CS 5472 - Advanced Topics in Computer Security

Topic 7: Ransomware (1)

Spring 2022 Semester

Instructor: Bo Chen

bchen@mtu.edu

https://cs.mtu.edu/~bchen

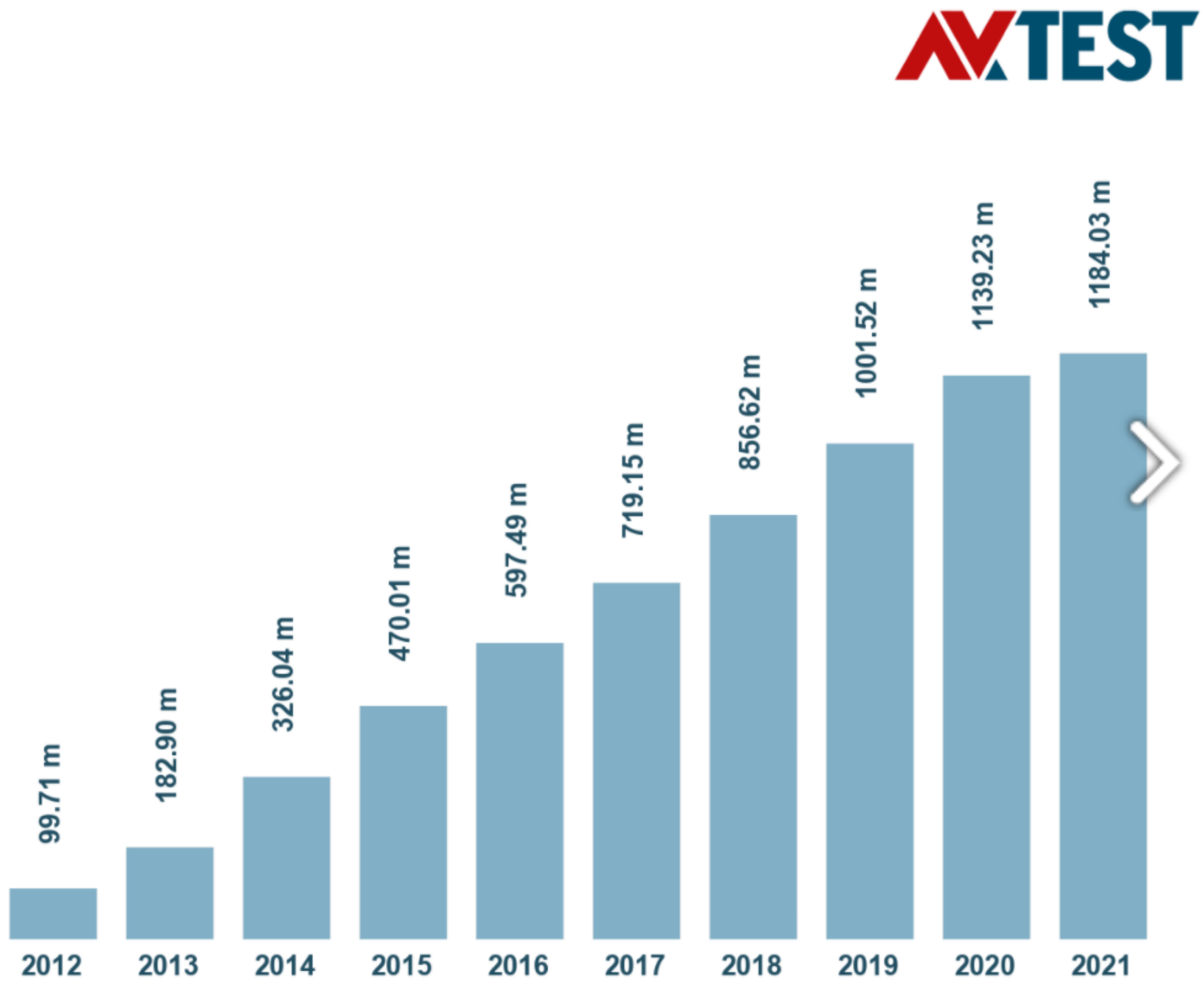
https://snp.cs.mtu.edu

Malware

- Malware (a portmanteau for malicious software): any software intentionally designed to cause damage to a computer, server, client, or computer network
  - By contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug.
- A wide variety of malware types exist
  - Computer viruses
  - Worms
  - Trojan horses
  - Ransomware
  - Spyware
  - Adware
  - Rootkit
  - Backdoor
  - Etc.

