



ENJOY SAFER TECHNOLOGY™

# Ransomware

Evolúcia, protiopatrenia, očakávania.





Global  
**RANSOMWARE**  
**30 MIN**  
2016

**\$47,717**



“Cyber-criminals collected **\$209 million** in the first **three months of 2016** by extorting businesses and institutions to unlock computer servers. At that rate, **ransomware is on pace to be a \$1 billion a year crime this year.**”

[FBI for money.CNN.com](http://FBIfor.money.CNN.com), April 2016

**\$ 1,000,000,000**  
**business**



# Caesar vs. Sicilian pirates

50 talents (1550 kg) of silver



# AIDS Info Disk

“Licensing enforcement”



The screenshot shows a Windows XP file explorer window with the address bar set to `C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures`. The window contains four files:

- `!_READ_ME!.txt` (Text Document, 1 KB)
- `Blue hills.jpg._CRYPT` (\_CRYPT File, 28 KB)
- `Sunset.jpg._CRYPT` (\_CRYPT File, 70 KB)
- `Water lilies.jpg._CRYPT` (\_CRYPT File, 82 KB)

A blue "ATTENTION !" dialog box is overlaid on the window. It features a yellow warning triangle icon and the following text:

Your files are encrypted with RSA-1024 algorithm. To recovery your files you need to buy our decryptor. To buy decrypting tool contact us at: [redacted]@yahoo.com

An "OK" button is located at the bottom center of the dialog box.

## Computer is Blocked!

Your computer is blocked for viewing, copying and dissemination of video materials containing elements of pedophilia and rape of children. In order to remove the block You are required to pay a fine in the amount of 500 rubles to the (telephone) number 8-965-265-90-84. In case of payment of the sum equal to or greater the amount fine there will be an unblock code on the receipt. You'll need to enter the code in the lower portion of the window and press the "unblock" button. Once the block is removed you must delete all materials containing elements of rape and pedophilia. If you do not pay the fine within 12 hours, all information on your personal computer will be permanently deleted and the case will be sent to court for investigation in accordance to chapter 242 part 1 of the Penal Code of Russian Federation.

Rebooting or turning off of the computer will lead to prompt removal of all data, including the operating system and BIOS, without ability of further restoration.







## All activities of this computer have been recorded

All your files are encrypted. Don't try to unlock your computer!

Your browser has been blocked due to at least one of the reasons specified below.

**You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents**, thus infringing Article 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

**You have been viewing or distributing prohibited Pornographic content** (Child Porno photos and etc were found on your computer). Thus violating article 202 of the Criminal Code of United States of America, Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

**Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware**, thus you are violating the law on Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to \$100,000 and/or deprivation of liberty for four to nine years.

Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.



Your IP:

Location:

SECURE PAYMENT FORM

Enter the code MoneyDak



Private key will be destroyed on  
**10/20/2013**  
**12:37 PM**

Time left  
**72 : 34 : 50**

## 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 the 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.

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

Next >>







## What is BitCoin

BitCoin is a software-based secure payment system approved by international law enforcement agencies.

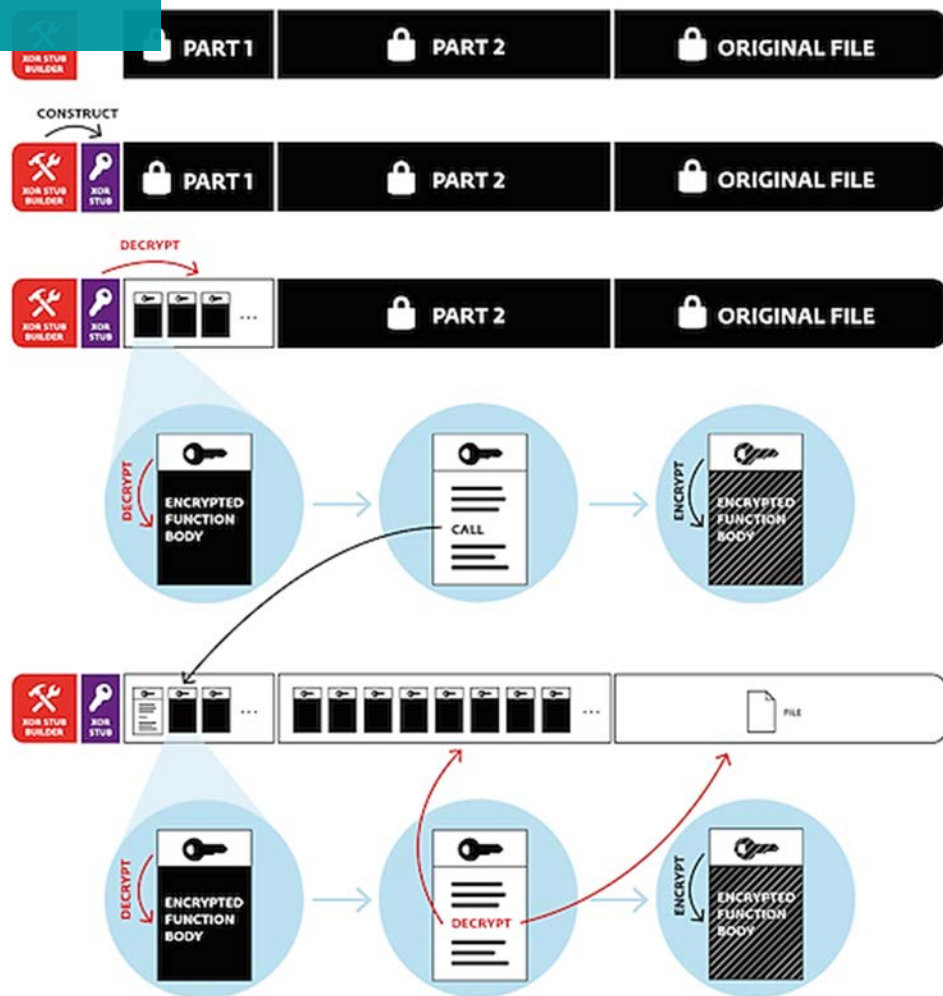
### How to pay a fine?

