



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异



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
2023-2024学年

恶意代码分析与防治技术

- 学分：2.5
- 教学：
 - 2023-2024学年第一学期（1-18周）
 - 星期一 8：00-9：40 ，津南**公教楼B**区202
- 实验：
 - 2023-2024学年第一学期（3-18周）
 - 星期一 10：00-11：40，津南**实验楼A**区205





允公允能 日新月异

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, dcy@nankai.edu.cn



南开大学
Nankai University



允公允能 日新月异

考试成绩

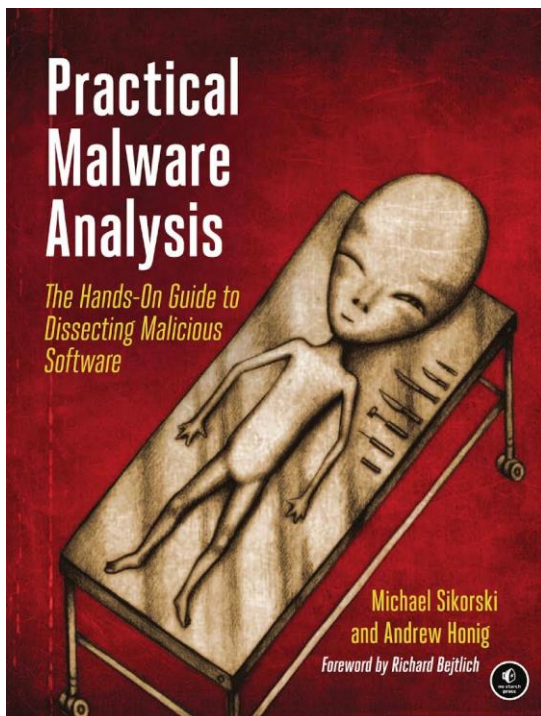
- 平时成绩 20%
 - 考勤、课堂交互、课后讨论、论文阅读与分享
- 实验成绩 30%
 - 实验报告、病毒样本分析
- 期末考试 50%
 - 闭卷考试





允公允能 日新月异

Textbook



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

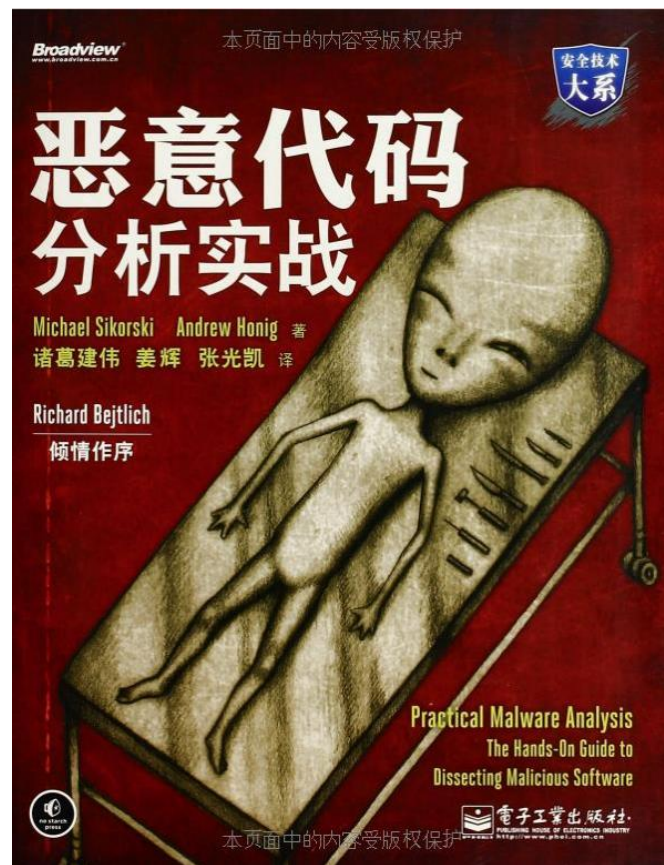


南开大学
Nankai University



允公允能 日新月异

恶意代码分析实战



南开大学
Nankai University

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





允公允能 日新月异

Contents

- PART1: Basic Analysis
 - Chapter1: Basic Static Analysis
 - Chapter2: Malware Analysis in Virtual Machines
 - Chapter3: Basic Dynamic Analysis
 - **++ Yara**





