Petya and Mischa for All! The RaaS Boom Expands to Include the Petya/Mischa Combo

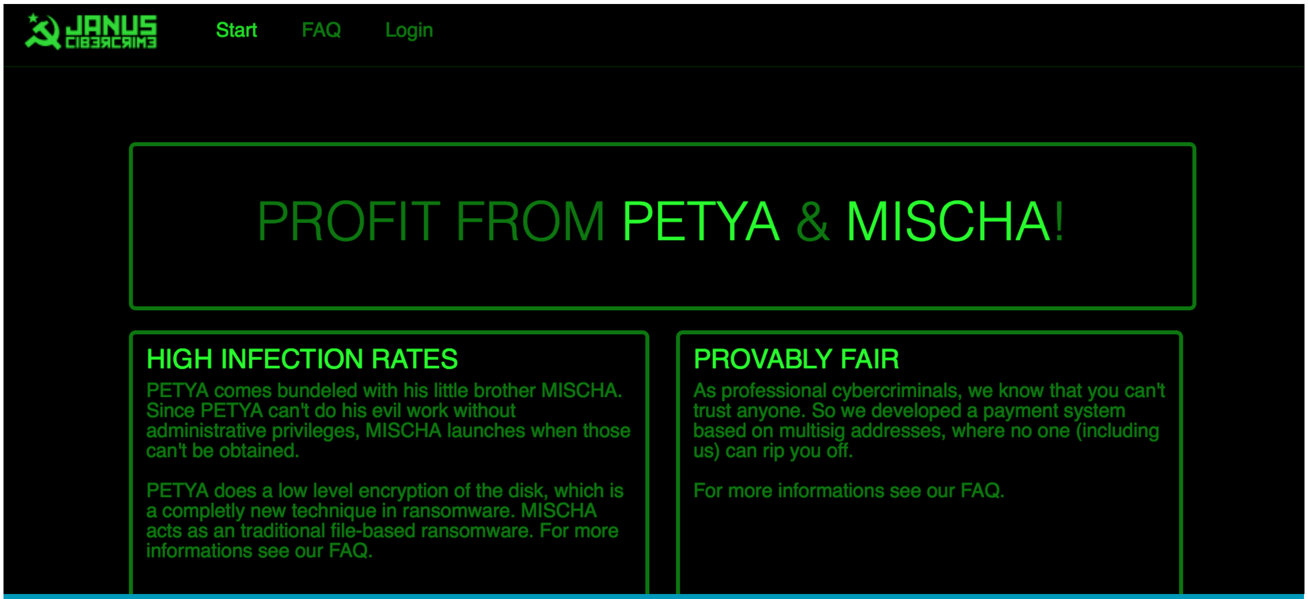
blogs.blackberry.com/en/2016/05/petya-and-mischa-for-all-the-raas-boom-expands-to-include-the-petya-mischa-combo

Jim Walter

FEATURE / 05.19.16 / Jim Walter

News recently broke [1] of the ransomware Trojan Petya coming bundled together with an additional, secondary Trojan. The second Trojan, Mischa, is included as a fallback or failsafe. If the initial Petya installation routine is unable to acquire proper privileges on the system to do its dirty work, Mischa can run instead.

Often, the logged-in user is an employee using a company system and does not have admin rights, or User Account Control (UAC) prompts allow a user to disallow code. This can frustrate the malware authors and ultimately eat into their profits. You can understand why it would then make sense for them to include Mischa as a backup.
Towards the end of April 2016, the public face of Petya and Mischa, self-described ‘professional cybercriminals’ Janus Cybercrime Solutions, began updating various resources. This included the creation of their Twitter handle (@janussec) and updates to their dark web presence.



PROFIT FROM PETYA & MISCHA!

HIGH INFECTION RATES

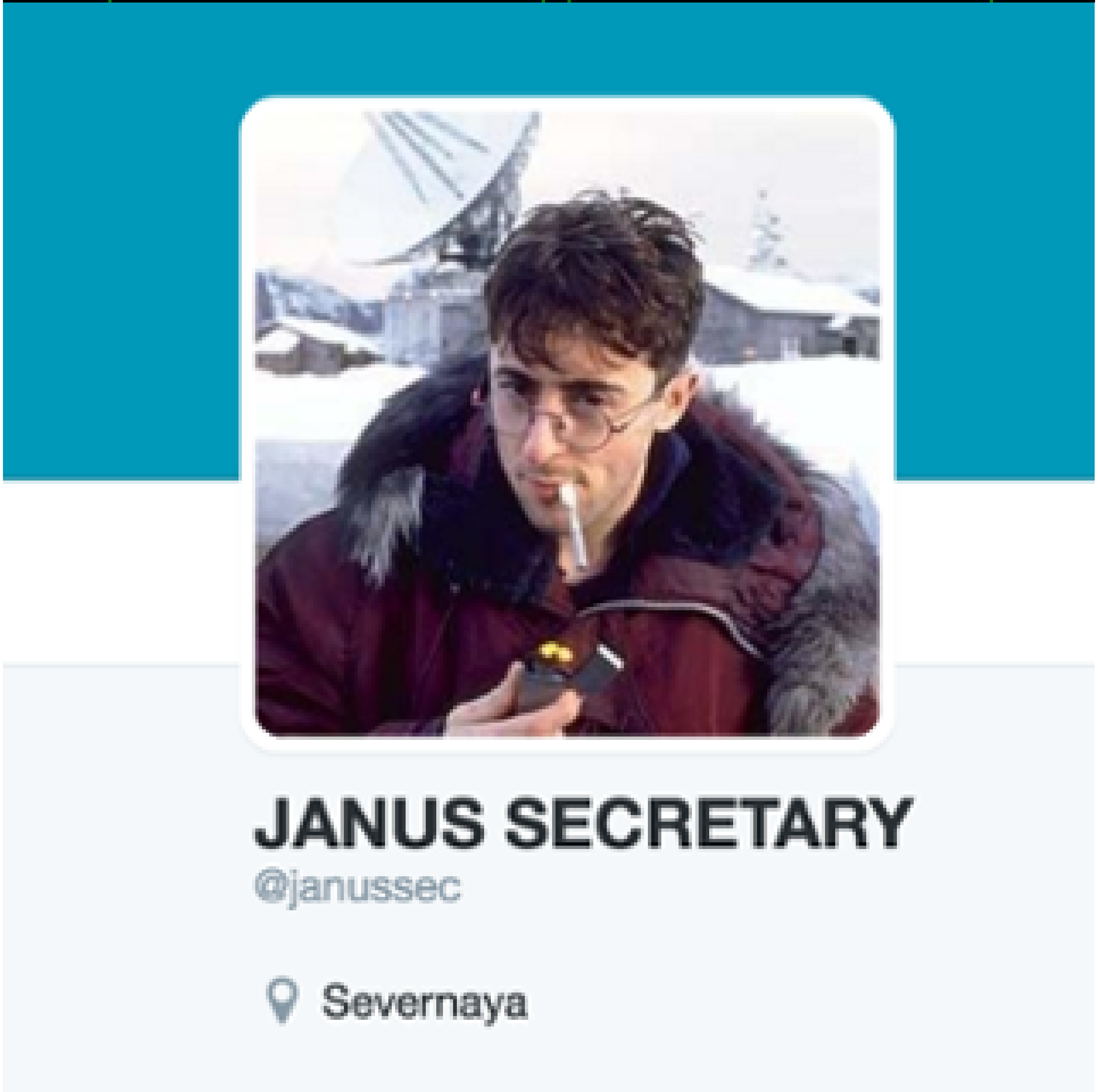
PETYA comes bundeled with his little brother MISCHA. Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained.

PETYA does a low level encryption of the disk, which is a completly new technique in ransomware. MISCHA acts as an traditional file-based ransomware. For more informations see our FAQ.

PROVABLY FAIR

As professional cybercriminals, we know that you can't trust anyone. So we developed a payment system based on multisig addresses, where no one (including us) can rip you off.

For more informations see our FAQ.



JANUS SECRETARY

@janussec

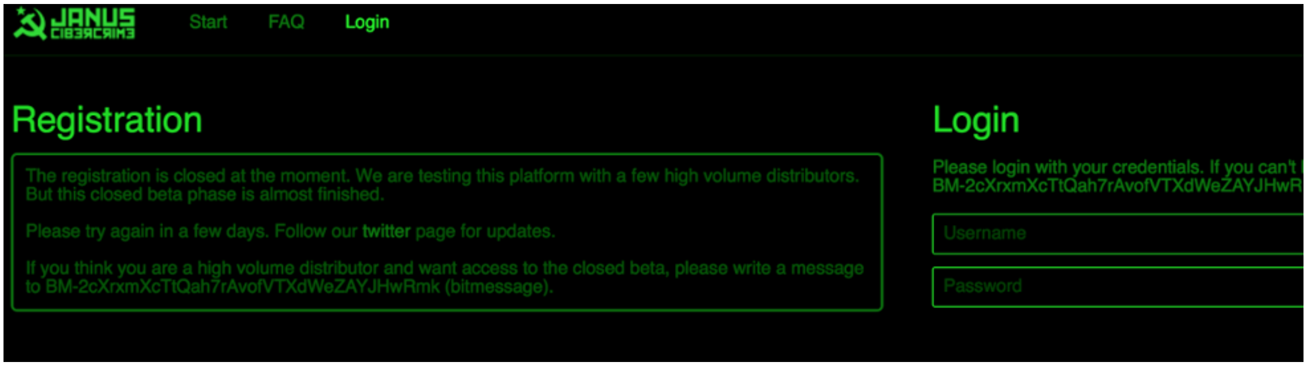
Severnaya

Promotion then began for a closed and exclusive beta phase of the new combined malware. Currently this program is closed off to all but approved “high-volume distributors”. The current message on the site reads as follows:

The registration is closed at the moment. We are testing this platform with a few high volume distributors. But this closed beta phase is almost finished.

Please try again in a few days. Follow our twitter page for updates.