1. Purchase bitcoins from an exchange or an ATM.
  2. Transfer to the address (click to copy): 1N43vMz9qB1xcBFFzCGnENSmBrE3sXifr
- To locate the nearest exchange or an ATM open the corresponding tab below.

If you purchased a paper wallet or you want to register a new bitcoin wallet follow the instructions below: Open Internet Browser. Go to the address: [blockchain.info/wallet](http://blockchain.info/wallet) and click 'Start A New Wallet'. Enter your e-mail address (optional) and password. Make sure your password is secure. Save your password safely, preferably offline (click Notepad). Follow the steps prompted on the website and pay close attention to the security recommendations. Login to your Bitcoin wallet [blockchain.info/wallet/login](http://blockchain.info/wallet/login) Click on Import / Export. Enter the paper wallet's private key by typing it manually (case sensitive) and click on 'Add Private Key'. Click 'Sweep Key'. Make sure your Bitcoin balance reflects the new deposit.

Making BitCoin payment: click 'Send Money' on the menu, enter the bitcoin address, click 'Send Payment'.

### Learn more about BitCoin



**ALL YOUR PERSONAL FILES HAS BEEN ENCRYPTED**

All your data (photos, documents, databases, etc) have been encrypted with a private and unique key generated for this computer. This means that you will not be able to access your files anymore until they are decrypted. The private key is stored in our servers and the only way to receive your key to decrypt your files is making a payment.

The payment has to be done in Bitcoins to a unique address that we generated for you. Bitcoins are a virtual currency to make online payments. If you don't know how to get Bitcoins, you can click the button "How to buy Bitcoins" below and follow the instructions.

**You only have 4 days to submit the payment.** When the provided time ends, the payment will increase to 1 Bitcoins (\$350 aprox.). Also, if you don't pay in 7 days, your unique key will be destroyed and you won't be able to recover your files anymore.

**Payment raise****3 days, 23:46:43****Final destruction****6 days, 23:46:43**

To recover your files and unlock your computer, you must send 0.1 Bitcoins (\$35 aprox.) to the next Bitcoin address:

[Redacted Bitcoin address]

[Check payment](#)[How to buy Bitcoins](#)

For you to check that we truly have the keys saved and your files will be decrypted when you pay, we let you select ONE file that will be decrypted for free. The key will be decrypted in the server.

[Select file](#)

## Ransom32 - Stats

Address   
Payout ratio 75%

Installs    
Lockscreens    
Paid    
Paid BTC

## Client download

BTC amount to ask:   
Don't be too greedy or people will not pay

Fully lock the computer

Low CPU usage

Show the lockscreen before encrypting

Show a message box

- Critical Error
- Yellow Exclamation
- White Information

Latent Timeout

- Days:

- Hours:

- Minutes:

[Download client.scr](#)

Don't worry if the download "hangs". While the download bar is shown, Tor is receiving the file. Just wait.



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://petya37h5tbhyvki.onion/>

<http://petya5koahtsf7sv.onion/>

3. Enter your personal decryption code there:

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

Key: \_

# PROFIT FROM PETYA & MISCHA!

## HIGH INFECTION RATES

PETYA comes bundled 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 completely 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.

# 2016: Jigsaw

I will play a game with you. Let me explain the rules:  
Your personal files are being deleted. Your photos, videos, documents, etc...  
But, don't worry! It will only happen if you don't comply.  
However I've already encrypted your personal files, so you cannot access them.