The Growth of Malware Recently

Total malware



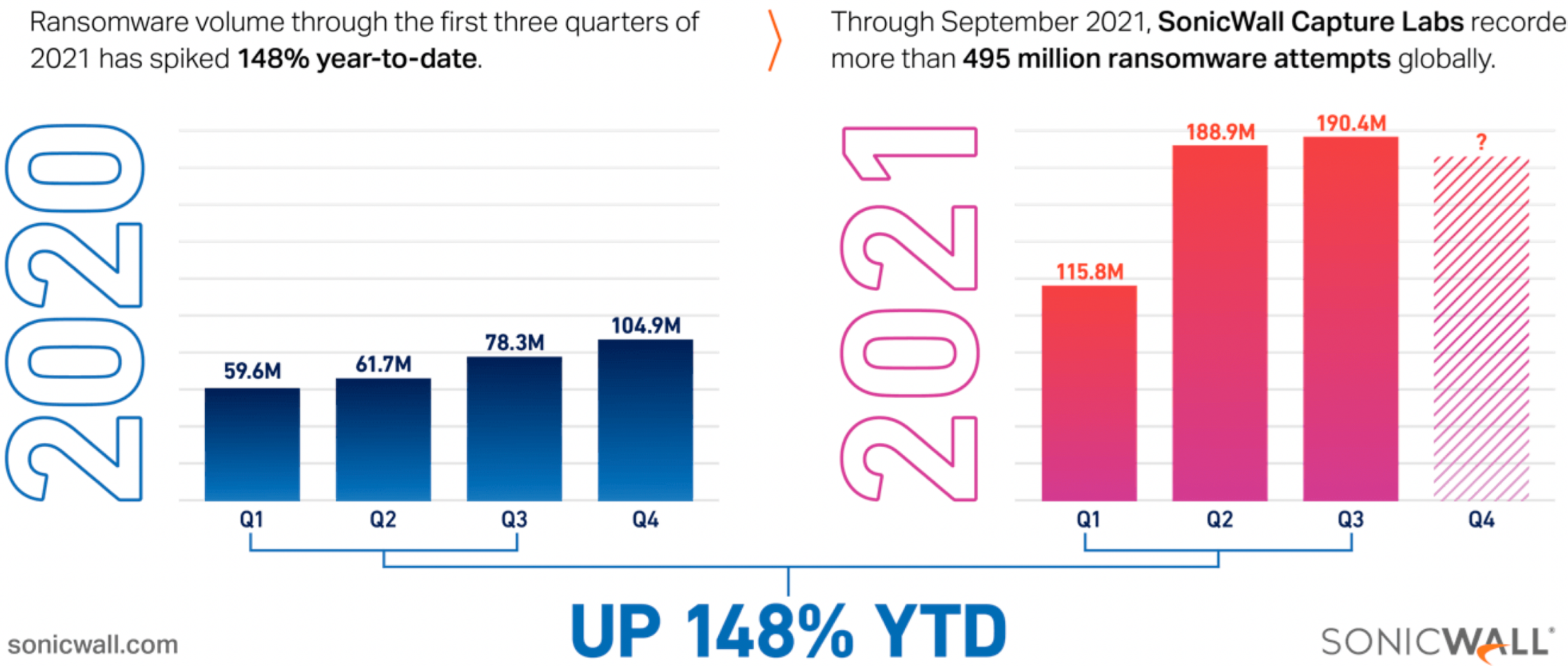
Last update: March 14, 2021

Copyright © AV-TEST GmbH, www.av-test.org

Ransomware

- Ransomware is a special type of malware:
  - infects a computer and restricts access to the computer and/or its files
  - asks for a ransom to be paid in order for the restriction to be removed
- Starting from around 2012, the use of ransomware scams has grown internationally.
  - There were 181.5 million ransomware attacks in the first six months of 2018. This record marks a 229% increase over this same time frame in 2017.

Ransomware Attacks in 2020-2021



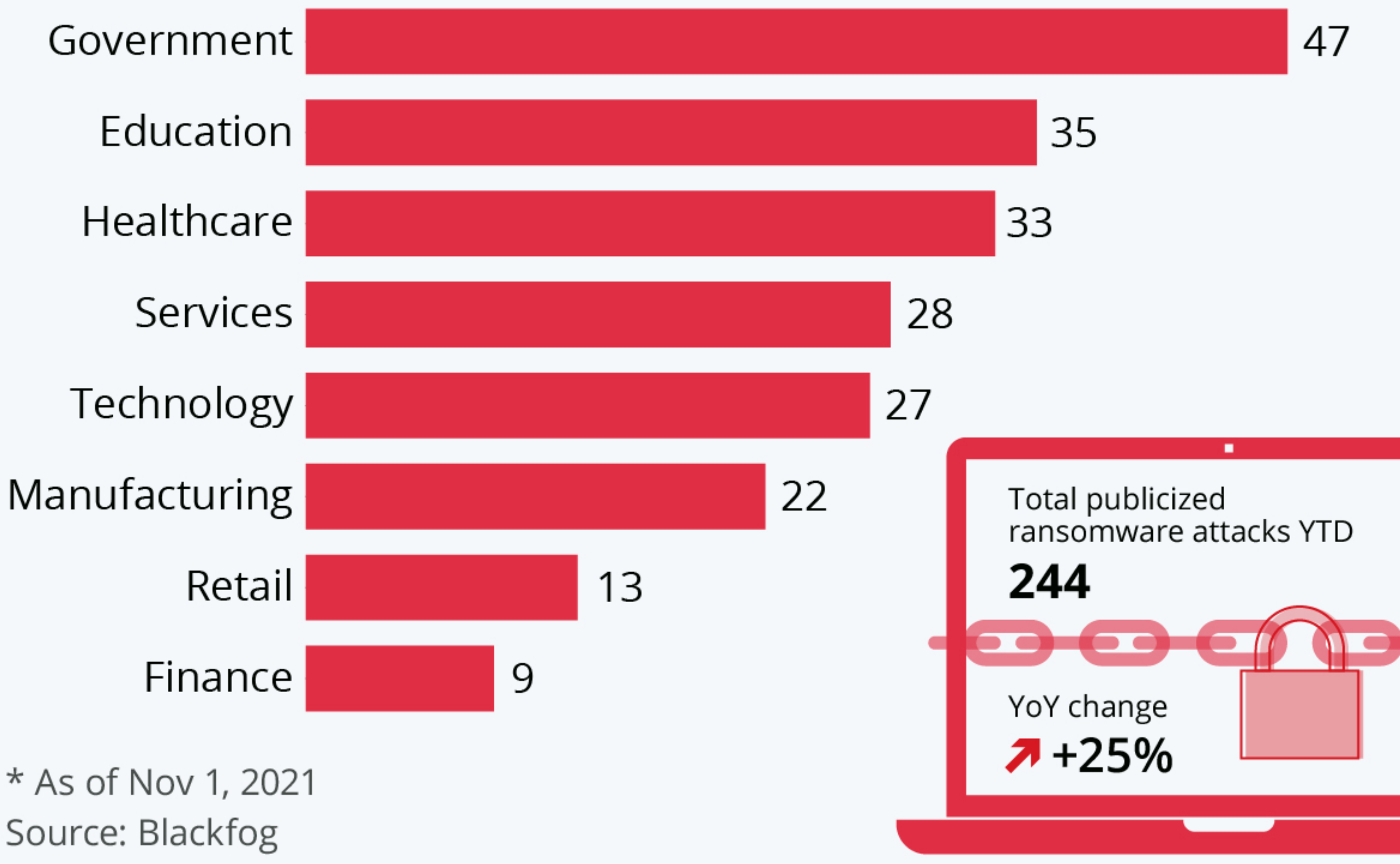
Ransomware volume through the first three quarters of 2021 has spiked **148% year-to-date**.