允公允能 日新月异

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
 - BinaryNinja



南开大学
Nankai University



允公允能 日新月异

Contents

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



南开大学
Nankai University



允公允能 日新月异

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**





允公允能 日新月异

Chapter 0

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





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



The Goals of Malware Analysis

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

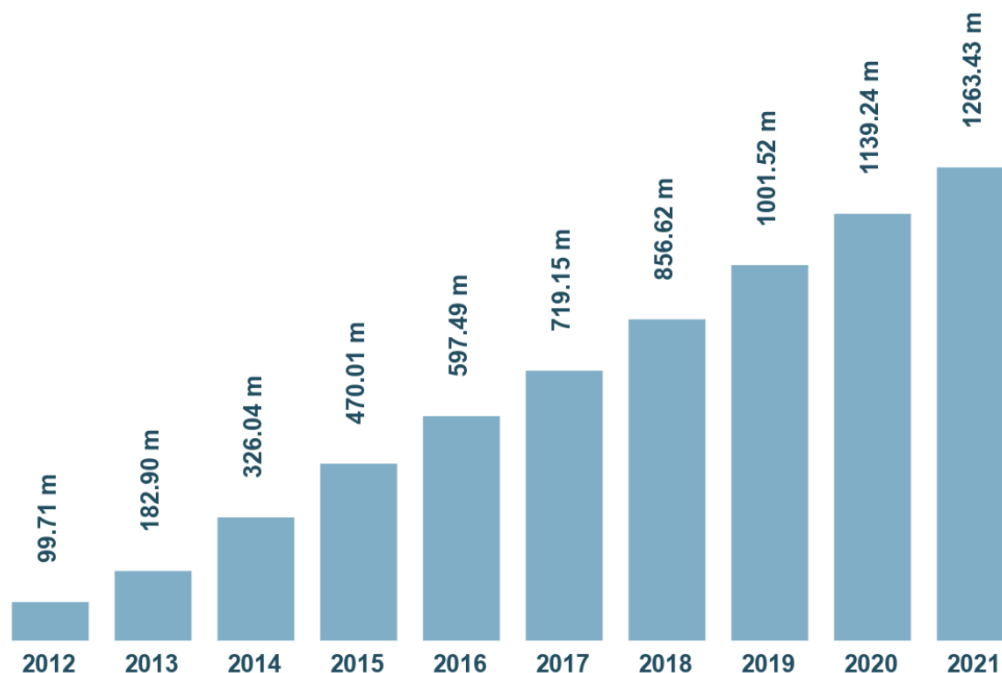




允公允能 日新月异

AVTEST Total Malware

Total malware



Last update: September 03, 2021

Copyright © AV-TEST GmbH, www.av-test.org

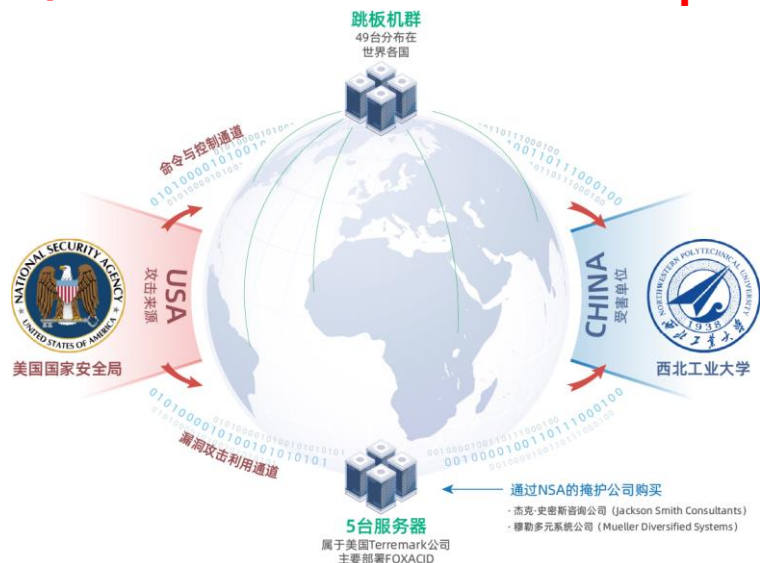
Every day, over
350,000 new
malware and
potentially
unwanted
applications.



