EECS 3482

THE EVOLUTION OF

By Osama Masood, Xavon Charles and Sibu Varghese Jacob

What is Ransomware??

What does it do?

Who creates Ransomware??

Why are they created?

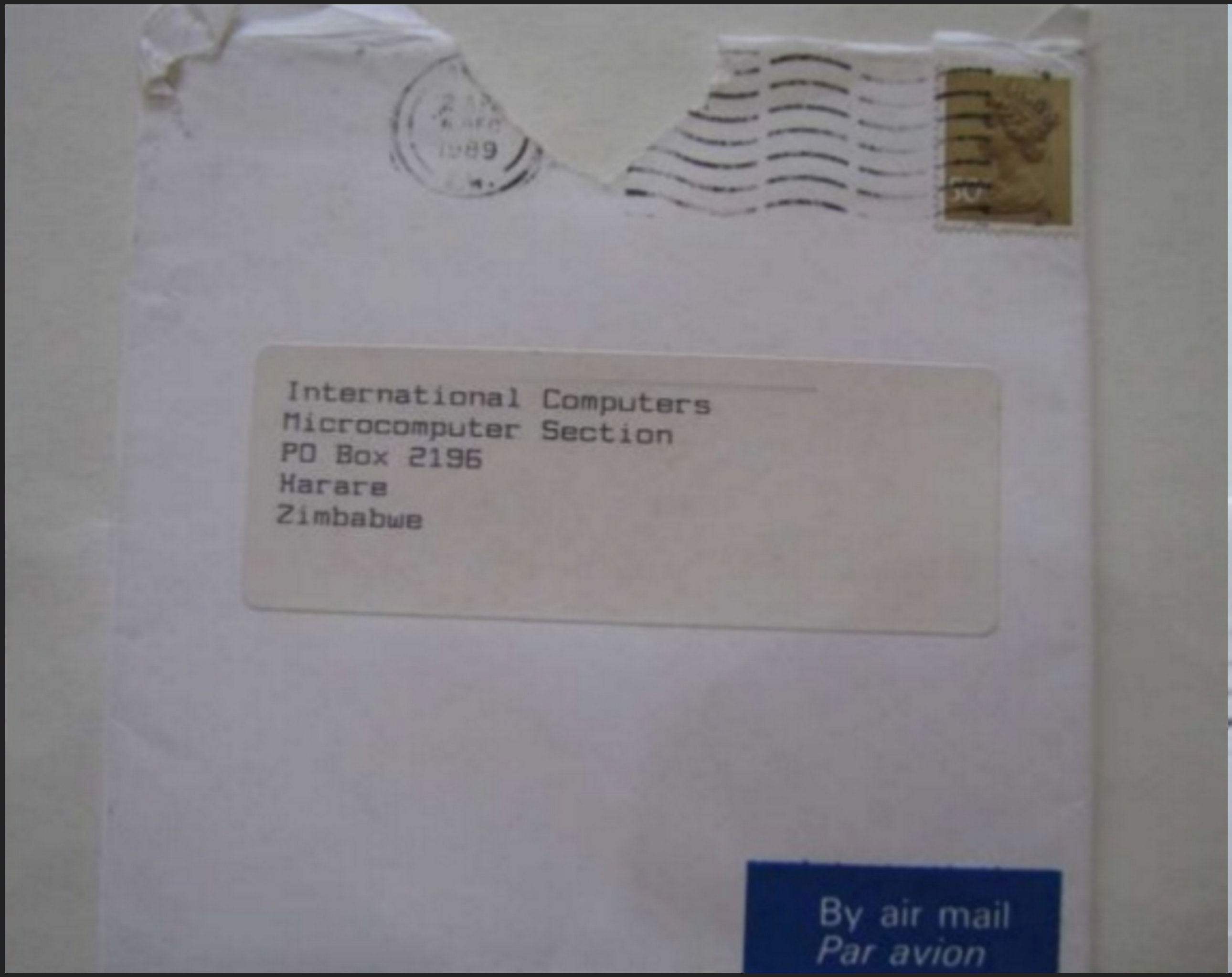
THE FIRST RANSOMWARE

- Discovered in 1989 and made by biologist Joseph Popp
- PC Cyborg virus AKA AIDS
- Transmitted by snail mail using 5$^{1/4}$ diskettes
- The disks were labelled as “AIDS Information - Introductory Diskettes”