Through September 2021, **SonicWall Capture Labs** recorded more than **495 million ransomware attempts** globally.

Ransomware Attacks by Sectors

The Industries Most Affected by Ransomware

Number of publicized ransomware attacks worldwide by sector in 2021*



Total publicized ransomware attacks YTD

244

YoY change

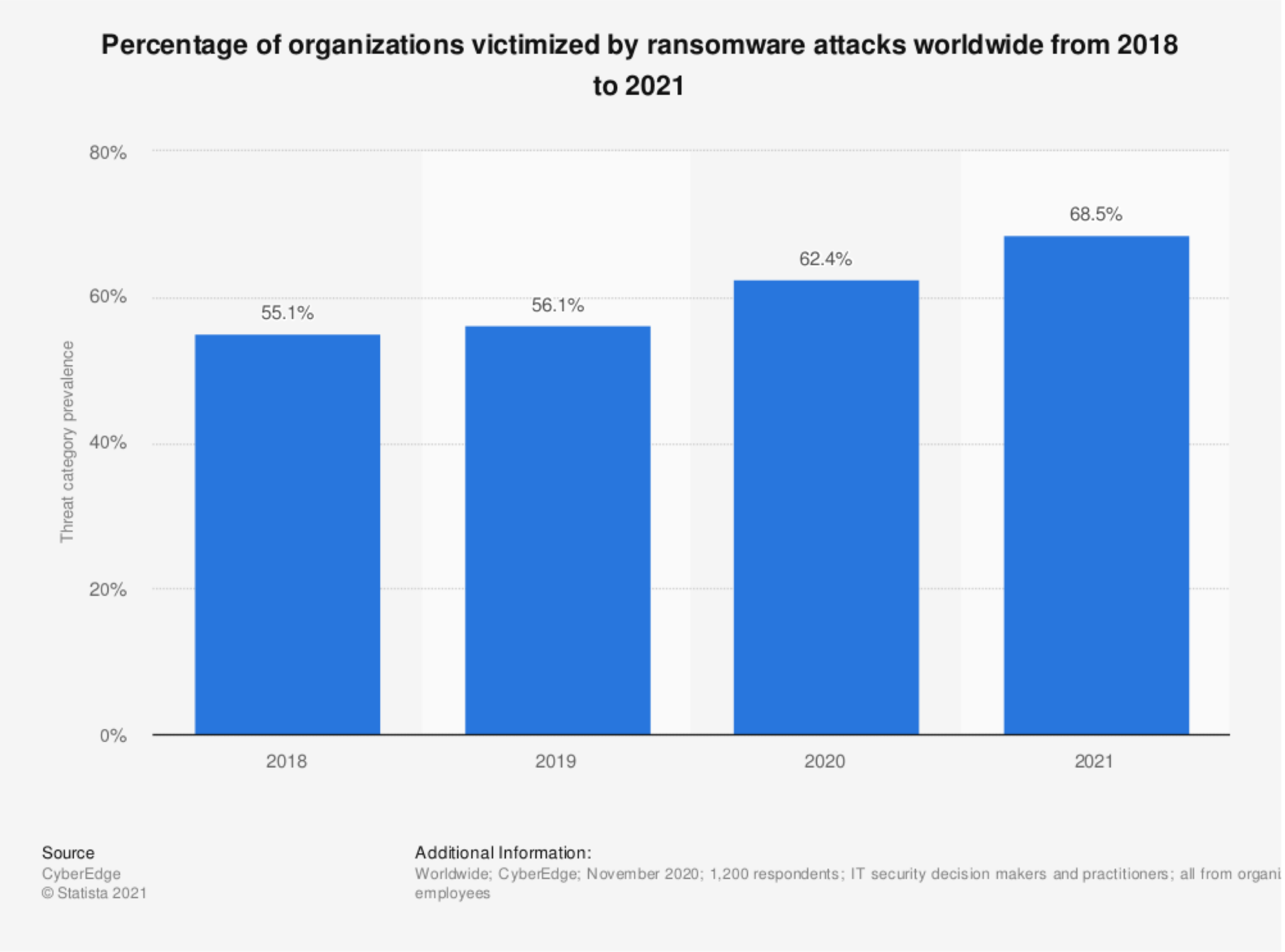
↗ **+25%**

* As of Nov 1, 2021

