



Northeastern University

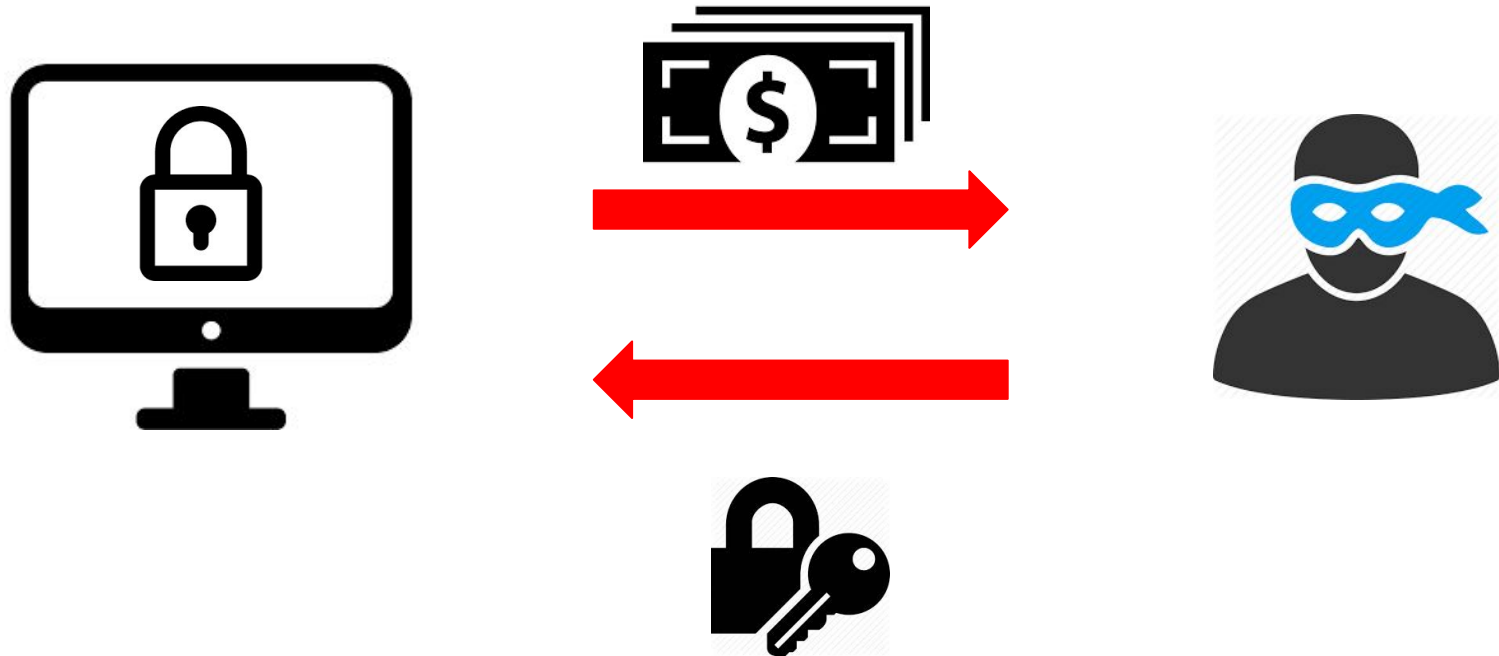
International Secure Systems Lab

A Large-Scale, Automated Approach to Detecting Ransomware

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

What is a ransomware attack?

- 1 Paying the ransom fee
- 2 Receiving the decryption key



A Typical Ransom Note



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.**

View **95:59:29** **Next >>**

Attacks on Hospitals

Privacy & Security

Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money

Kansas Heart Hospital declined to pay the second ransom, saying that would not be wise. Security experts, meanwhile, are warning that ransomware attacks will only get worse.

By [Bill Siwicki](#) | May 23, 2016 | 02:58 PM

SHARE



Kansas Heart Hospital was the victim of a ransomware attack and after it paid the first one, attackers boldly demanded a second ransom to decrypt data.

Kansas Heart Hospital president Greg Duick, MD told local media that patient

University Pays \$16,000 to Stop Ransomware Attack JUNE 8, 2016

Michael Phelps Picks Up His 20th Gold in 200-Meter Butterfly 10:37 PM EDT

USA's Katie Ledecky Clinches the Gold Again in 200m Freestyle 10:17 PM EDT

Two Years After Ferguson, What Has Changed? 8:00 PM EDT

Wild and Weird, Drone Racing May be the Sport of the Future 7:57 PM EDT

Elon Musk Says SolarCity Will Sell a Roof Integrated With Solar Panels 7:56 PM EDT

Disney Hedges Its Bets on TV With BAMTech Stake and ESPN Streaming 7:26 PM EDT

TECH CHANGING FACE OF SECURITY

University Pays \$16,000 to Stop Ransomware Attack

by Jeff John Roberts @jeffjohnroberts JUNE 8, 2016, 1:29 PM EDT



Police pay ransom after cyberterror attack on network

Story

Comments (1)

Print  Font Size:  



**Thomas Murphy, Daniel Sawicki
and Lt. Scott Keddie**

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.

New estimates from the FBI show that the costs from so-called ransomware have reached an all-time high.

“Cyber-criminals collected \$209 million in the first three months of 2016 by extorting businesses and institutions to unlock computer servers.”

– CNN Interview with FBI, April 2016

How to defend against ransomware attacks?

