RANSOMWARE

WHAT YOU NEED TO KNOW

JULY 20, 2016

Check Point
SOFTWARE TECHNOLOGIES LTD.

TABLE OF CONTENTS

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

RANSOMWARE: WHAT YOU NEED TO KNOW

In recent years, there has been a surge of ransomware. It's been reported all over security blogs, tech websites and in the news. It doesn't seem to stop; in fact, it seems to be getting worse.

Cryptolocker, the first famous ransomware, was observed in the wild in 2013. From then until the end of 2015, there were only a few active ransomware variants. Some of these variants were weak enough that it was possible to decrypt files without paying ransom. The infection methods were limited.

While quite a lot of variants have been created since then, many of them either don't persist in infecting users or run a low profile campaign. A good example is TeslaCrypt, an infamous ransomware whose authors released a master key for anyone to use. In other cases, new ransomware variants – even ones that are widely distributed and constantly make headlines – are quickly found to have bugs when it comes to implementing the encryption itself, such as the recently published decryption tool for Jigsaw ransomware. These flaws are either fixed in a newer version, or the ransomware is abandoned.

There seems to be a fairly large difference between the top-tier of ransomware, which usually maintain several active campaigns, and the trendy new ransomware variants which come and go. In this article, we provide an overview of the exciting world of ransomware. We highlight the differences between the most prevalent ransomware families, and present several smaller yet unique ransomwares. We also present several methods for protection and mitigation.

KNOW YOUR ENEMY

THE FOUNDING FATHERS

While not the first ransomware ever observed in the wild, these are the ones who blazed the trail.

Cryptolocker

First observed in the wild in September 2013, Cryptolocker quickly became the leader of the ransomware trend.

After it completes the encryption, Cryptolocker displays a prompt that informs the victims their files have been 'taken hostage', and demands a ransom payment for the encryption keys that enable the files to be decrypted.

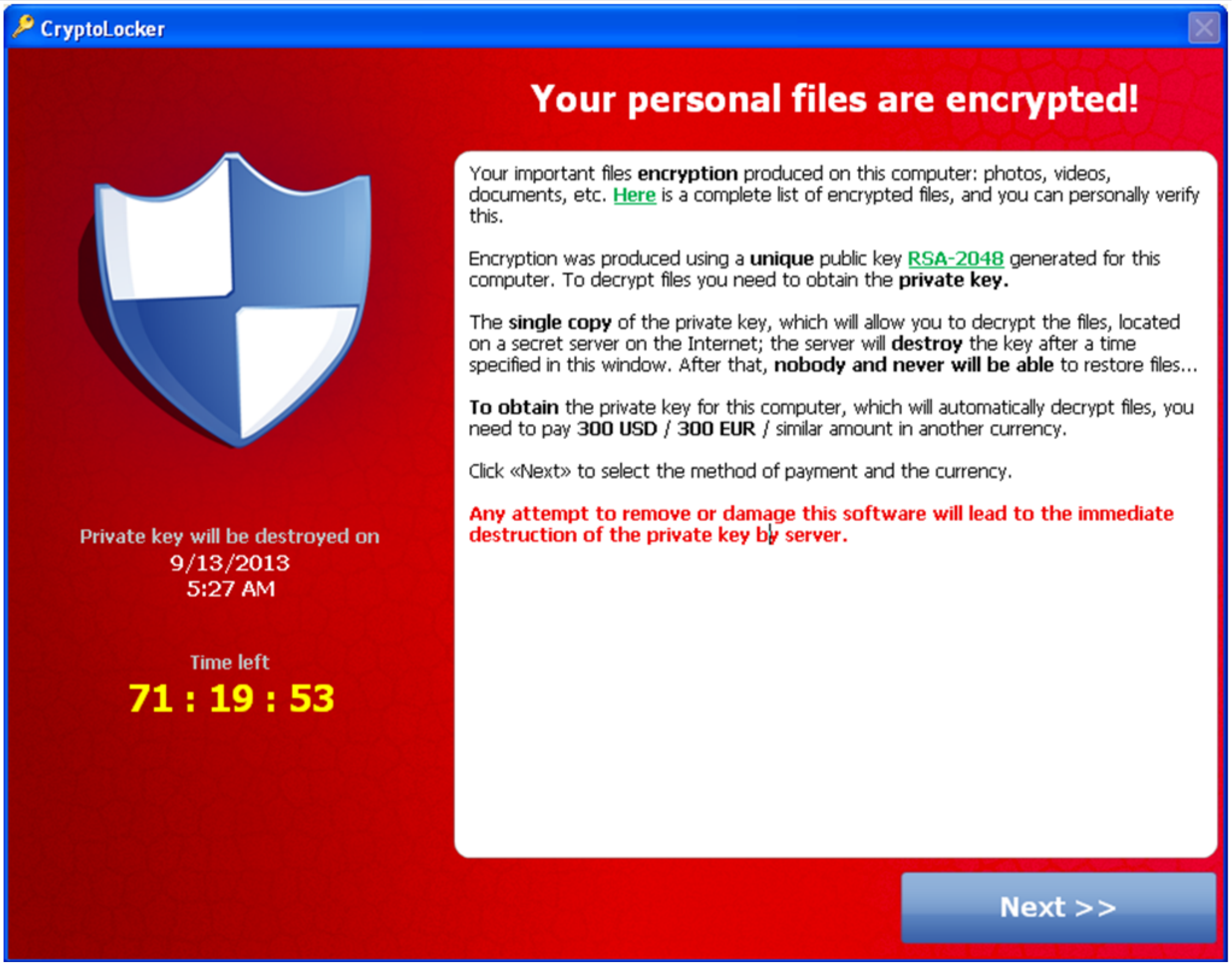
The ransom is usually about 300 USD or EUR. The amount can increase to 10 BitCoin (currently about 6,600 USD) if the user does not pay the ransom immediately. The ransom message further states that if the user does not comply within the payment window, the private key needed for decryption will be deleted from the attackers' servers, rendering the victim's data permanently unrecoverable.

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

Cryptolocker was spread mainly through infected websites and spam campaigns. There is currently no known alternative method for restoring access to the encrypted files.

On May 2015, Cryptolocker was taken down along with the Game Over Zeus botnet, in a multi-national law enforcement operation called 'Operation Tovar.' The operation led to the arrest of the malware creators and the end of Cryptolocker infections.

Most current ransomware follow the Cryptolocker pattern, including encryption, the ransom note style, and a countdown for an increase in the ransom. In fact, Cryptowall and Torrentlocker, two famous ransomwares, are direct clones of Cryptolocker and have even claimed to be Cryptolocker (as Torrentlocker still does).



