KASPERSKY lab

GREAT

STAND AND DELIVER!
YOUR MONEY OR YOUR FILES

David Emm

Global Research and Analysis Team

WHAT IS RANSOMWARE?

‘A type of malicious software designed to block access to a computer system until a sum of money is paid’

www.oxforddictionaries.com

‘Ransomware is malware for data kidnapping, an exploit in which the attacker encrypts the victim’s data and demands payment for the decryption’

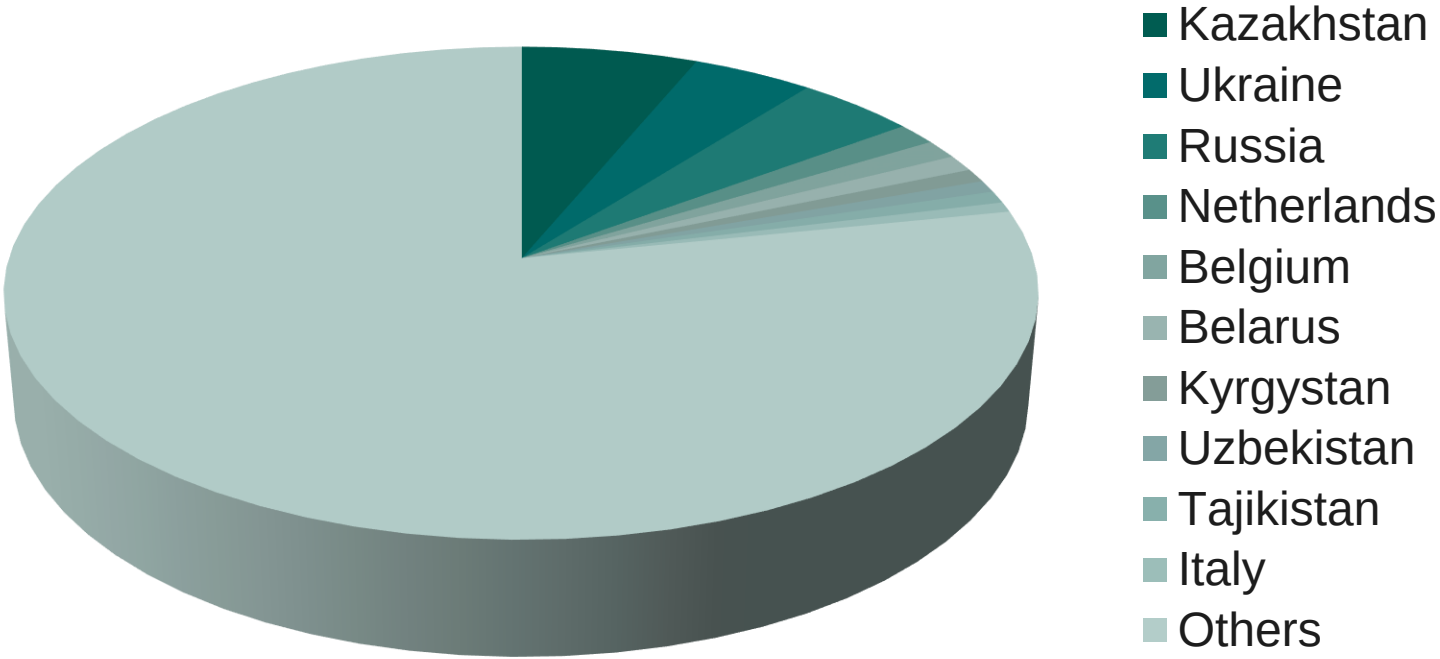
www.whatis.techtarget.com

A GROWING PROBLEM

- 753,684 detections in 2015
- 179,209 were cryptors
- ~20 per cent were in the corporate sector
- 40 per cent increase from 2014
- The numbers under-estimate the problem
  - Signature detections only
  - ~ 40 per cent of all detections
- 17 per cent of detections were on Android devices

THE GEOGRAPHY OF RANSOMWARE

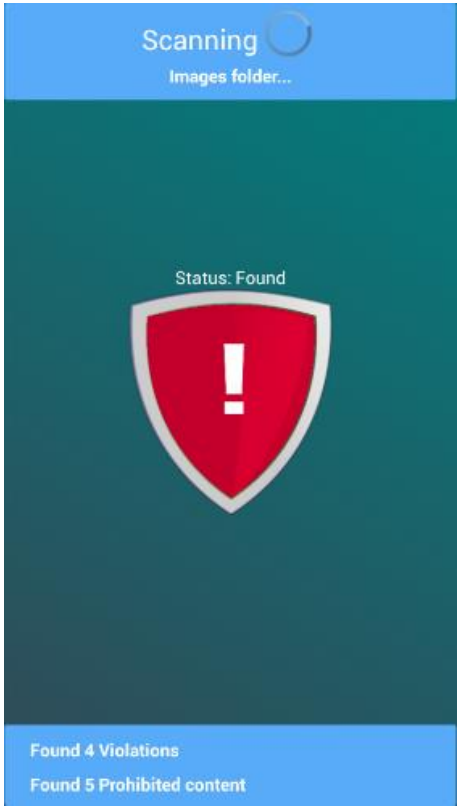
Top 10 countries by risk of infection in 2015