- Educating end-users
 - Have a reliable *backup* policy
 - Avoid risky online behavior
- 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 online behavior
- 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

Threat Model

- Ransomware can employ any techniques to attack
 - Inject code into benign processes
 - Perform encrypted communication
 - Leverage arbitrary cryptosystems
- We assume that OS kernel, and underlying software and hardware stack are free of malicious code.
- Unveil detects ransomware during *dynamic analysis phase*, and *not* at end-user machines.
 - Complements current dynamic analysis systems
 - A cloud-based malware analysis service, sample sharing

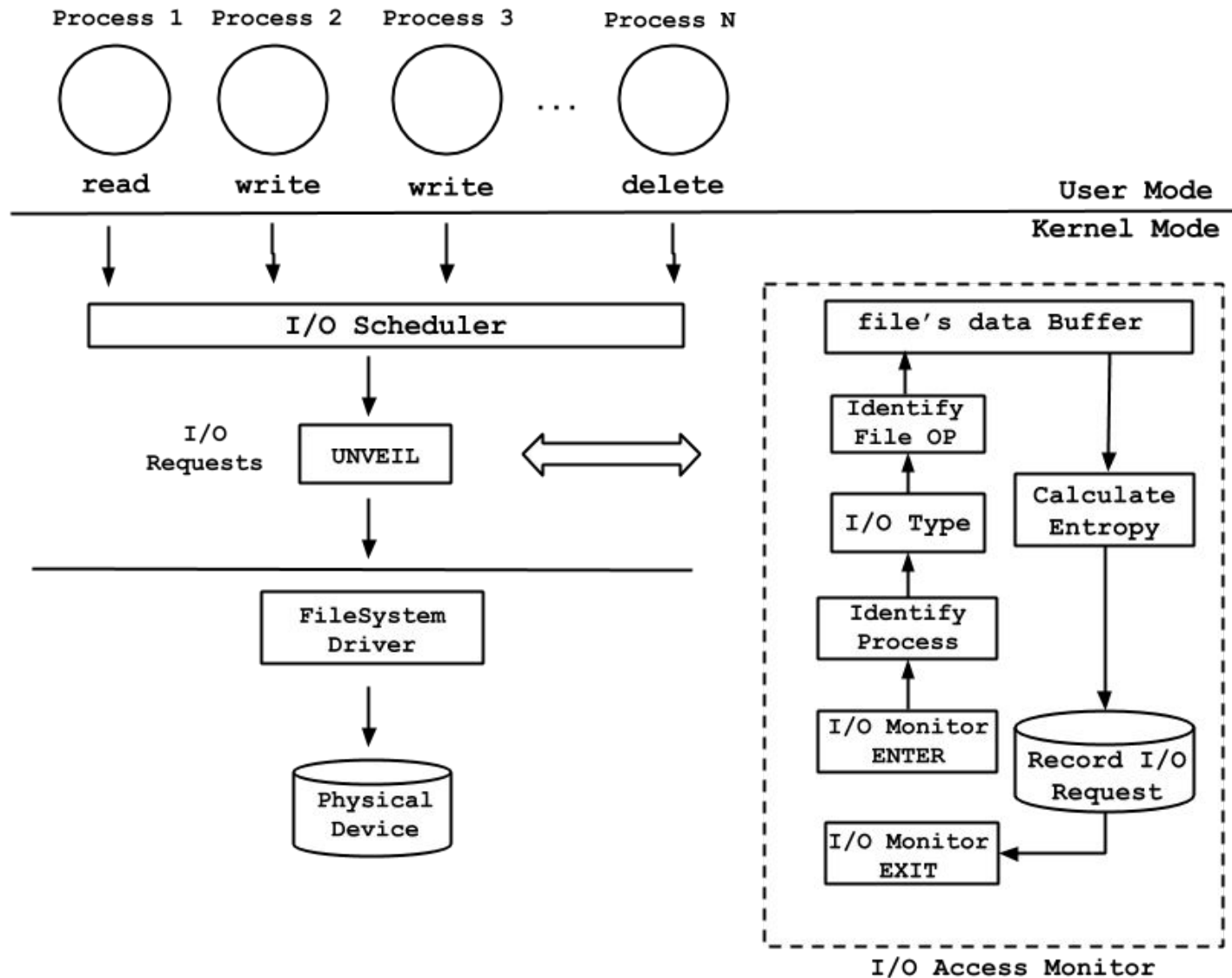
But, how can we detect a ransomware sample?

Achilles' Heel of Ransomware

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

UNVEIL: An Early Warning Dynamic Detection System for Ransomware

UNVEIL's Architecture



Approach

- Detecting Cryptographic Ransomware:
 - Generating a fake (and attractive) user environment
 - Finding a reliable method for monitoring filesystem activity

Why do we generate fake user environments?

- Making the analysis environment more realistic
- Protecting the analysis system from some user environment fingerprinting
 - A static user environment can be *easily* detected by a malware

Approach

- Detecting Cryptographic Ransomware:
 - Generating a fake (and attractive) user environment
 - Finding a reliable method for monitoring filesystem activity

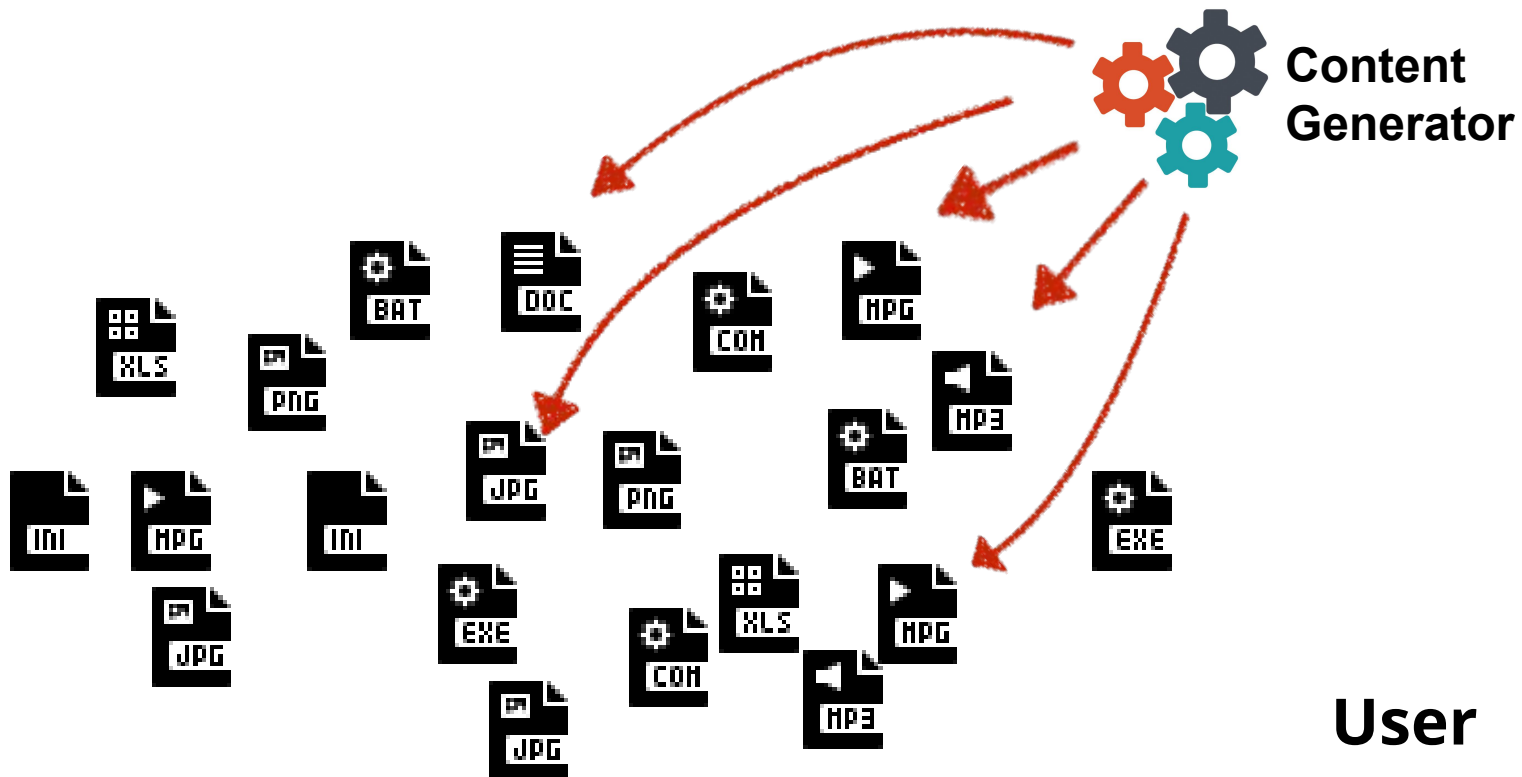
Why do we generate fake user environments?

