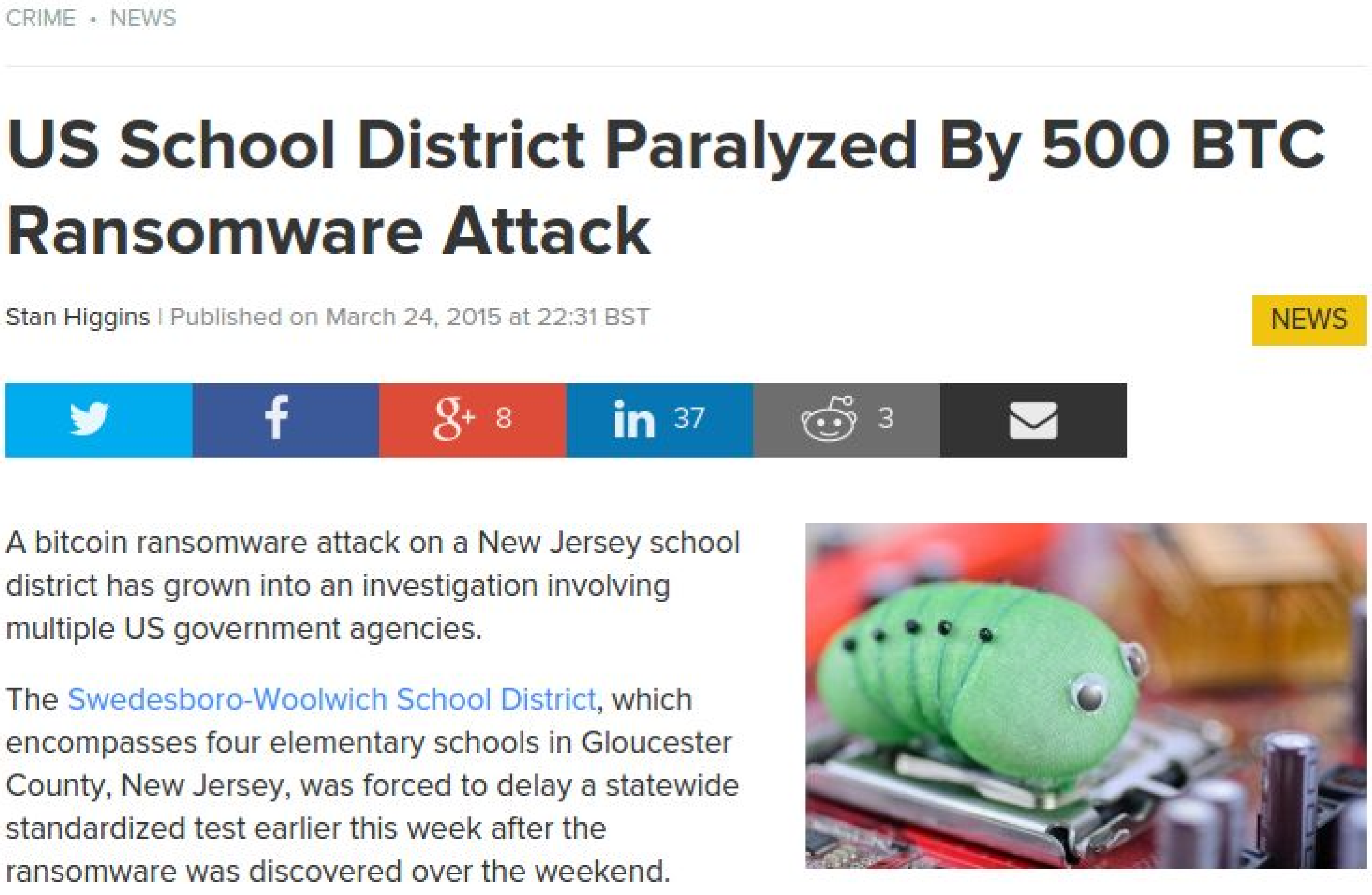
Northeastern University

International Secure Systems Lab

A Large-Scale, Automated Approach to Detecting Ransomware

Amin Kharraz, Sajjad Arshad, Collin Mulliner,
William Robertson, Engin Kirda

Attacks on School Districts

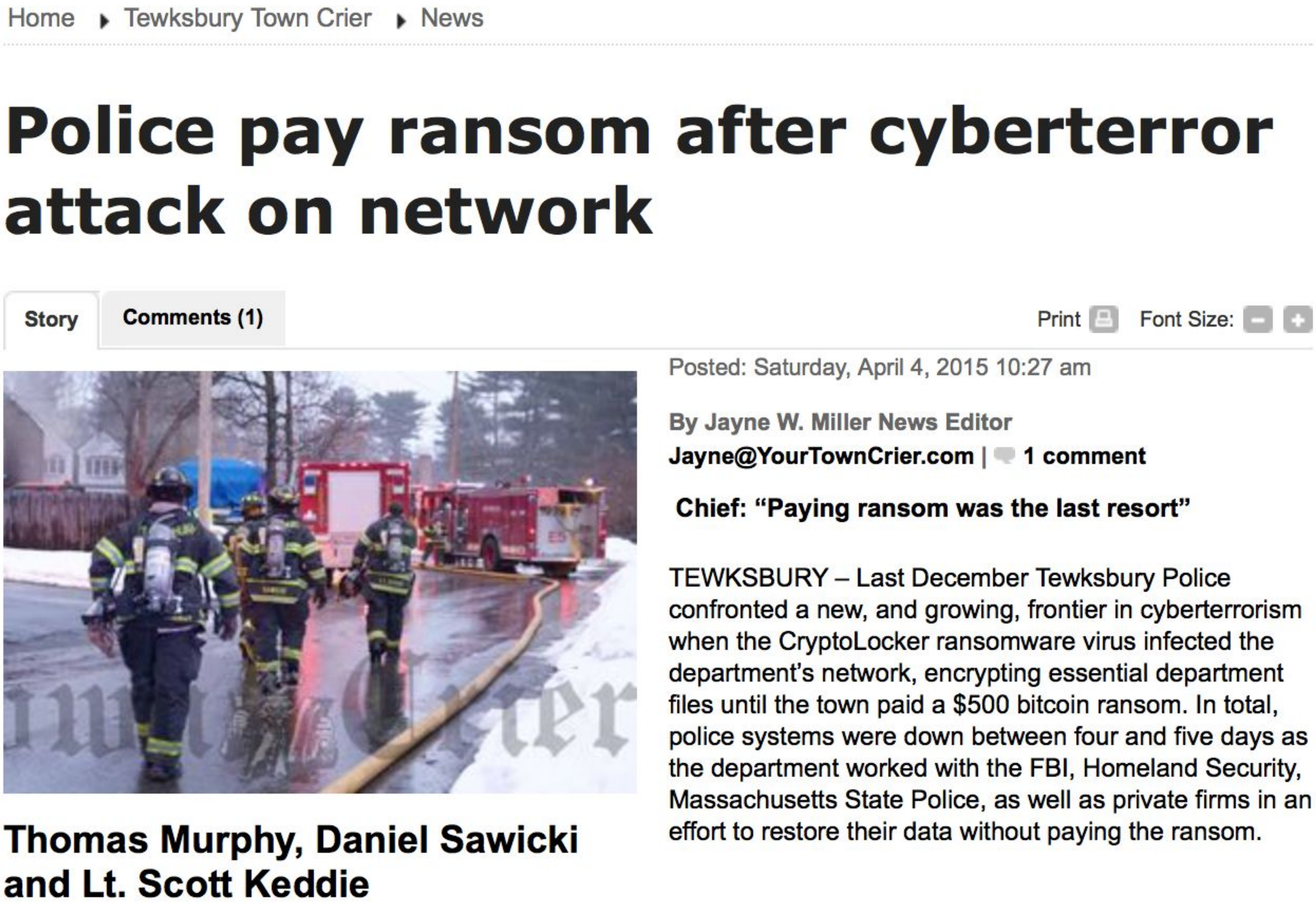


US School District Paralyzed By 500 BTC Ransomware Attack

Stan Higgins | Published on March 24, 2015 at 22:31 BST

A bitcoin ransomware attack on a New Jersey school district has grown into an investigation involving multiple US government agencies.

The Swedesboro-Woolwich School District, which encompasses four elementary schools in Gloucester County, New Jersey, was forced to delay a statewide standardized test earlier this week after the ransomware was discovered over the weekend.



Home ▸ Tewksbury Town Crier ▸ News

Police pay ransom after cyberterror attack on network

Story | Comments (1) | Print | Font Size:

Posted: Saturday, April 4, 2015 10:27 am

By Jayne W. Miller News Editor
Jayne@YourTownCrier.com | 1 comment

Chief: "Paying ransom was the last resort"

TEWKSBURY – Last December Tewksbury Police confronted a new, and growing, frontier in cyberterrorism when the CryptoLocker ransomware virus infected the department's network, encrypting essential department files until the town paid a $500 bitcoin ransom. In total, police systems were down between four and five days as the department worked with the FBI, Homeland Security, Massachusetts State Police, as well as private firms in an effort to restore their data without paying the ransom.

Thomas Murphy, Daniel Sawicki and Lt. Scott Keddie

Attacks on Hospitals

YOUR PERSONAL FILES
ARE ENCRYPTED
TIME LEFT TO PAY:
71:59:02

Public Service Announcement

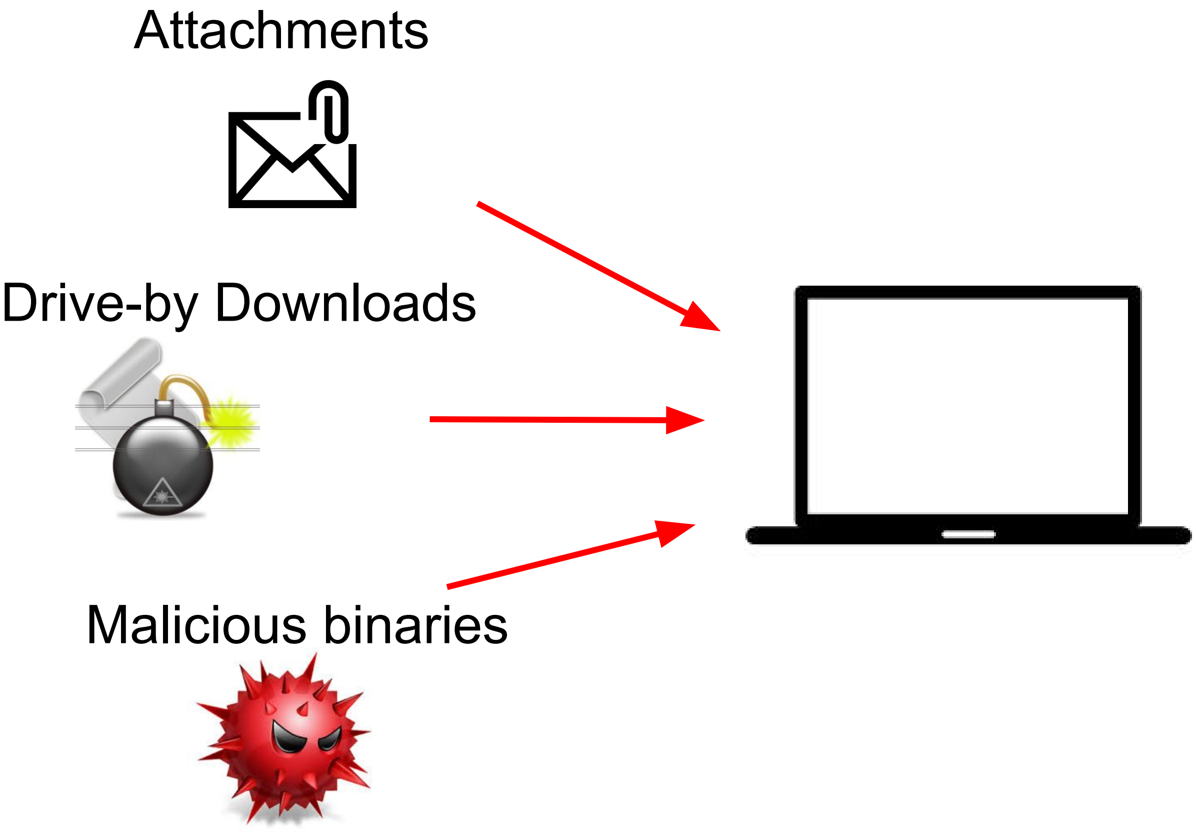
FEDERAL BUREAU OF INVESTIGATION

“Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.”

– FBI Security Bulletin, June 2015

What is a ransomware attack?

❶ Infecting the machine

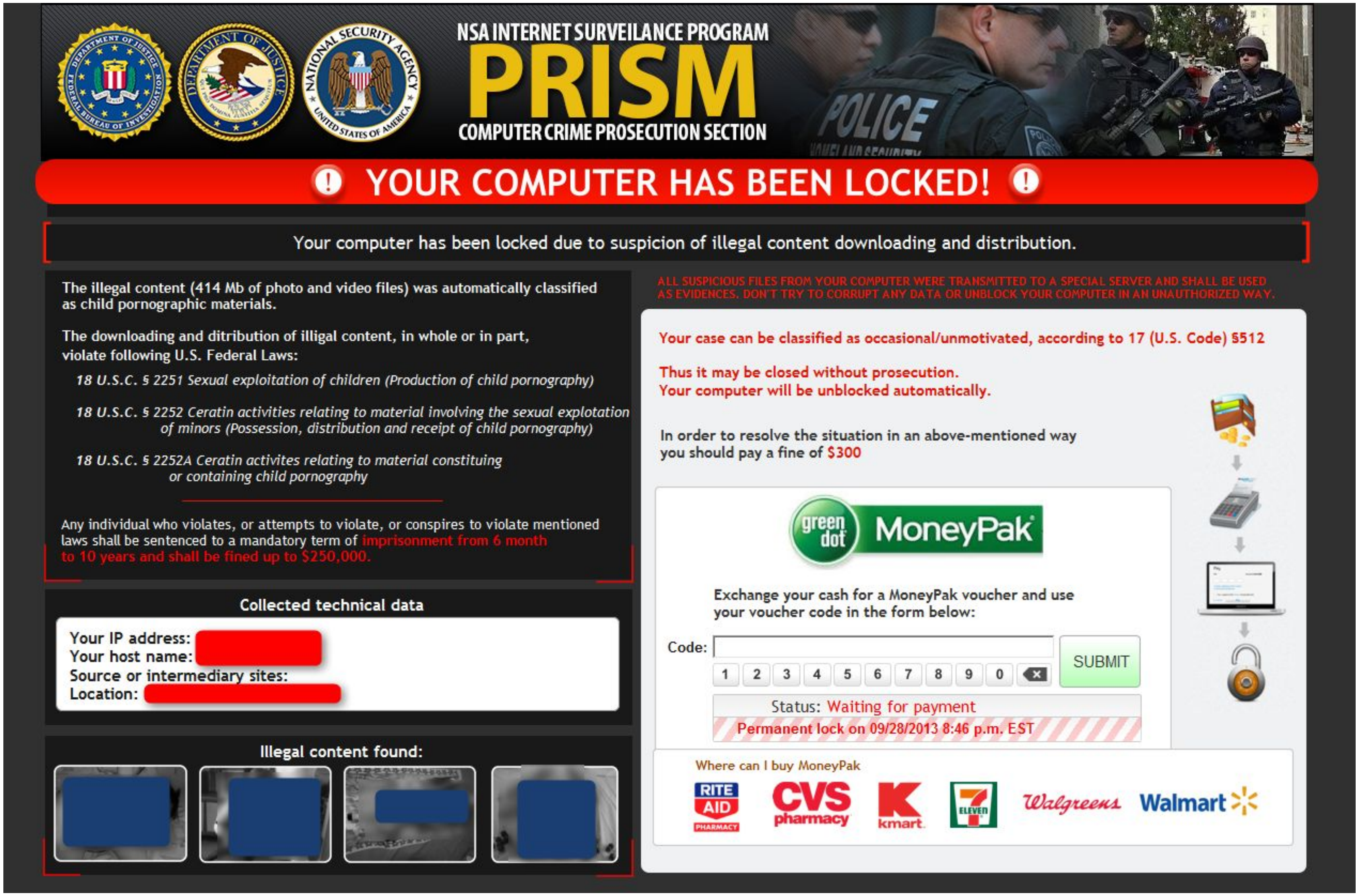


Attachments

Drive-by Downloads

Malicious binaries

A Typical Ransom Note



NSA INTERNET SURVEILANCE PROGRAM
PRISM
COMPUTER CRIME PROSECUTION SECTION
POLICE

YOUR COMPUTER HAS BEEN LOCKED!