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/13/2013
5:27 AM

Time left
71 : 19 : 53

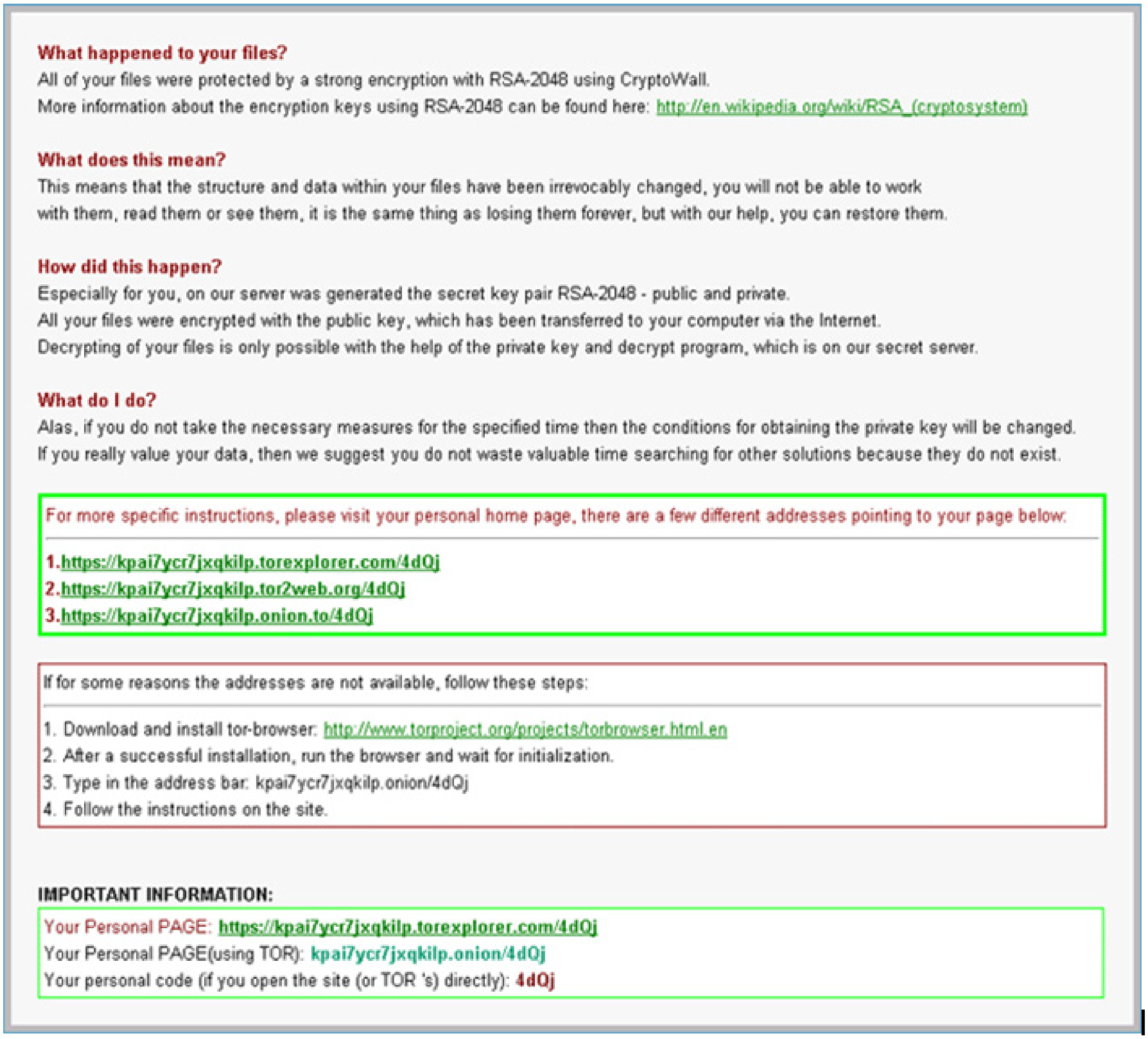
Figure 1 – Cryptolocker Ransom Note

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

Cryptowall

Cryptowall was first observed in the wild in November 2013, and is also known as Cryptodef and Cryptobit. The ransomware started as a Cryptolocker doppelgänger, but eventually surpassed it. After the takedown of Cryptolocker, Cryptowall became one of the most prominent ransomwares to date. Ransom payment is in BitCoin, which makes it harder for law enforcement agencies and security vendors to trace back to the malware operator.

Cryptowall is known for its use of AES encryption and for conducting its C&C communications over the Tor anonymous network. It is widely distributed via exploit kits, malvertising, and phishing campaigns. Four major versions of the ransomware have been observed. The most recent iteration surfaced in late 2015, with improved encryption tactics and better evasion and anti-sandboxing techniques. Currently, none of the ransomware versions have a decryption tool.



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.https://kpai7ycr7jxqkilp.torexplorer.com/4dQj
2.https://kpai7ycr7jxqkilp.tor2web.org/4dQj
3.https://kpai7ycr7jxqkilp.onion.to/4dQj

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: kpai7ycr7jxqkilp.onion/4dQj
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your Personal PAGE: https://kpai7ycr7jxqkilp.torexplorer.com/4dQj
Your Personal PAGE(using TOR): kpai7ycr7jxqkilp.onion/4dQj
Your personal code (if you open the site (or TOR 's) directly): 4dQj

Figure 2 – Cryptowall Ransom Note

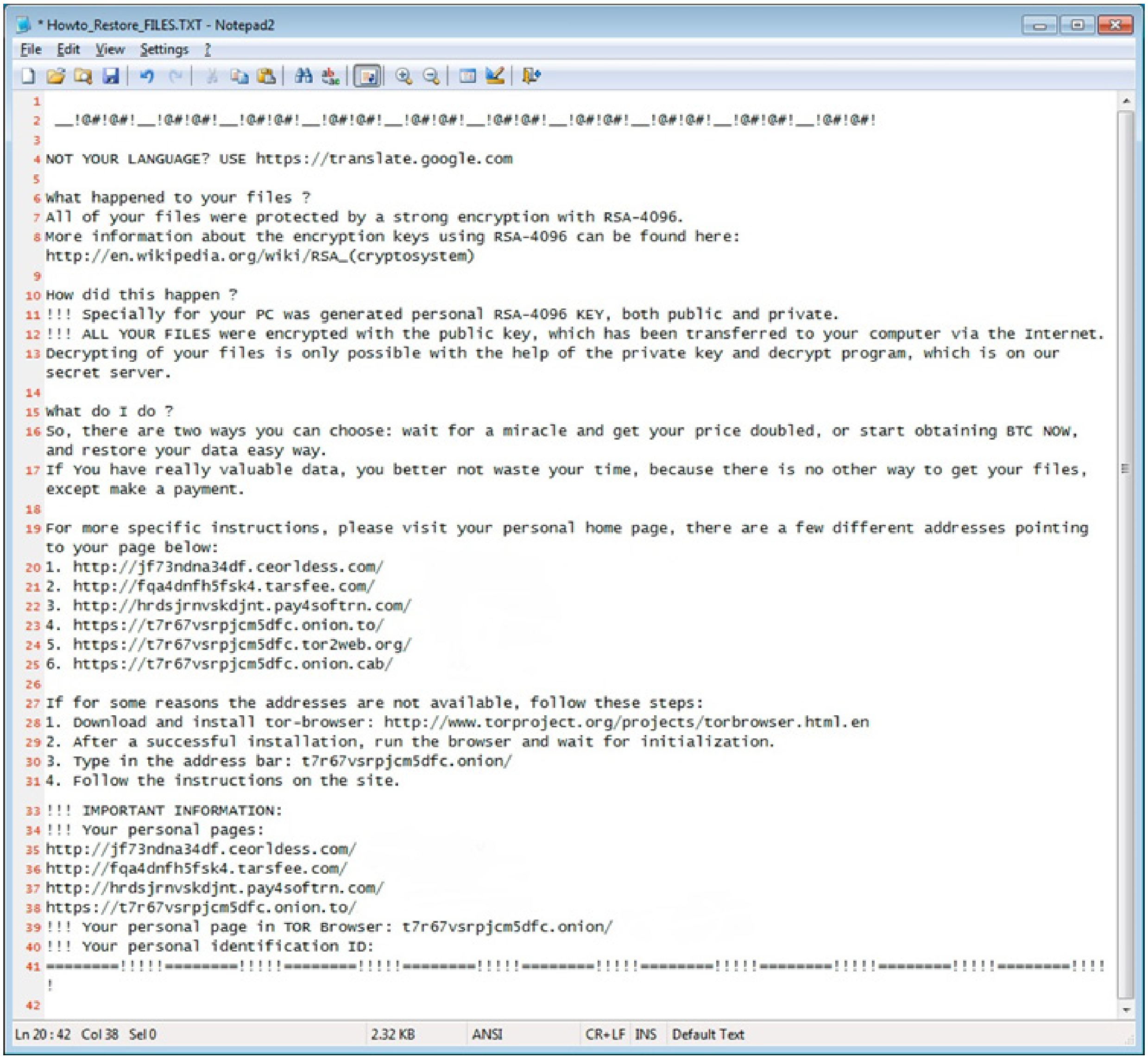
©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

TeslaCrypt

Until May 2016, TeslaCrypt was one of the most notable ransomwares. The ransomware, which was spread mainly via common exploit kits such as Angler and originally only targeted gaming users with specific games installed, is now defunct. Its authors stopped the malware campaign, apologized for the operation, and released a public recovery key. Security researchers reported that TeslaCrypt's distributors have switched to distributing CryptXXX ransomware instead.

During its long operation, TeslaCrypt was one of the top ransomwares in terms of infection rates. Its activity declined rather abruptly near the end of April 2016, which led a security researcher to ask Telacrypt's tech supporters for the decryption key.

