

Perché i malware continuano a
funzionare e perché non
smetteranno di farlo ancora per
un po'

Aaron Visaggio

Università degli Studi del Sannio

DefenceTech

Cascade

```
C:\DOS cd.  
>  
C:\>DIR /  
: d r w  
o l m e i n d r i e C i s M S D O S _ 5  
V o l u m e o a M u m r i s 1 2 2 - 8 3  
U i u o y \  
r b - 8 0  
[ 0 c . i C O M A N D . C O M I M 0 . 6 C N F I G . S Y S A U 0 X C . B A  
[ f l A D . C O M 0 W  
D A E 9 9 b y t e A 2  
S 3 0 2 e e  
A  
C  
  
0  
0  
  
e  
D e S u N  
T S I t r o C : C C 5 9 8 s  
:\>DIR 7 file(s) 31 555 7 bytes fr 38 0 T E E T
```

ILOVEYOU –
The first
2000's worm





Oops, your files have been encrypted:

English

Payment will be raised on

5/15/2017 15:58:08

Time Left

02:23:58:59

Your files will be lost on

5/19/2017 15:58:08

Time Left

06:23:58:59

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

CMT from Monday to Friday

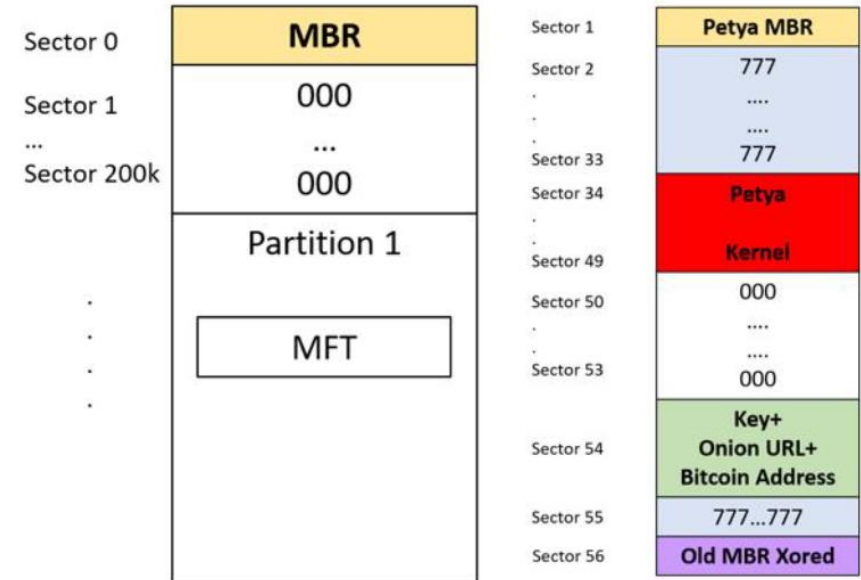
Send \$300 worth of bitcoin to this address:

What they have

- Business Model
- Infrastructure
- Organization

PETYA

- Encrypts the **MFT** (Master File Table) of the **NTFS** filesystem **preventing Windows from booting**
- The **old MBR** is not deleted, but **encrypted** by xoring with the key “7” and **moved** in the sector 56.
- Replaces the **MBR** with the **Petya Bootloader**
- “*NtRaiseHardError()*” -> crash the system in user mode -> reboot -> the machine executes **Petya MBR**



the evolution
after a
couple of
months

- What's new:
 1. It **cyphers** some **user files before** the **reboot** of the machine
 2. It uses the famous and devastating **Eternalblue exploit**, based on a vulnerability of SMB Windows protocol (MS17-010; CVE-2017-0143) -> **worm behavior**.
 3. It **schedules** a **legal reboot** instead of forcing it
 4. It presents a **different user interface** after the reboot.