Every hour I select some of them to delete permanently,  
therefore I won't be able to access them, either.  
Are you familiar with the concept of exponential growth? Let me help you out.  
It starts out slowly then increases rapidly.  
During the first 24 hour you will only lose a few files,  
the second day a few hundred, the third day a few thousand, and so on.

If you turn off your computer or try to close me, when I start next time  
you will get 1000 files deleted as a punishment.  
Yes you will want me to start next time, since I am the only one that  
is capable to decrypt your personal data for you.

Now, let's start and enjoy our little game together! \_



59:47

**1 file will be deleted.**

[View encrypted files](#)

**Please, send at least \$23 worth of Bitcoin here:**



[I made a payment, now give me back my files!](#)





Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

1. Go to [REDACTED] ( IF NOT WORKING JUST DOWNLOAD TOR BROWSER AND OPEN THIS LINK: [REDACTED] )
2. Use [REDACTED] as your ID for authentication
3. Pay 1 BTC (~407.97\$) for decryption pack using bitcoins (wallet is your ID for authentication - [REDACTED])
4. Download decrypt pack and run

---> Also at [REDACTED] you can decrypt 1 file for FREE to make sure decryption is working.

Also we have ticket system inside, so if you have any questions - you are welcome. We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS

HOW TO BUY BITCOINS:

<https://localbitcoins.com/guides/how-to-buy-bitcoins>

[https://en.bitcoin.it/wiki/Buying\\_Bitcoins\\_\(the\\_newbie\\_version\)](https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version))