- Making the analysis environment more realistic
- Protecting the analysis system from bare-user environment fingerprinting
 - A static user environment can be *easily* detected by a malware

How do we generate fake user environments?

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



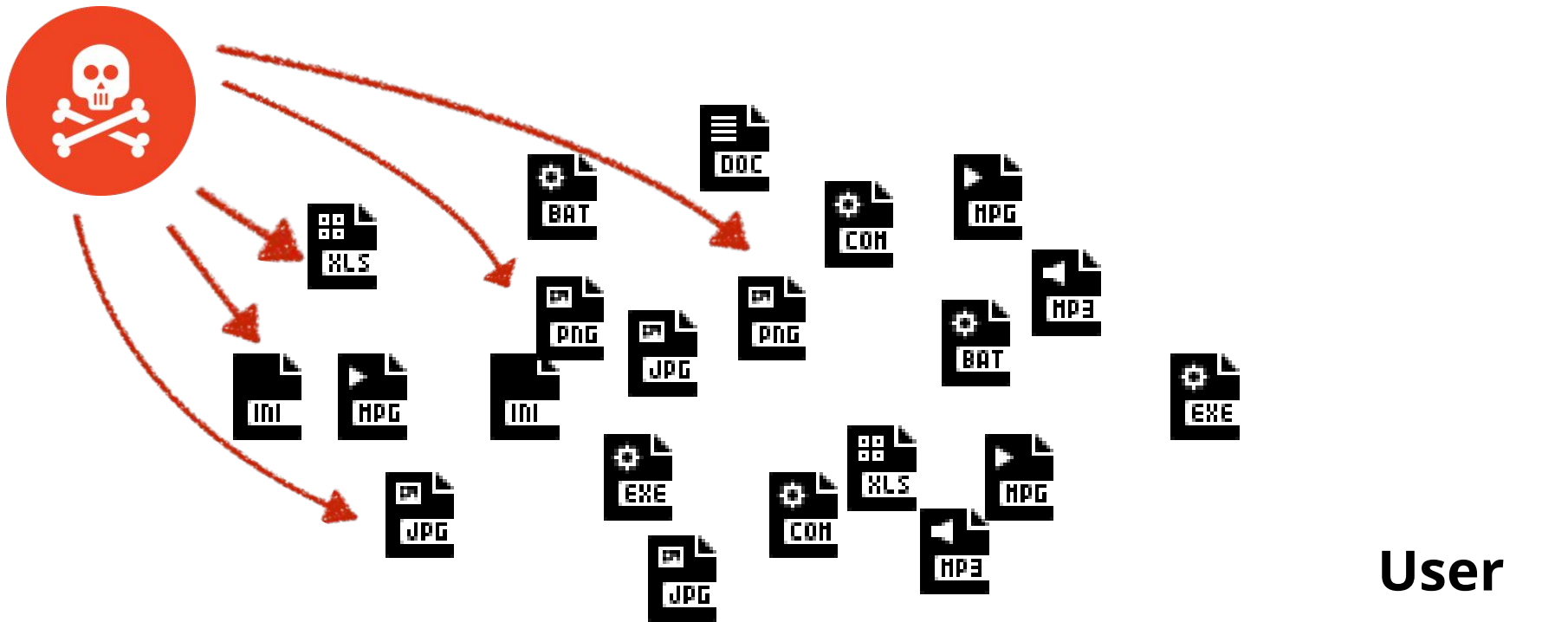
I/O MANAGER



UNVEIL

User

Kernel



I/O MANAGER

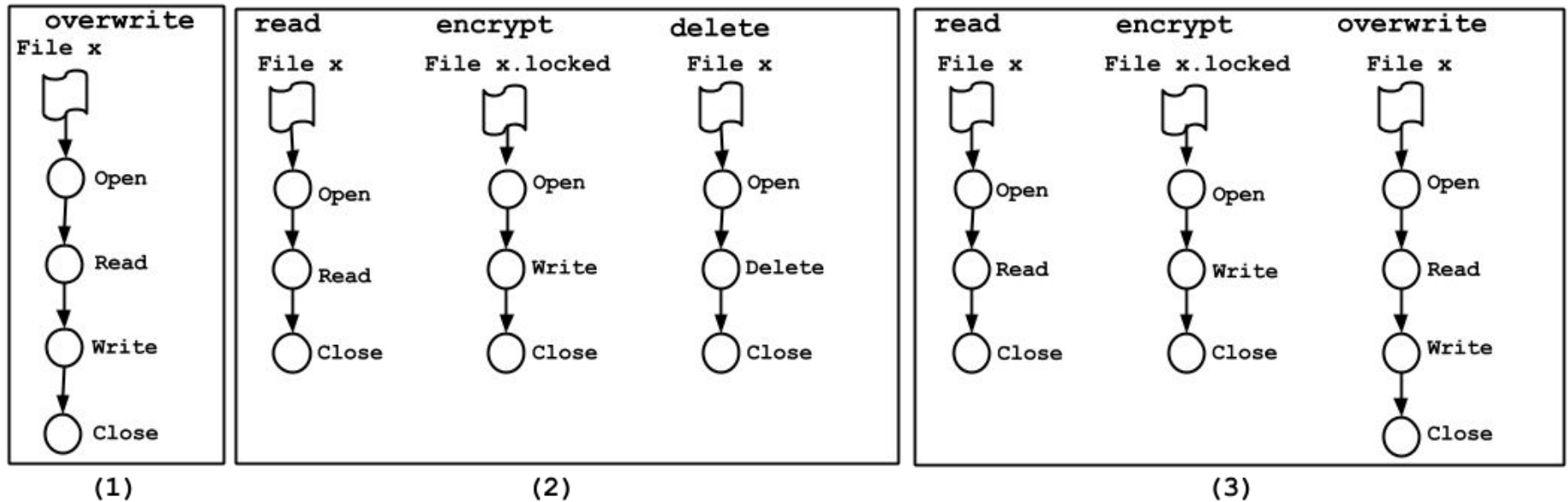
Kernel



UNVEIL

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

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

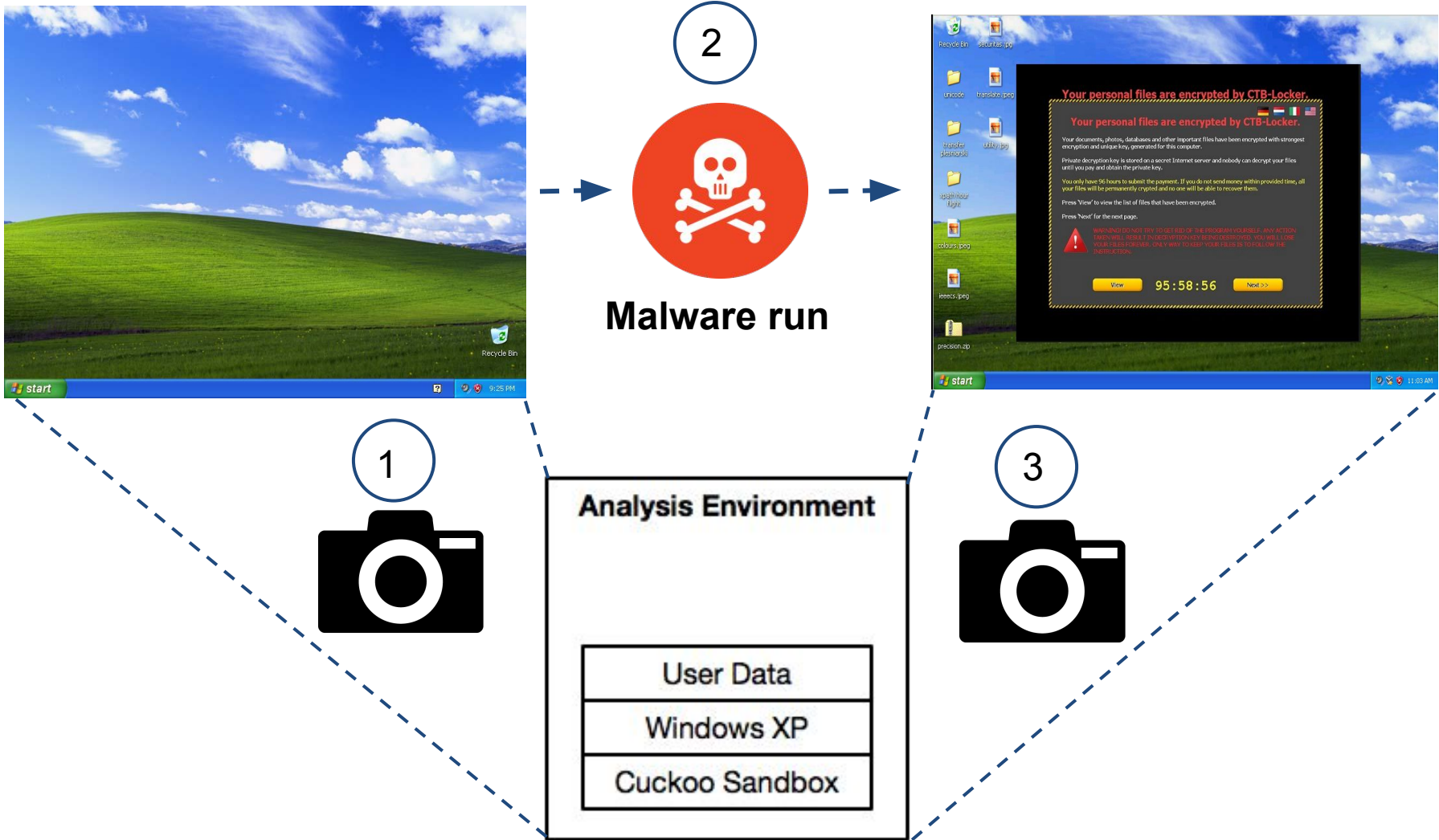
IO Access Sequences in Multiple Ransomware Families

Ransomware Family	IRP Operation	Process	Filename	File Offset	Entropy	Description
CryptoWall	IRP_MJ_CREATE	explorer.exe	honeyfile.doc			Read, write
	Read → IRP_MJ_READ	explorer.exe	honeyfile.doc	[0, 4096)	4.21	
	Write → 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
	New File → IRP_MJ_CREATE	svchost.exe	honeyfile.doc.crypt			Read, write
	IRP_MJ_READ	svchost.exe	honeyfile.doc	[0, 4096)	4.21	
	Encrypted → 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			
	Deleting the Original File → 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
	New File → IRP_MJ_CREATE	explorer.exe	balance.doc.vault			Read, write
	IRP_MJ_READ	explorer.exe	balance.doc	[0, 41014)	4.33	
	Encrypted → 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
	Secure → IRP_MJ_WRITE	explorer.exe	balance.doc	[0, 4096)	4.02	
	Deletion → 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				