What they have

- Business Model
- Infrastructure
- Organization
- Ability to (quickly) Evolve

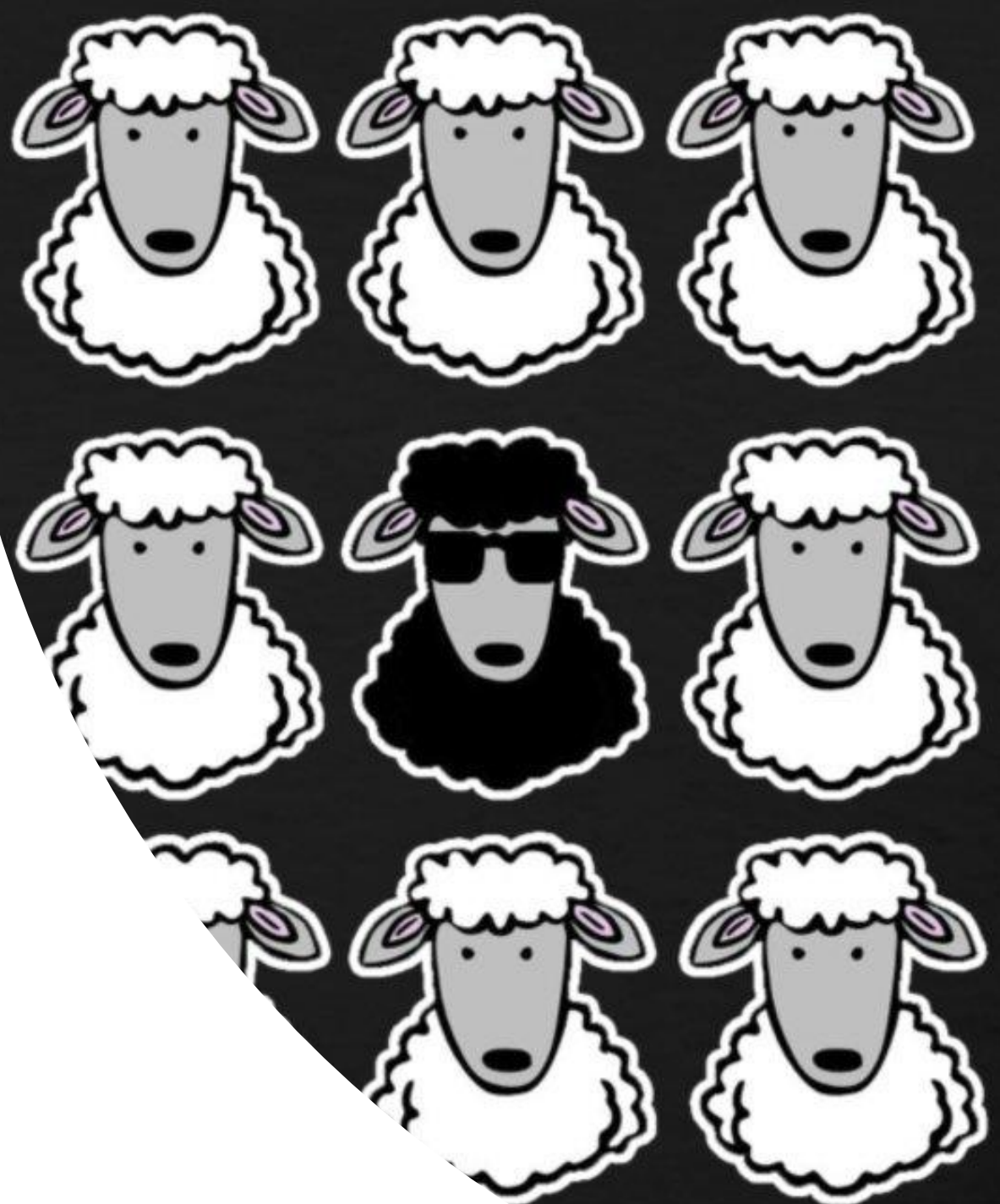
Malware: the bare facts

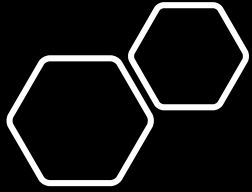
- **7M** new malware juns in jbruary
- **1 billion** malware in the wild
- **Targeted malware** vs automatic generated malware
- **Zero-day** e conceived cyber-arsenals



Malware Analysis con Machine Learning

- **Classification:** it includes two stages, the **model construction** e the **model usage**. The classifier labels the testing set relying on the **model** and the extracted **features**.
- **Clustering:** to group all the malware that shows **similar behaviors**. It helps to define the signatures.