 犯罪者情報

 オフェンス情報

 ファインのお支払い

 取扱説明の解除



注意！お使いのデバイスがロックされている、その理由を以下に示します

残り時間は、罰金を支払います

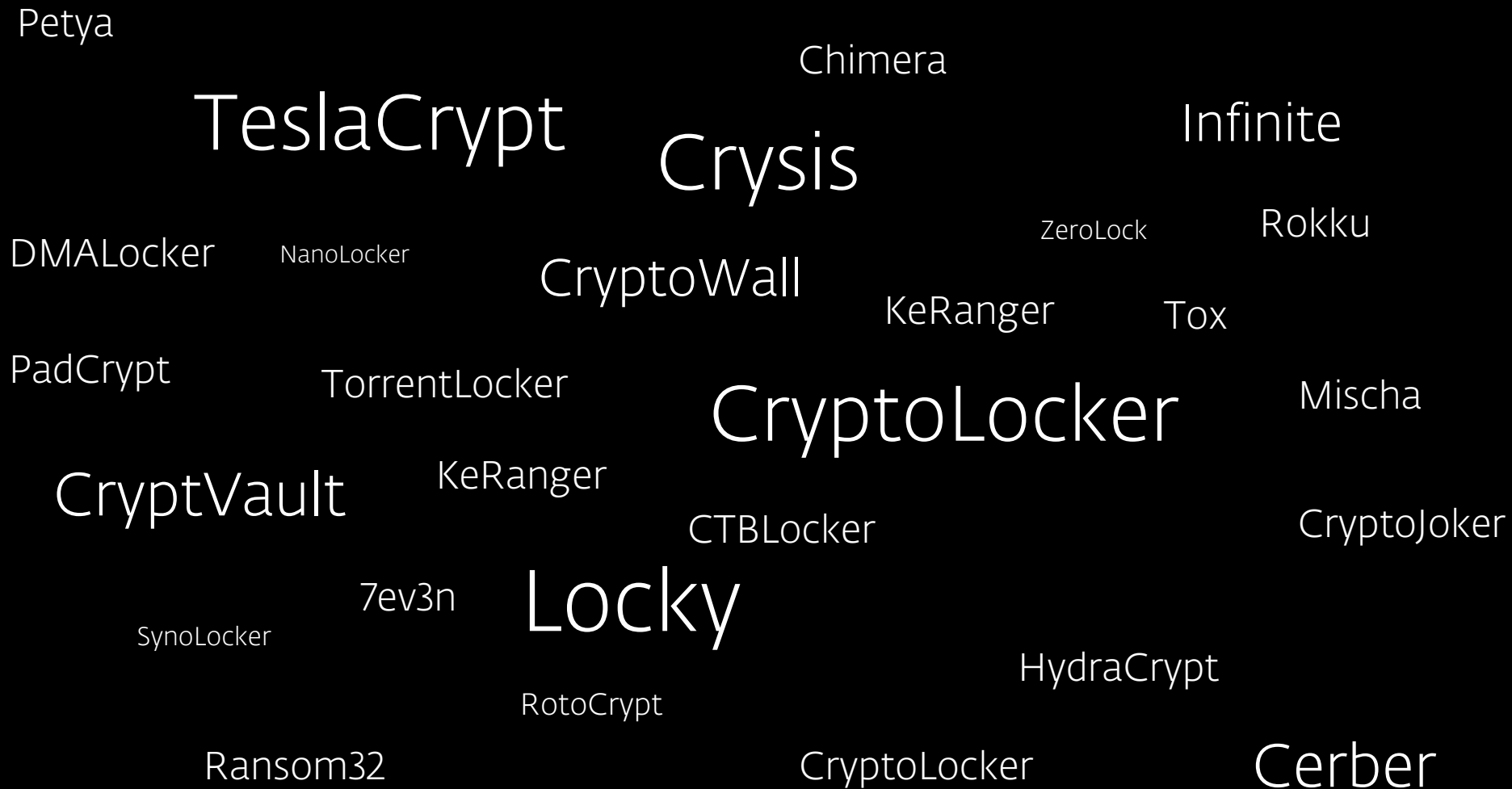
71:58:24

それ以外の場合はケースファイルは、裁判所に転送されます

履歴クエリは、国土安全保障省のデータベースに格納されています

犯罪者情報





A word cloud of ransomware names on a black background. The names are in white, sans-serif font. The size of each name varies, with 'CryptoLocker' and 'Locky' being the largest. Other names include 'TeslaCrypt', 'Crysis', 'Chimera', 'Infinite', 'CryptoWall', 'KeRanger', 'TorrentLocker', 'CryptVault', 'CTBLocker', '7ev3n', 'Ransom32', 'Rokku', 'ZeroLock', 'Tox', 'Mischa', 'CryptoJoker', 'HydraCrypt', 'Cerber', 'Petya', 'DMALocker', 'NanoLocker', 'PadCrypt', 'SynoLocker', and 'RotoCrypt'.