Source: Blackfog

statista

Percentage of Organization Victimized by Ransomware Attacks



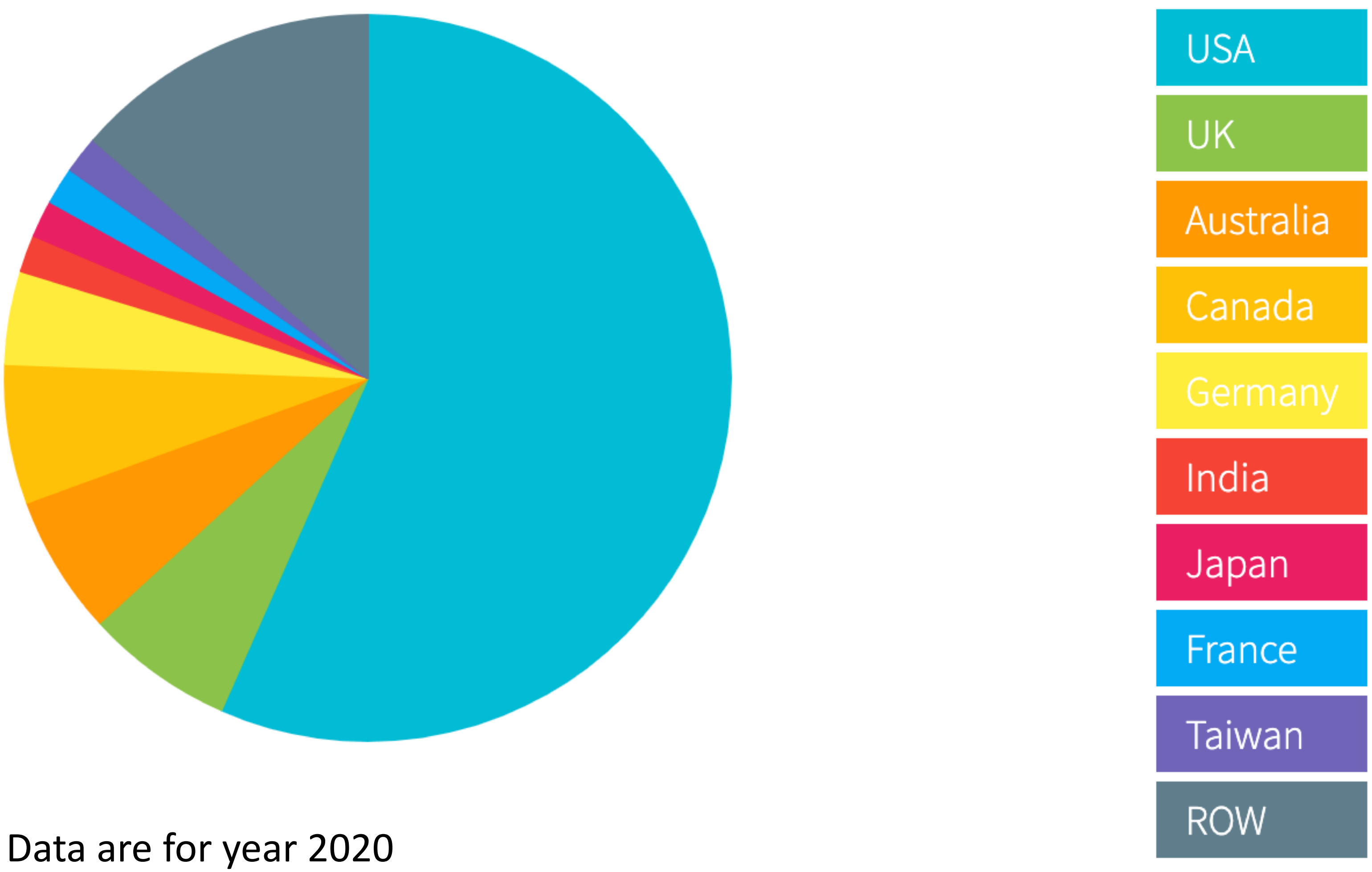
Percentage of organizations victimized by ransomware attacks worldwide from 2018 to 2021

Source
CyberEdge
© Statista 2021

Additional Information:
Worldwide; CyberEdge; November 2020; 1,200 respondents; IT security decision makers and practitioners; all from organi
employees

