



SECURITY TASKFORCE

RANSOMWARE hits your server.

"All your data are encrypted. Your Business is down for hours, days or weeks or definitively.

*You are losing **untold amounts of revenue**; new customers will click away and maybe won't return to your company. Ransomware attacks are here to stay, and **no business can afford to be unprotected.**" Classic scenario.*

There are two types of ransomware in circulation:

1. Encrypting ransomware, which incorporates advanced encryption algorithms. It's designed to block system files and demand payment to provide the victim with the key that can decrypt the blocked content.
2. Locker ransomware, which locks the victim out of the operating system, making it impossible to access the desktop and any apps or files. The files are not encrypted in this case, but the attackers still ask for a ransom to unlock the infected computer.

You must Know Your Enemy

Ransomware is a \$1.5 billion business that often evades traditional anti-malware. Learn what you're up against and how to stop it.

How Ransomware Attacks Spread

2019 has seen ransomware trending away from brute force, large scale attacks to focused, planned and manually executed attacks that are much harder to detect and block.

Let's take a look at how the different forms of ransomware operate and what your organization should be doing to minimize vulnerability to an attack.

Cyber criminals simply look for the easiest way to infect a system or network and use that backdoor to spread the malicious content

How do ransomware infections happen?

Though the infection phase is slightly different for each ransomware version, the key stages are the following:

1. Initially, the victim receives an email which includes a malicious link or a malware-laden attachment. Alternatively, the infection can originate from a malicious website that delivers a security exploit to create a backdoor on the victim's PC by using a vulnerable software from the system.
2. If the victim clicks on the link or downloads and opens the attachment, a downloader (payload) will be placed on the affected PC.
3. The downloader uses a list of domains or C&C servers controlled by cyber criminals to download the ransomware program on the system.
4. The contacted C&C server responds by sending back the requested data.
5. The malware then encrypts the entire hard disk content, personal files, and sensitive information. Everything, including data stored in cloud accounts (Google Drive, Dropbox) synced on the PC. It can also encrypt data on other computers connected to the local network.
6. A warning pops up on the screen with instructions on how to pay for the decryption key



Will Ransomware go away in the future?

The simple answer to this is no for sure!

All of the indicators suggest that Ransomware will remain a major and rapidly growing threat, fueled by anonymizing networks and payment methods.

You can see the story behind the Locker-Goga, Ryuk that was spread via spear-phishing email to major industries companies using malware like EMOTET and TRICKBOT to deploy these very nasty crypto-ransomwares. Expect to see an increase in Ransomware variants which target complete infrastructure very fast and placing your business in a critical position. When a machine or server is attacked the Ransomware will hold the whole company files, pages and images for ransom.

We propose to have in place Anti-Ransomware solution that use an algorithm that can detect ransomware action and prevent further activity over shared documents.

The results show that it can detect ransomware activity in less than 20 s, before more than 10 files are lost. And including Firewall that can help to mitigates the risk.

Sample of Ryuk:



First of all, Ryuk is considered to be the next groundbreaking virtual attack, because of the damage that it has been already done in just a couple weeks of its existence and suspected relation to the **Lazarus Group**, which was behind such famous attacks like HERMES (that earned Korean hackers around \$60 million dollars), WannaCry, SamSam and 2014 Sony Pictures scandal.

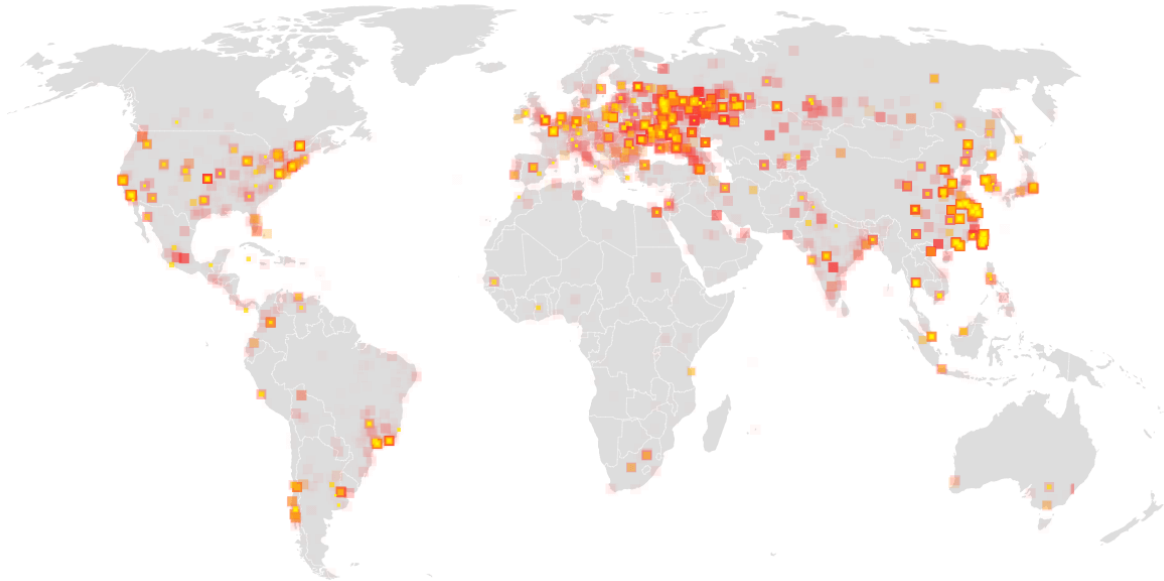
This makes developers believe that Ryuk ransomware is attempting to follow the recent BitPaymer and Emotet multi-vector attack path performing targeted attacks towards companies and government as well.

