恶意代码分析与防治技术

王志
zwang@nankai.edu.cn

南开大学网络空间安全学院
2022-2023学年

恶意代码分析与防治技术

- 学分：2.5
- 教学：
  - 2022-2023学年第一学期（4-16周）
  - 星期一 8：00-9：40 ，津南公教楼C区530
- 实验：
  - 2022-2023学年第一学期（6-16周）
  - 星期一 12：00-13：40，津南实验楼A区203、204

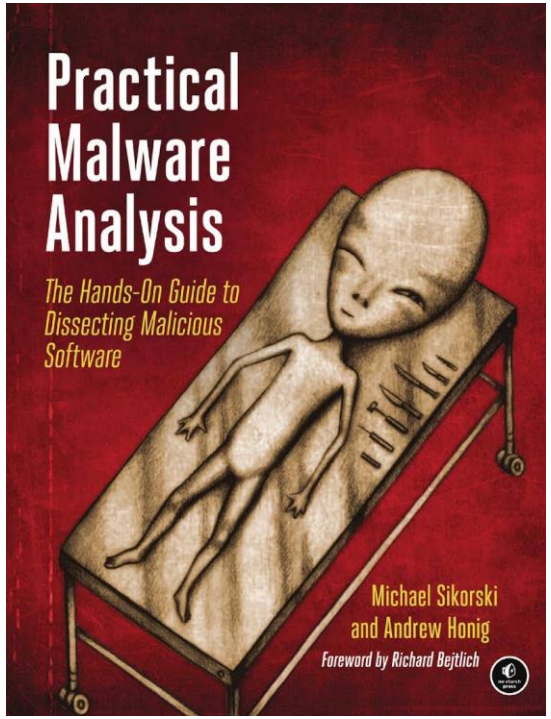
恶意代码分析与防治技术

- 授课教师：王志、邓琮弋
  - 王志，zwang@nankai.edu.cn
  - 邓琮弋，dengcongyi0701@163.com

考试成绩

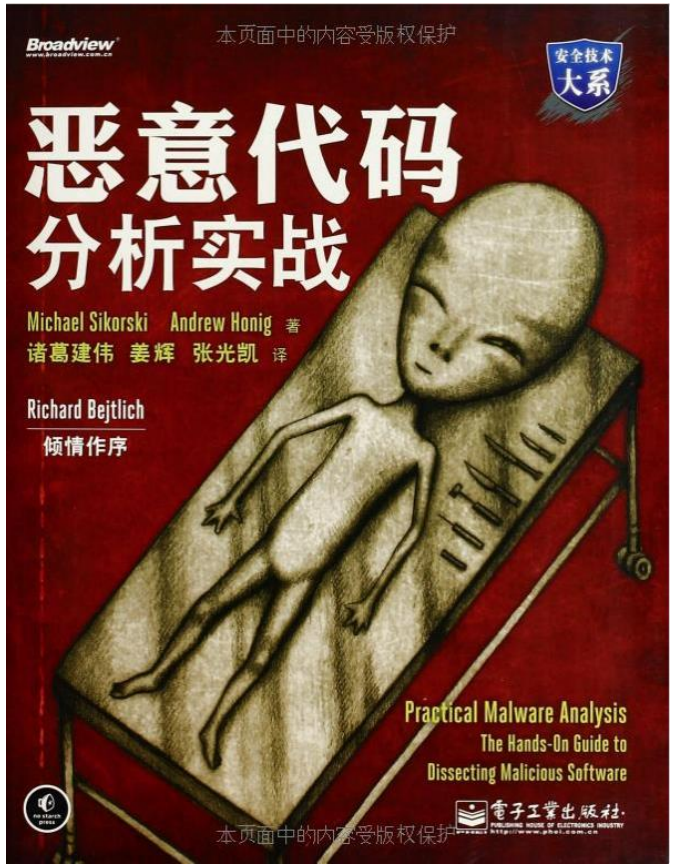
- 平时成绩 25%
  - 考勤、课堂交互、课后讨论、顶会论文阅读与综述
- 实验成绩 25%
  - 实验报告、杀毒软件开发
- 期末考试 50%
  - 闭卷考试

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


Broadview
本页面中的内容受版权保护
安全技术大系
恶意代码
分析实战
Michael Sikorski Andrew Honig 著
诸葛建伟 姜辉 张光凯 译
Richard Bejtlich
倾情作序
Practical Malware Analysis
The Hands-On Guide to
Dissecting Malicious Software
電子工業出版社
本页面中的内容受版权保护

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

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

单选题 1分

设置

恶意代码数量的变化趋势?