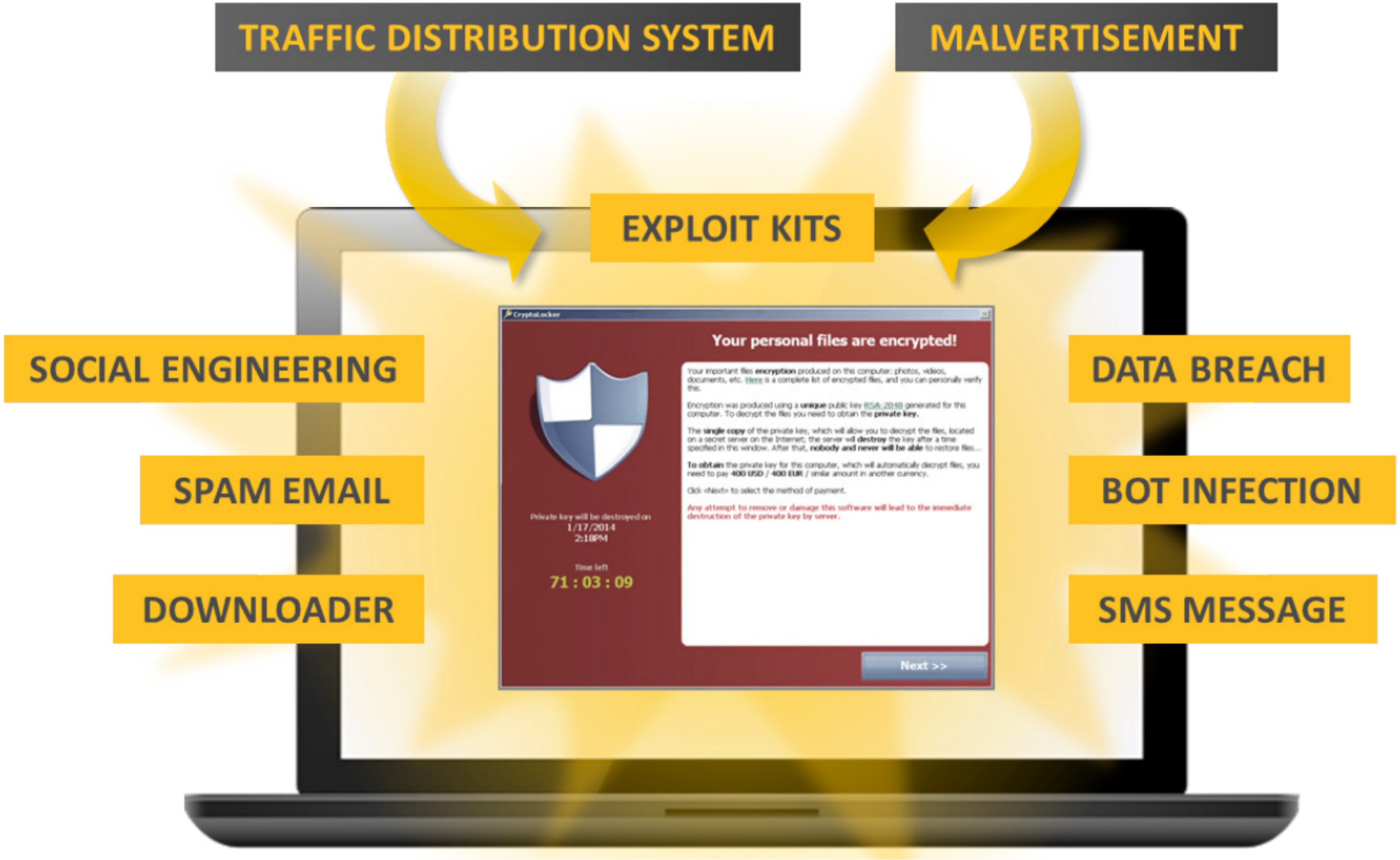
Ransomware Attacks by Countries

Ransomware Attacks by Country



Data are for year 2020

Ransomware Propagation



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 **400 USD** / **400 EUR** / similar amount in another currency.

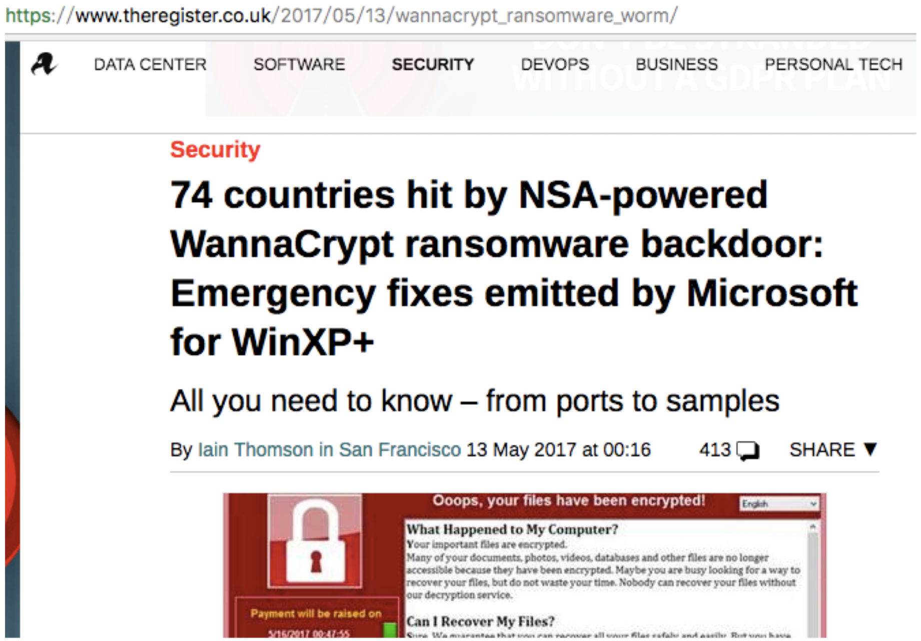
Click «Next» to select the method of payment.

