Your Security Guide against Ransomware

How to prepare for and avoid a Cryptoware infection

What do you fear most in today's security landscape?

Do you fear viruses that disrupt normal computer operation, data stealing malware that retrieves e-mail credentials or ransomware threats that encrypt your computer content and take your money?

We believe most people fear ransomware threats because they are difficult to detect, remove or block from encrypting sensitive content. At the same time, it is the fact that we are helpless in doing anything, but follow the cybercriminals' instructions.

What is ransomware?

Ransomware (or crypto-ransomware) is a sophisticated piece of software that incorporates advanced **encryption algorithms** to block system files and **demands payment** in return for the key that can decrypt the blocked content.

In a similar way to advanced financial and data stealing malware, ***ransomware is able to evade detection by normal antivirus products***. But this is where the similarity ends.

As soon as the ransomware threat is on the system, it encrypts the content and lets the user know that money need to be delivered in a certain amount of time. **If the ransom is not paid, encrypted content is lost for good**.

For this reason, victims of ransomware are very much affected, because you may pay the money, but it's not sure if the blocked content will become available again.

An in-depth **ransomware analysis** from Bromium, resulted in a few troublesome conclusions:

- there are more than **6 large ransomware families;**
- crypto-ransomware use every possible **attack vector** to infect a machine;
- ransomware samples use **obfuscation techniques** to evade detection from traditional antivirus products;
- **communication** with C&C servers is also **encrypted** and difficult to detect in network traffic;
- all recent ransomware accepts payment in **Bitcoins** to avoid tracking from **law enforcement agencies;**
- creators of ransomware use traffic anonymizers – like **TOR** – and **Bitcoin** to receive ransom payments and avoid tracking devices by law enforcement agencies.

How do ransomware threats spread?

Ransomware and any other advanced piece of financial or **data stealing malware spread by any available means**. They simply look for **the easiest way to infect a system** or network and **use that backdoor to spread the malicious content**.

Nevertheless, these are **the most common methods used by cybercriminals to spread ransomware**:

- spam e-mail campaigns that contain malicious links or attachments;
- malicious websites
- legitimate websites that have malicious code injected in web pages
- drive-by downloads
- security exploits in vulnerable software

How does the infection phase take place?

Though the infection phase is slightly different for each ransomware version, there are still similar steps that appear:

1. Initially, an **e-mail** is received by the victim, which contains a malicious **link** or an **attachment**. Nevertheless, the infection may also originate from a **malicious website** that delivers a security **exploit** to create a **breach** by using a **vulnerable software** from the system.
2. When the **link** is followed or the **attachment** is accessed, **a downloader is placed on the system**.
3. The downloader uses a list of **domains or C&C servers controlled by cybercriminals** to download the ransomware program on the system.
4. The contacted C&C server responds by **sending back the requested data**, in our case, the ransomware.
5. The ransomware starts to **encrypt the entire hard disk content**, personal files and sensitive information. **Everything**.
6. A warning is displayed on the screen with **instructions on how to pay** for the **decryption key**.

4 Ransomware Threats You Need to Know

Reveton

source

In 2012, the major ransomware known as Reveton started to spread. It was based on the Citadel trojan, which was in turn part of the Zeus family.

This type of ransomware has become known to display a warning from law enforcement agencies, which made people name it “police trojan” or “police virus“.