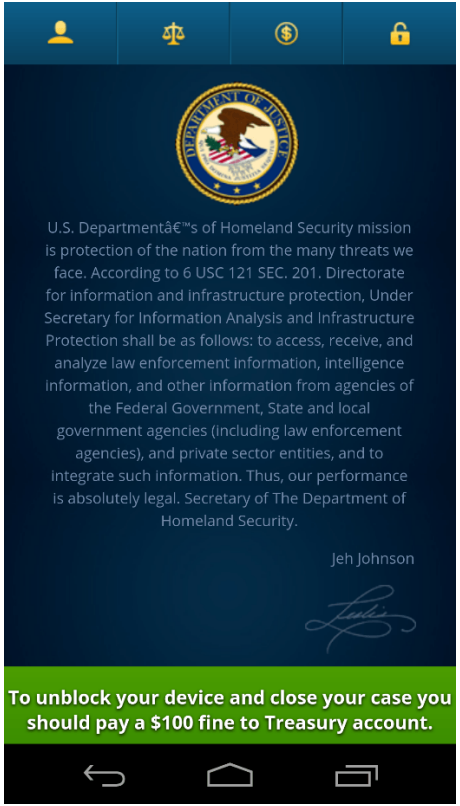


BLOCKERS

За просмотр запрещенного(Педофилия,Зоофилия и т.д.) порно ваш телефон блокирован!

Все Фото и видео материалы с вашей камеры переданны на рассмотрение.
Для разблокировки вашего телефона и удаление метериалов
вам необходимо оплатить штраф 1000 руб. в течении 24 часов
Для этого вам нужно пополнить Номер +79147011354
В ближайшем терминале оплаты.
ВНИМАНИЕ: При попытке избежать штрафа
Все данные будут направленны в публичные источники





YOUR FILES HAVE BEEN

CoinVault

View encrypted filelist

Time untill costs raise

Loading...

How to pay | One free decrypt!

Total costs:

btc € 0,00

Paid:

btc € 0,00

Check payment and receive keys

key: IV:

Decrypt using keys

Your personal documents and files on this computer have just been encrypted.
The original files have been deleted and will only be recovered by following the steps described below.
Click on "View encrypted files" to see a list of files that got encrypted.

The encryption was done with a unique generated encryption key (using AES-256).
This means the encrypted files are of no use until they get decrypted using a key stored on a server.

This server will only release the key if the amount of Bitcoins (displayed left of this window)
is send to the Bitcoin address shown underneath this window.

Each time the timer hits zero, the total costs will raise with the starting price.

After the purchase is made, please wait a few minutes for confirmation of the Bitcoins.
You can check whether the Bitcoins are confirmed with the 'check payment and receive keys' button.
After payment and confirmation, your keys will appear in the textboxes.
After that, you simply click 'decrypt using keys'.
Your files will be decrypted and restored to their original location.

You can decrypt one file for free, using the 'One free decrypt' button.

You can easily delete this software, but know that without it, you will never be able
to get your original files back.

For more information on how to buy and send Bitcoins, click 'How to pay'.

Need help or support?
mail: coinvault@openmailbox.org (primary e-mail address)
backup mail: coinvault@tutanota.de (in case primary e-mail doesn't work)

Last check: 1/21/2016 12:08:37 PM

Send bitcoins to this bitcoin address: Copy

TorLocker

Your important files produced in this computer and network shares: photos, videos, documents, pdf, music, autocad, spreadsheets, etc. , were encrypted.

If you see this text but do not see the "TorLocker" window, then your antivirus removed "TorLocker" from your computer.

If you need your files back, you have to recover "TorLocker" from the antivirus quarantine, or find a copy of "TorLocker" in the internet and start it again.

Please disable any Firewall or Antivirus permanently if the Payment address don't show to you

You can download "TorLocker" from the link given below, using the tool "Tor Browser Bundle"

http://[redacted].onion/851B1EA29B9323685D6812D6D9F9D660.exe

INFECTION

- Decrypts its own data section using 256-bit AES key
  - The first four bytes of this key are added to the end of encrypted files and are used as Trojan ID
- Searches for ‘taskmgr.exe’, ‘regedit.exe’, ‘procexp.exe’ and ‘procexp64’ processes and terminates them
- Deletes all system recovery points
- Edits registry to load Trojan automatically at start-up

