COMP482 Cybersecurity Week 1 - Friday

Dr. Nicholas Polanco
(he/him)

KALAMAZOO COLLEGE

Attendance Trivia

1. General Knowledge: What is the largest planet in our solar system?

2. Music: Which legendary band was known as "The Fab Four"?

3. Geography: The Great Barrier Reef is located off the coast of which country?

4. Movies: In the film *The Lion King*, what is the name of Simba's father?

5. Sports: Which country has won the most FIFA World Cup titles in men's soccer? What about women's soccer?

Attendance Trivia (continued)

1. General Knowledge: What is the largest planet in our solar system?
   Answer: Jupiter.

2. Music: Which legendary band was known as "The Fab Four"?
   Answer: The Beatles.

3. Geography: The Great Barrier Reef is located off the coast of which country?
   Answer: Australia.

4. Movies: In the film *The Lion King*, what is the name of Simba's father?
   Answer: Mufasa.

5. Sports: Which country has won the most FIFA World Cup titles in men's soccer? What about women's soccer?
   Answer: Brazil and USA.

Important Notes

1. You should go to SIP Fest next week!
2. I have updated Kit, the assignments should be visible now.
   a. I will *try* and do grading within 48 hours of when an assignment is due. Does that sound fair?
      - I can try to do 24 hours, but I am grading alone :(
      - I would grade early if you submit early, but would people be okay with this…..?
3. I am seeing if I need to add additional activities for next week (on TryHackMe, and in-class)
   a. If you are working ahead that is fine, but Monday may have additional things on the schedule so don't panic.
4. I may update previous weeks to as I move along and get feedback, don't panic.

Important Dates (Week 2)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
		Due: Think Like a Hacker Activity		Due: Recent Attacks Reflection 1 Project “Idea” Meeting		

History of Cybersecurity

ARPANET (1969)

This was the precursor to what we now know today as, the modern internet, the U.S Department of Defense's **Advanced Research Project Agency (ARPANET)**

- This was designed to enable research institutions to communicate and withstand potential disruptions in case of nuclear attacks.

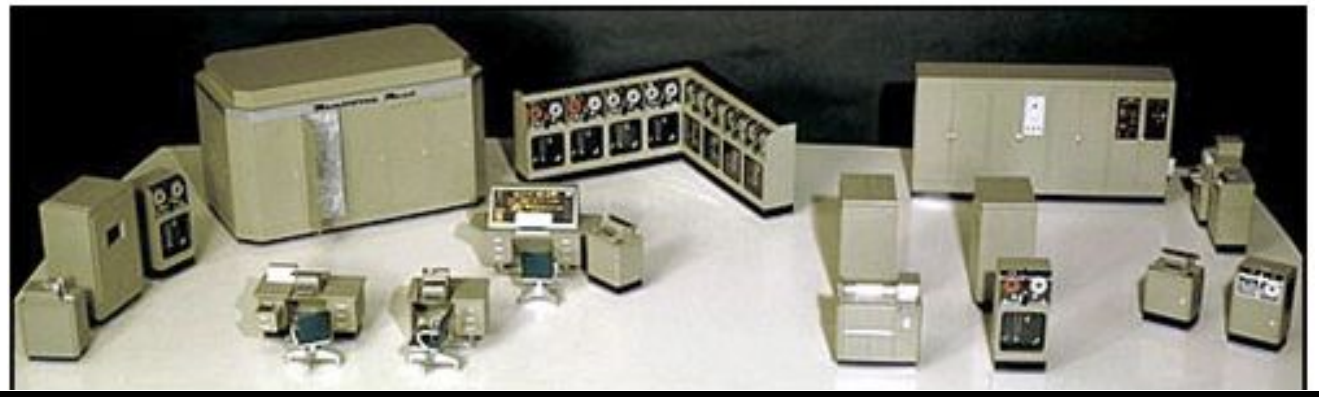

Image Credit: https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml#:~:text=Sharing%20Resources,government%20researchers%20to%20share%20information.

KALAMAZOO COLLEGE

Discussion

Why does the intended function of ARPANET cause issues for creating a secure “internet” in today’s society?

CREEPER Virus (1971)

This was the first known computer worm (or virus), it was made as an experimental self-replicating program.