Your computer has been locked due to suspicion of illegal content downloading and distribution.

The illegal content (414 Mb of photo and video files) was automatically classified as child pornographic materials.

The downloading and ditribution of illigal content, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251 Sexual exploitation of children (Production of child pornography)

18 U.S.C. § 2252 Ceratin activities relating to material involving the sexual explotation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A Ceratin activites relating to material constituing or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 6 month to 10 years and shall be fined up to $250,000.

Collected technical data

Your IP address: [redacted]
Your host name:
Source or intermediary sites:
Location: [redacted]

Illegal content found:

ALL SUSPICIOUS FILES FROM YOUR COMPUTER WERE TRANSMITTED TO A SPECIAL SERVER AND SHALL BE USED AS EVIDENCES. DON'T TRY TO CORRUPT ANY DATA OR UNBLOCK YOUR COMPUTER IN AN UNAUTHORIZED WAY.

Your case can be classified as occasional/unmotivated, according to 17 (U.S. Code) §512

Thus it may be closed without prosecution.
Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300

Exchange your cash for a MoneyPak voucher and use your voucher code in the form below:

Code:

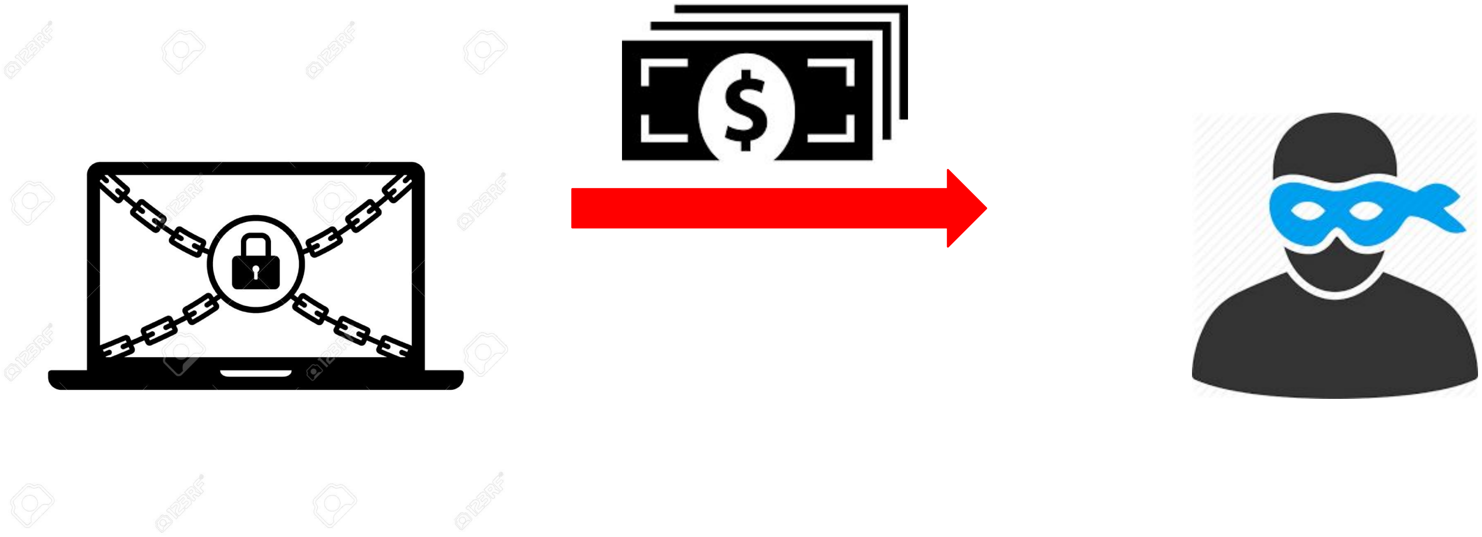
Status: Waiting for payment

Permanent lock on 09/28/2013 8:46 p.m. EST

Where can I buy MoneyPak

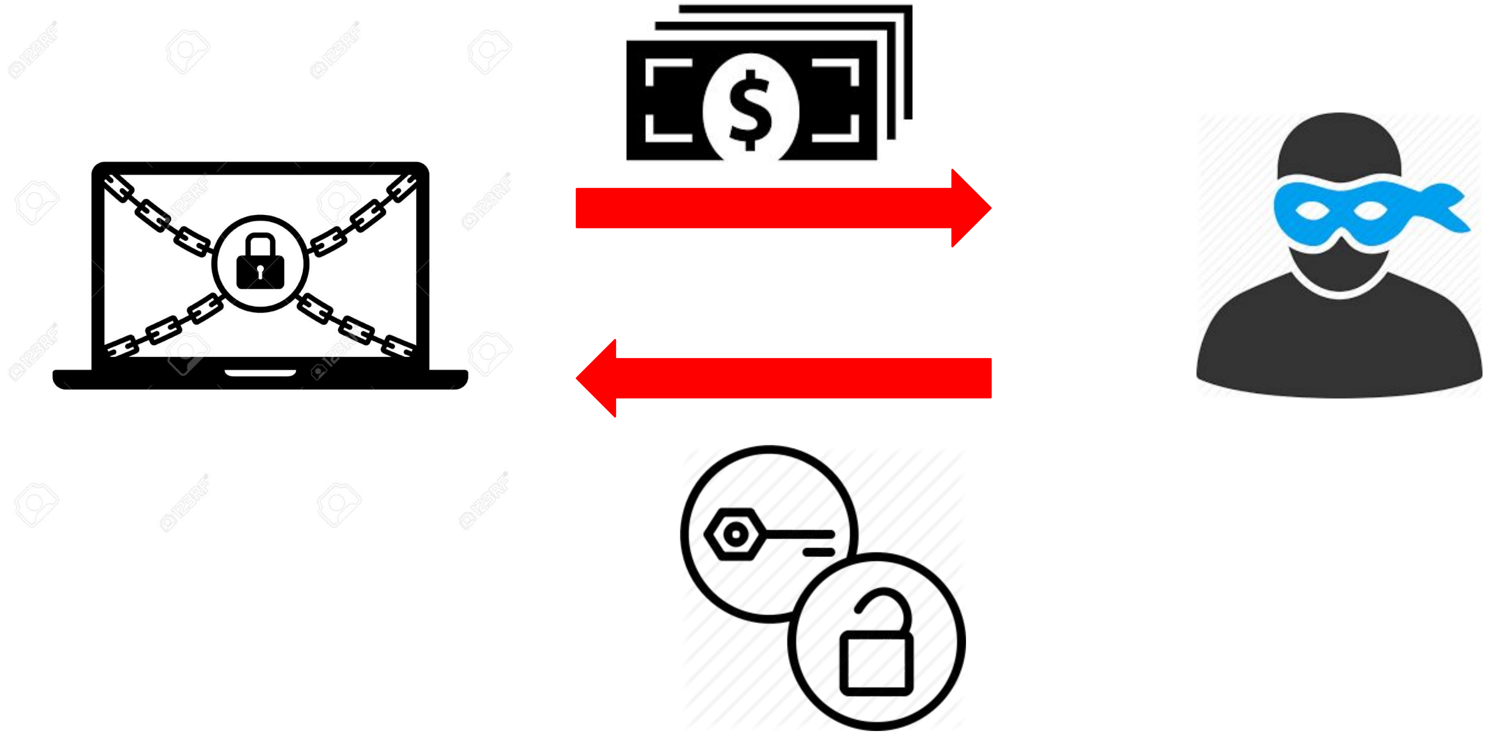
What is a ransomware attack?

❷ Paying the ransom fee



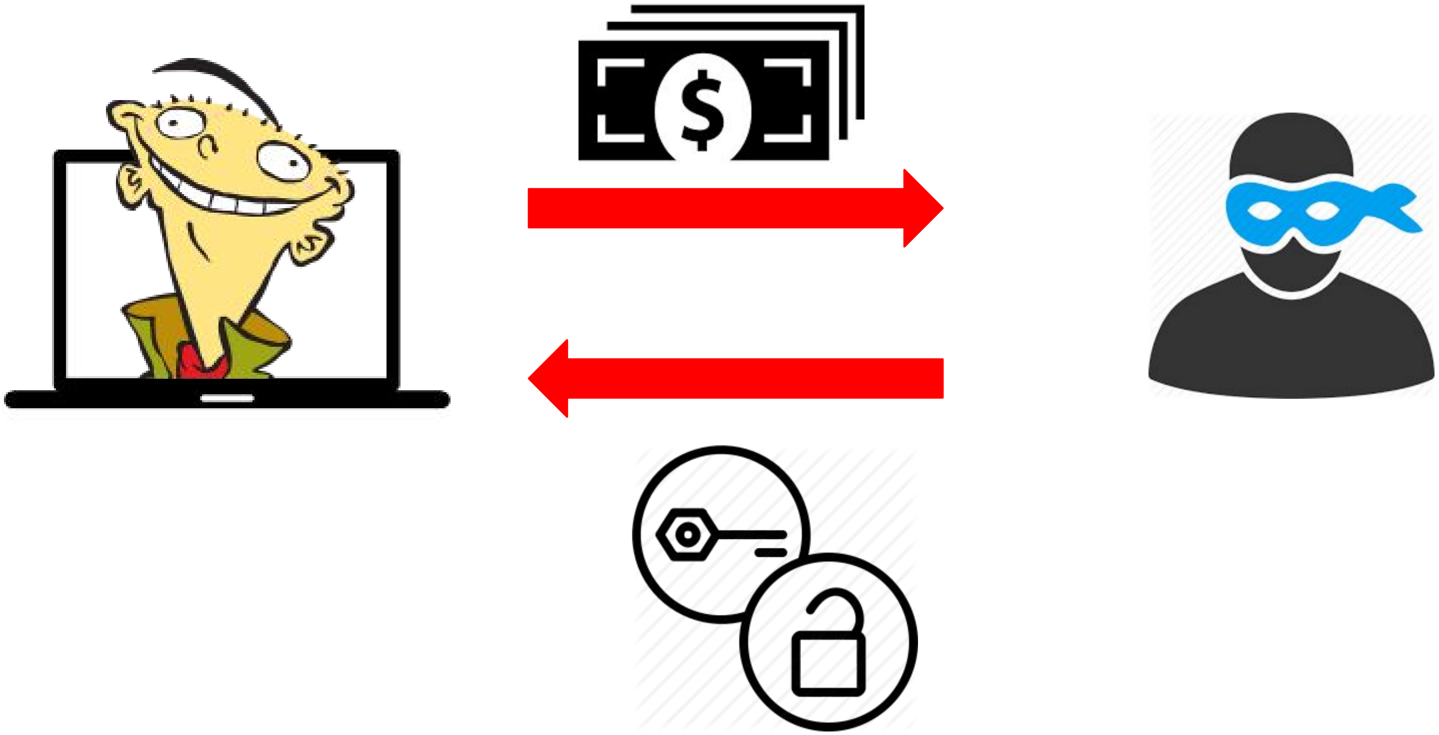
What is a ransomware attack?

❸ Receiving the decryption key



What is a ransomware attack?

❹ Unlocking the machine



How to defend against ransomware attacks?

- Educating end-users
  - Have a reliable *backup* policy
  - Avoid risky browsing
- Developing *detection* tools to assist defenders
  - Providing insight from *internal* behavior
- Developing *protection* tools to enhance AV capabilities
  - Stopping the attack, and keeping the data consistent

How to defend against ransomware attacks?

- Educating end-users
  - Have a reliable *backup* policy
  - Avoid risky browsing
- Developing *detection* tools to assist defenders
  - Providing insight from *internal* behavior
- Developing *protection* tools to enhance AV capabilities
  - Stopping the attack, and keeping the data consistent

But, How can we detect a ransomware sample?

Achilles' Heel of Ransomware

- Ransomware *has to inform* victim that attack has taken place
  - Behavior inherent in its nature
- Ransomware has certain behaviors that are predictable
  - e.g., entropy changes, modal dialogs and background activity, accessing "honey" files
- A good sandbox that looks for some of these signs helps here…

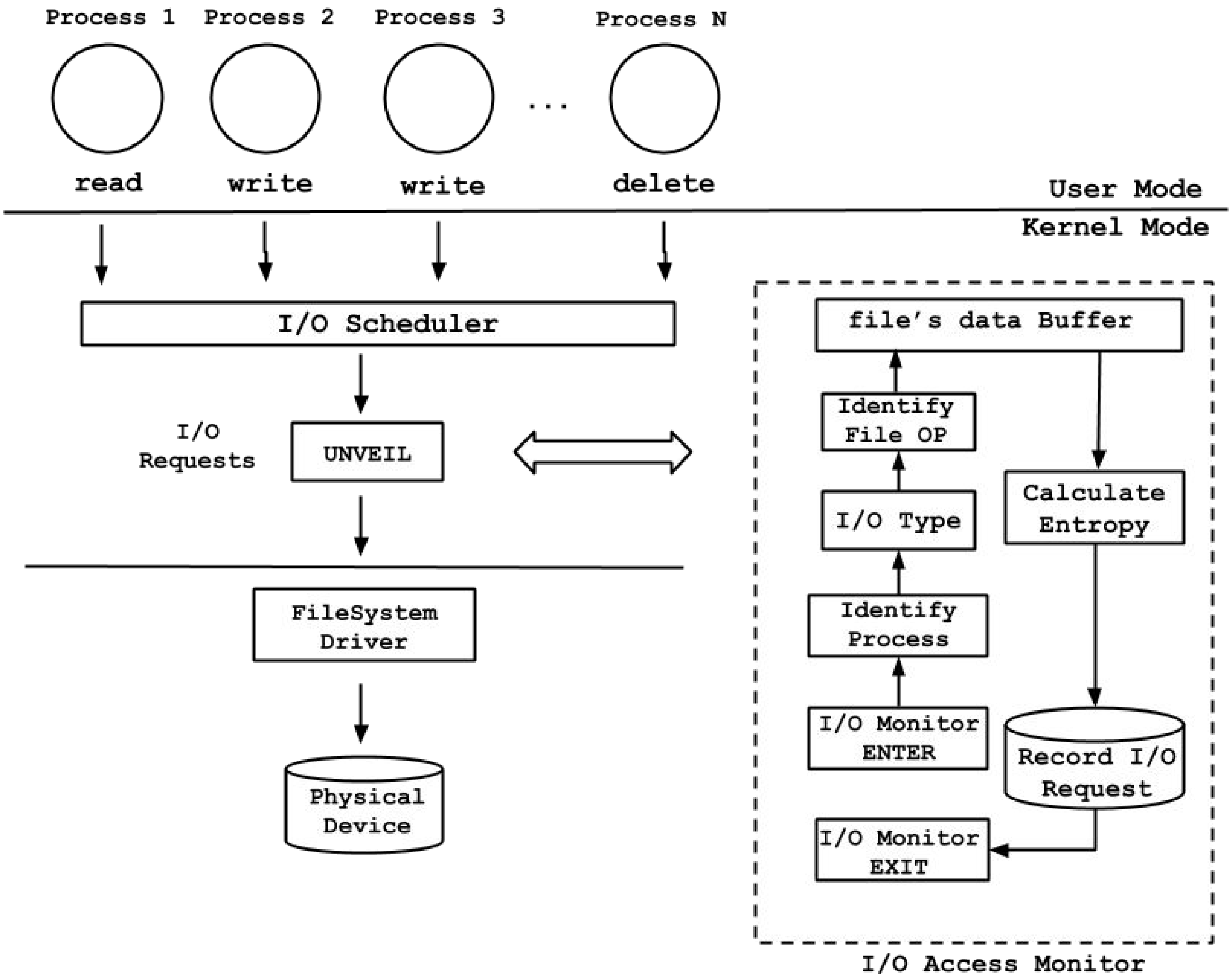
UNVEIL: An Early Warning Dynamic Detection System for Ransomware

Approach

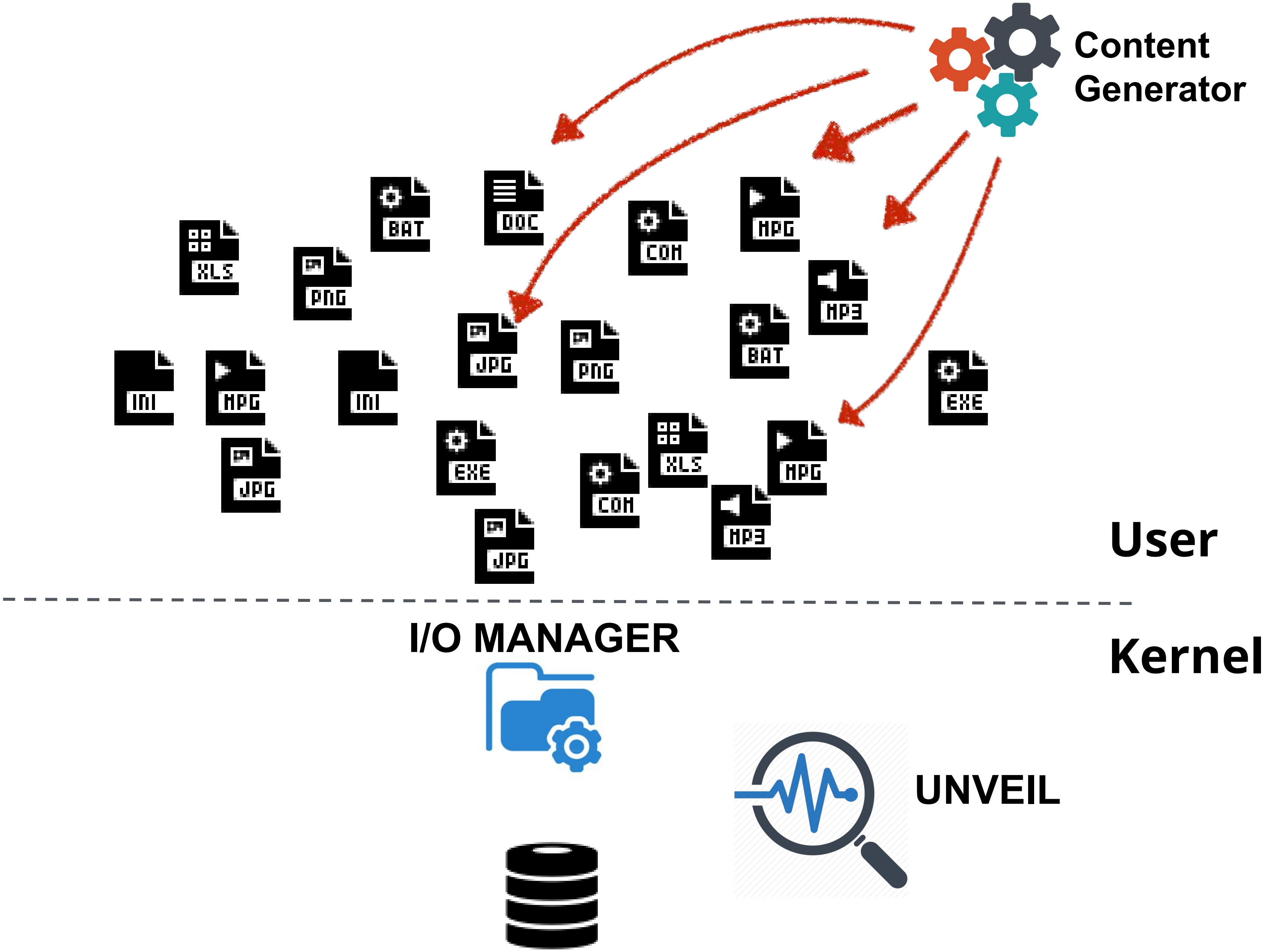
- Detecting ransomware based on two techniques:
  - 1) Crypto-style Ransomware
    - Generating a fake (and attractive) user environment
    - Finding a reliable method for monitoring filesystem activity
  - 2) Desktop Locker
    - Going after the ransom note and using heuristics to detect such a message to the user

Generating Fake (Honey) Content

- Real files with valid headers
  - Using standard libraries (e.g., *python- docx, python-pptx, OpenSSL*)
  - Content that appears meaningful
  - File names do not look random, and appear realistic
- File paths
  - User's directory structure is generated randomly, but meaningfully
- File attributes
  - Generate content with different creation, modification, and access times



UNVEIL's Architecture



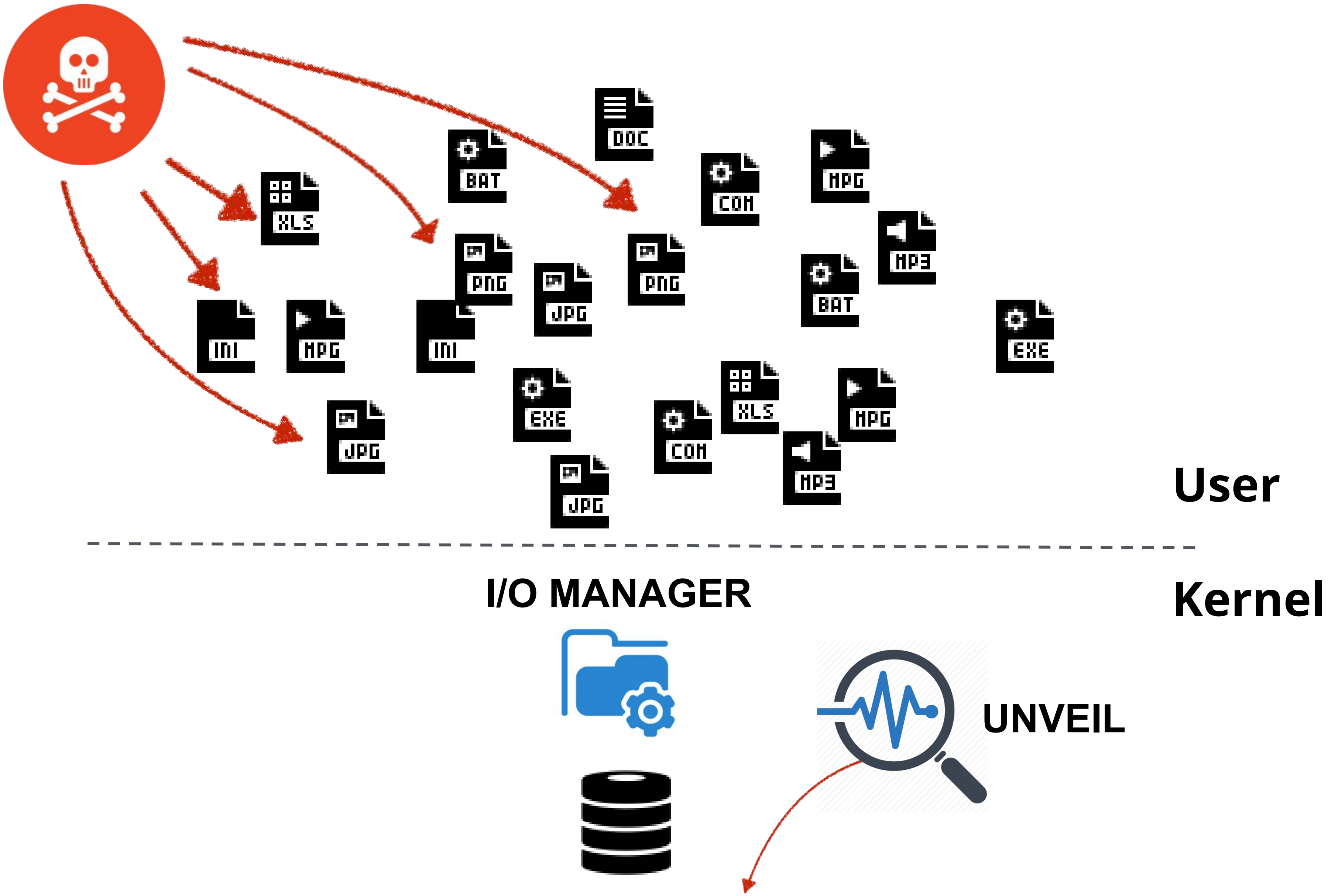
Content Generator

User

Kernel

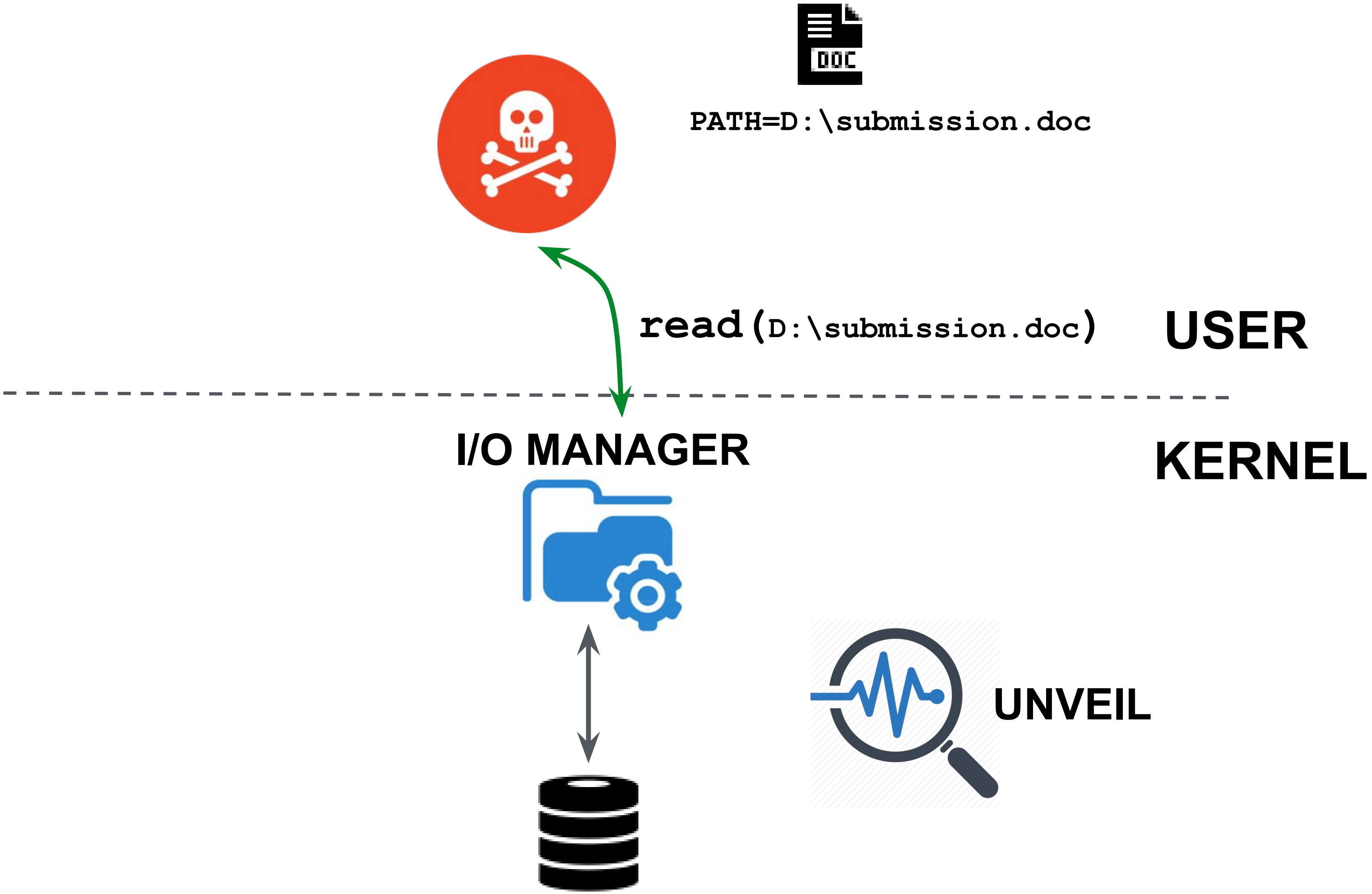
I/O MANAGER

UNVEIL



$$R_{fs} = \langle \mathrm{Time}, P_{name}, P_{id}, PP_{id}, IRP_{flag}, \mathrm{Arg}, \mathrm{Result}, \mathrm{Buf}_{Entropy} \rangle$$

❶ Reading user’s file content



PATH=D:\submission.doc

read(D:\submission.doc)

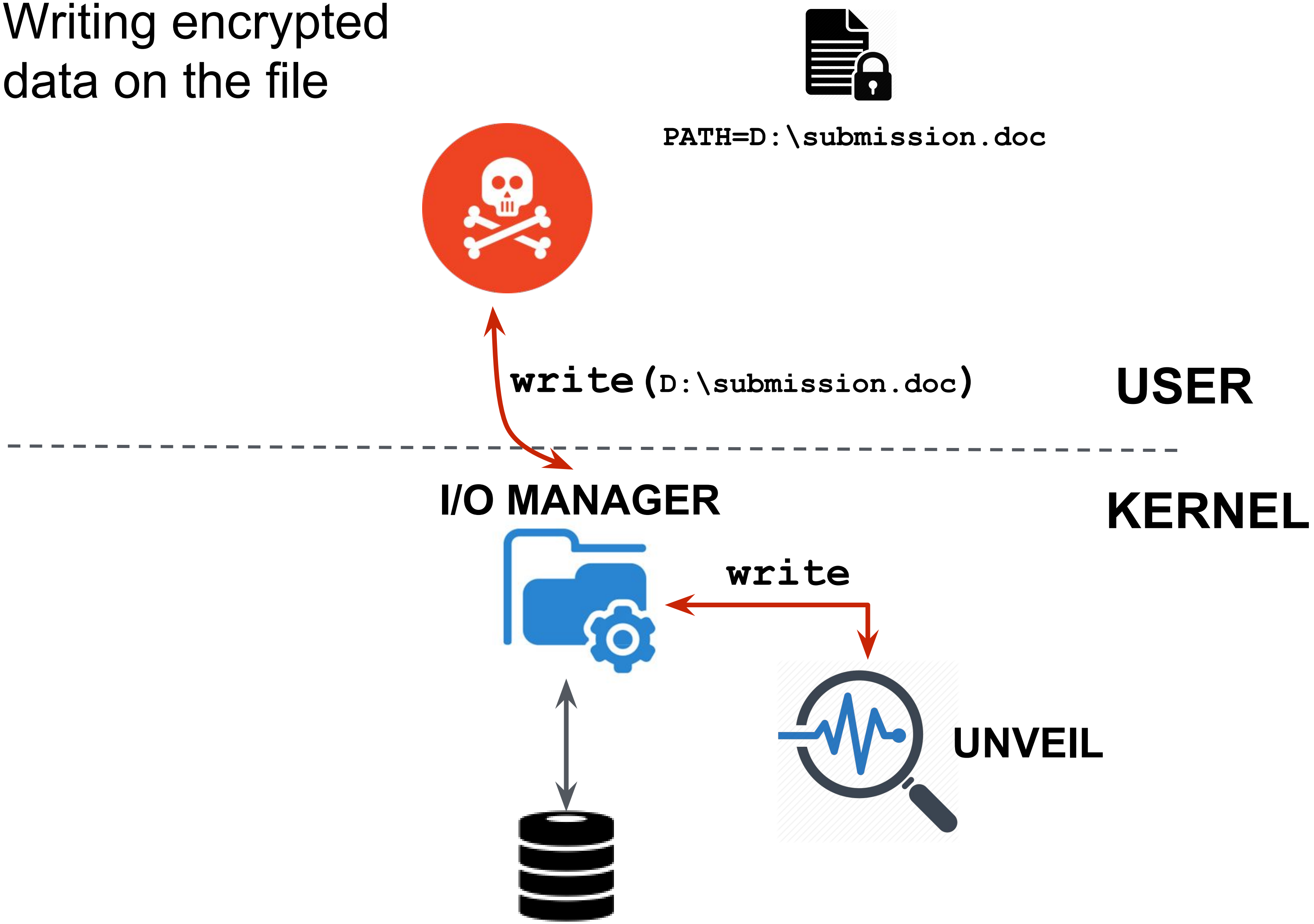
USER

KERNEL

I/O MANAGER

UNVEIL

2 Writing encrypted data on the file



PATH=D:\submission.doc

write(D:\submission.doc)

