CS 5472 - Advanced Topics in Computer Security

Topic 7: Ransomware (1)

Spring 2021 Semester

Instructor: Bo Chen

bchen@mtu.edu

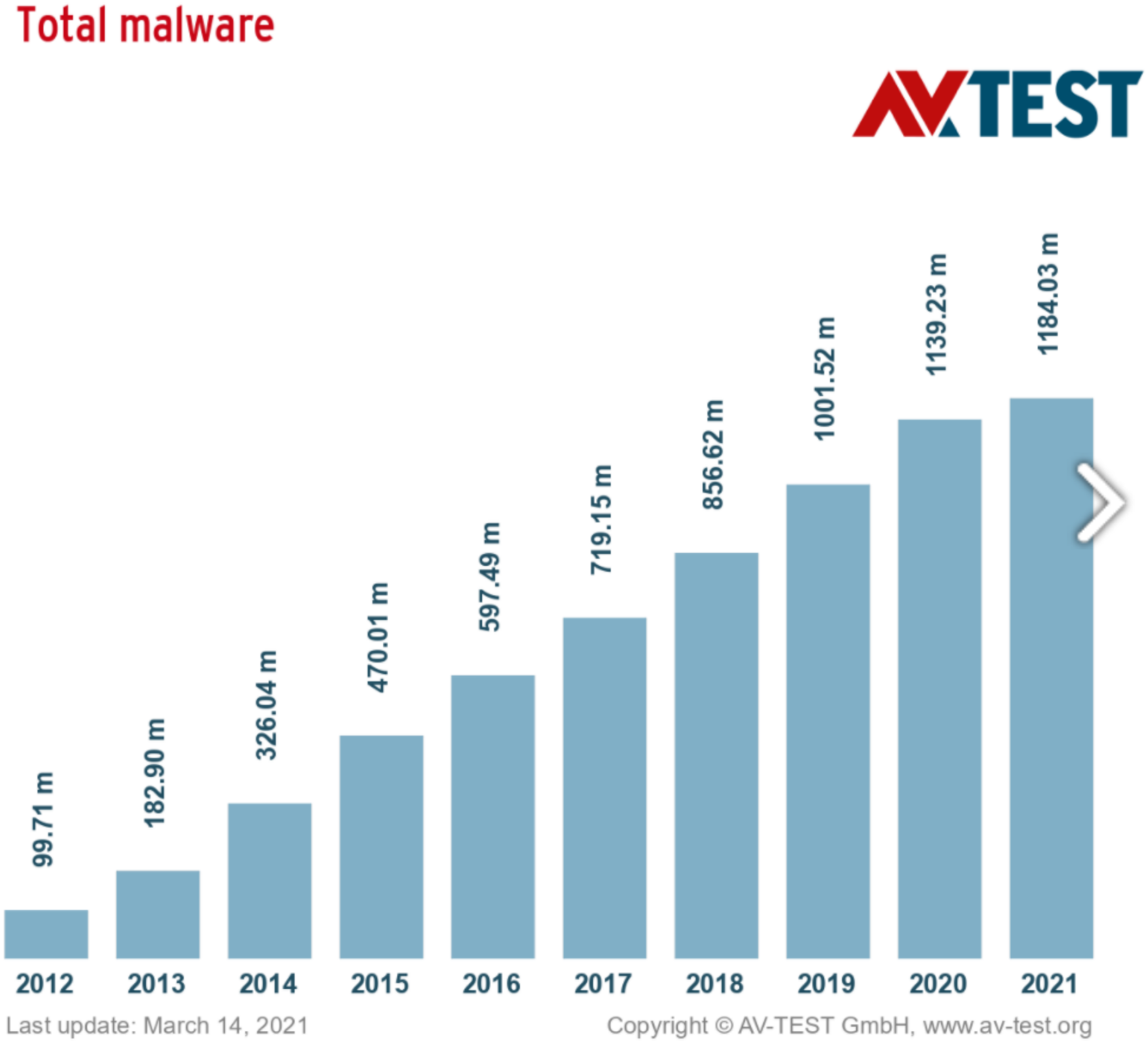
https://cs.mtu.edu/~bchen

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.

