



ENJOY SAFER TECHNOLOGY™

RANSOMWARE V PRAXI

Peter Stančík

AGENDA

- Evolúcia a súčasný stav
- Ako chránime my
- Aké sú naše odporúčania

AGENDA



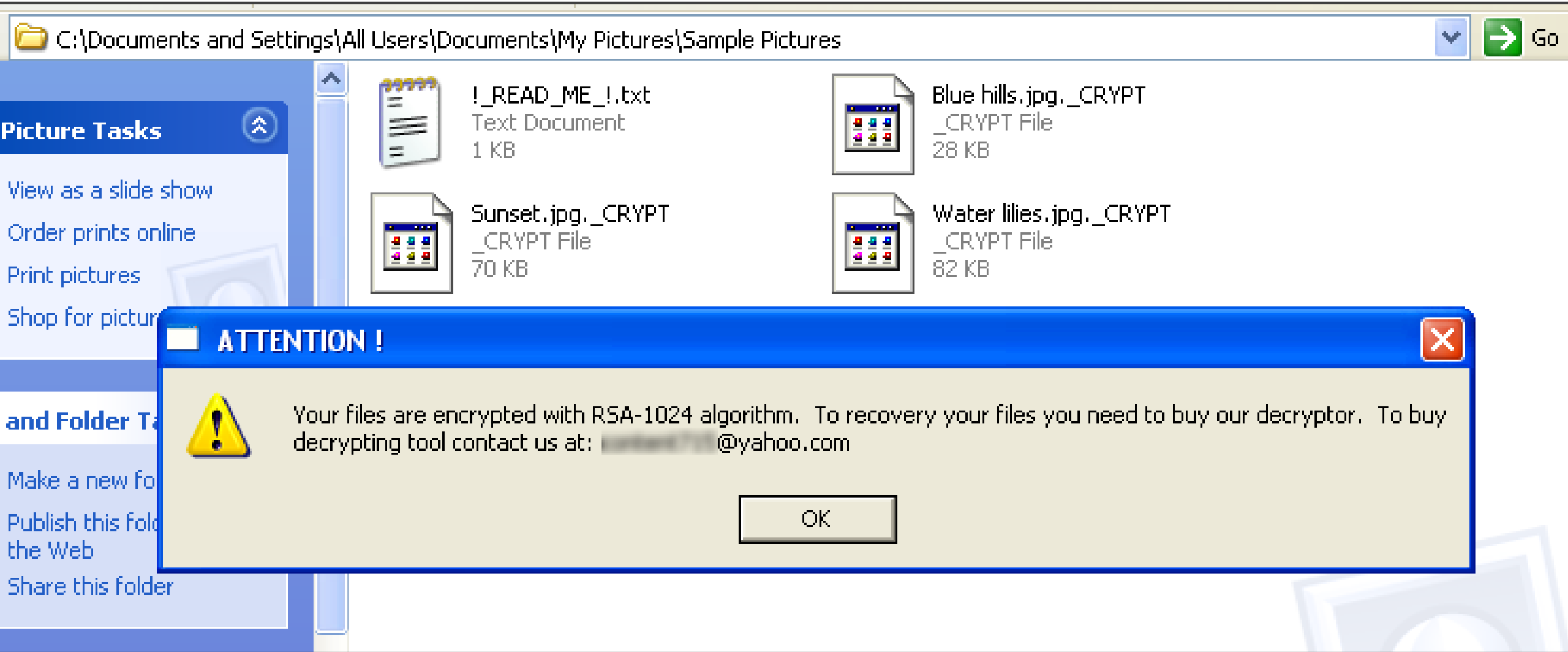
“Cyber- criminals collected \$209 million in the first three months of 2016 by extorting businesses and institutions to unlock computer servers. At that rate, ransomware is on pace to be a \$1 billion a year crime this year. ”