USER

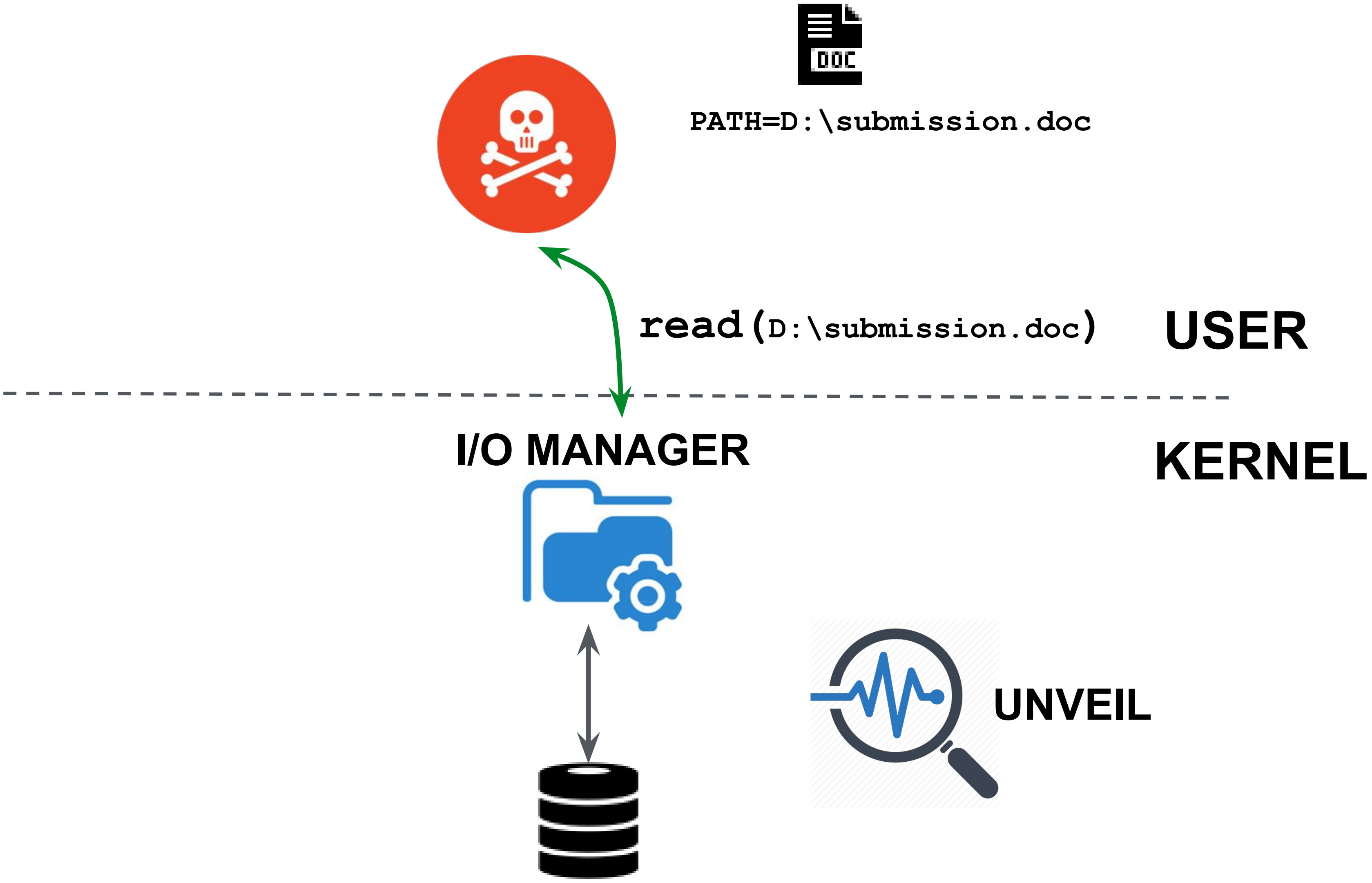
KERNEL

I/O MANAGER

write

UNVEIL

❶ Reading user’s file content



PATH=D:\submission.doc

read(D:\submission.doc)

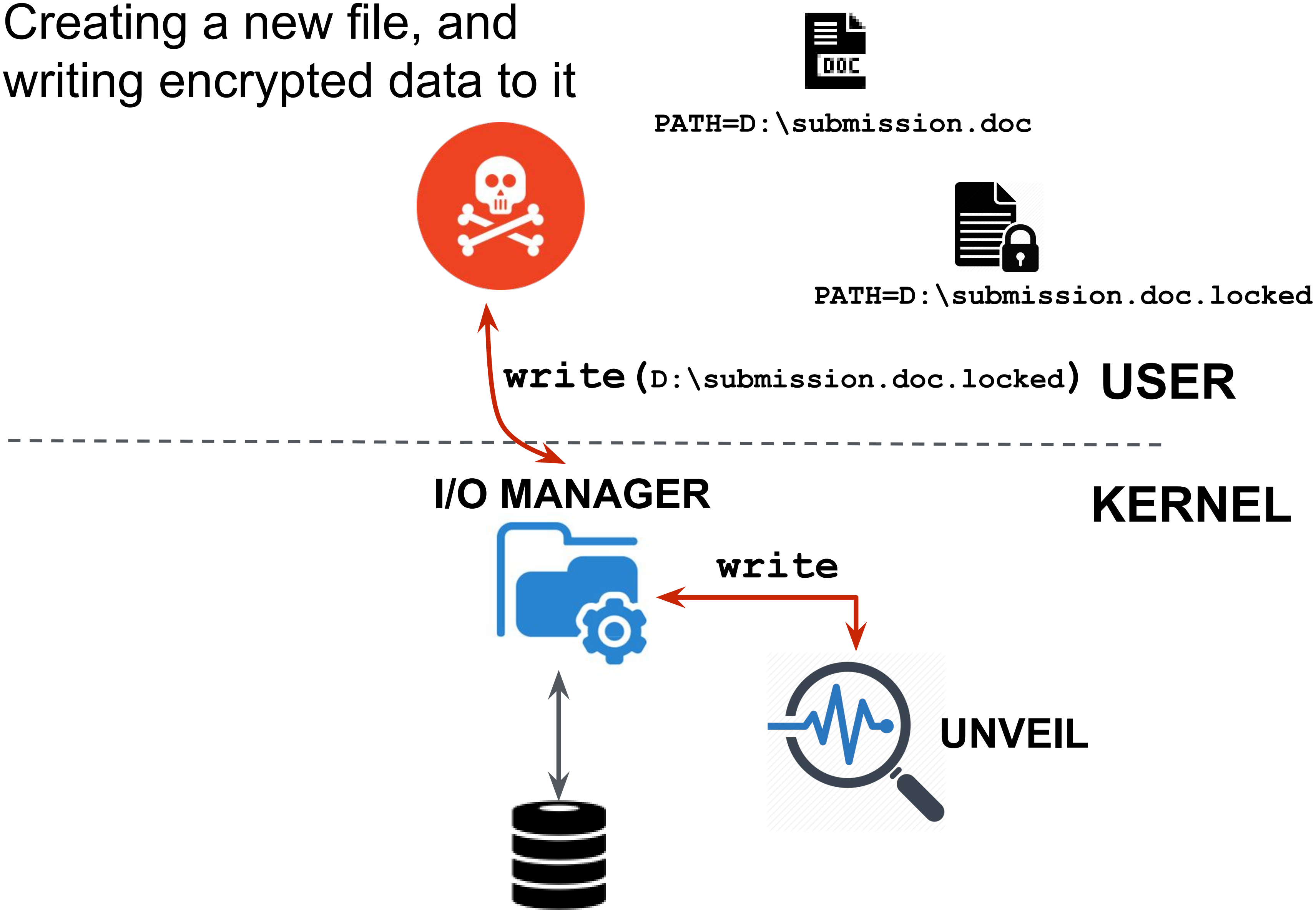
USER

KERNEL

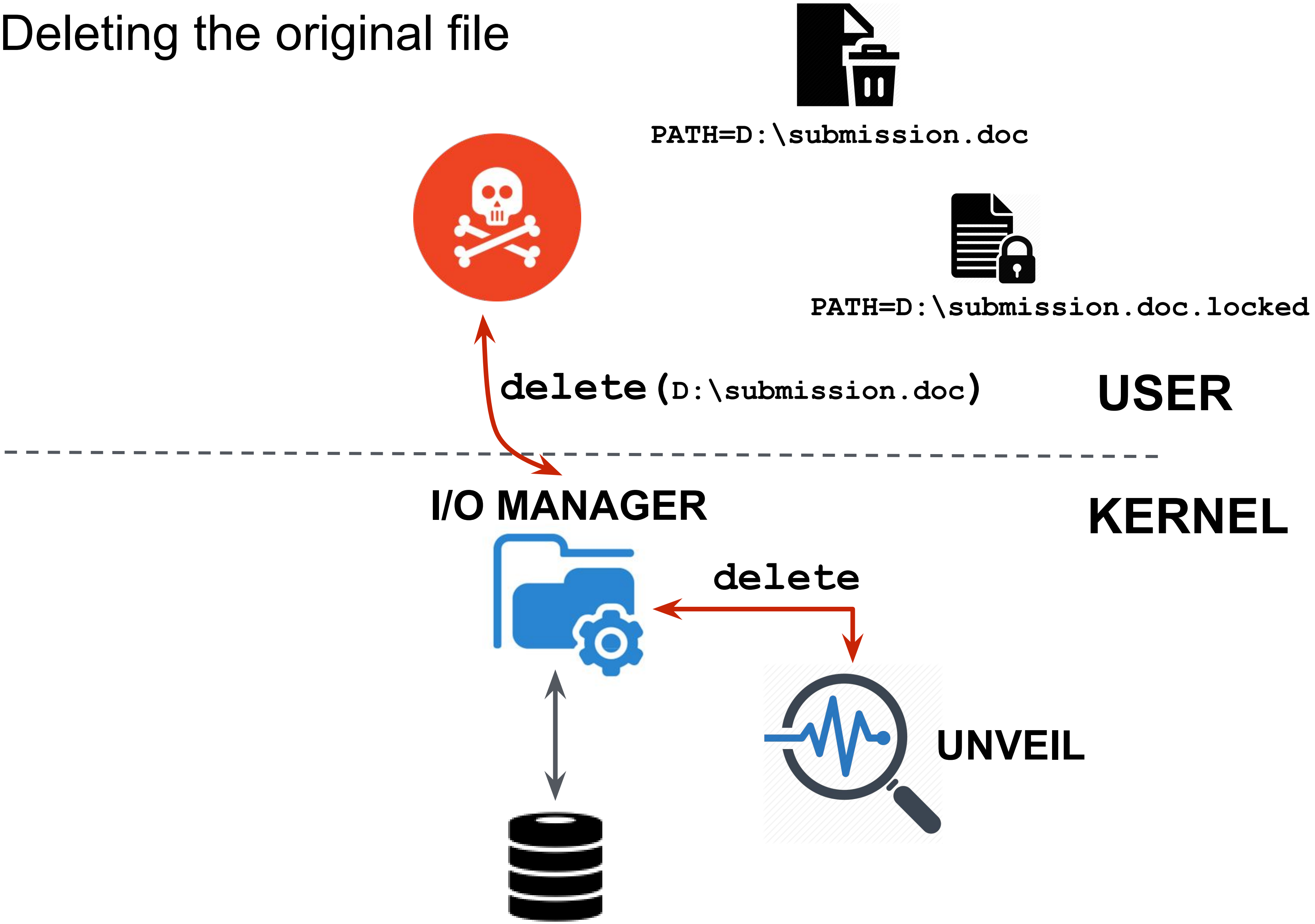
I/O MANAGER

UNVEIL

❷ Creating a new file, and writing encrypted data to it


DOC
PATH=D:\submission.doc
PATH=D:\submission.doc.locked
write(D:\submission.doc.locked)
USER
I/O MANAGER
KERNEL
write
UNVEIL

❸ Deleting the original file



PATH=D:\submission.doc

PATH=D:\submission.doc.locked

delete(D:\submission.doc)