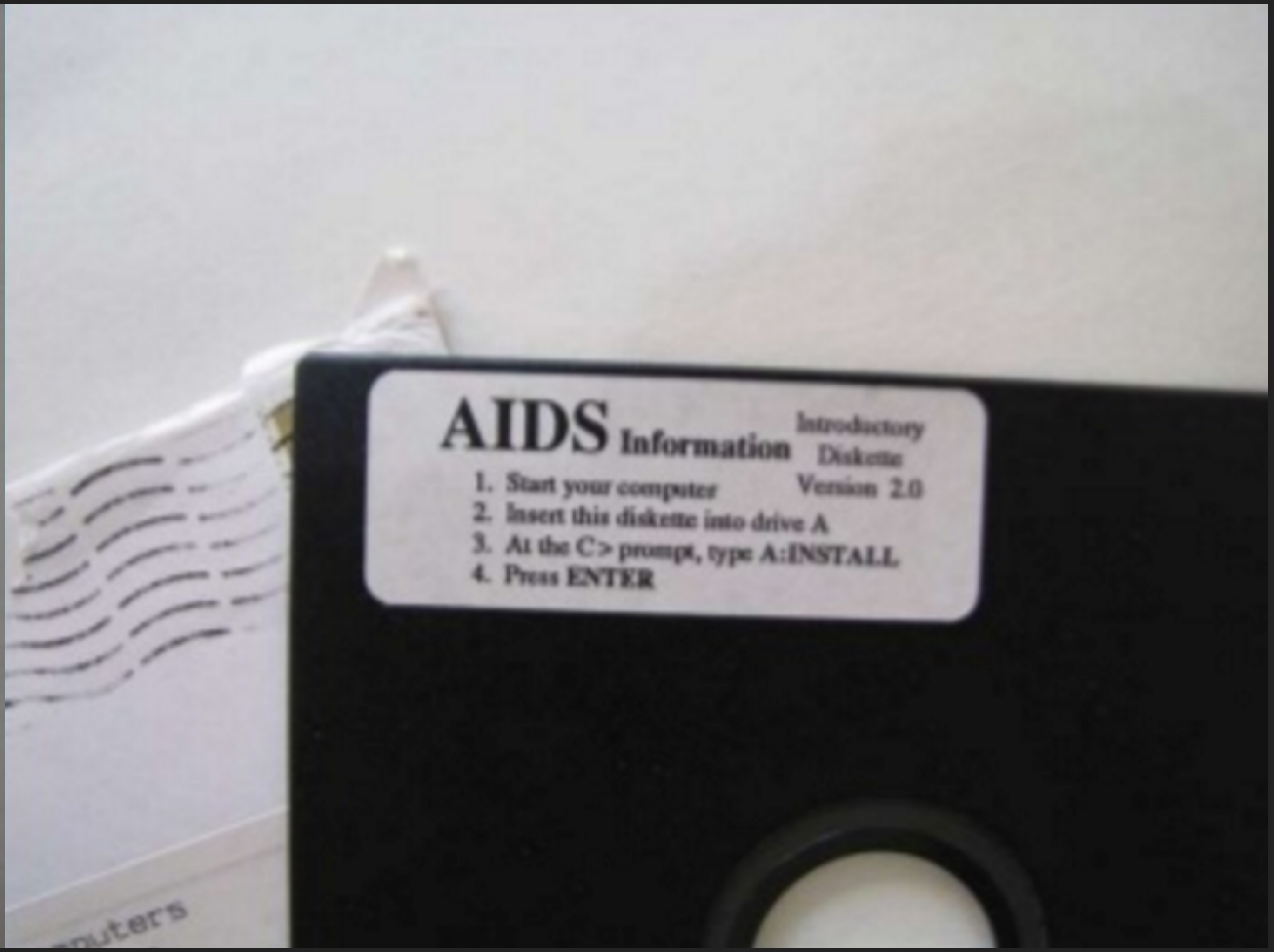
https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf

https://www.knowbe4.com/aids-trojan

ORIGINAL PACKAGING



International Computers
Microcomputer Section
PO Box 2196
Harare
Zimbabwe

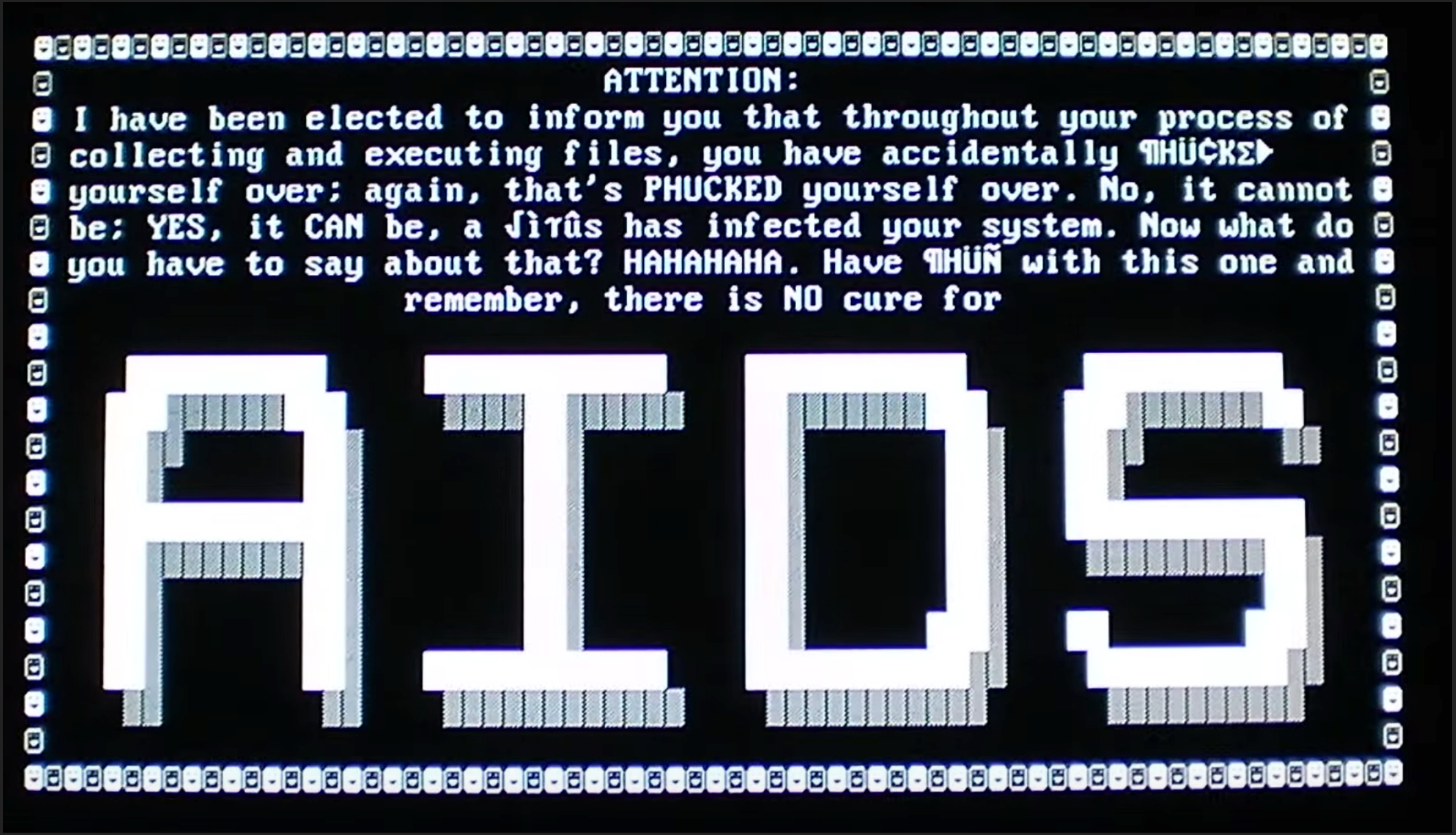


AIDS Information Introductory Diskette Version 2.0

1. Start your computer
2. Insert this diskette into drive A
3. At the C> prompt, type A:INSTALL
4. Press ENTER

HOW IT WORKED?