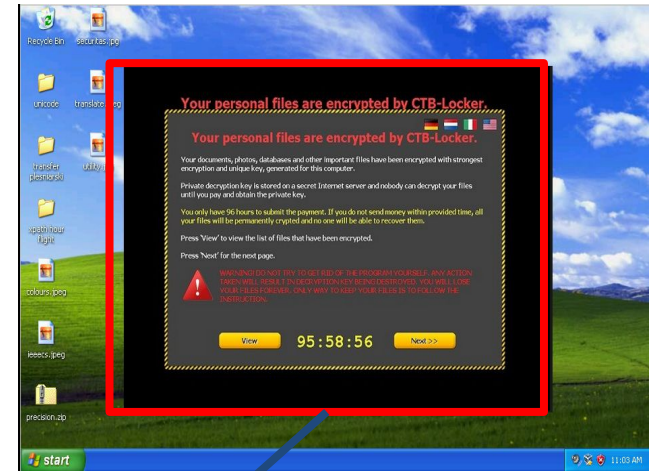
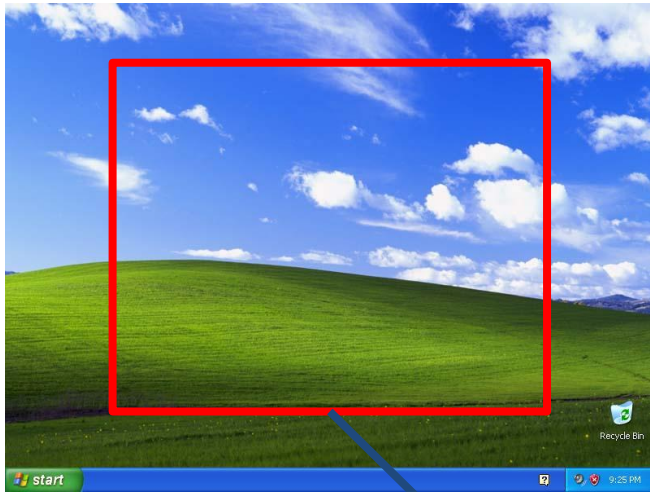
Iteration over files during a CryptoWall attack

File	Operation	Process	Entropy
midterm_paper.docx	IRP_MJ_CREATE	svchost.exe	—
midterm_paper.docx	IRP_MJ_READ	svchost.exe	4.01
midterm_paper.docx	IRP_MJ_WRITE	svchost.exe	7.28
...
midterm_paper.docx	IRP_MJ_CLEANUP	svchost.exe	—
midterm_paper.docx	IRP_MJ_CLOSE	svchost.exe	—
myweddingparty.mpeg	IRP_MJ_CREATE	svchost.exe	—
myweddingparty.mpeg	IRP_MJ_READ	svchost.exe	5.14
myweddingparty.mpeg	IRP_MJ_WRITE	svchost.exe	7.24
...
myweddingparty.mpeg	IRP_MJ_CLEANUP	svchost.exe	—
myweddingparty.mpeg	IRP_MJ_CLOSE	svchost.exe	—

Desktop Locker Ransomware



Desktop Locker Ransomware



Dissimilarity Score



Preparing the Analysis Environment

- UNVEIL is deployed on top of Cuckoo Sandbox
 - UNVEIL supports all versions of Windows platforms.
 - Our tool is deployed in Kernel.
 - Bypassing UNVEIL is not technically easy in user-mode.
- Finding active malware is not easy
 - We modified some parts of Cuckoo to make it more resilient to environmentally sensitive samples
 - e.g., fake response to some of the environment checks
 - Other anti-evasion measures to look more realistic
 - e.g., defining multiple NTFS drives, changing IP address range and MAC addresses

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

Dissimilarity score is different from family to family

Schweizerische Eidgenossenschaft
Confédération Suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police

Achtung!

Ein Vorgang illegaler Aktivitäten wurde erkannt.

Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Schweiz gesperrt! Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet [redacted] mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen.
Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt! Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Aktivitäten zu unterbinden.

Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von CHF 150 zu zahlen.
Die Zahlung ist innerhalb von 24 Stunden zu leisten. Sollte der Eingang der Zahlung in der vorgegebenen Zeit nicht erfolgen, so wird Ihre Festplatte unwiderruflich formatiert (gelöscht).

Die Zahlung per Paysafecard begleichen:
Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK)

Paysafecard via SMS auf dein Handy!

Mit der neuen SMS Funktion Kannst du schnell,
Spontan und bequem
Deine paysafecard kaufen!
Egal welcher Tarif – Egal welches Angebot – ob
Prepaid Handy oder
Handy mit Abo – Vertrag – paysafecard funktioniert
Auf allen Mobilfunkgeräten,
De SMS empfangen oder versenden können.