A 不断增多

B 逐渐减少

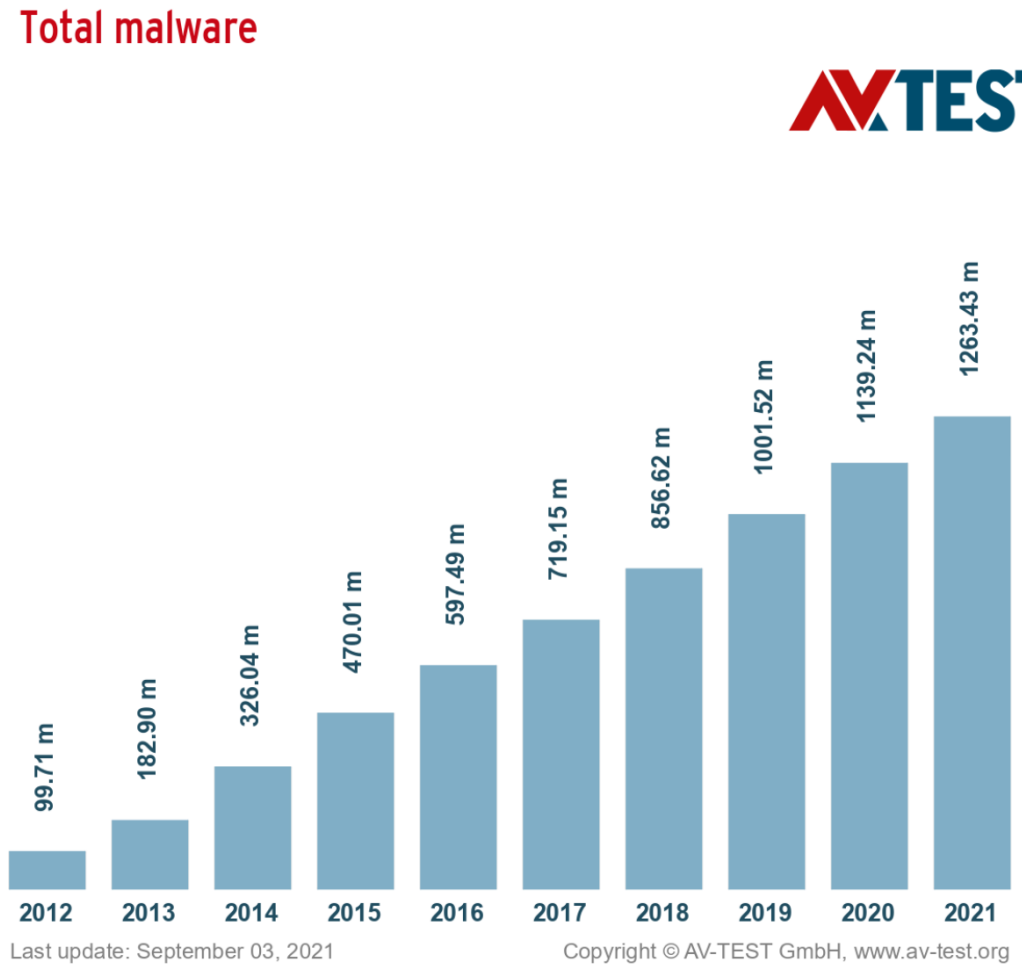
C 保持基本稳定

D 趋于消失

提交

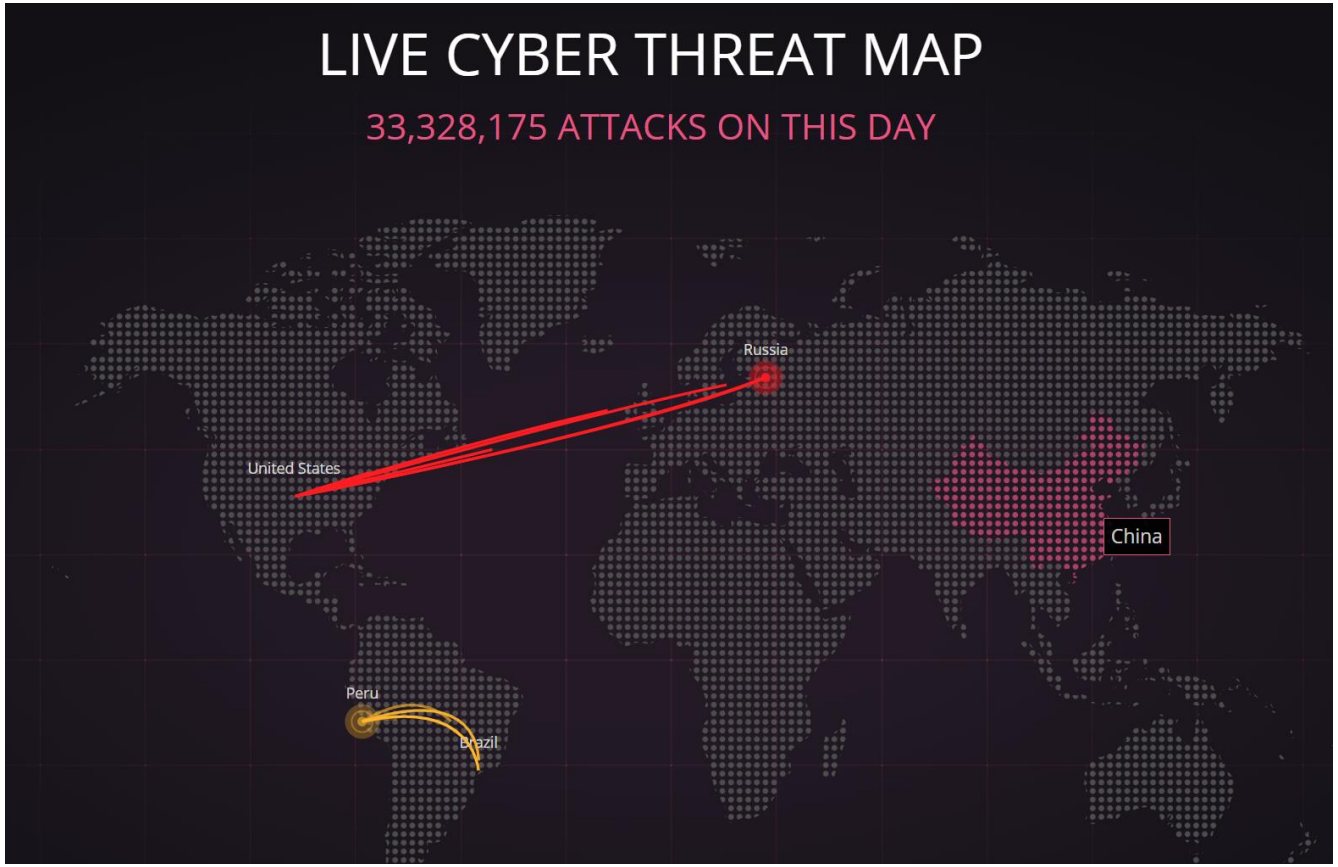
南開大學 Nankai University

AVTEST Total Malware

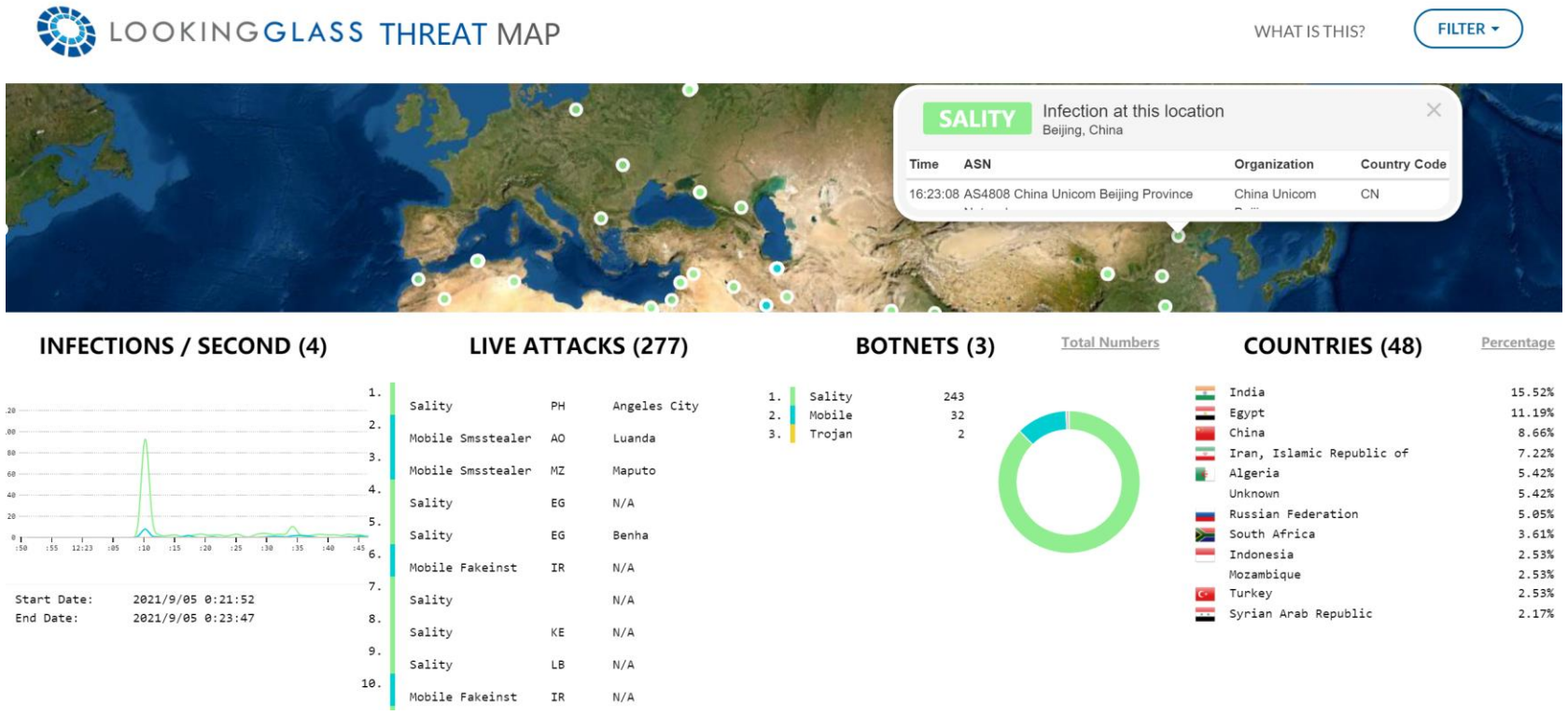