[FBI for money.CNN.com](#), April 2016

Case \$1,000,000,000 rates

50 talents (1550 kg) of silver
business





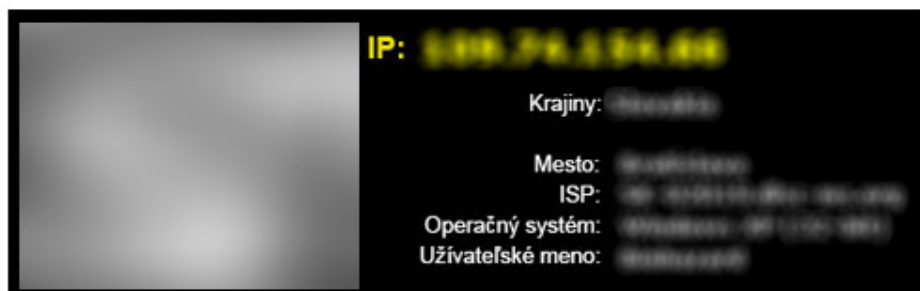
Computer is Blocked!

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.



Zostávajúci čas: 47:56:09



VAROVANIE! Váš osobný počítač je uzamknutý z bezpečnostných dôvodov by z nasledujúcich dôvodov:

Ste obvinený z prezerania/skladovania a/alebo distribúcia pornografických materiálov zakázané obsahu (detská pornografia/zvierackosti atď) že ste porušil Všeobecnú deklaráciu o boji proti šíreniu detskej pornografie a obvinený z trestného činu podľa článku 161 trestného zákonníka Slovenskej republiky.

Článok 161 trestného zákonníka Slovenskej republiky ustanovuje ako trest odňatia slobody v trvaní 5-11 rokov.

Tiež ste osoba podozrivá z porušenia "zákon o autorskom práve a právach súvisiacich s právom" (sťahovanie pirátskej hudby, videa neletsenzionnogo softvér) a použitia a/alebo šírenie obsahu chráneného autorským právom. Tým ste osoba podozrivá z porušenia článku 148 trestného zákonníka Slovenskej republiky.

Článok 148 trestného zákonníka Slovenskej republiky, musí byť trest pokuta 150 až 550 základných jednotiek alebo odňatím slobody na dobu 3-7 rokov.

S počítačom došlo k neoprávnenému prístupu k obmedzenému prístupu verejnosti k informáciám a informáciám celoštátneho významu v Internete.

Neautorizovaný prístup si môžete dojednať zámerne z sebeckých motívov alebo neoprávneným

PIN kód

 100

 1 2 3 4 5 6 7 8 9 0

Odoslať

Kde môžem získať peňažné poukážku PaySafeCard?

Prehľad predajcov: PaySafeCard dostaneš v mnohých supermarketoch, trafikách. PaySafeCard dostaneš na viac ako 101 čerpacích staniách Agipu a OMV, vo vybraných pobočkách stávkovej kancelárie Tipsport, všetkých predajných miestach GG Tabaku a vo CBA.





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 >>



**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:

[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 [REDACTED]
Payout ratio 75%

Installs i	0
Lockscreens i	0
Paid i	0
Paid BTC i	0

Client download

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

☒ Fully lock the computer i

☒ Low CPU usage i

☒ Show the lockscreen before encrypting i

☒ Show a message box i

- ☐ Critical Error
- ☒ Yellow Exclamation
- ☐ White Information

☒ Latent Timeout i

- 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 haddisks 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.

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ense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



Restoring your files - The fast and easy way

To get your files fast, please transfer **1.0 Bitcoin** to our wallet address **1LEiPgVh699VEXWV2dZytSRd7e9B1bWt3**. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

Restoring your files - The nasty way

Send the link below to other people, if two or more people will install the file and pay, we will decrypt your files for free.

<https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5>



Petya

Chimera

TeslaCrypt

Infinite

Crysis

DMA Locker

NanoLocker

ZeroLock

Rokku

CryptoWall

KeRanger

Tox

PadCrypt

WannaCryptor

CryptoLocker

Mischa

CryptVault

KeRanger

CTBLocker

CryptoJoker

7ev3n

Locky

SynoLocker

HydraCrypt

RotoCrypt

Ransom32

CryptoLocker

Cerber

Hundreds of families !

New family every day !

i News The Essential

HACKED

Malware

What is 'WanaCryptor 2.0' ransomware and why is it attacking the NHS?

Malicious software has attacked computers across the NHS and companies in Spain, Russia, the Ukraine and Taiwan. What is it and how is it holding data to ransom?