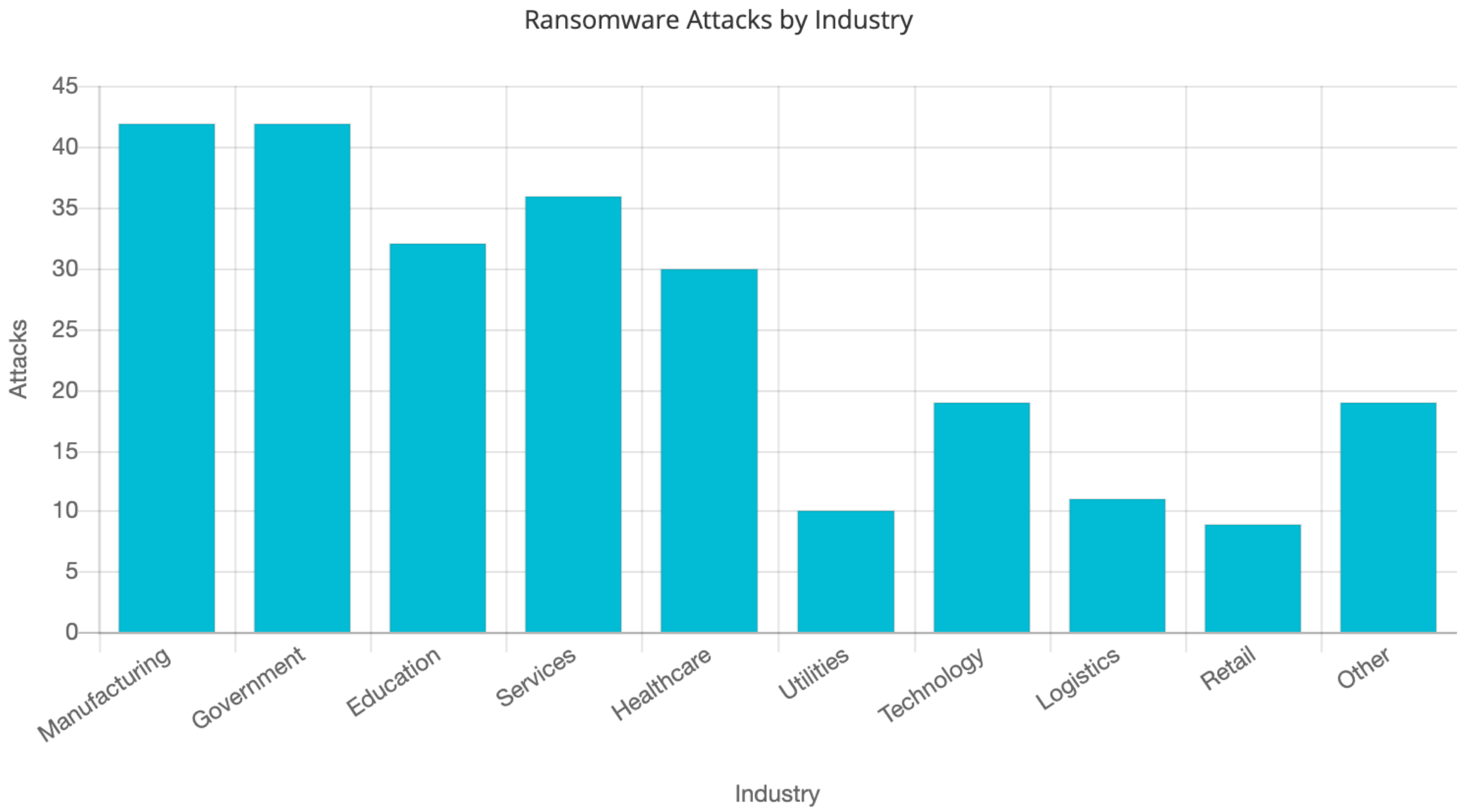
The Growth of Malware Recently



Ransomware

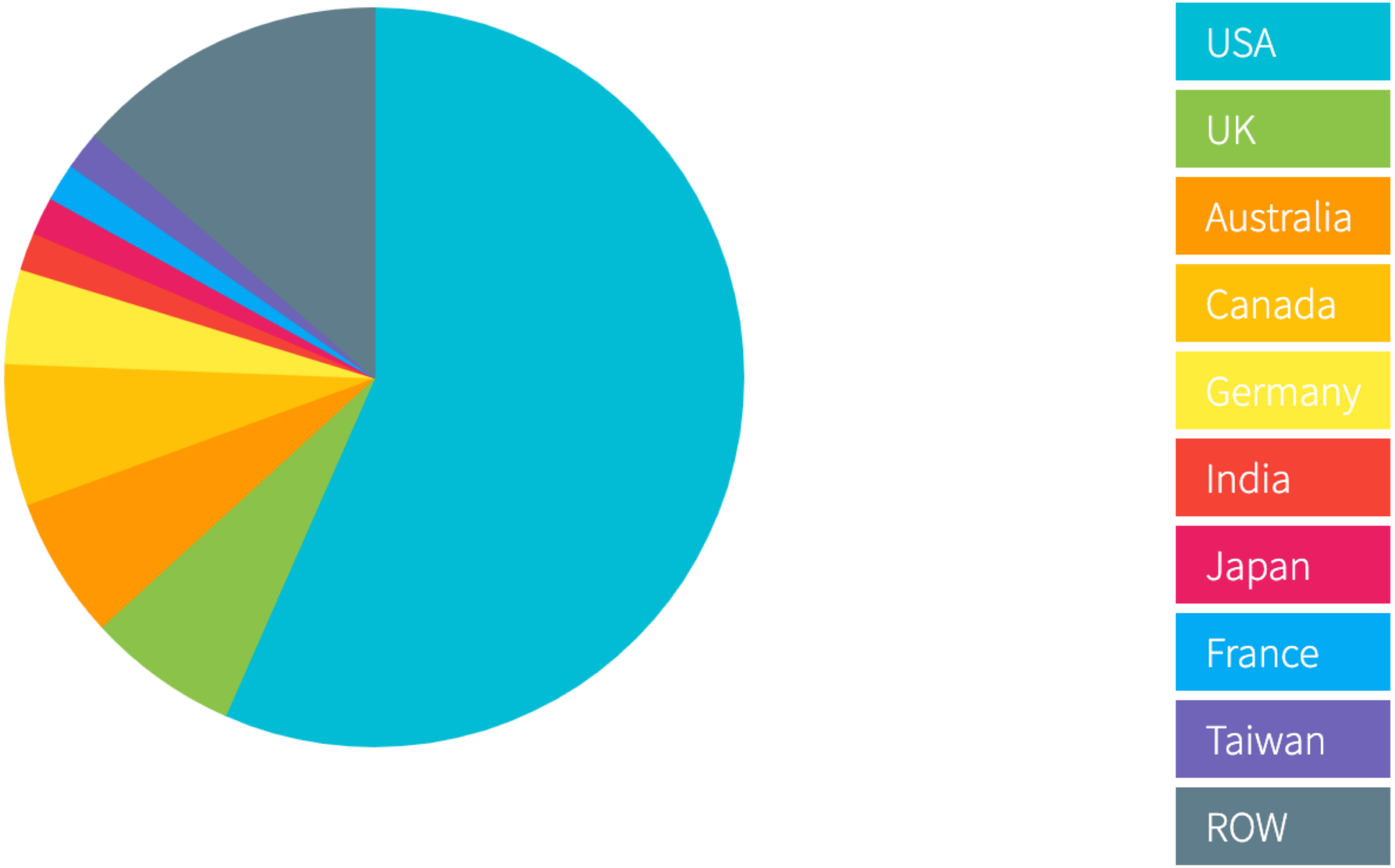
- Ransomware is a special type of malware:
  - infects a computer and restricts access to the computer and/or its files
  - asks for a ransom to be paid in order for the restriction to be removed
- Starting from around 2012, the use of ransomware scams has grown internationally.
  - There were 181.5 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