Despite Teslacrypt's popularity and impressive infection rate, decryption tools were available for most versions before the recovery key became publicly available. Now, all versions of the ransomware can be decrypted.



```

 __!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!

NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files ?
All of your files were protected by a strong encryption with RSA-4096.
More information about the encryption keys using RSA-4096 can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen ?
!!! Specially for your PC was generated personal RSA-4096 KEY, both public and private.
!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our
secret server.

What do I do ?
So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BTC NOW,
and restore your data easy way.
If You have really valuable data, you better not waste your time, because there is no other way to get your files,
except make a payment.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing
to your page below:
1. http://jf73ndna34df.ceorldess.com/
2. http://fqa4dnfh5fsk4.tarsfee.com/
3. http://hrdsjrnvskdjnt.pay4softrn.com/
4. https://t7r67vsrpjcm5dfc.onion.to/
5. https://t7r67vsrpjcm5dfc.tor2web.org/
6. https://t7r67vsrpjcm5dfc.onion.cab/

If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: t7r67vsrpjcm5dfc.onion/
4. Follow the instructions on the site.

!!! IMPORTANT INFORMATION:
!!! Your personal pages:
http://jf73ndna34df.ceorldess.com/
http://fqa4dnfh5fsk4.tarsfee.com/
http://hrdsjrnvskdjnt.pay4softrn.com/
https://t7r67vsrpjcm5dfc.onion.to/
!!! Your personal page in TOR Browser: t7r67vsrpjcm5dfc.onion/
!!! Your personal identification ID:
========!!!!!========!!!!!========!!!!!========!!!!!========!!!!!========!!!!!========!!!!!========!!!!!========!!!!
!

```

Figure 3– TeslaCrypt Ransom Note

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

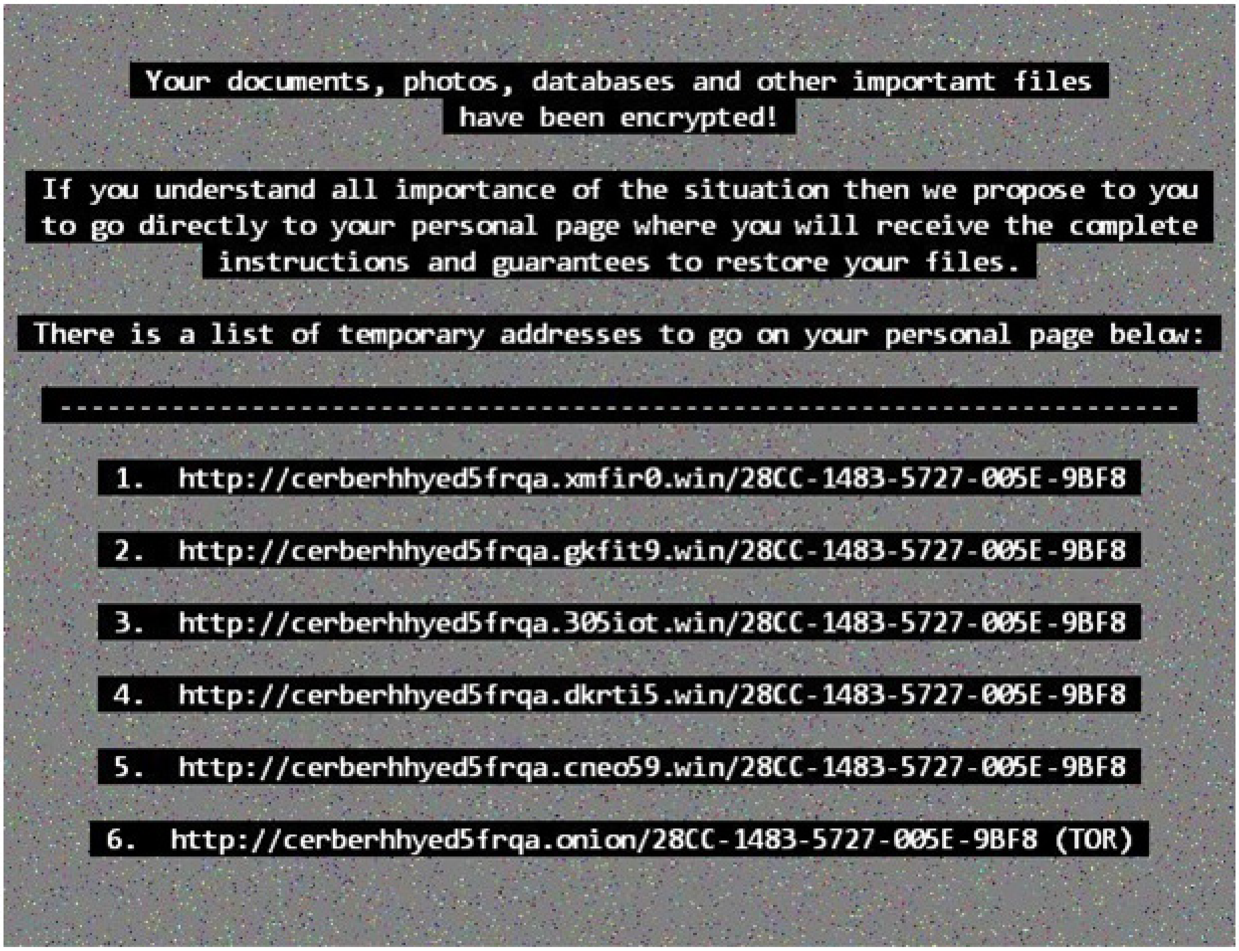
CURRENT TOP TIER

These currently active malware families demonstrate the most professional implementation and maintain a high infection rate.

Cerber

First published in February 2016, Cerber is one of the most widespread ransomwares in the past year. Until recently, it was spread mainly by the Neutrino and Nuclear exploit kits. At this time, it appears that the ransomware is also distributed by malicious spam techniques. Its features include:

- Audio delivery of the ransom message using Microsoft Speech API.
- Encryption of many incriminating strings inside the executable file, as an evasion technique.
- Ignoring machines from the following countries – Armenia, Azerbaijan, Belarus, Georgia, Kirgizstan, Kazakhstan, Moldova, Russia, Turkmenistan, Tajikistan, Ukraine, and Uzbekistan – as well as machines that use the local languages spoken in these countries. This means that using the location or language of one of those countries renders the user "immune" to this malware.



```
Your documents, photos, databases and other important files
have been encrypted!

If you understand all importance of the situation then we propose to you
to go directly to your personal page where you will receive the complete
instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

---------------------------------------------------------------

1.  http://cerberhhyed5frqa.xmfir0.win/28CC-1483-5727-005E-9BF8

2.  http://cerberhhyed5frqa.gkfit9.win/28CC-1483-5727-005E-9BF8

3.  http://cerberhhyed5frqa.305iot.win/28CC-1483-5727-005E-9BF8

4.  http://cerberhhyed5frqa.dkrti5.win/28CC-1483-5727-005E-9BF8

5.  http://cerberhhyed5frqa.cneo59.win/28CC-1483-5727-005E-9BF8

6.  http://cerberhhyed5frqa.onion/28CC-1483-5727-005E-9BF8 (TOR)
```

Figure 4 – Cerber
Cerber changes your desktop to the following ransom note, and drops a test file and an html file in every directory.
The text file contains quite a manifesto while the html contains a list of the files in the current directory.