南开大学
Nankai University

西北工业大学攻击事件

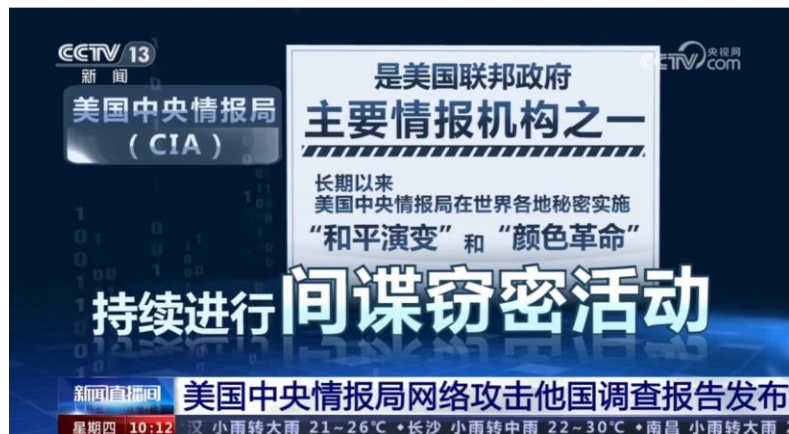
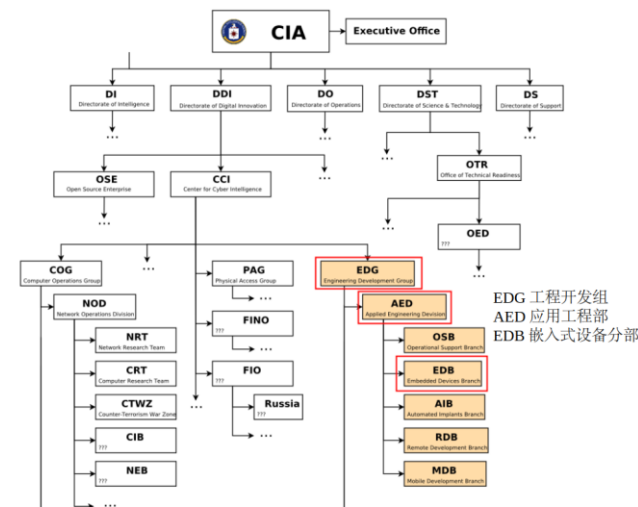
2022年9月5日，国家计算机病毒应急处理中心和**360公司**分别发布了关于**西北工业大学遭受境外网络攻击的调查报告**。调查中，国家计算机病毒应急处理中心和360公司联合组成技术团队，全程参与了此案的技术分析工作。技术团队先后从西北工业大学的多个信息系统和上网终端中提取到了多款木马样本，综合使用国内现有数据资源和分析手段，并得到了欧洲、南亚部分国家合作伙伴的通力支持，全面还原了相关攻击事件的总体概貌、技术特征、攻击武器、攻击路径和攻击源头，初步判明相关攻击活动源自**美国国家安全局（NSA）“特定入侵行动办公室”（Office of Tailored Access Operation，简称TAO）**。



CIA网络攻击调查报告



“美国中央情报局紧密关联的木马程序、功能插件和攻击平台样本。这些相关网络武器都进行了极其严格的**规范化、流程化和专业化**的软件工程管理，而目前只有美国中央情报局严格遵守这些**标准**和**规范**开发网络攻击武器。”--CCTV新闻直播间



“各种攻击手法**前后呼应、环环相扣**，现已覆盖全球几乎所有互联网和物联网资产，可以随时随地控制别国网络，盗取别国重要、敏感数据，而这无疑需要**大量的财力、技术和人力资源**支撑”-CCTV新闻直播间



武汉地震检测中心遭攻击事件

8月14日针对武汉市应急管理局地震监测中心的网络攻击事件，**国家计算机病毒应急处理中心和360公司组成的联合调查组**已取得新进展，发现了符合美国情报机构特征的后门恶意软件。

联合调查组已经在受害单位的网络中发现了技术非常复杂的后门恶意软件，符合美国情报机构特征，**具有很强的隐蔽性**，并且通过恶意软件的功能和受影响的系统判断，攻击者的目的是窃取地震监测相关数据，而且具有明显的军事侦察目的。



“这些传感器所感知采集的综合震动声波数据，尤其是次声波数据，对研判地质地形、分析武器系统试验、核试验等均有重要情报价值。”——全国政协委员，安天集团董事长、首席技术架构师肖新光