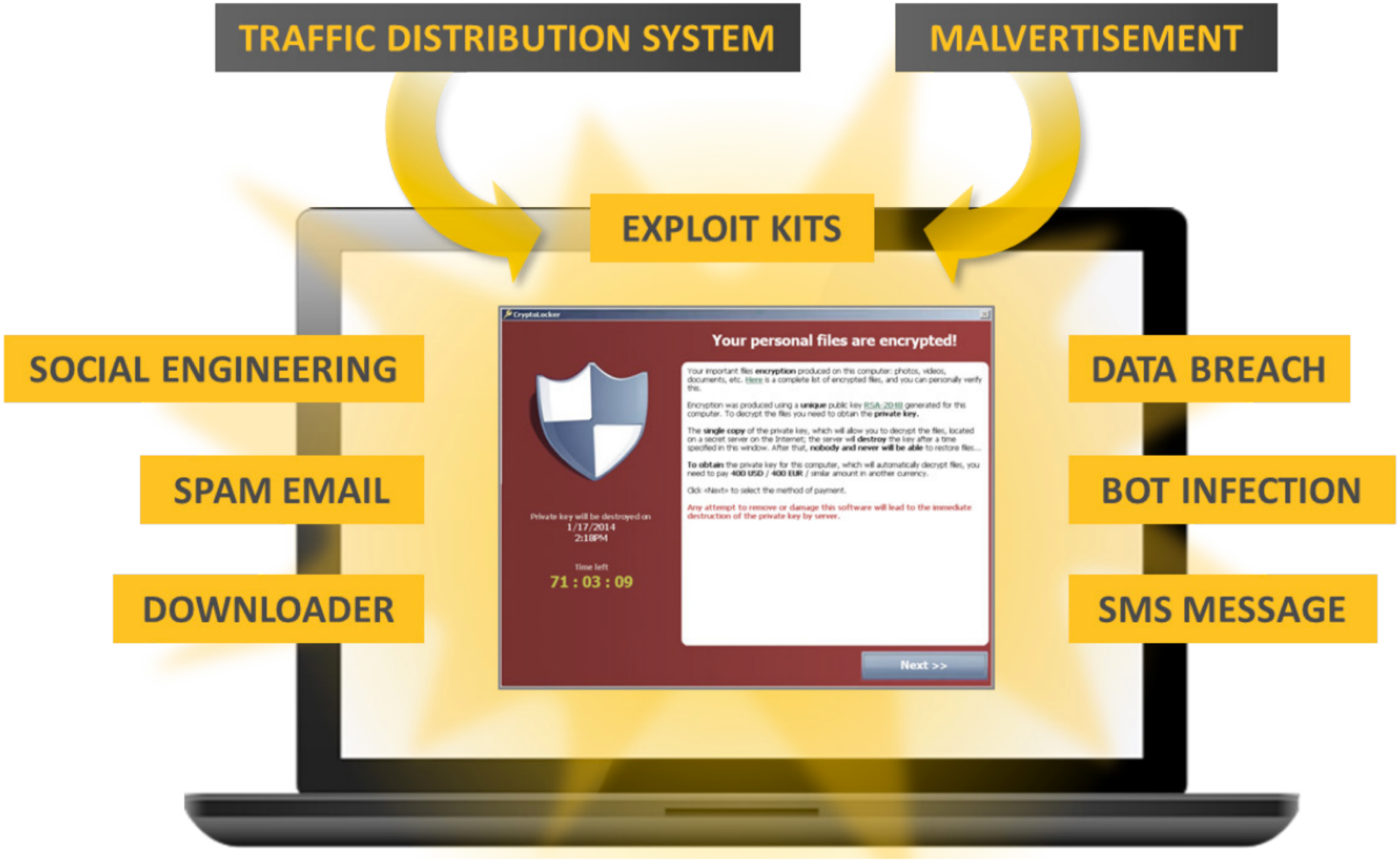


Ransomware Attacks in 2020

Ransomware Attacks by Country



Ransomware Propagation



TRAFFIC DISTRIBUTION SYSTEM

MALVERTISEMENT

EXPLOIT KITS

SOCIAL ENGINEERING

SPAM EMAIL

DOWNLOADER

DATA BREACH

BOT INFECTION

SMS MESSAGE

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.

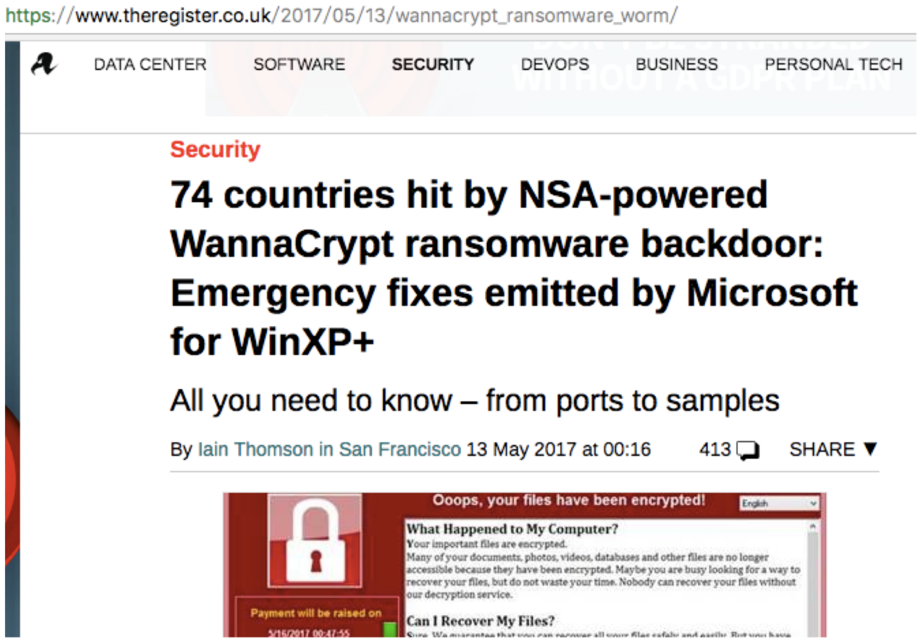
Click «Next» to select the method of payment.

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

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!

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.

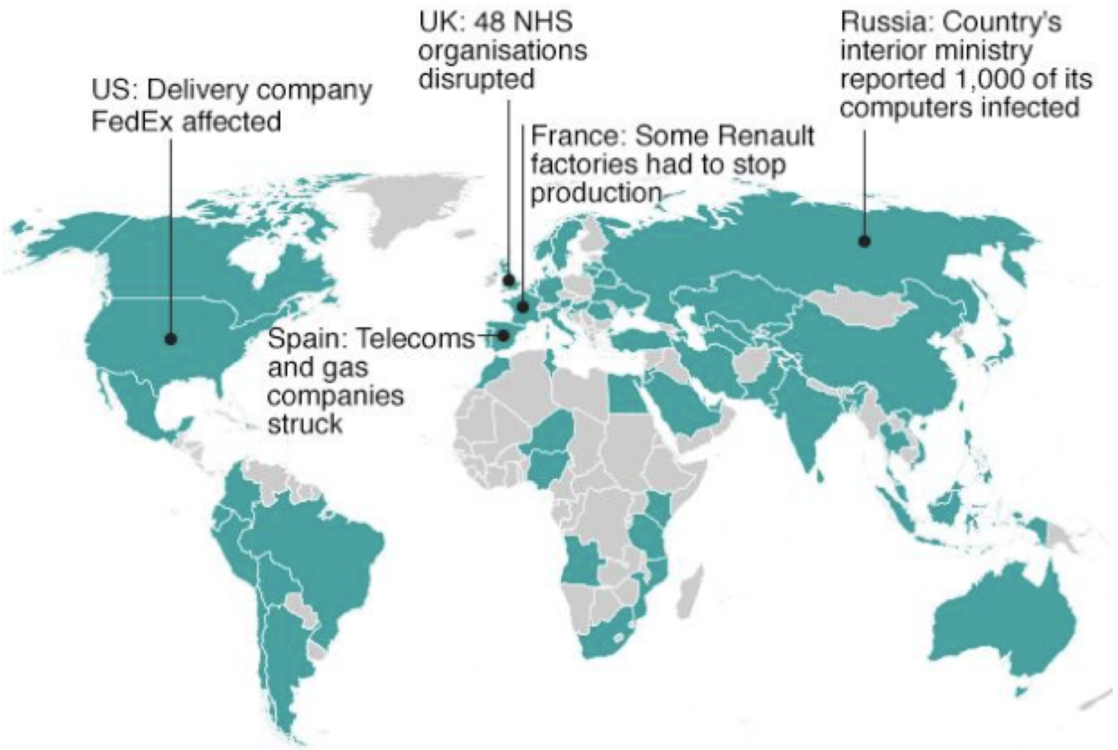
Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have