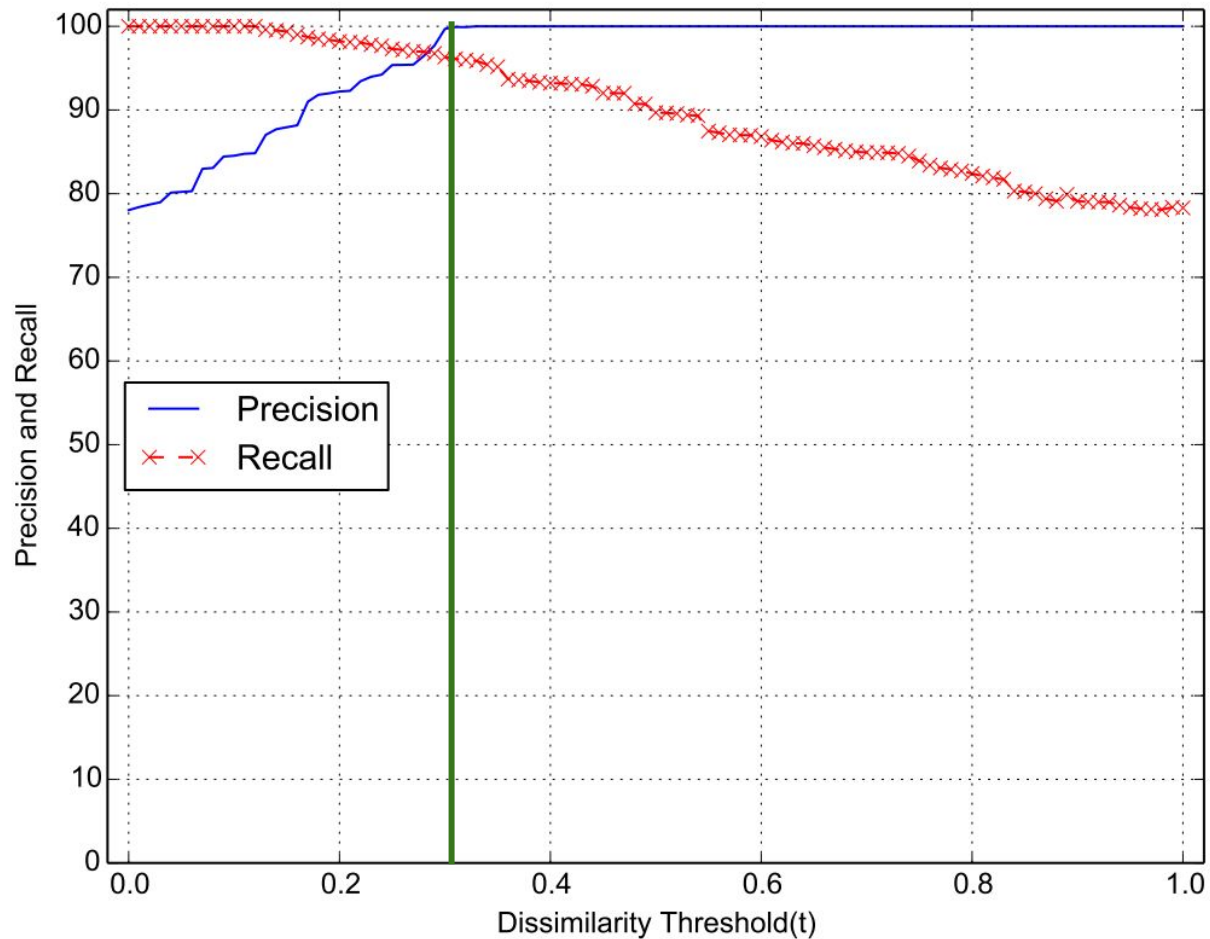


PostFinance
DIE POST



paysafecard
pay cash. pay safe.