以下那一场战争运用了网络攻防对抗技术？

- ☒ A 海湾战争
- ☒ B 科索沃战争
- ☐ C 第二次世界大战
- ☒ D 俄乌战争

提交



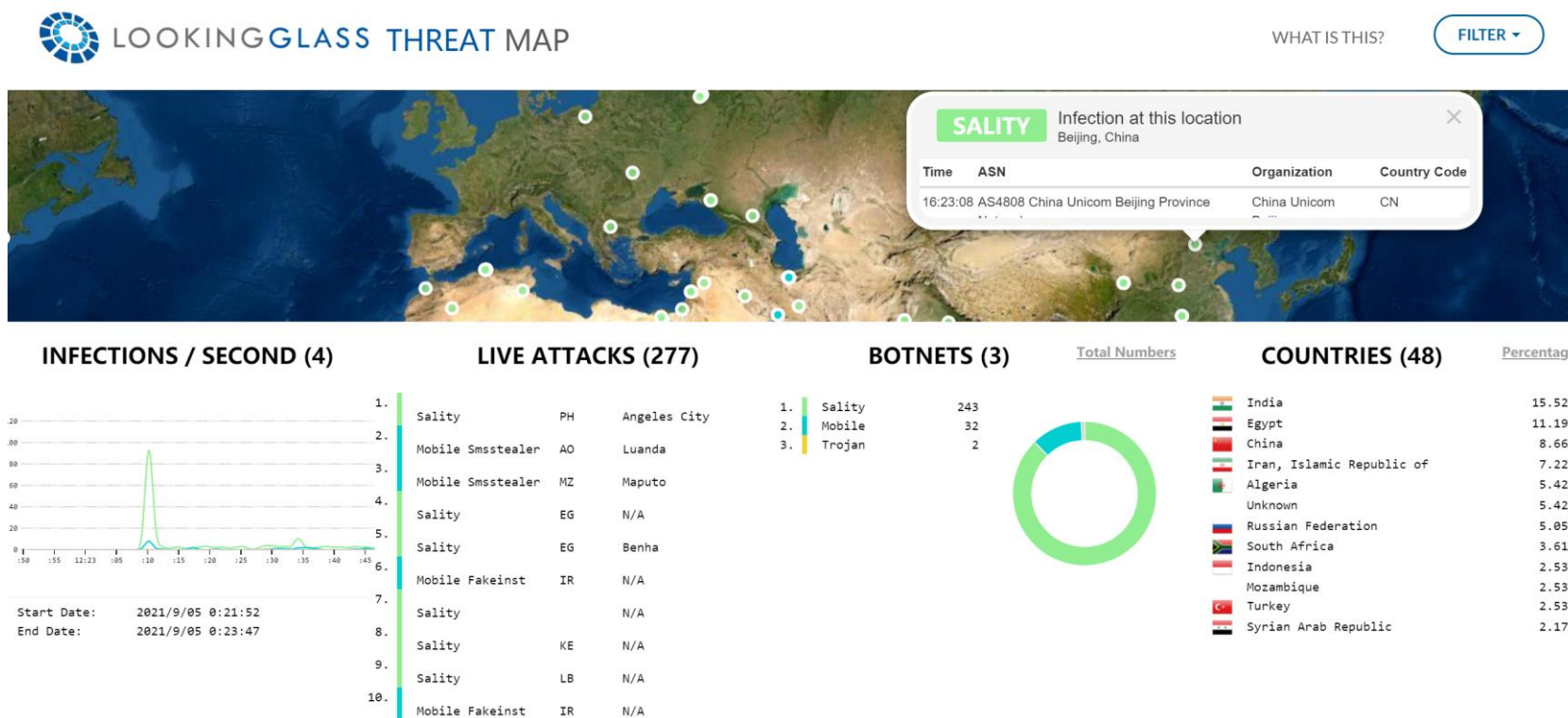
允公允能 日新月异

<https://threatmap.checkpoint.com/>



南开大学
Nankai University

<https://map.lookingglasscyber.com/>



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