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

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

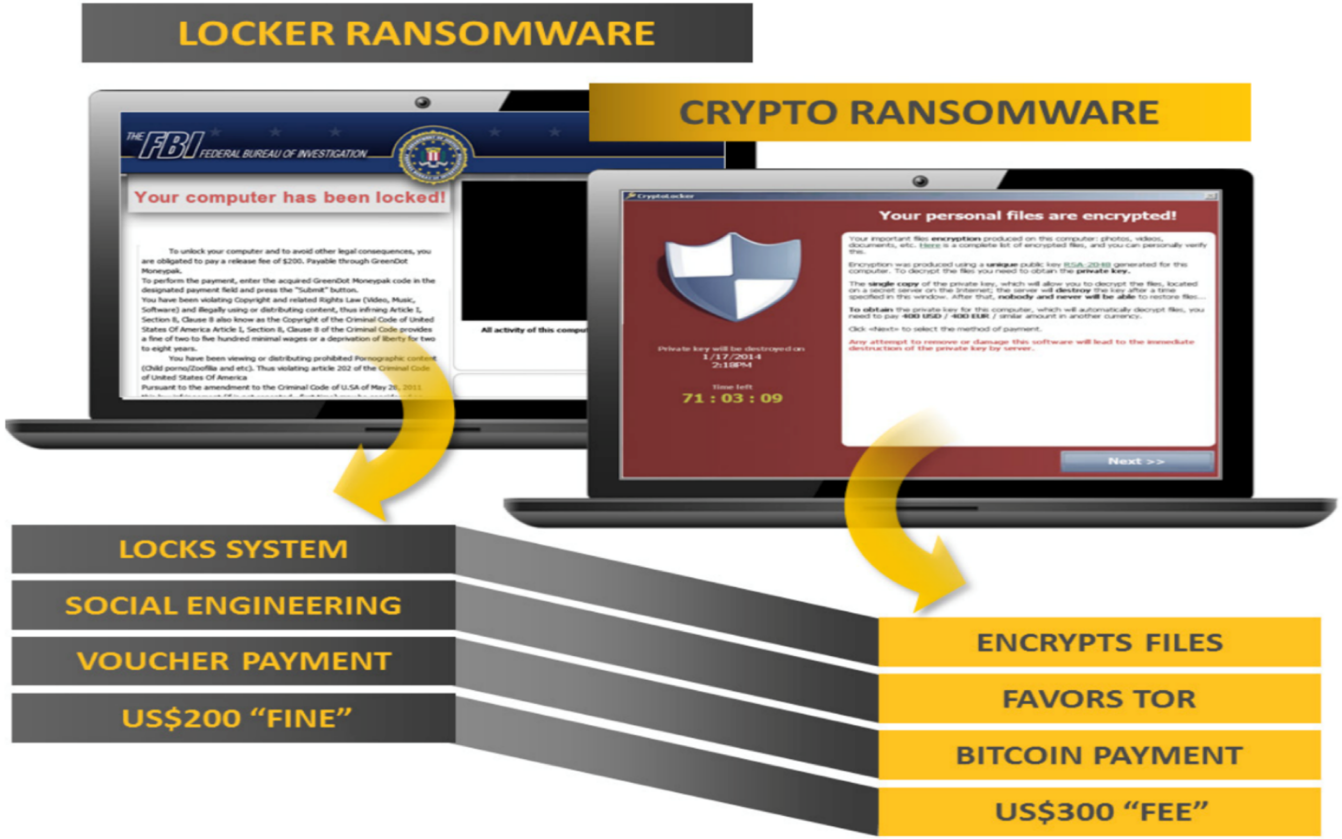
Source: Kaspersky Lab's Global Research & Analysis Team

BBC

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.SA of May 28, 2011

All activity of this compu

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.

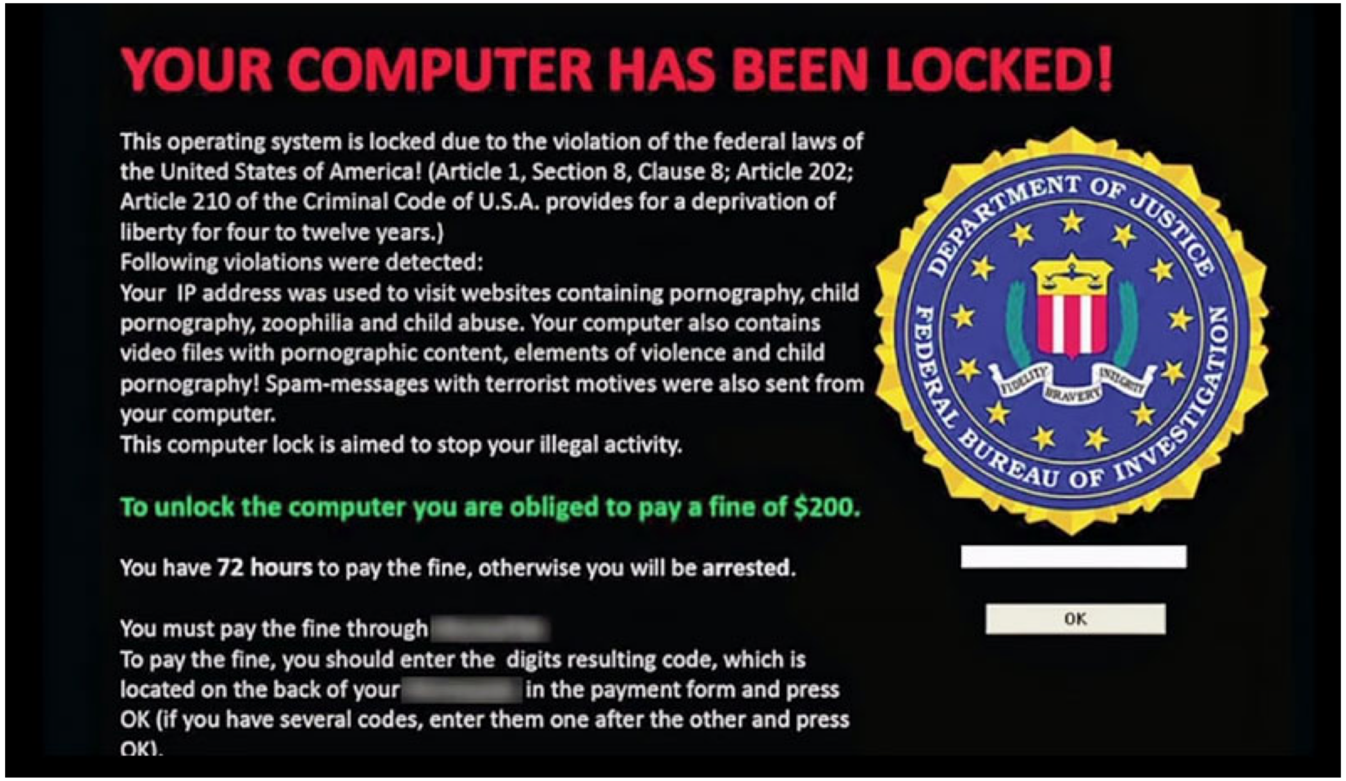
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

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

Time left
71 : 03 : 09

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?

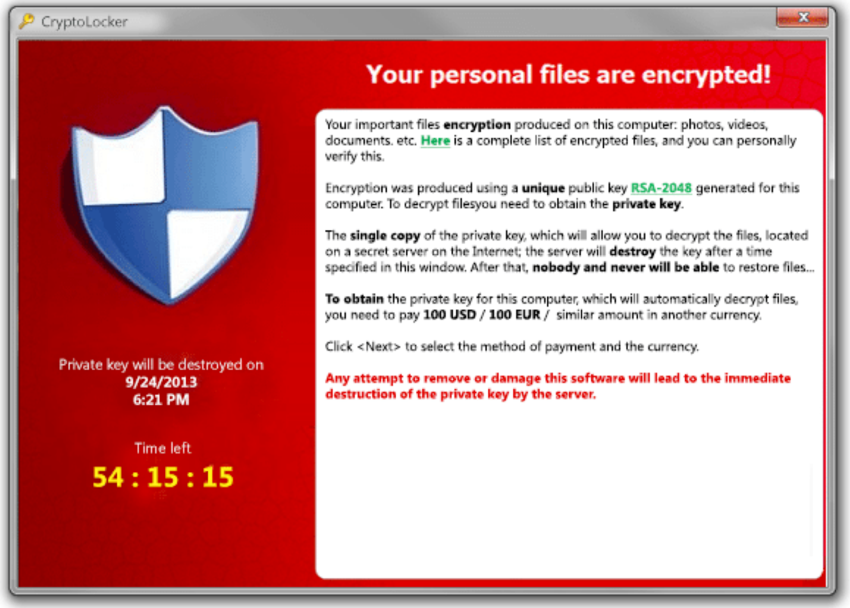
- Observation: only the system is locked by the ransomware, but the data are stored intact