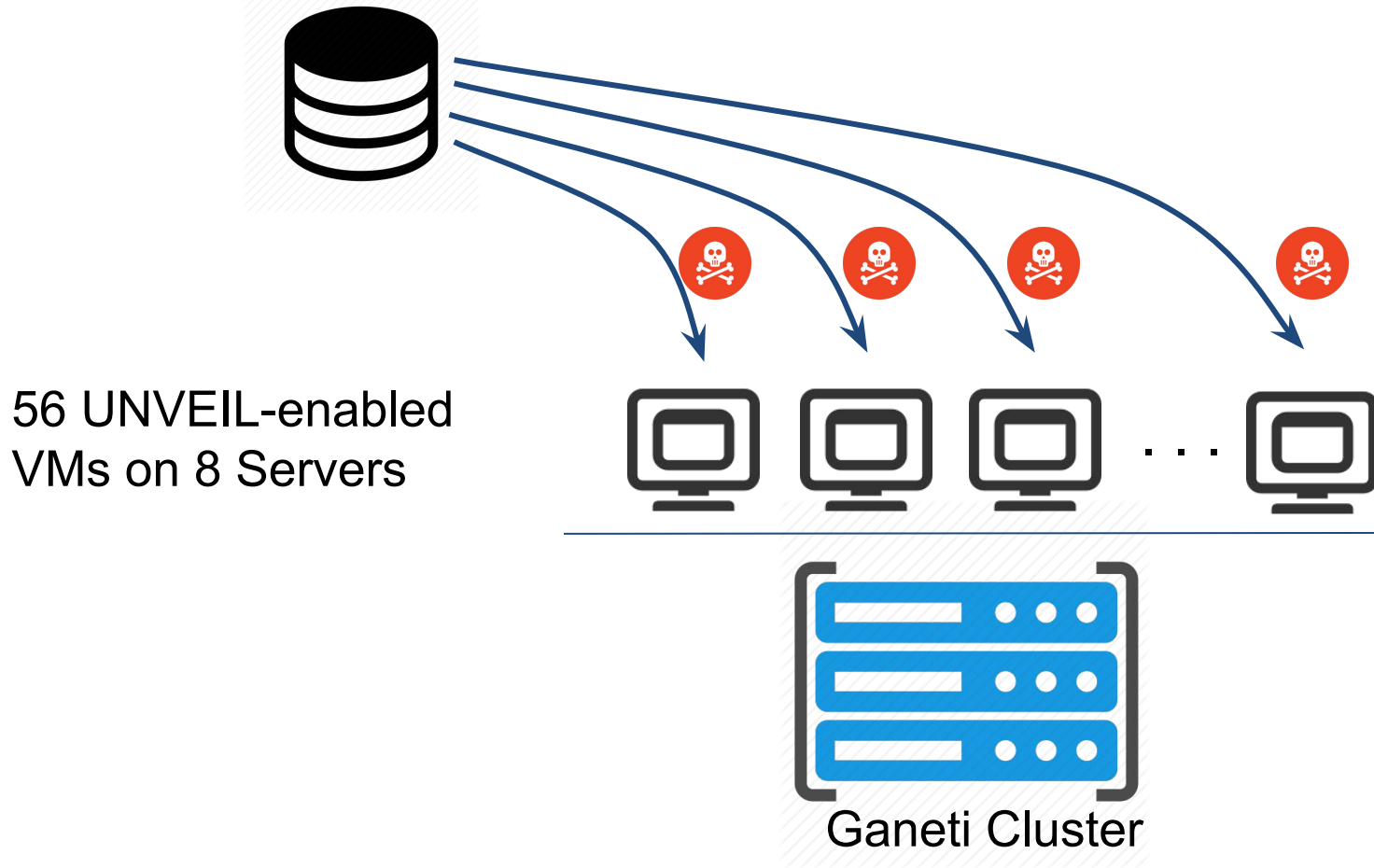
Detecting known ransomware samples



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

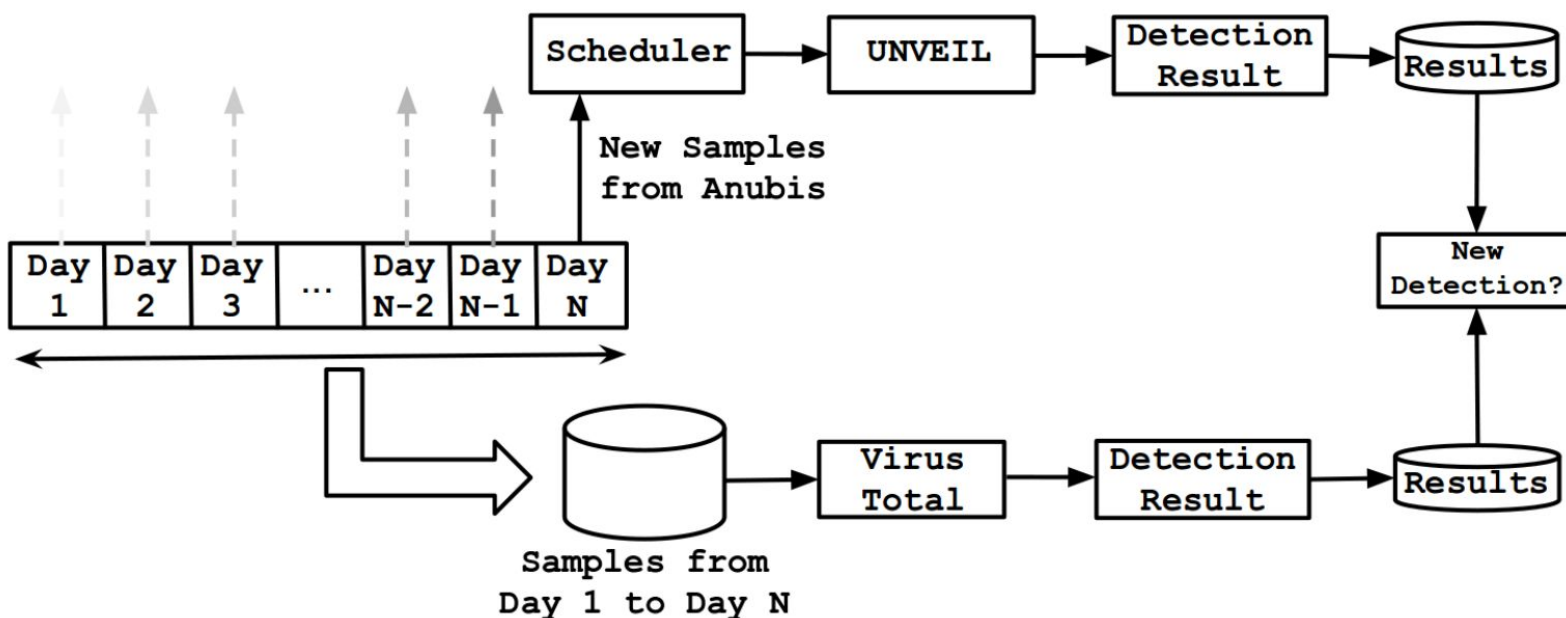
Evaluation UNVEIL with unknown samples

~ 1200 malware samples per day

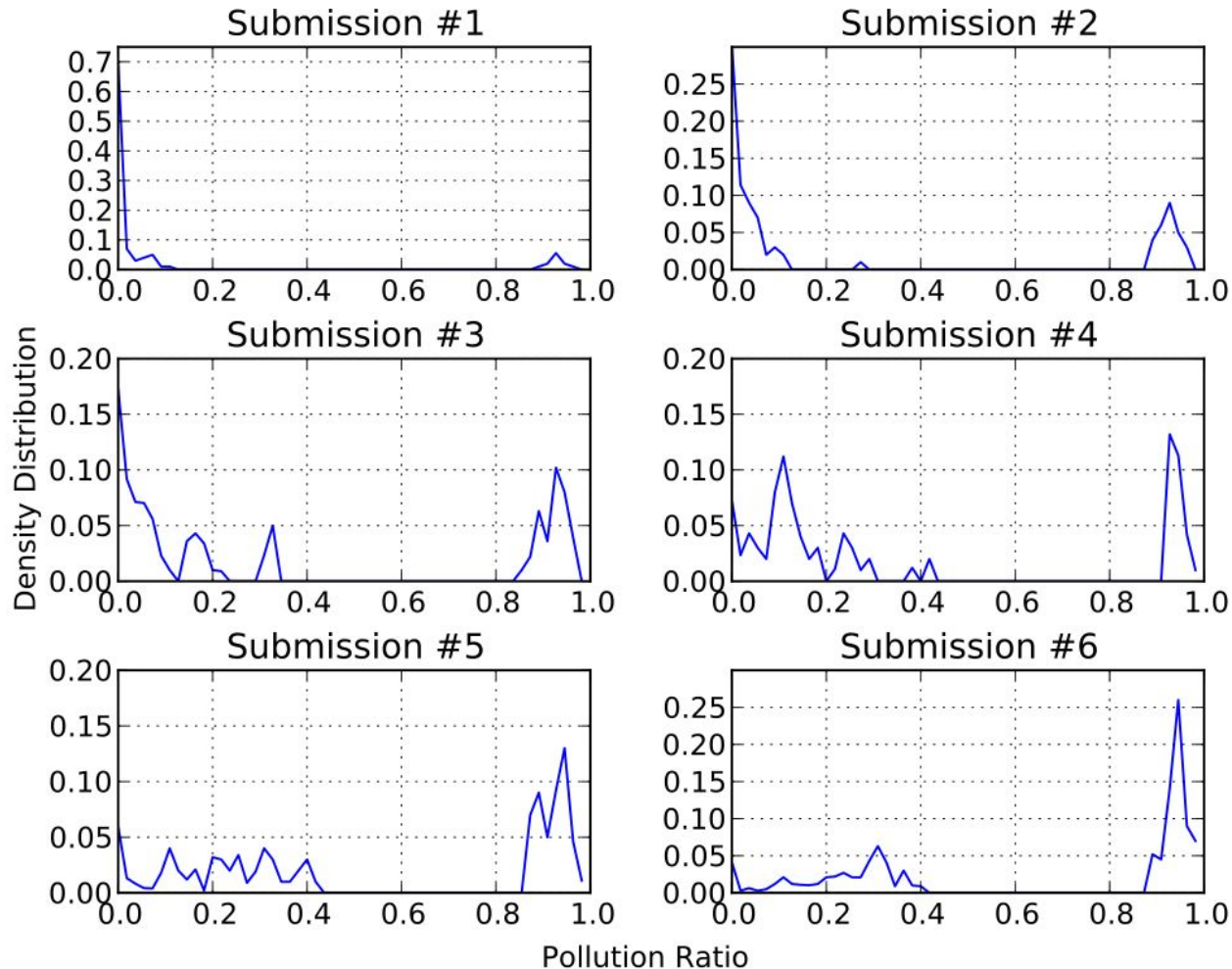


Evaluation UNVEIL with unknown samples

- 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

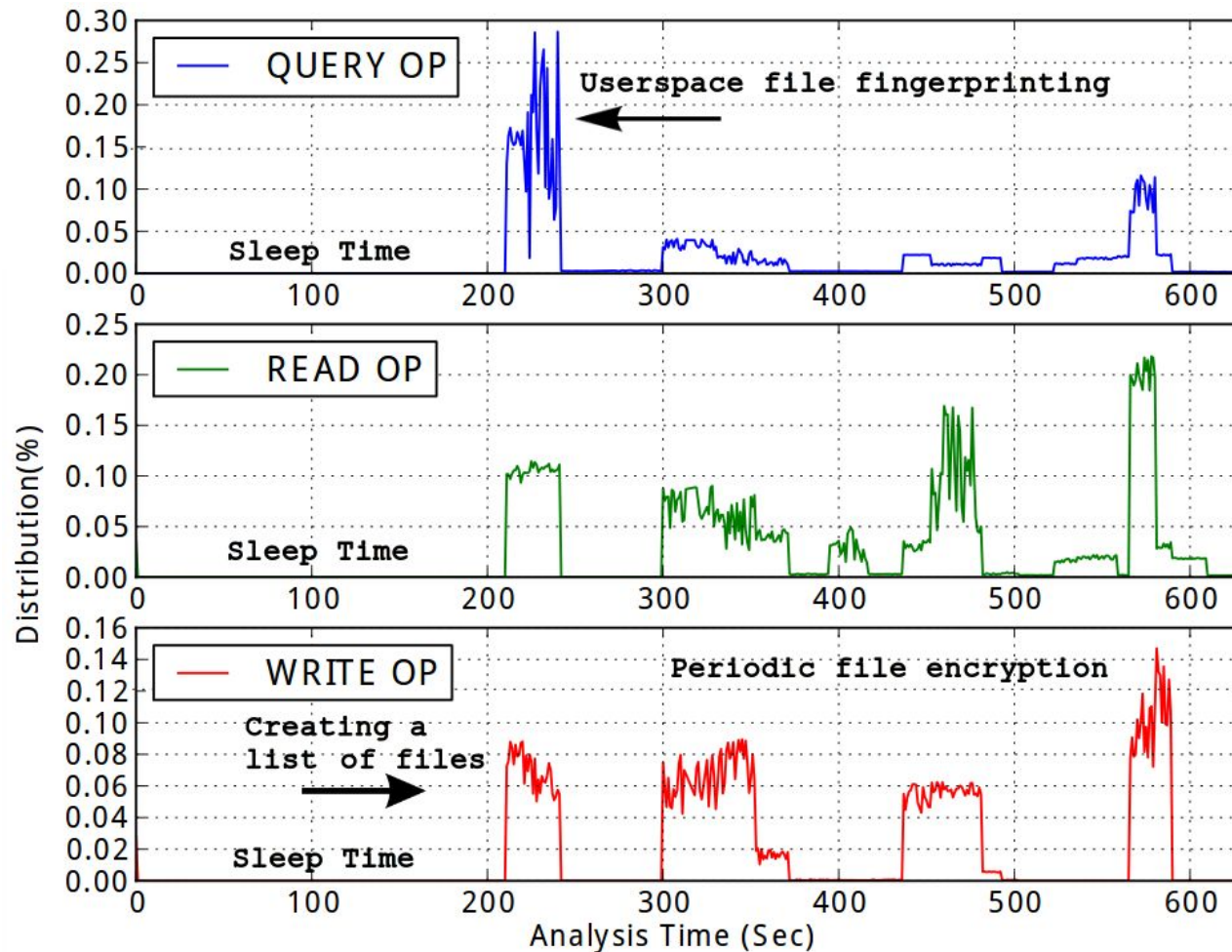


- Pollution ratio is defined as the ratio of the number of scanners that identified the sample to the number of scanners in VirusTotal

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



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

silentcrypt ransomware - Google Search - Chromium

https://www.google.com/search?site=&source=hp&q=silentcrypt+ransomware&og=silent&gs_l=hp.3.0.35i39j0i67j0i20j0i67j0i20j0i67j0i2.22884.24627.0.25426.9.8.1.0.0.177.731.1j4.5.0...0...1c.1.64.hp..3.5.587

Google silentcrypt ransomware

All News Images Videos Maps More Search tools

5 results (0.71 seconds)

Did you mean: [silent crypt ransomware](#)

SilentCrypt: A new ransomware Family - YouTube
<https://www.youtube.com/watch?v=qASKA4BMck>
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

Copy of unveil...pdf | precision_rec...pdf | Copy of sequ...png | Copy of Copy ...png | Show all downloads...

Conclusion

- Ransomware is a serious threat
- UNVEIL introduces concrete models to detect Ransomware
- Detecting an unknown family shows that the solutions are useful in practice
- We continue to improve functionality tuned towards detecting ransomware

Thank You