Every day, over 350,000 new malware and potentially unwanted applications.

https://threatmap.checkpoint.com/



https://map.lookingglasscyber.com/



多选题 2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

南開大學 Nankai University


汽车之家 AUTOHOME.COM.CN


SMART HUB

Malware Used as a Cyber Weapon Against Critical Infrastructure

主观题 2分

设置

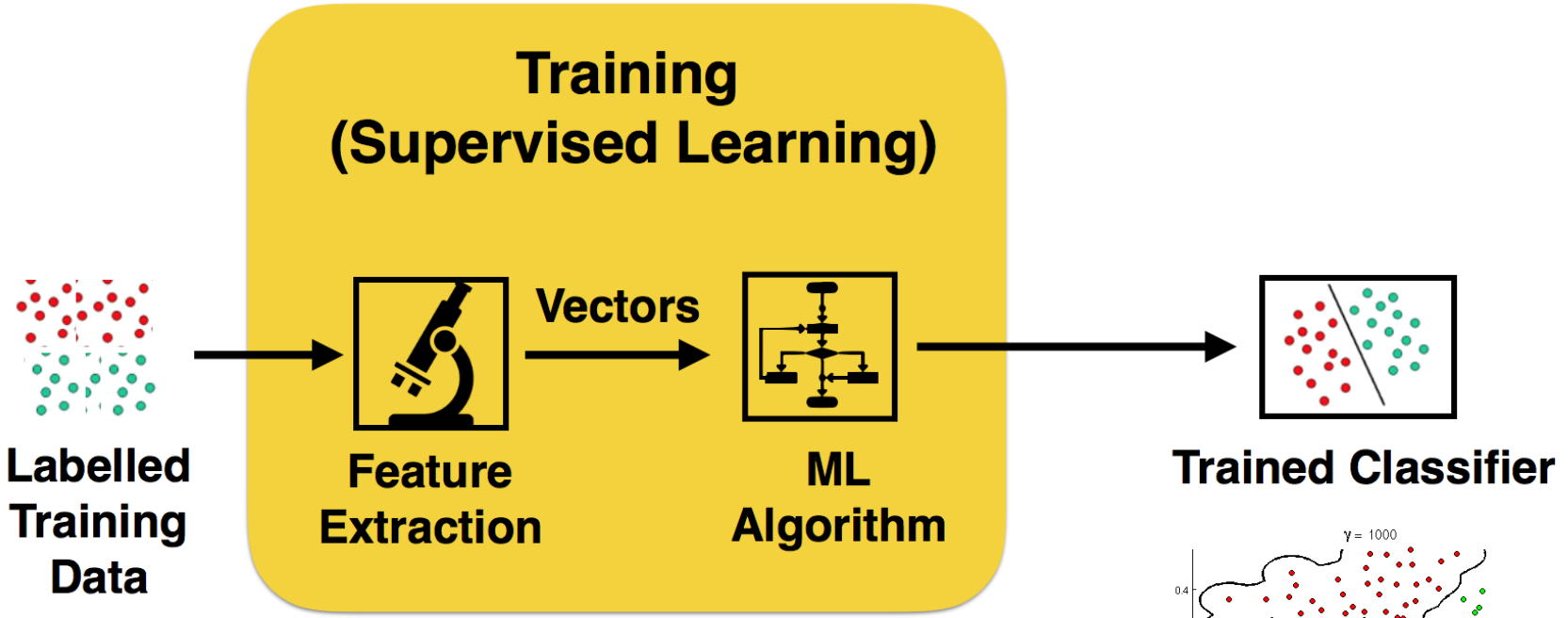
如何对抗每天新出现的海量恶意代码?