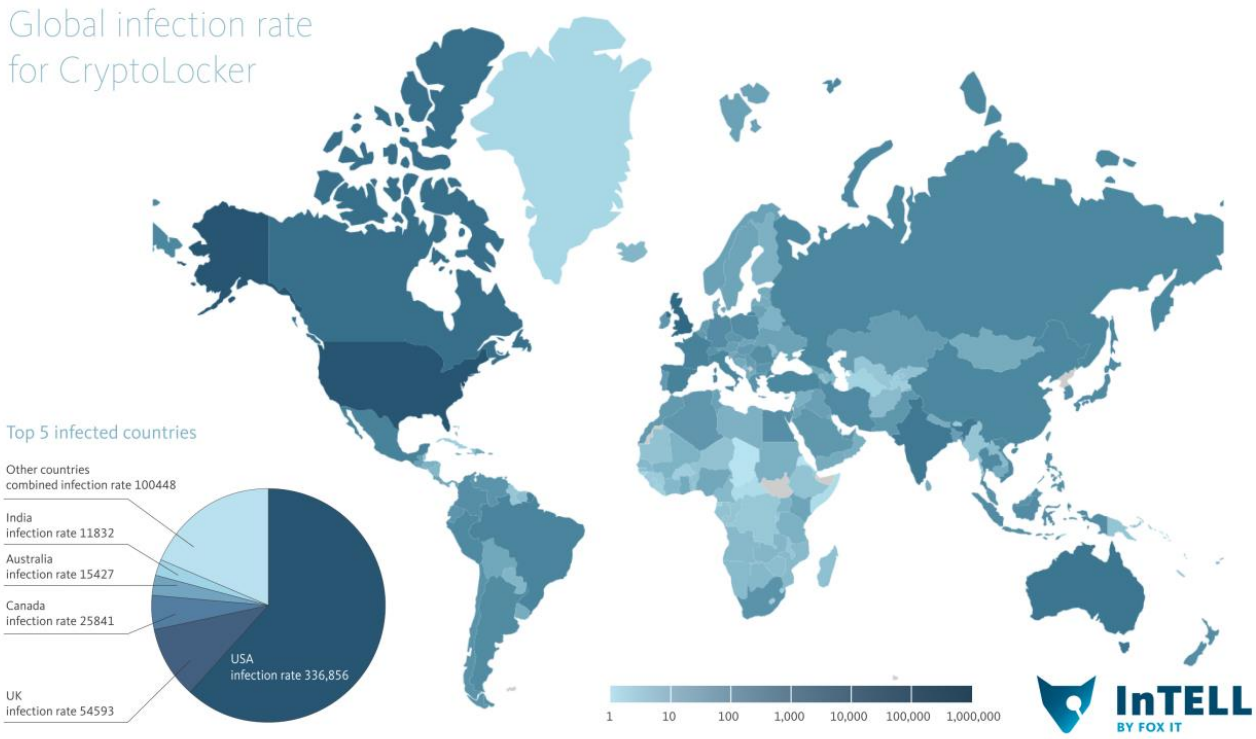
Once the warning appears, the victim is informed that the computer has been used for illegal activities, such as torrent downloads or for watching porn.

The graphic display enforced the idea that everything is real. Elements like the computer **IP address**, **logo from the law enforcement organization** in that specific country or the **localized content**, all of these created the general illusion that everything is real.

A larger post on Reveton has been published by **Brian Krebs**, who indicated that security exploits have been used by cybercriminals and that:

insecure and outdated installations of Java remain by far the most popular vehicle for exploiting PCs.

CryptoLocker



source

In June 2014, Deputy Attorney General **James Cole**, from the **US Department of Justice**, declared that the large joint operation between law agencies and security companies employed:

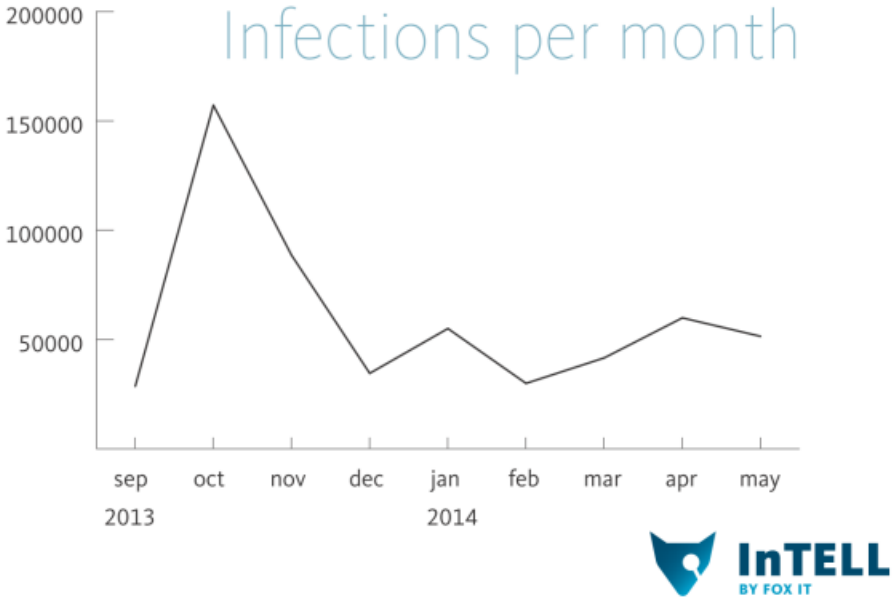
traditional law enforcement techniques and cutting edge technical measures necessary to combat highly sophisticated cyber schemes targeting our citizens and businesses.

