Data and Network Security

(Master Degree in Computer Science and Cybersecurity)

Lecture 2

SAPIENZA
UNIVERSITÀ DI ROMA

Outline for today

- Recap previous lecture
- Malware types
- Emerging threats

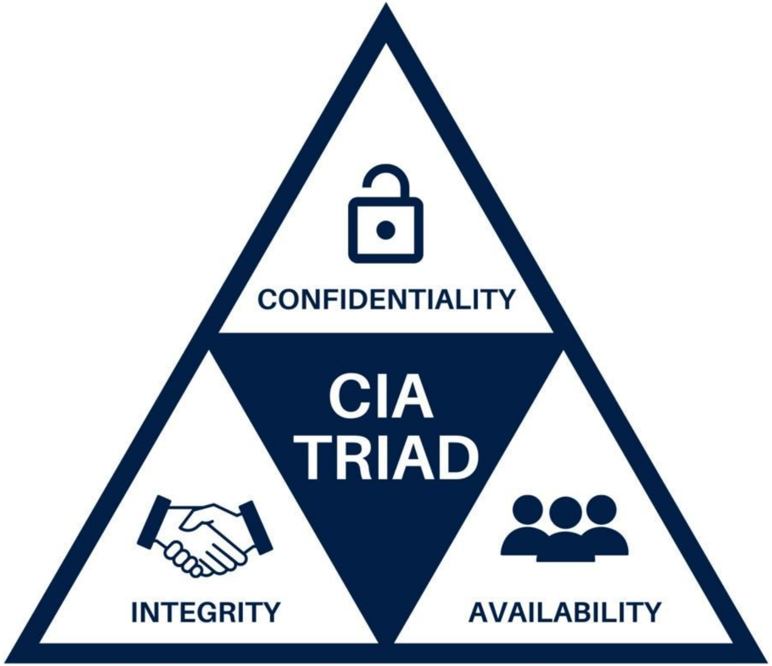
Outline for today

- **Recap previous lecture**
- Malware types
- Emerging threats

Cybersecurity / Data and Network Security?

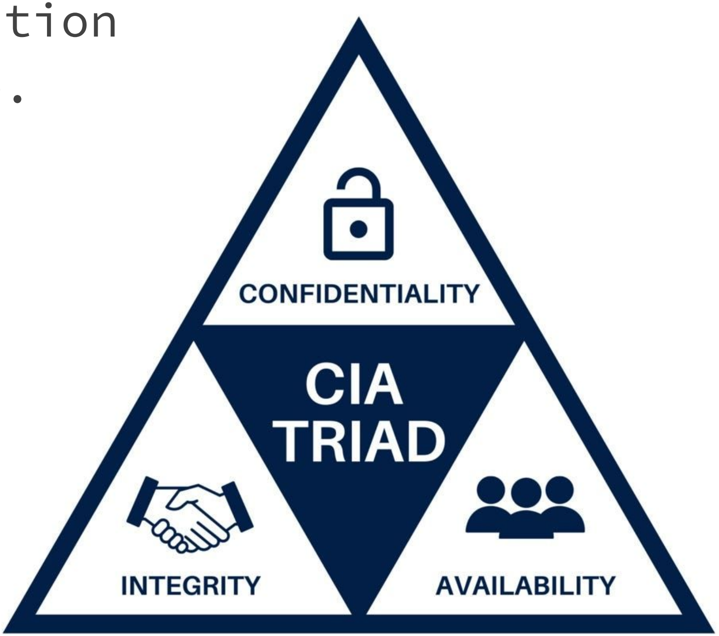
Cybersecurity is the practice of protecting digital systems, networks, and data from unauthorized access, alteration, or destruction. It encompasses various technologies, processes, and practices designed to safeguard information assets against a wide range of cyber threats.

The goals of DNS



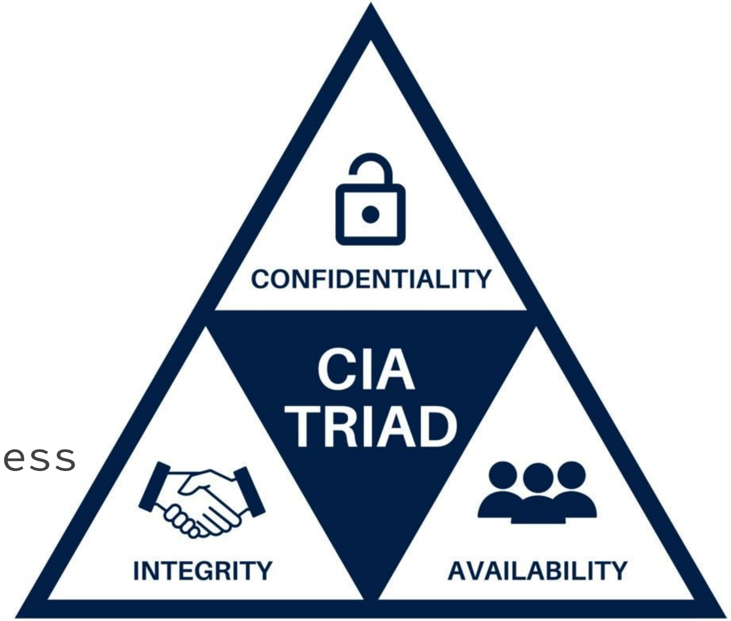
Confidentiality

Protecting sensitive information from unauthorized disclosure.

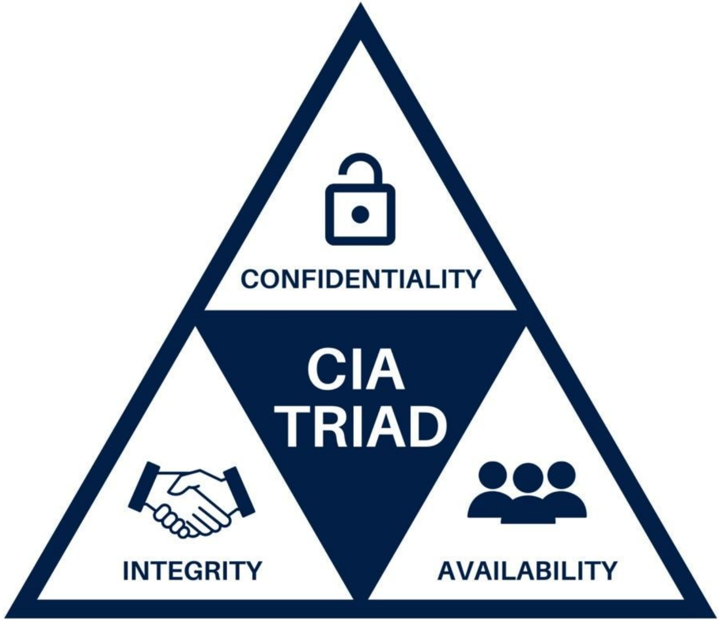


Integrity

Ensuring the accuracy and trustworthiness of data by preventing unauthorized modifications