- 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 fastly, since the detection is time-sensitive

Paper Presentation

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

- Presented by Soheil

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

Professor: Dr. Bo Chen

Student: Soheil Sepahyar

Class: CS 5472 (Advanced Topic In Computer Security)

Michigan Technological University

1885

OUTLINE

- Introduction To Ransomware Attacks and Background
- How to defend against ransomware attacks?
- Threat Model
- UNVEIL Design (Early Warning Dynamic Detection for Ransomware)
  - Detecting the File Locker
  - Detecting Screen Locker
- UNVEIL Analysis Environment Preparation
- Evaluation
  - Experimental Setup
  - First Experiment and Ground Truth (Labeled Dataset)
  - Second Experiment and Detecting Zero-Day Ransomware
  - New Case Study type of Ransomware (Automated Detection Of a New Ransomware Family)

OUTLINE

- Discussion and Limitations
- Conclusion and My Final Thoughts
- Q & A
- References

1. *Introduction To Ransomware Attacks and Background*

What is Ransomware attacks?

Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again

1. *Introduction To Ransomware Attacks and Background*

What are the recent and the Most Important Ransomware attacks in 2020 and other years?

1) Communications & Power Industries (CPI) Ransomware Attack

2) University of California San Francisco (UCSF) Ransomware Attack

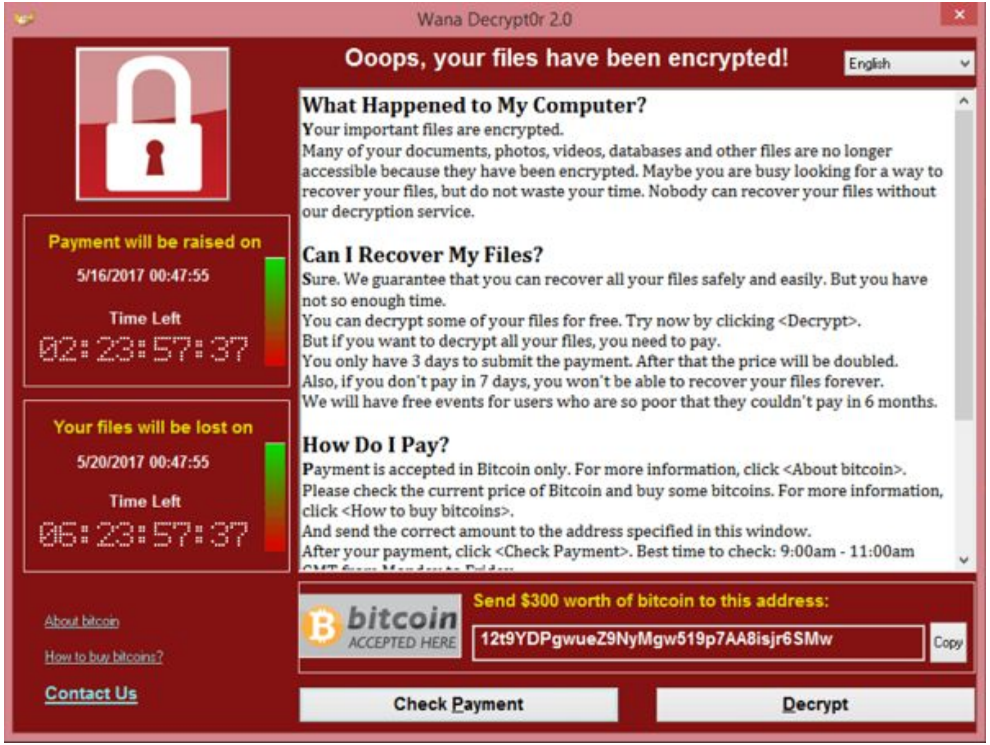
3) WannaCry Outbreak and ...

On 12 May 2017, an updated version of WCry/WannaCry ransomware called “WanaCrypt0r 2.0” struck hospitals belonging to the United Kingdom’s National Health Service (NHS), internet service provider Telefonica and other high-profile targets around the world. Researchers ultimately determined that WannaCry had made its rounds by exploiting EternalBlue, a vulnerability which Microsoft patched in a security bulletin in March 2017. In total, WannaCry demanded $300 in bitcoin from more than 300,000 organizations worldwide through that attack.

1. *Introduction To Ransomware Attacks and Background*

A post-mortem on the impact of WannaCry found the outbreak cost U.K. hospitals almost $100 million pounds and caused significant disruption to patient care, such as the cancellation of some 19,000 appointments — including operations — and the disruption of IT systems for at least a third of all **U.K. National Health Service** (NHS) hospitals and eight percent of general practitioners. In several cases, hospitals in the U.K. were forced to divert emergency room visitors to other hospitals.

WannaCry is an example of crypto **ransomware**, a type of malicious software (**malware**) used by cybercriminals to extort money.



Ooops, your files have been encrypted!

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 not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

How to defend against ransomware attacks?

1) Backup Everything, Every day
2) Screen Your Emails and Don’t Click Suspicious Links or Ads
3) Install an Antivirus Firewall
4) Invest in Security Awareness Training

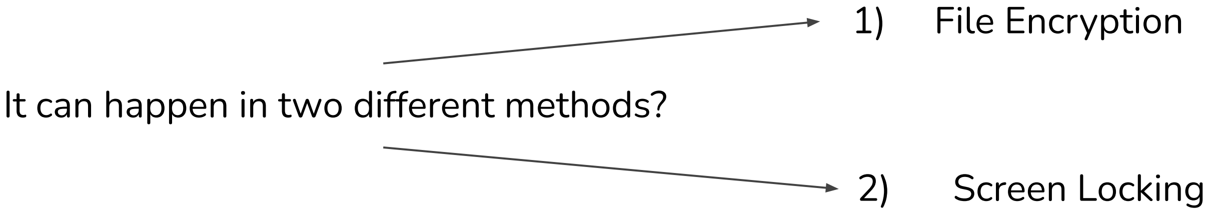
1) Developing detection tools to assist defenders ⇒ Providing insight from internal behavior

2) Developing protection tools (sitting on the End User Machine and Kill Them) ⇒ Stopping the attack, and keeping the data consistent and Monitor the Virus.

Thread Model

Ransomware can use any techniques to attack the users such as:

1) Inject code into benign processes
2) Perform encrypted communication with the C&C server
3) Leverage arbitrary cryptosystems



It can happen in two different methods?

1) File Encryption

2) Screen Locking

Thread Model

Base Part of Ransomware:

- Ransomware informs the victim that attack has taken place
- Ransomware has certain behaviors that can be predictable (such as entropy changes, Iteration of files due to the good amount of access to the data for encryption, Background Activity, accessing user files, Or it might lock your screen!)

Now These hints can be very helpful to detect Ransomwares!!