USER

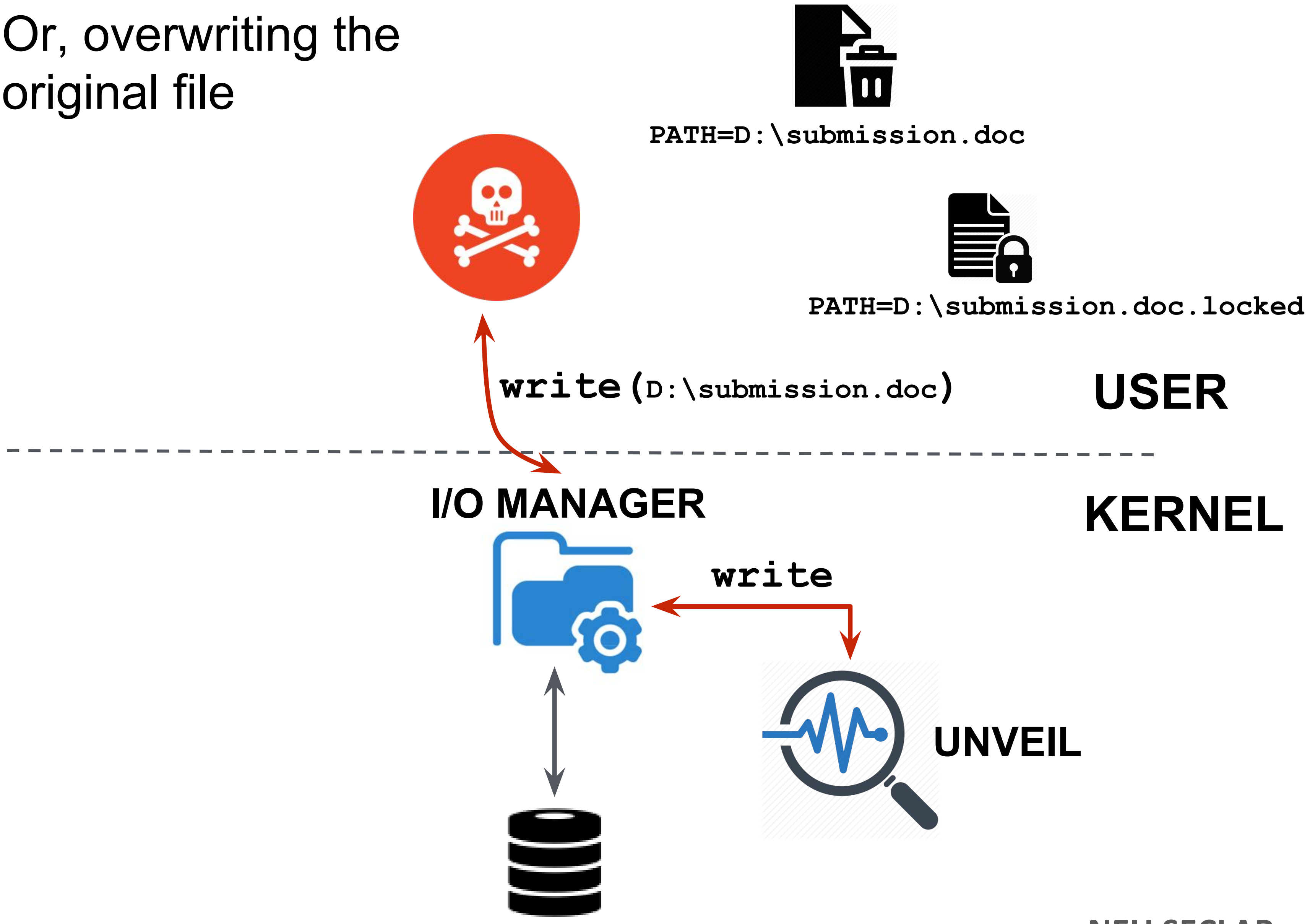
KERNEL

I/O MANAGER

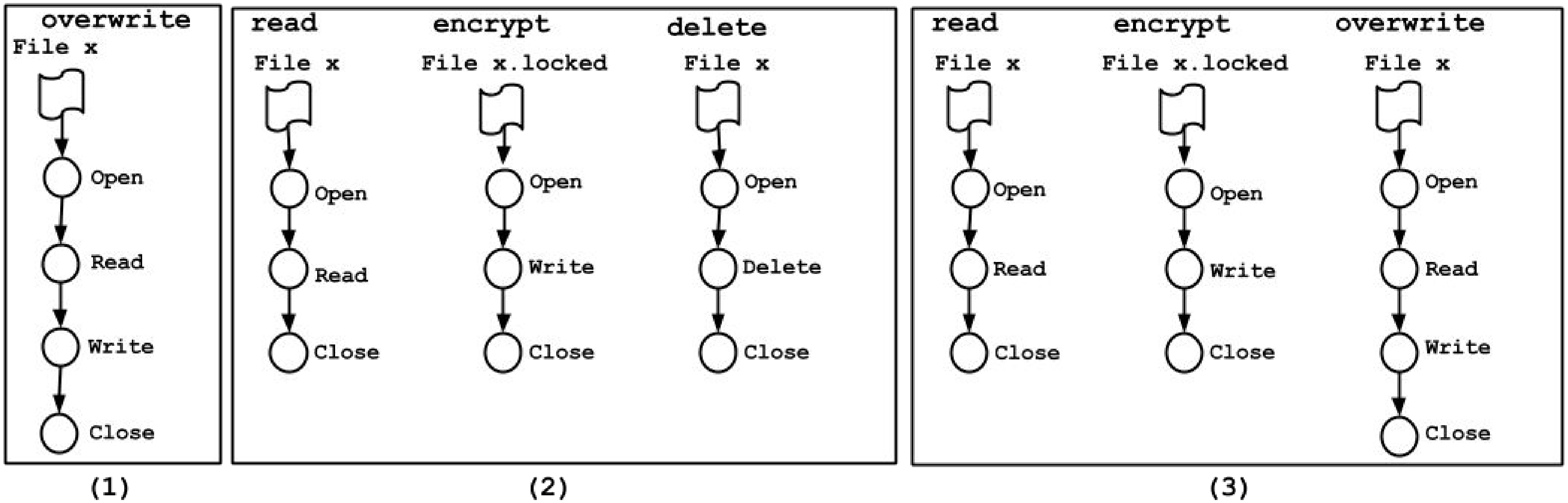
delete

UNVEIL

3 Or, overwriting the original file



Extracting I/O Access Sequences

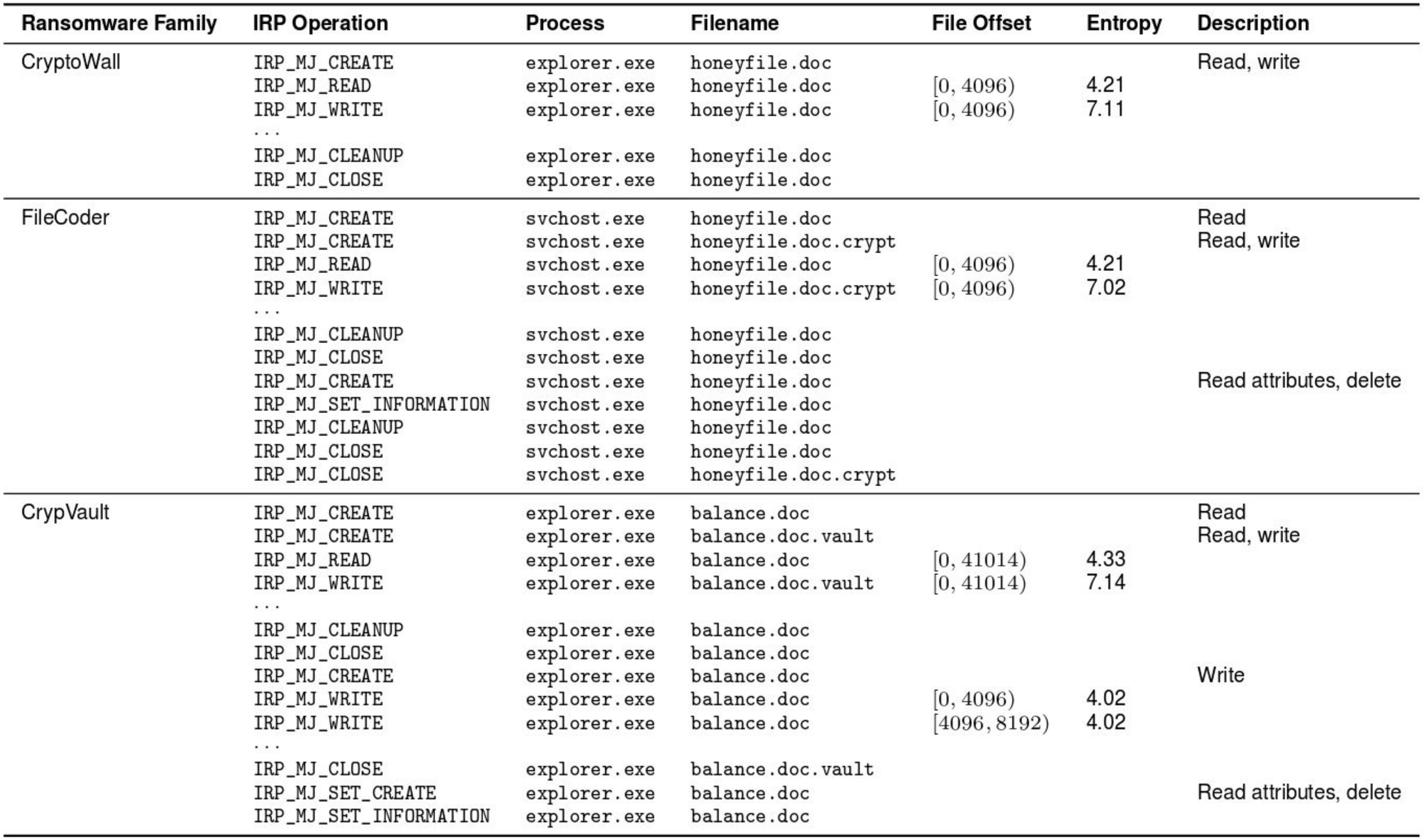


(1) Overwrites the users' file with an encrypted version

(2) reads, encrypts and deletes files without wiping them from storage

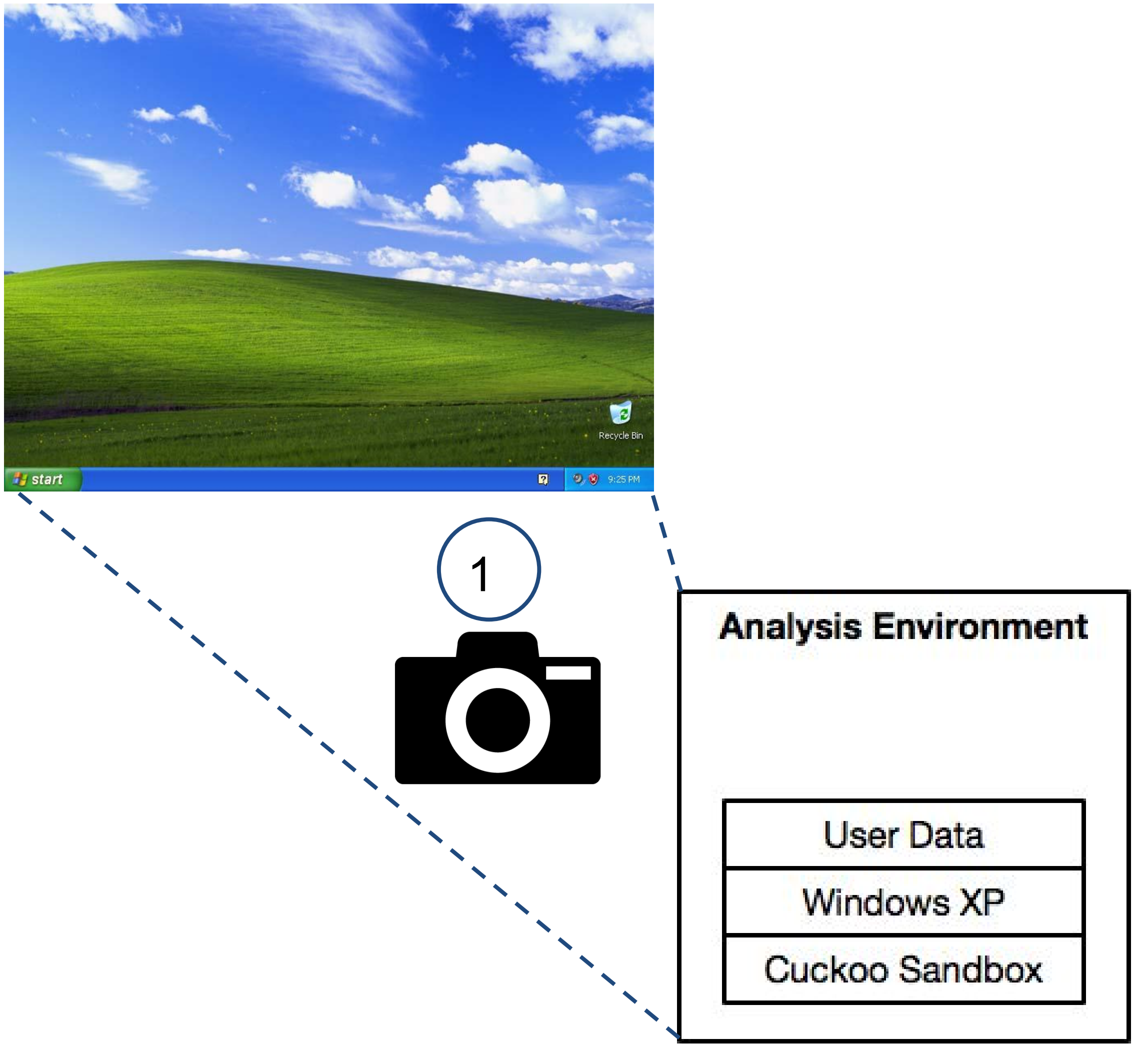
(3) reads, creates a new encrypted version, and securely deletes
the original files

IO Access Sequences in Multiple Ransomware Families



Ransomware Family	IRP Operation	Process	Filename	File Offset	Entropy	Description
CryptoWall	IRP_MJ_CREATE	explorer.exe	honeyfile.doc			Read, write
	IRP_MJ_READ	explorer.exe	honeyfile.doc	$[0, 4096)$	4.21	
	IRP_MJ_WRITE	explorer.exe	honeyfile.doc	$[0, 4096)$	7.11	
	...					
	IRP_MJ_CLEANUP	explorer.exe	honeyfile.doc			
	IRP_MJ_CLOSE	explorer.exe	honeyfile.doc			
FileCoder	IRP_MJ_CREATE	svchost.exe	honeyfile.doc			Read
	IRP_MJ_CREATE	svchost.exe	honeyfile.doc.crypt			Read, write
	IRP_MJ_READ	svchost.exe	honeyfile.doc	$[0, 4096)$	4.21	
	IRP_MJ_WRITE	svchost.exe	honeyfile.doc.crypt	$[0, 4096)$	7.02	
	...					
	IRP_MJ_CLEANUP	svchost.exe	honeyfile.doc			
	IRP_MJ_CLOSE	svchost.exe	honeyfile.doc			
	IRP_MJ_CREATE	svchost.exe	honeyfile.doc			Read attributes, delete
	IRP_MJ_SET_INFORMATION	svchost.exe	honeyfile.doc			
	IRP_MJ_CLEANUP	svchost.exe	honeyfile.doc			
	IRP_MJ_CLOSE	svchost.exe	honeyfile.doc			
	IRP_MJ_CLOSE	svchost.exe	honeyfile.doc.crypt			
CrypVault	IRP_MJ_CREATE	explorer.exe	balance.doc			Read
	IRP_MJ_CREATE	explorer.exe	balance.doc.vault			Read, write
	IRP_MJ_READ	explorer.exe	balance.doc	$[0, 41014)$	4.33	
	IRP_MJ_WRITE	explorer.exe	balance.doc.vault	$[0, 41014)$	7.14	
	...					
	IRP_MJ_CLEANUP	explorer.exe	balance.doc			
	IRP_MJ_CLOSE	explorer.exe	balance.doc			
	IRP_MJ_CREATE	explorer.exe	balance.doc			Write
	IRP_MJ_WRITE	explorer.exe	balance.doc	$[0, 4096)$	4.02	
	IRP_MJ_WRITE	explorer.exe	balance.doc	$[4096, 8192)$	4.02	
	...					
	IRP_MJ_CLOSE	explorer.exe	balance.doc.vault			
	IRP_MJ_SET_CREATE	explorer.exe	balance.doc			Read attributes, delete
	IRP_MJ_SET_INFORMATION	explorer.exe	balance.doc			