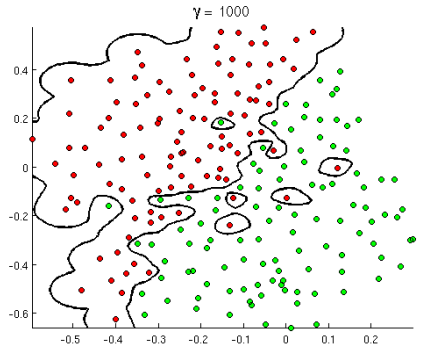
正常使用主观题需2.0以上版本雨课堂

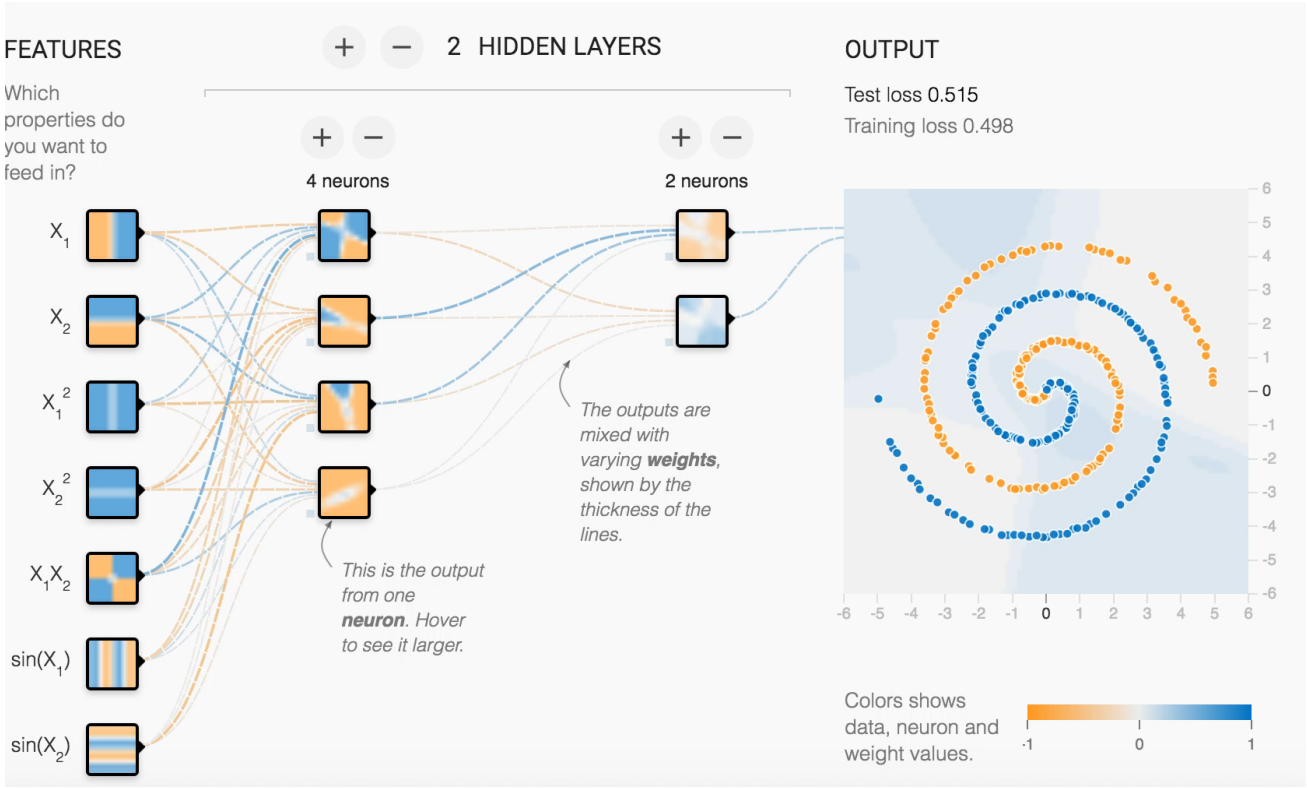
作答

南開大學 Nankai University

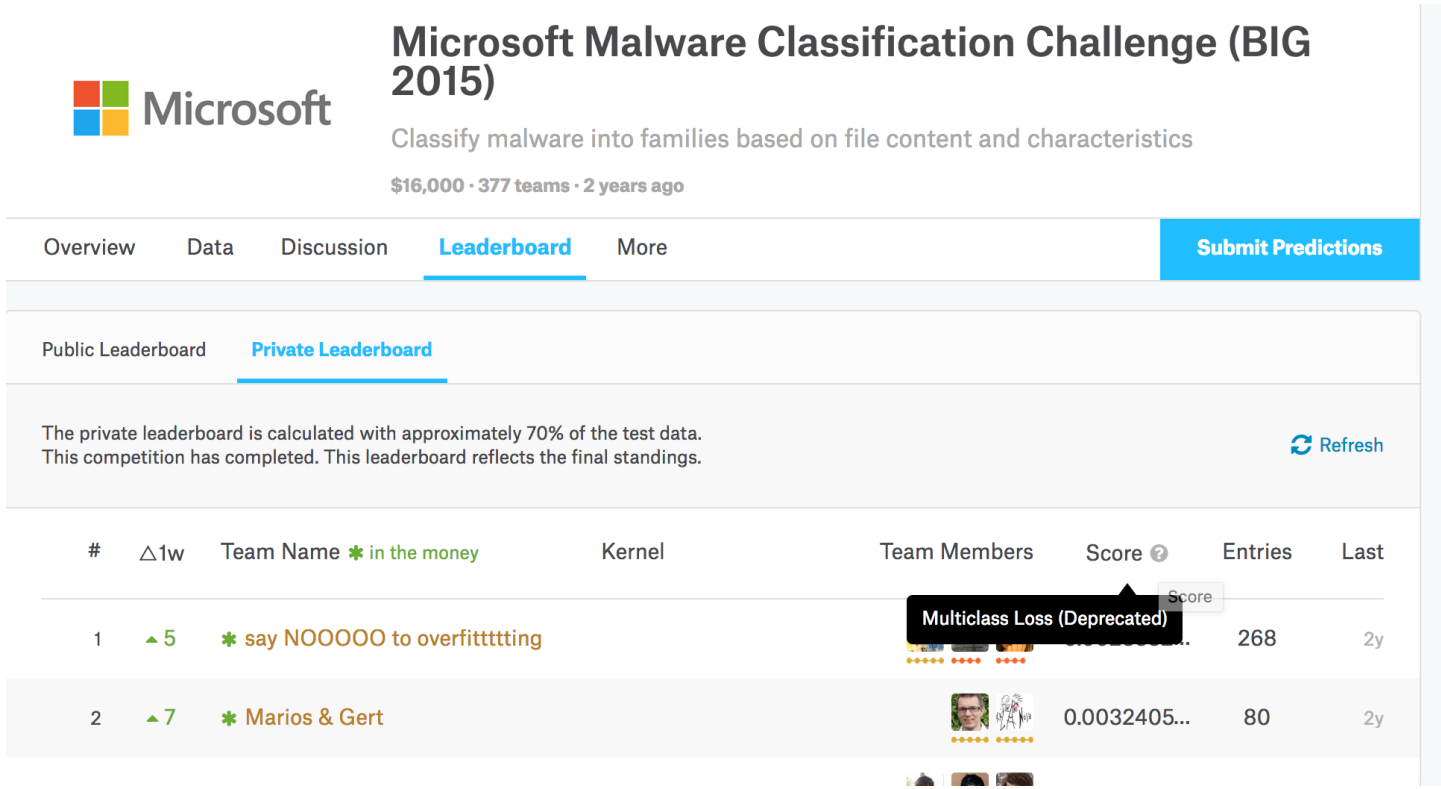
Machine Learning






FEATURES
Which properties do you want to feed in?
2 HIDDEN LAYERS
4 neurons
2 neurons
X1
X2
X1²
X2²
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.
OUTPUT
Test loss 0.515
Training loss 0.498