允公允能 日新月异



南开大学
Nankai University

允公允能 日新月异

Malware Used as a Cyber Weapon Against Critical Infrastructure



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

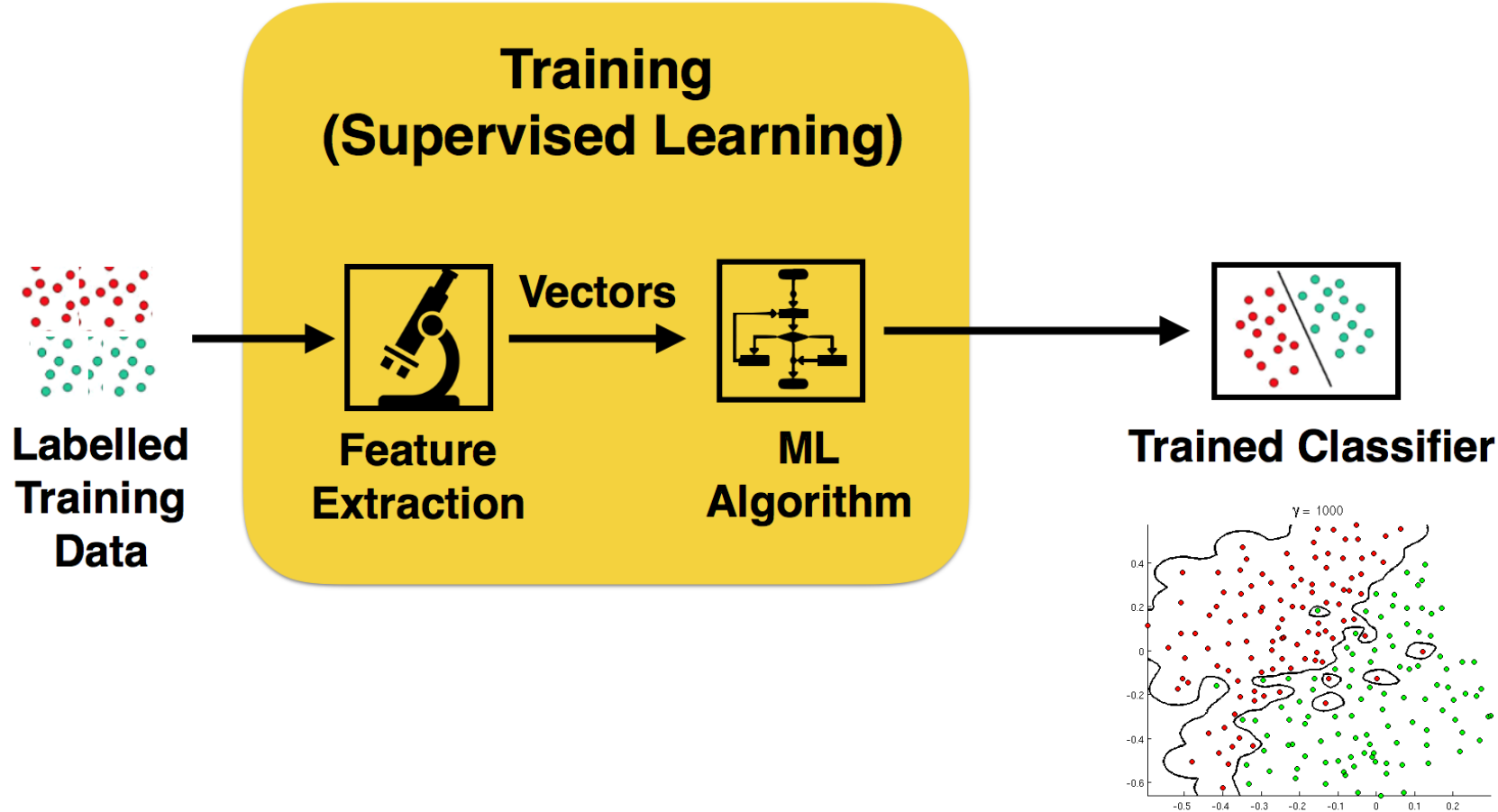
作答



南开大学
Nankai University