Alex Hern and Samuel Gibbs

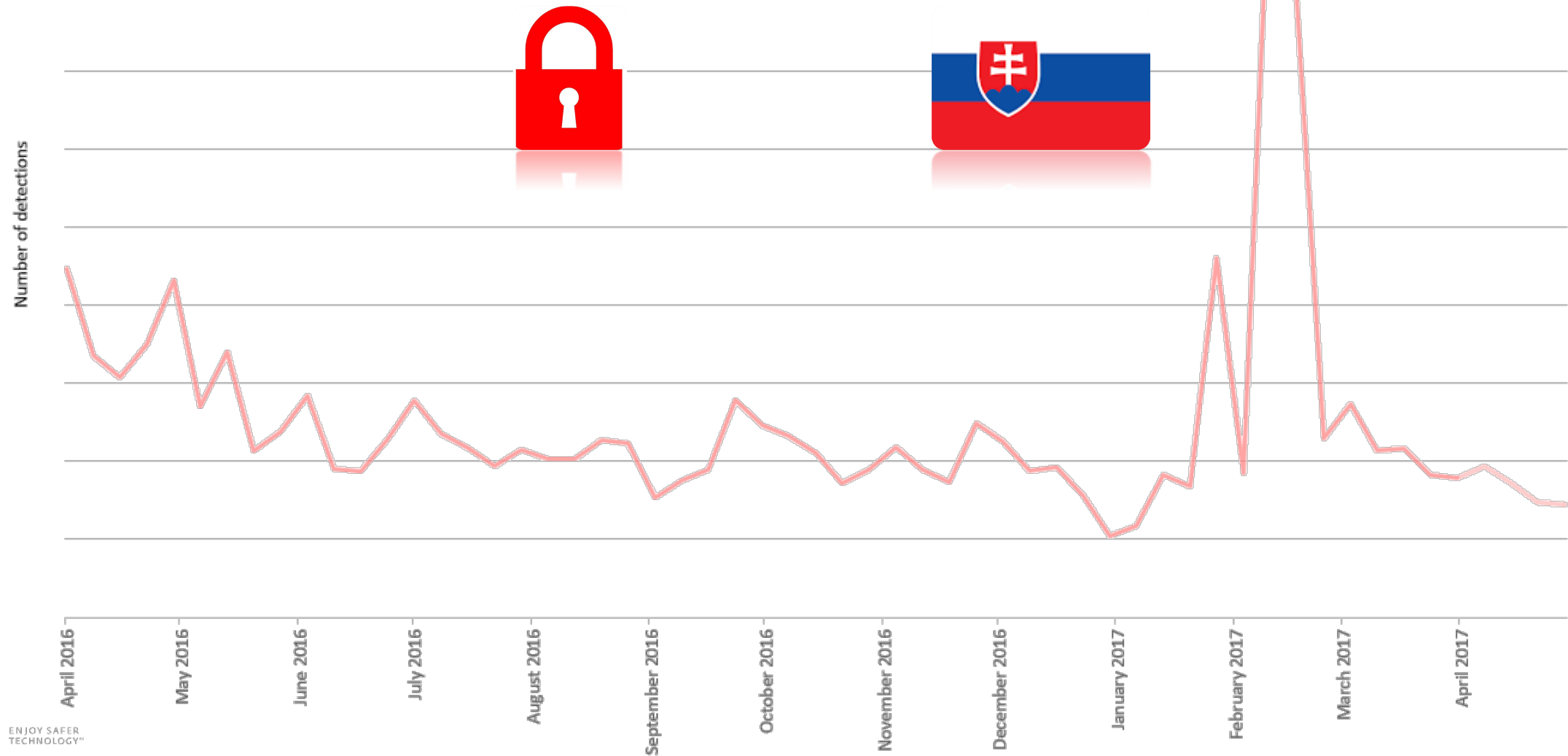
Friday 12 May 2017 17.16 BST



PBELL