Colors shows data, neuron and weight values.
-1
0
1

Machine Learning and Detection Models



Microsoft

Microsoft Malware Classification Challenge (BIG 2015)

Classify malware into families based on file content and characteristics

$16,000 · 377 teams · 2 years ago

Overview | Data | Discussion | Leaderboard | More | Submit Predictions

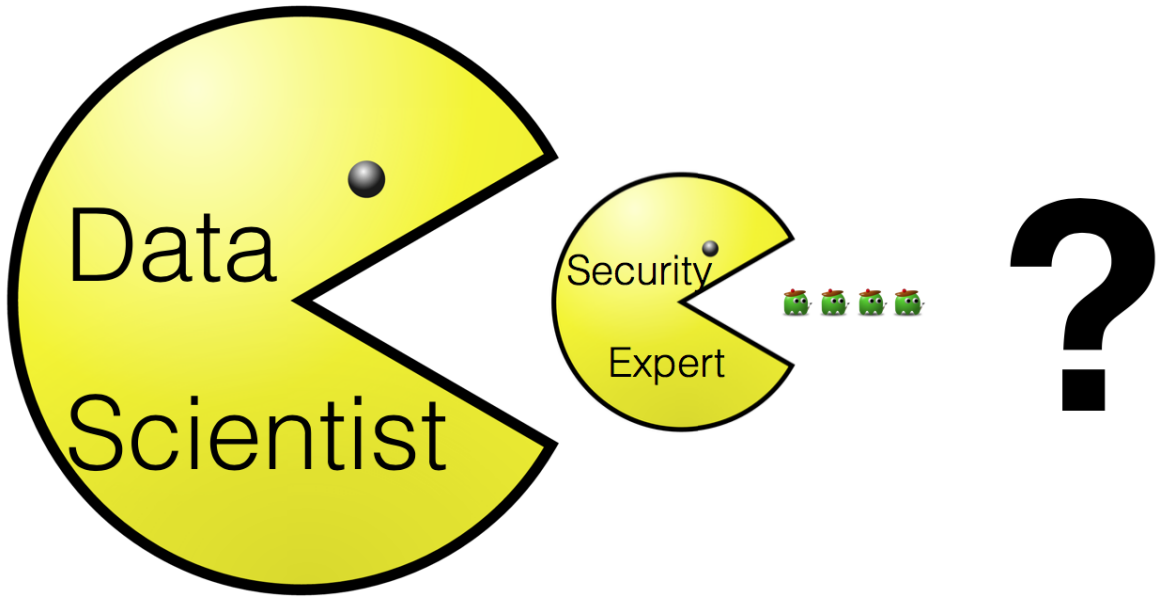
Public Leaderboard | Private Leaderboard