The most notorious ransomware families

WannaCry

On Friday, May 12, 2017, around 11 AM ET/3PM GMT, a ransomware attack of "unprecedented level" (Europol) started spreading WannaCry around the world. It used a vulnerability in Windows that allowed it to infect victim's PC's without them taking any action.

Until May 24, 2017, the infection has affected over 200,000 victims in 150 countries and it keeps spreading.



Petya ransomware

The Petya ransomware family was first discovered in 2016, and its trademark includes infecting the Master Boot Record in order to execute the payload and encrypt the data available locally.

A strain similar to Petya started creating havoc in late June 2017, when it emerged, enhanced with self-replicating abilities.

Locky

One of the newest and most daring ransomware families to date is definitely Locky.

First spotted in February 2016, this strain made its entrance with a bang by extorting a hospital in Hollywood for about \$17,000.

Since then, Locky has had a rampant distribution across the world.

TorrentLocker

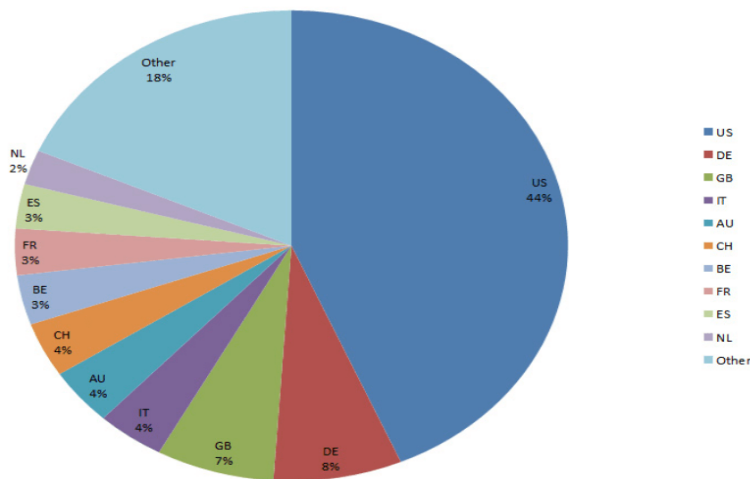
This file-encrypting malware emerged in early 2014 and its makers often tried to refer to it as CryptoLocker, in order to piggyback on its awareness.

TorrentLocker creators proved that they were attentively looking at what's going on with their targeted "audience" when they corrected a flaw in their encryption mechanism. Until that point, a decryption tool created by a malware researcher had worked.

But soon they released [a new variant](#) which featured stronger encryption and narrowed the chances for breaking it to zero.

Its abilities to harvest email addresses from the infected PC are also noteworthy. Naturally, these emails were used in subsequent spam campaigns to further distribute the TorrentLocker.

TorrentLocker Endpoints by Country



@

Reference: <https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf>



Practices to Stop Ransomware

Ransomware attacks are becoming more targeted, tailored and stealthy. But they are still capable of wreaking havoc on organizations' networks, encrypting files and extorting payment for retrieval.

Modern firewalls are purpose-built to defend against these kinds of attacks, but they need to be given an opportunity to do their job.

Update your IDS systems with exploit kit detection rules

Many IDS, IPS and firewall systems come with exploit detection features. Exploit kits are used as a way to get Ransomware onto a client through malspam or via compromised websites.

The two most common exploit kits (EK) associated with Ransomware are the Neutrino EK and the Angler EK. Check if your network security monitoring systems are up to date and see if they have the capability to detect exploit kits.

Sophos brand includes the Snort IDS system which supports the detection of exploit kits. Watch out for any activity in the Top Network Events report from your firewall IDS.

Use client based anti-ransomware agents

Over the past few months companies like Kaspersky Anti-Ransomware or Sophos intercept-X have released anti-ransomware software applications. These are designed to run in the background and block attempts by Ransomware to encrypt data.

They also monitor the Windows registry for text strings known to be associated with Ransomware. The problem with this approach is that you will need to install client software on every network device.

Researchers are also looking at ways to 'crash' computer systems when droppers are detected. Droppers are small applications that first infect target machines in preparation for downloading the main malware payloads.

This will likely mean that the system is sent to IT where the attack should be discovered.

You should also inform your network users to avoid installing agents themselves.

There is too much of a risk that they will install the wrong agent, or they end up install more malware on their systems.