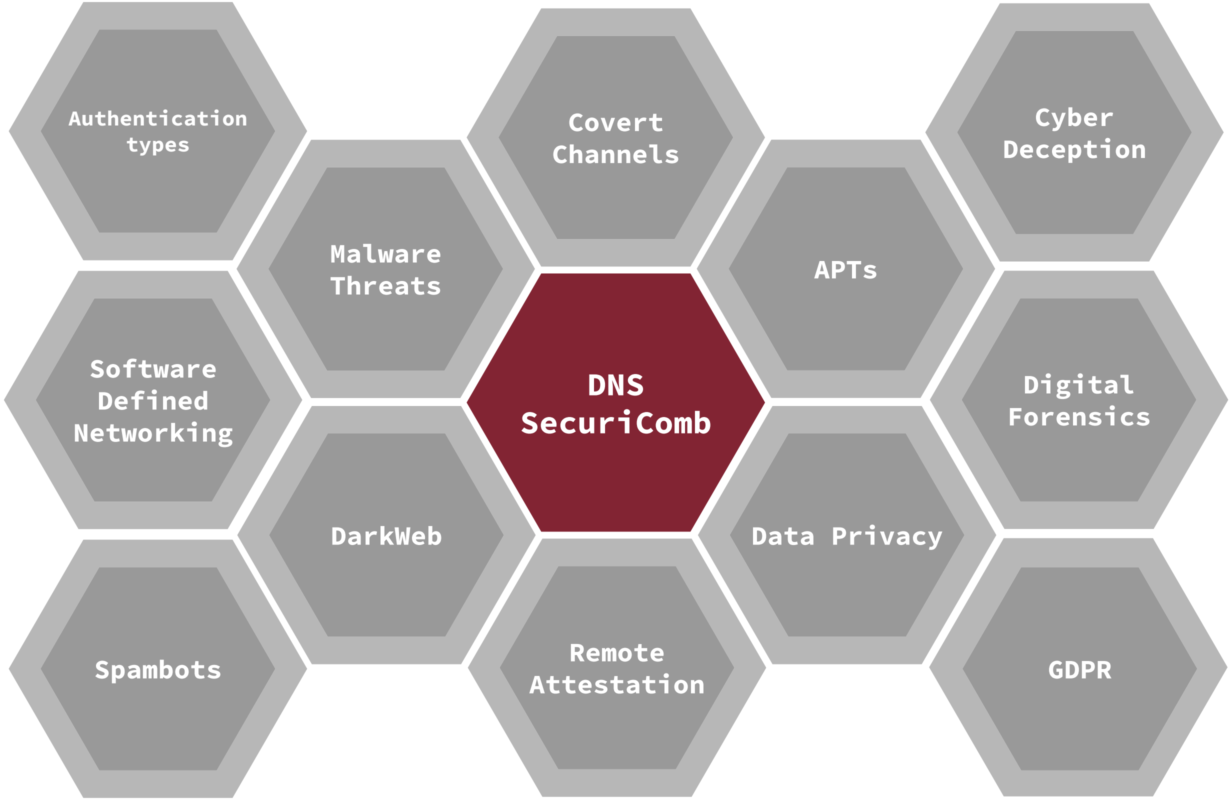
Availability



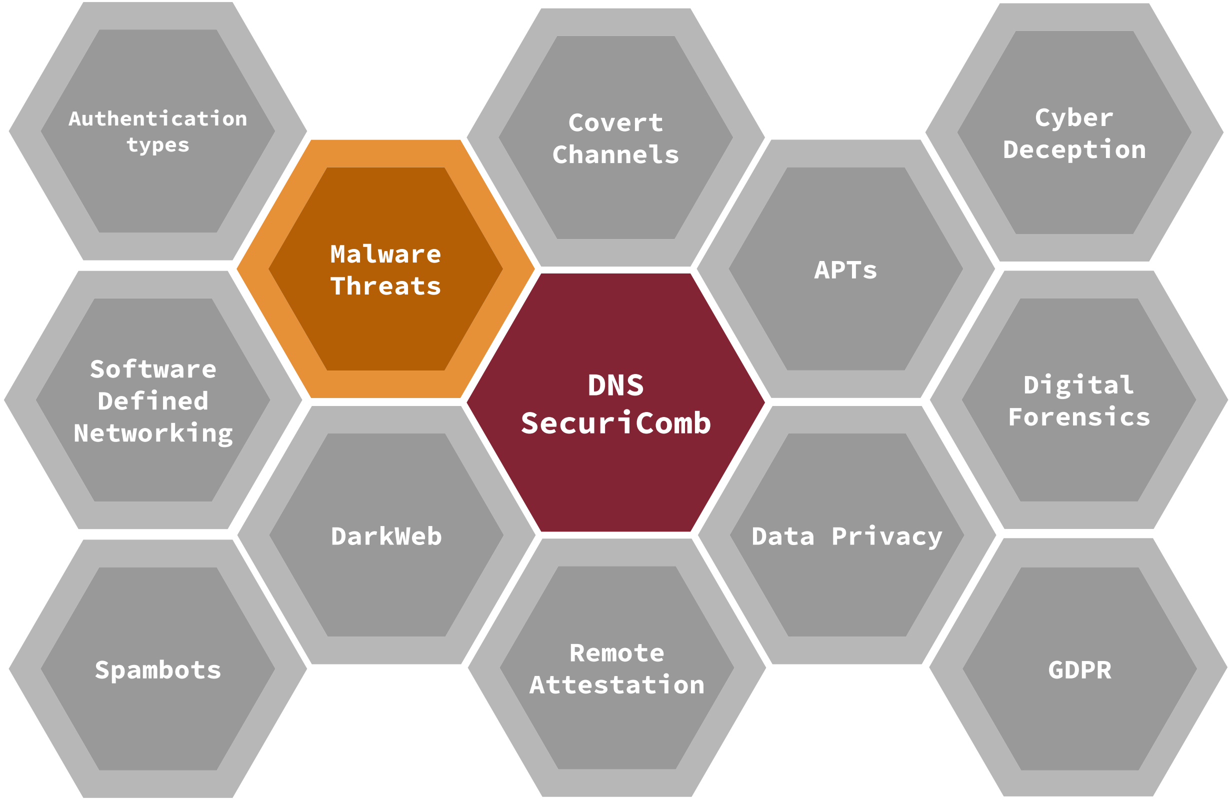
Ensuring that data and resources are available and accessible to authorized users when needed.

Major Threats to DATAs CIA

SecuriComb


Authentication types
Software Defined Networking
Spambots
Malware Threats
DarkWeb
Covert Channels
DNS SecuriComb
Remote Attestation
APTs
Data Privacy
Cyber Deception
Digital Forensics
GDPR

SecuriComb


Authentication types
Malware Threats
Covert Channels
APTs
Cyber Deception
Software Defined Networking
DNS SecuriComb
Digital Forensics
DarkWeb
Data Privacy
Spambots
Remote Attestation
GDPR

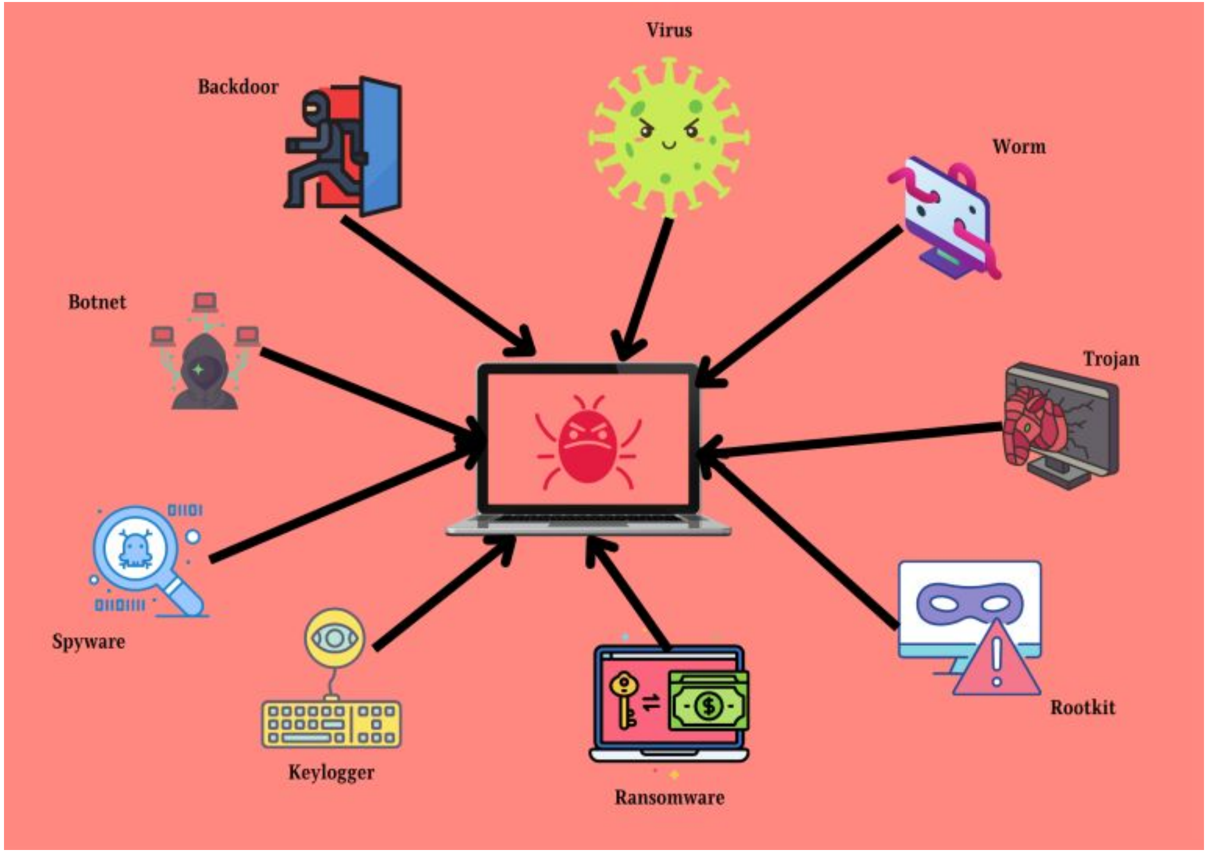
Malware Threats

Malware:

Type of software program or code specifically designed to infiltrate, damage, disrupt, or gain unauthorized access to computer systems, networks, or devices, often with malicious intent.

Broad category that encompasses various types of malicious programs, each with its own specific behavior and objectives.

Malware Types



Malware Threats - knowing them

1. Identification and Detection
2. Prevention and mitigation
3. Remediation
4. Risk (assessment and management)
5. General user education
6. Adapting towards evolving threats

Malware Threats - knowing them

1. **Identification and Detection**

By recognizing the signs of malicious activity, such as unusual network activity or unauthorized system changes, security teams can respond promptly to mitigate potential risks.

Malware Threats - knowing them

1. Identification and Detection
2. **Prevention and mitigation**
3. Remediation
4. Risk (assessment and management)
5. General user education
6. Adapting towards evolving threats

Malware Threats - knowing them

2. Prevention and mitigation

Understanding how malware operates enables organizations to implement **proactive** measures to prevent and mitigate malware.

Employing security controls such as **antivirus**, **firewalls**, **IDS**, and secure configuration practices, organizations can reduce the likelihood of malware attacks and limit their impact.

Malware Threats - knowing them

1. Identification and Detection
2. Prevention and mitigation
3. **Remediation**
4. Risk (assessment and management)
5. General user education
6. Adapting towards evolving threats

Malware Threats - knowing them

3. Remediation

Knowing malware types and how they operate facilitates an effective response and remediation process.

Security teams can leverage their understanding of specific malware behaviors to contain infections, remove malicious code, and restore affected systems to a secure state.

Malware Threats - knowing them

1. Identification and Detection
2. Prevention and mitigation
3. Remediation
4. **Risk (assessment and management)**
5. General user education
6. Adapting towards evolving threats

Malware Threats - knowing them

4. Risk (assessment and management)

Identifying potential threats and vulnerabilities associated with different malware, entities can prioritize security measures and allocate resources to address the most significant risks.

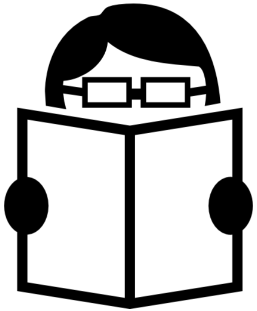
Malware Threats - knowing them

1. Identification and Detection
2. Prevention and mitigation
3. Remediation
4. Risk (assessment and management)
5. **General user education**
6. Adapting towards evolving threats

Malware Threats - knowing them

5. General user education

Teaching users to recognize common signs of malware attacks, such as suspicious emails or unexpected pop-up messages, organizations can assist them in taking proactive measures to protect themselves and the organization.



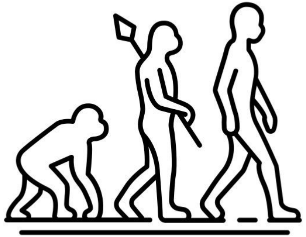
Malware Threats - knowing them

1. Identification and Detection
2. Prevention and mitigation
3. Remediation
4. Risk (assessment and management)
5. General user education
6. **Adapting towards evolving threats**

Malware Threats - knowing them

6. Adapting towards evolving threats

Continuously monitoring and analyzing emerging malware trends, organizations can enhance their cybersecurity position and try to stay one step ahead of adversaries.

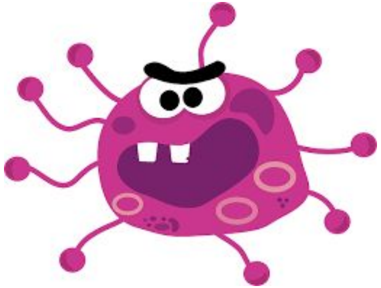


Malware Types - Common

- Viruses
- Worms
- Trojans
- Ransomware
- Spyware
- Adware
- Rootkits
- Scareware

Virus

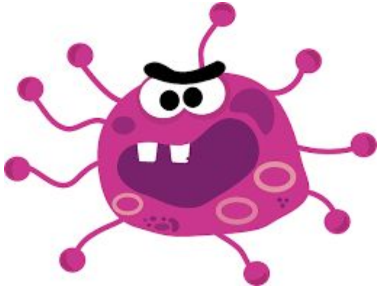
Program that can infect other programs by modifying them to include a, possibly evolved, version of itself, with intent to cause damage.