The private leaderboard is calculated with approximately 70% of the test data.
This competition has completed. This leaderboard reflects the final standings.

Refresh

#	△1w	Team Name * in the money	Kernel	Team Members	Score	Entries	Last
1	▲5	* say NOOOOO to overfitttttting			Multiclass Loss (Deprecated)	268	2y
2	▲7	* Marios & Gert			0.0032405...	80	2y

Machine Learning is Eating the World



单选题 2分

设置

数据科学家是否会取代计算机病毒分析工程师?

A 数据科学家会取代计算机病毒分析工程师;

B 数据科学家不能解决计算机病毒问题;

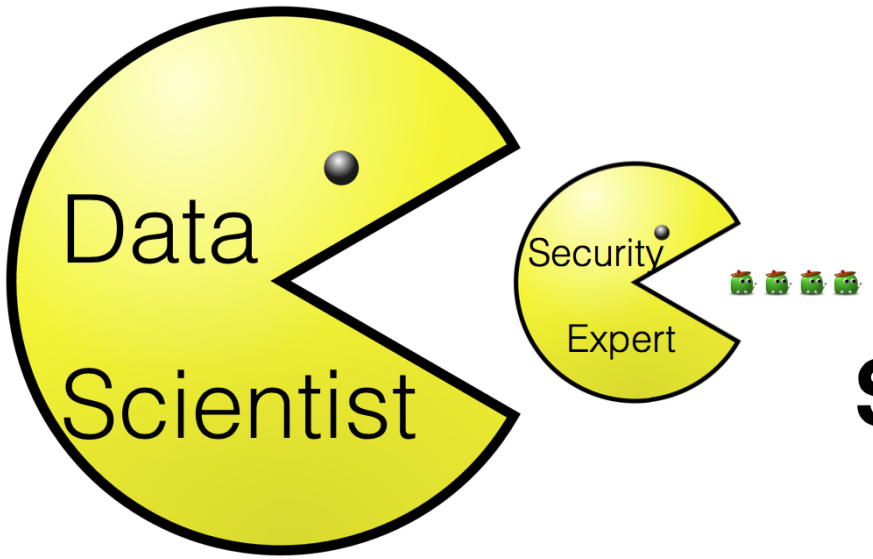
C 网络安全法，震慑了计算机病毒作者，没有人写计算机病毒了;

D 网络安全教育的普及，使计算机病毒威胁越来越小，不需要病毒防治了

提交

ML is not a panacea

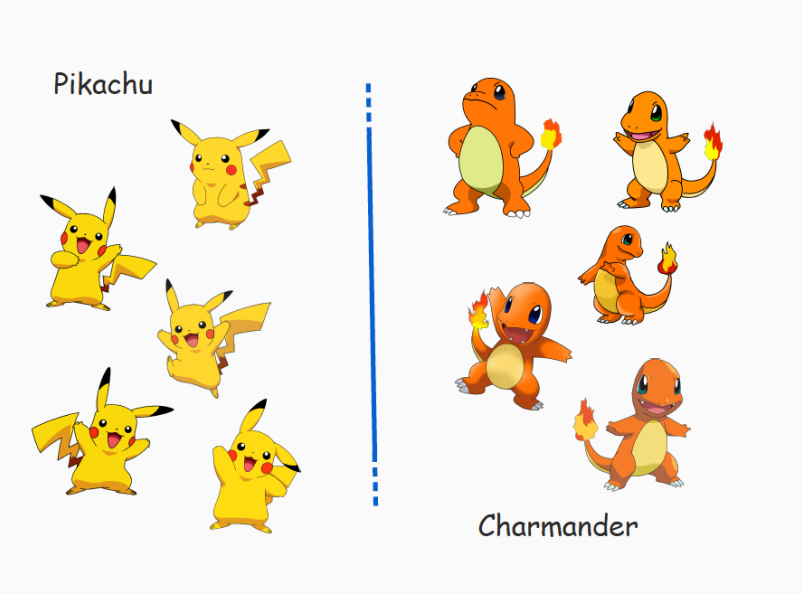
Machine Learning is Eating the World



No!
Security is different.

