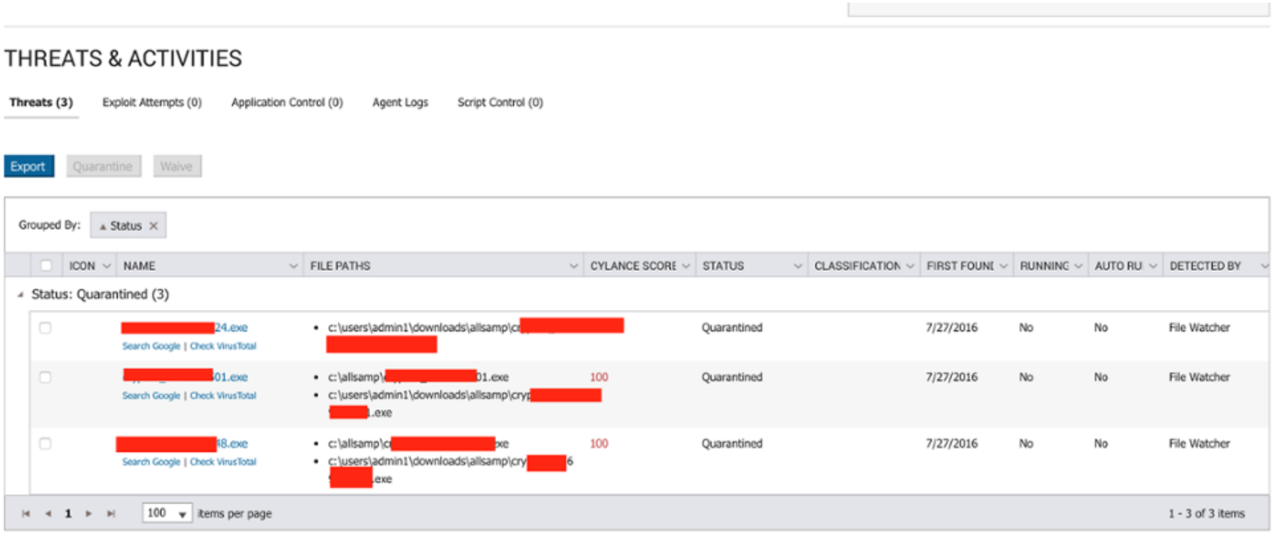
PROTECT [redacted]

File	Category	Found	ID
[Quarantined: [redacted].exe	Quarantined	1	093AFEABB8E[redacted]
[Quarantined: [redacted].exe	Quarantined	2	52A673C82AB[redacted]
[Quarantined: [redacted].exe	Quarantined	2	6B8D450B9B2[redacted]

Analyzed Files: 1409 Quarantined: 3

Background Detection Running

Figure 19: CylancePROTECT Console View, Showing the Detection and Quarantine of Petya/ Mischa Binaries



THREATS & ACTIVITIES

Grouped By: ▲ Status ✕

Status: Quarantined (3)

☐	ICON	NAME	FILE PATHS	CYLANCE SCORE	STATUS	CLASSIFICATION	FIRST FOUN	RUNNING	AUTO RU	DETECTED BY
☐		[redacted]24.exe Search Google | Check VirusTotal	• c:\users\admin1\downloads\allsamp\c[redacted] [redacted]		Quarantined		7/27/2016	No	No	File Watcher
☐		[redacted]01.exe Search Google | Check VirusTotal	• c:\allsamp\[redacted]01.exe • c:\users\admin1\downloads\allsamp\cryp[redacted] [redacted].exe	100	Quarantined		7/27/2016	No	No	File Watcher
☐		[redacted]8.exe Search Google | Check VirusTotal	• c:\allsamp\c[redacted]xe • c:\users\admin1\downloads\allsamp\cry[redacted]6 [redacted].exe	100	Quarantined		7/27/2016	No	No	File Watcher

1 100 items per page 1 - 3 of 3 items

Figure 20: CylancePROTECT Threats and Activities Tab, Showing the Pre-Execution Quarantine of Petya/ Mischa Binaries

Believe the Math!

(NOTE: Sample hashes withheld intentionally.)

[1] Encryptor RaaS was discontinued recently, on 7/6/2016

About Jim Walter

Senior Security Researcher at Cylance

Jim Walter is a Senior Security Researcher at Cylance.

Back