ENCRYPTION

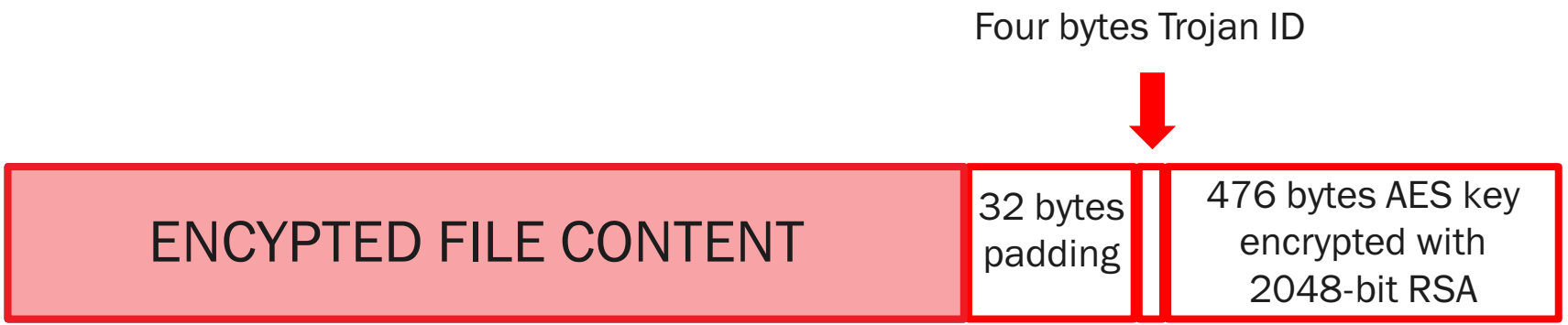
- Encrypts data on hard disk and network drives
- Each sample contains its own set of public keys
- Selects one of 128 public RSA keys hard-coded in Trojan
  - Based on computer name and the serial number of the logical drive
- Number (n) of the public RSA key is calculated as follows:

> **n = (VolumeSerialNumber * strlen(ComputerName)) mod 128,**
> where **strlen(ComputerName)** is the length of the computer's name, and **VolumeSerialNumber** is the serial number of the logical drive on which Winsow is installed.

ENCRYPTION

GREAT

- Encrypts files using 256-bit AES
- Randomly-generated one-time key
- Individual encryption key for each file



www.securelist.com/blog/research/69481/a-flawed-ransomware-encryptor/

KASPERSKY lab

WHAT IS A 256-BIT KEY?

- A string of 256 ones and/or zeroes: 1001010010101010111 …
- 2^{256} possible combinations
- If you find the key in the first 50 per cent, you only have 2^{255} combinations
- If you had a billion modern GPUs at 2 Gigaflops each, you could crack $6.3x10^{25}$ keys per year
- $2^{255} \div 6.3x10^{25} = 9.1x10^{50}$ years
- It would take ~ $7x10^{40}$ times longer than the age of the universe to exhaust half the key-space of a 256-bit AES key

https://www.reddit.com/r/theydidthemath/comments/1x50xl/time_and_energy_required_to_bruteforce_a_aes256/

Your personal files are encrypted!

Private key will be destroyed on

Time Left

Your important files are encrypted produced on this computer: photos, videos, documents, etc. Click <<List Of Encrypted files>> to see a complete list of encrypted files, and you can verify this.

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

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

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

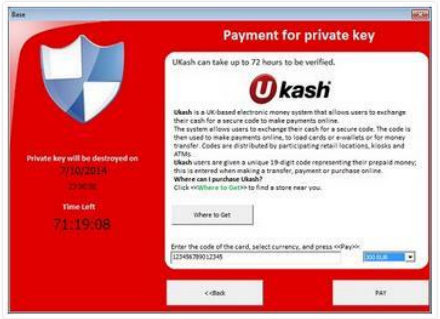
Click <<Next>> to select the method of payment.

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

DECRYPTION

- Receives ransom payment
- Contacts the C2, using Tor and the Polipo proxy server, to obtain the private RSA key
- Decrypts AES key for each file and then decrypts the files

PARTNER PROGRAMME



Details | Feedback | Return Policy

Description

NEWS:

- PaySafeCard support added
- Ukash support added
- Screens changed

TorLocker 2.0 Ransomware - 70% profit

Details | Feedback | Return Policy

Description

- PHP Panel goes without encryption
- needs Linux server at least 8G RAM
- PaySafeCard support added
- Ukash support added
- Moneypak support added
- Setup included
- Screens changed

TorLocker 2.0 + PHP panel + manual - 100% profit

By [redacted]

BTC 9.9959

Currently unavailable.

Option

Escrow	Yes, escrow by [redacted] is available.
Class	Digital
Ships From	Worldwide

RANSOMWARE TRENDS

- Multi-key crypto
- Script-based ransomware
- Linux and Mac ransomware
- Servers targeted
- Use of legal tools
- C2 servers in Tor
- Payment in bitcoins
- Use of BitMessage
- Disk level infection

HOW [NOT] TO DEAL WITH THE PROBLEM

‘To be honest, we often advise people just to pay the ransom’

Joseph Bonovolonta, Assistant Special Agent, FBI

HOW TO DEAL WITH THE PROBLEM

- Signatures
- Heuristics
- System Watcher
  - Cryptomalware Countermeasures Subsystem
  - Automatic Exploit Prevention
  - Rollback of malware actions
- Application Privilege Control
  - https://www.youtube.com/watch?v=QWzDKBU0A6k

HOW TO DEAL WITH THE PROBLEM

- Backup
- Education

GREAT

THANK YOU

David Emm
Global Research and Analysis Team

KASPERSKY lab