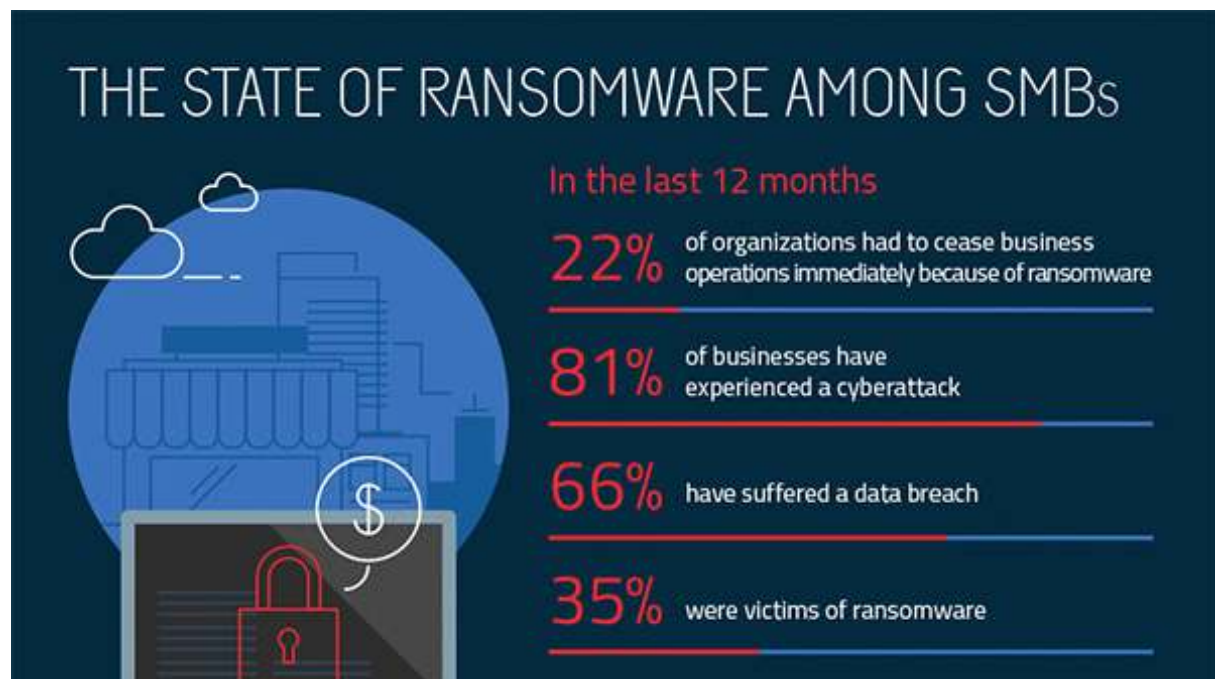


Kaspersky Anti-Ransomware Tool for Business KASPERSKY

Protection against ransomware is on

GET PREMIUM PROTECTION

Global Kaspersky Security Network in the last 24 hours Global Kaspersky Security Network statistics



THE STATE OF RANSOMWARE AMONG SMBs

In the last 12 months

- 22% of organizations had to cease business operations immediately because of ransomware
- 81% of businesses have experienced a cyberattack
- 66% have suffered a data breach
- 35% were victims of ransomware

Recommendation's to avoid being hit by ransomware on your pc

1. I don't store important data only on my PC.
2. I have 2 backups of my data: on an external hard drive and in the cloud – Dropbox/Google Drive/etc.
3. The Dropbox/Google Drive/OneDrive/etc. application on my computer is not turned on by default. I only open them once a day, to sync my data, and close them once this is done.
4. My operating system and the software I use is up to date, including the latest security updates.
5. For daily use, I don't use an administrator account on my computer. I use a guest account with limited privileges.
6. I have turned off macros in the Microsoft Office suite – Word, Excel, PowerPoint, etc.
In the browser
7. I have removed outdated plugins and add-ons from my browsers. I only kept the ones I use on a daily basis and I keep them updated to the latest version.
8. I use an ad-blocker to avoid the threat of potentially malicious ads.

Online behavior

11. I never open spam emails or emails from unknown senders.
12. I never download attachments from spam emails or suspicious emails.
13. I never click links in spam emails or suspicious emails.

Anti-ransomware security tools

14. I use a reliable, paid antivirus product that includes an automatic update module and a real-time scanner.
15. I understand the importance of having a traffic-filtering solution that can provide proactive anti-ransomware protection.

There are two key lessons here:

Ensure you are backing up your data properly on different locations and patch all your infrastructure and servers.

Keep the website operating system UpToDate and infrastructure fully patched.

Ransomware is also a growing problem for users of mobile devices. Lock-screen types and file-encrypting variants: lock screen Ransomware will stop you from accessing anything on your mobile device and file encrypting variants will encrypt data stored on the device.

You can decrease your chances of an attack, by avoiding unofficial app stores and by keeping your mobile device and apps updated.

We'll finish by repeating the advice: ensure you backup all of your personal and work data. **Educate users on the risks** and disconnect problematic users from sensitive data.

TESESLACRYPT

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ~ = 550 USD.
Your Bitcoin address for payment: [1234567890123456789012345678901234567890](#)

\$ PURCHASE PRIVATE KEY WITH BITCOIN

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)

Contact: info@security-taskforce.be

Or

just call: **+32 496619154**