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



Registration

The registration is closed at the moment. We are testing this platform with a few high volume distributors. But this closed beta phase is almost finished.

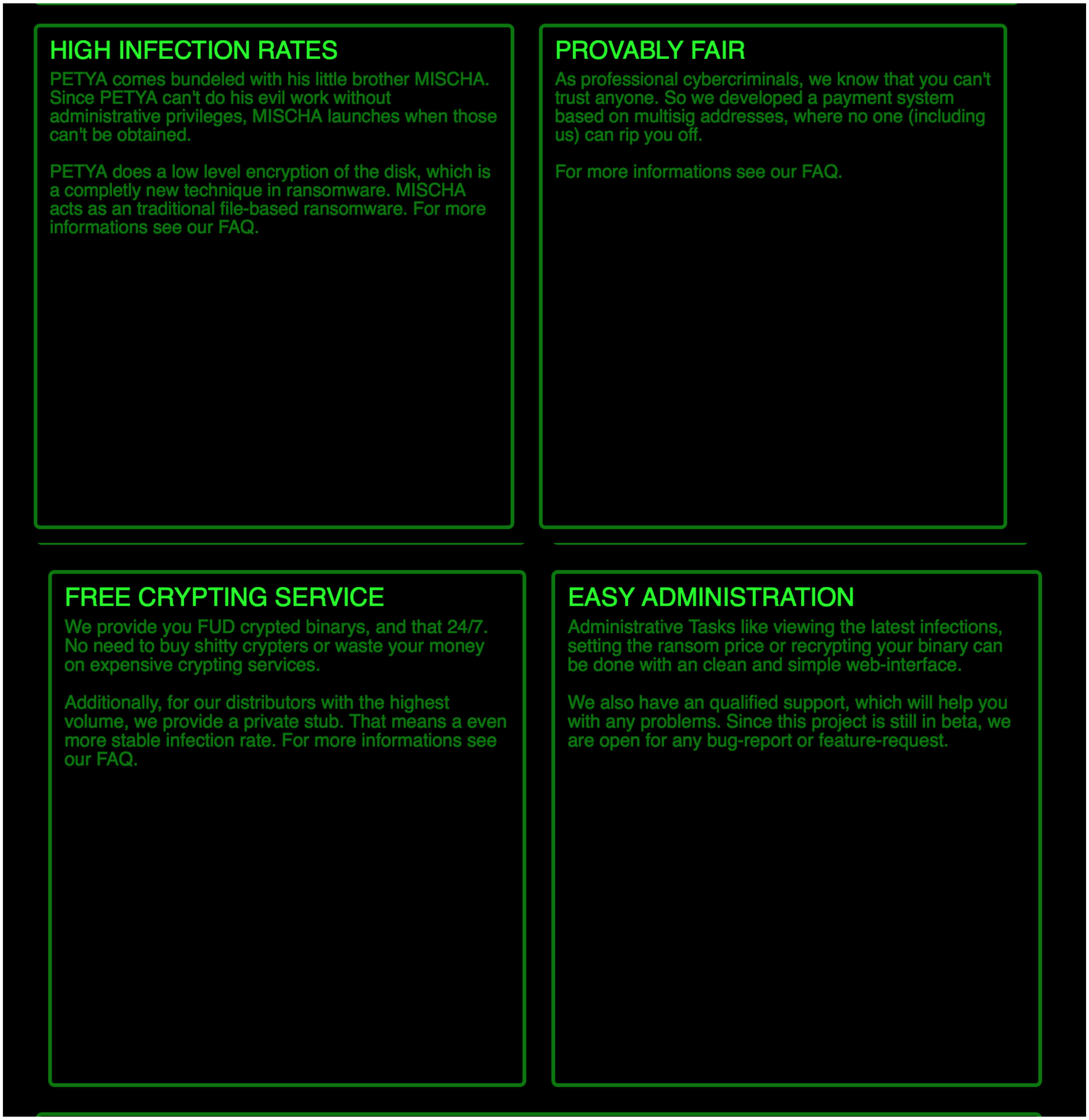
Please try again in a few days. Follow our twitter page for updates.

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

Login

Please login with your credentials. If you can't
BM-2cXrxmXcTtQah7rAvofVTXdWeZAYJHwR

Furthermore, the page highlights the new features of the combined ransomware:



HIGH INFECTION RATES

PETYA comes bundeled with his little brother MISCHA. Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained.

PETYA does a low level encryption of the disk, which is a completly new technique in ransomware. MISCHA acts as an traditional file-based ransomware. For more informations see our FAQ.

PROVABLY FAIR

As professional cybercriminals, we know that you can't trust anyone. So we developed a payment system based on multisig addresses, where no one (including us) can rip you off.

For more informations see our FAQ.

FREE CRYPTING SERVICE

We provide you FUD crypted binarys, and that 24/7. No need to buy shitty crypters or waste your money on expensive crypting services.

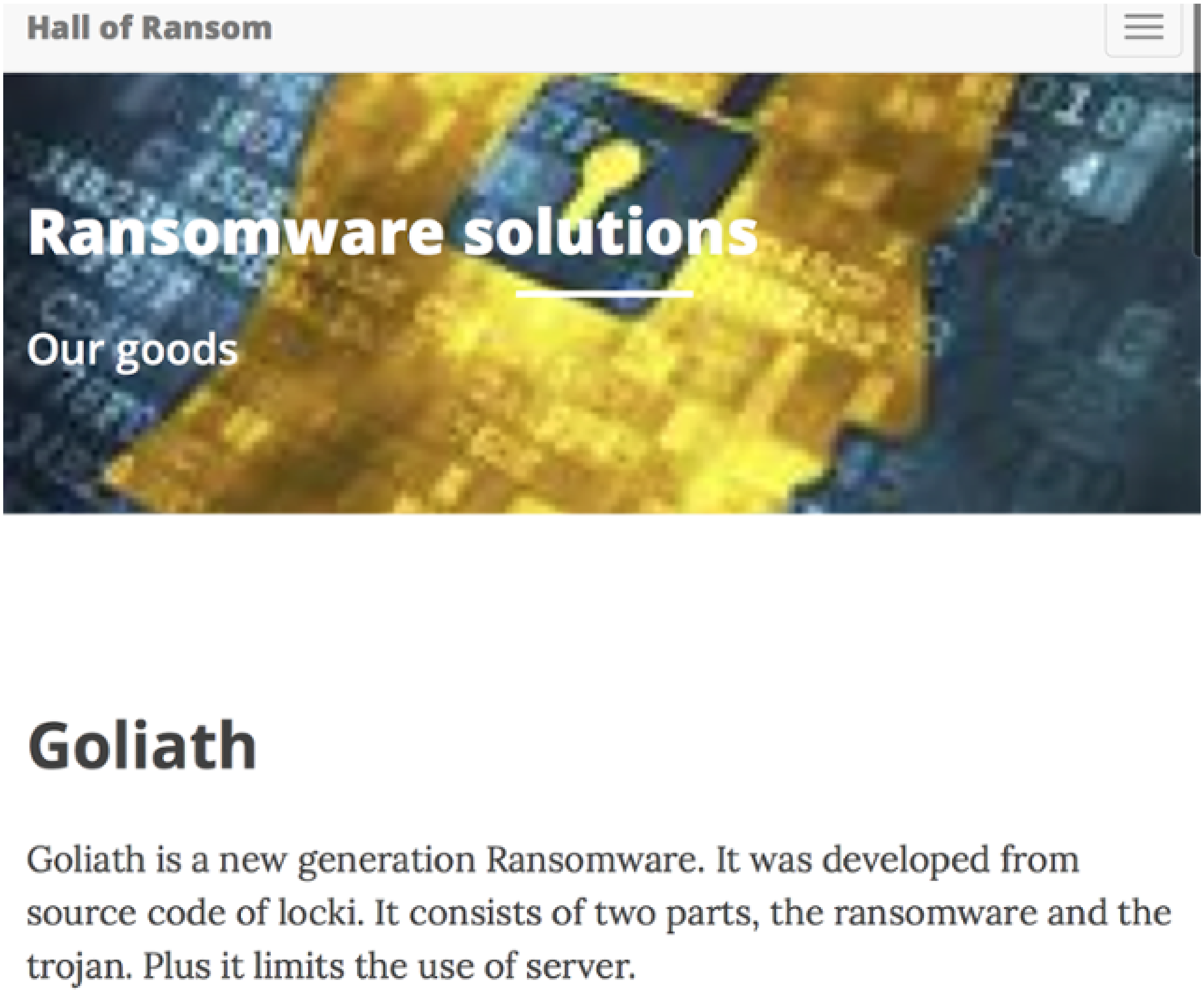
Additionally, for our distributors with the highest volume, we provide a private stub. That means a even more stable infection rate. For more informations see our FAQ.

EASY ADMINISTRATION

Administrative Tasks like viewing the latest infections, setting the ransom price or recrypting your binary can be done with an clean and simple web-interface.

We also have an qualified support, which will help you with any problems. Since this project is still in beta, we are open for any bug-report or feature-request.

Petya is considered by malware experts to be above average in terms of sophistication, which makes it surprising to see it spring up so quickly as a pseudo-public ransomware-as-a-service (RaaS) offering. From a code and execution perspective, it is far beyond previous offerings, including the likes of Tox, Ransom32, and especially the Goliath offering from 'Hall of Ransom'.