Virus

Program that can infect other programs by modifying them to include a, possibly evolved, version of itself, with intent to cause damage.

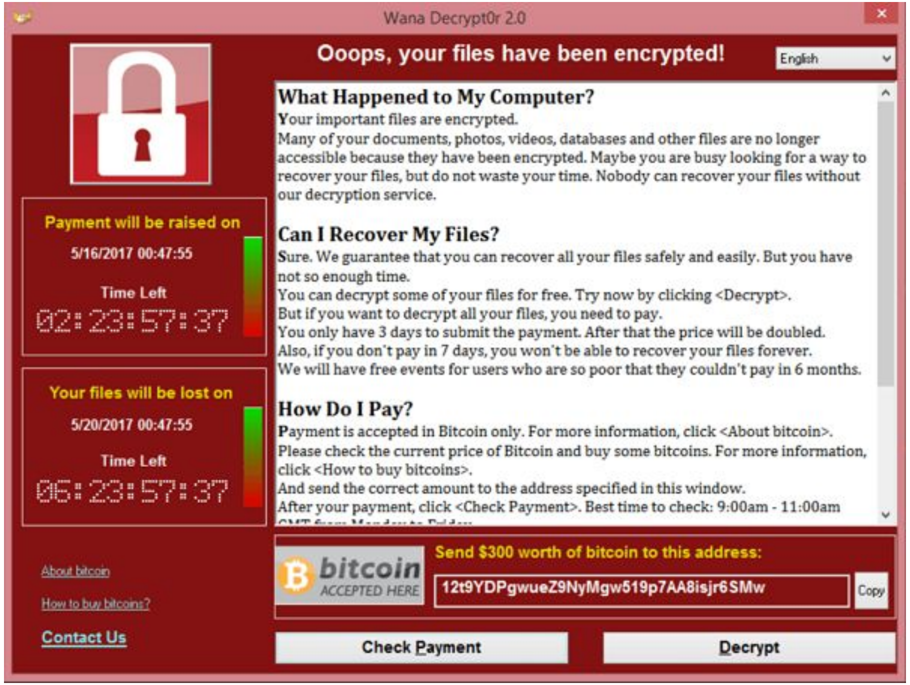
ILOVEYOU (discovered in 2000). The malware was delivered to millions of users as an email attachment with the subject line “ILOVEYOU.” Once opened, it spread to every contact in a user’s Microsoft Outlook address book and overwrite certain files (e.g., JPEG and MP3 files) from the hard drive.



Trojan

Class of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that usually allow unauthorized access to the victim computer.

Ransomware



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.

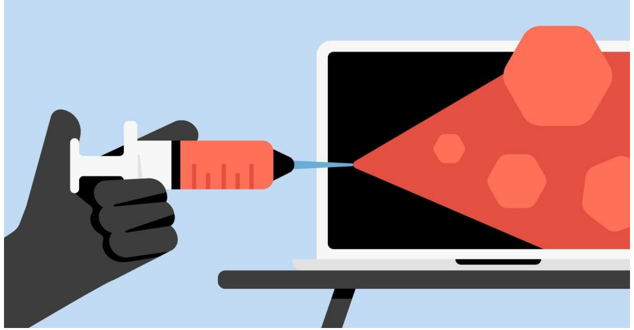
Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

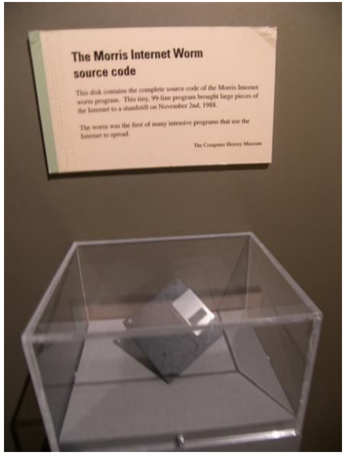
Rootkit

A rootkit is a program or a collection of malicious software tools that give an adversary remote access to and control over a computer.



Worms

A computer worm is a type of malware that can automatically propagate or self-replicate without human interaction, enabling its spread to other computers across a network.


The Morris Internet Worm
source code
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.
The worm was the first of many intrusive programs that use the Internet to spread.
The Computer History Museum

Spyware

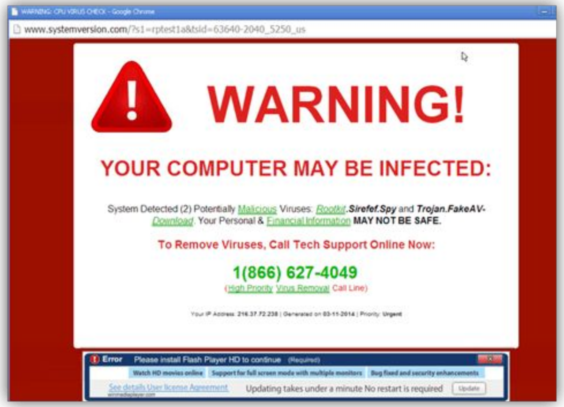
Malicious software that infects PCs and mobile devices in order to collect information on users and data on browsing habits, internet use, etc.

Adware

Adware is a type of malicious software that secretly installs itself on your device and displays unwanted advertisements and pop-ups. In some cases, adware can even track your online behavior and display personalized ads.

Scareware

Malware that scares people into visiting spoofed or infected websites or downloading malicious software. Scareware can come in the form of pop-up ads that appear on a user's computer or spread through spam email attacks.



WARNING: CPU VIRUS CHECK - Google Chrome
www.systemversion.com/?s1=rptest1a&tsid=63640-2040_5250_us

WARNING!

YOUR COMPUTER MAY BE INFECTED:

System Detected (2) Potentially Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.FakeAV-Download. Your Personal & Financial Information MAY NOT BE SAFE.

To Remove Viruses, Call Tech Support Online Now:

1(866) 627-4049
(High Priority Virus Removal Call Line)

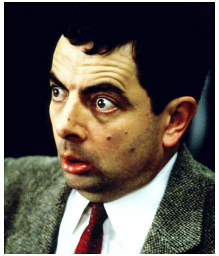
Your IP Address: 216.37.72.238 | Generated on 03-11-2014 | Priority: Urgent

Error Please install Flash Player HD to continue (Required)

Watch HD movies online | Support for full screen mode with multiple monitors | Bug fixed and security enhancements

See details User license Agreement

Updating takes under a minute No restart is required



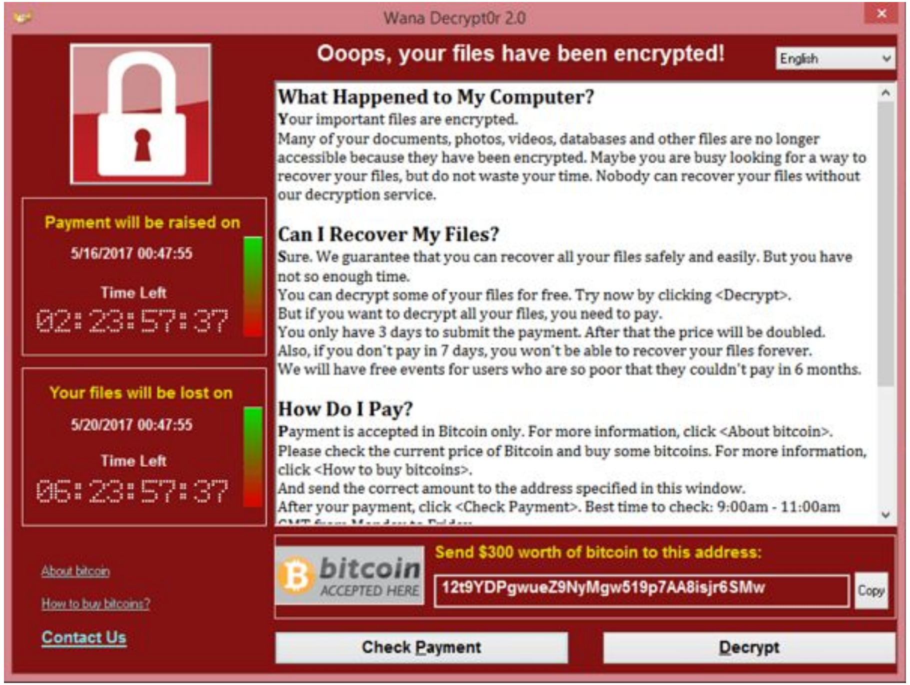
Outline for today

- Recap previous lecture
- Malware types
- Emerging threats

Outline for today

- Recap previous lecture
- Malware types
- **Emerging threats**

Ransomware



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

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.

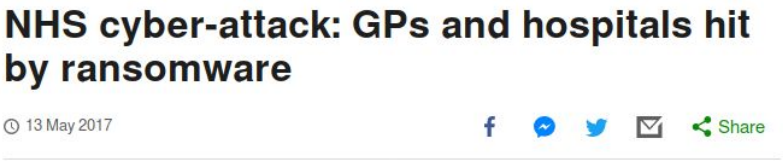
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

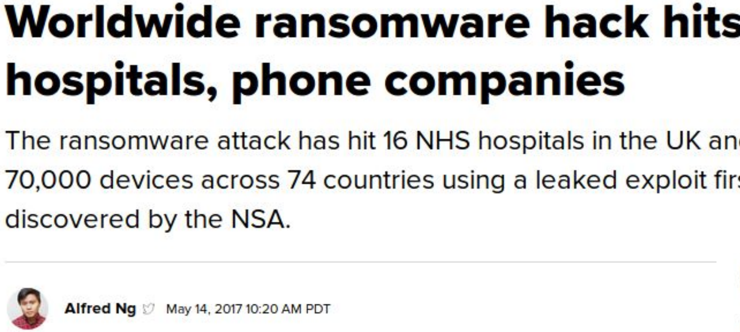
The Ransomware Threat



NHS cyber-attack: GPs and hospitals hit by ransomware

13 May 2017

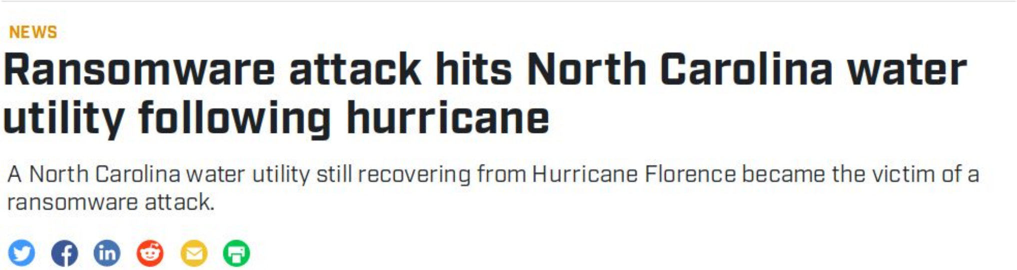
Share



Worldwide ransomware hack hits hospitals, phone companies

The ransomware attack has hit 16 NHS hospitals in the UK and up to 70,000 devices across 74 countries using a leaked exploit first discovered by the NSA.