Desktop Locker Ransomware



1

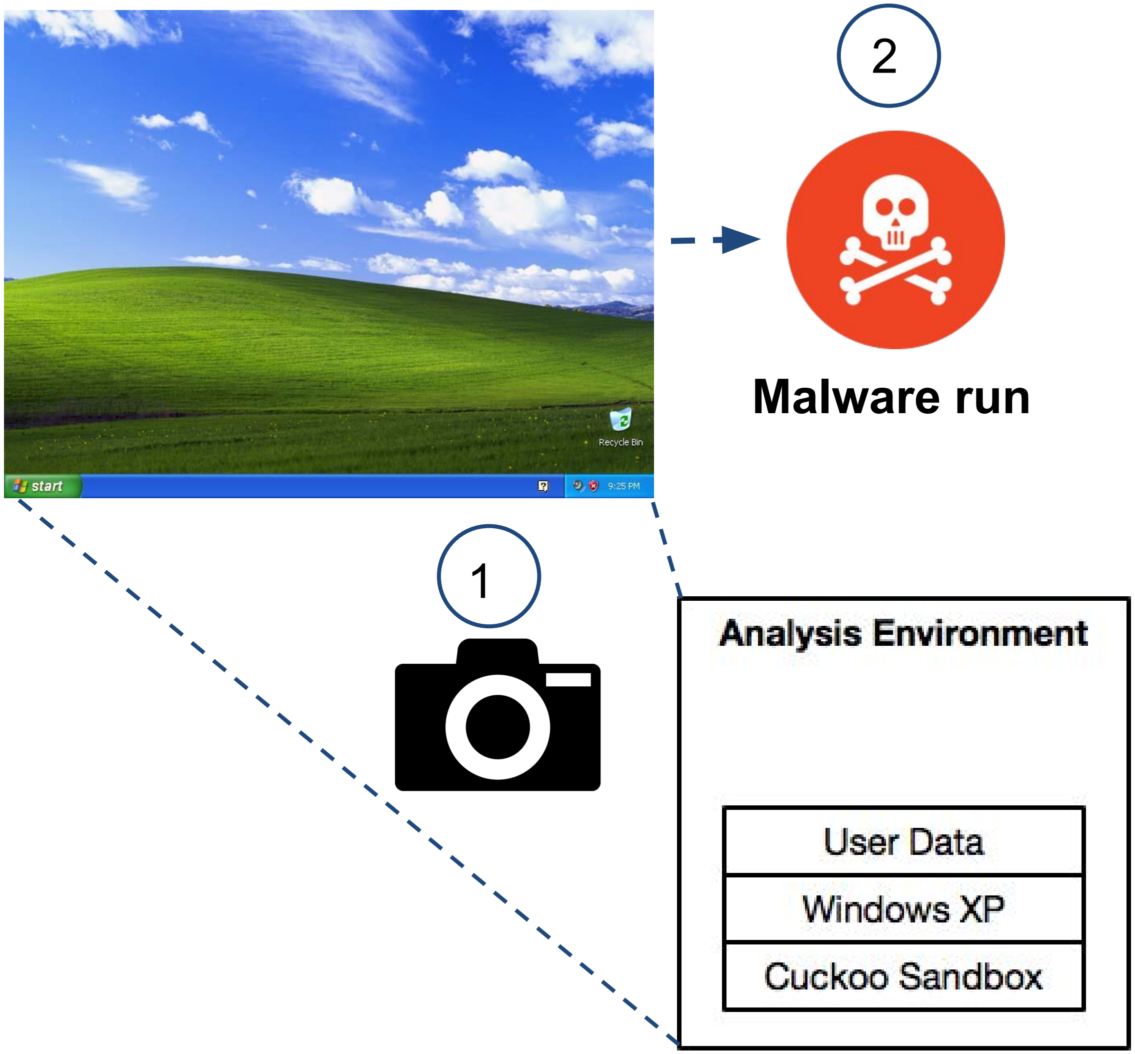
Analysis Environment

User Data

Windows XP

Cuckoo Sandbox

Desktop Locker Ransomware



2

Malware run

1

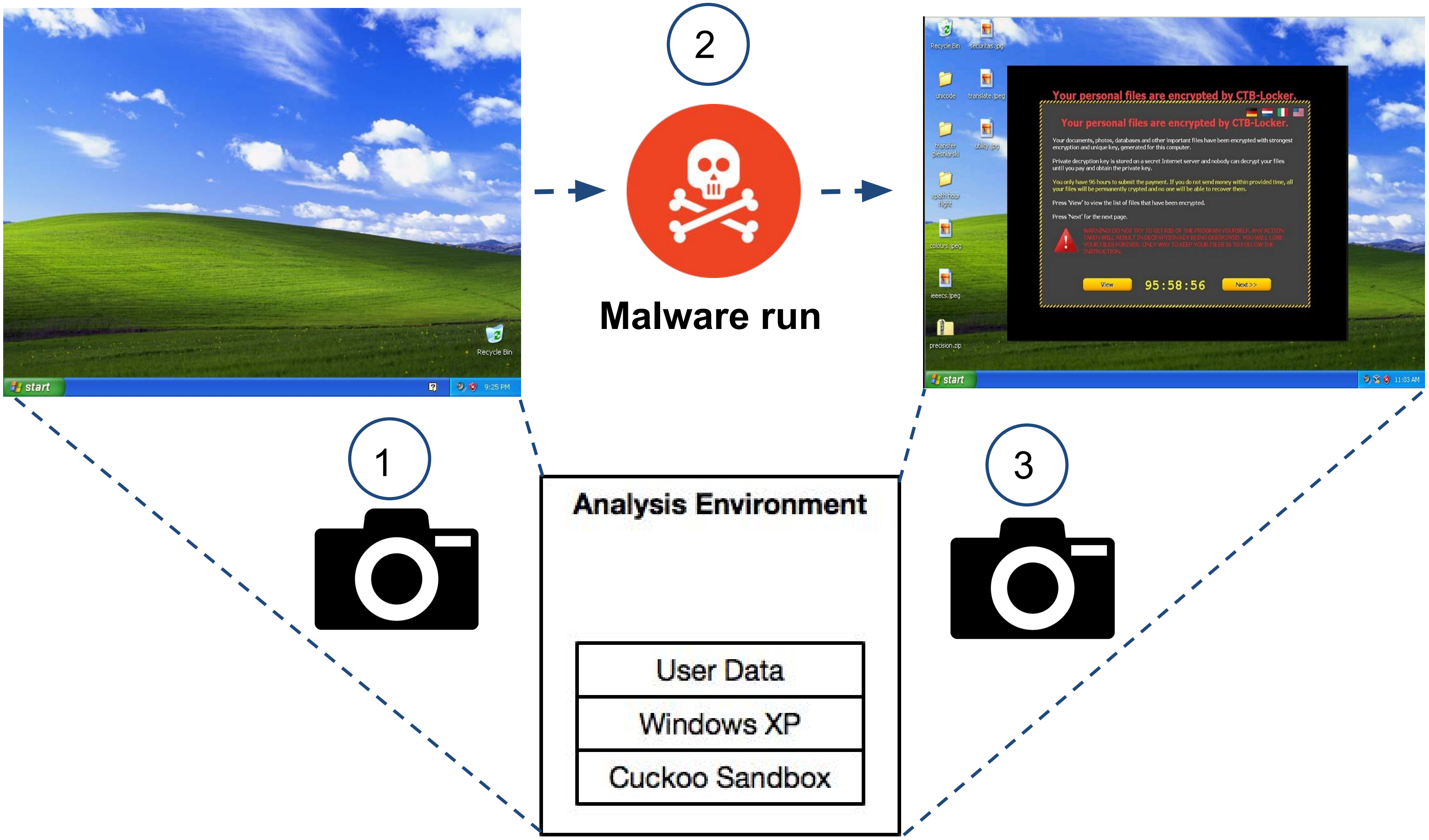
Analysis Environment

User Data

Windows XP

Cuckoo Sandbox

Desktop Locker Ransomware



Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

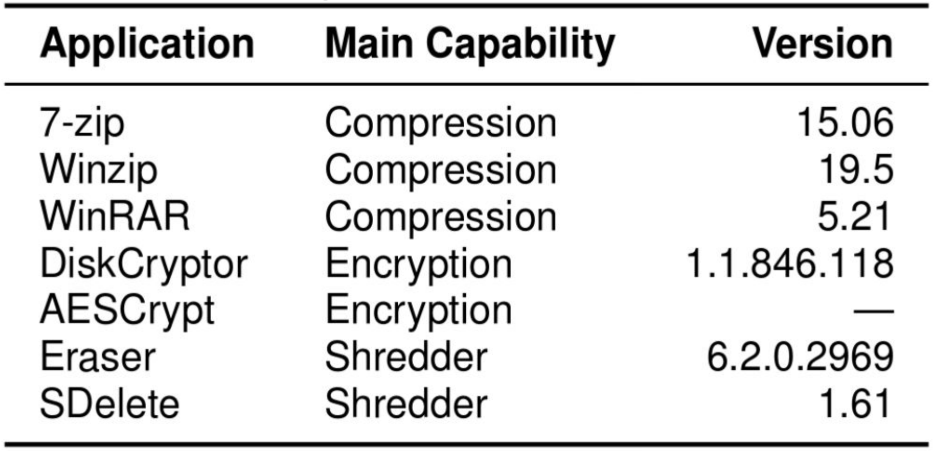
95:58:56

Evaluation

1) Detecting known ransomware samples

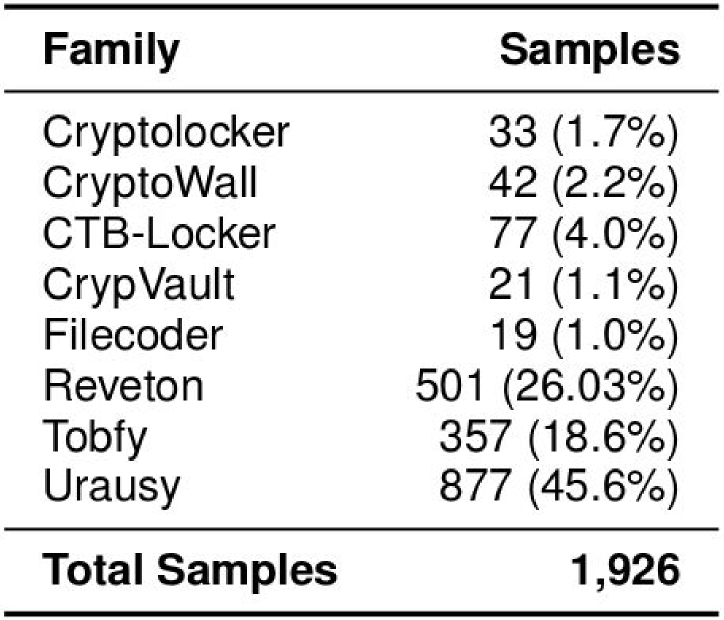
a) Collecting ~3500 ransomware from public repo, Anubis, two security companies.
b) 149 benign executables including ransomware-like behavior
c) 348 malware samples from 36 malware families

Benign Applications



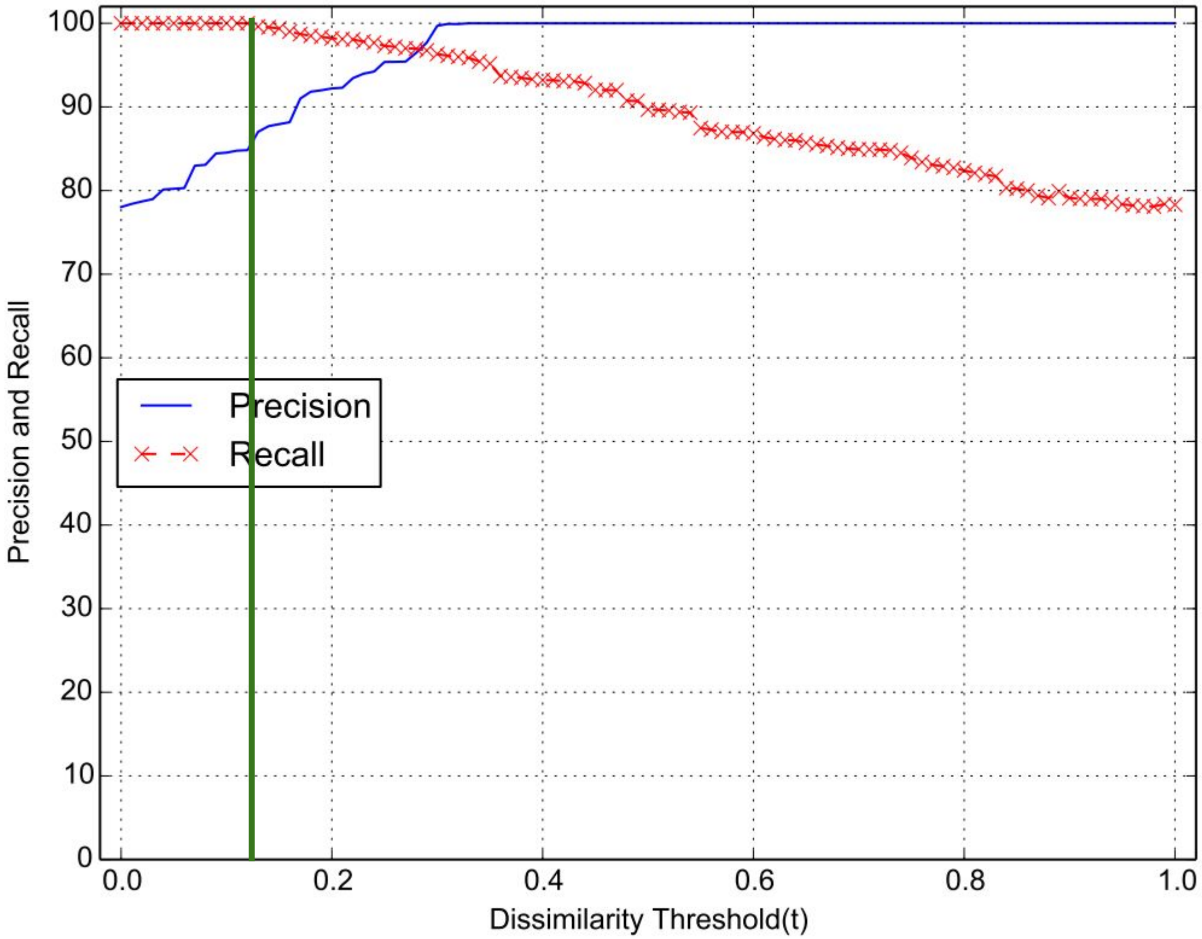
Application	Main Capability	Version
7-zip	Compression	15.06
Winzip	Compression	19.5
WinRAR	Compression	5.21
DiskCryptor	Encryption	1.1.846.118
AESCrypt	Encryption	—
Eraser	Shredder	6.2.0.2969
SDelete	Shredder	1.61

Ransomware Families

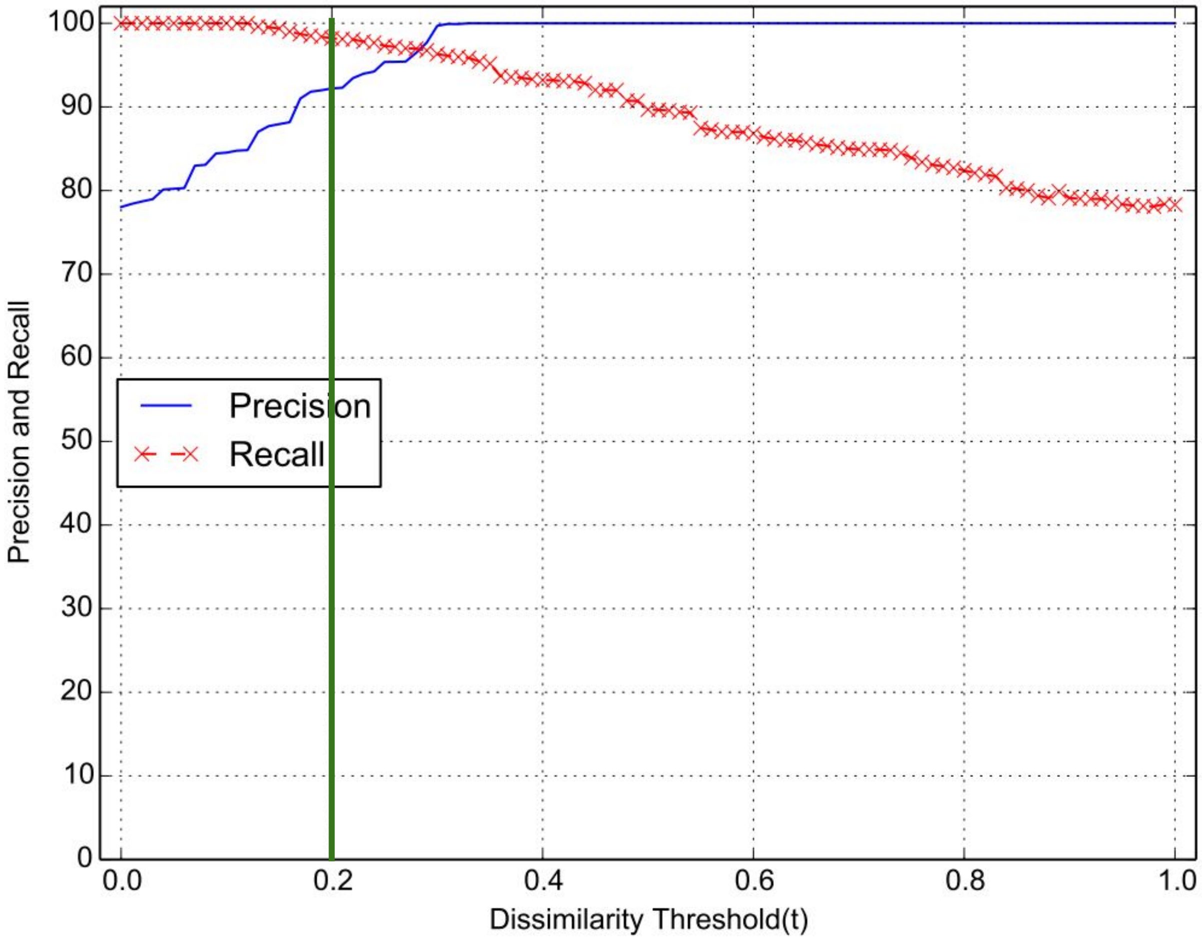


Family	Samples
Cryptolocker	33 (1.7%)
CryptoWall	42 (2.2%)
CTB-Locker	77 (4.0%)
CrypVault	21 (1.1%)
Filecoder	19 (1.0%)
Reveton	501 (26.03%)
Tobfy	357 (18.6%)
Urausy	877 (45.6%)
Total Samples	**1,926**