Hall of Ransom

Ransomware solutions

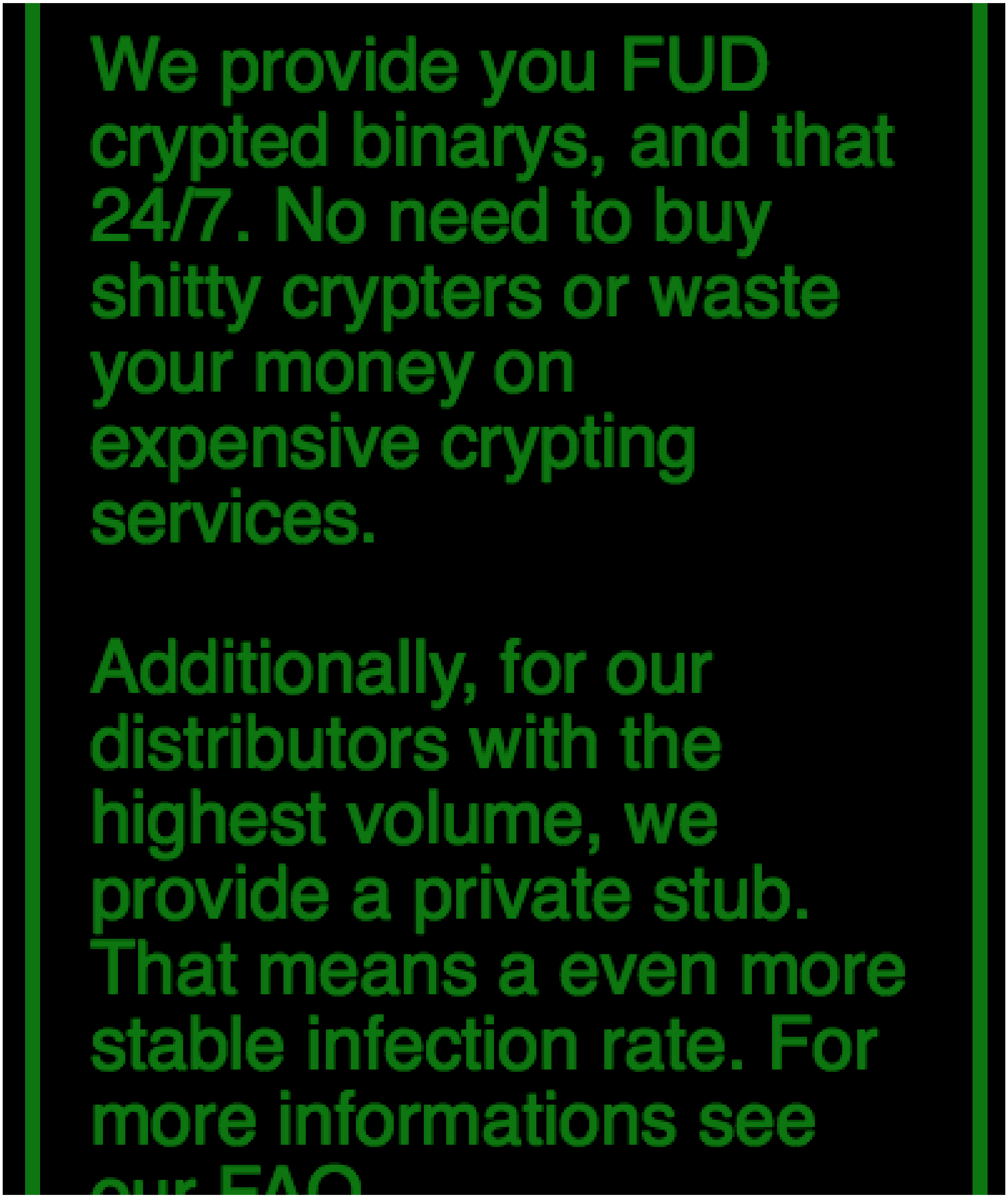
Our goods

Goliath

Goliath is a new generation Ransomware. It was developed from source code of locki. It consists of two parts, the ransomware and the trojan. Plus it limits the use of server.

In addition to the new combined Petya/Mischa offering, it is very important to note the FUD/Evasion offering. For those enrolled, free crypting/FUD services are included. The authors are providing assurance that your binaries will go undetected, ongoing and 24/7. As a bonus, if you are one of their 'high-volume distributors', you will get your own unique stub. This step further assures evasion, as private stubs are 100% unique to those recipients.

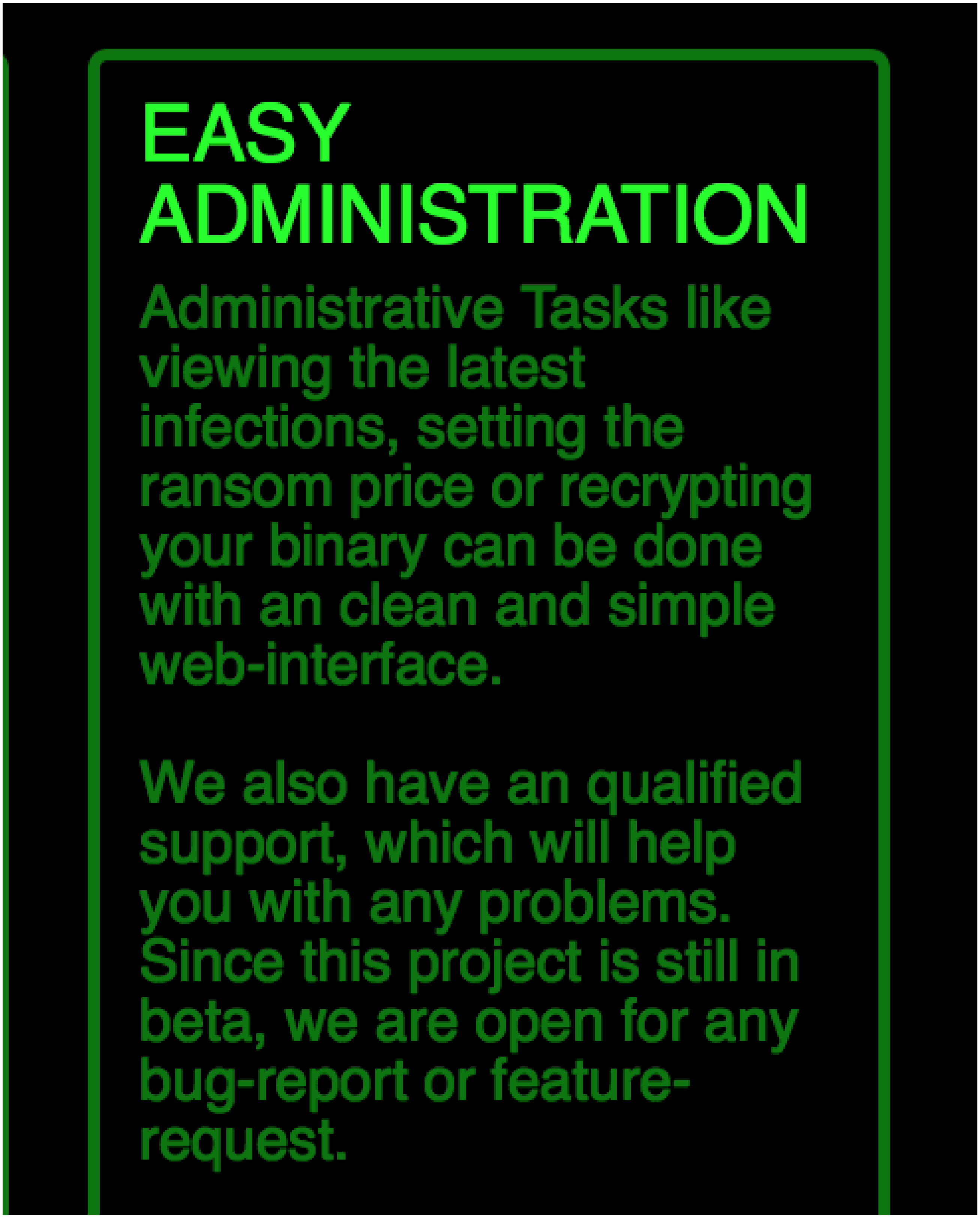
This step helps reduce the amount of 'leakage' of the binaries into the wild, and gives them an advantage, evasion-wise, over the public/non-private stub crypts.



We provide you FUD crypted binarys, and that 24/7. No need to buy shitty crypters or waste your money on expensive crypting services.

Additionally, for our distributors with the highest volume, we provide a private stub. That means a even more stable infection rate. For more informations see our FAQ

Similar to other RaaSofferings, administration duties for the ransomware are handled via a simple web interface. The provided interface gives the ransomware buyer basic administration access, which includes management of payment amounts, victim tracking, binary updating/recrypting and more. You also get full support for any issues that might arise. Consider this as the cybercriminal’s version of a gold-level technical support package.



EASY ADMINISTRATION

Administrative Tasks like viewing the latest infections, setting the ransom price or recrypting your binary can be done with an clean and simple web-interface.

We also have an qualified support, which will help you with any problems. Since this project is still in beta, we are open for any bug-report or feature-request.

Their FAQ provides basic answers to questions around infection, encryption and options around payment:

Petya/ Mischa FAQ Section

is the infection screen shown before Windows starts?

Our system has a strong physical low level encryption, which encrypts all of your data storages, include USB devices. Windows repair programs or other diagnostic tools can't restore any data.

What will happen if I just reinstall my computer?

