Dashboard of Cyberattacks and their Historic Timeline

Gideon Survoy and Keeler Sparks- Mentors Dr. Clemente Izurieta, Yvette Hastings

Results

FIG. 1: CYBERATTACK TIMELINE IN ORDER OF EVENTS

Morris Worm

What Happened: Worm released by Robert Morris designed to exploit several UNIX weaknesses which cahsed the machines to overload and either crash or significantly slow down.
Importance: First attack through thee internet which affected roughly 6000 computers (10% of thee internet)
Damages: $100 Thousand-$10 Million
Impact: Led to creation of first Computer Emergency Response Team and shaped the 1986 Computer Fraud and Abuse Act enforcement.

Stuxnet

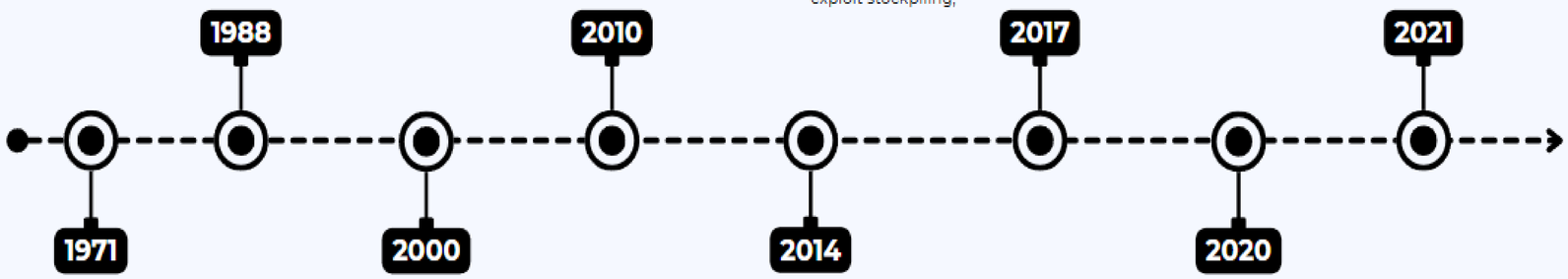
What Happened: A worm targeted Iran's Nanatz uranium enrichment facility, creating small changes in the controllers that caused more wear. This is believed to be a joint U.S.-Israeli Operation.
Importance: First cyberattack to cause physical destruction to over 1000 centrifuges.
Damages: $500 Million in equipment loss and delays
Impact: Elevated ICS/SCADA cybersecurity globally and brought state-sponsored attacks to spotlight.

Wannacry

What Happened: Ransomware was globally spread, leveraging a leaked NSA exploit that encrypted systems and demanded Bitcoin. This also severely impacted the UK's National Health Service.
Importance: It showed how quickly ransomware could cripple essential services, as it had taken effecting mere hours.
Damages: $4 Billion
Impact: Reiterated emphasis on software catching backup practices and government accountability of exploit stockpiling,

Colonial Pipeline Ransomware

What Happened: Darkside hackers used stolen credentials to launch ransomware against Colonial Pipeline, which shut down fuel delivery to the East Coast.
Importance: First cyberattack to cause significant disruption to the US energy infrastructure
Damages: $4.4 Million ransom and fuel shortages
Impact: Triggered new TSA security directives, Executive 14028, and the formation of the Joint Cyber Defense Collaborative



Creeper Program

What Happened: First known self-replicating computer program, infecting DEC mainframes on ARPANET. Also included Reaper Program which was designed to remove it.
Importance: Introduced malware and program defense (viruses and antiviruses).
Damages: None
Impact: First recognition of risks by autonomous code.

ILOVEYOU Virus

What Happened: A worm sent through email with the subject "ILOVEYOU" spread through opening the attachment, which destroyed files and emailed itself to contacts
Importance: The first big email-based attacks exposed how easily people could be manipulated.
Damages: $5 Billion-$10 Billion

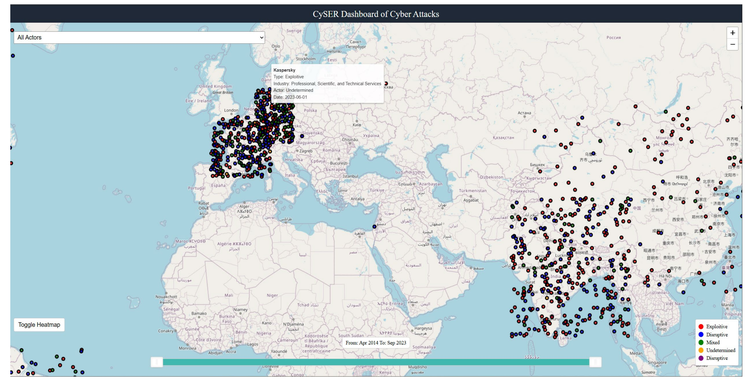
Sony Pictures Hack

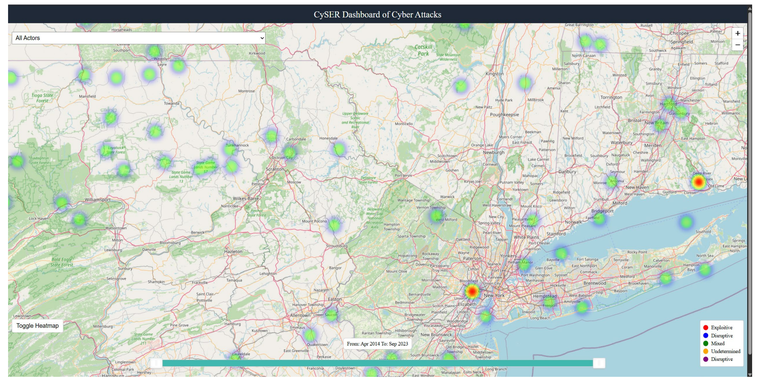
What Happened: A group linked to North Korea called the Guardians of Peace infiltrated Sony's systems and leaked emails, films, and employee data in response to the film The Interview.
Importance: Significant attacks based on political motives and demonstrated a state-sponsored attack on a private company
Damages: $100 Million
Impact: Forced corporations to reconsider threats and prepare for geopolitical cyberattacks.

Solarwinds supply chain attack

What Happened: Russian hackers compromised the SolarWinds Orion software updates, giving them access to US government agencies and private systems for several months.
Importance: Exposed the risk of software supply chain vulnerabilities on a large scale.
Damages: Unknown
Impact: Led to federal mandates on software development transparency as well as limited trust architecture in government systems.

FIGS. 2 & 3: CYBERATTACK DASHBOARD





Introduction

Cyberattacks have become a constant and growing threat in today's connected world. From data breaches to state-sponsored attacks, these digital threats can disrupt infrastructure, steal sensitive data, and impact everyday life. This project highlights how cyberattacks have evolved into a defining challenge of the digital age, revealing their patterns, impact, and global significance.

Objective

Our objective is to showcase cyberattack frequency, locations, perpetrators, and impacts, enabling cybersecurity professionals to identify recurring patterns and trends that inform cybersecurity strategies. Additionally, we showcase a timeline to provide additional context to when some of the major attacks occurred with valuable context for them.

Methods

To build the timeline (Fig. 1)[1–8], we researched some of the most impactful cyberattacks and found valuable information, including damages, dates, and effectiveness. The metadata from a cyberattack database[9] was loaded into an optimized HTML dynamic webpage to create the dashboard (Figs. 2 & 3).

Conclusion

As cyberattacks become increasingly common, it is crucial to understand how they have shaped and disrupted society throughout the evolution of the internet and our growing reliance on digital infrastructure. Recognizing the scale and seriousness of these threats allows us to better prepare for the future. By developing stronger cyber deterrents and adopting industry best practices, we can work toward safeguarding our systems and protecting society from the rising tide of cyber threats.

Acknowledgements

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.

References

1) (Creeper Program) https://www.exabeam.com/blog/infosec-trends/creeper-the-worlds-first-computer-virus/
2) (Morris Worm) https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218
3) (ILOVEYOU Virus) https://www.goldskysecurity.com/the-history-and-impact-of-the-iloveyou-virus/
4) (Stuxnet) https://spectrum.ieee.org/the-real-story-of-stuxnet
5) (Sony Pictures Hack) https://www.fbi.gov/news/press-releases/update-on-sony-investigation
6) (WannaCry) https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware
7) (Solarwinds) https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic
8) (Colonial Pipeline) https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
9) (Cyberattack Dashboard Source) https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents