Malware Analysis

Chapter 0: Malware Analysis Primer

王志
zwang@nankai.edu.cn

updated on 5th Sep. 2021

College of Cyber Science
Nankai University

2021/2022

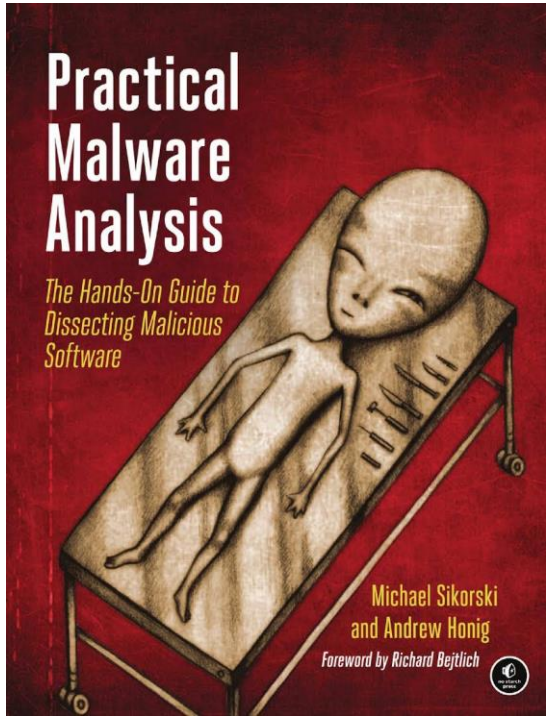
计算机病毒及其防治技术

- 学分：3
- 教学：
  - 2021-2022学年第一学期（1-17周）
  - 星期一 8：00-9：40 ，津南**公教楼**A区114
- 实验：
  - 2021-2022学年第一学期（3-17周）
  - 星期一 12：00-13：40，津南**实验楼**A区210

计算机病毒及其防治技术

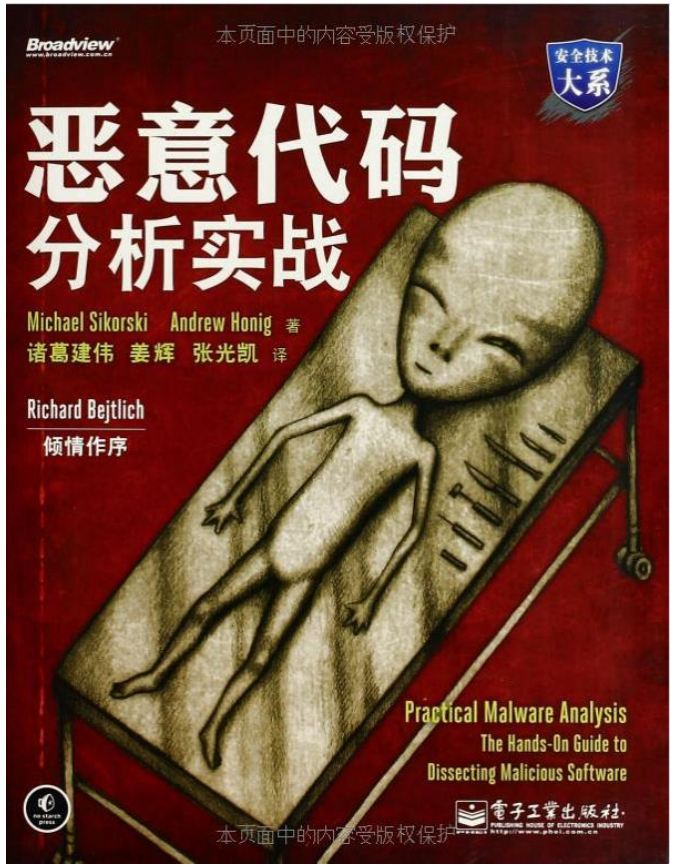
- 授课教师：王志
  - 办公室：网安学院605
  - 邮箱：zwang@nankai.edu.cn

Textbook



- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software
  - Michael Sikorski and Andrew Honig

恶意代码分析实战



课程教材和拓展阅读资料

- 逆向工程核心原理，【韩】李承远 著，武传海 译，人民邮电出版社；
- 加密与解密，段钢 编著，电子工业出版社；
- Intel汇编语言程序设计，Assembly Language for Intel-Based Computers （Fifth Edition），【美】Kip R. Irvine著，温玉杰、梅广宇、罗云彬等译，电子工业出版社；

课程教材和拓展阅读资料

- Practical Reverse Engineering, Bruce Dang, Alexandre Gazet and Elias Bachaalany, Wiley;
- IDA Pro 权威指南（第二版），【美】Chris Eagle 著，石华耀、段桂菊 译，人民邮电出版社
- 有趣的二进制，【日】爱甲健二 著，周自恒 译，人民邮电出版社

学堂在线（xuetangx.com）

南開大學
Nankai University

学堂在线（xuetangx.com）

- （2021秋）计算机病毒分析（慕课）
  - 课前预习视频
  - 课后讨论
  - 课后练习题
  - 实验报告提交

Contents

- PART1: Basic Analysis
  - Chapter1: Basic Static Analysis
  - Chapter2: Malware Analysis in Virtual Machines
  - Chaper3: Basic Dynamic Analysis
  - **++ Yara**

Contents

- PART 2: Advanced Static Analysis
  - Chapter 4: A Crash Course in x86 Disassembly
  - Chapter 5: IDA Pro
  - Chapter 6: Recognizing C Code Constructs in Assembly
  - Chapter 7: Analyzing Malicious Windows Programs
  - **++ IDA Python**

Contents

- PART 3: Advanced Dynamic Analysis
  - Chapter 8: Debugging
  - Chapter 9: OllyDbg
  - Chapter 10: Kernel Debugging with WinDbg
  - **+ Cuckoo**

Contents

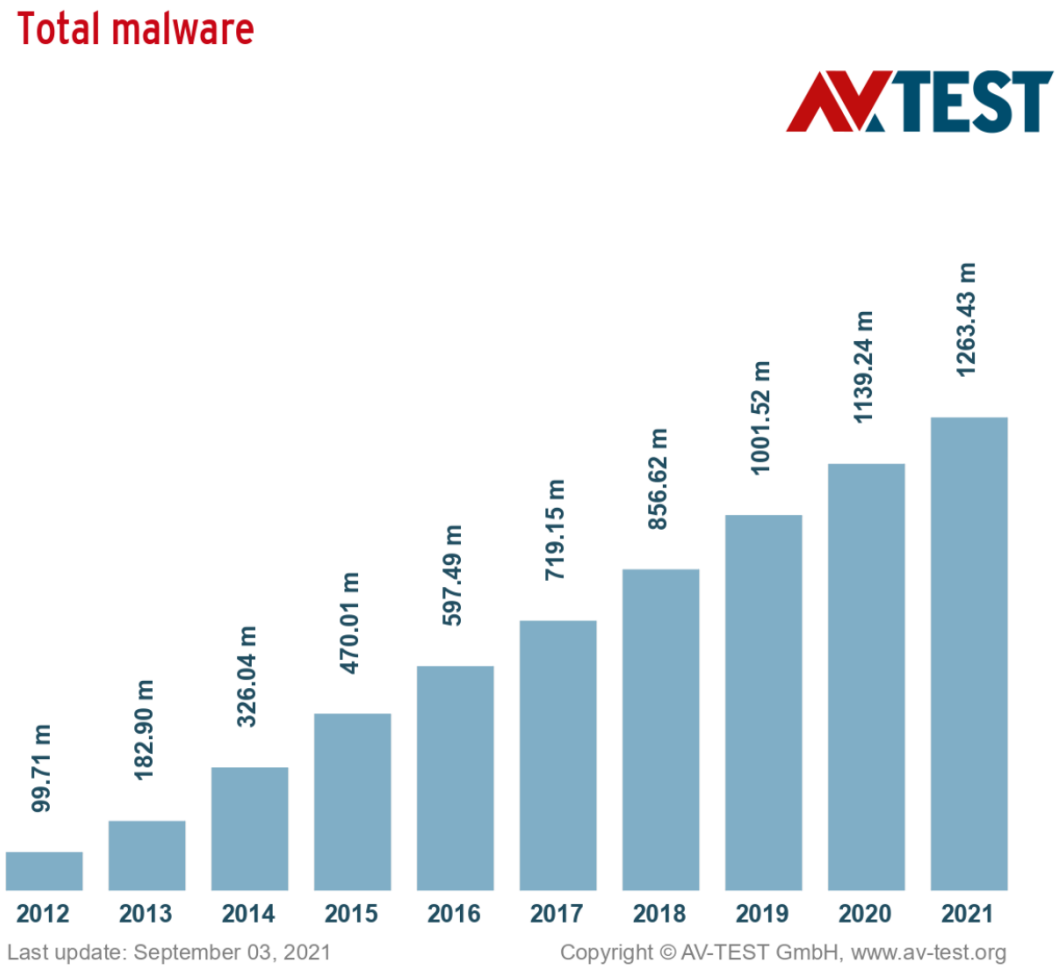
- PART 4: Malware Functionality
  - Chapter 11: Malware Behavior
  - Chapter 12: Covert Malware Launching
  - Chapter 13: Data Encoding
  - Chapter 14: Malware-Focused Network Signature
  - **++ Machine Learning Techniques**

Chapter 0

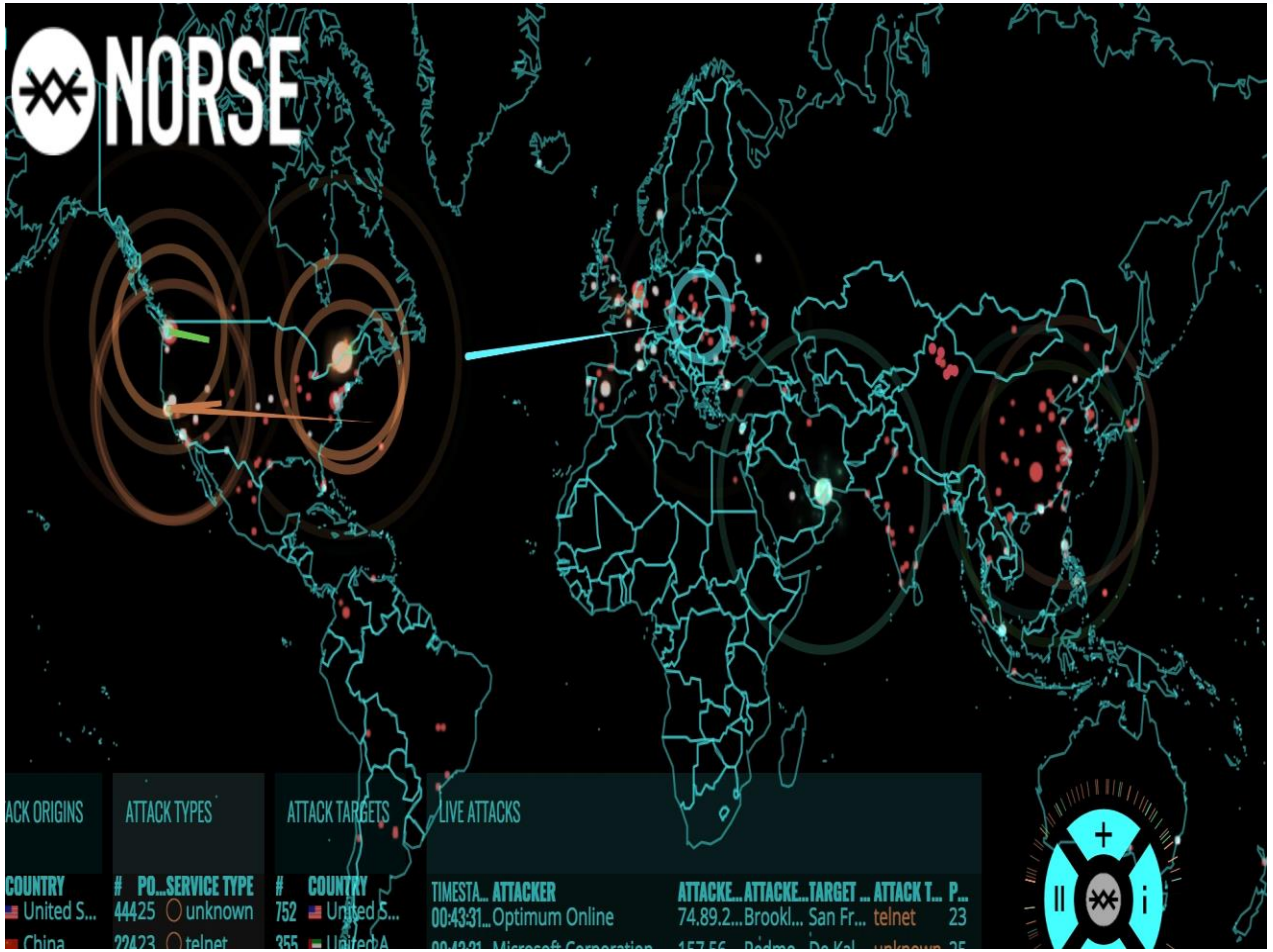
- The goals of malware analysis
- Malware analysis techniques
- Types of Malware
- General rules for malware analysis

The Goals of Malware Analysis

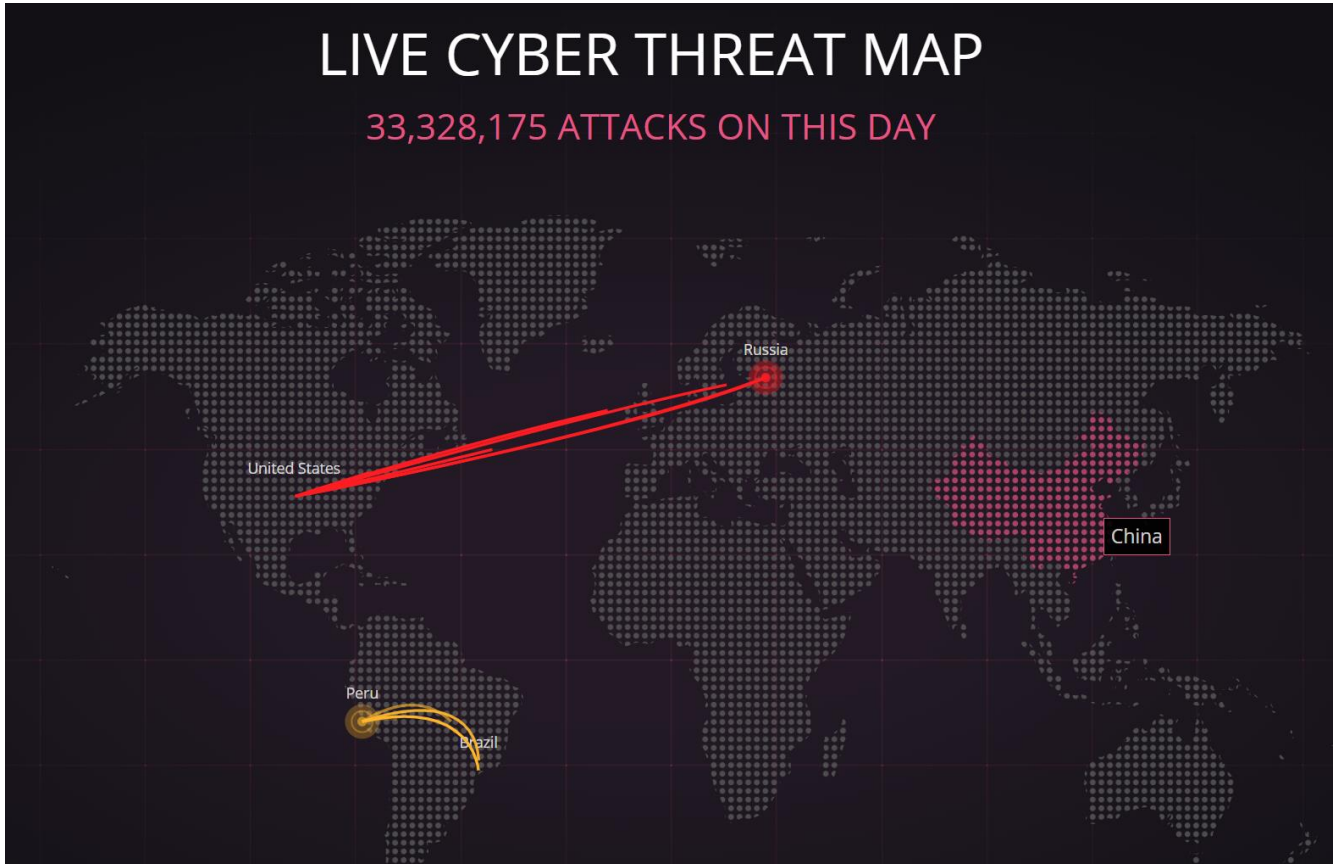
AVTEST Total Malware



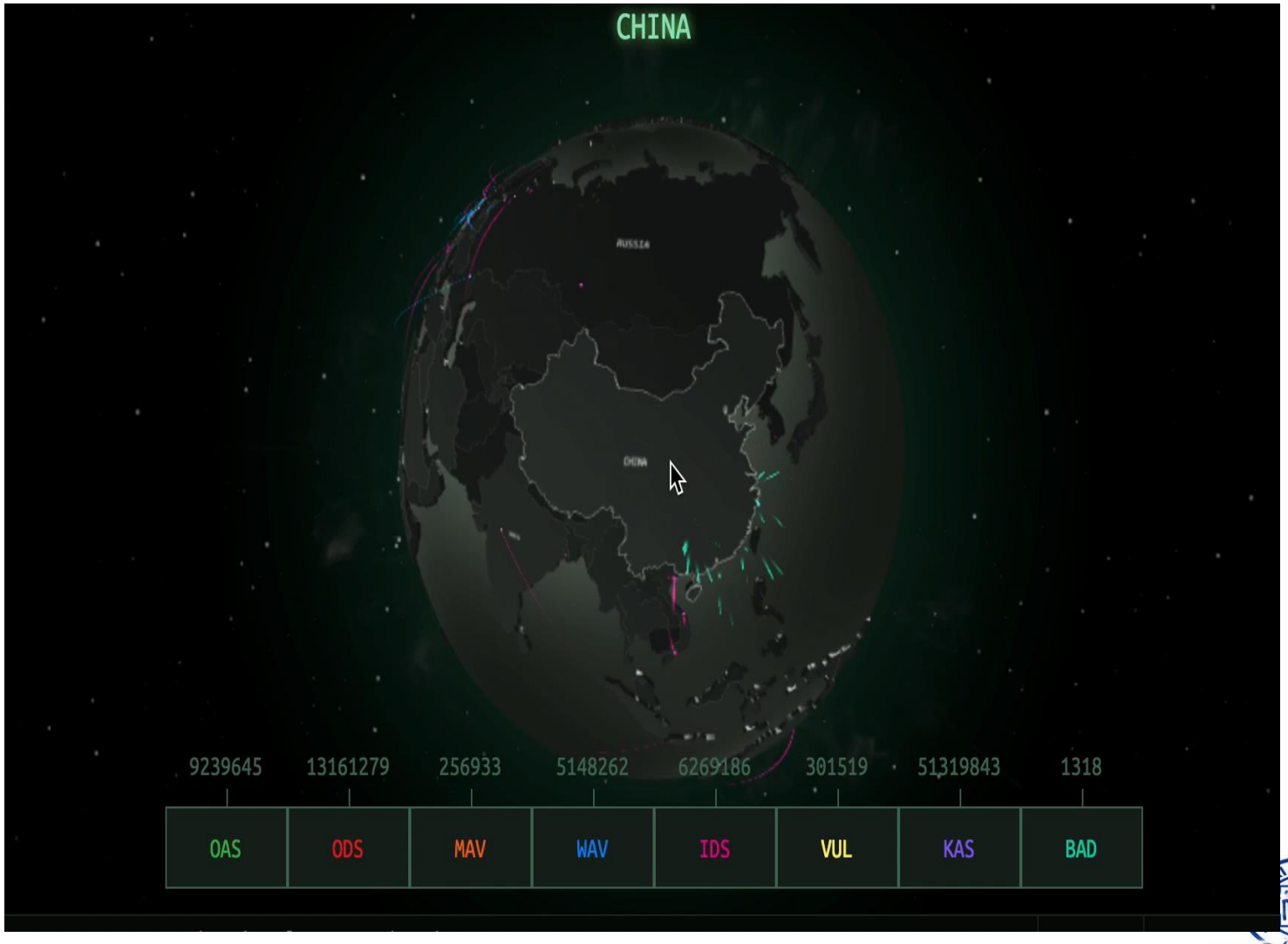
Every day, over 350,000 new malware and potentially unwanted applications.


NORSE
ACK ORIGINS
ATTACK TYPES
ATTACK TARGETS
LIVE ATTACKS
COUNTRY
United S...
PO...SERVICE TYPE
44425 unknown
COUNTRY
752 United S...
TIMESTA... ATTACKER
00:43:31... Optimum Online
ATTACKE... ATTACKE... TARGET ... ATTACK T... P...
74.89.2... Brookl... San Fr... telnet 23

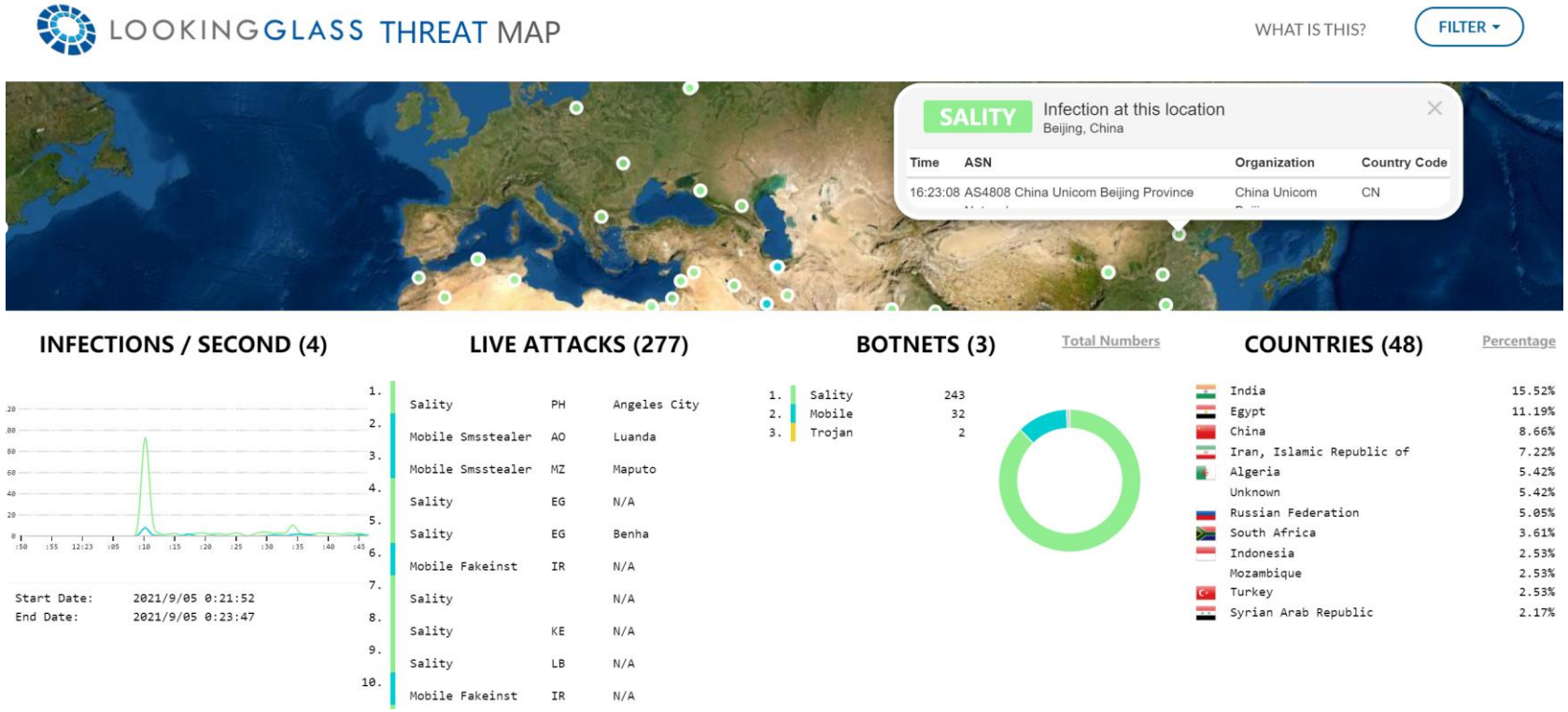
https://threatmap.checkpoint.com/



https://cybermap.kaspersky.com/



https://map.lookingglasscyber.com/



多选题 10分

设置

下面哪些系统或设备可能被计算机病毒感染?

A 计算机、智能手机

B 打印机、网络路由器

C 摄像头、智能家居设备

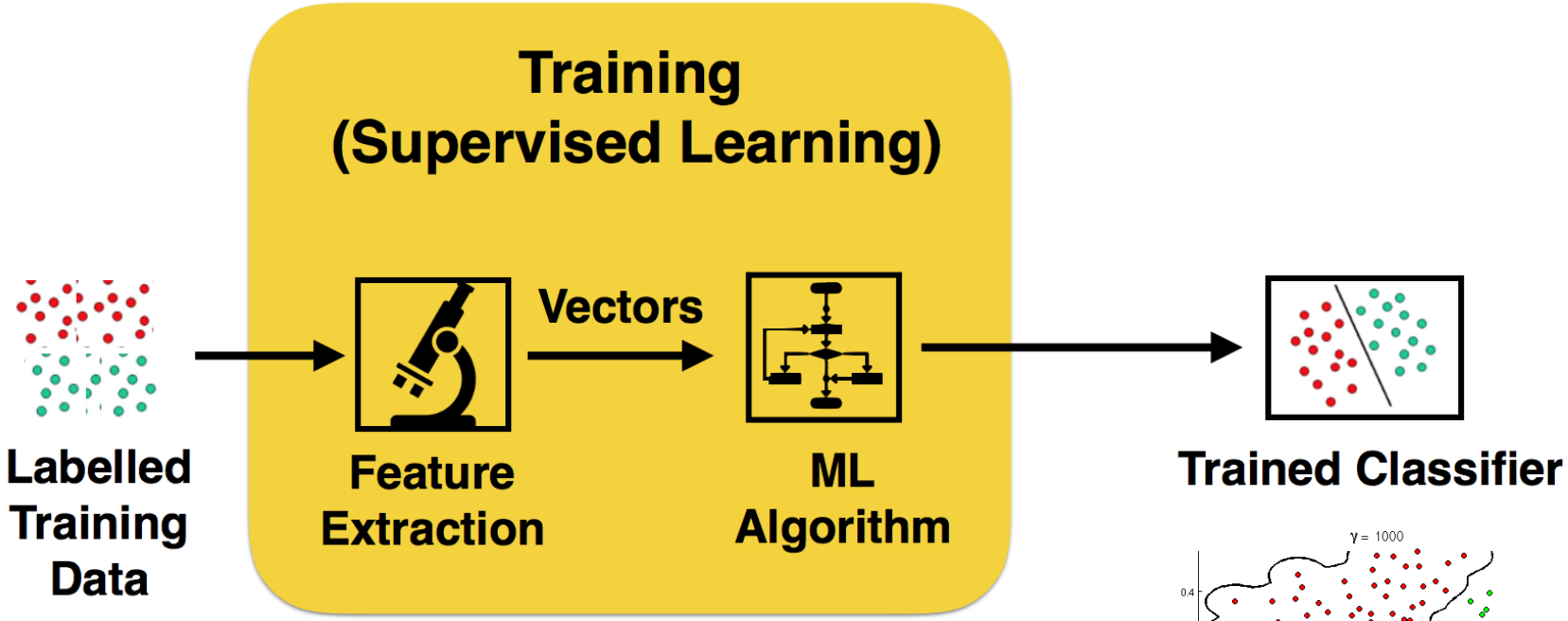
D 智能汽车、智能电网、智慧城市

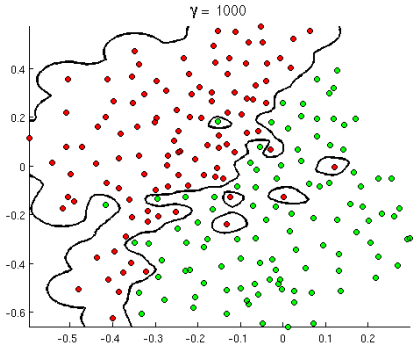
提交

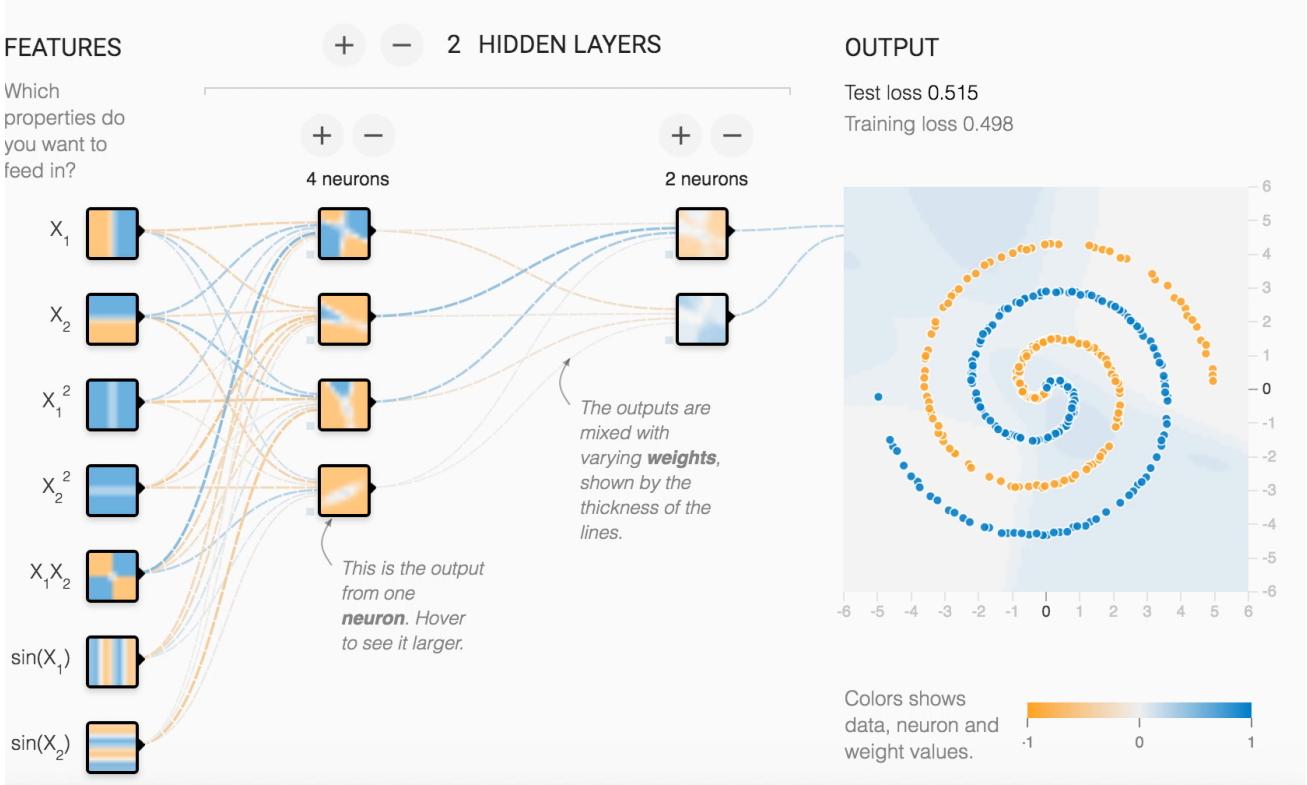

汽车之家 AUTOHOME.COM.CN
SMART HUB

Malware Used as a Cyber Weapon Against Critical Infrastructure

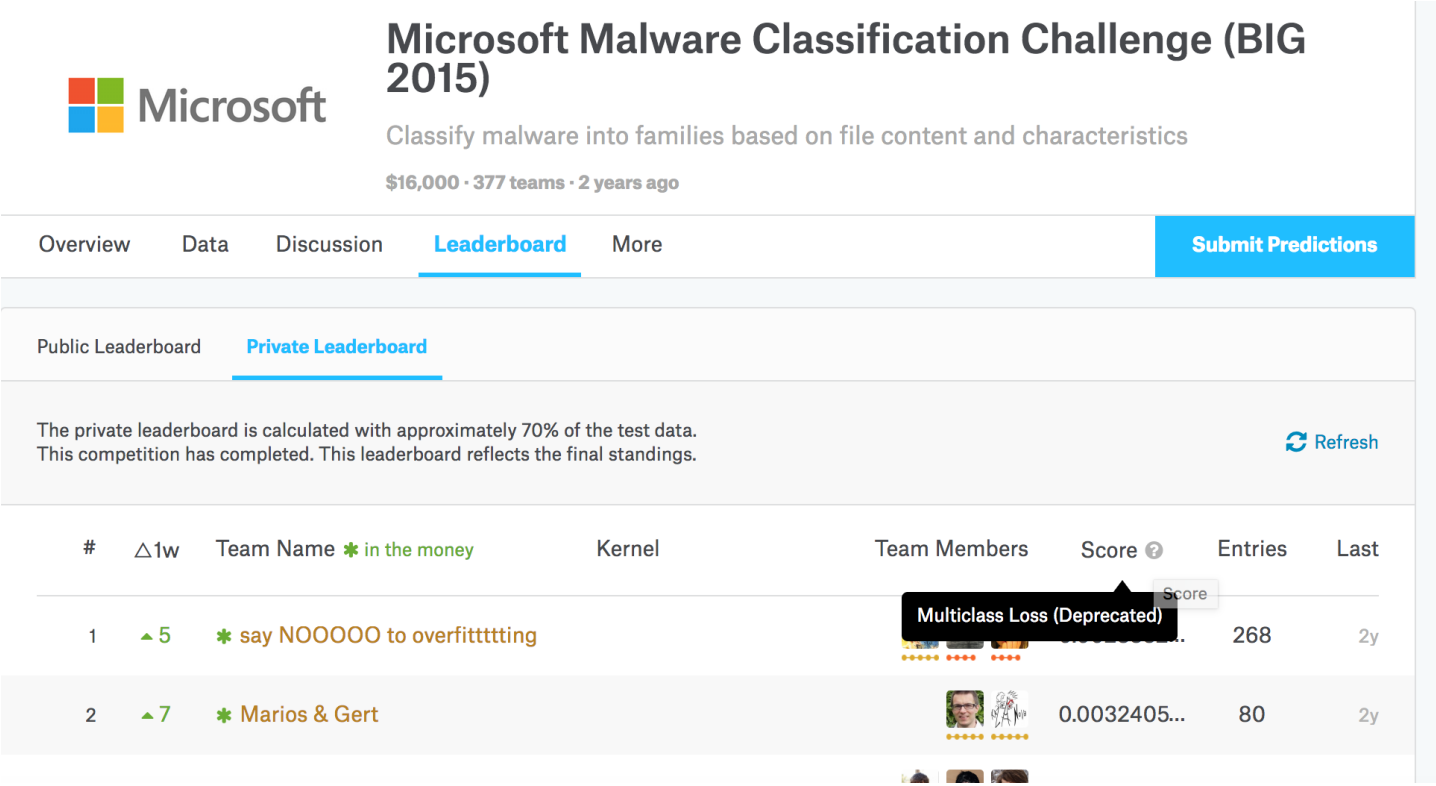
Machine Learning



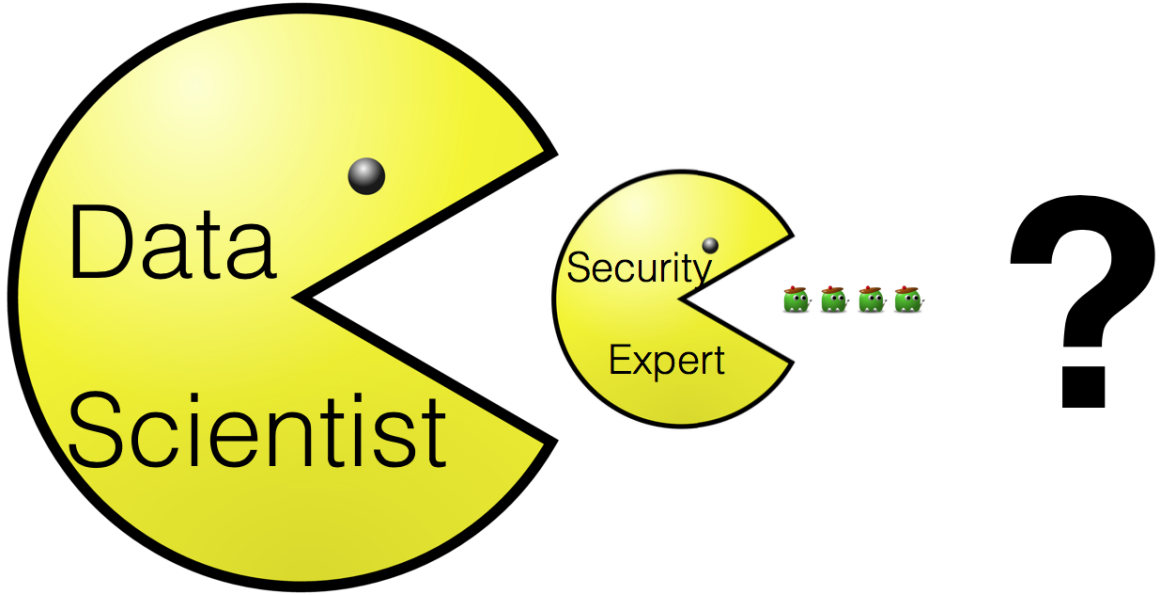



FEATURES
Which properties do you want to feed in?
2 HIDDEN LAYERS
4 neurons
2 neurons
OUTPUT
Test loss 0.515
Training loss 0.498
X1
X2
X1 2
X2 2
X1X2
sin(X1)
sin(X2)
This is the output from one neuron. Hover to see it larger.
The outputs are mixed with varying weights, shown by the thickness of the lines.
Colors shows data, neuron and weight values.
-1
0
1

Machine Learning and Detection Models

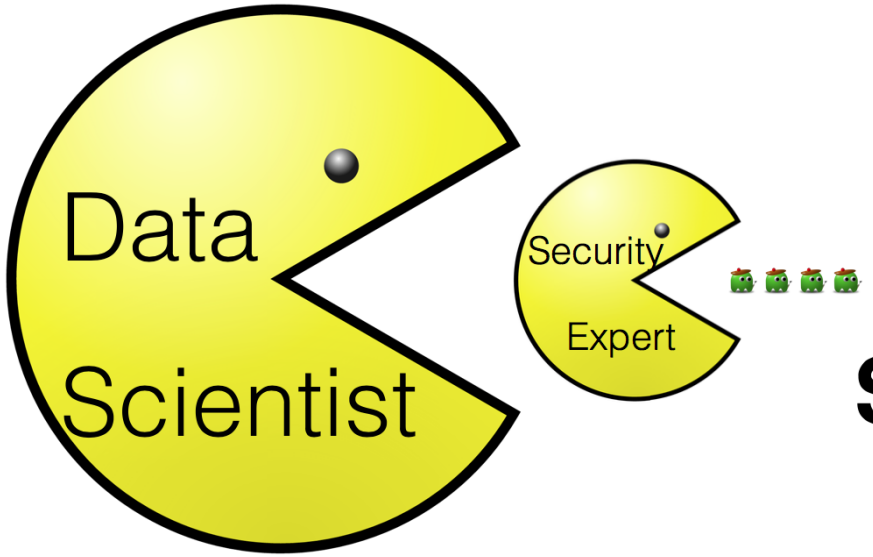


Machine Learning is Eating the World



ML is not a panacea

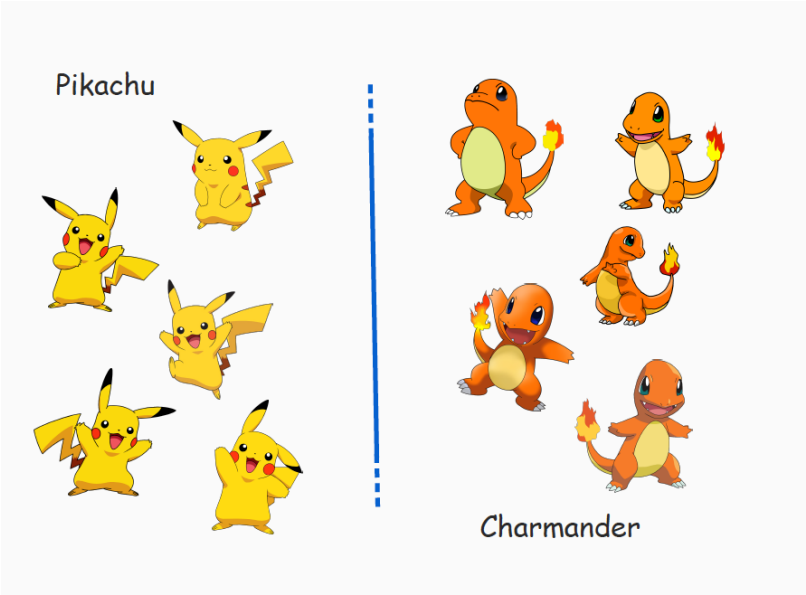
Machine Learning is Eating the World



No!
Security is different.

恶意代码与人工智能系统的博弈

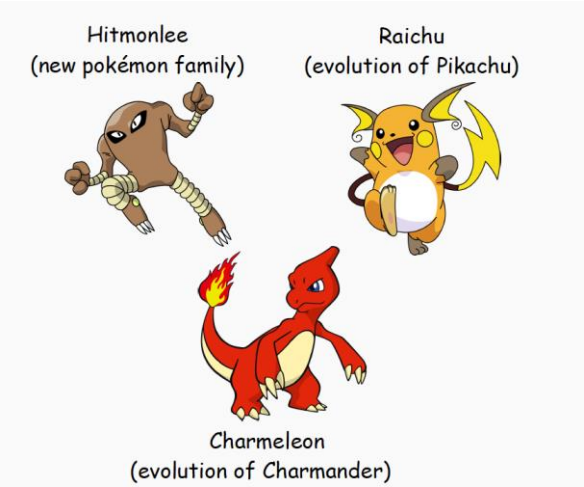
机器学习的前提假设是数据分布具有稳定性



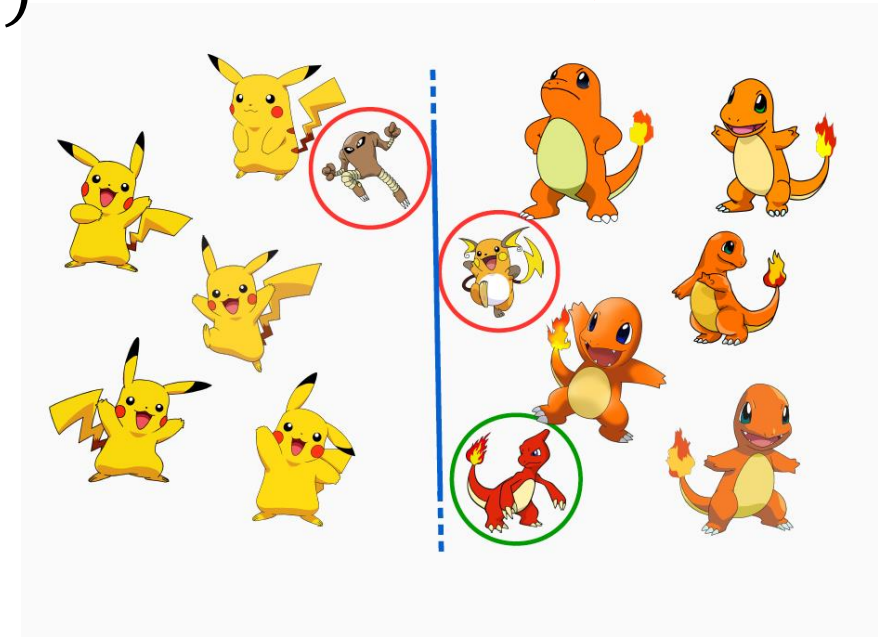
Concept Drift

（概念漂移）

$$\exists x: p_{t_0}(x,y) \neq p_{t_1}(x,y)$$



机器学习加快了计算机病毒的**进化**过程



100% security is not exist

- Polymorphic and Metamorphic
- Mimicry Attack
- Gradient Descent Attack
- Poisoning Attack

The Goals of Malware Analysis

- Exactly what happened
- Ensure you've located all infected machines and files
- Dissect the suspect files
- Find signatures for detection
- Build detection models based on machine learning
- How to measure and contain the damage

Dissecting

- Dissecting malware to understand
  - How it works
  - How to identify it
  - How to defeat or eliminate it
- A critical part of incident response

Signatures

- Host-based signatures
  - Identify files or registry keys on a victim computer that indicate an infection
  - Focus on what the malware did to the system, not the malware itself
    - Different from antivirus signatures
- Network signatures
  - Detect malware by analyzing network traffic
  - More effective when made using malware analysis

Yara引擎

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

Identify and classify malware families based on textual or binary patterns

Malware Analysis Techniques

Malware Analysis Technique

	Static Analysis	Dynamic Analysis
Basic Analysis	Basic Static	Basic Dynamic
Advanced Analysis	Advanced Static	Advanced Dynamic

Static vs. Dynamic Analysis

- Static Analysis
  - Examines malware without running it
  - Tools: VirusTotal, strings, a disassembler like IDA Pro
- Dynamic Analysis
  - Run the malware and monitor its effect
  - Use a virtual machine and take snapshots
  - Tools: RegShot, Process Monitor, Process Hacker, CaptureBAT
  - RAM Analysis: Mandant Redline and Volatility

Basic Analysis

- Basic static analysis
  - View malware without looking at instructions
  - Tools: VirusTotal, strings
  - Quick and easy but fails for advanced malware and can miss important behavior
- Basic dynamic analysis
  - Easy but requires a safe test environment
  - Not effective on all malware

Advanced Analysis

- Advanced static analysis
  - Reverse-engineering with a disassembler
  - Complex, requires understanding of assembly code, constructs, OS concepts
- Advanced Dynamic Analysis
  - Run code in a debugger
  - Examines internal state of a running malicious executable

Types of Malware

Types of Malware

- Backdoor
  - Allows attacker to control the system
- Botnet
  - All infected computers receive instructions from the same Command-and-Control (C&C) server
- Downloader
  - Malicious code that exists only to download other malicious code
  - Used when attacker first gains access

Types of Malware

- Information-stealing malware
  - Sniffers, keyloggers, password hash grabbers
- Launcher
  - Malicious program used to launch other malicious programs
  - Often uses nontraditional techniques to ensure stealth or greater access to a system
- Rootkit
  - Malware that conceals the existence of other code
  - Usually paired with a backdoor

Types of Malware

- Scareware
  - Frightens user into buying something

Fake FBI warning tricks man into surrendering himself for possession of child porn

29 Jul, 2013 | by Nishtha Kanal | Like 3 | +1 0 | Tweet 3 | Share

Here's a weird one. We've heard of viruses and malware bringing harm to computers but in a rare instance, a "ransomware" has brought a positive outcome. A man in the US turned himself in to the police after a pop-up caused by a ransomware informed him that child porn had been identified on his machine.

Jay Matthew Riley, a 21-year-old from Virginia was browsing the Internet, when a pop-up containing an "FBI warning" informed him that it had detected child pornography on his machine. The message went on to tell Riley to pay up a fine online or face the consequences.

Types of Malware

- Spam-sending malware
  - Attacker rents machine to spammers
- Worms or viruses
  - Malicious code that can copy itself and infect additional computers
- Ransomware
  - encrypt victim's data as hostage
  - ask for ransom to recover the data

Types of Malware

- Backdoor: remote access
- Botnet: a army
- Downloader: install other malware
- Lancher: run other malware
- Rootkit: conceal malware
- Worm or Virus: recruit new machines
- Trojan or Ransomware: make money

Mass vs. Targeted Malware

- Mass malware
  - Intended to infect as many machines as possible
  - Most common type
- Targeted malware （APT）
  - Tailored to a specific target
  - Very difficult to detect, prevent, and remove
  - Requires advanced analysis
  - Ex: Stuxnet

General Rules for Malware Analysis

General Rules for Malware Analysis

- Don't Get Caught in Details
  - You don't need to understand 100% of the code
  - Focus on key features
- Try Several Tools
  - If one tool fails, try another
  - Don't get stuck on a hard issue, move along
- Malware authors are constantly raising the bar
  - cat-and-mouse game

General Rules

- If anything is certain, it is that change is certain. The world we are planning for today will not exist in this form tomorrow.

-- Philip Crosby