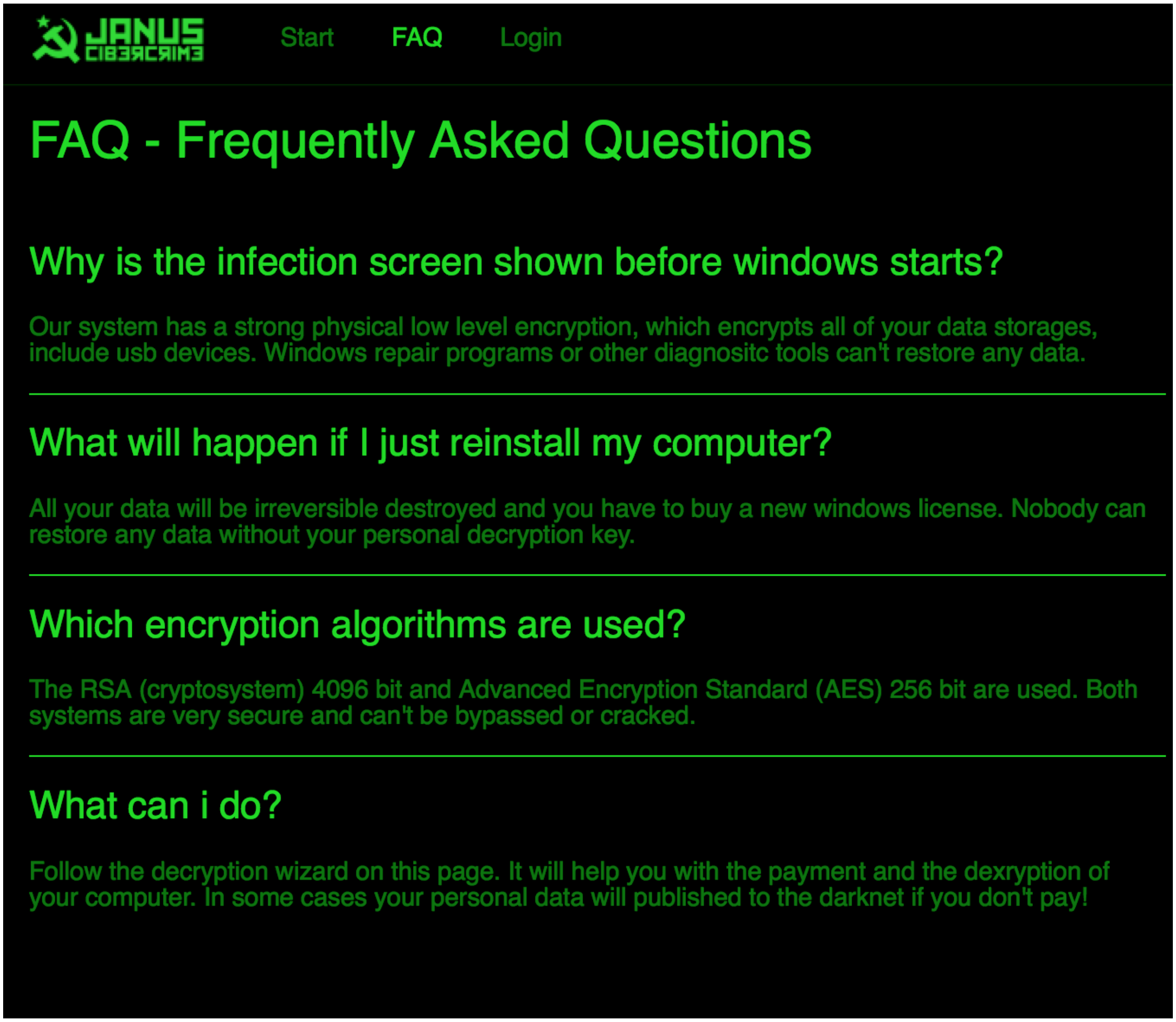
All your data will be irreversible destroyed and you have to buy a new windows license. Nobody can restore any data without your personal decryption key.

Which encryption algorithms are used?

The RSA (cryptosystem) 4096 bit and Advanced Encryption Standard (AES) 256 bit are used. Both systems are very secure and can't be bypassed or cracked.

What can I do?

Follow the decryption wizard on this page. It will help you with the payment and the dexryption of your computer. In some cases your personal data will published to the darknet if you don't pay!



FAQ - Frequently Asked Questions

Why is the infection screen shown before windows starts?

Our system has a strong physical low level encryption, which encrypts all of your data storages, include usb devices. Windows repair programs or other diagnositc tools can't restore any data.

What will happen if I just reinstall my computer?

All your data will be irreversible destroyed and you have to buy a new windows license. Nobody can restore any data without your personal decryption key.

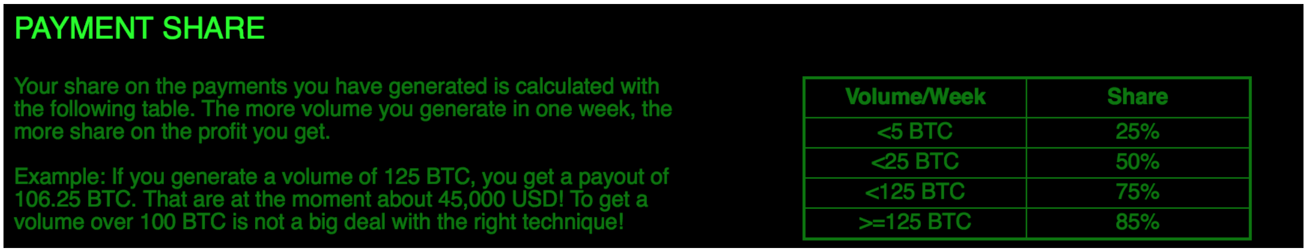
Which encryption algorithms are used?

The RSA (cryptosystem) 4096 bit and Advanced Encryption Standard (AES) 256 bit are used. Both systems are very secure and can't be bypassed or cracked.

What can i do?

Follow the decryption wizard on this page. It will help you with the payment and the dexryption of your computer. In some cases your personal data will published to the darknet if you don't pay!

Revenue and profit sharing is set up to benefit the highest-volume distributors of the ransomware. Again, the fact that Mischa is included as a user-context failsafe makes this goal far more attractive and achievable.



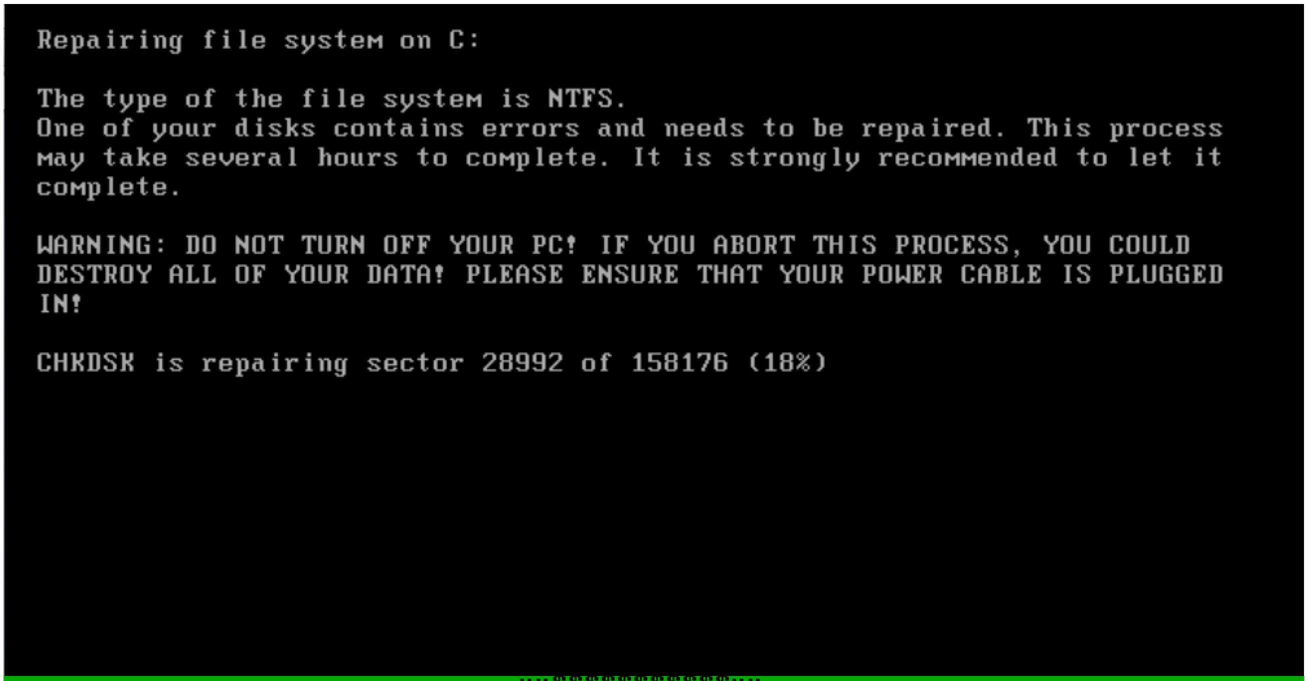
PAYMENT SHARE

Your share on the payments you have generated is calculated with the following table. The more volume you generate in one week, the more share on the profit you get.

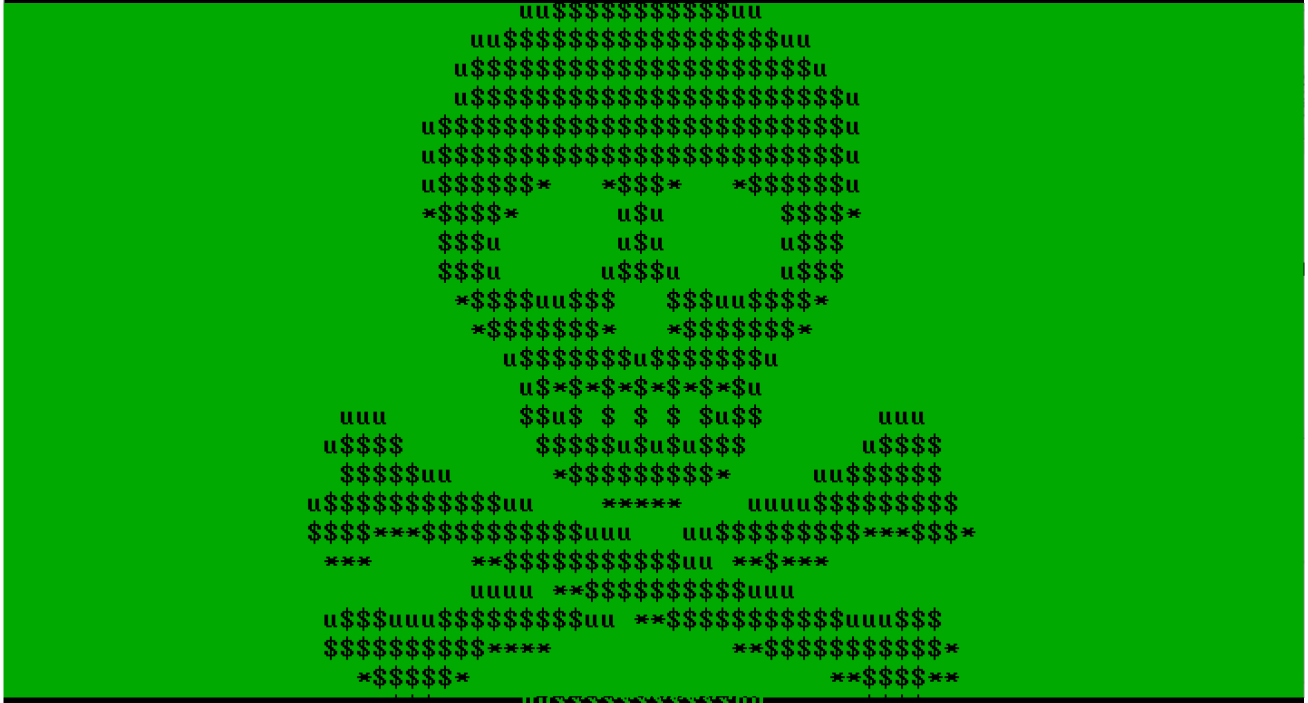
Example: If you generate a volume of 125 BTC, you get a payout of 106.25 BTC. That are at the moment about 45,000 USD! To get a volume over 100 BTC is not a big deal with the right technique!