Though the largest number of machines were infected by **Zeus GameOver** Trojan and less by **CryptoLocker**, the difficulty to remove this threat and recover personal files made this **infamous** malware as one infection (**disaster**) **you really need to avoid**.

As Brian Krebs mentioned in his take on CryptoLocker:

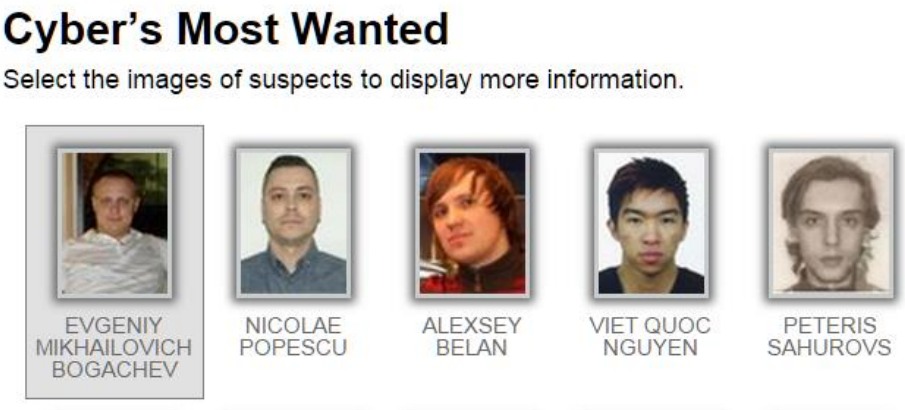
„The trouble with CryptoLocker is not so much in removing the malware — that process appears to be surprisingly trivial in most cases. The real bummer is that all of your important files — pictures, documents, movies, MP3s — will remain scrambled with virtually unbreakable encryption…"

The highest point reached by CryptoLocker happened in October 2013, when it was infecting around **150,000 computers a month!**

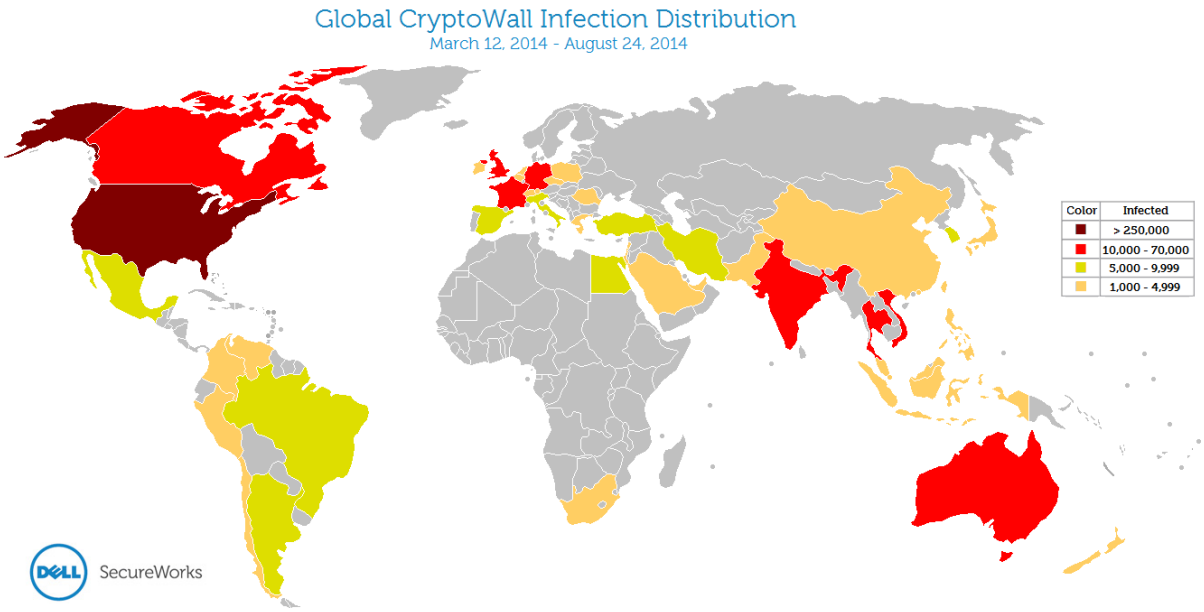


source

Evgeniy Bogachev is even now considered the **mastermind** behind the large infrastructure that deployed **Zeus GameOver and CryptoLocker** and he is still **number one most wanted cybercriminal** on the FBI list.