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

Private key will be destroyed on
1/17/2014
2:18PM

Time left
71 : 03 : 09

Cast Study: WannaCry



https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/

DATA CENTER SOFTWARE **SECURITY** DEVOPS BUSINESS PERSONAL TECH

Security

74 countries hit by NSA-powered WannaCrypt ransomware backdoor: Emergency fixes emitted by Microsoft for WinXP+

All you need to know – from ports to samples

By Iain Thomson in San Francisco 13 May 2017 at 00:16 413 SHARE ▼

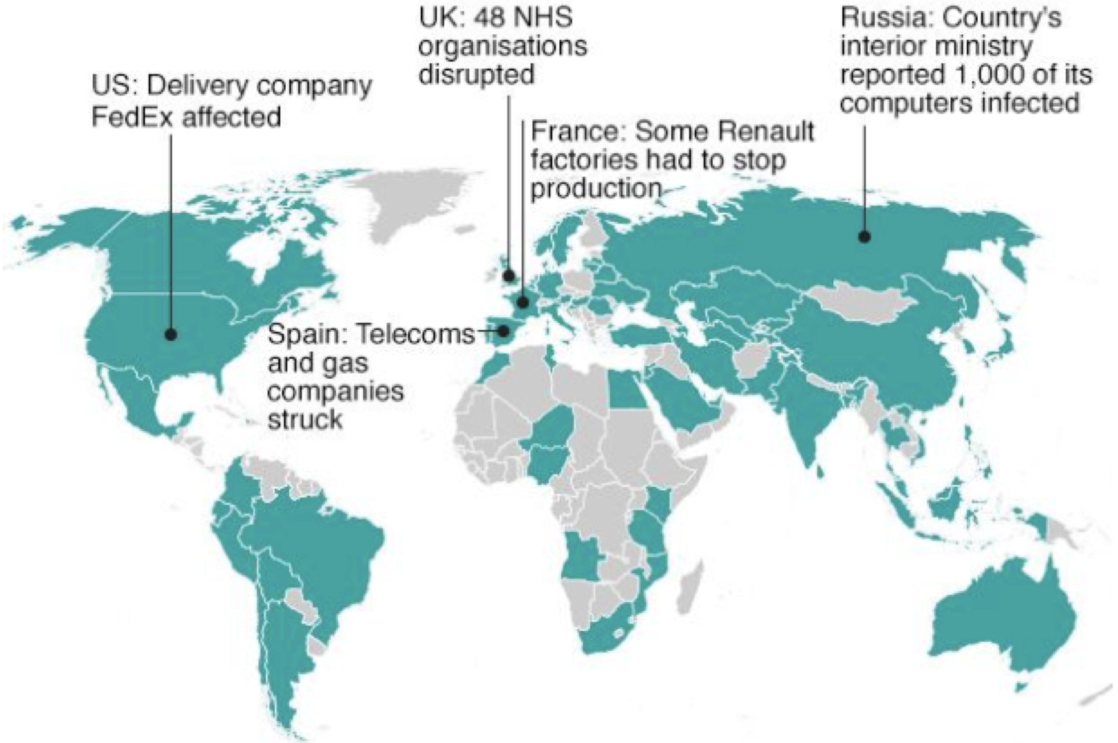
Ooops, your files have been encrypted! English

Payment will be raised on
5/16/2017 00:47:55

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have

Countries hit in initial hours of cyber-attack


US: Delivery company FedEx affected
UK: 48 NHS organisations disrupted
France: Some Renault factories had to stop production
Russia: Country's interior ministry reported 1,000 of its computers infected
Spain: Telecoms and gas companies struck

*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Noway, where incidents have been reported since