UNVEIL Architecture

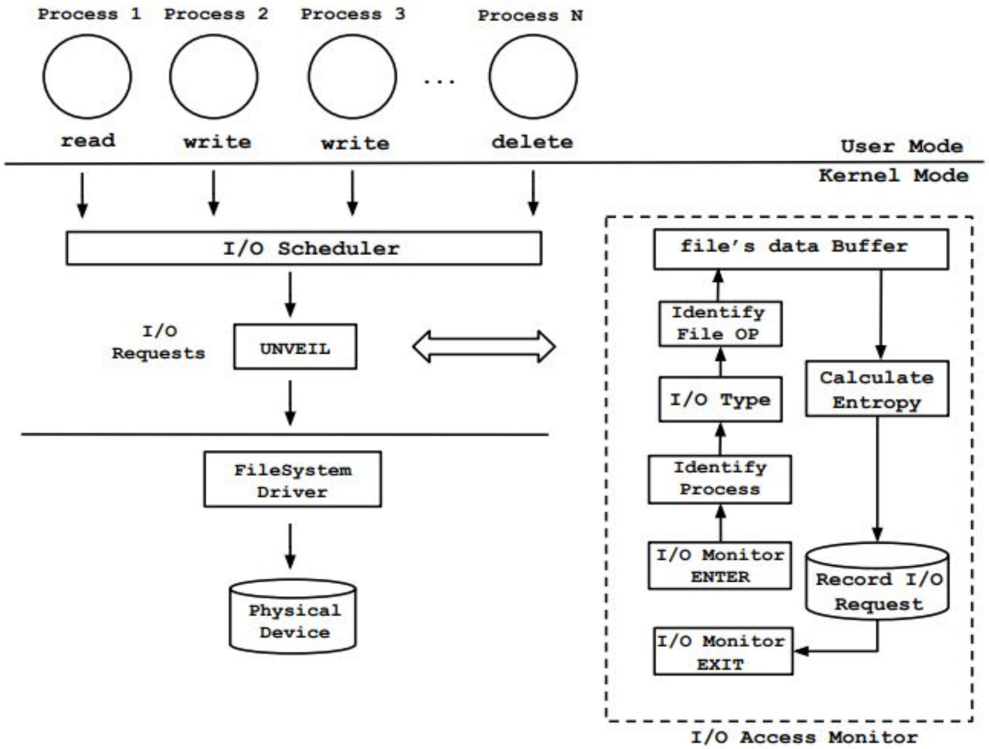


Figure 1: Overview of the design of I/O access monitor in UNVEIL. The module monitors system-wide filesystem accesses of user-mode processes. This allows UNVEIL to have full visibility into interactions with user files.

UNVEIL Design (Early Warning Dynamic Detection for Ransomware)

Detecting The File Locker:

(How UNVEIL uses the output of the filesystem monitor to detect ransomware?)

Detecting Cryptographic Ransomware:

1) Generating a fake (and attractive) user environment
2) Finding a reliable method for monitoring filesystem activity

UNVEIL Design (Early Warning Dynamic Detection for Ransomware)

Why the fake user environment was generated?

1) Making the analysis environment more realistic.

2) Protecting the analysis system from some user environment fingerprinting since static environment can be easily tracked.

UNVEIL Design (Early Warning Dynamic Detection for Ransomware)

Generating Fake (Honey) Content:

1) Files with Valid Header →
   - Using standard libraries (e.g., python- docx, python-pptx)
   - Meaningful Content
   - Realistic Filename which is not random generated

2) File Path → User’s directory structure is generated randomly, but meaningfully

3) File attributes → Generate content with different creation, modification, and access times

Extracting I/O Access Sequences

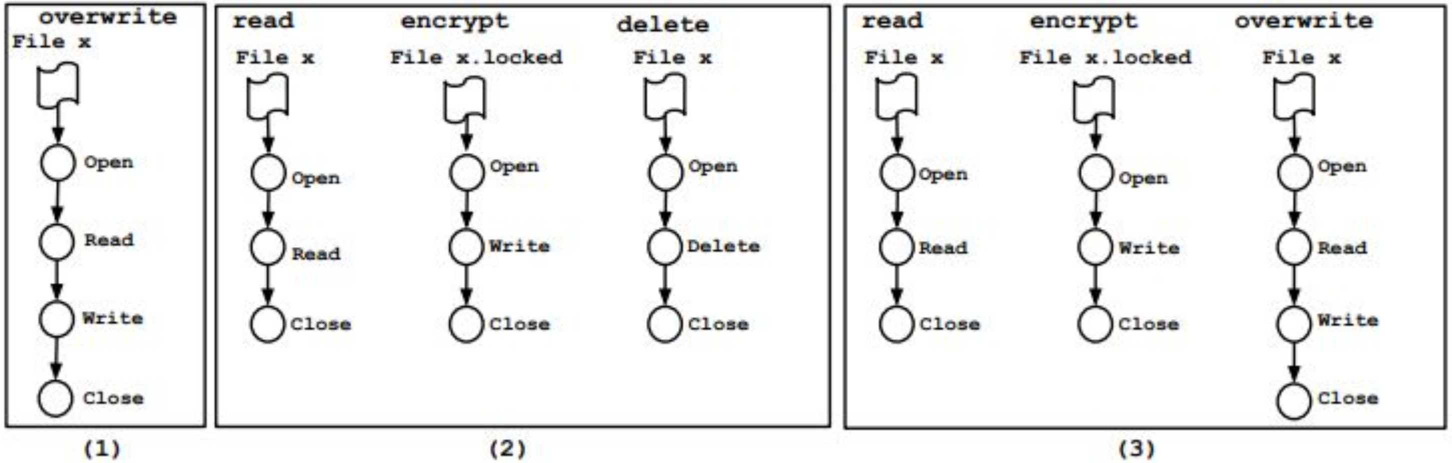
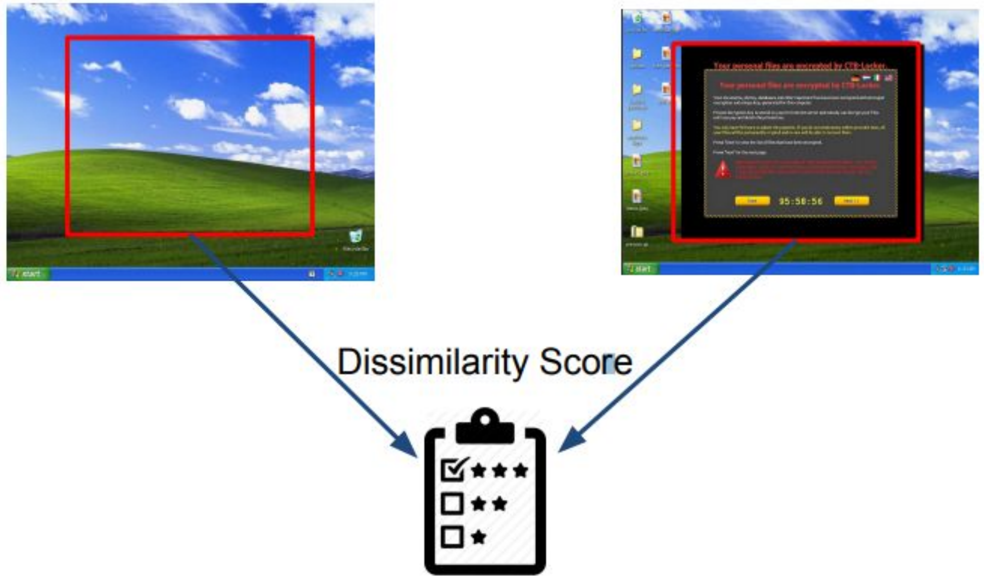


Figure 2: Strategies differ across ransomware families with respect to I/O access patterns. (1) Attacker overwrites the users' file with an encrypted version; (2) Attacker reads, encrypts and deletes files without wiping them from storage; (3) Attacker reads, creates a new encrypted version, and securely deletes the original files by overwriting the content.