1, 2016

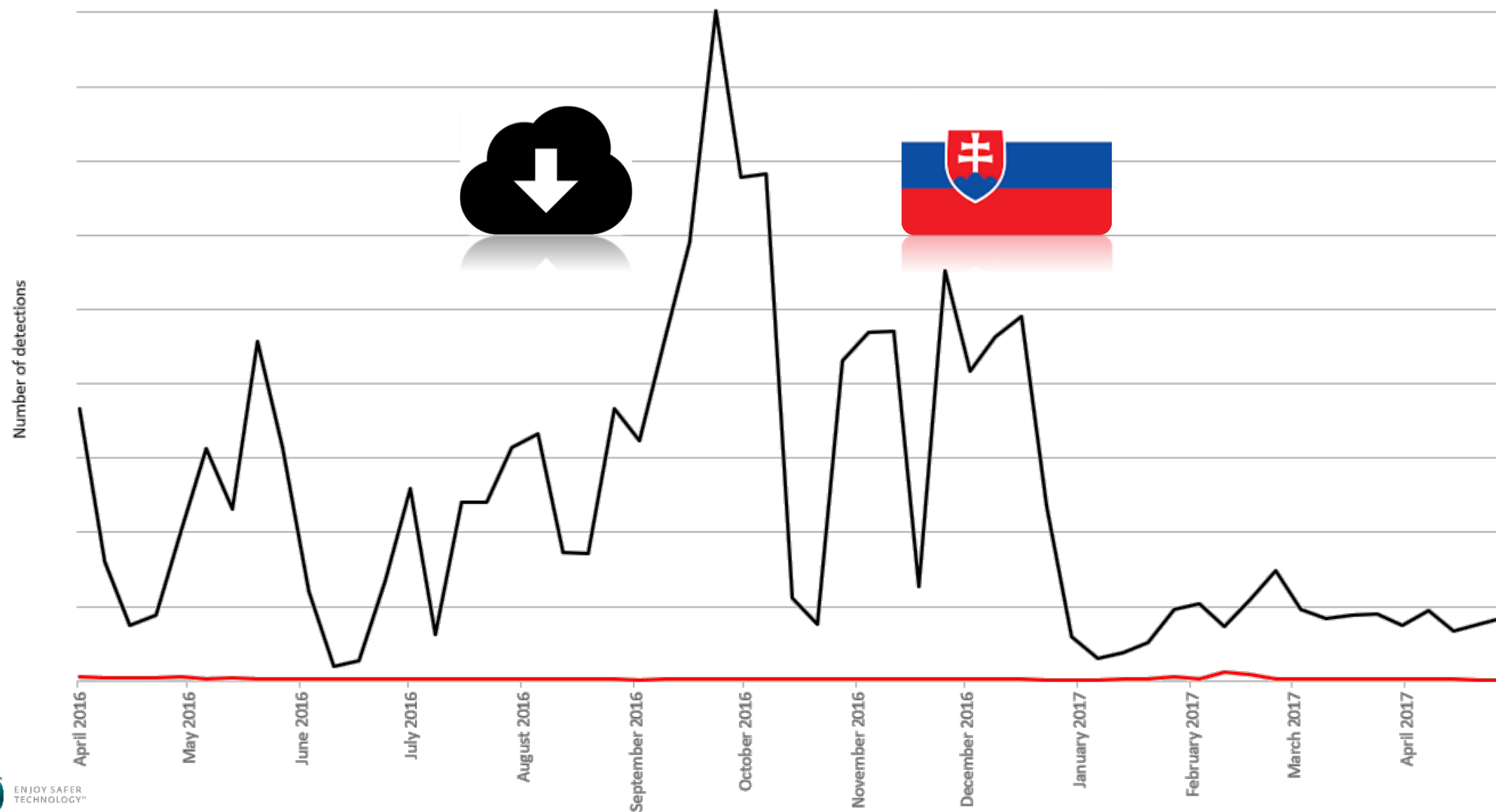
Ransomware detection statistics in Slovakia Apr 2016 - Apr 2017