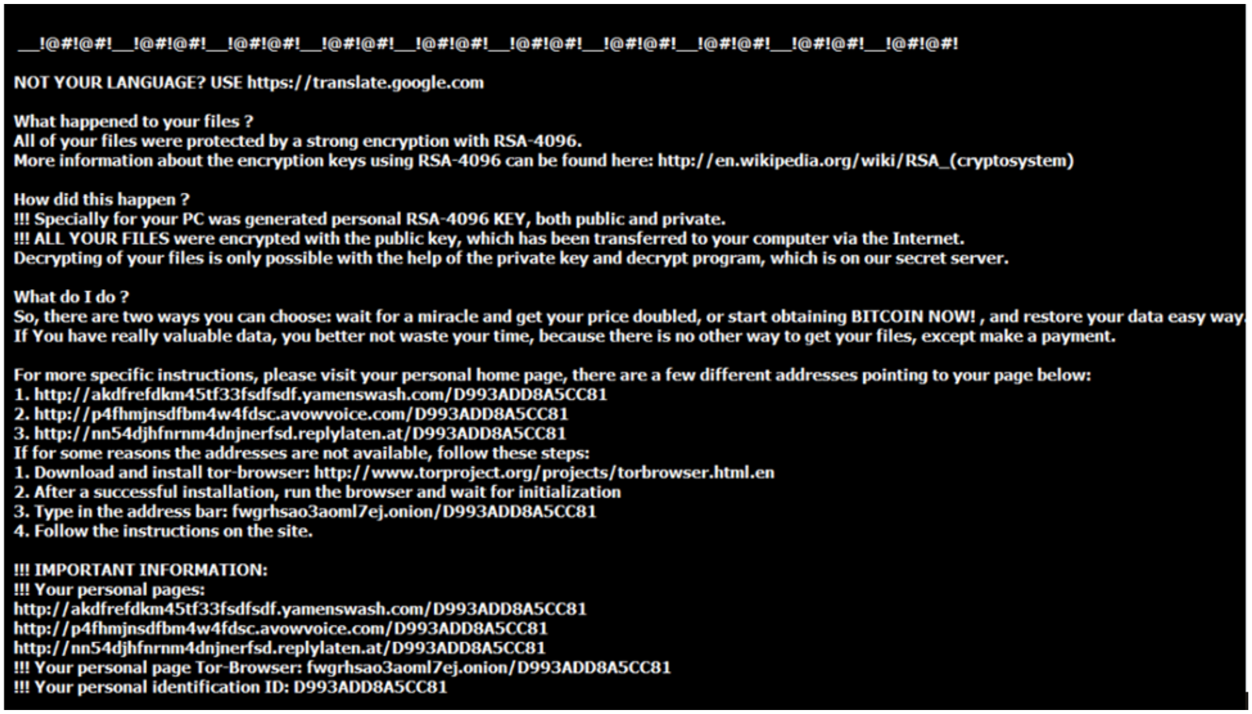
©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

Locky

Locky ransomware became famous in February 2016, due to its fast and wide distribution. During its first month in the wild, its reported infection rates were between one to five computers every second. Approximately 250,000 PCs were infected within its first three days of activity.

Locky's distribution method is similar to that of the infamous Dridex banking Trojan: spam emails which contain an attached Word document. The document is disguised as an invoice and contains a malicious macro. The similarity in distribution methods lead researchers to believe that the same threat actor is behind both malwares. Once the user enables the macro, the file is executed and then downloads the malware and installs it on the victim's computer. Similar to Cerber, Locky tries to avoid infecting machines located in Russia.

Locky made headlines after causing a hospital to enter a state of emergency, as well as for its mass amount of infections in a short period. According to our observations, there have been two large spikes in the malware's infections – in the middle of February and in the middle of June. In the last month, Necurs, one of Locky's main distributors, was down and Locky's infection rate was lower than usual. Both are now up once more.



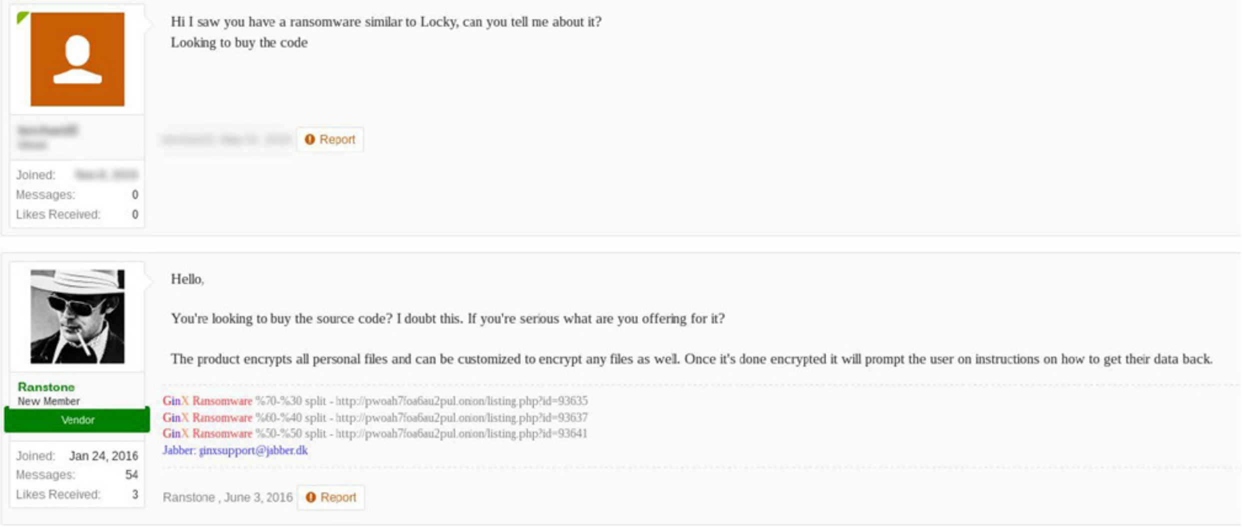
```
__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!

NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files ?
All of your files were protected by a strong encryption with RSA-4096.
More information about the encryption keys using RSA-4096 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen ?
!!! Specially for your PC was generated personal RSA-4096 KEY, both public and private.
!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do ?
So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BITCOIN NOW! , and restore your data easy way
If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1. http://akdfrefdkm45tf33fsdfsdf.yamenswash.com/D993ADD8A5CC81
2. http://p4fhmjnsdfbm4w4fdsc.avowvoice.com/D993ADD8A5CC81
3. http://nn54djhfnrnm4dnjnerfsd.replylaten.at/D993ADD8A5CC81
If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization
3. Type in the address bar: fwgrhsao3aoml7ej.onion/D993ADD8A5CC81
4. Follow the instructions on the site.

!!! IMPORTANT INFORMATION:
!!! Your personal pages:
http://akdfrefdkm45tf33fsdfsdf.yamenswash.com/D993ADD8A5CC81
http://p4fhmjnsdfbm4w4fdsc.avowvoice.com/D993ADD8A5CC81
http://nn54djhfnrnm4dnjnerfsd.replylaten.at/D993ADD8A5CC81
!!! Your personal page Tor-Browser: fwgrhsao3aoml7ej.onion/D993ADD8A5CC81
!!! Your personal identification ID: D993ADD8A5CC81
```

Figure 5 – Locky Ransom Note

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

Locky ransomware is a great malware to take a closer look at while studying today's thriving ransomware scene from the developers' and attackers' perspective. *IntSights*, a security provider specializing in advanced cyber intelligence, conducted a thorough research of Locky in various underground forums, and produced a broad picture of Locky's market, or more accurately, the Locky imitators' market.

According to the users IntSights contacted during the investigation, the original Locky source code isn't offered for sale, and is said to be distributed only by the original author. The author him/herself is not active on underground forums and markets, but instead, various other actors sell cheap knockoffs of Locky. A user named EnglishMafia, who claims he has the source code of a specific version of Locky which doesn't use C&C servers, offers it for sale for only 80 USD. However, the BTC address EnglishMafia provided hasn't received any transactions, which means it's either a scam or the actor creates a unique address for each buyer. Another user named Ranstone says that he wrote a ransomware very similar to Locky, which he calls Ginx. Ranstone sells the ransomware on a prominent black market in a semi-affiliate method – you pay less for the malware if you split your profits with the seller.



[redacted]

Joined: [redacted]
Messages: 0
Likes Received: 0

Hi I saw you have a ransomware similar to Locky, can you tell me about it?
Looking to buy the code

[redacted] Report

Ranstone
New Member
Vendor

Joined: Jan 24, 2016
Messages: 54
Likes Received: 3

Hello,

You're looking to buy the source code? I doubt this. If you're serious what are you offering for it?

The product encrypts all personal files and can be customized to encrypt any files as well. Once it's done encrypted it will prompt the user on instructions on how to get their data back.