Source: Kaspersky Lab's Global Research & Analysis Team BBC

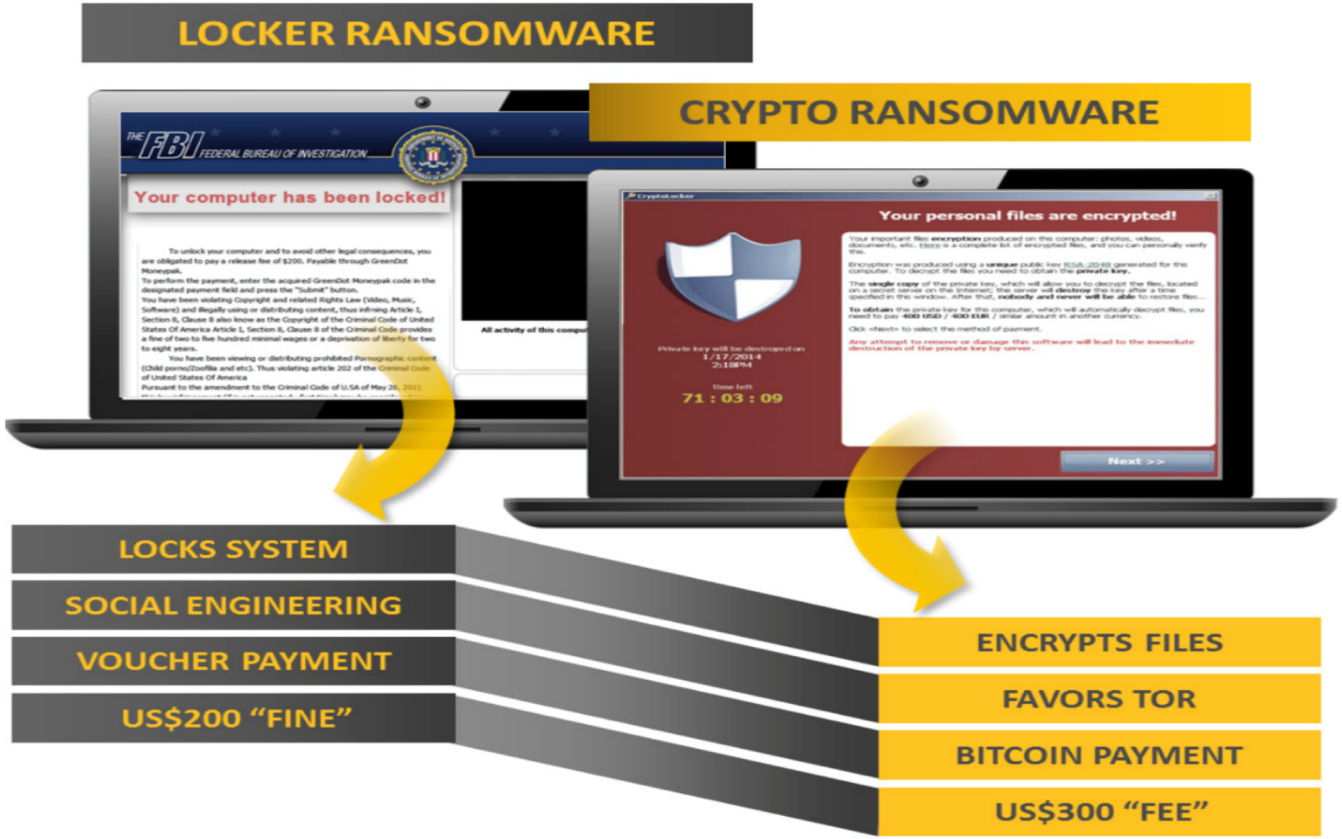
Propagated through EternalBlue, an exploit developed by the US National Security Agency (NSA) for older Windows systems

- Vulnerabilities in Windows Server Message Block (SMB) protocol
- **NSA discovered the vulnerability, but used it to create an exploit for its own offensive work, rather than report it to Microsoft**

Within a day the code was reported to have infected more than 230,000 computers in over 150 countries

Types of Ransomware

- Locker ransomware
- Crypto ransomware



Your computer has been locked!

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $200. Payable through GreenDot Moneypak.
To perform the payment, enter the acquired GreenDot Moneypak code in the designated payment field and press the "Submit" button.
You have been violating Copyright and related Rights Law (Video, Music, Software) and illegally using or distributing content, thus infrning Article I, Section 8, Clause 8 also know as the Copyright of the Criminal Code of United States Of America Article I, Section 8, Clause 8 of the Criminal Code provides 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/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States Of America
Pursuant to the amendment to the Criminal Code of U.S.A of May 28, 2011

All activity of this comput

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 **400 USD / 400 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.

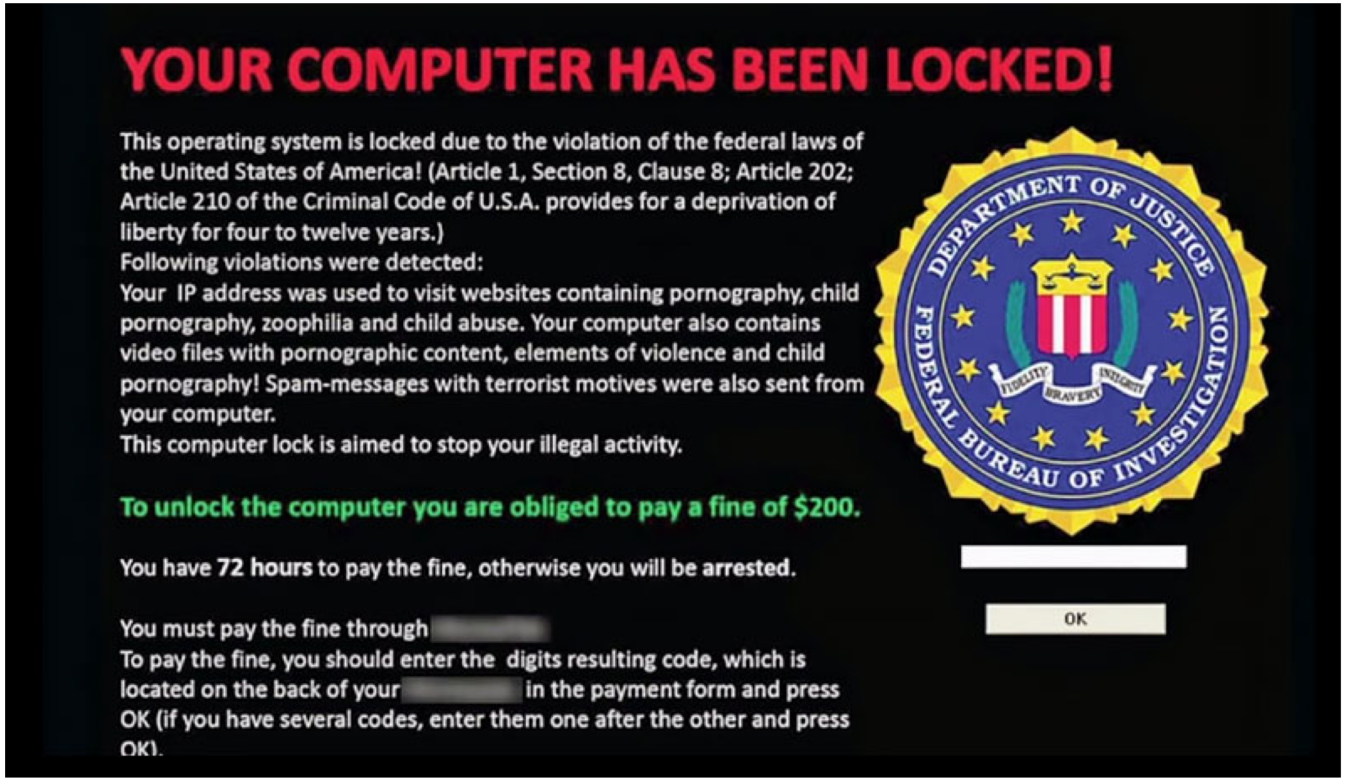
Private key will be destroyed on
1/17/2014
2:18PM