- AIDS.EXE claims it requires INSTALL.EXE to run
- INSTALL.EXE performs at least four different functions:
    - Installation
    - Counting
    - Triggering
    - Faking

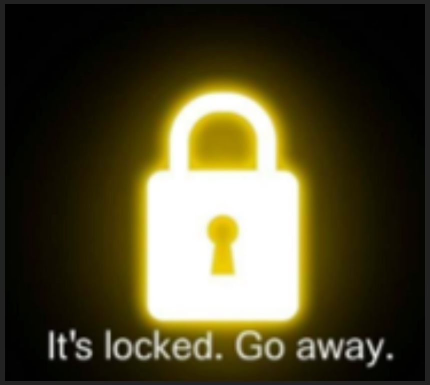


```
                         ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accidentally ¶HÜ¢KΣ▶
yourself over; again, that's PHUCKED yourself over. No, it cannot
be; YES, it CAN be, a √ìτûs has infected your system. Now what do
you have to say about that? HAHAHAHA. Have ¶HÜÑ with this one and
              remember, there is NO cure for

AIDS
```

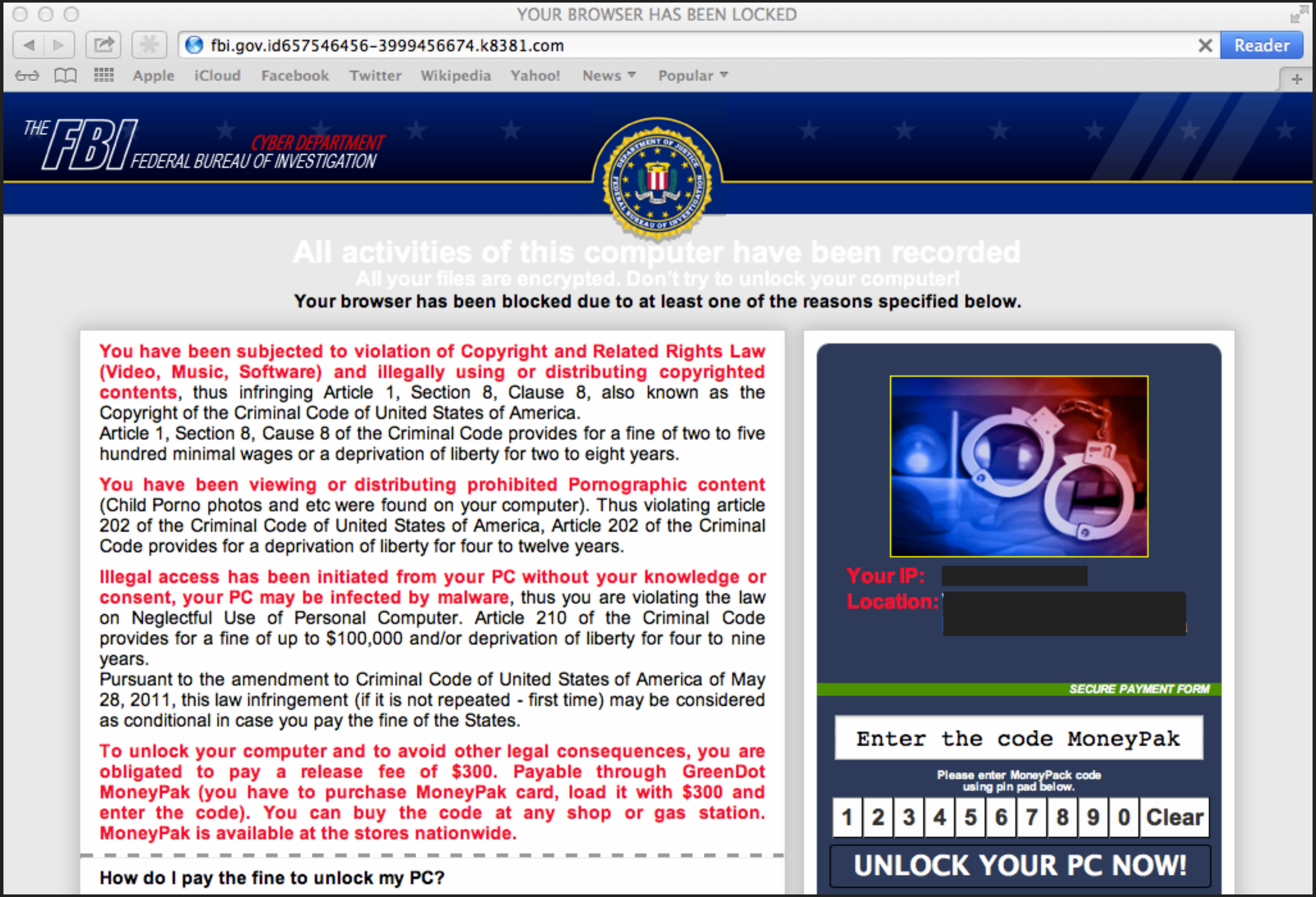
WINLOCKER RANSOMWARE

- Lock user’s computer and demands payment to unlock
- They usually ask for online payment
- This type of Ransomware uses Social engineering
- Usually uses scare tactics to trick the user



http://www.infosecurityeurope.com/__novadocuments/89024?v=635703301368700000
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

AN EXAMPLE OF WINLOCKER – USING THE I AM THE FBI SCARE TACTIC



YOUR BROWSER HAS BEEN LOCKED

fbi.gov.id657546456-3999456674.k8381.com

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.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300. Payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with $300 and enter the code). You can buy the code at any shop or gas station. MoneyPak is available at the stores nationwide.

How do I pay the fine to unlock my PC?