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

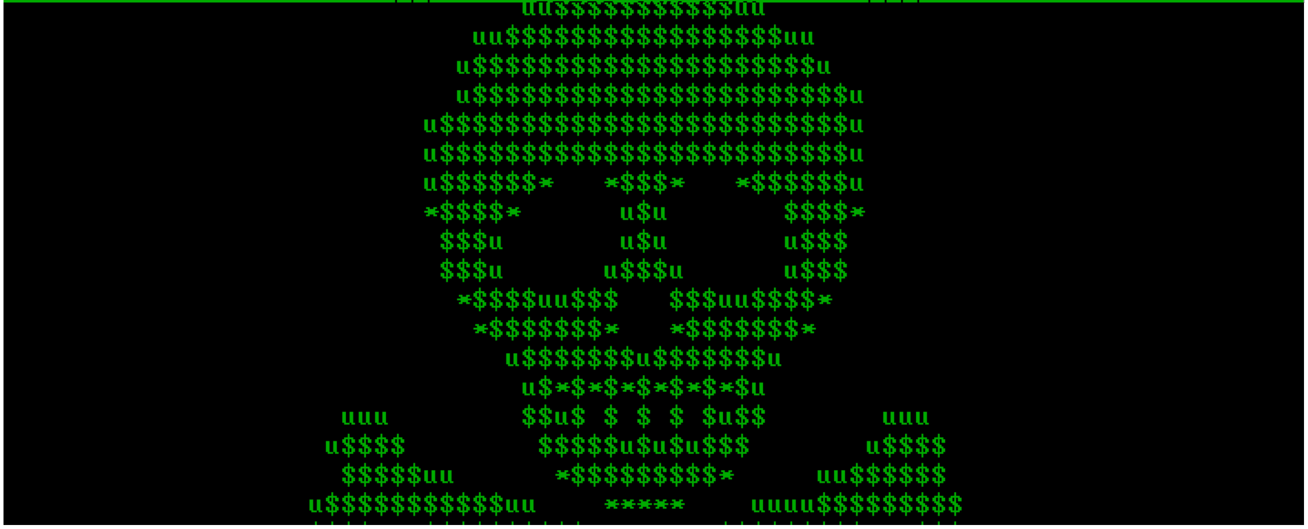
Behavior-wise, the malware behaves in a very similar fashion to prior versions of Petya. A few seconds after execution, the system reboots and the victim is presented with a fake chkdsk screen. Allowing this process to complete, or forcing a reboot results in the familiar skull and crossbones strobe (as shown below), albeit an updated version to match their new color scheme:



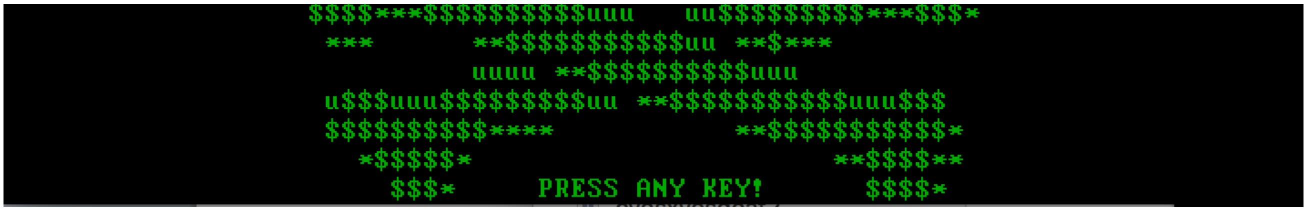
```
Repairing file system on C:

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 28992 of 158176 (18%)
```



```
             uu$$$$$$$$$$$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$$$$u$u$u$$$       u$$$$
  $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
```