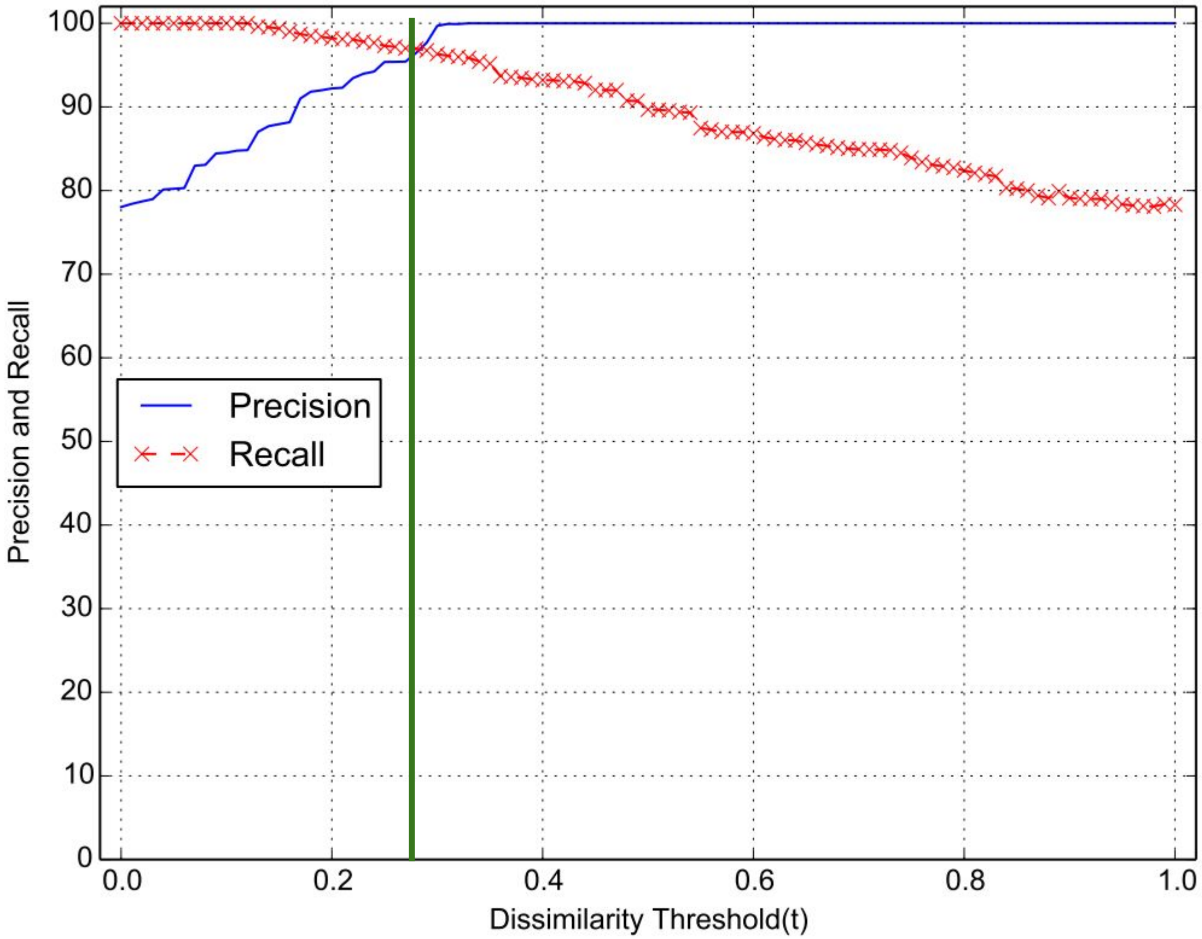
Finding the best threshold value



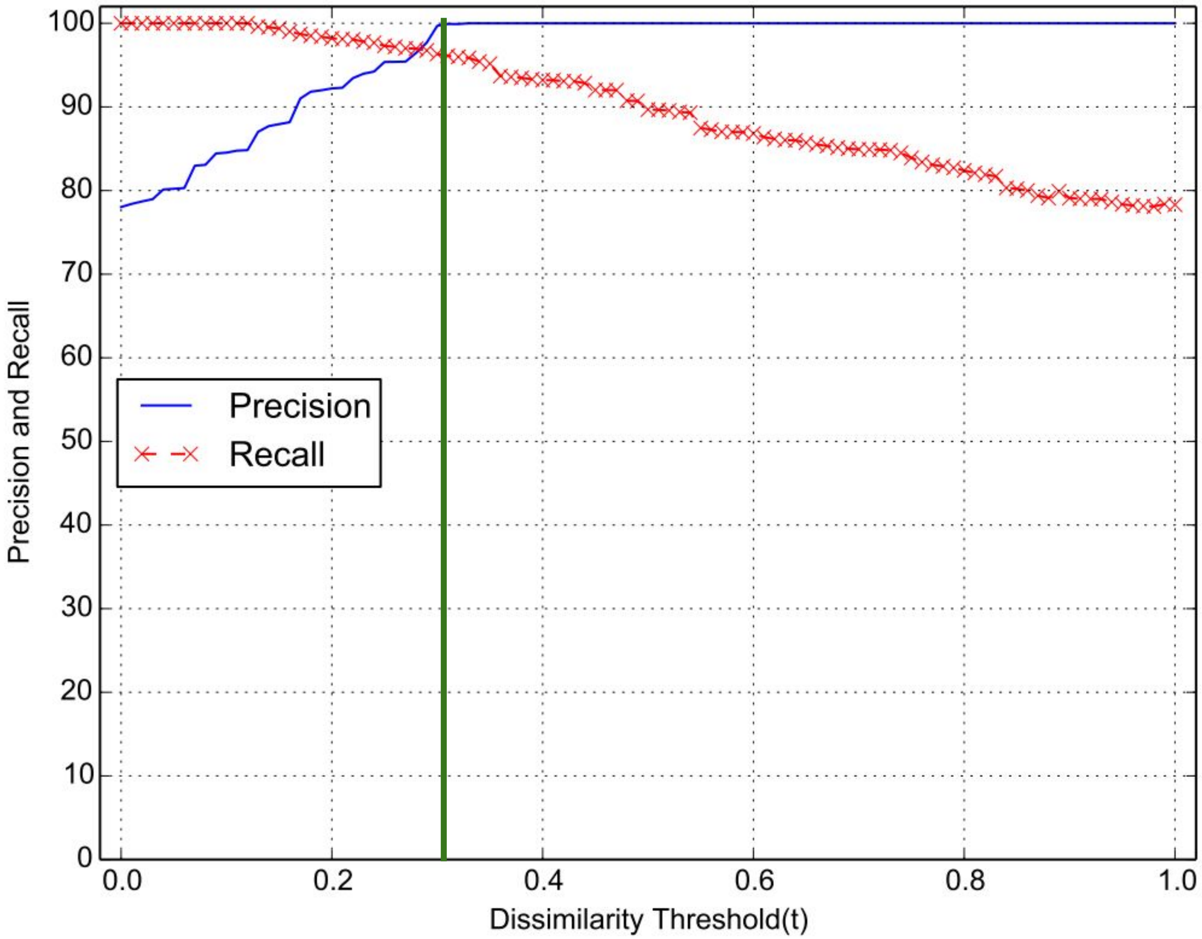
Detecting known ransomware samples



Detecting known ransomware samples



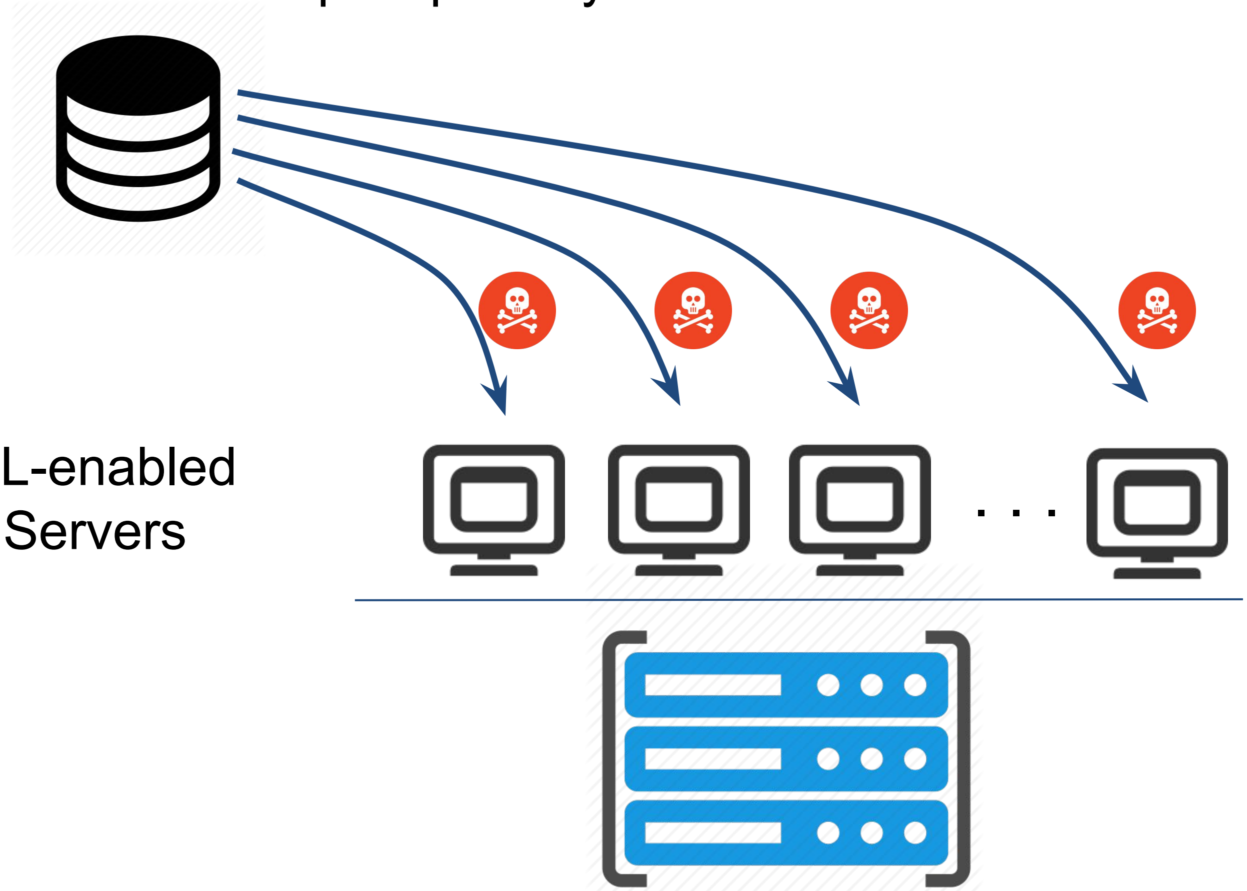
Detecting known ransomware samples



The threshold value *t* = 0.32 gives the highest recall with 100% precision

Large-Scale Evaluation

~ 1200 malware samples per day

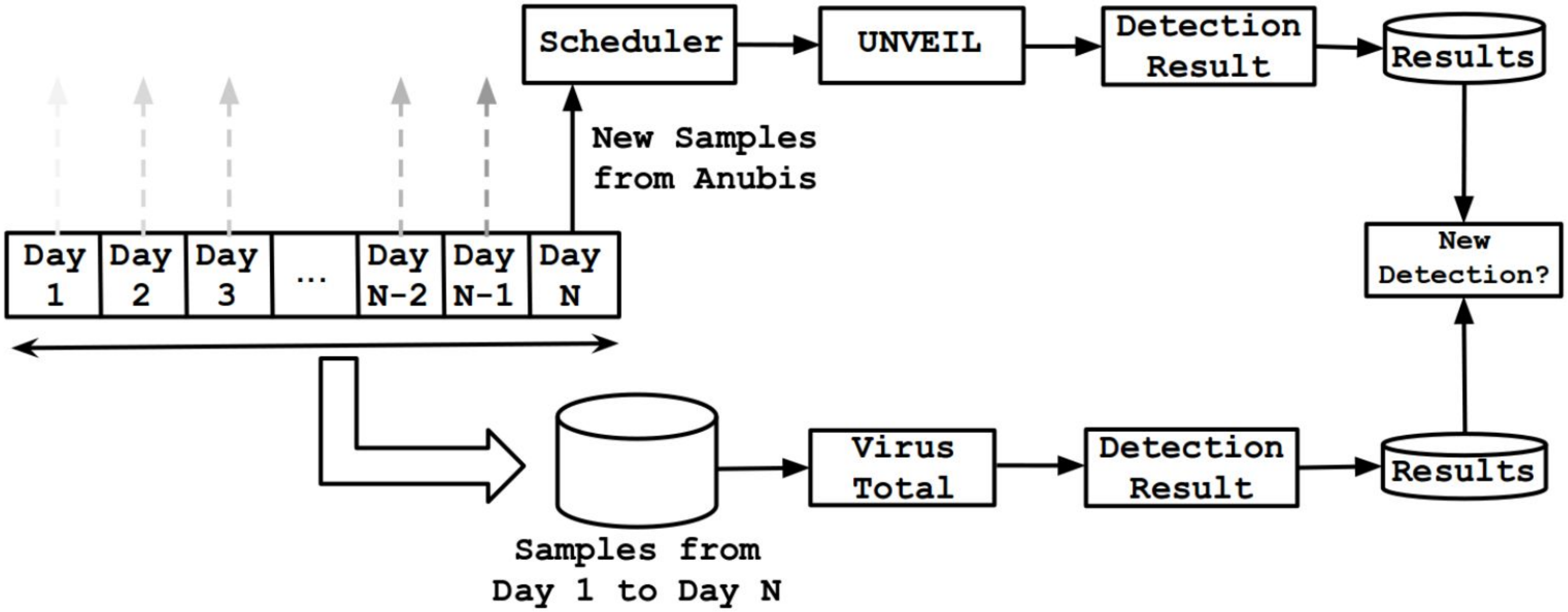


56 UNVEIL-enabled
VMs on 8 Servers

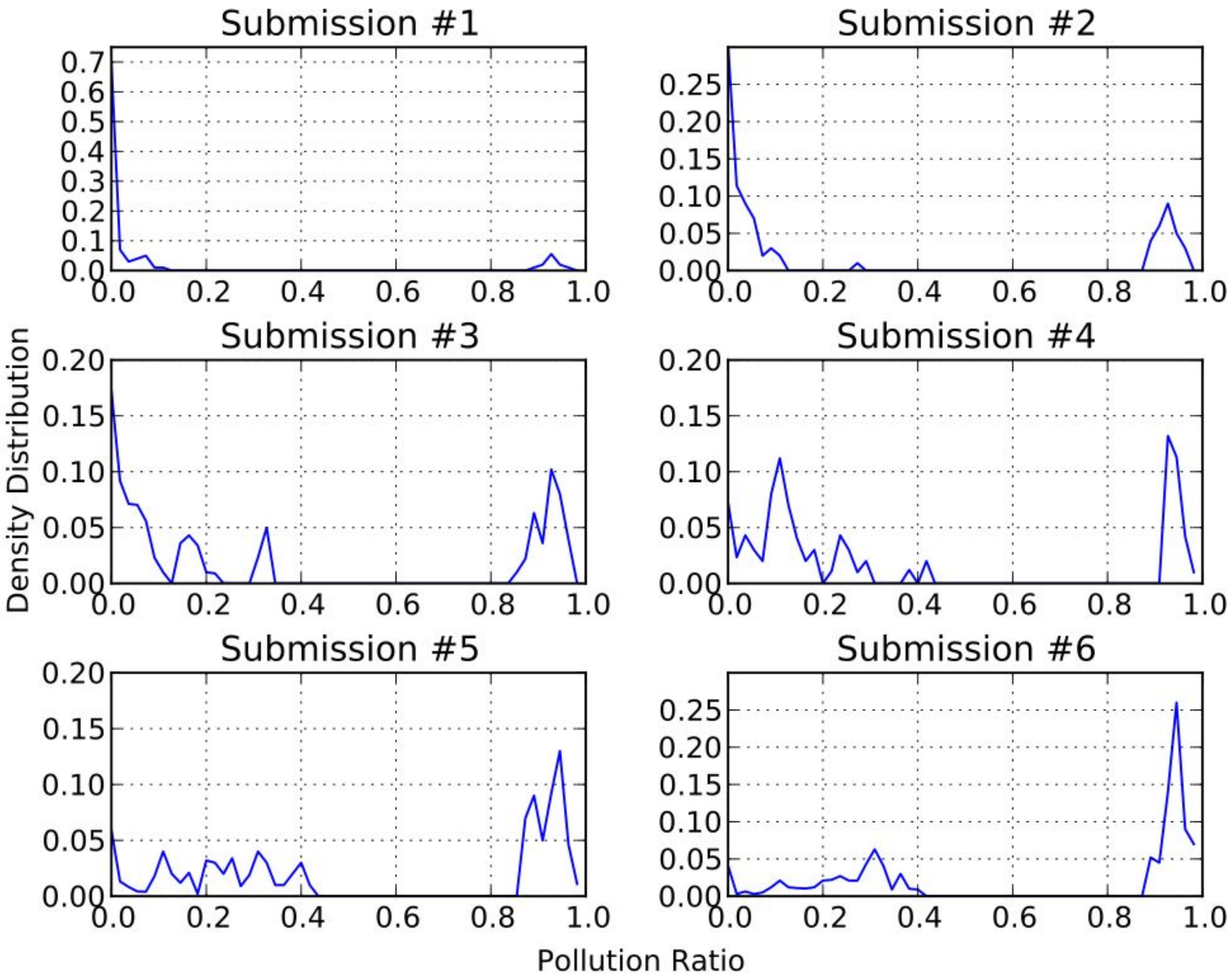
Ganeti Cluster
(4 compute nodes)