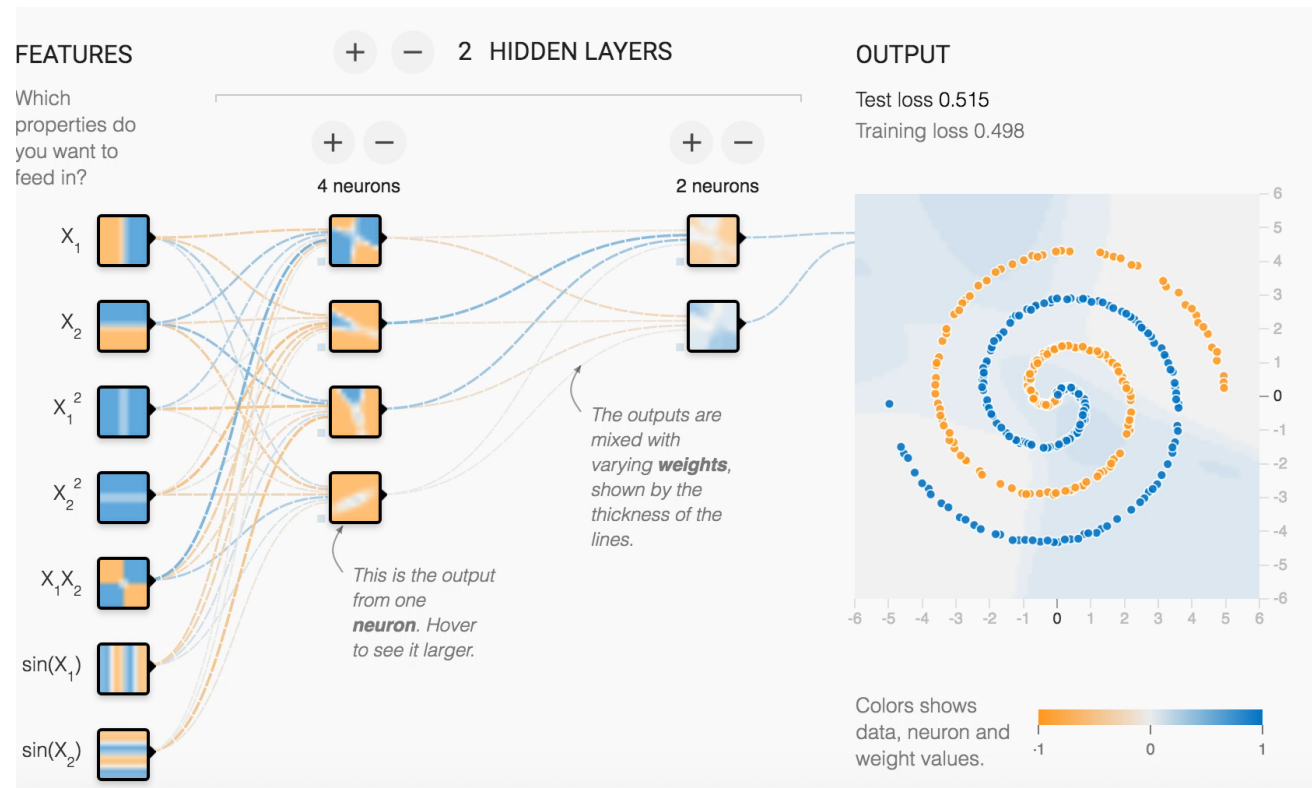


Machine Learning





允公允能 日新月异





允公允能 日新月异

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 overfittttting		<div>Multiclass Loss (Deprecated)</div>		268	2y
2	▲ 7	✱ Marios & Gert		<div></div>	0.0032405...	80	2y