Petya

Chimera

TeslaCrypt

Crysis

Infinite

DMALocker

NanoLocker

CryptoWall

ZeroLock

Rokku

KeRanger

Tox

PadCrypt

TorrentLocker

CryptoLocker

Mischa

CryptVault

KeRanger

CTBLocker

CryptoJoker

7ev3n

Locky

SynoLocker

RotoCrypt

HydraCrypt

Ransom32

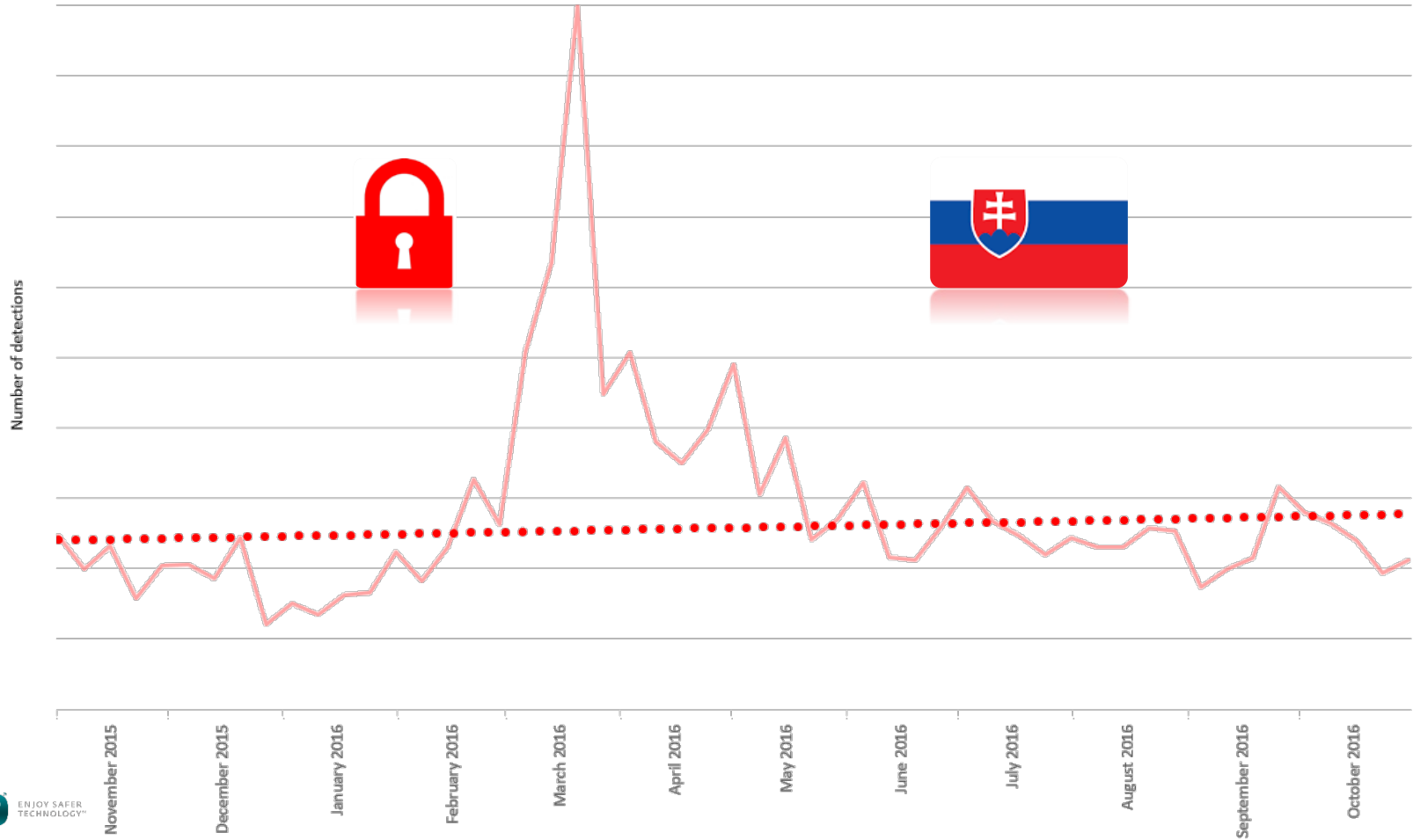
CryptoLocker

Cerber

Hundreds of families !

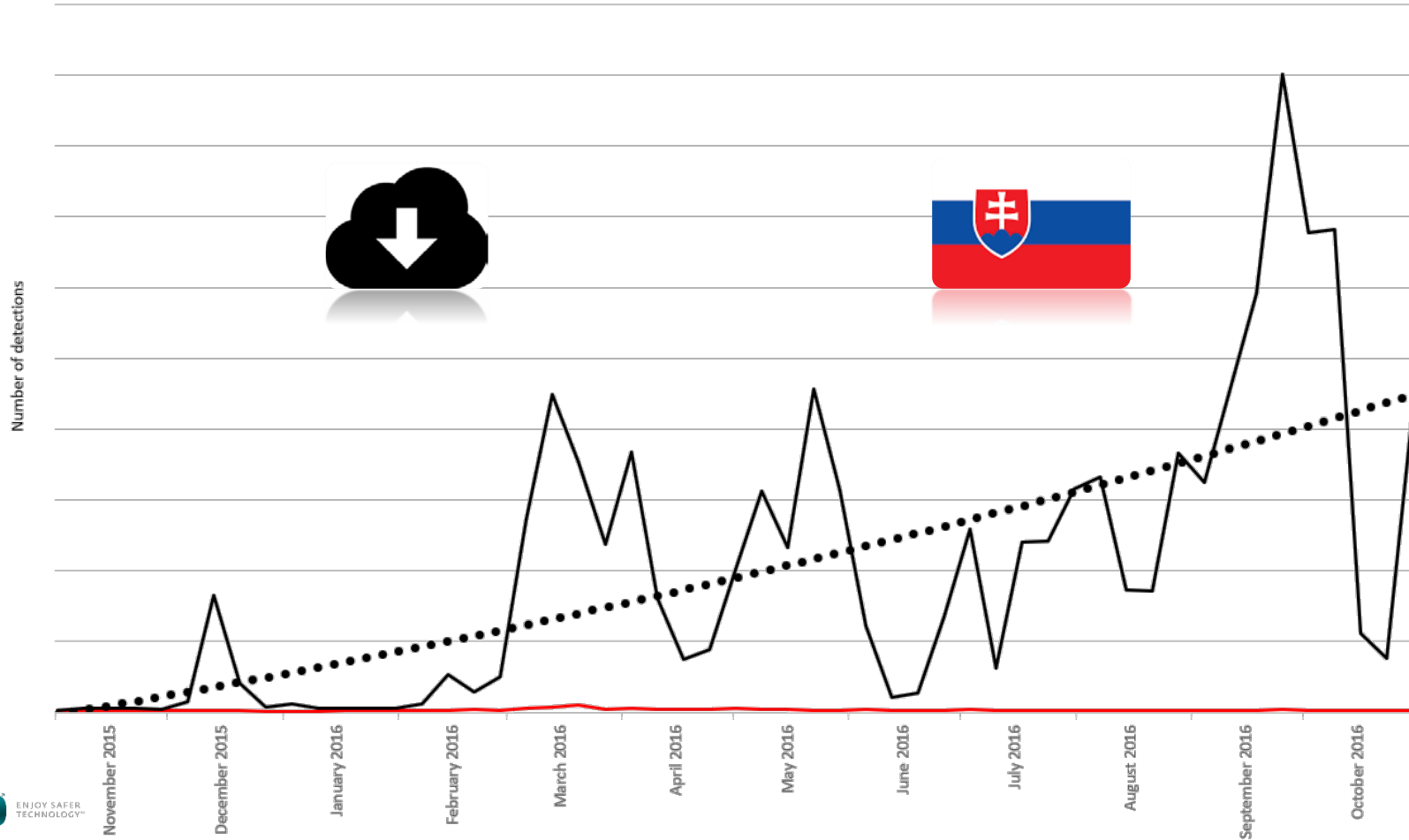
New family every day !