CryptoWall



source

Though CryptoLocker infrastructure may have been temporarily down, it doesn't mean that cybercriminals didn't find other methods and tools to spread similar ransomware variants. CryptoWall is such a variant and it has already reached its third version, **CryptoWall 3.0**. ***Only this single element indicates how fast this malware is improved and used online!***

At the beginning of this year, we were informed by FBI that ransomware is here to stay and this time, it won't stop to home computers, but it will spread to infect:

„Businesses, financial institutions, government agencies, academic institutions, and other organizations… resulting in the loss of sensitive or proprietary information."

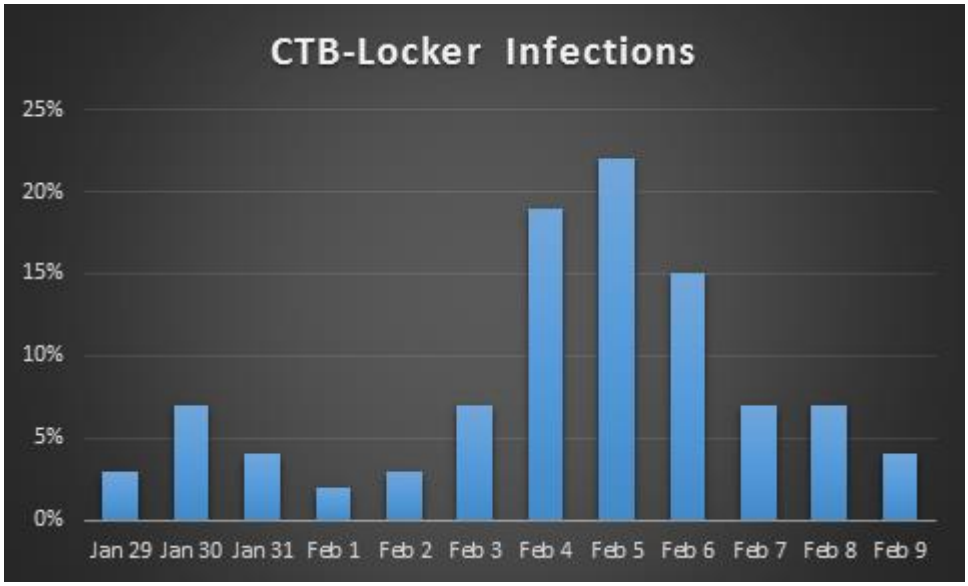
In the similar manner to CryptoLocker, **CryptoWall** has spread through various infection vectors since, including **browser exploit kits, drive-by downloads** and **malicious email attachments**.
The recent phishing and spam campaigns that targeted Europe invite users to click malicious links or access e-mail attachments.

What's new in the latest CryptoWall 3.0 variant?

Security analyst, Kafeine, displayed in a post the main differences or improvements that this ransomware suffered:

- communication with the malicious C&C servers uses RC4 encryption algorithm and it doesn't rely solely on the **TOR network**, but it also makes use of **I2P anonymity network** in order to conceal the hacker's identity;
- the displayed messages towards the victims are now **localized** to send the message in the corresponding **language**;

CTB Locker



source

CTB Locker is one of the latest ransomware variants of CryptoLocker, but at a totally different level of sophistication.

Let's take a quick look at its name, what CTB stands for?

- C comes from **Curve**, which refers to its persistent **cryptography based on elliptic curves** that encrypt the affected files with a unique RSA key;

- T comes from **TOR**, the malicious server placed in **onion-domain**, which can hide the cybercriminals' activities from **law enforcement** agencies
- B comes from **Bitcoin**, the **payment** method used by potential victims, which again can hide the online criminals' location.