Large-Scale Evaluation

- We used the same similarity threshold (t = 0.32) for the large scale experiment.
- 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.

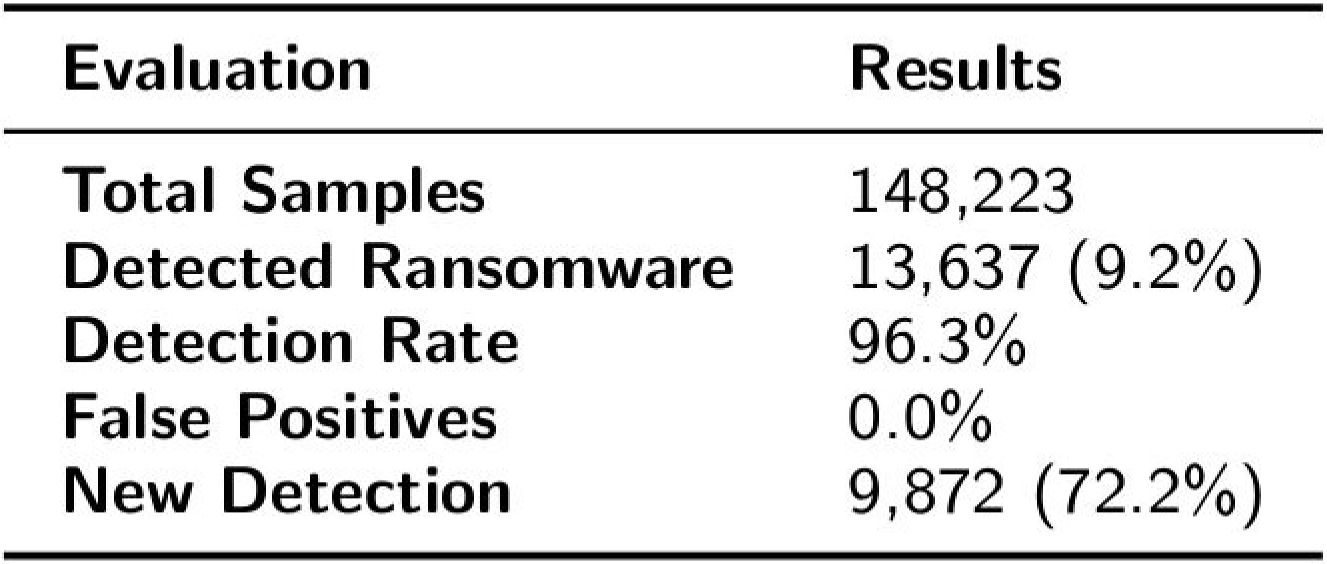


Cross-checking with VirusTotal



- The results are concentrated either towards small or very large detection ratios.
- A sample is either detected by a relatively small number, or almost all of the scanners.

Detection Results

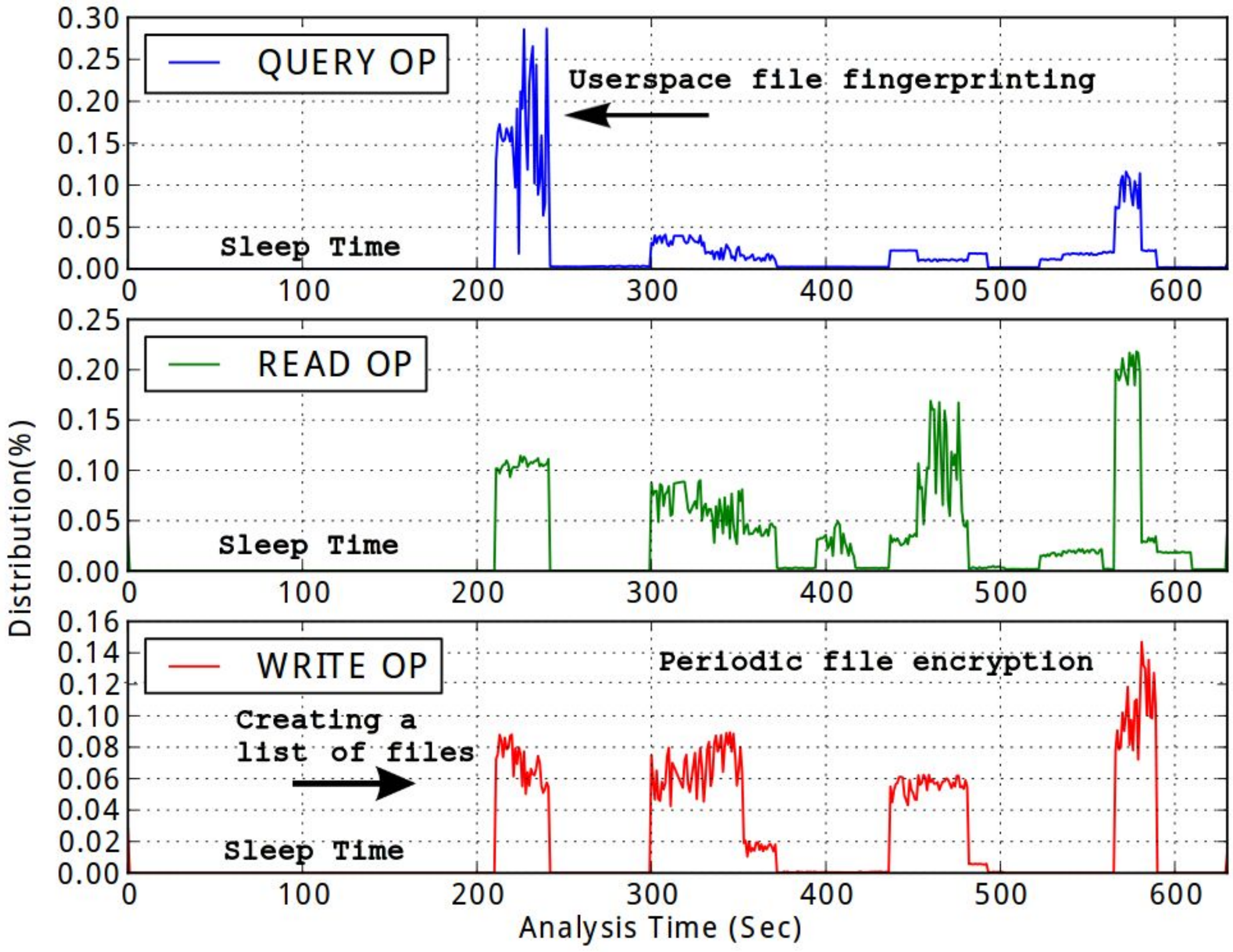


Evaluation	Results
Total Samples	148,223
Detected Ransomware	13,637 (9.2%)
Detection Rate	96.3%
False Positives	0.0%
New Detection	9,872 (72.2%)

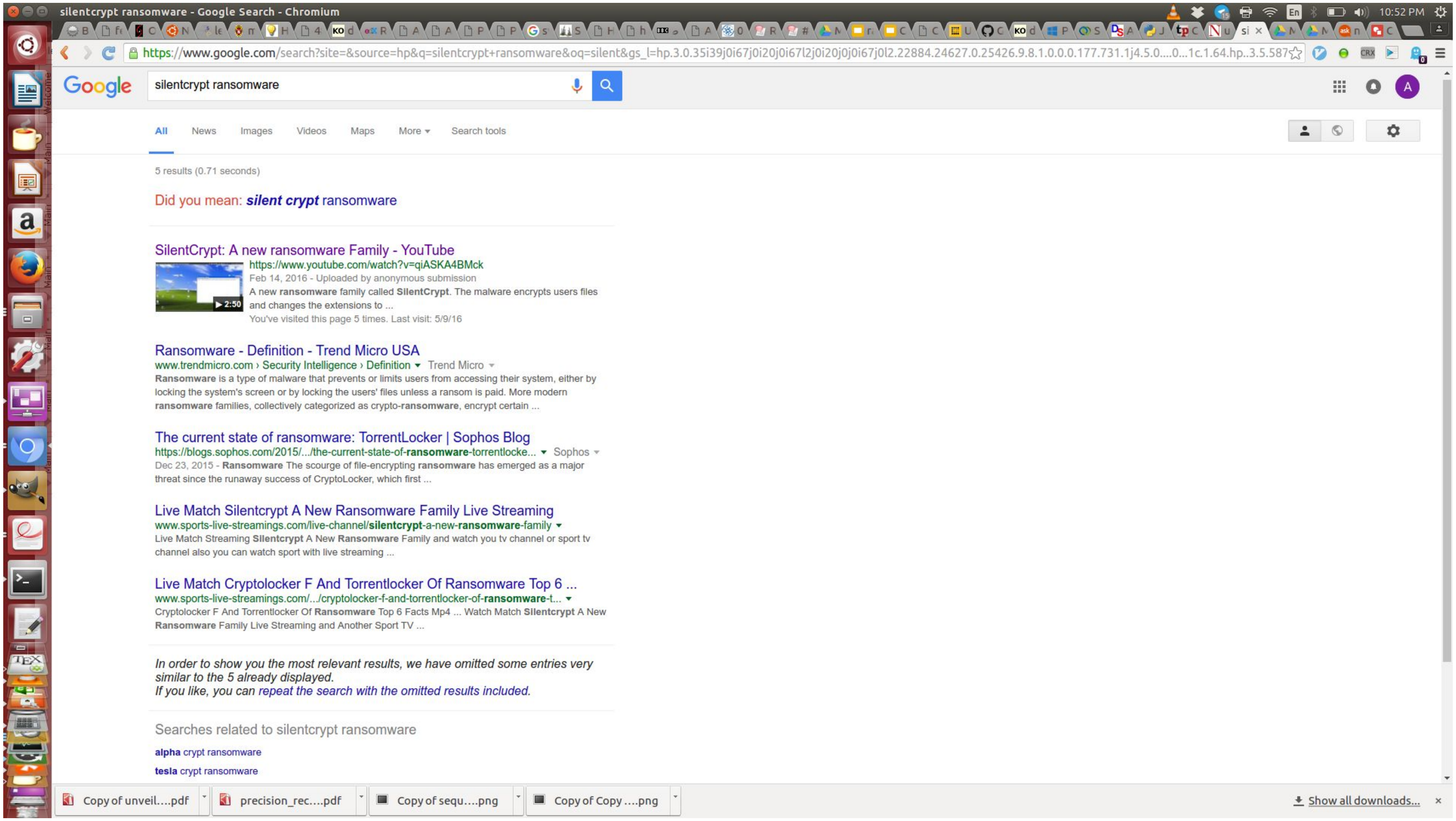
Detection: New Ransomware Family

- During our experiments, we discovered a new malware family
  - We call it “SilentCrypt”
  - After we reported it, others started detecting it as well
  - We were not able to find any information about this family online
  - The ransomware first checks for private files of a user, contacts the C&C server, and starts the attack based on the answer

Detection: New Ransomware Family



Detection: New Ransomware Family



silentcrypt ransomware - Google Search - Chromium
10:52 PM
https://www.google.com/search?site=&source=hp&q=silentcrypt+ransomware&oq=silent&gs_l=hp.3.0.35i39j0i67j0i20j0i67l2j0i20j0j0i67j0l2.22884.24627.0.25426.9.8.1.0.0.0.177.731.1j4.5.0....0...1c.1.64.hp..3.5.587
silentcrypt ransomware
All
News
Images
Videos
Maps
More ▾
Search tools
Copy of unveil....pdf
precision_rec....pdf
Copy of sequ....png
Copy of Copy ....png
Show all downloads...

5 results (0.71 seconds)

Did you mean: ***silent crypt*** ransomware

SilentCrypt: A new ransomware Family - YouTube
https://www.youtube.com/watch?v=qiASKA4BMck
Feb 14, 2016 - Uploaded by anonymous submission
A new **ransomware** family called **SilentCrypt**. The malware encrypts users files and changes the extensions to ...
You've visited this page 5 times. Last visit: 5/9/16

Ransomware - Definition - Trend Micro USA
www.trendmicro.com › Security Intelligence › Definition ▾ Trend Micro ▾
Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern **ransomware** families, collectively categorized as crypto-**ransomware**, encrypt certain ...

The current state of ransomware: TorrentLocker | Sophos Blog
https://blogs.sophos.com/2015/.../the-current-state-of-**ransomware**-torrentlocke... ▾ Sophos ▾
Dec 23, 2015 - **Ransomware** The scourge of file-encrypting **ransomware** has emerged as a major threat since the runaway success of CryptoLocker, which first ...

Live Match Silentcrypt A New Ransomware Family Live Streaming
www.sports-live-streamings.com/live-channel/**silentcrypt**-a-new-**ransomware**-family ▾
Live Match Streaming **Silentcrypt** A New **Ransomware** Family and watch you tv channel or sport tv channel also you can watch sport with live streaming ...

Live Match Cryptolocker F And Torrentlocker Of Ransomware Top 6 ...
www.sports-live-streamings.com/.../cryptolocker-f-and-torrentlocker-of-**ransomware**-t... ▾
Cryptolocker F And Torrentlocker Of **Ransomware** Top 6 Facts Mp4 ... Watch Match **Silentcrypt** A New **Ransomware** Family Live Streaming and Another Sport TV ...

In order to show you the most relevant results, we have omitted some entries very similar to the 5 already displayed.
If you like, you can repeat the search with the omitted results included.

Searches related to silentcrypt ransomware

alpha crypt ransomware

tesla crypt ransomware

Conclusion

- Defending against ransomware is not as *complex* as it is reported.
- Current analysis systems are not still ready to detect evasive ransomware attacks.
- UNVEIL is the introduction of concrete techniques to detect ransomware.
- SilentCrypt shows that AV industry is not still ready to detect *evasive* samples.

.

Thank You