GinX Ransomware %70-%30 split - http://pwoah7foa6au2pul.onion/listing.php?id=93635
GinX Ransomware %60-%40 split - http://pwoah7foa6au2pul.onion/listing.php?id=93637
GinX Ransomware %50-%50 split - http://pwoah7foa6au2pul.onion/listing.php?id=93641
Jabber: ginxsupport@jabber.dk

Ranstone , June 3, 2016 Report

Figure 6 – Reventon's Offer

IntSights' findings are proof of Locky's high popularity and reputation. The ransomware has become a brand, resulting in threat actors designing malwares based on Locky's characteristics and marketing them as related to Locky.

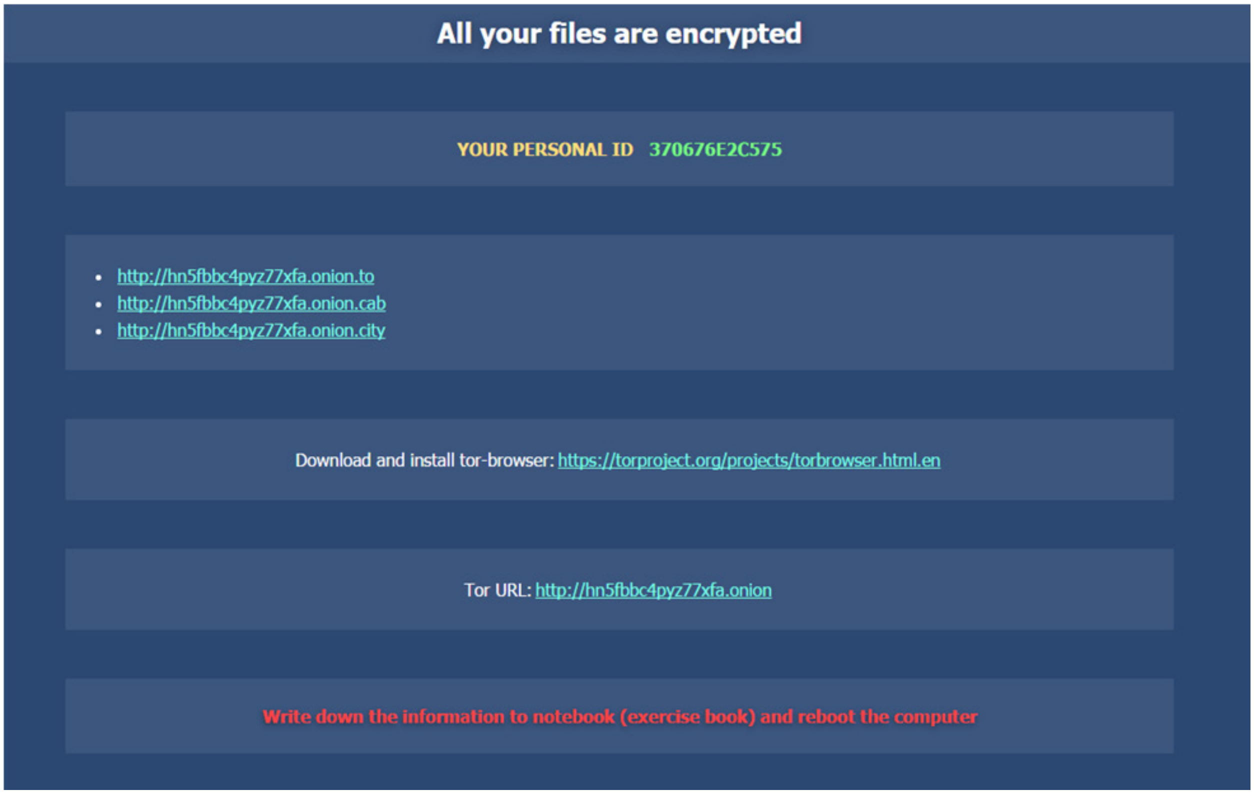
©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

CryptXXX

In April 2016, a new ransomware dubbed CryptXXX was spotted in the wild. This malware is distributed by both the Angler exploit kit and the Bedep Trojan, which drop it as a second-stage infection. As Angler is the most popular and infecting exploit kit in the wild, CryptXXX was widely distributed as well. Due to several similarities in the attack vector, several researchers speculate that the same operator is behind both Angler and CryptXXX.

Another finding which supports this speculation is that the real name of Angler exploit kit is XXX. This name was found on two strings in the unpacked binary on CryptXXX – Z:\CryptProjectXXX\Loader\InstDecode.pas and Z:\CryptProjectXXX\Loader\DDetours.pas.

CryptXXX has one additional feature, which differentiates it from most ransomwares observed in the wild today: info-stealing capabilities. The first version of CryptXXX attempted to access the BitCoin wallet used to pay the ransom. The recent version, 3.1, installs a general-purpose info stealer in addition to encrypting the user's files. Versions 1.0 and 2.0 had a decryptor released by Kaspersky and so in version 3.0, the authors changed the encryption method. However, they accidentally eliminated the malware's ability to recover the encrypted files after the ransom was paid. This was fixed a day later. Recently, there are reports that a new version of CryptXXX rebrands itself as Microsoft Decryptor. Among several changes, the ransomware abandons the unique file extensions such as .crypt and .crypz which were previously added to all encrypted files.



All your files are encrypted

YOUR PERSONAL ID 370676E2C575

- http://hn5fbbc4pyz77xfa.onion.to
- http://hn5fbbc4pyz77xfa.onion.cab
- http://hn5fbbc4pyz77xfa.onion.city

Download and install tor-browser: https://torproject.org/projects/torbrowser.html.en