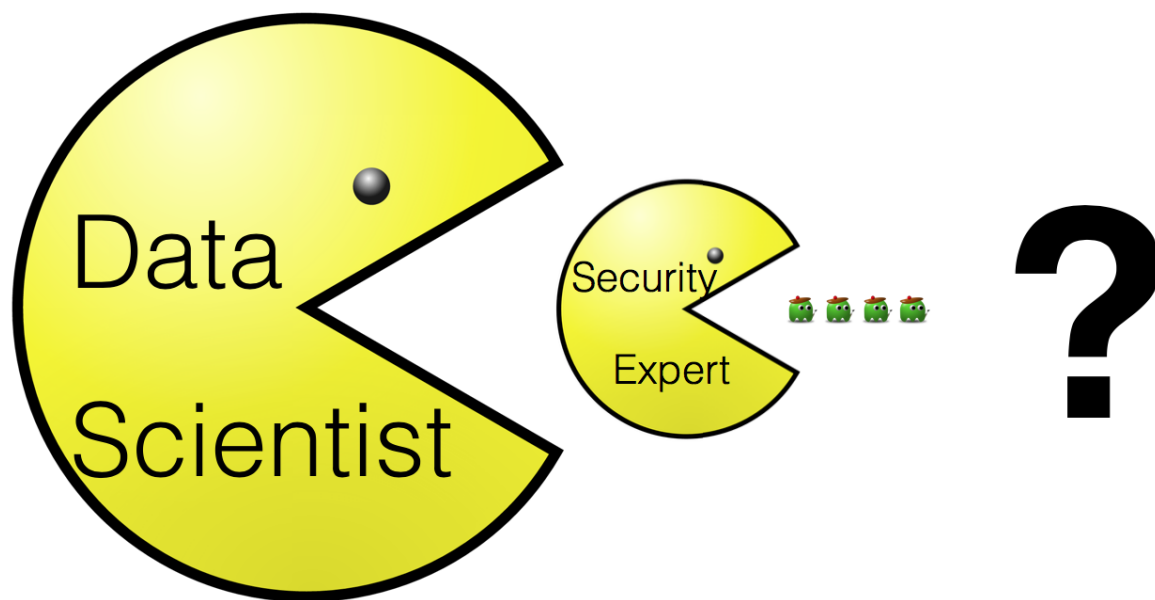


南开大学
Nankai University



允公允能 日新月异

Machine Learning is Eating the World



南开大学
Nankai University

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

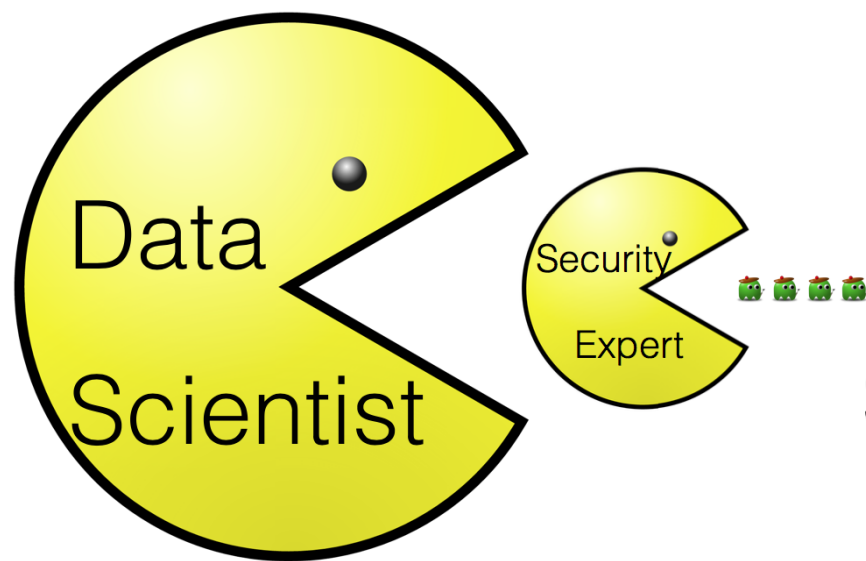




允公允能 日新月异

ML is not a panacea

Machine Learning is Eating the World



No!
Security is different.