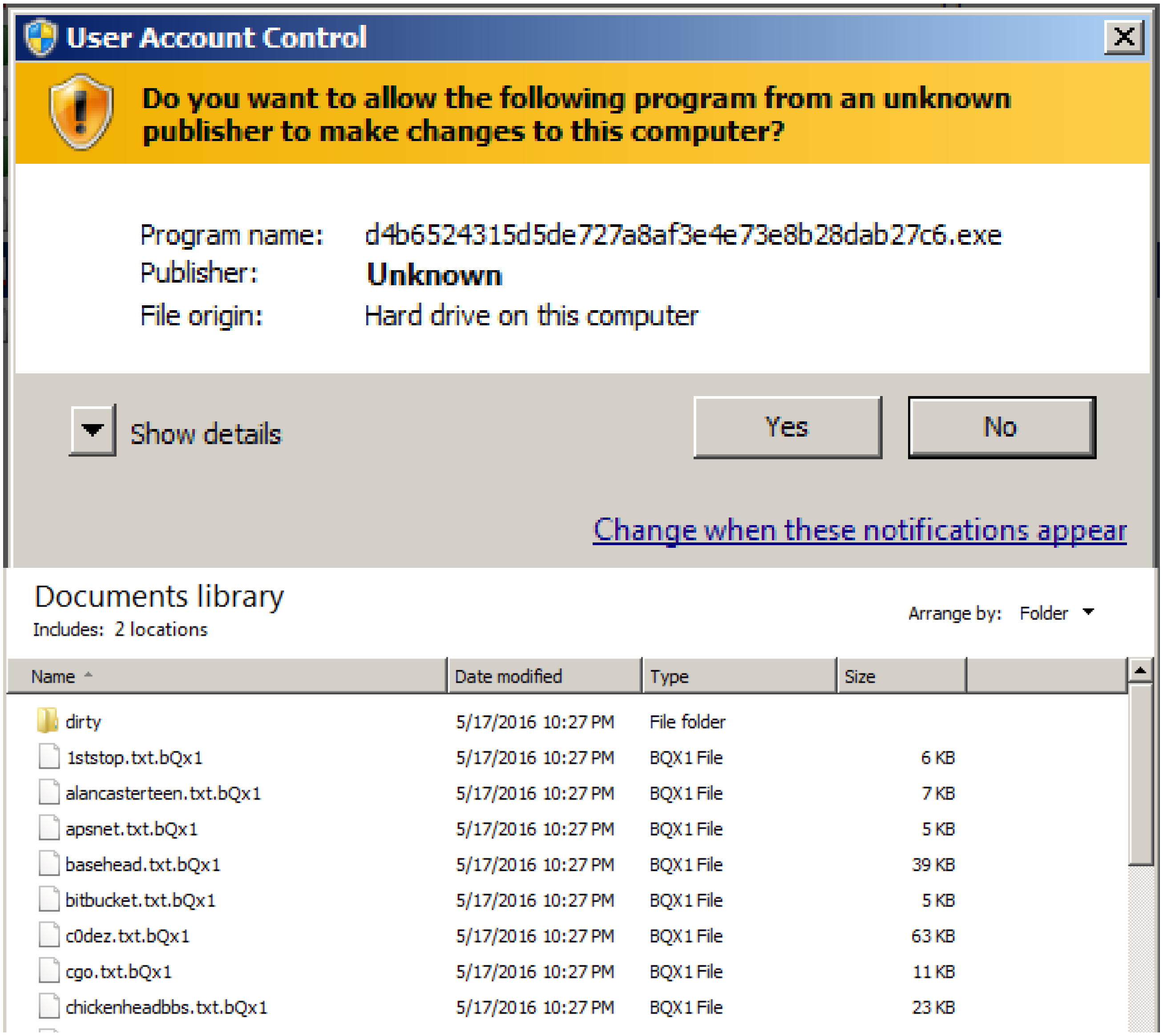
```
             uu$$$$$$$$$$$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$$$$u$u$u$$$       u$$$$
  $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$
```



```
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```

Once again, this is exactly what occurs when Petya is able to get full administrative privileges. When Petya is unable to gain admin rights (due to UAC or other controls), Mischa then deploys.

Mischa infections resemble the more traditional ransomware cases. There are no skulls or fancy special effects. You simply get notified of the encryption via a plain text file on the desktop. All encrypted files are appended with a ‘.bQx1’ extension. The instructions include links for ‘potential’ recovery of the files.



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

Program name: d4b6524315d5de727a8af3e4e73e8b28dab27c6.exe

Publisher: **Unknown**

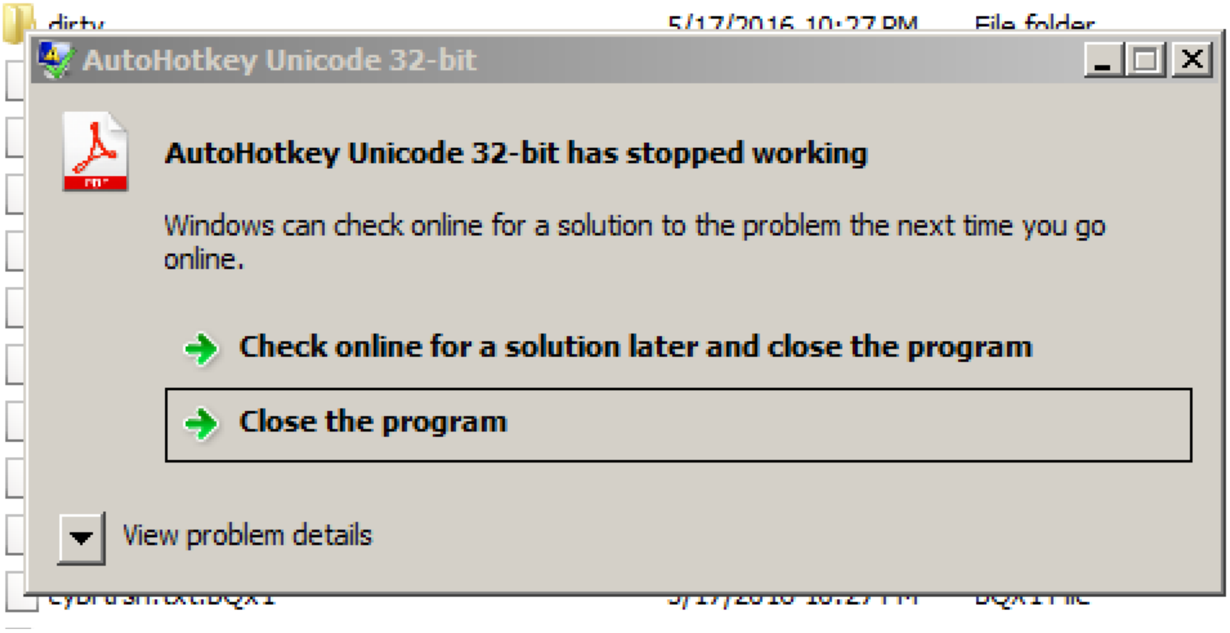
File origin: Hard drive on this computer

Documents library

Includes: 2 locations

Arrange by: Folder

Name	Date modified	Type	Size
dirty	5/17/2016 10:27 PM	File folder	
1ststop.txt.bQx1	5/17/2016 10:27 PM	BQX1 File	6 KB
alancasterteen.txt.bQx1	5/17/2016 10:27 PM	BQX1 File	7 KB
apsnet.txt.bQx1	5/17/2016 10:27 PM	BQX1 File	5 KB
basehead.txt.bQx1	5/17/2016 10:27 PM	BQX1 File	39 KB
bitbucket.txt.bQx1	5/17/2016 10:27 PM	BQX1 File	5 KB
c0dez.txt.bQx1	5/17/2016 10:27 PM	BQX1 File	63 KB
cgo.txt.bQx1	5/17/2016 10:27 PM	BQX1 File	11 KB
chickenheadbbs.txt.bQx1	5/17/2016 10:27 PM	BQX1 File	23 KB



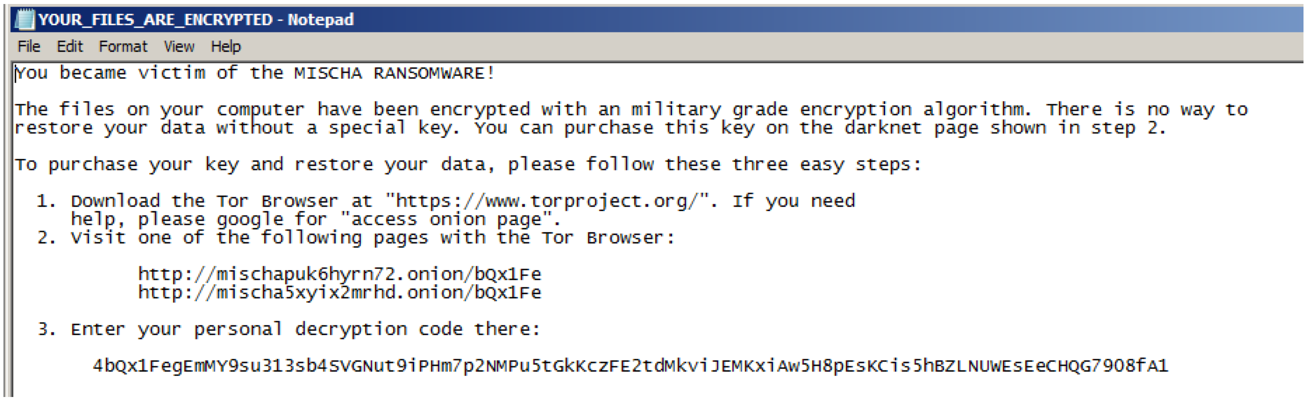
dirty 5/17/2016 10:27 PM File folder

AutoHotkey Unicode 32-bit

AutoHotkey Unicode 32-bit has stopped working

Windows can check online for a solution to the problem the next time you go online.

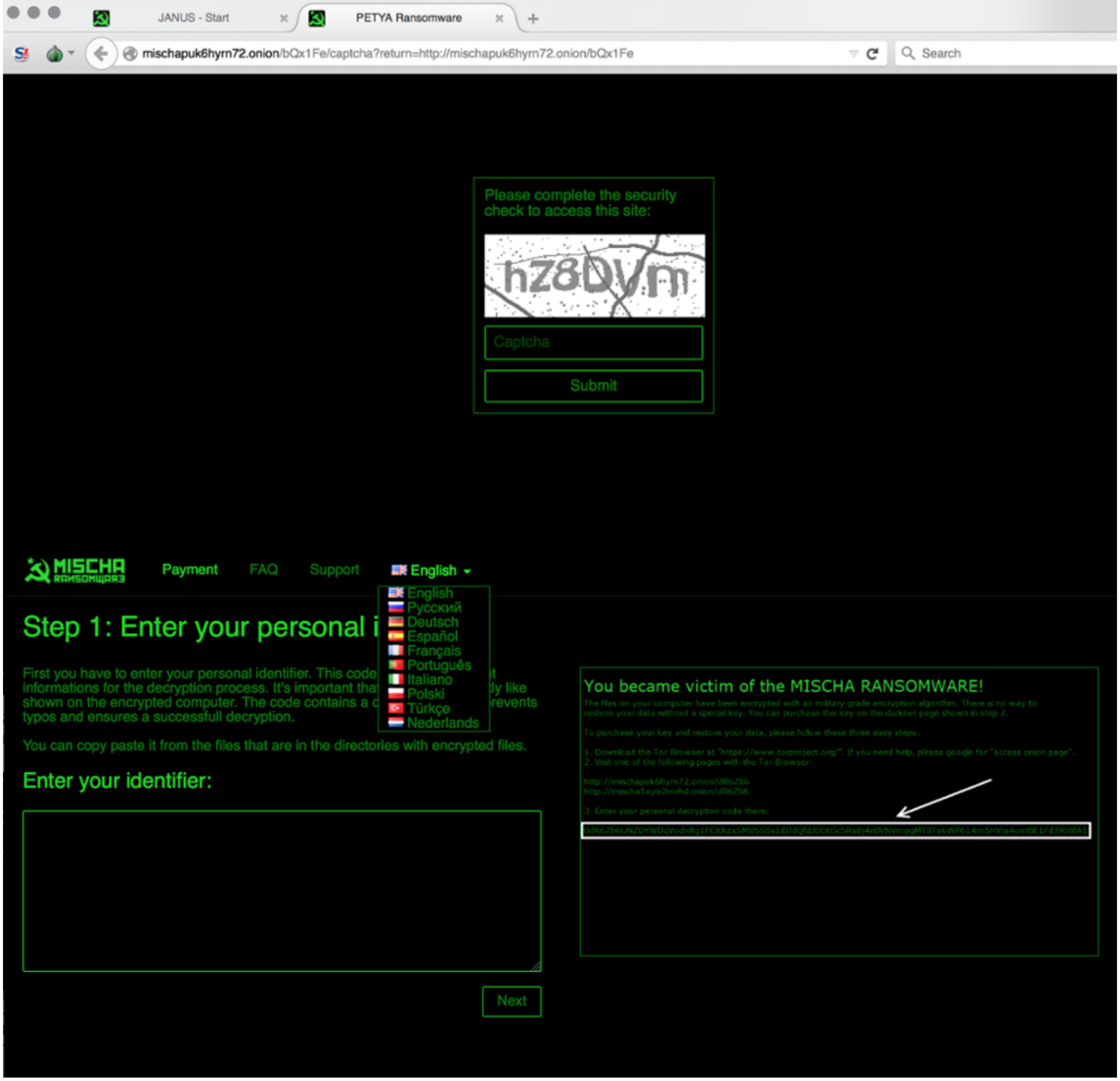
Check online for a solution later and close the program
Close the program
View problem details



YOUR_FILES_ARE_ENCRYPTED - Notepad
File Edit Format View Help

```
You became victim of the MISCHA RANSOMWARE!