Tor URL: http://hn5fbbc4pyz77xfa.onion

Write down the information to notebook (exercise book) and reboot the computer

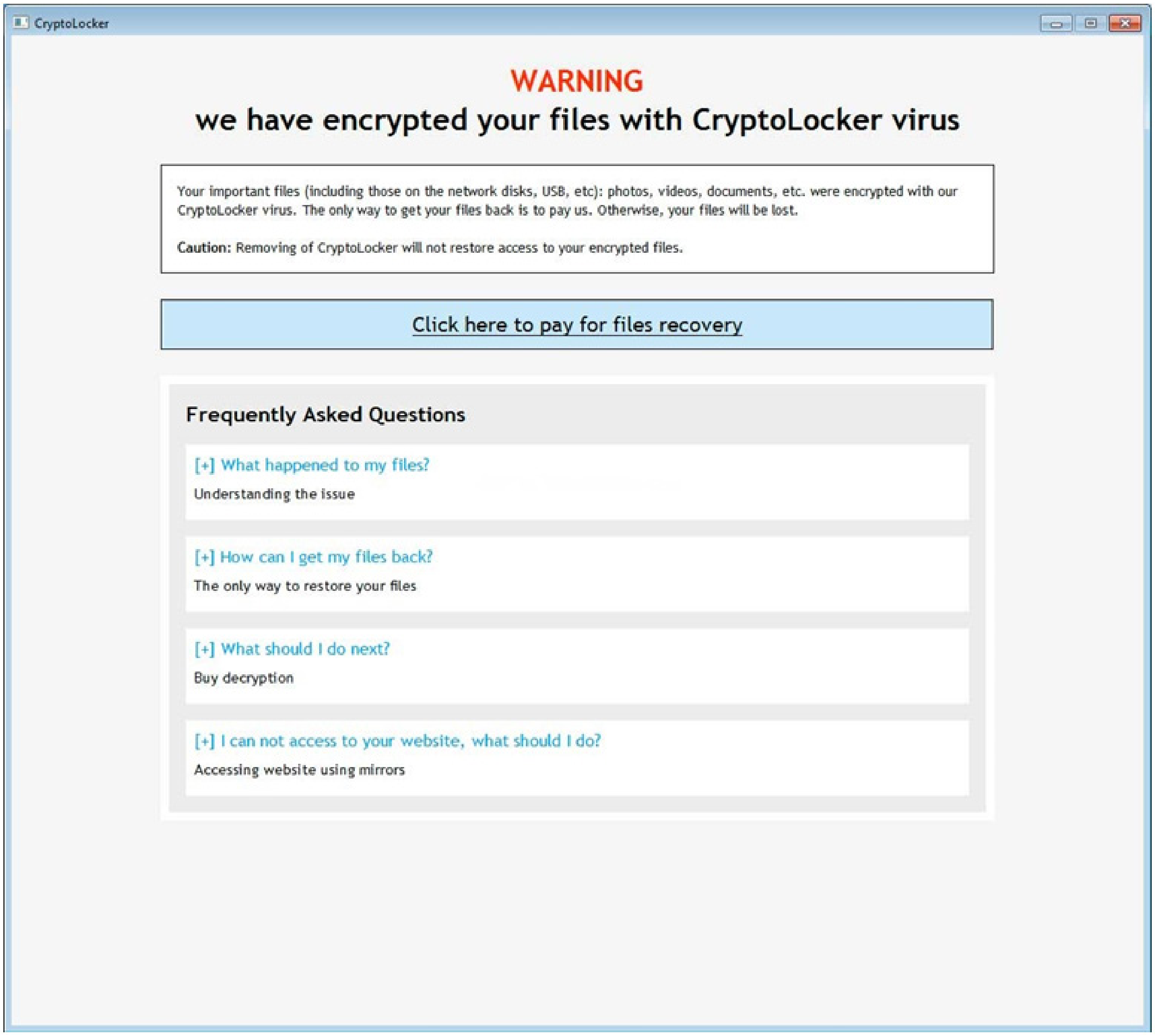
Figure 7 – CryptXXX Ransom Note

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

TorrentLocker

TorrentLocker is referred to by its operators as 'Cryptolocker', similar to the old and famous ransomware. However, due to the fact it uses a registry key with the value 'Bit Torrent Application', it was dubbed TorrentLocker. It was first spotted in February 2014. Although it is an older ransomware, TorrentLocker is currently active and its latest version cannot be decrypted. As of December 2015, less than a year after it first appeared, at least five versions of the malware have been observed. The first three versions contain a bug which enables recovery of the decrypted files. Before the release of version four, the flaw was fixed and from this version on, the files cannot be recovered. TorrentLocker is distributed almost exclusively through email. The TorrentLocker phishing massages are very well-written, which implies that they are most likely crafted by native speakers.

TorrentLocker is also geographically targeted – the ransom note and message content are tailored to a specific region. Most campaigns are location-oriented. Ransom payment is conducted with BitCoin and payment webpages are hosted in the Tor network.



WARNING
we have encrypted your files with CryptoLocker virus

Your important files (including those on the network disks, USB, etc): photos, videos, documents, etc. were encrypted with our CryptoLocker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.

Caution: Removing of CryptoLocker will not restore access to your encrypted files.

Frequently Asked Questions

[+] What happened to my files?
Understanding the issue

[+] How can I get my files back?
The only way to restore your files

[+] What should I do next?
Buy decryption

[+] I can not access to your website, what should I do?
Accessing website using mirrors

Figure 8 – TorrentLocker Ransom Note, distributed under the name "CryptoLocker"

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

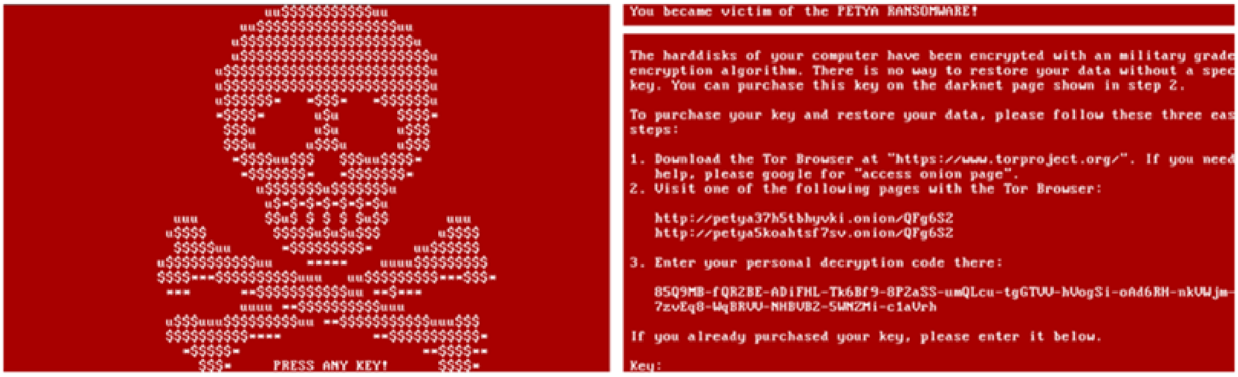
INTERESTING CASES

Some ransomware authors do not have the resources to acquire or develop high quality distribution tools and techniques. Therefore, they decide to take a different path and use unusual infection and encryption methods. The ransomwares listed below play a smaller part in the ransomware scene, but still stand out and make headlines due to their unique features and operations.

Petya and Mischa

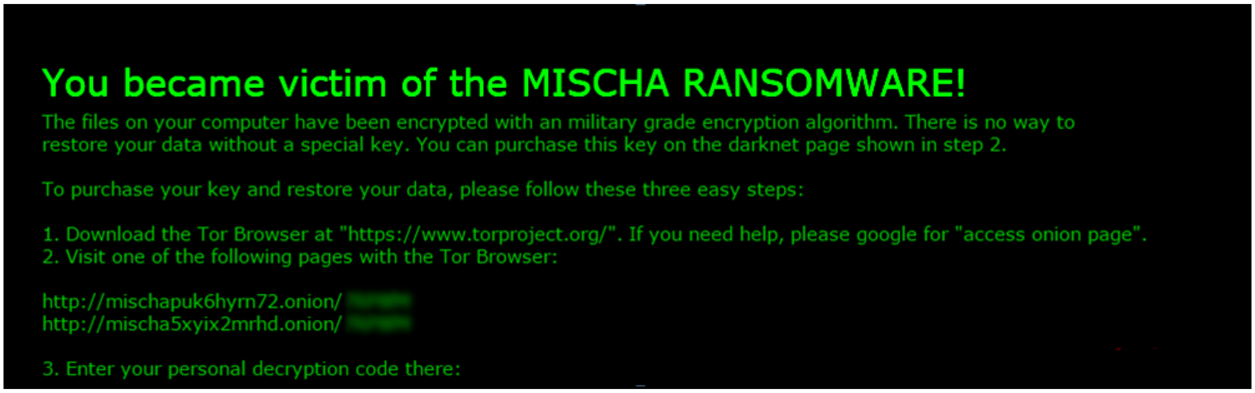
In March 2016, a new type of ransomware was discovered. Petya ransomware not only encrypts all files found on the victim's hard-drive, but its operators decided to hold the entire hard-drive's content hostage as well by encrypting its Master-File-Table (MFT). This renders the entire file system useless until the ransom is paid. This unique technique immediately flagged Petya as the next step in ransomware evolution. Check Point researchers revealed multiple flaws in the encryption algorithm implementation, and provided a method to restore all data encrypted by Petya, including the encrypted MFT. Additionally, to gain write access to the MFT, administrator permissions, which require user authorization, are needed. If those are not granted, Petya ceases its activity.

A more recent version of Petya installs an additional ransomware dubbed Mischa. Mischa only encrypts files, and doesn't require admin permissions. Therefore, if the executable is run and the user is prompted to grant it administrator privileges, clicking 'Yes' leads to the delivery of Petya, and clicking 'No' leads to the delivery of Mischa, which only encrypts files and leaves the MFT intact.



```
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 spec
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 eas
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/QFg6S2
   http://petya5koahtsf7sv.onion/QFg6S2

3. Enter your personal decryption code there:

   85Q9MB-fQRZBE-ADiFHL-Tk6Bf9-8PZaSS-umQLcu-tgGTVU-hUogSi-oAd6RH-nkUWjm-
   7zvEq8-WqBRUU-NHBVBZ-SWNZMi-c1aUrh

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

Key:
```

Figure 9 – Petya Ransom Note



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/ [redacted]
http://mischa5xyix2mrhd.onion/ [redacted]