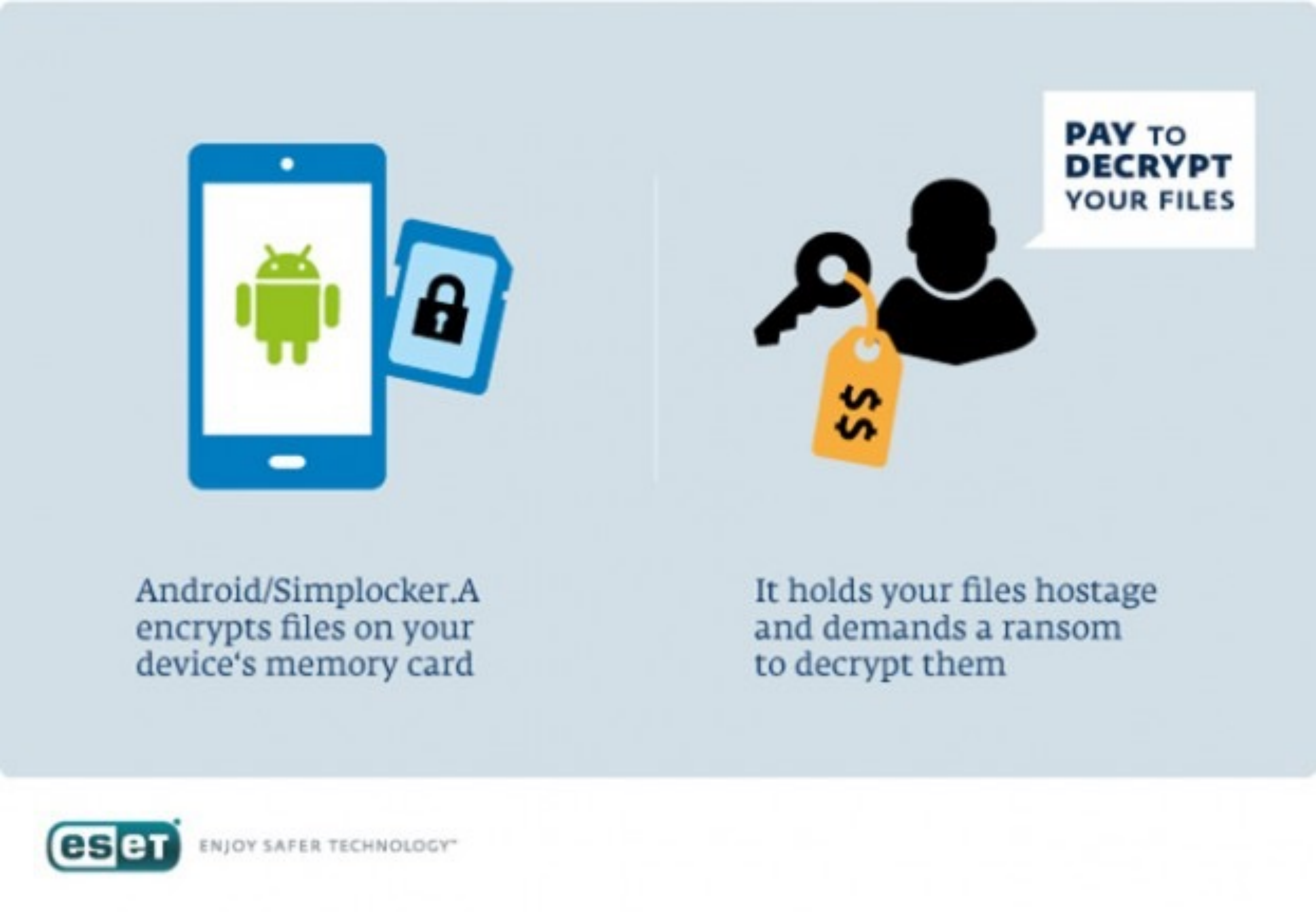
Your IP: [redacted]
Location: [redacted]

Enter the code MoneyPak

Please enter MoneyPack code using pin pad below.

SIMPLocker – first mobile ransomware

- A type of crypto ransomware
- Commonly disguised as a popular app, e.g a game or a photo editor
- Contacts the hacker after installation and encrypts the user data on the memory card
- Demands ransom for decryption key