Ransomware detection statistics in Slovakia Nov 2015 - Oct 2016, according to ESET LiveGrid®

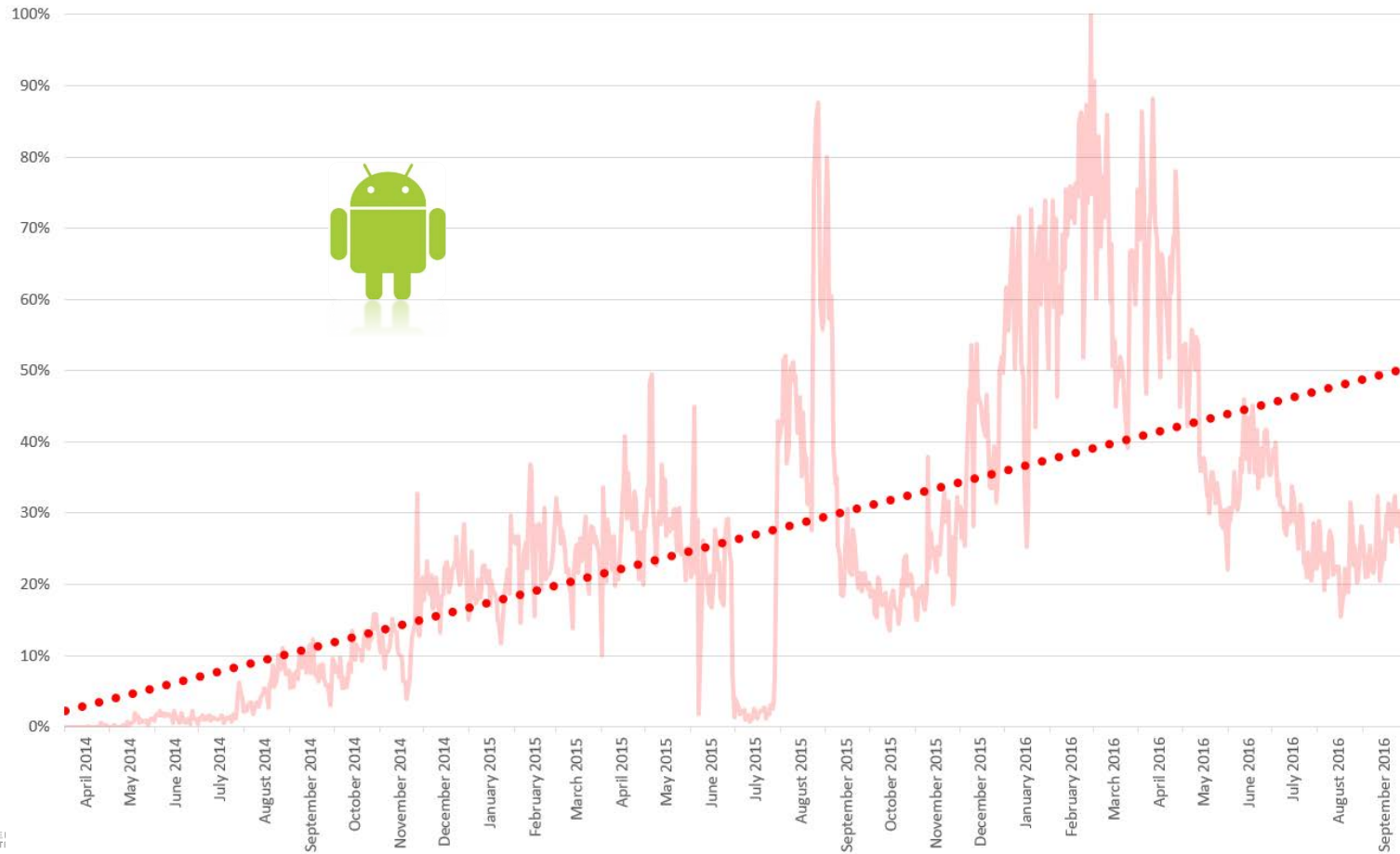




Detection statistics of downloaders often trying to download ransomware in Slovakia Nov 2015 - Oct 2016, according to ESET LiveGrid®