Source: ESET LiveGrid®

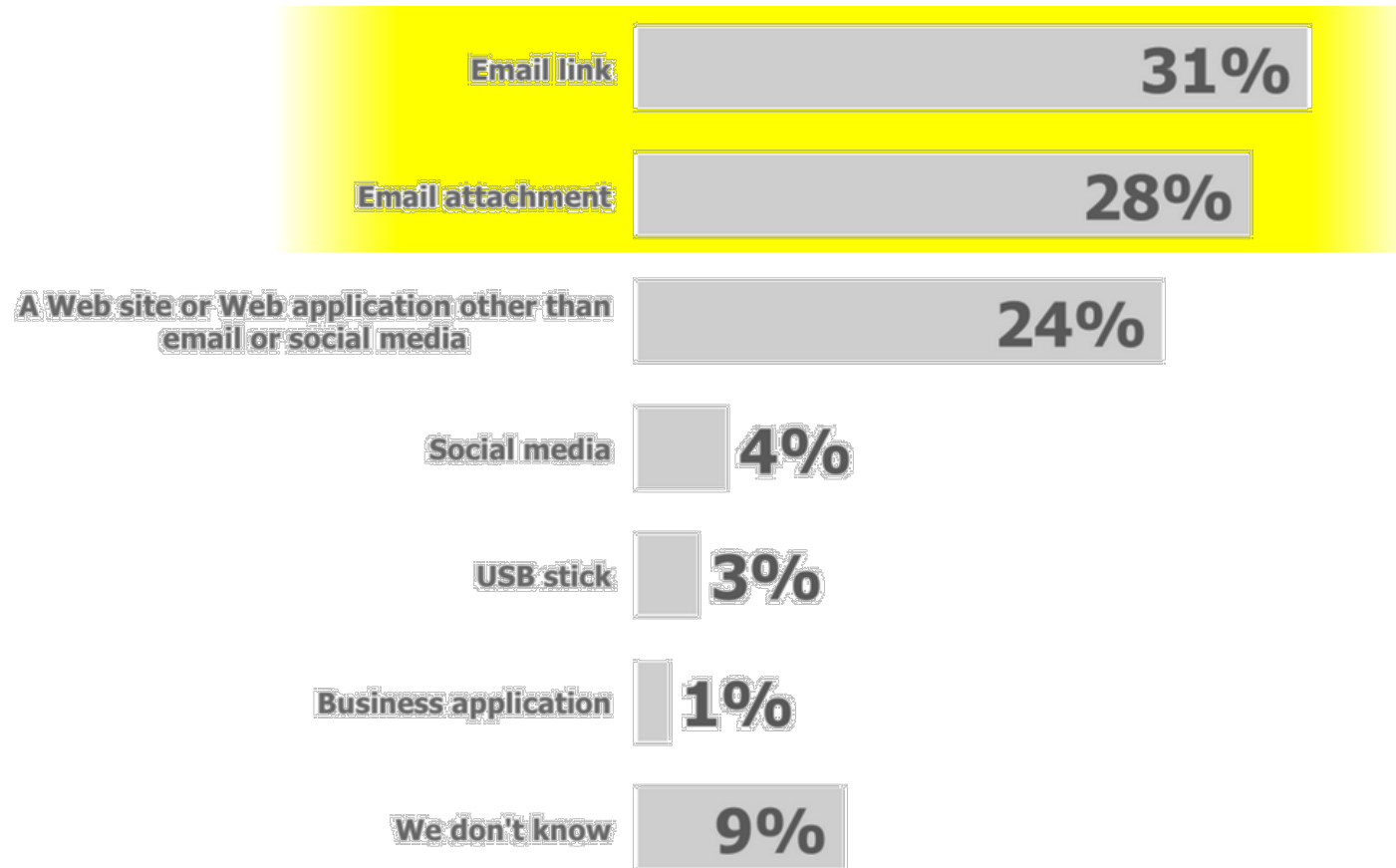


Detection statistics of downloaders often trying to download ransomware in Slovakia Apr 2016 - Apr 2017

Source: ESET LiveGrid®



“Applications by which ransomware entered the organization”



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

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

January 2016 Cybersecurity Snapshot Global Results

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	52%
Watering hole	2%
Insider threats	40%
Malware	30%
Mobile malware	19%
Unpatched systems	31%
Cybercrime	32%
None of the above	1%