Time left
71 : 03 : 09

Next >>

Locker Ransomware

- Lock the victim system



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

- Easy to be combat, since only the system is locked, but data remain intact

How to Combat Locker Ransomware?

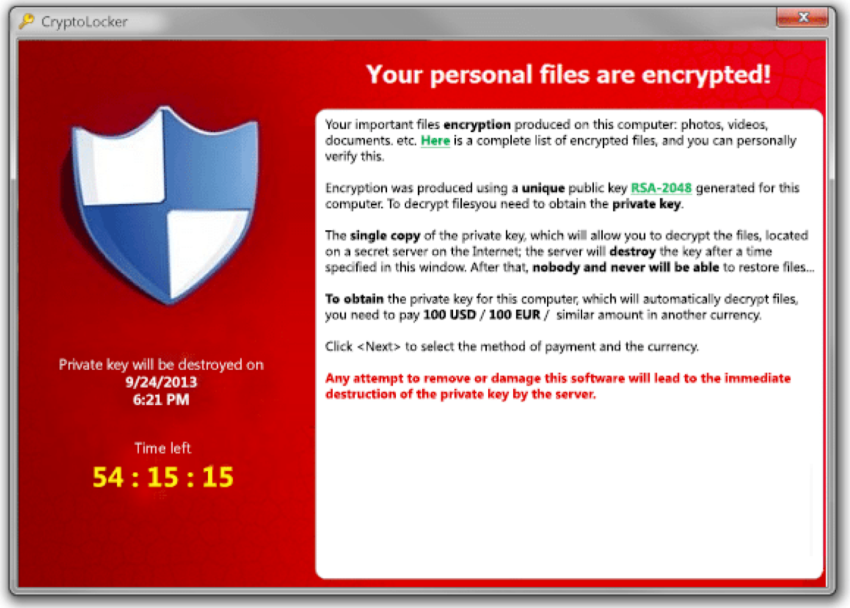
- Observation: only the system is locked by the ransomware, but the data are stored intact

- Unplug the storage medium(e.g., hard drives, SSD drives, SD cards), plug the storage medium to a new computing device, and copy out the data

- Plug the storage device back to the device which has been locked, and re-install/initialize the system, then copy the data back

Crypto Ransomware

- The victim data are encrypted, and cannot be recovered if not able to obtain the key for decryption



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 filesyou 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 **100 USD / 100 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 the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

- How does it work
  - Symmetric encryption: the encryption and decryption are using the same key
    - Good for ransomware: fast encryption
    - Bad for ransomware: the encryption key in plaintext needs to be distributed during encryption process, and can be easily leaked
  - Asymmetric encryption: use public key to encrypt, but private key to decrypt
    - Good for ransomware: only need to distribute the public key during encryption process
    - Bad for ransomware: the asymmetric encryption is expensive, and can be easily detected

How to Combat Ransomware

- Detection: detect the ransomware once it starts to work (focus of today)
  - Detection needs to be fast enough so that ransomware can be blocked before it causes damages to the victim
  - Rationale: ransomware has some sort of working patterns (e.g., the crypto-ransomware always needs to encrypt the victim's data, and delete/ overwrite the original data)

- Recovery: if all the data encrypted by ransomware can guarantee to be recovered, ransomware would not be a problem (focus of Thursday)
  - Obtaining the key: pay the ransom; extract the key in the victim system
  - Backup
    - Off-device backup: e.g., iCloud
    - In-device backup: e.g., utilizing the out-of-place update property of flash memory, such that old data can be temporarily preserved
  - Detection + recovery

A Little More on Ransomware Detection

- Crypto ransomware may be detected since it behaves differently from normal software and other types of malware
- Crypto ransomware usually encrypts a large amount of data in a short time, and over-writes the old data
  - A large number of read access
  - Expensive computation is required for a large amount of encryptions
  - A large number of writes/over-writes in a short time

The most challenging issue is how to detect the crypto ransomware as fast as possible, since the detection is time-sensitive

Paper Presentation

- UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware

- Presented by Charles Warren