# Android ransomware detection statistics, according to ESET LiveGrid®



**i** News The Essen

Dozens of N  
by cyber bla

**HACKED**  
FUTURE. TECHNOLOGY.

**REPORT: HEALTHCARE SERVICES PAY NEARLY \$100 MILLION TO RANSOMWARE**

Los Angeles Times

Hollywood hospital pays \$17,000 in bitcoin to hackers; FBI investigating

23 March 2016 | Technology

FEBRUARY 18, 2016, 10:44 AM

New server-targeting malware hitting healthcare

SEAN GALLAGHER - 3/30/2016, 1:11 AM

**SOFTPEDIA**®  
DESKTOP

Softpedia > News > Security > Virus alerts

**Brazilian Hospitals Infected with Ransomware After RDP Brute-Force Attacks**

Share:

Los Angeles Times

# Hollywood hospital pays \$17,000 in bitcoin to hackers; FBI investigating

FEBRUARY 18, 2016, 10:44 AM

- ⚡ No email access
- ⚡ No access to patient records/medical test results, documentation disrupted
- ⚡ Lab work disrupted, pharmacy disrupted
- ⚡ No CT scans, Radiation Oncology department temporarily shut down
- ⚡ Ambulances and patients turned away and sent to other hospitals Unable to access
- ⚡ 10 days downtime, ransom paid \$17,000



## January 2016 Cybersecurity Snapshot Global Results

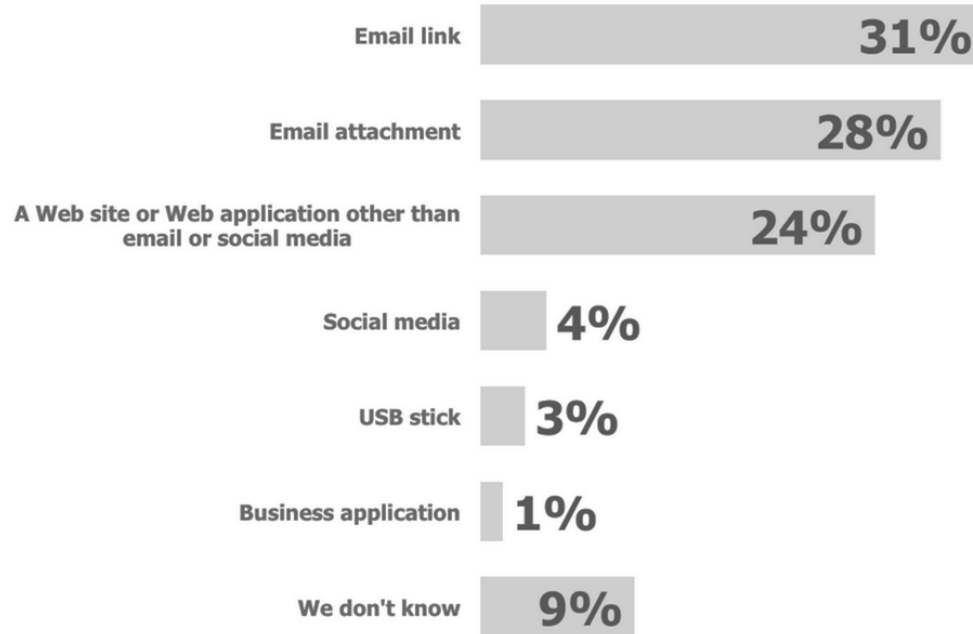
[www.isaca.org/2016-cybersecurity-snapshot](http://www.isaca.org/2016-cybersecurity-snapshot)

Number of respondents (n) = 2,920

3. Of the following threats, which **THREE** are of most concern to your organization in 2016? (Please select up to three.) *n=2,920*

Advanced persistent threat (APT)	39%
DDoS	25%
Ransomware	20%
Social engineering	<b>52%</b>
Watering hole	2%
Insider threats	40%
Malware	30%
Mobile malware	19%
Unpatched systems	31%
Cybercrime	32%
None of the above	1%

# “Applications by which ransomware entered the organization”



***“More than 97% of phishing emails delivered in 2016 contained ransomware..”***

Reported by **PHISHME**.com, Q3 2016

# Prevenca

1. OS & aplikácie aktualizované a zaplátané
  - ✓ Prípony súborov (faktura.PDF.**EXE**)
  - ✓ Spustiteľné prílohy emailu (BAT, CMD, EXE, SCR, JS, VBS...)
  - ✓ Zdieľané lokality
  - ✓ Používateľské práva
  - ✓ System Restore
  - ✓ RDP
  - ✓ Windows Script Host
  - ✓ „Open with...“ Notepad
  - ✓ %LocalAppData% a %AppData%
2. Bezpečnostné riešenie
3. Pravidelné zálohovanie (offline, Schrödinger)
4. Tréning zamestnancov