UNVEIL Design (Early Warning Dynamic Detection for Ransomware)

Detecting Screen Locker:

The second core component of UNVEIL is aimed at detecting screen locker ransomware. The key insight behind this component is that the attacker must display a ransom note to the victim in order to receive a payment.


Your personal files are encrypted by CTB-Locker.
Your personal files are encrypted by CTB-Locker.
95:58:56
start
Dissimilarity Score

UNVEIL Analysis Environment Preparation

- **UNVEIL is working on top of Cuckoo Sandbox**
  - Support All Windows (Looks Like XP is their experimental OS)
  - This Tool Deployed in the Kernel ⇒ Better Access to the Files
  - Bypassing UNVEIL is not technically easy in user-mode (I think since it has access to the OS layers and resources)

- **Finding Active Malwares**
  - modified some parts of Cuckoo to make it more resilient to environmentally sensitive samples
  - Other anti-evasion measures to look more realistic (such as having Multiple NTFS Drives, IP address changing, etc)

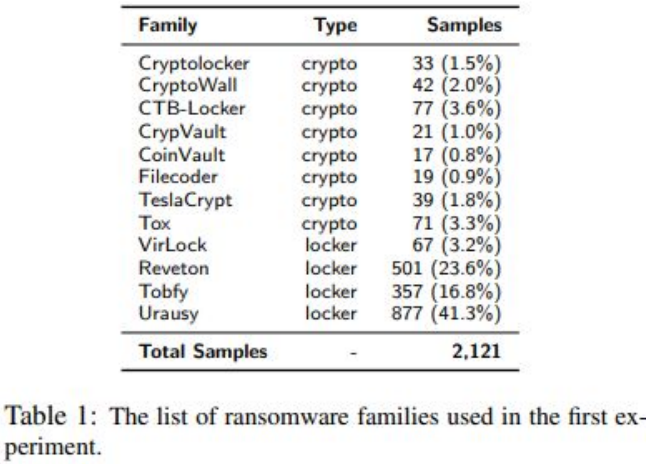
UNVEIL Analysis Environment Preparation

They evaluated UNVEIL using 56 VMs running Windows XP SP3 on a Ganeti cluster based on Ubuntu 14.04 LTS. While Windows XP is not required by UNVEIL, it was chosen because it is well-supported by Cuckoo sandbox.

Each VM had multiple NTFS drives. They took antievasion measures against popular tricks such as changing the IP address range and the MAC addresses of the VMs to prevent the VMs from being fingerprinted by malware authors.

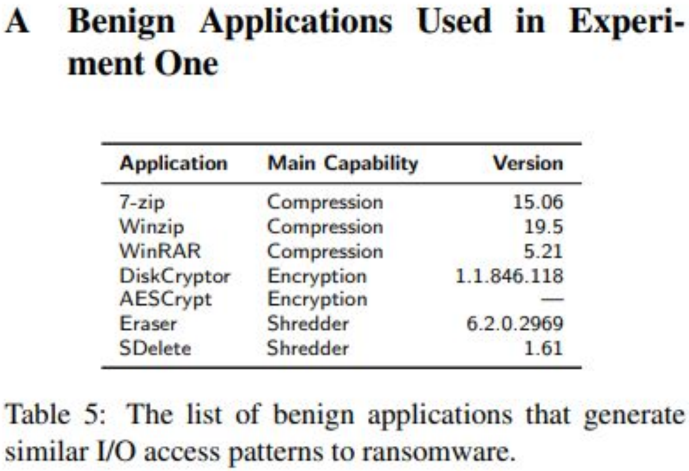
Evaluation

1) **Detecting known ransomware samples**
   - Collecting ~3500 ransomware from public repo, Anubis, two security companies.
   - 149 benign executables including ransomware-like behavior.
   - 348 malware samples from 36 malware families



Family	Type	Samples
Cryptolocker	crypto	33 (1.5%)
CryptoWall	crypto	42 (2.0%)
CTB-Locker	crypto	77 (3.6%)
CrypVault	crypto	21 (1.0%)
CoinVault	crypto	17 (0.8%)
Filecoder	crypto	19 (0.9%)
TeslaCrypt	crypto	39 (1.8%)
Tox	crypto	71 (3.3%)
VirLock	locker	67 (3.2%)
Reveton	locker	501 (23.6%)
Tobfy	locker	357 (16.8%)
Urausy	locker	877 (41.3%)
Total Samples	-	**2,121**

Table 1: The list of ransomware families used in the first experiment.



A Benign Applications Used in Experiment One

Application	Main Capability	Version
7-zip	Compression	15.06
Winzip	Compression	19.5
WinRAR	Compression	5.21
DiskCryptor	Encryption	1.1.846.118
AESCrypt	Encryption	—
Eraser	Shredder	6.2.0.2969
SDelete	Shredder	1.61

Table 5: The list of benign applications that generate similar I/O access patterns to ransomware.

Evaluation

2) Evaluation UNVEIL with unknown samples

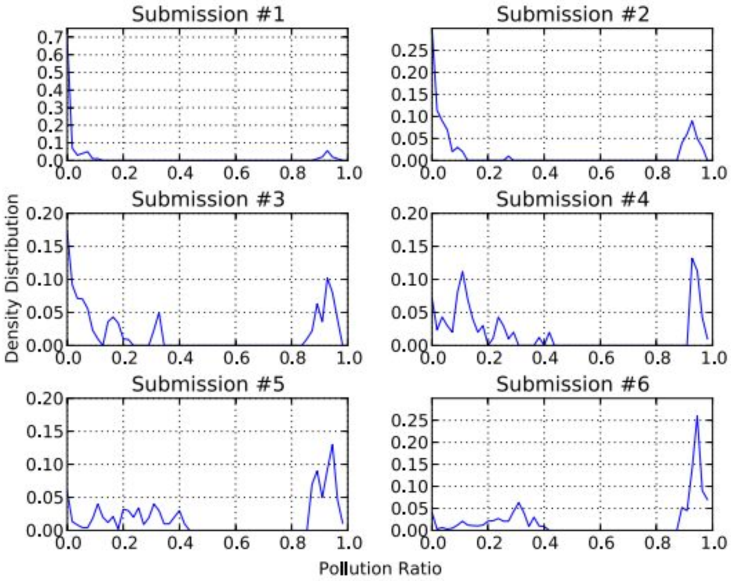
- The incoming samples were acquired from the daily malware feed provided by Anubis from March 18 to February 12, 2016.

- The dataset contained 148,223 distinct samples.