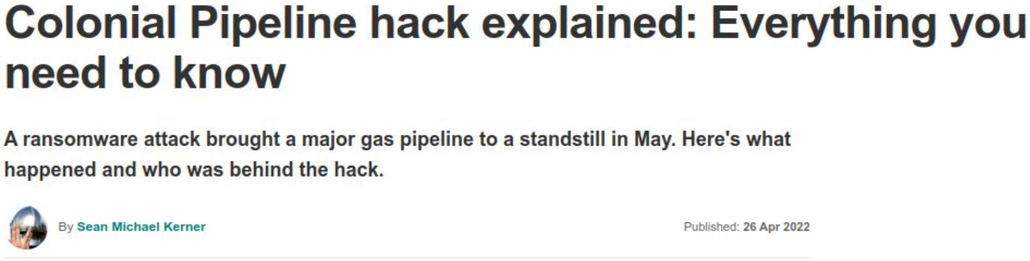
Alfred Ng May 14, 2017 10:20 AM PDT



NEWS

Ransomware attack hits North Carolina water utility following hurricane

A North Carolina water utility still recovering from Hurricane Florence became the victim of a ransomware attack.



Colonial Pipeline hack explained: Everything you need to know

A ransomware attack brought a major gas pipeline to a standstill in May. Here's what happened and who was behind the hack.

By Sean Michael Kerner Published: 26 Apr 2022

Signature based vs. Behaviour based detection

Signature based vs. Behaviour based detection

Signature based detection works by searching for a known identity – or signature – for each specific event.

- Very efficient (as long as it is kept up to date)

Signature based vs. Behaviour based detection

Analysing and monitoring how a process behaves in the system, for example how many files it accesses, what locations of the storage affects etc.

Ransomware detectors

ShieldFS: A Self-healing, Ransomware-aware Filesystem

Andrea Continella andrea.continella@polimi.it
Alessandro Guagnelli alessandro.guagnelli@polimi.it
Giovanni Zingaro giovanni.zingaro@polimi.it
Giulio De Pasquale giulio.depasquale@polimi.it
Alessandro Barenghi alessandro.barenghi@polimi.it
Stefano Zanero stefano.zanero@polimi.it
Federico Maggi federico.maggi@polimi.it
DEIB, Politecnico di Milano, Milan, Italy

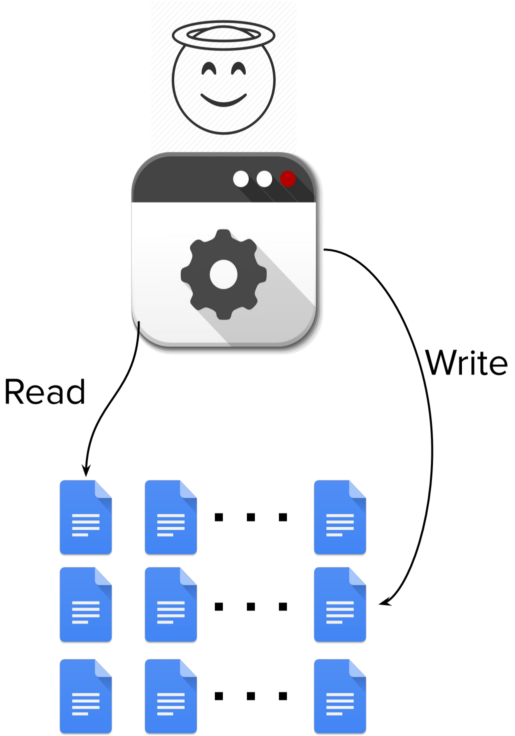
Malwarebytes

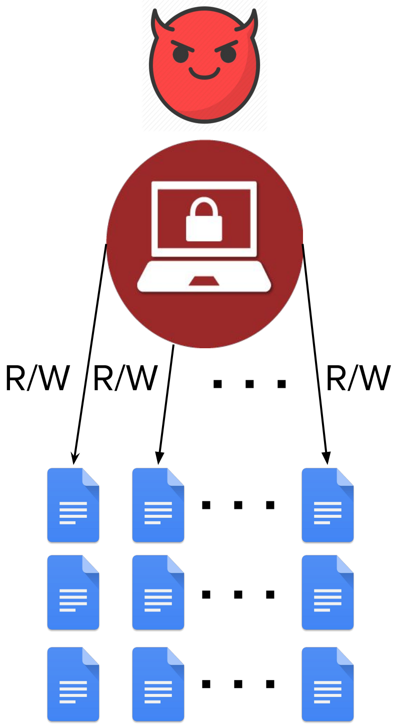
RWGuard: A Real-Time Detection System Against Cryptographic Ransomware

Shagufta Mehnaz(✉), Anand Mudgerikar, and Elisa Bertino

Purdue University, West Lafayette, IN, USA
{smehnaz,amudgeri,bertino}@purdue.edu

Ransomware behaviour





Ransomware features

- Encrypts files ->- high entropy

  - overwrites whole file

  - completely changes file content (no similarity)

  - changes file type

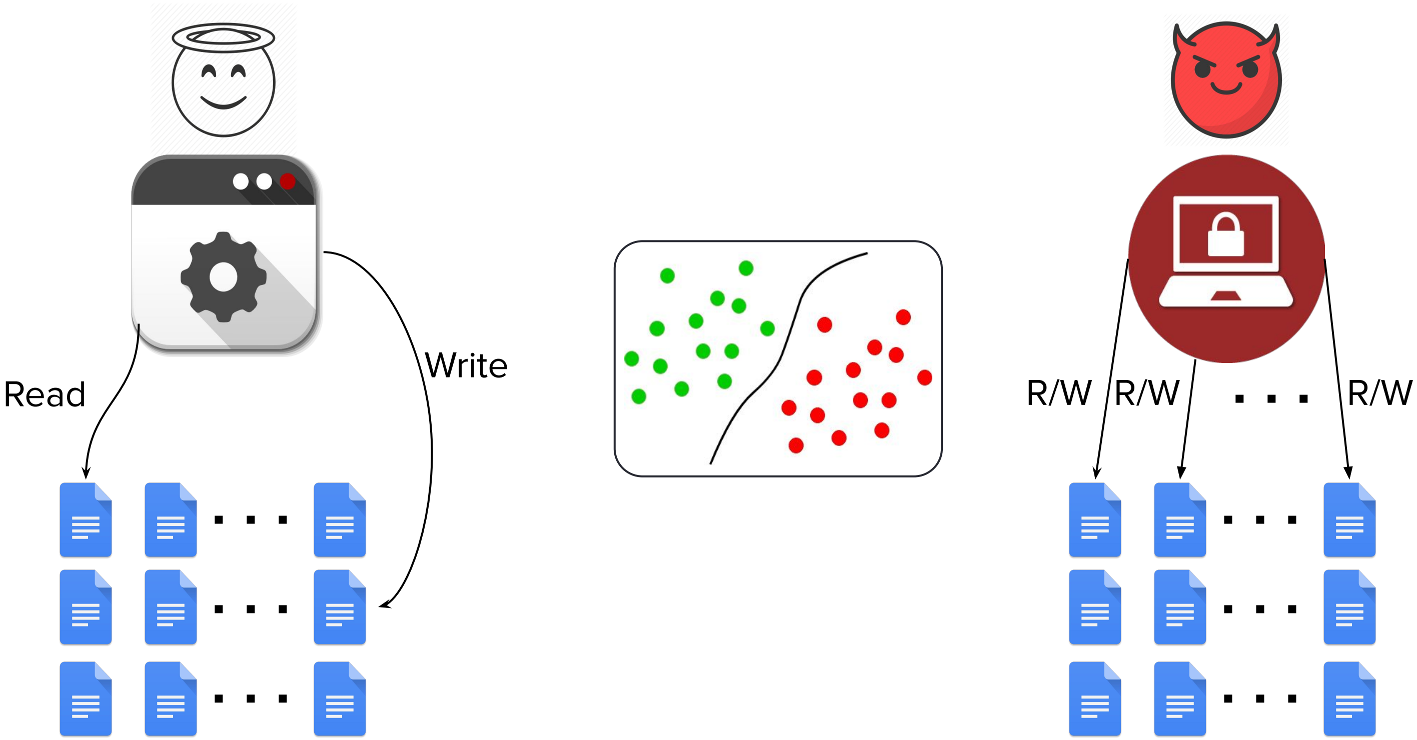
- Access as many files as possible -> lots of listing/read/write/open/create/close

- Encrypt all user files -> - access different, unrelated file types

  - access all files in every directory

- Encrypts as fast as possible -> very high access frequency

Ransomware detectors



Behavioural Classification

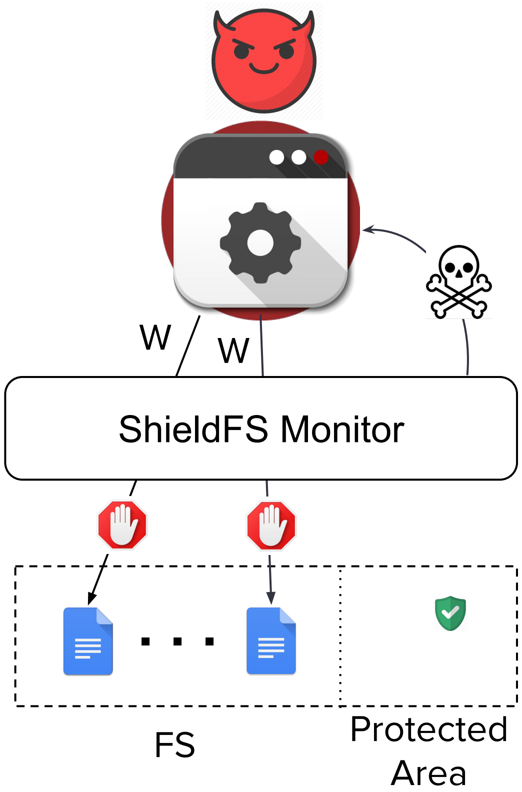
Behavioural classifiers analyse features inextricably linked with ransomware

- e.g., high number of read/write/directory listing, high entropy writes

Model behavior of individual processes

- per-process feature collection

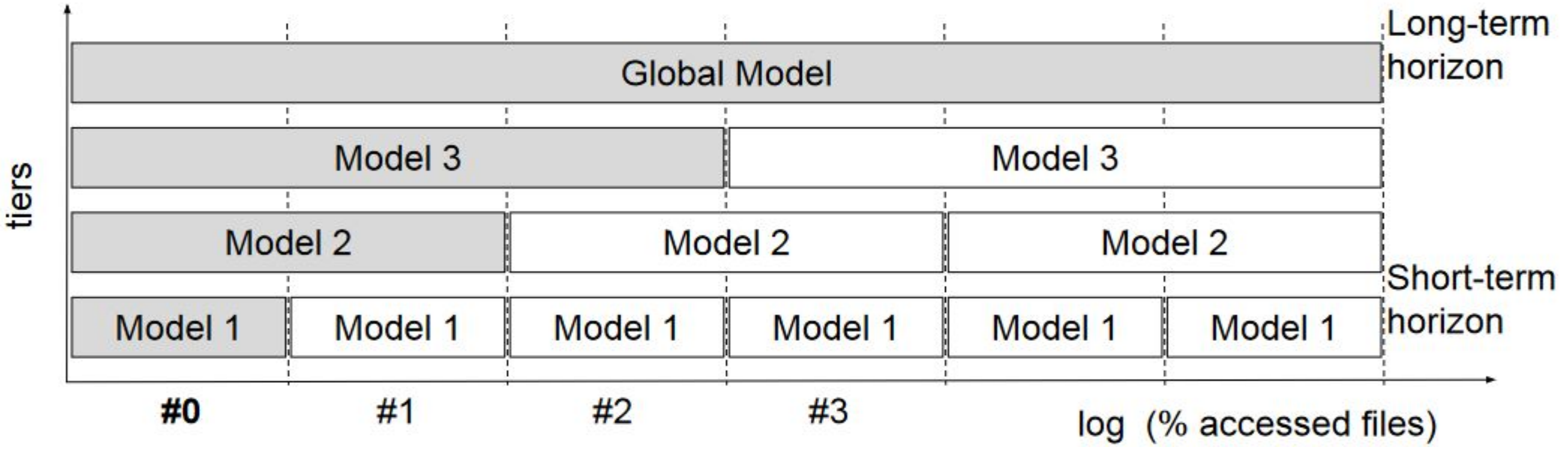
ShieldFS by Continella et al.



Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, Federico Maggi, **ShieldFS: A Self-healing, Ransomware-aware Filesystem**, In Proceedings of the Annual Computer Security Applications Conference (ACSAC), 2016

ShieldFS Detector

tick #0



Long-term horizon

Global Model

Model 3 | Model 3

Model 2 | Model 2 | Model 2

Model 1 | Model 1 | Model 1 | Model 1 | Model 1 | Model 1

Short-term horizon

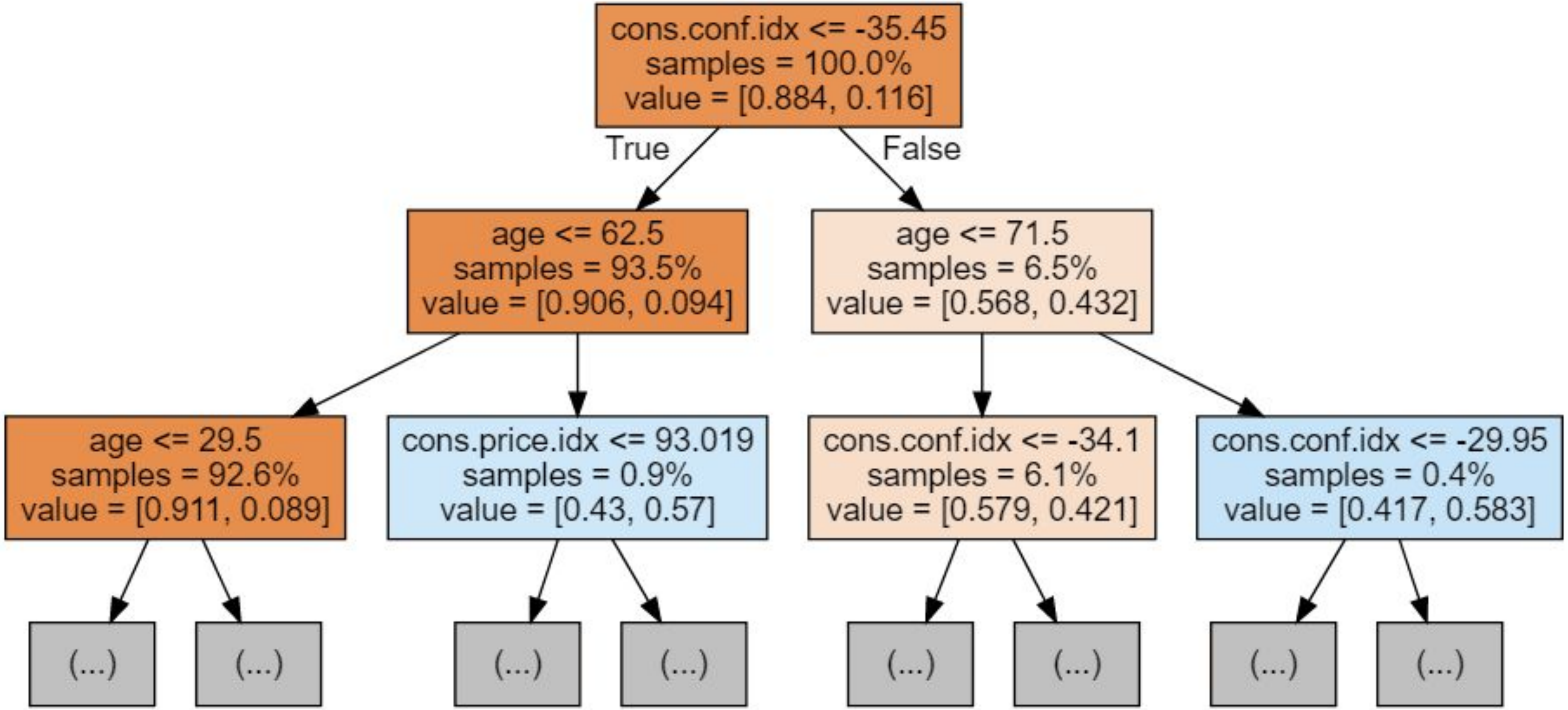
tiers

#0 #1 #2 #3

log (% accessed files)

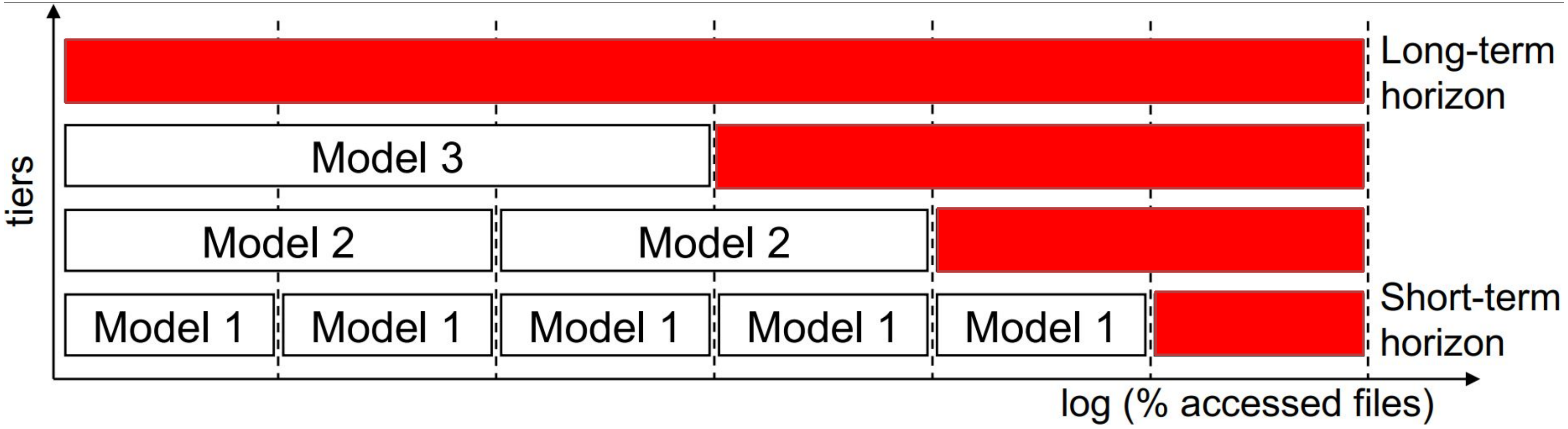
ShieldFS Detector - Random Forests?

$<f1, f2, \ldots, f_N>$



***illustrative example**

ShieldFS Detection Process



Long-term horizon

Model 3

Model 2

Model 2

Short-term horizon

Model 1

Model 1

Model 1

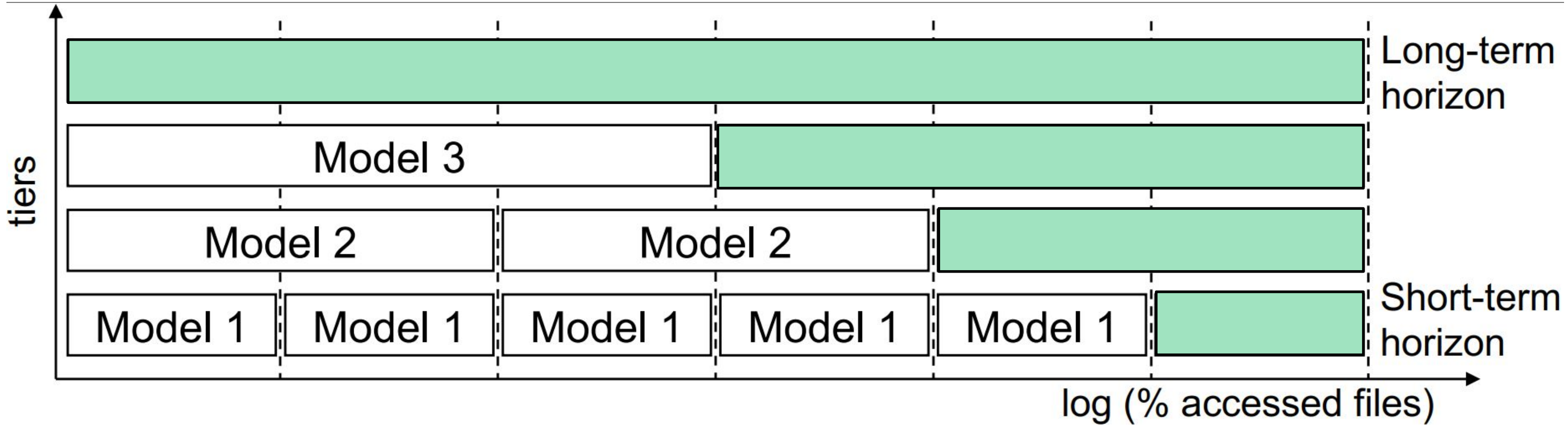
Model 1

Model 1

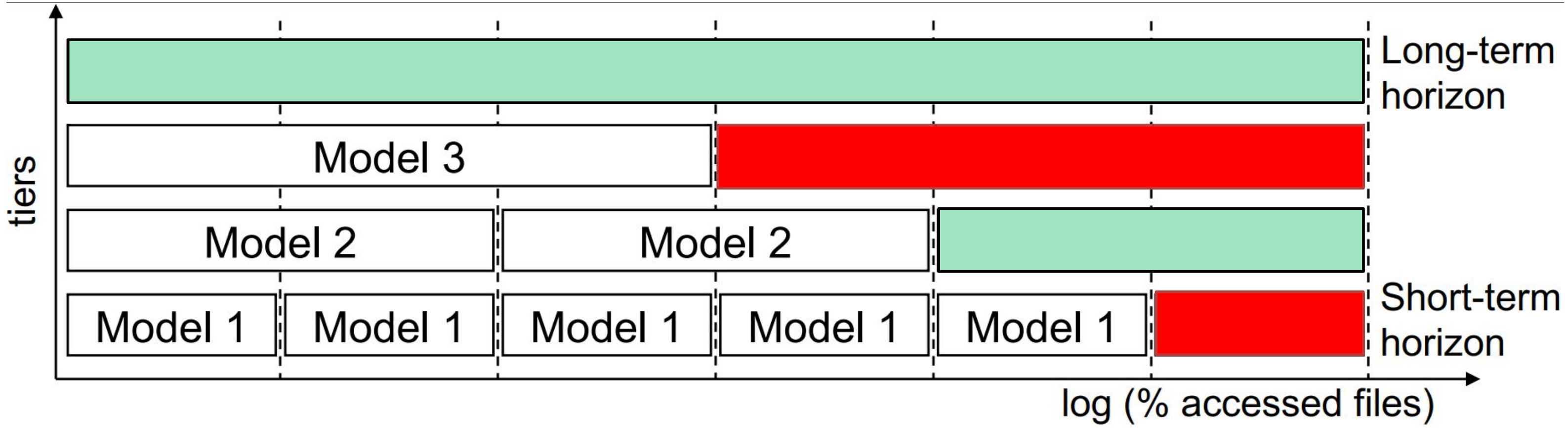
tiers

log (% accessed files)

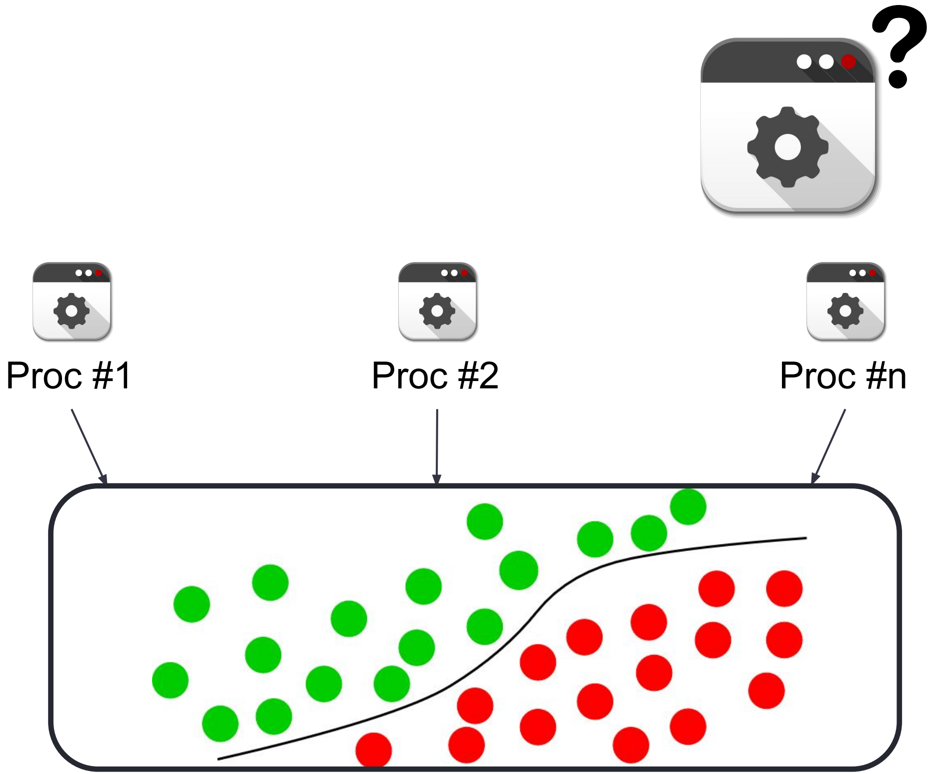
ShieldFS Detection Process



ShieldFS Detection Process



ShieldFS Detection Process



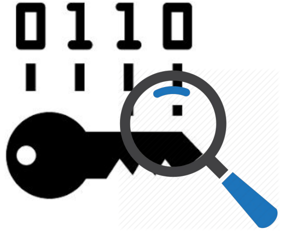
Proc #1

Proc #2

Proc #n

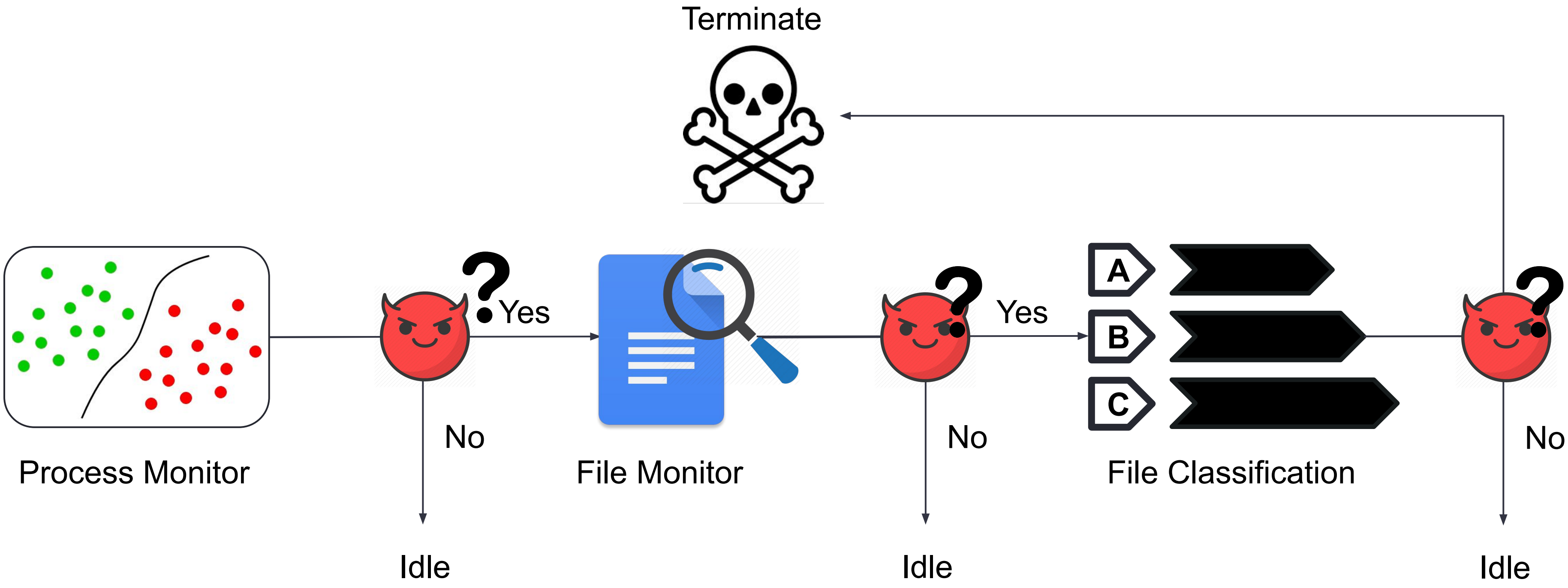
System-Centric Model

+



Search for Crypto Functions

RWGuard by Mehnaz et al.



Mehnaz Shagufta, Mudgerikar Anand, Bertino Elisa. **RWGuard: A Real-Time Detection System Against Cryptographic Ransomware**, RAID, 2018

Are these approaches reliable in adversarial conditions?

Evading Behavioural Classification

How can we lower the expression of all ransomware features at the process level?

- **Reduce feature expression by reducing #operations**

Evading Behavioural Classification

How can we lower the expression of all ransomware features at the process level?

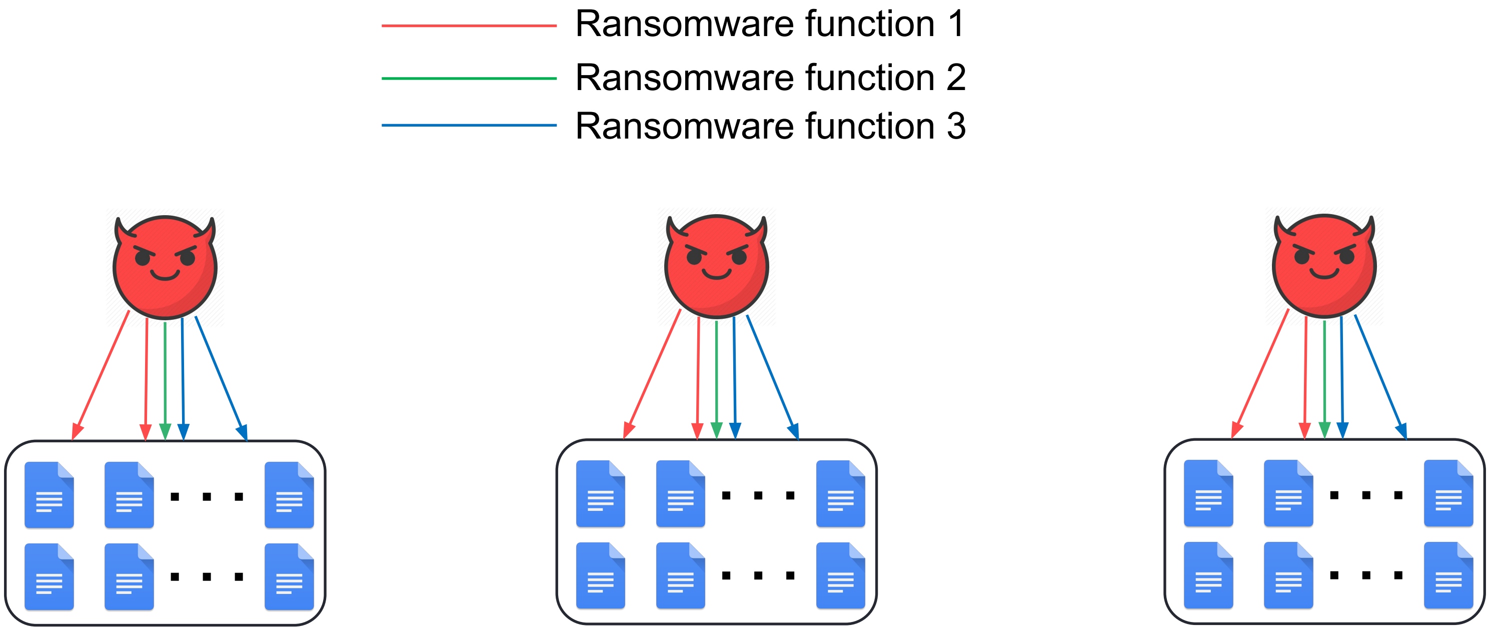
- **Reduce feature expression by reducing #operations**

<u>Distribute ransomware operations over independent, cooperating processes</u>

- **Process Splitting**
- **Functional Splitting**
- **Mimicry**

Process splitting

Process Splitting

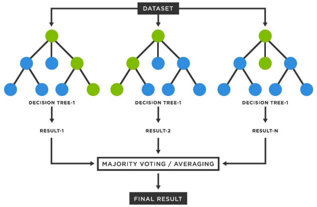


Ransomware function 1

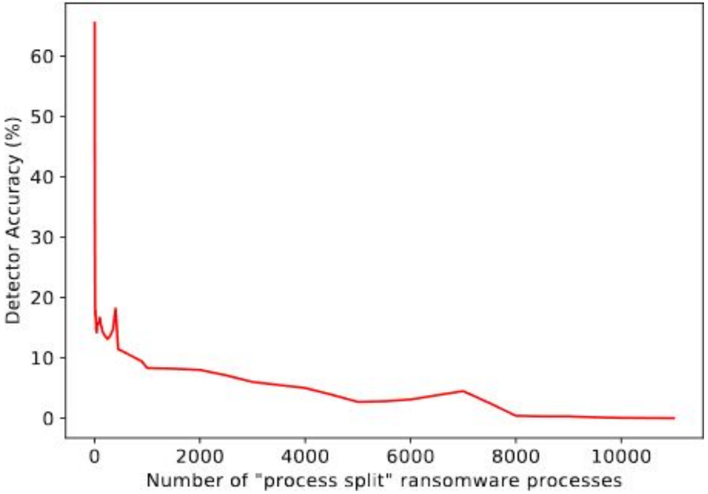
Ransomware function 2

Ransomware function 3

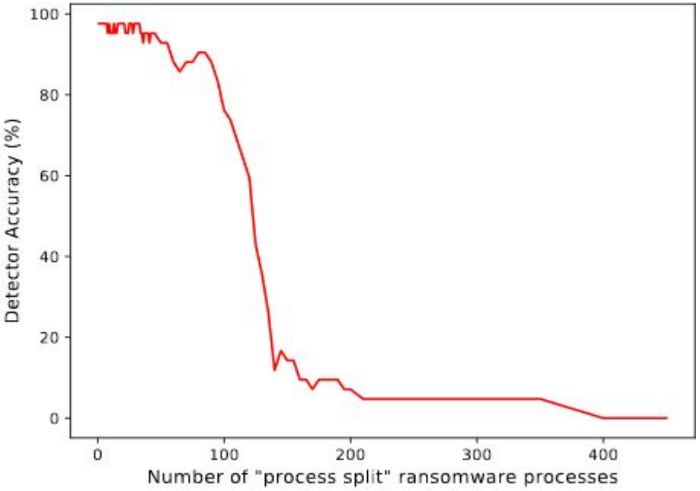
Process Splitting Evaluation



ShieldFS



RWGuard



Functional splitting

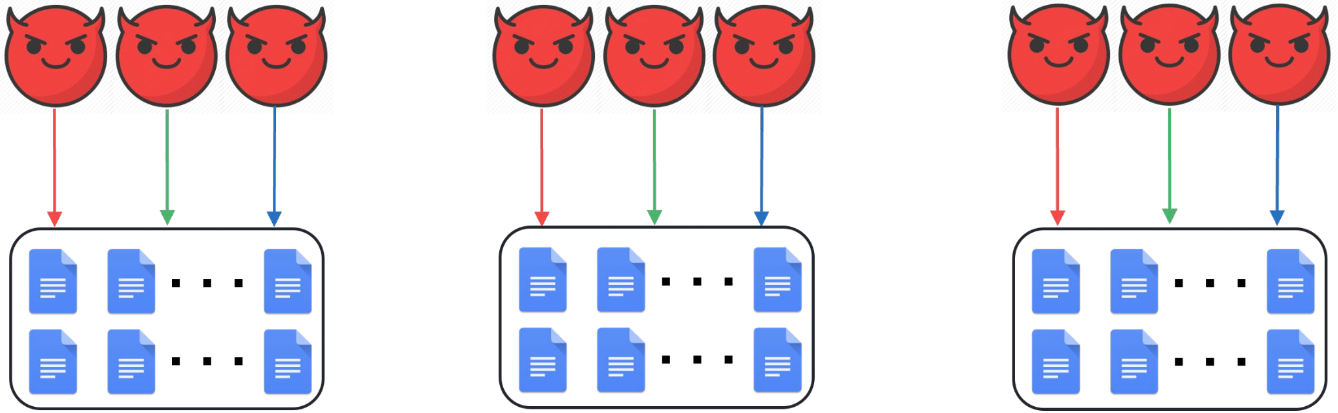
Functional

Splitting

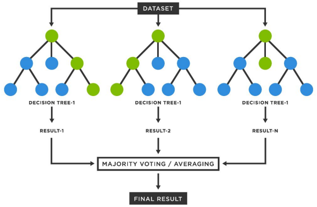
🟥 Ransomware function 1

🟩 Ransomware function 2

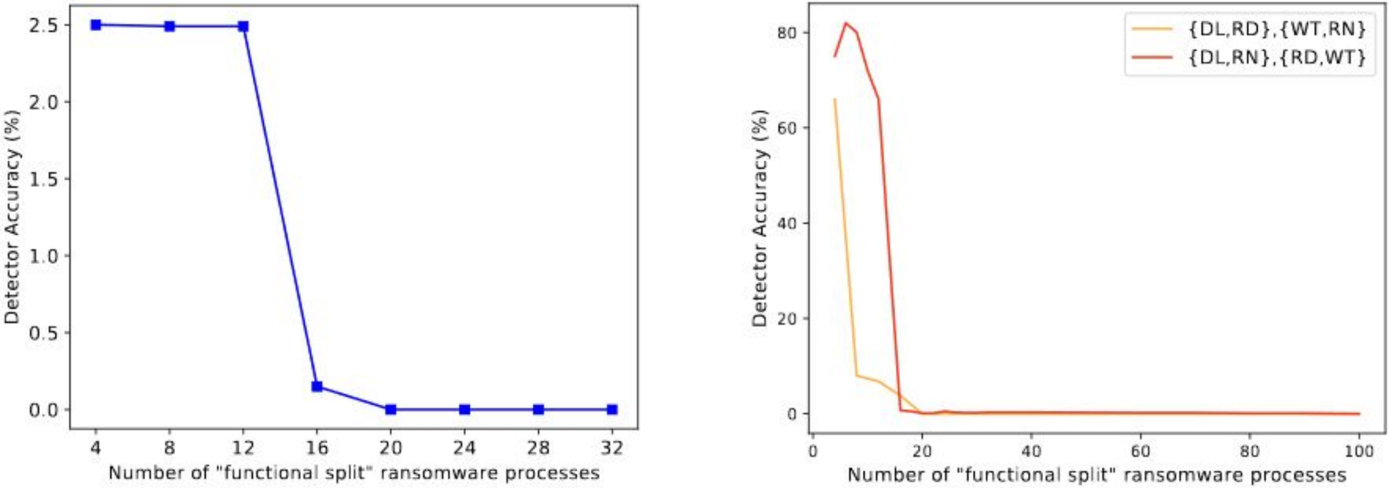
🟦 Ransomware function 3



Functional Splitting Evaluation



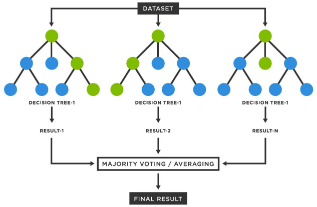
ShieldFS



(a) Single functional splitting

(b) Combined Functional Splitting

Functional Splitting Evaluation


DATASET

DECISION TREE-1

DECISION TREE-1

DECISION TREE-1

RESULT-1

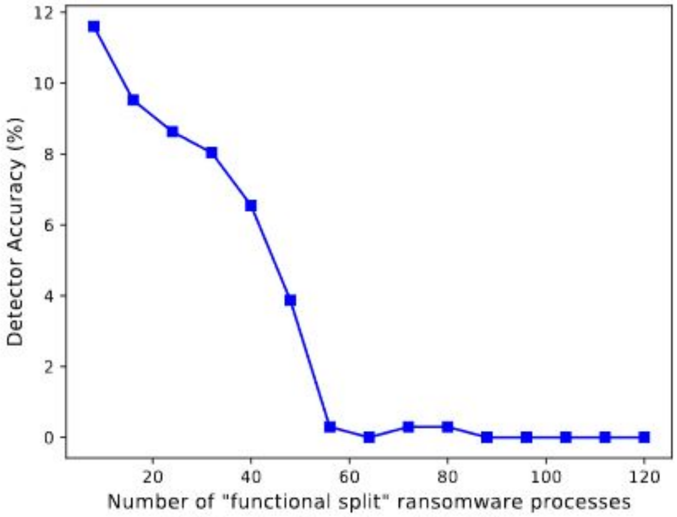
RESULT-2

RESULT-N

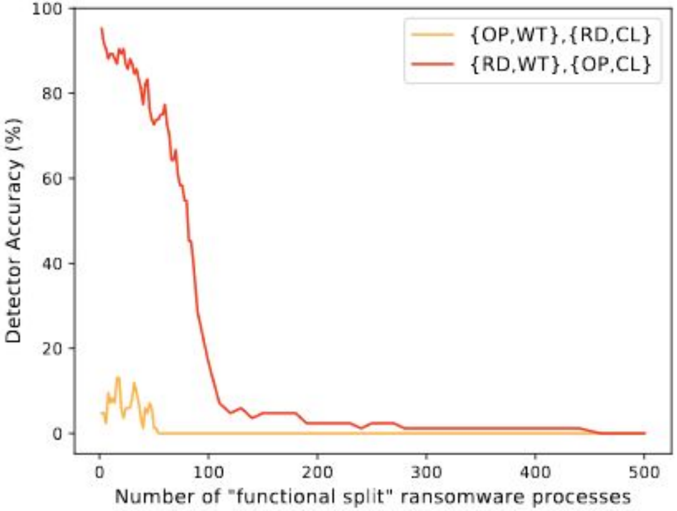
MAJORITY VOTING / AVERAGING

FINAL RESULT

RWGuard



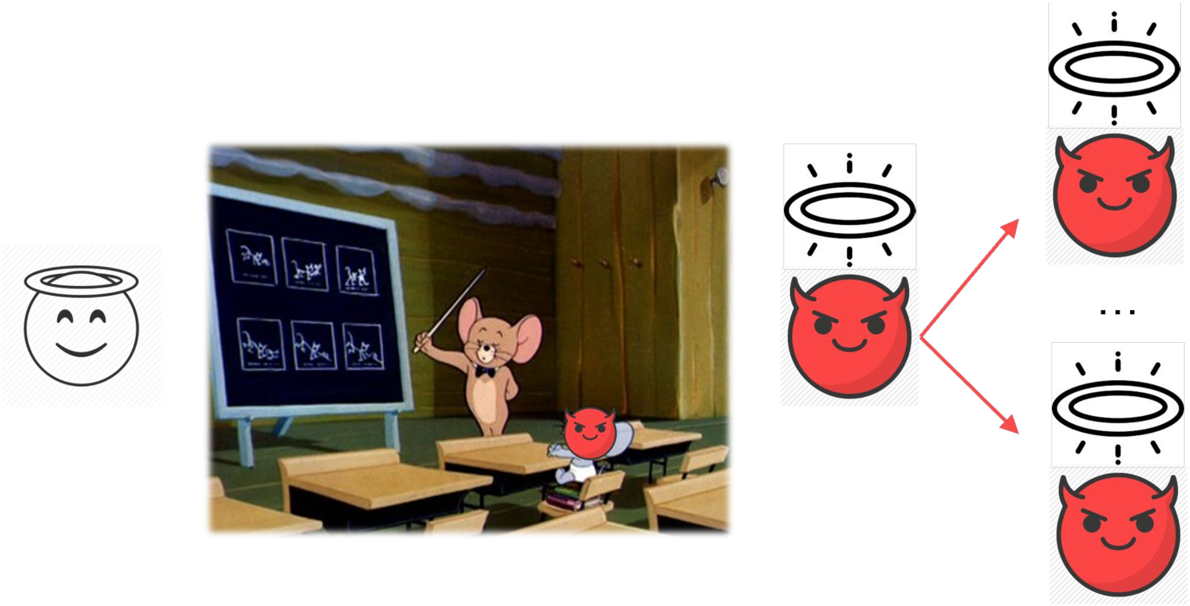
(a) Single Functional Splitting



(b) Combined Functional Splitting.

Mimicry

Mimicry:



Mimicry Evaluation

ShieldFS: full evasion

- 170 mimicry processes

RWGuard: full evasion

- 170 mimicry processes

Malwarebytes: full evasion

- 470 mimicry processes

Ransomware detectors

ShieldFS: A Self-healing, Ransomware-aware Filesystem

Andrea Continella
andrea.continella@polimi.it

Alessandro Guagnelli
alessandro.guagnelli@polimi.it

Giovanni Zingaro
giovanni.zingaro@polimi.it

Giulio De Pasquale
giulio.depasquale@polimi.it

Alessandro Barenghi
alessandro.barenghi@polimi.it

Stefano Zanero
stefano.zanero@polimi.it

Federico Maggi
federico.maggi@polimi.it

DEIB, Politecnico di Milano, Milan, Italy

Malwarebytes

RWGuard: A Real-Time Detection System Against Cryptographic Ransomware

Shagufta Mehnaz(✉), Anand Mudgerikar, and Elisa Bertino

Purdue University, West Lafayette, IN, USA
{smehnaz,amudgeri,bertino}@purdue.edu

Process centric fails

Can we make these approaches more reliable?

A naive approach

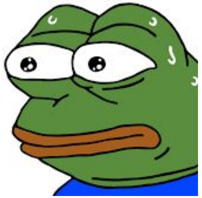
- Update the behavioural classifiers on these workload distribution attacks

A naive approach

- **Update the behavioural classifiers on these workload distribution attacks**
    - **works on process splitting and functional splitting**

A naive approach

- Update the behavioural classifiers on these workload distribution attacks
  - works on process splitting and functional splitting
  - **But what about Mimicry?**



Will shifting focus help?

Process-Level Features

File-Level Features

Process-Level Features

File-Level Features

Detection Components

- Disk activity monitor
- File based behavioral detector
- File recovery module

Detection Components

- Disk activity monitor
- **File based behavioral detector**
- File recovery module

File-level features

- Read/Write data mismatch
- File write ratio
- File read ratio
- Number of Processes Reading or Writing the File
- Number of Operations on the File

File-level features

- **Read/Write data mismatch**
- File write ratio
- File read ratio
- Number of Processes Reading or Writing the File
- Number of Operations on the File

File-level features

- Read/Write data mismatch
- **File write ratio**
- File read ratio
- Number of Processes Reading or Writing the File
- Number of Operations on the File

File-level features

- Read/Write data mismatch
- File write ratio
- **File read ratio**
- Number of Processes Reading or Writing the File
- Number of Operations on the File

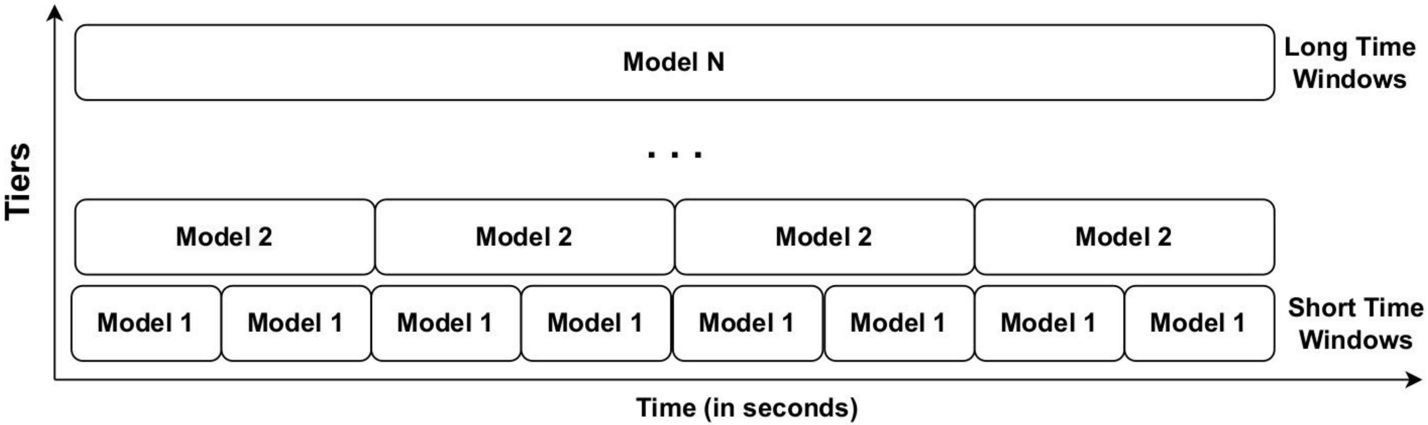
File-level features

- Read/Write data mismatch
- File write ratio
- File read ratio
- **Number of Processes Reading or Writing the File**
- Number of Operations on the File

File-level features

- Read/Write data mismatch
- File write ratio
- File read ratio
- Number of Processes Reading or Writing the File
- **Number of Operations on the File**

Detectors - ShieldFS inspired



Model N

Long Time Windows

. . .

Model 2 | Model 2 | Model 2 | Model 2

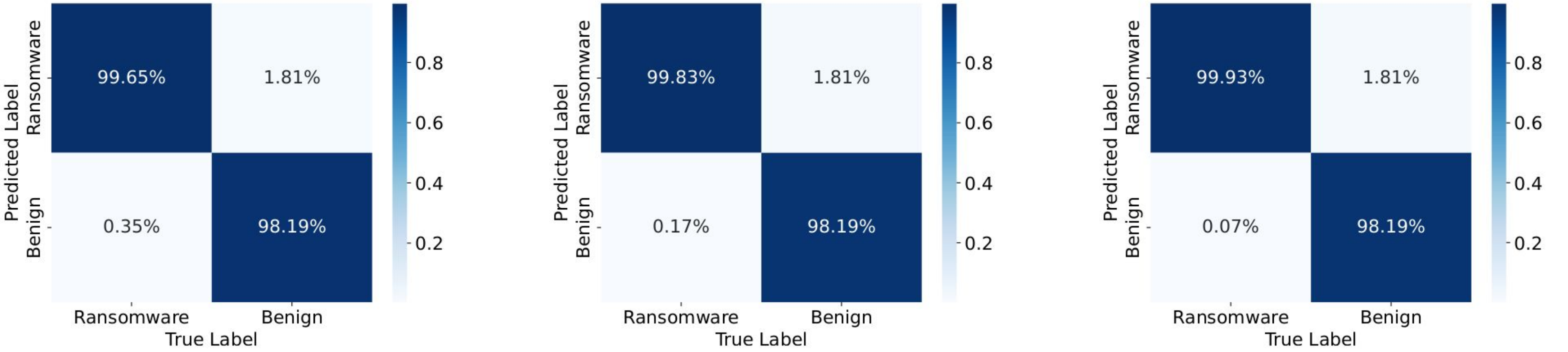
Model 1 | Model 1 | Model 1 | Model 1 | Model 1 | Model 1 | Model 1 | Model 1

Short Time Windows

Tiers

Time (in seconds)

File-centric: How does it perform?



(a) Benign vs. Traditional Ransomware

(b) Benign vs. Evasive Ransomware

(c) Benign vs. Adaptive Ransomware

Reading Material

1. See attached files to this post on Google Classroom.

NOTE: All reading material are included in the oral examination unless specified otherwise.