The files on 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://mischapuk6hyrn72.onion/bQx1Fe
           http://mischa5xyix2mrhd.onion/bQx1Fe

  3. Enter your personal decryption code there:

       4bQx1FegEmMY9su313sb4SVGNut9iPHm7p2NMPu5tGkKczFE2tdMkviJEMKxiAw5H8pEsKCis5hBZLNUWEsEeCHQG7908fA1
```

The Mischa .onion links lead to an updated Petya Ransomware decryption service page:



Please complete the security check to access this site:

Step 1: Enter your personal i

First you have to enter your personal identifier. This code … t informations for the decryption process. It's important tha … ly like shown on the encrypted computer. The code contains a c … revents typos and ensures a successfull decryption.

You can copy paste it from the files that are in the directories with encrypted files.

Enter your identifier:

You became victim of the MISCHA RANSOMWARE!

The files on 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:

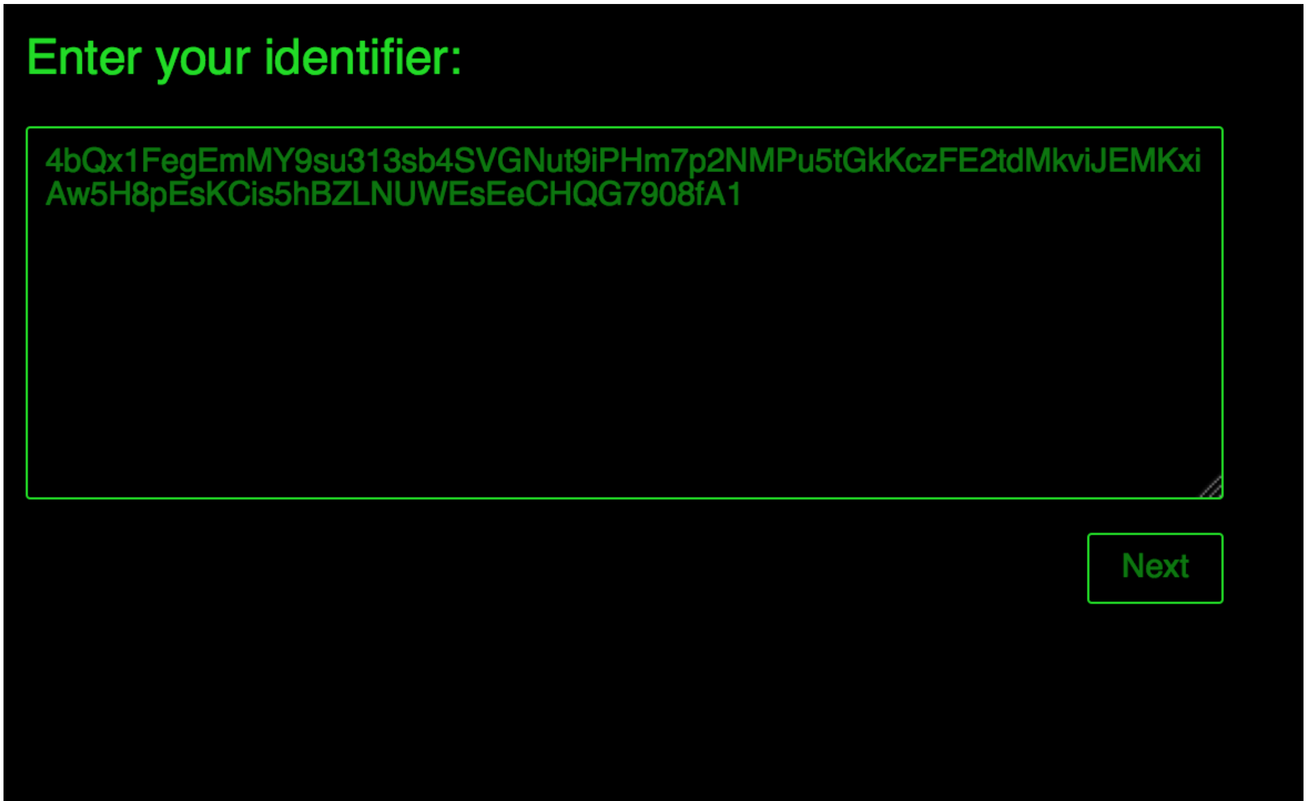
1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

http://mischapuk6hyrn72.onion/dR6Zb6
http://mischa5xyix2mrhd.onion/dR6Zb6

3. Enter your personal decryption code there:

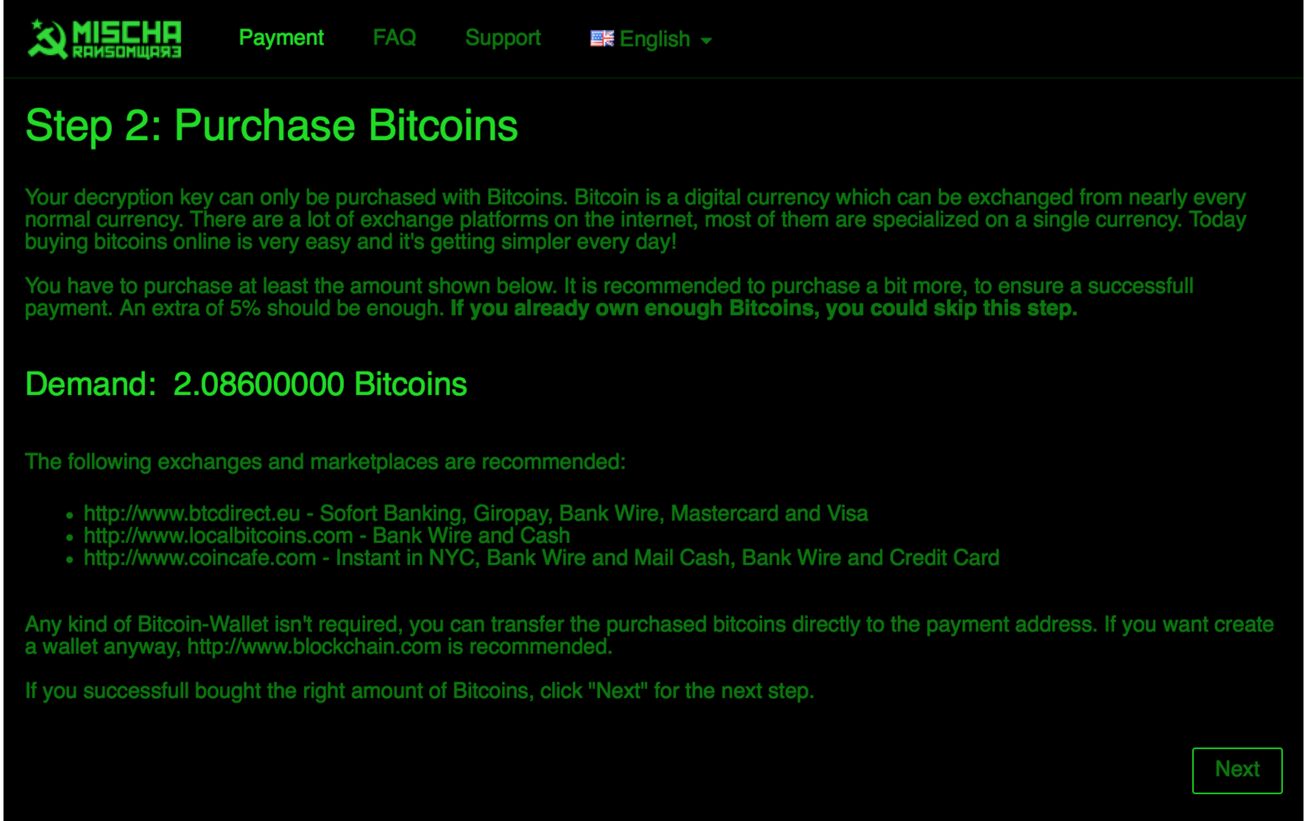
0dR6Zb6UNZDYWDqVodnRg1FCKRzxSMVSSSs1dDJdQfdJDDtGcSRs8j4eDVNVmpgMT8Tx6WP614m5HYta4ontBE1FdJ908fA1

When entering the personal decryption code, you are presented with details on how to purchase bitcoins (BTC), and shown the amount demanded. In the example above, the Mischa decryption price is 2.08600000 BTC, which is roughly $947.00 USD.



Enter your identifier:

```
4bQx1FegEmMY9su313sb4SVGNut9iPHm7p2NMPu5tGkKczFE2tdMkviJEMKxi
Aw5H8pEsKCis5hBZLNUWEsEeCHQG7908fA1
```



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.**

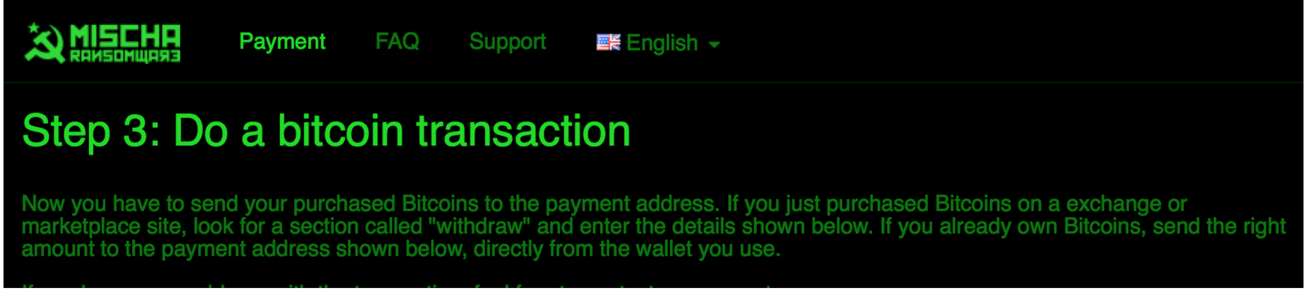
Demand: 2.08600000 Bitcoins

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

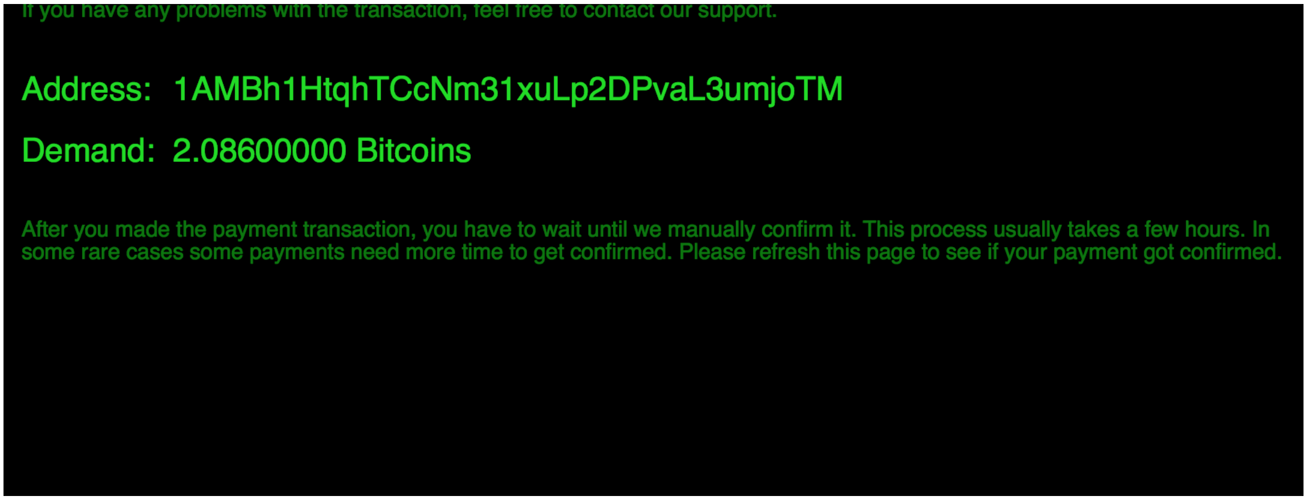
Any kind of Bitcoin-Wallet isn't required, you can transfer the purchased bitcoins directly to the payment address. If you want create a wallet anyway, http://www.blockchain.com is recommended.

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



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: 1AMBh1HtqhTCcNm31xuLp2DPvaL3umjoTM

Demand: 2.08600000 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.

The BTC wallet cited in our example is: **1AMBh1HtqhTCcNm31xuLp2DPvaL3umjoTM**

It is highly likely that the payment wallets are processed though several layers of obfuscation (washing). The wallet above currently holds 0.00 (no funds) with no attached transactions, according to Blockchain.

Analysis on the service side of this is ongoing. We will update this blog as new developments become available.

Detection

One sample has been circulated in multiple recent blogs and articles:

SHA256: d4b6524315d5de727a8af3e4e73e8b28dab27c62fd0a6a7a891460061c2f3d60

Upon analysis of this file, we came across a few other samples that are similar/ directly related.

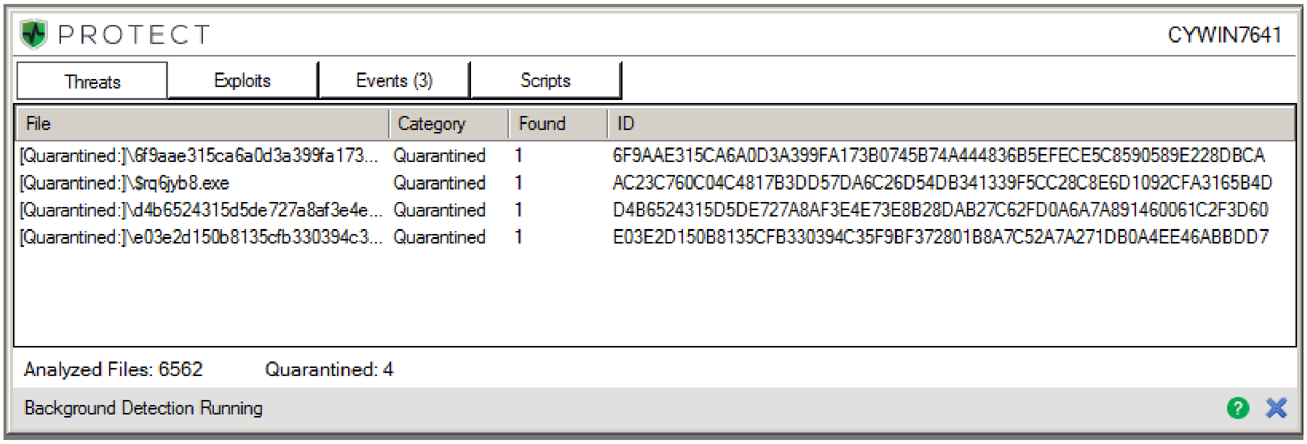
Note: Compilation dates on all these are as follows:

d4b6524315d5de727a8af3e4e73e8b28dab27c62fd0a6a7a891460061c2f3d60
3/27/2016
6f9aae315ca6a0d3a399fa173b0745b74a444836b5efece5c8590589e228dbca
3/27/2016
e03e2d150b8135cfb330394c35f9bf372801b8a7c52a7a271db0a4ee46abbdd7
3/27/2016

CylancePROTECT® vs. Petya and Mischa

CylancePROTECT is able to detect and prevent execution on 100% of the binaries from this particular malware family - even with the malware authors' guarantee of 24/7 FUD and evasion. This level of detection does not exist with the more traditional, signature-based AV technologies.

Here are the CylancePROTECT detection results for the prior-noted binaries. As you can see, CylancePROTECT detected and quarantined each malicious binary, pre-execution:



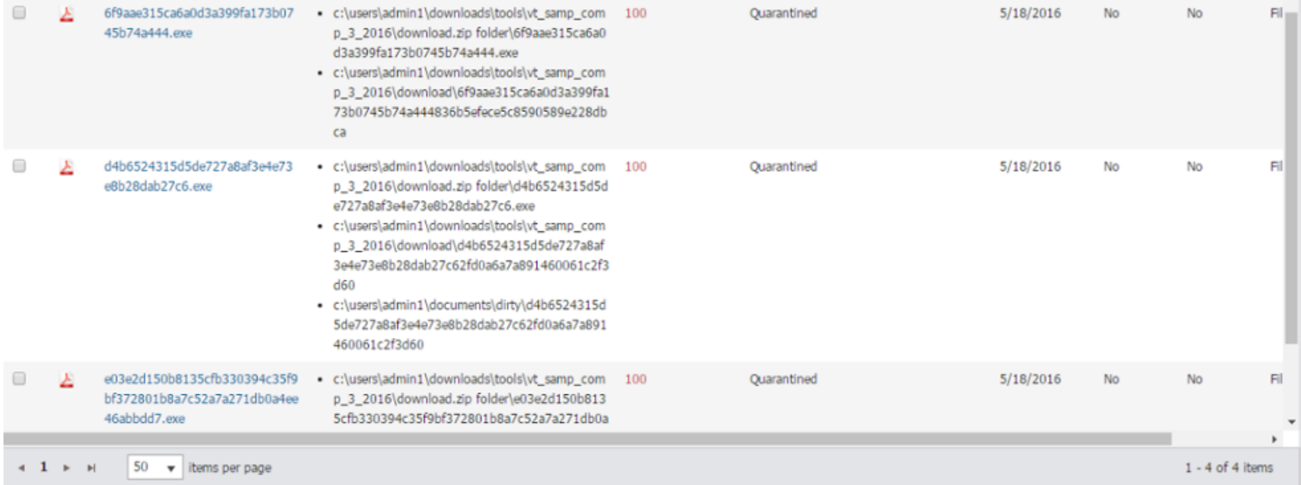
PROTECT

CYWIN7641

File	Category	Found	ID
[Quarantined:]\6f9aae315ca6a0d3a399fa173...	Quarantined	1	6F9AAE315CA6A0D3A399FA173B0745B74A444836B5EFECE5C8590589E228DBCA
[Quarantined:]\$rq6jyb8.exe	Quarantined	1	AC23C760C04C4817B3DD57DA6C26D54DB341339F5CC28C8E6D1092CFA3165B4D
[Quarantined:]\d4b6524315d5de727a8af3e4e...	Quarantined	1	D4B6524315D5DE727A8AF3E4E73E8B28DAB27C62FD0A6A7A891460061C2F3D60
[Quarantined:]\e03e2d150b8135cfb330394c3...	Quarantined	1	E03E2D150B8135CFB330394C35F9BF372801B8A7C52A7A271DB0A4EE46ABBDD7

Analyzed Files: 6562 Quarantined: 4

Background Detection Running



□	6f9aae315ca6a0d3a399fa173b0745b74a444.exe	• c:\users\admin1\downloads\tools\vt_samp_comp_3_2016\download.zip folder\6f9aae315ca6a0d3a399fa173b0745b74a444.exe • c:\users\admin1\downloads\tools\vt_samp_comp_3_2016\download\6f9aae315ca6a0d3a399fa173b0745b74a444836b5efece5c8590589e228dbca	100	Quarantined	5/18/2016	No	No	Fil
□	d4b6524315d5de727a8af3e4e73e8b28dab27c6.exe	• c:\users\admin1\downloads\tools\vt_samp_comp_3_2016\download.zip folder\d4b6524315d5de727a8af3e4e73e8b28dab27c6.exe • c:\users\admin1\downloads\tools\vt_samp_comp_3_2016\download\d4b6524315d5de727a8af3e4e73e8b28dab27c62fd0a6a7a891460061c2f3d60 • c:\users\admin1\documents\dirty\d4b6524315d5de727a8af3e4e73e8b28dab27c62fd0a6a7a891460061c2f3d60	100	Quarantined	5/18/2016	No	No	Fil
□	e03e2d150b8135cfb330394c35f9bf372801b8a7c52a7a271db0a4ee46abbdd7.exe	• c:\users\admin1\downloads\tools\vt_samp_comp_3_2016\download.zip folder\e03e2d150b8135cfb330394c35f9bf372801b8a7c52a7a271db0a	100	Quarantined	5/18/2016	No	No	Fil

Offerings like the Petya/Mischa combo are sure to flourish and become far more prevalent and accessible. Advanced, artificial intelligence based AV solutions are now required to provide ongoing and preventative protection.

Believe the Math!

[1] http://www.securityweek.com/upgraded-petya-malware-installs-additional-ransomware

About Jim Walter

Senior Security Researcher at Cylance

Jim Walter is a Senior Security Researcher at Cylance.

Back