Evaluation

2) **Evaluation UNVEIL with unknown samples**

VT == VirusTotal



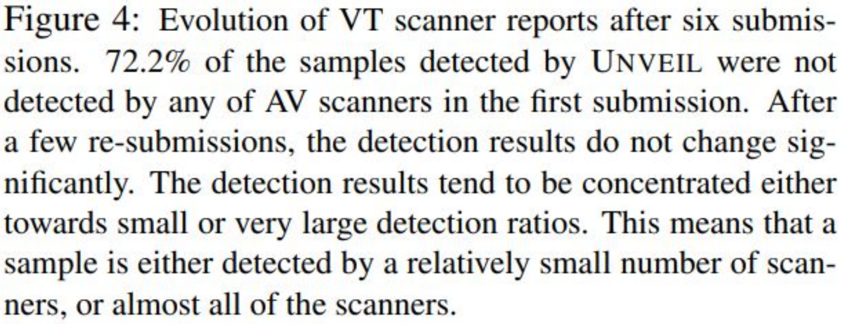
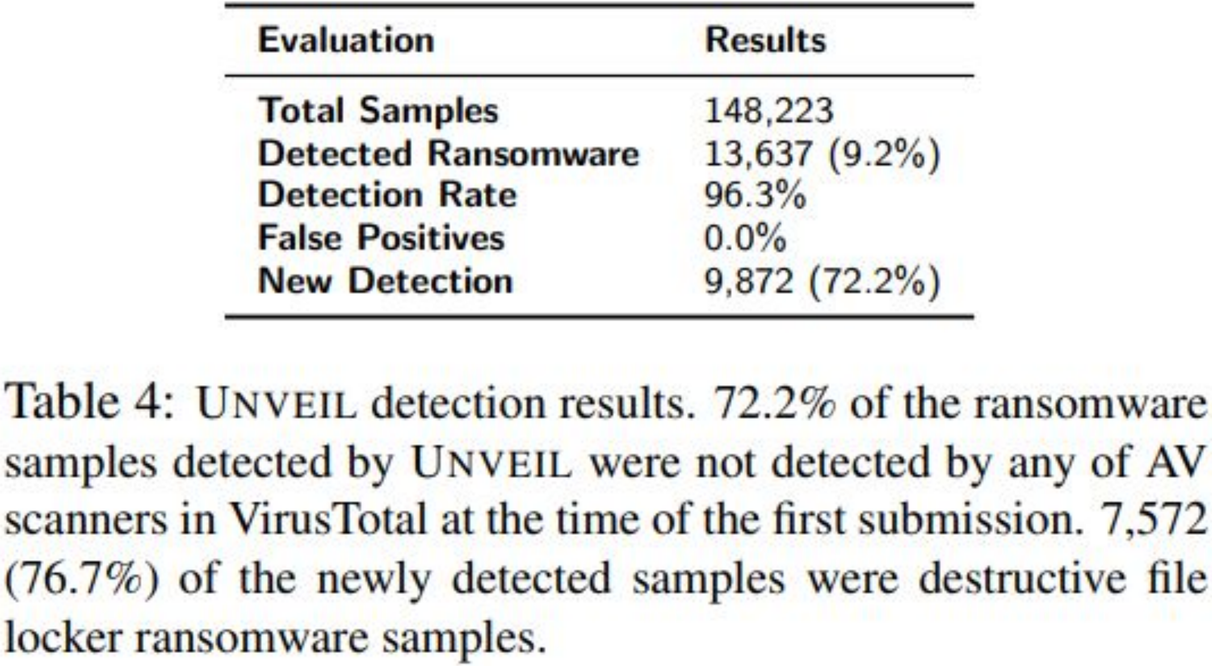


Figure 4: Evolution of VT scanner reports after six submissions. 72.2% of the samples detected by UNVEIL were not detected by any of AV scanners in the first submission. After a few re-submissions, the detection results do not change significantly. The detection results tend to be concentrated either towards small or very large detection ratios. This means that a sample is either detected by a relatively small number of scanners, or almost all of the scanners.

Evaluation (Final Results)



Evaluation	Results
Total Samples	148,223
Detected Ransomware	13,637 (9.2%)
Detection Rate	96.3%
False Positives	0.0%
New Detection	9,872 (72.2%)

Table 4: UNVEIL detection results. 72.2% of the ransomware samples detected by UNVEIL were not detected by any of AV scanners in VirusTotal at the time of the first submission. 7,572 (76.7%) of the newly detected samples were destructive file locker ransomware samples.

Evaluation

New Case Study type of Ransomware (Automated Detection Of a New Ransomware Family)

During the experiments, they discovered a new malware family named “**SilentCrypt**”:

analysis concluded that the malicious activity is started only if user activity is detected. Unlike other ransomware samples that immediately attack a victim’s files when they are executed.

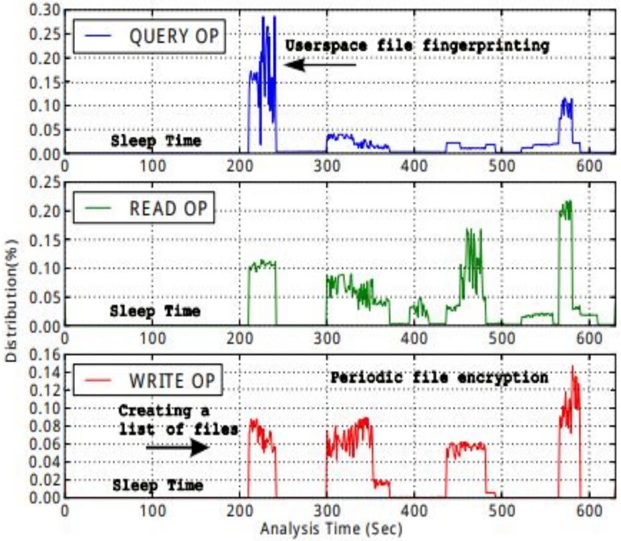


Figure 5: I/O activities of a previously unknown ransomware family detected by UNVEIL. The sample first performs victim file fingerprinting to ensure that the running environment is not a bare user environment.

Discussion and Limitations

- The evaluation section demonstrates that UNVEIL achieves good, practical, and useful detection results on a large, real-world dataset compare with a lot of other advanced AV scanner.

- Another possibility is that a malware might only encrypt a specific part of a file instead of aggressively encrypting the entire file, or simply shuffle the file content using a specific pattern that makes the files unreadable.

- Clearly, there is always the possibility that an attacker will be able to fingerprint the dynamic analysis environment. For example, stalling code has become increasingly popular to prevent the dynamic analysis of a sample. Such code takes longer to execute in a virtual environment, preventing execution from completing during an analysis.

Static and Dynamic Analyses Explained

1) Static analysis is performed in a non-runtime environment. Static application security testing (SAST) is a testing process that looks at the application from the inside out. This test process is performed without executing the program, but rather by examining the source code, byte code or application binaries for signs of security vulnerabilities.

2) Dynamic application security testing (DAST) looks at the application from the outside in — by examining it in its running state and trying to manipulate it in order to discover security vulnerabilities. The dynamic test simulates attacks against a web application and analyzes the application’s reactions, determining whether it is vulnerable.

Conclusion and My Final Thoughts

- Ransomware is a serious threat.
- UNVEIL introduces concrete models to detect Ransomware.
- Detecting an unknown family shows that the solutions are useful in practice.
- Great Job regarding the importance of this work and ransomware.
- I think Screen Lockers detection can be very much improved with Machine Learning and Deep Learning algorithms rather than mostly pure algorithms. (One example can be transparency issue of the ransomware app on the desktop)
- I also think the author also could put more effort into the changes in the entropy of the file to detect ransomware in addition to checking file system monitoring…

Questions?

References

1. https://www.keepnetlabs.com/top-11-ransomware-attacks-in-2020-2021/

2. A Large-Scale, Automated Approach to Detecting Ransomware Amin Kharraz, Sajjad Arshad, Collin Mulliner, William Robertson, Engin Kirda

3. SilentCrypt: A new ransomware family. https: //www.youtube.com/watch?v=qiASKA4BMck, 2016.

4. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

5. KHARRAZ, A., ROBERTSON, W., BALZAROTTI, D., BILGE, L., AND KIRDA, E. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) (07 2015).

6. https://www.veracode.com/blog/secure-development/static-testing-vs-dynamic-testing