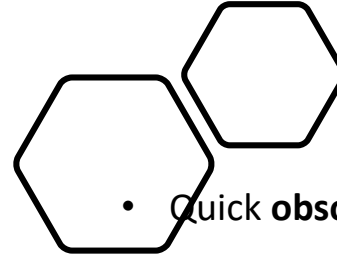




2 biases in malware classification

- ***Spatial bias*** refers to unrealistic assumptions about the ratio of goodware to malware in the data.
- ***Temporal bias*** refers to temporally inconsistent evaluations which integrate future knowledge about the testing objects into the training phase or create unrealistic settings.
- The ***base-rate fallacy*** [Axelsson, 2000] describes how evaluation metrics such as TPR and FPR are misleading in intrusion detection, due to significant class imbalance (most traffic is benign).
- Pendlebury and colleagues [Pendlebury et al., 2019] experimentally verify on a dataset of 129K apps (with 10% malware) that, due to bias, performance can decrease up to 50% in practice in two well-known Android malware classifiers, DREBIN [Arp et al., 2014] and MAMADROID [Mariconti et al., 2017]

Main issues regarding dataset



- Quick **obsolescence** of dataset
- **Incomplete/ imbalanced** coverage of dataset
 - Windows vs Linux/MacOS
 - Android vs IOS
 - Workstation vs SCADA
- **Representativeness** of population
 - IOT is a typical example
- To which extent can we **trust** the dataset?
- How much does the dataset **polarize** the research strategy and goals?

Evasion Techniques

- **Obfuscation** generally hides the code and increases the complexity in order to evade detection (polymorphism, code packing, code encryption and code protection)
 - Difficult to **extract signatures** and **de-obfuscate** the malware code
 - **Packers** are compressed executable with decompressed code and compressed data/payload.
 - It injects the malicious code into live process
 - Avoid reverse engineering
 - **Cryptor** use self-encryption to defend itself.
 - According to Kaspersky 2016 security bulletin, 14,450,434 systems were infected by Cryptor¹.
 - **Protector** is also an obfuscation technique used to perform multiple encryption and decryption to pack the same code using polymorphic encryption scheme
- ¹https://go.kaspersky.com/Global_Security_Bulletin_2016_Stats_SOC_2016.html, 2016.

Motivation

- Over **80%** of **malware** is packed¹ -> to create software that is more difficult to detect
- By creating packers, the cybercriminal can **increase the costs of detecting** the software and hence increase their expected returns.
- Knowing **how** an attacker has **obscured** their software can be the key in any **successful incident handling** exercise involving malware, which is nearly all incidents these days and is only growing worse.



- Over **80%** of malware is packed -> to create software that is more difficult to detect
- By creating packers, the cybercriminal can **increase the costs of detecting** the software and hence increase their expected returns.
- Knowing **how** an attacker has **obscured** their software can be the key in any **successful incident handling** exercise involving malware, which is nearly all incidents these days and is only growing worse.



Dynamic Analysis Evasion

Manual Dynamic Analysis Evasion (Anti-Debugger)

Automated Dynamic Analysis Evasion (Sandbox Evasion)

Detection-Dependent

Detection-Independent

Detection-Dependant

Detection-Independent

Fingerprinting

Traps

Targeted

Debugger-Specific

Control Flow Manipulation

Lockout Attacks

Fileless (AVT) Attacks

Targeted

Fingerprinting

Reverse Turing Test

Stalling

Trigger-based

Fileless (AVT) attacks

What they have

- Business Model
- Infrastructure
- Organization
- Ability to (quickly) Evolve
- Research

GAN

- **GAN:** A GAN is a tool that produces adversarial samples by using the **adversarial machine learning**
- **Adversarial machine learning** has been applied with a certain success especially to the field of image recognition with some surprising results, but also to speech recognition, and biometric recognition.



Genuine Sample


Adversarial Sample

Ian Goodfellow, Patrick McDaniel, and Nicolas Papernot. ***Making machine learning robust against adversarial inputs***. Communications of the ACM, 61(7):56–66, 2018.