南开大学
Nankai University

恶意代码与人工智能系统的博弈

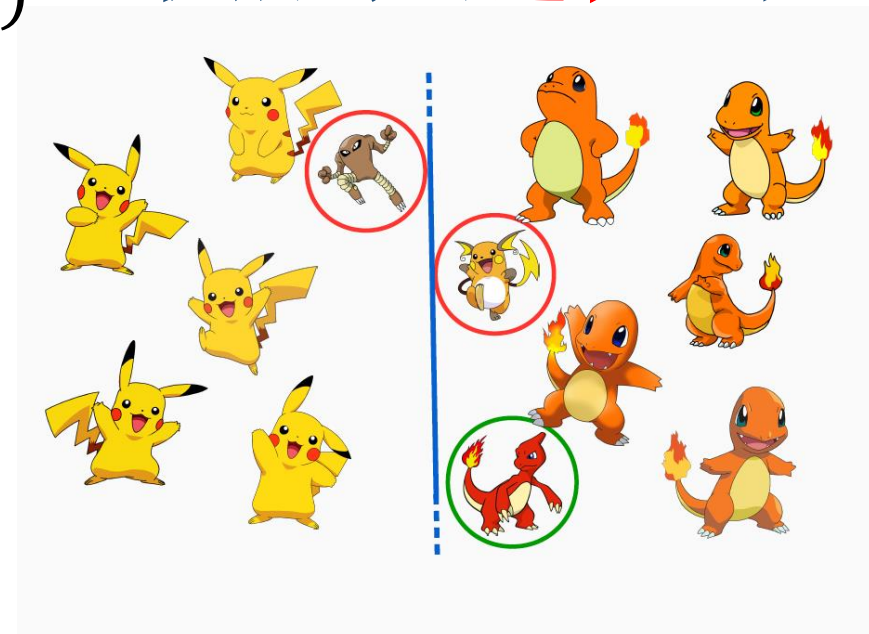
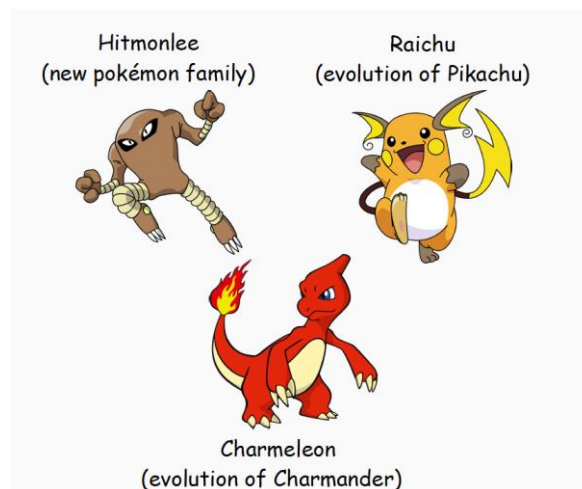
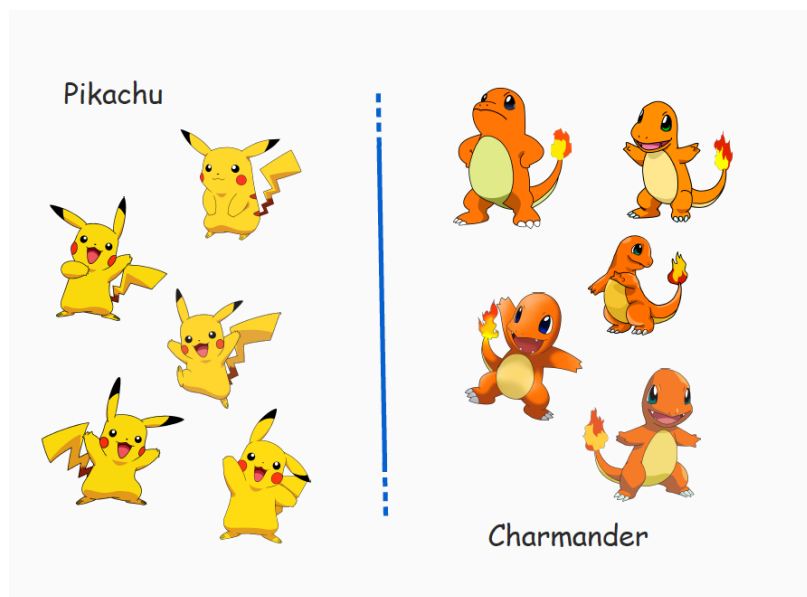
机器学习的前提假设是数据分布具有**稳定性**

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





允公允能 日新月异

100% security is not exist



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



南开大学
Nankai University



允公允能 日新月异

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



南开大学
Nankai University



允公允能 日新月异

Dissecting

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



南开大学
Nankai University



允公允能 日新月异

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





允公允能 日新月异

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



南开大学
Nankai University

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



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, P.R. CHINA 1919

允公允能 日新月異



Malware Analysis Techniques



允公允能 日新月异

Malware Analysis Technique

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





允公允能 日新月异

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



南开大学
Nankai University



允公允能 日新月异

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



南开大学
Nankai University



允公允能 日新月异

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



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





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



Types of Malware

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



南开大学
Nankai University



允公允能 日新月异

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





允公允能 日新月异

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



南开大学
Nankai University

Types of Malware

- Scareware

- Frightens

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

29 Jul, 2013 | by Nishtha Kanal



f Like

3

+1

0

Tweet

3

in Share

Secure Your Application Today!

CHECKMARX

Learn more

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.





允公允能 日新月异

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



南开大学
Nankai University



允公允能 日新月异

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





允公允能 日新月异

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



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, P.R. CHINA 1919

允公允能 日新月異



General Rules for Malware Analysis



允公允能 日新月异

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



南开大学
Nankai University

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。



允公允能 日新月异

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



南开大学
Nankai University



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异



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
2023-2024学年