- It was created by Bob Thomas
- This spread across ARPANET and displayed the message seen below:

Image Credit:
https://www.historyofinformation.com/image.php?id=5351

KALAMAZOO COLLEGE

REAPER Antivirus (1971)

Reaper was the first anti-virus software that was designed to delete Creeper by moving across the ARPANET.

- It was created by Ray Tomlinson

Bob Thomas and Ray Tomlinson

Bob Thomas

- He discovered that computer programs could travel through networks.
- He developed some of the first security protocols and practices still in use today.
- Often regarded as “the father of cybersecurity,”

Ray Tomlinson

- This is the programmer who implemented the first email program on ARPANET.

Viruses and Worms Emerge (1970s - 80s)

The growth of viruses and worms became more prevalent as personal computers become widely available.

The first *significant* computer attack is often attributed to the Morris Worm, but the Rabbit (or Wabbit) virus is also worth noting.

<u>Why would viruses and worms suddenly become more prevalent?</u>

Rabbit (or Wabbit) (1974)

This worm (or virus) duplicated itself over and over until it had a lot of copies that severely reduced performance and eventually crashed the machine.

- It created an infinite loop that continually creates system processes and creates copies of Wabbit.
- This consumes operating system resources and creates a high number of CPU cycles, eventually causing a crash.

<u>Does anyone have any idea why it was named Rabbit (or Wabbit)?</u>
<u>Would we argue that it is malicious?</u>

Image Credit: https://en.wikipedia.org/wiki/Elmer_Fudd#/media/File:Elmer_in_Rabbit_Fire_(1951).png

KALAMAZOO COLLEGE

Notable Milestones (1980's)

1983: The ARPANET systems were hacked by a group that called themselves 414.

1987: The Vienna Virus, which destroyed random files, was one of the first that was destroyed with antivirus programs.

1987: John McAfee created the first commercial antivirus software. Does this sound familiar?

The Morris Worm (1988)

The Morris Worm was released on November 2nd, 1988. This is the significant events as it was the first major spread of a computer worm across the Internet.

- **This brought a significant amount of awareness to the importance of network security.**

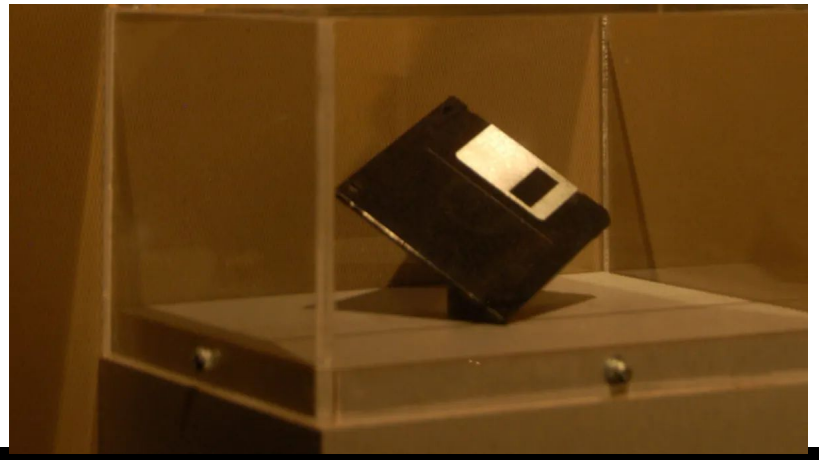

Image Credit: https://www.zdnet.com/article/the-day-computer-security-turned-real-the-morris-worm-turns-30/

KALAMAZOO COLLEGE

The Morris Worm (1988) (continued)

The worm spread using these vulnerabilities:

1. Weak Passwords - It essentially tried to *guess* them
2. Known Exploits - It leveraged exploits in the Unix *sendmail* program and the *fingerd* network service.
3. Re-Infection - It then infected each computer **multiple times**, with each process slowing down the PC until it would crash.

The Morris Worm (1988) (continued)

What did this do?

- It spread to ~6,000 computers
  - It eventually spread through the US and took down the entire internet
- It caused financial damage of around ~$100,000 - $10,000,000 in terms of lost productivity, damages, and system downtime.

Robert Morris was actually a graduate student at Cornell, and the worm was not intended to be malicious!

- It was to gauge the size of the internet and **expose** Unix system vulnerabilities

<u>What do we think the punishment for something like this is?</u>

The Morris Worm (1988) (continued)

Punishment

- Robert Morris became the first person convicted under the 1986 Computer Fraud and Abuse Act
- 3 years of probation
- 400 hours of community service
- $10,000 fine.

* He also got **a lot** of job offers!

<u>Did you think the punishment would be more or less severe than it was?</u>

Cyber Attacks in the 1990s

- **Increase in Scale and Sophistication:** The internet was growing, so larger networks began to be targeted.
- **Commercialization of Internet:** The growth of e-commerce online created targets for cybercriminals
- **Phishing Attacks:** These began and were tricking users into divulging sensitive data
- **Denial of Service (DoS) Attacks:** The development of attacks focused on overwhelming networks with excessive traffic

Cyber Attacks in the 1990s (continued)

- **Network-Based Attacked:** The infrastructure and protocols of the internet were targeted.
- **Cryptographic Vulnerabilities:** The methods used to defend against these things began getting attacked.
- **Government/Corporate Attacks:** The use of computer systems by large entities made them targets of data theft and espionage.
- **Hacker Groups:** We saw a rise in groups, either ideological or profit-driven, focusing as a team to attack entities.
- **Regulatory Response:** The development of cybersecurity regulations began to help combat these attacks.

Polymorphic Virus (1990)

This attack emerges that had the capability of changing/mutating to evade detection.

- This posed a significant challenge to traditional antivirus defenses.

The first was called 1260 (or V2PX), and was originally intended to **warn internet users.**

- However, this actually inspired a wave of criminal activity that was based on the capabilities of this virus.

* This type of virus has actually been backed by AI capabilities now to help mutate more effectively, making them harder to detect or combat.

Kevin Mitnick (1990's)

He was a former hacker in the 1990s, most noted for his hacking that involved social engineering.

- In 1979 (he was 16), he got the phone number for Ark and was able to maneuver his way into the computer network, he the copied the software and continued to exploit it until he was charged and convicted in 1988.

Image Credit: https://ciso.economictimes.indiatimes.com/news/ciso-strategies/ode-to-kevin-mitnick-a-legacy-of-cybersecurity-brilliance/102008065

KALAMAZOO COLLEGE

Kevin Mitnick (1990's) (continued)

He was arrested in June of 1992 by the FBI

- Crimes Charged: Wire fraud (14 counts), possession of unauthorized access devices (8 counts), interception of wire or electronic communications, unauthorized access to a federal computer, and causing damage to a computer

Data Encryption Standard (DES) (1995)

This was created and adopted to help secure communication via electronic devices.

- This started the foundation for encryption standards we have today and how to protect sensitive data.

Older Standards:

- 1865 - The International Telecommunication Union (ITU)
- 1901 - National Institute of Standards and Technology (NIST)
- 1947 - The International Organization for Standardization (ISO)
- 1992 - Internet Society (ISOC)

Melissa Virus (1999)

This was spotted in March 1999, spreading to the public via internet forums and emails

- It was a word document, that when opened executed the malicious code
- If macros were enabled, spread itself to first 50 contacts in Outlook by an email with the attached document
- It was estimated to cause around $80 million in damages

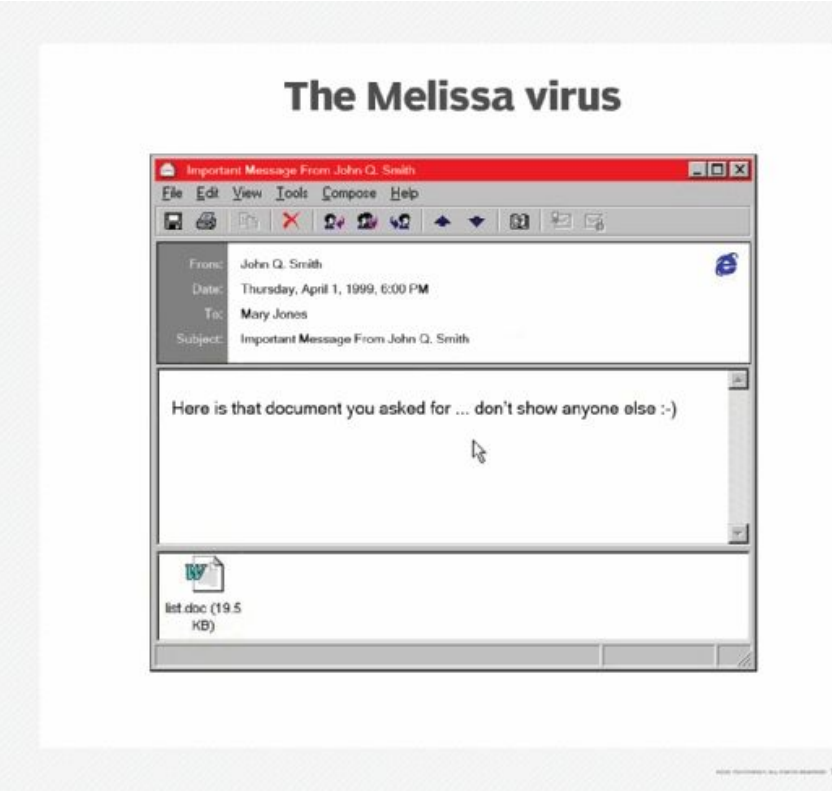

Image Credit:
https://www.techtarget.com/searchsecurity/definition/Melissa-virus

KALAMAZOO COLLEGE

Discussion

Why is this case interesting?

What could the attacker have been after? Why does this become difficult to defend against?

Would you consider this a virus or a social engineering?

ILOVEYOU (2000)

This was technically a virus, but the way it was delivered was like a trojan horse (and also some social engineering).

- An email attachment with the subject line “ILOVEYOU.”
  - If opened, spread to every contact in a user’s Microsoft Outlook address book
- Also started overwriting certain files (e.g., JPEG and MP3 files) from the hard drive
- $5.5–8.7 billion in damages, David Smith was the creator, arrested and sentenced to 20 months in prison.

Image Credit:
https://cyberhoot.com/cybrary/iloveyou-virus/

Other Attacks in the Early 2000s

Code Red (2001): This worm leveraged an issue with Microsoft's IIS web server, caused disruption and defacement of websites.

SQL Slammer (2003): A worm that treated a vulnerability in Microsoft SQL Server 2000, caused network congestion and outages.

Blaster Worm or MSBlast (2003): This exploited a vulnerablity in Windows XP and Windows 2000 that caused system crashes and network issues.

Other Attacks in the Early 2000s (continued)

Sasser Worm (2004): This exploited another vulnerability in Windows, causing reboots and network issues.

The Apple Macintosh was released on January 24, 1984.

- Why has this not been targeted by many attacks up until this point?

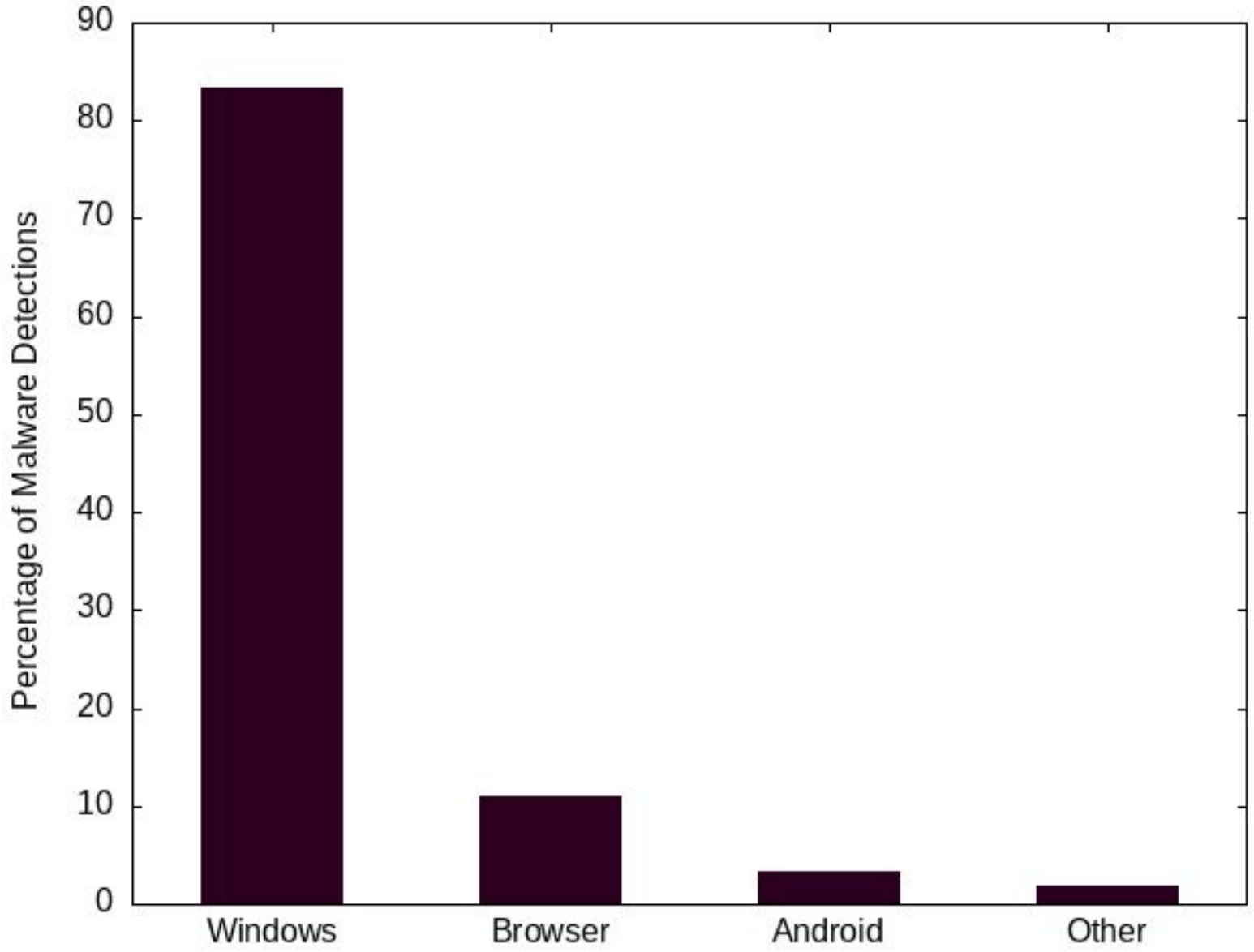

Image Credit:
https://web.njit.edu/~rt494/security/#_malware

KALAMAZOO COLLEGE

Pause: Types of Hacker “Hats”

What are the types of hacker “hats” you can think of? What other types of hackers can you think of?

Image Credit:
https://www.techtarget.com/searchsecurity/answer/What-is-red-and-white-hat-hacking

KALAMAZOO COLLEGE

WannaCry (2017)

This exploited a vulnerability in Microsoft Windows (EternalBlue).

- It spread to over 200,000 computers, in 150 countries.
- This was trying to target healthcare institutions and other critical infrastructure.

Image Credit: https://www.healthcareitnews.com/news/wannacry-timeline-how-it-happened-and-industry-response-ransomware-attack

KALAMAZOO COLLEGE

Legal Milestones in Cybersecurity

This history matters because it gave way to the different standards and legal milestones we have today, such as:

1. General Data Protection Regulation (GDPR) (2018): This sets out requirements for how to handle personal data, specifically for organizations.
2. California Consumer Privacy Act (CCPA) (2018): This gives more control over personal information that businesses collect about them.
3. Health Insurance Portability and Accountability Act (HIPAA) (1996): These are standards for protecting health information.

Legal Milestones in Cybersecurity (continued)

4. Family Educational Rights and Privacy Act (FERPA) (1974): A federal law that protects the privacy of students' educational records.
5. Data Protection Act (2018): This updates data protection laws
6. Payment Card Industry Data Security Standard (PCI DSS) (2004): This was intended to help with payment card account data security and more consistent data security measures

Activity: Recent Attacks

You can work in groups for this activity, but we are going to take a look at 3 recent cybersecurity breaches. The details can be found on the webpage.

You may also finish up your Activity: Think Like a Hacker! if you are not done yet.

Questions?