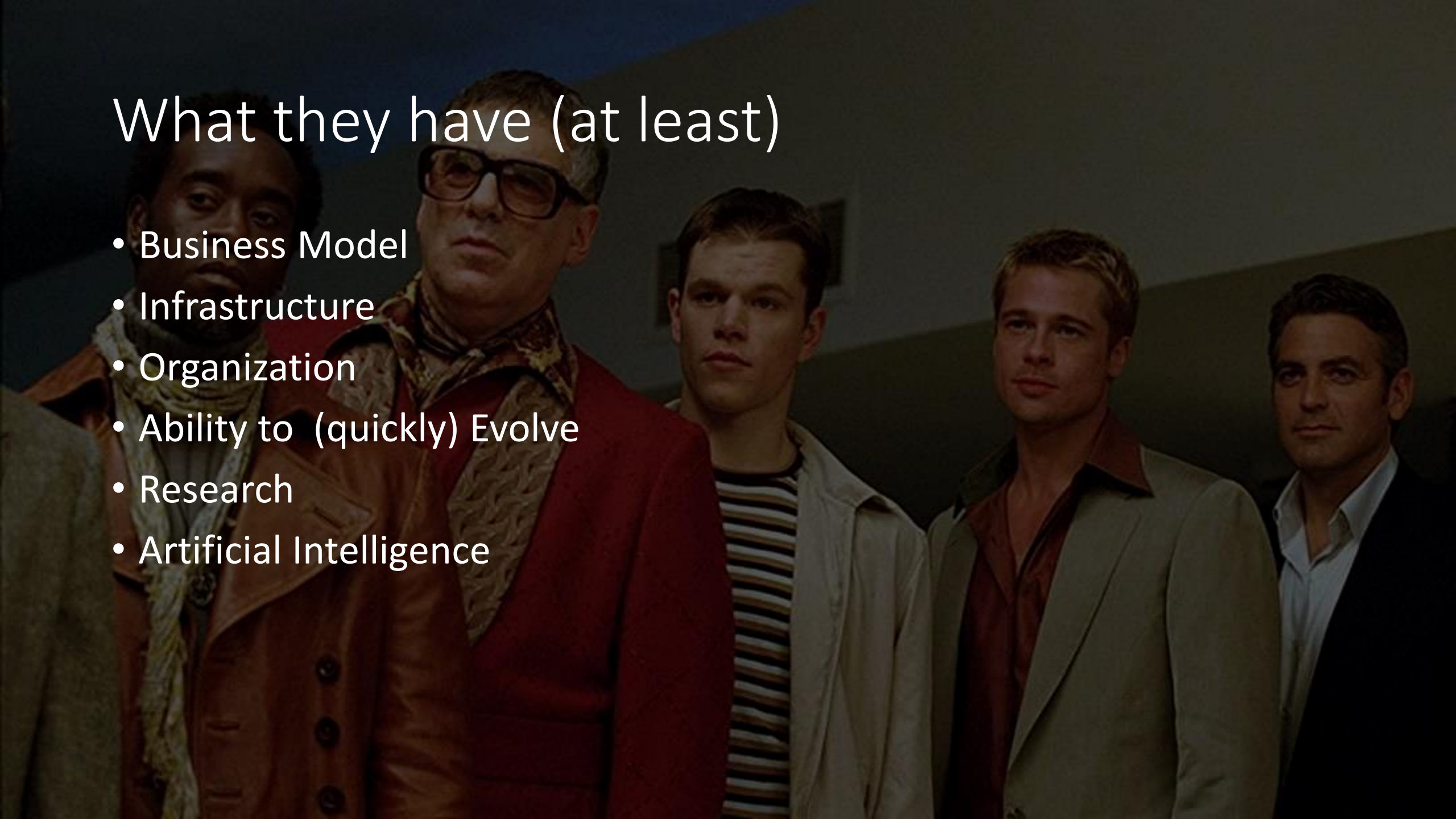
Question is:

how and how much GANs are able to degrade the performance of malware detectors based on machine learning?



What they have (at least)

- Business Model
- Infrastructure
- Organization
- Ability to (quickly) Evolve
- Research
- Artificial Intelligence



Issues

- Butterfly threats
- Infobesity
- Co-evolution
- Tailored Attacks
- Evasive Attacks
- AI-flaws

(Possible) Solutions

- Threat Intelligence Cooperation
- Ability to summarize information
- Investments on Research
- Improve the overall Cyber Posture
- AI-test