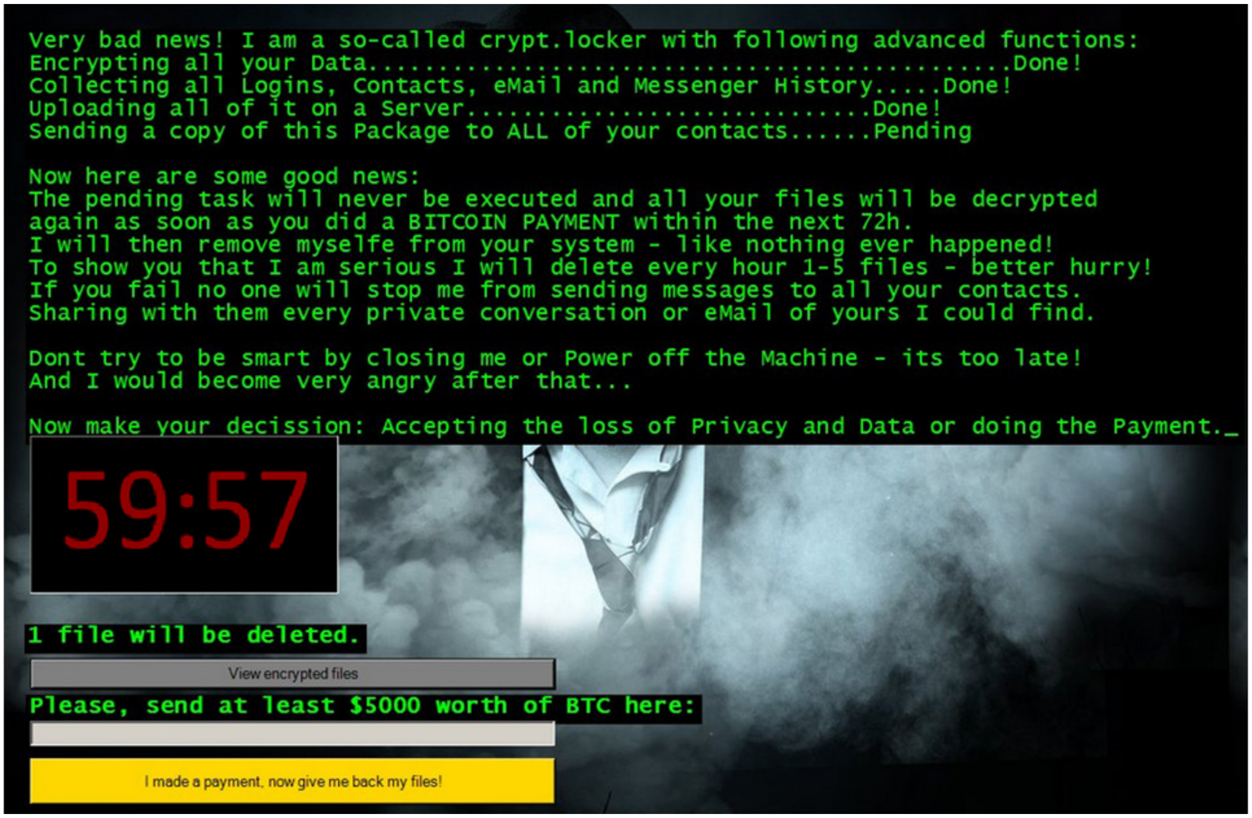
3. Enter your personal decryption code there:

Figure 10 – Mischa Ransom Note

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

Jigsaw

The Jigsaw ransomware, whose name was inspired by the horror movie 'The Saw', was first spotted in April 2016 and quickly became infamous thanks to an image of the killer from the movie displayed on the ransom note. The ransomware has a unique way of persuading victims to comply: if payments aren't made within an hour, Jigsaw not only raises the demanded price, but also starts to delete files from the infected machine on an hourly basis. If the user restarts the machine hoping that the ransom message will not reappear, Jigsaw deletes 1000 files. Fortunately, a decryption tool which can recover files encrypted by multiple Jigsaw variants has been released to the public.



```
Very bad news! I am a so-called crypt.locker with following advanced functions:
Encrypting all your Data..............................................Done!
Collecting all Logins, Contacts, eMail and Messenger History.....Done!
Uploading all of it on a Server.............................Done!
Sending a copy of this Package to ALL of your contacts......Pending

Now here are some good news:
The pending task will never be executed and all your files will be decrypted
again as soon as you did a BITCOIN PAYMENT within the next 72h.
I will then remove myselfe from your system - like nothing ever happened!
To show you that I am serious I will delete every hour 1-5 files - better hurry!
If you fail no one will stop me from sending messages to all your contacts.
Sharing with them every private conversation or eMail of yours I could find.

Dont try to be smart by closing me or Power off the Machine - its too late!
And I would become very angry after that...

Now make your decission: Accepting the loss of Privacy and Data or doing the Payment._
```

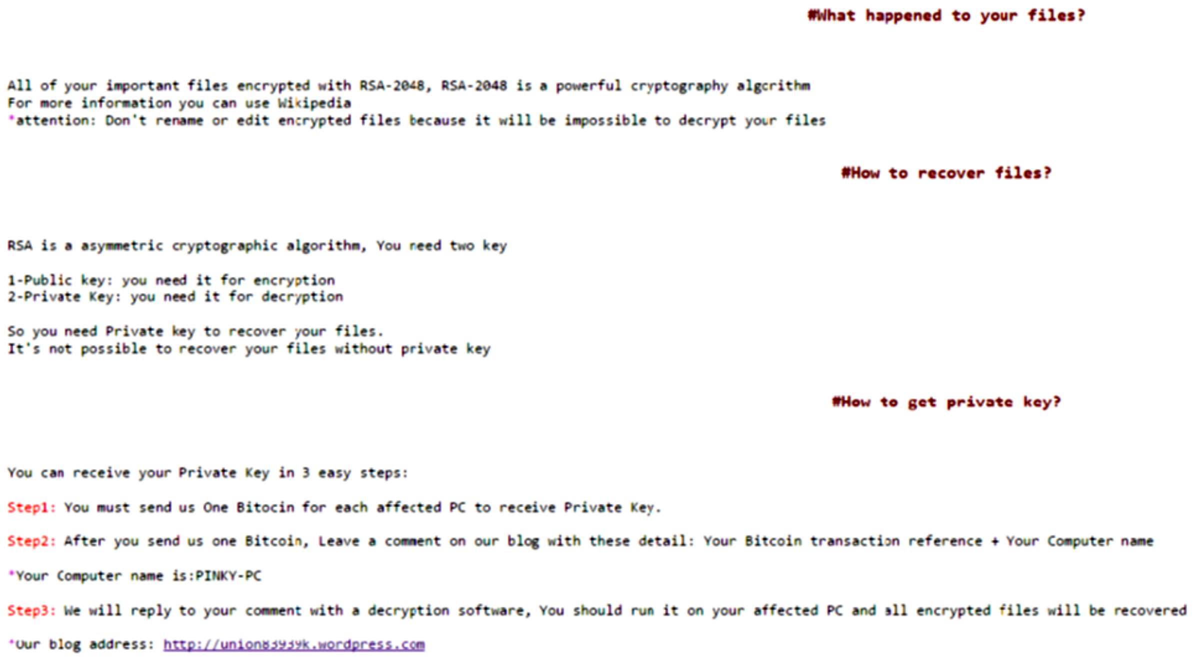
```
1 file will be deleted.
Please, send at least $5000 worth of BTC here:
```

Figure 11 – Jigsaw Ransom Note
Files are deleted on an hourly basis if the ransom isn't made within one hour.

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

SamSam (Samsa)

What distinguishes SamSam from most common ransomwares is its unique infection method. SamSam is not spread by spam/phishing emails and there is no need for any user action such as clicking on a certain link or opening a malicious attachment. Instead, the infection is done through an action by the attacker. First, the attacker scans for servers running a vulnerable JBoss application and exploits the vulnerability. The attackers can then trigger the ransomware remotely. Once a network has been breached, either by exploiting vulnerabilities or using an info-stealer to obtain user credentials, SamSam spreads through the local network to infect additional computers. The ransomware uses PsExec, a legitimate remote administration tool, to run remotely. This method places SamSam as a threat mainly for large organizations rather than for private users.