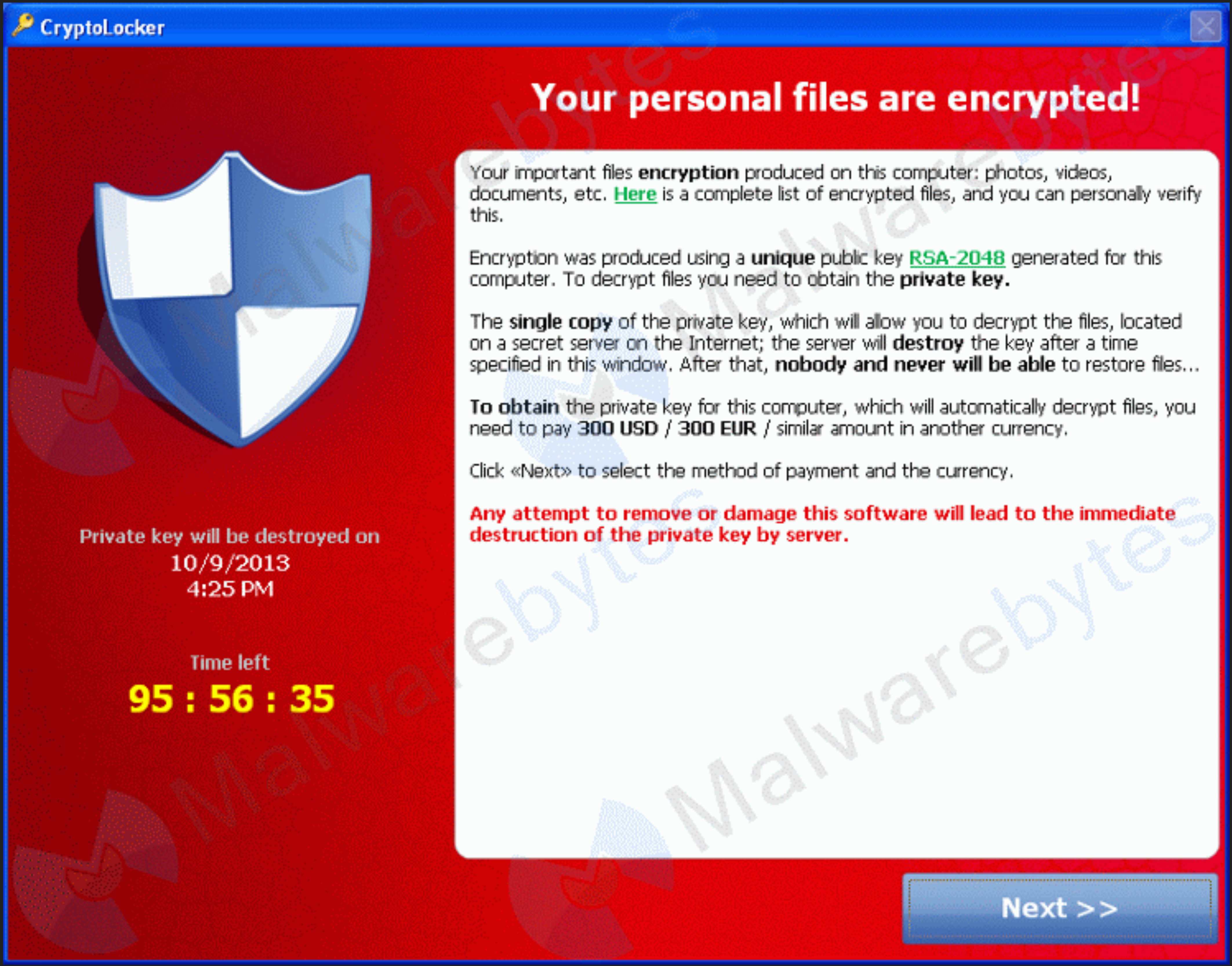


Android/Simplocker.A encrypts files on your device's memory card

It holds your files hostage and demands a ransom to decrypt them

CRYPTO RANSOMWARE

- Most commonly used ransomware
- Evolve as more advanced encryption algorithms are created
- Encrypts files on the victims device and then demands a fee for the decryption key



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 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 and the currency.