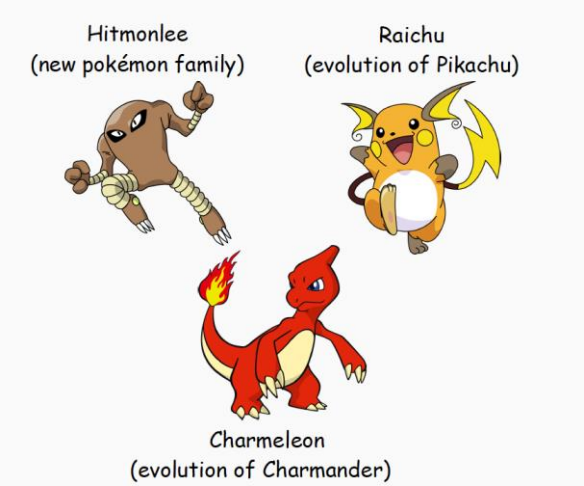
恶意代码与人工智能系统的博弈

机器学习的前提假设是数据分布具有稳定性

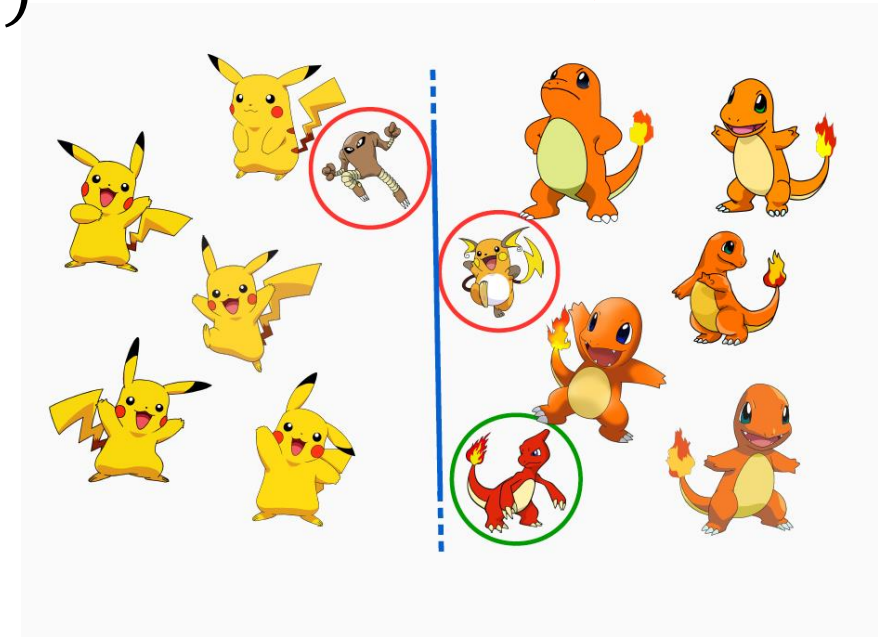


Concept Drift
（概念漂移）

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



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

单选题 1分

设置

以下不是恶意代码分析目标的是（）

A 对可疑程序进行深入分析，确定该程序是否有恶意行为

B 定位被感染的机器或者文件

C 恶意代码的优化和改进

D 衡量并消除恶意代码对系统造成的破坏

提交

投票 最多可选1项

设置

恶意代码分析与恶意代码检测技术是有区别的吗?

A 有区别

B 没有区别

提交

南開大學 Nankai University

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

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

多选题 2分

设置

恶意代码分析技术包括（）

A 基本静态分析，例如virustotal、strings

B 基本动态分析，例如沙箱等

C 高级静态分析，例如IDA Pro等

D 高级动态分析，例如OllyDbg、WinDbg等

提交

Types of Malware

主观题 2分

设置

有哪些恶意代码的类型?

正常使用主观题需2.0以上版本雨课堂

作答

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

Types of Malware

- Scareware
  - Frightens u

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

多选题 2分

设置

以下描述错误的是（）

A Mass恶意代码会尽可能多的感染各种计算机

B APT恶意代码只针对特定的目标进行感染

C Mass恶意代码比APT有更大的威胁，杀毒软件更难检测到

D APT恶意代码可能会“潜伏”很多年不被杀毒软件查杀

提交

南開大學 Nankai University

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

多选题 1分

设置

以下哪些方法是恶意代码分析过程中不建议使用的（）

A 在进入细节分析之前对恶意代码要有一个概要性的理解

B 尝试多从不同角度，使用不同工具和方法来分析恶意代码

C 对全部反汇编指令直接进行逐行分析

D 先使用基本的动态和静态分析工具，定位可疑的静态和动态特征。

提交

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

恶意代码分析与防治技术

王志
zwang@nankai.edu.cn

南开大学网络空间安全学院
2022-2023学年