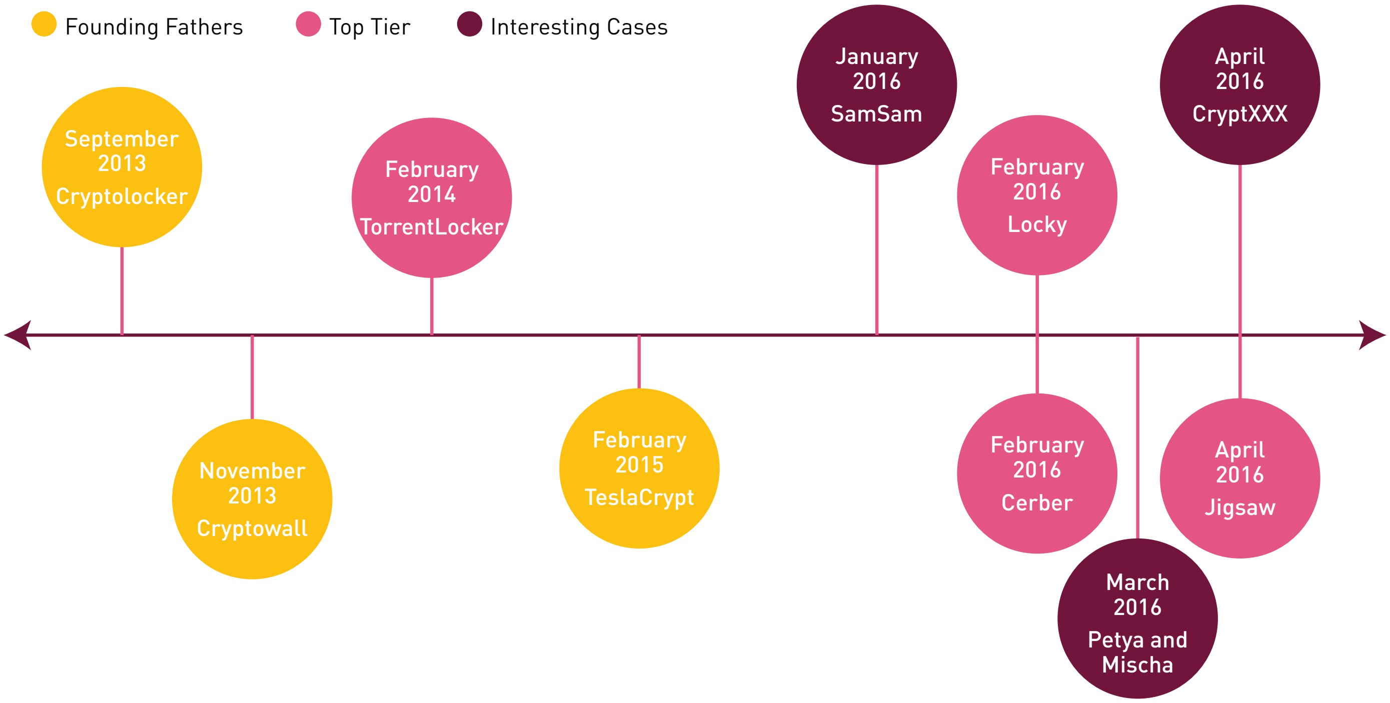


```
                                                #What happened to your files?

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
*attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files

                                                  #How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

1-Public key: you need it for encryption
2-Private Key: you need it for decryption

So you need Private key to recover your files.
It's not possible to recover your files without private key

                                                 #How to get private key?

You can receive your Private Key in 3 easy steps:

Step1: You must send us One Bitocin for each affected PC to receive Private Key.

Step2: After you send us one Bitcoin, Leave a comment on our blog with these detail: Your Bitcoin transaction reference + Your Computer name

*Your Computer name is:PINKY-PC

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our blog address: http://union83939k.wordpress.com
```

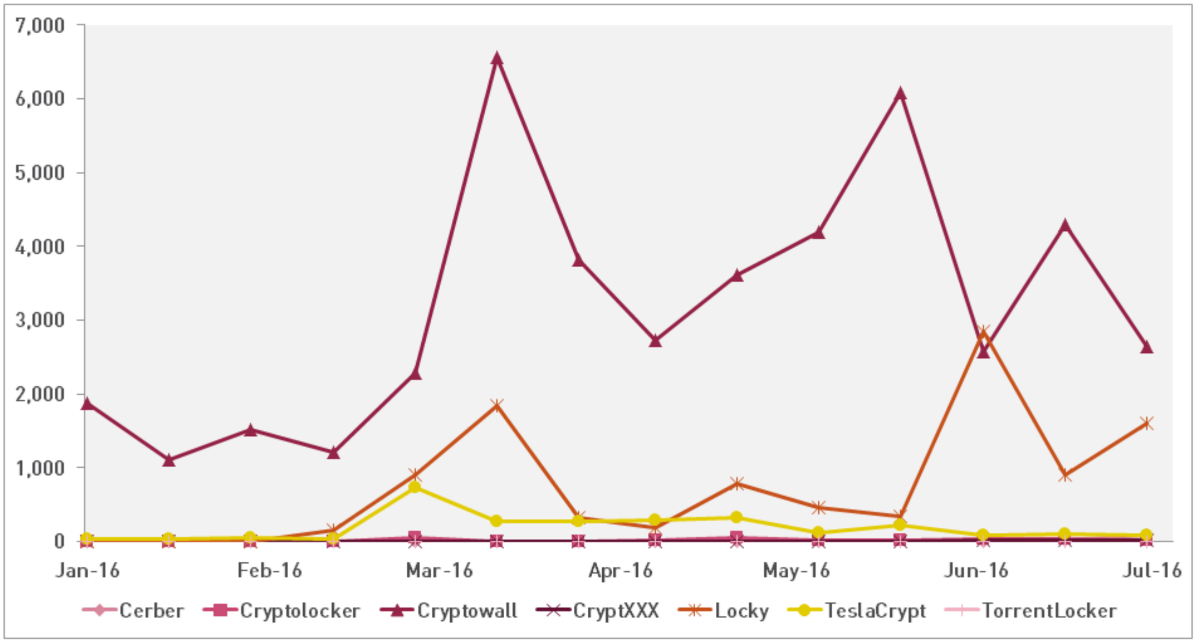
Figure 12 – SamSam Ransom Note

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

RANSOMWARE TIMELINE



RANSOMWARE ACTIVITY



©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

POWER OF THE COMMUNITY

There's a positive side to the rise of ransomware: researchers now share knowledge on a daily basis via a variety of sharing platforms and alliances, and the victims are now more personally engaged in the process of beating malware.

Bleepingcomputer.com hosts a Ransomware tech support and help forum, which maintains a sample repository based on a wide range of infected machines and is accessible to malware researchers.

The malware hunter team and security researcher Michael Gillespie have created ID-Ransomware, where a victim can upload the ransom note or an encrypted file and receive information about the ransomware, including a decryption tool if one exists. Michael Gillespie, Kaspersky, Emsisoft, Check Point and other vendors have also created and published decryption tools for many ransomware variants.

This spreadsheet contains information about most known ransomware, including links to decryption tools and prevention methods. It was first created by Mosh, one of the founders of MalwareMustDie.com, but has many additional contributors.

HOW TO PROTECT YOURSELF

We highly recommend you take these steps to protect yourself from ransomware, or at least mitigate its effects:

- **Backup your most important files** – Make an offline copy of your files on an external device and an online cloud stage service. This method protects your files not only from ransomware but from other hazards as well.

  Note: external devices should be used for backup ONLY and be disconnected immediately after the backup is completed.

- **Exercise caution** – We usually don't sense any danger while using our computers or other devices, but it's there. Threat actors are constantly trying to steal your money, your private data and your machine resources – don't let them have it. Don't open e-mails you don't expect to receive, and if you are asked to run macros on an Office file, DON'T! The only situation in which you should run macros is in the rare case that you know exactly what those macros will do. Additionally, keep track of the latest major malware campaigns to ensure that you will not fall victim to a new and unique phishing technique or download a malicious app, which can lead to malware installation on your computer or theft of your credentials.

- **Have a comprehensive, up-to-date, security solution** – High quality security solutions and products protect you from a variety of malware types and attack vectors. Today's Anti-Virus, IPS and sandboxing solutions can detect and block Office documents that contain malicious macros, and prevent many exploit kits from exploiting your system even prior to the malware infection. Check Point Sandblast solution efficiently detects and blocks ransomware samples, and extracts malicious content from files delivered by spam and phishing campaigns.

©2016 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]