AGENDA

- Evolúcia a súčasný stav
- Ako chránime my
- Aké sú naše odporúčania



NETWORK ATTACK
PROTECTION



REPUTATION
& CACHE



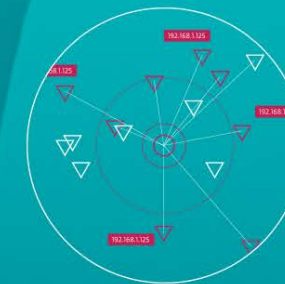
CLOUD BASED
PROTECTION SYSTEM



ADVANCED
MEMORY SCANNER



EXPLOIT
BLOCKER



BOTNET
PROTECTION



ADVANCED
HEURISTICS

ESET Ransomware Shield



Hľadanie chýb ransomwaru

- ✓ Slabý generátor kľúčov ([DMA](#), [Crypt Project XXX](#))
- ✓ Slabý šifrovací algoritmus ([XORist](#), [7ev3n](#))
- ✓ Chyby v implementácii šifrovacieho algoritmu ([Pet ya](#))
- ✓ Kľúč v kóde ([Simplocker](#), [Jgsaw](#))
- ✓ 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

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:

  eSet

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...
```

HOT TOPIC

5 ARTICLES RELATED TO:

GOOGLE PLAY PORN CLICKER



A stylized world map in shades of teal and light blue, centered on the Atlantic Ocean. The map shows the outlines of continents and some internal country borders. The number 126.564 is superimposed over the map.

126.564

AGENDA

- Evolúcia a súčasný stav
- Ako chránime my
- Aké sú naše odporúčania

Prevencia

1. OS & aplikácie aktualizované a zaplátané
2. Bezpečnostné riešenie
3. Pravidelné zálohovanie
4. Tréning zamestnancov

Prevencia

1. OS & aplikácie aktualizované a zaplátané
2. Bezpečnostné riešenie
 - ✓ Prípony súborov (faktura.PDF.EXE)
3. Prípustné náhľady emailu (BAT, CMD, EXE, SCR, JS, VBS...)
4. Zdieľané lokality
 - ✓ Používateľské práva
 - ✓ System Restore
 - ✓ RDP
 - ✓ Windows Script Host
 - ✓ „Open with...” Notepad
 - ✓ %LocalAppData% a %AppData%



Prevencia

1 OS & aplikácie aktualizované a zaplátané

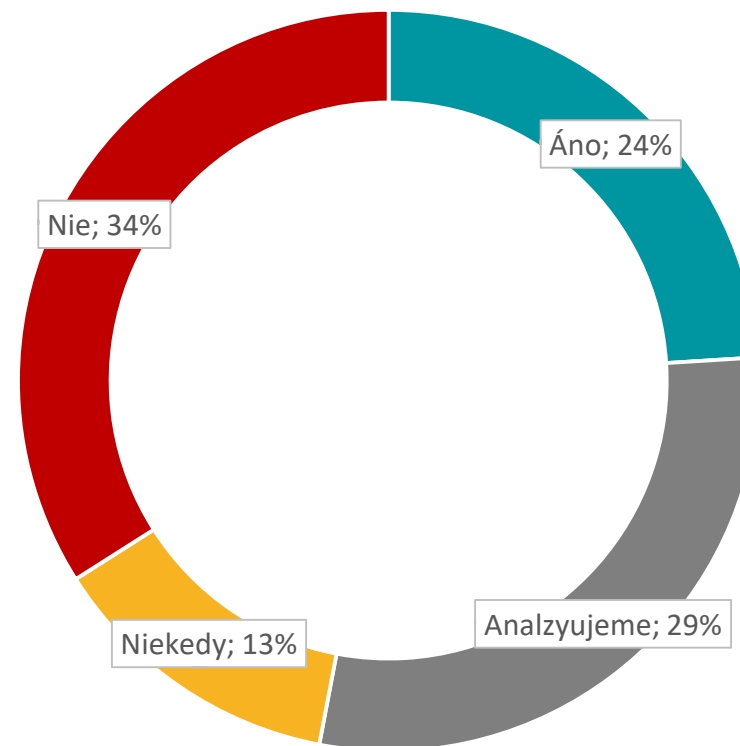
- ✓ Najnovšia verzia
- ✓ Aktualizovaná malware databáza
- ✓ LiveGrid
- ✓ HIPS



- ## 2. Bezpečnostné riešenie
- ## 3. Pravidelné zálohovanie
- ## 4. Tréning zamestnancov

Čo v prípade infekcie?

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



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





ENJOY SAFER TECHNOLOGY™

ĎAKUJEM

Peter Stančík

Security Research and Awareness Manager

stancik@eset.sk

eset.com | welivesecurity.com