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

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

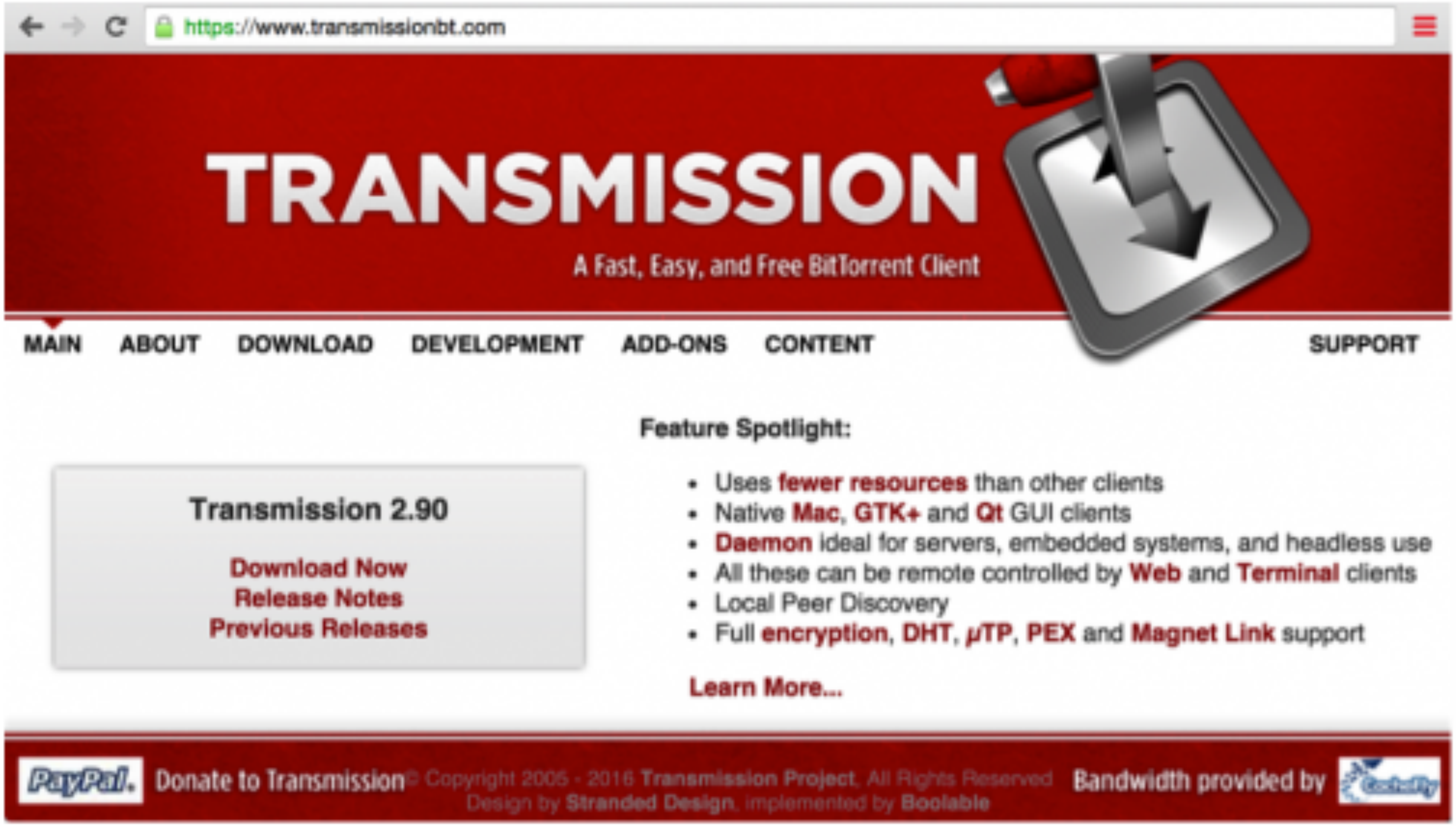
MAC OS RANSOMWARES?

- MAC OS Impenetrable?
- Nicknamed “KeRanger”
- Hidden in “Transmission”, a bit torrent client
- Dormant until activated after 3 days

MAC OS RANSOMWARES?

- The malware encrypts certain types of documents and data files in the system
- Demands 1 bitcoin after encryption is completed
- Encrypts Time machine backup data
- Polymorphing type of malware

MAC OS RANSOMWARES?



Transmission 2.90

Download Now
Release Notes
Previous Releases

Feature Spotlight:

- Uses **fewer resources** than other clients
- Native **Mac**, **GTK+** and **Qt** GUI clients
- **Daemon** ideal for servers, embedded systems, and headless use
- All these can be remote controlled by **Web** and **Terminal** clients
- Local Peer Discovery
- Full **encryption**, **DHT**, **µTP**, **PEX** and **Magnet Link** support

Learn More...

© Copyright 2005 - 2016 Transmission Project. All Rights Reserved
Design by Stranded Design, implemented by Boolable

Figure 1 KeRanger hosted in Transmission's official website

Source: http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/

HOW TO PROTECT OURSELVES?

TO PAY OR NOT TO PAY?

WHAT SHOULD WE DO?

HOW TO PROTECT OURSELVES?

- Update antivirus
- Download from trusted sources
- Offline Backups
- Update System OS

TO PAY OR NOT TO PAY?

- Generally discouraged
- Depends on data and resources

WHAT SHOULD WE DO?

- Raise awareness and report incidents
- Educate people

QUESTIONS?