# Prevenca

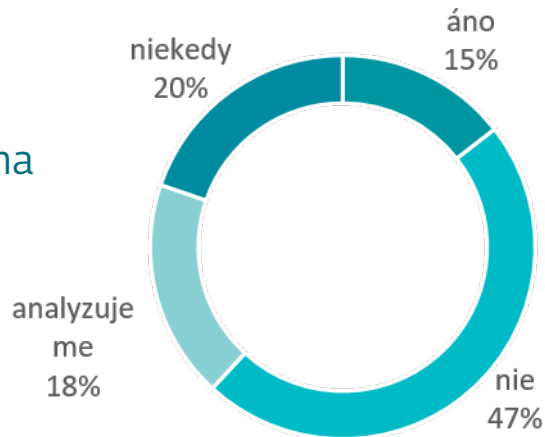
1. OS & aplikácie aktualizované a zaplátané
  - ✓ Najnovšia verzia
  - ✓ Aktualizovaná malware databáza
  - ✓ LiveGrid
  - ✓ HIPS



2. Bezpečnostné riešenie
3. Pravidelné zálohovanie (offline, Schrödinger)
4. Tréning zamestnancov

# Čo v prípade infekcie?

1. Zastaviť šifrovanie
2. Kontaktovať technickú podporu
  - ✓ Logy
  - ✓ Vzorky (ne/zašifrované)
  - ✓ Dešifrovanie
  - ✓ Obnova zo zálohy
  - ✓ Uchovanie do budúca



# Hľadanie chýb ransomwaru

- ✓ Slabý generátor kľúčov (DMA, CryptProjectXXX)
- ✓ Slabý šifrovací algoritmus (XORist, 7ev3n)
- ✓ Chyby v implementácii šifrovacieho algoritmu (Petya)
- ✓ Kľúč v kóde (Simplocker, Jigsaw)
- ✓ Uniknuté kľúče (Chimera)
- ✓ ...

[All Posts](#)[Latest Research](#)[How To](#)[Multimedia ▾](#)[Papers ▾](#)[Our Experts](#)

## ESET releases new decryptor for TeslaCrypt ransomware

BY PETER STANCIK POSTED 18 MAY 2016 - 08:51PM

CYBERCRIME

Follow us



Sign up to our newsletter

The latest security news direct to your inbox

HOT TOPIC

5 ARTICLES RELATED TO:

### GOOGLE PLAY PORN CLICKER



5.3K

Like




37

G+

328

in Share

```
C:\WINDOWS\system32\cmd.exe - ESETTeslaCryptDecoder.exe c:
C:\Documents and Settings\Administrator\Desktop>ESETTeslaCryptDecoder.exe c:



TeslaCrypt decryptor
Version: 1.1.0.0
Built: May 18 2016

Copyright (c) ESET, spol. s r.o.
1992-2015. All rights reserved.

OS: 5.1.2600 SP3
Product Type: Workstation
WoW64: False
Machine guid: 113B62F0-8DF1-4776-918E-0710E7F0FEE6

Supported TeslaCrypt version : 3.0.0 - 4.2
Looking for infected files...
```

# Crysis decryptor

```
C:\Documents and Settings\Administrator\Desktop\ESETCrysisDecryptor.exe

ESET

Crysis decryptor
Version: 2.0.0.0
Built: Nov 18 2016

Copyright (c) ESET, spol. s r.o.
1992-2016. All rights reserved.

-----

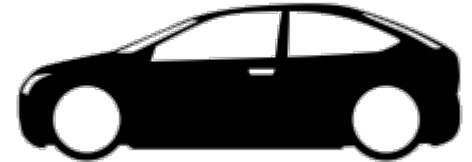
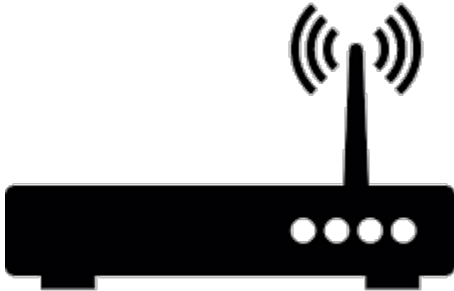
OS: 5.1.2600 SP3
Product Type: Workstation
WoW64: False
Machine guid: 113B62F0-8DF1-4776-918E-0710E7F0FEE6

Supported Crysis file extensions: .xtbl, .crisis, .crypt
```

# Will it go away soon?



# Will it go away soon?



# Platiť, či neplatiť?



1. Žiadna záruka ochoty / schopnosti súbory dešifrovať
2. Zaplatením podporíte vývoj ďalšieho malwaru
3. Žiadna záruka, že nezaútočia znova

✓ PREVENCIA

✓ ZÁLOHA

✓ DEKRYPTOR





Peter Stančík  
*Security Evangelist*

**stancik@eset.sk**

**welivesecurity.com**  
news, views and insight from the ESET security community