Ransomware for sale

Though it is not something new, we noticed an increasing tendency for cybercriminals to design ransomware in order to be sold on underground forums and hidden networks, such as **TOR**.
The interesting aspect is that ***future potential cybercriminals won't need a really strong technical background***, since the final product will be easy to use and access.
Malware analyst, **Kafeine**, has managed to access such a location and post all the advertised information by hackers.
By taking a quick look at the hackers' ad, we notice the following support services included:

- instructions on how to **install the Bitcoin payment** on the server
- how to adjust the **ransomware settings** in order to target the selected victims
- details such as the requested **price** and the localized **language** that should be used
- recommendations on the **price** that you can set for the decryption key

Our specialists noticed that **CTB Locker** spreads through spam campaigns, where the e-mail message appears as an urgent **FAX message**.

This is a **sample of the e-mail content**:

From: Spoofed / falsified content
Subject:
Fax from RAMP Industries Ltd
Incoming fax, NB-112420319-8448
New incoming fax message from +07829 062999
[Fax server]= +07955-168045
[Fax server]: [Random ID]

Content:

No.: +07434 20 65 74

Date: 2015/01/18 14:56:54 CST

We recommend this extensive presentation on this advanced, even sophisticated ransomware, which gives us some valuable protection steps, from the need of using a **backup solution** as soon as possible, how we can use **Dropbox** to save our files and finally, a **CryptoPrevent tool**, a free software that can prevent CTB Locker from launching on the system.

9 Easy Steps to Keep Your System Safe from Ransomware

1. Do not keep important data only on the local device, always consider a back-up location that is not directly connected to the local system, such as an online backup location. Use this guide to find out more about various back-up options for your system.

At this point we need to give credit to Brian Krebs:

„CryptoLocker might be the best advertisement yet for cloud data storage systems."

2. Do not access .zip attachments in e-mails from unknown senders. It is the main method of distribution for ransomware threats.

3. Do not click links in e-mails from unknown senders. It could send you to malicious websites that host ransomware. If you can see the actual link (try to hover with your mouse over the link), then you can test it on this location.

4. Keep your operating system and your vulnerable software up-to-date with the latest security patches. Another important method of spreading ransomware is by using security exploits in

vulnerable applications. To make things easier, use a free tool that does this job for you, without disturbing your work.

5. Use a reliable antivirus product that includes an automatic update module and a real-time scanner to detect any suspect behavior. **Even more, contact their Technical Support and ask them directly** if their antivirus product detects the latest ransomware threats.

6. Since **most antivirus products do not detect the latest ransomware** variants, or better said, the downloaders that bring the malicious content on the system, we recommend using a **specialized tool against financial stealing malware and ransomware threats**.

7. Follow some common sense guidelines to improve your online safety and keep you safe from most malicious websites that spread **ransomware threats**. **Avoid questionable websites**, never click links in unrequested e-mails or in unknown web pages, do not disclose personal or sensitive information on social media sites.

8. Increase your online protection level by adjusting your web browser security settings.

9. If you receive suspicious e-mails that contain links or attachments from unknown senders on your **work computer**, make sure to **inform the IT department** as soon as possible or take adequate measures if your personal computer is at risk.

Conclusion

Though ransomware is not a new threat for the IT industry, people did not treat it as something serious until recently. **That is until May 2014**, when private security companies joined law enforcement agencies – **FBI and Europol** – in a massive shutdown operation that took down the GameOver Zeus botnet and the large infrastructure that spread CryptoLocker ransomware.

What have we learned?

That large joint operation was a sign of alarm for everybody and a few lessons were learned at the end of the day:

- **creating malware or ransomware threats is now a business** and it should be treated as such;
- the **"lonely hacker in the basement"** stereotype has died long time ago;
- the present **threat landscape is dominated by well defined and funded group**s that employ advanced technical tools and **social engineering skills** to access computer systems and networks;
- even more, **cybercriminal groups are hired by large states** to target not only financial objectives, but political and strategic interests.

To quote our CEO, Morten Kjaersgaard:

„Though not so many machines were infected with CryptoLocker, due to infection's ferocity and its ransomware approach, this infamous malware became more popular and more dreaded than Zeus.

Stay safe and don't forget the best protection is always a back-up!"

If you want to learn more about cyber security, join the **FREE Cyber Security for Beginners course**, created by Heimdal Security: