



# The Rising Threat Of Computer Viruses

By: Brandon LaHaye, Fatimah Kamal, Hasan Waheed, Zeiad Alarkan



# INTRODUCTION

## Computer Viruses? A Rising Threat?

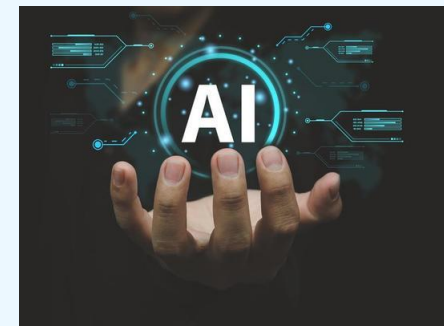
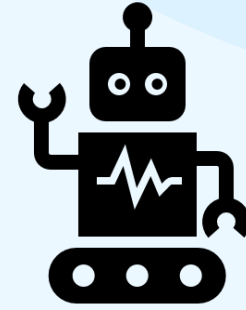
- ❖ **As Technology advances, so does the complexity and impact of computer viruses.**



- ❖ **Private Citizens, Corporations, Critical Infrastructure and Governments alike are all at risk.**
- ❖ **Newly emerging threats such as AI-driven malware, and Ransomware-as-a-service significantly impact our digital safety.**
- ❖ **Even IoT devices at home are not safe, in fact, such devices provide weaknesses which can be exploited.**

# The Impact of AI on Computer Viruses

The creation and enhancement of computer viruses via AI





(Truong et al., 2020)

# The Positives of AI on Computer Viruses

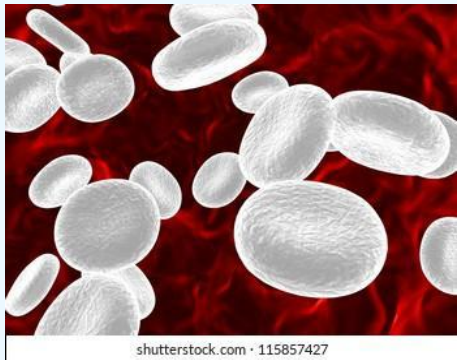


## AI Systems To Detect Viruses

- Malware or Intrusion detection on devices and systems
- Phishing and spam email detection
- Possibility of countering Advanced Persistent Threats (APT)

## Training AI to Detect Viruses

- Training AI via Supervised, Unsupervised, or Reinforcement learning
- AI Learning via Machine Learning (ML) or Deep Learning (DL)





(Truong et al., 2020)  
(Mifune, 2024)

# The Negatives of AI on Computer Viruses

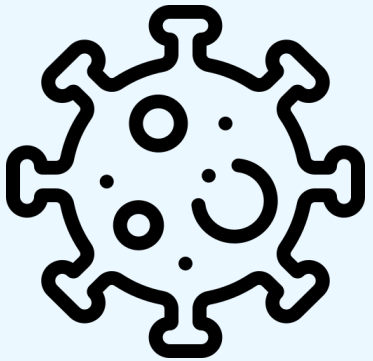


## AI-Enhanced Computer Viruses

- Previous viruses can become independent and widespread
- AI can be used to poison or sabotage trained AI models
- AI can create viruses such as ransomware

## AI Learning Social Engineering

- AI can learn how to identify features of people to send a personalized phishing email or spam
- AI can find large information databases to use for targeted attacks



# The evolution of Ransomware (RaaS)



# What is ransomware?

- Encrypts data, blocks access until ransom is paid
- Traditionally required advanced programming skills
- Evolved into RaaS (Ransomware as a Service)



# Accessibility of RaaS

- No need for advanced programming skills
- Available to a wide range of criminals
- Resulting in more cyberattacks globally
- RaaS removes technical barriers, accessible to criminals with minimal skills
- Available as subscription-based service
- Increased convenience, sophistication, and global surge in attacks

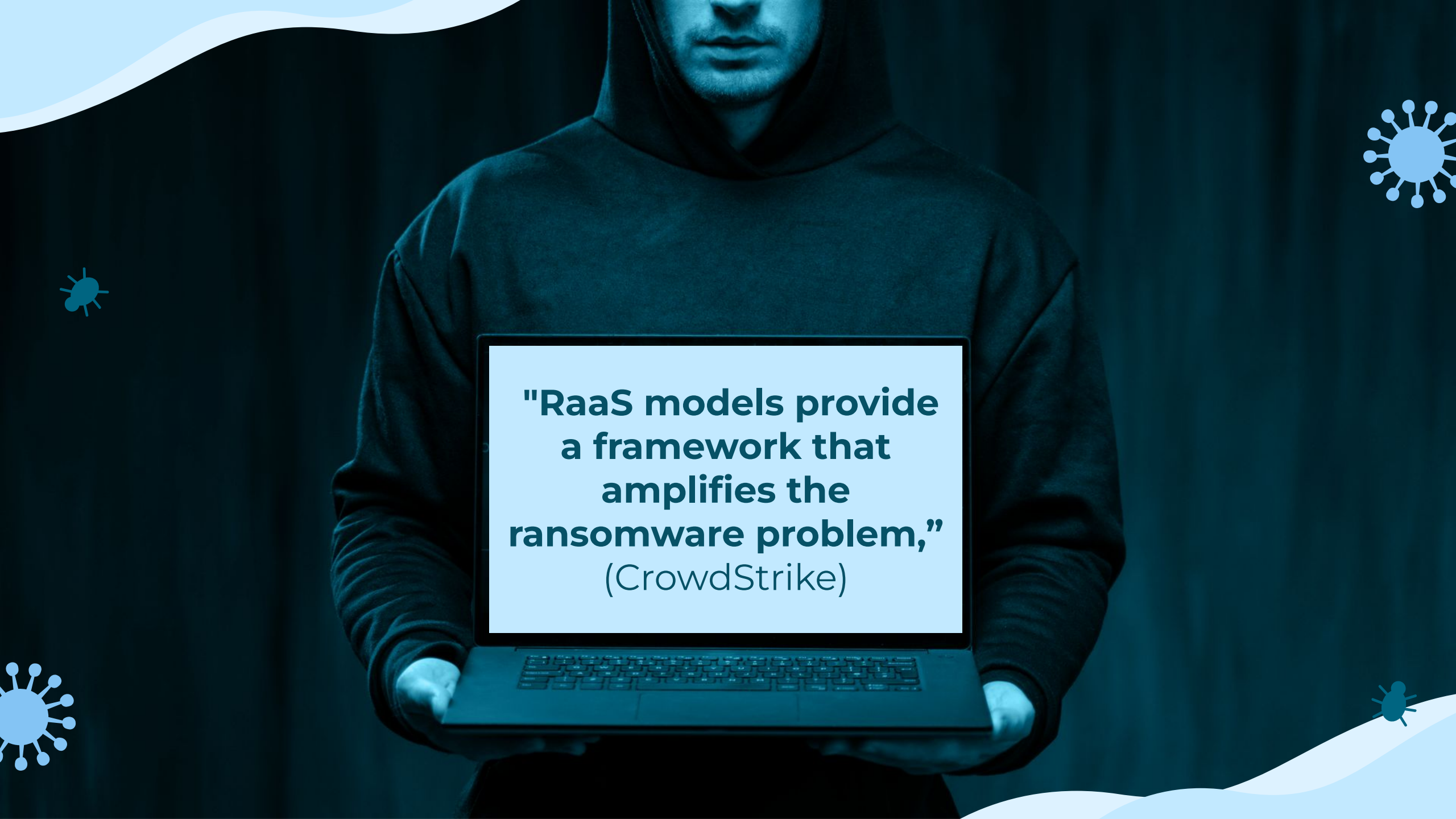




# RaaS: A Business-Like Operation

- Operates like legitimate businesses with organized networks
- Specialized roles and customer support (e.g., help desk)
- Harder for law enforcement to dismantle these structures
- RaaS providers continuously refine their tools
- Enhanced features and flexibility increase threat level
- Ongoing investment in exploiting system vulnerabilities

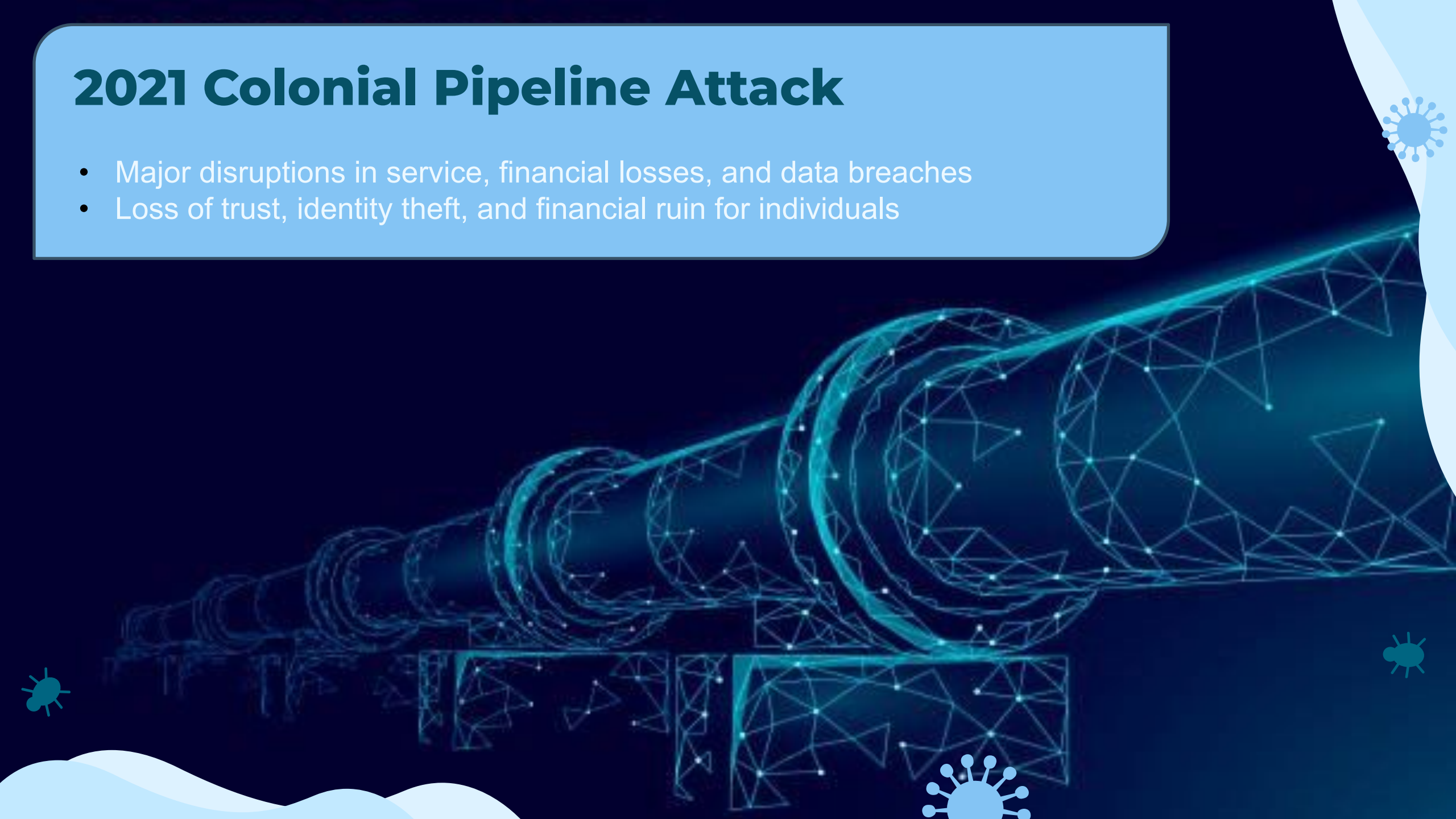




**"RaaS models provide  
a framework that  
amplifies the  
ransomware problem,"  
(CrowdStrike)**

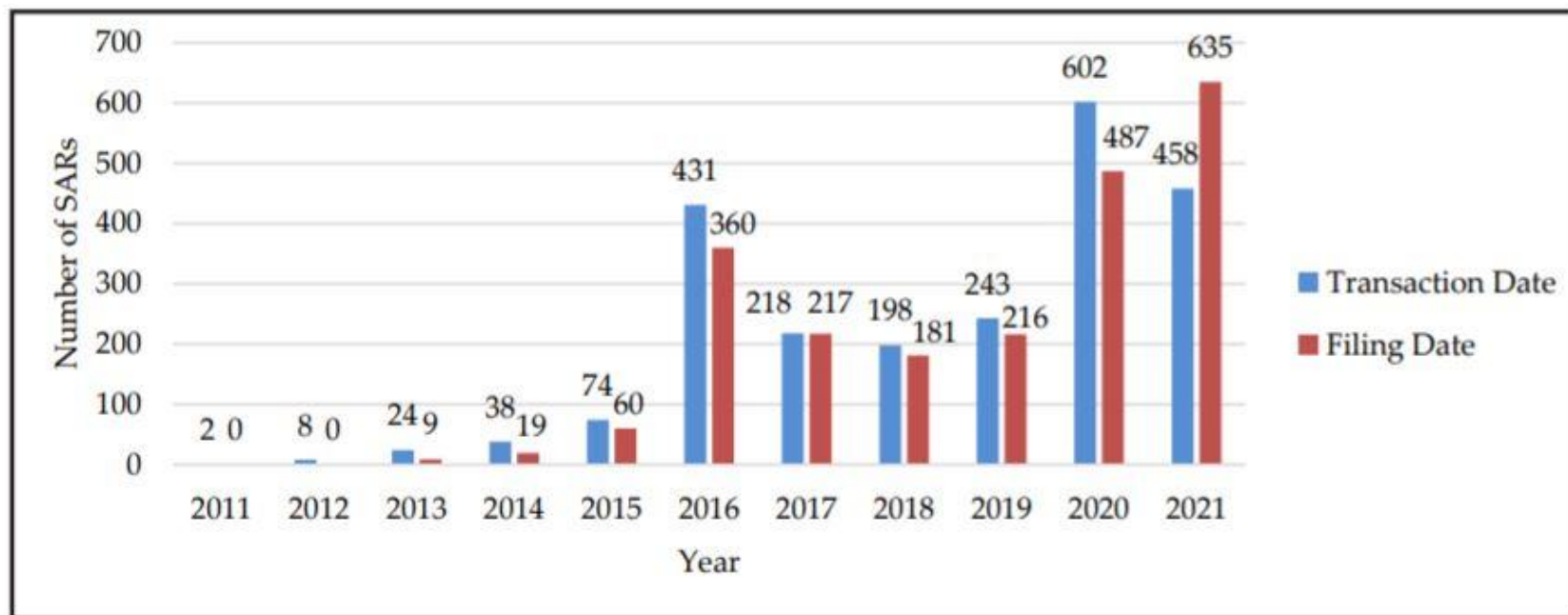
# 2021 Colonial Pipeline Attack

- Major disruptions in service, financial losses, and data breaches
- Loss of trust, identity theft, and financial ruin for individuals



# A Growing Threat

- RaaS is a growing cybersecurity threat due to its accessibility and complexity
- Continuous evolution makes it harder to combat
- Need for coordinated global efforts to protect critical infrastructure



# LOCKBIT 3.0

## A Brief Revision on LockBit's Origins

- ❖ **“LockBit” is a prominent ransomware group who’ve operated since 2020**
- ❖ **The group operates by contracting subscription models, otherwise known as “RaaS” (Ransomware-as-a-Service)**
- ❖ **The software has been regularly updated**

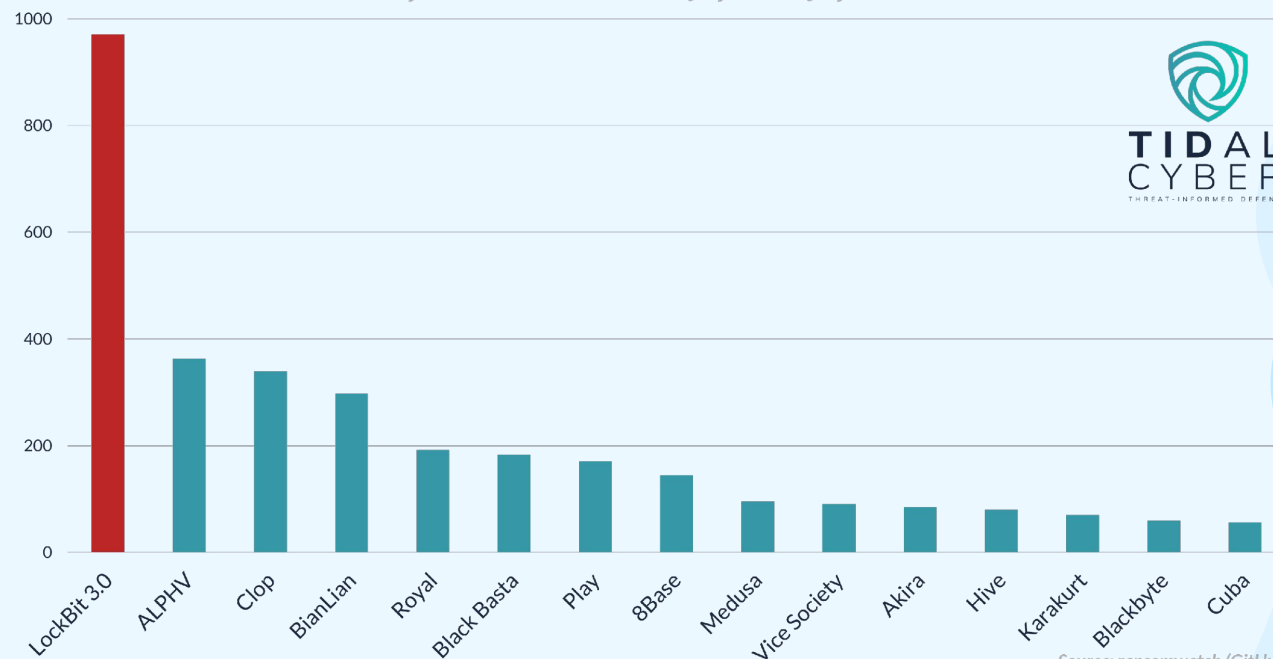
LockBit 2.0 launched  
June 2021

LockBit  
Linux-ESXi 1.0  
launched June  
2021

LockBit 3.0  
launched  
March 2022

## Top Ransomware & Extortion Operations

By Claimed Victim Count, July 2022-July 2023



Source: ransomwatch (GitHub)





❖ **Has generated over 91 Million Dollars from the United States in just 2020 (CISA, 2023).**

❖ **Bolstered International efforts to increase cybersecurity initiatives to identify and capture Cybercriminals**

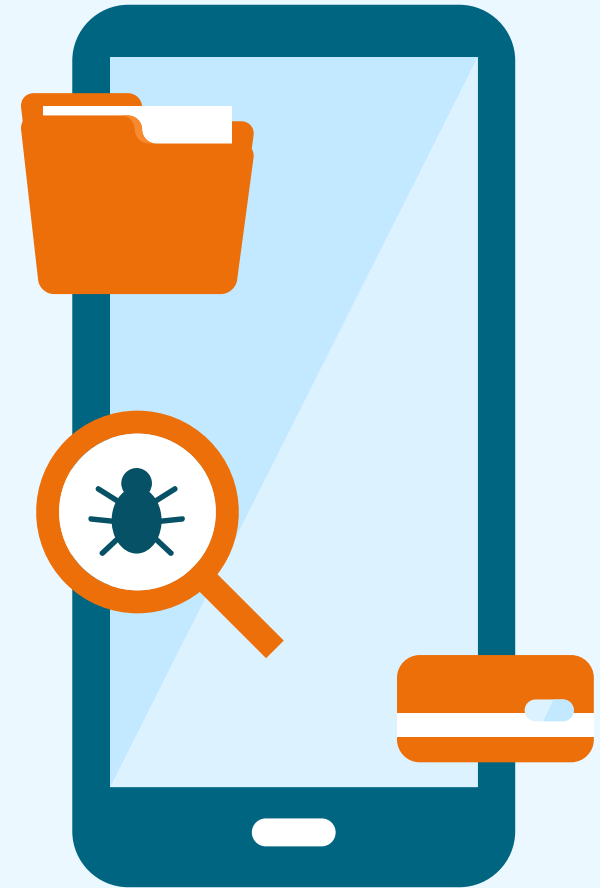
❖ **Highly Adaptable and capable of evading detection.**

# LOCKBIT 3.0

A Global Cybersecurity  
Threat



# Introduction to IoT and It's Issues








# **Introductory**

- AKA **Internet of Things**
- Invented In 1999 by computer scientist Kevin Ashton.
- Ashtons purpose with IoT was to track products using RFID chips in supply chains.
  - This was during his time as a Procter and Gamble
  - His goal was to not having anything stolen by perpetrators.
- Acts as a security and networking system for details including:
  - Sensors
  - Connectivity (ex; Bluetooth)
  - Software
  - Every piece of technology you hold contains IoT

# **Problems In IoT**

- No matter what security system is installed there will always be weaknesses exposed.
  - Hackers have figured out how to attack technology with IoT.
  - Imposes a threat to society.
  - The main reason for these situations to occur is because:
    - Manufactures prefer functionality over security.
    - If IT and cyber intelligence teams don't pounce now, hacking will continue to be a common practice.
- 
- 
- 



# **Let's Dive Into A Real-Life Example of An IoT Situation**

# IoT And The Fish Tank Attack



## General Information Of The Fish Tank

- Fish tank operating in a casino in North America.
- Only able to operate through internet connectivity.
- 10 gigabytes were installed in the system costing the casino boat loads of money.
- The fish tank was responsible for:
  - Automatic feedings
  - Adjusting temperature
  - Can be monitored through a camera remotely
- The data and security system is monitored by Darktrace.



# Fish Tank Hacking Scheme

- A group of unknown hackers main goal was to steal 10 gigabytes and data.
- The monitoring system was being sent to servers in Finland:
  - Included footage of the fish tank operating.
  - Used to cause distraction upon criminal activity.
- Dark Trace reported the incident to the casino
  - Fun Fact: Darktrace are one of the biggest cyber intelligence groups in North America .
- The hackers were unsuccessfully caught (No descriptions of the hackers were revealed).
- Darktrace concluded that the criminal activity was not easy to discover, and valuable items were stolen.

A statement from Dark Trace: **“This was a clear case of data exfiltration, but far more subtle than typical attempts at data theft” (Mathews, 2017)**



Source: (Matthews, 2017)




# KEY

# TAKAWAYS...

**1. Computer Viruses are a constantly evolving threat to global digital security. Awareness of computer security is essential.**

**2. Emerging threats such as AI- driven malware and ransomware highlight the need for international cooperation.**

**3. As more household devices connect to the web, private citizens face increased vulnerabilities.**



# THANK YOU!

Any Questions?





# REFERENCES

- Mifune, S. (2024, May 28). *Police arrest man after computer viruses created by misusing AI*. The Asahi Shimbun. <https://www.asahi.com/ajw/articles/15283413>
- Truong, T. C., Diep, Q. B., & Zelinka, I. (2020a). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry (Basel)*, 12(3), 410. <https://doi.org/10.3390/sym12030410> <https://www.mdpi.com/2073-8994/12/3/410>
- *What is ransomware as a service (raas)?*. CrowdStrike. (n.d.). <https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>
- Buxton, O. (2024, October 4). *7 dangerous new computer viruses & malware in 2024*. The 7 Most Dangerous New Computer Viruses & Malware of 2024. <https://www.avast.com/c-new-computer-viruses>
- *Rise in active raas groups parallel growing victim counts: Ransomware in 2H 2023*. Trend Micro (US). (n.d.). <https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/rise-in-active-raas-groups-parallel-growing-victim-counts-ransomware-in-2h-2023>
- Paganini, P. (2021, October 16). US treasury fincen linked \$5.2B in BTC Transactions to ransomware payments. Security Affairs. <https://securityaffairs.com/123431/malware/fincen-ransomware-payments.html>
- *Understanding ransomware threat actors: LockBit | CISA*. (2023b, June 14). Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a>
- *What Is the Internet of Things?* (n.d.). Oracle. Retrieved November 7, 2024, from <https://www.oracle.com/ca-en/internet-of-things/>
- *Top IoT Security Challenges and Best Practices*. (n.d.). Balbix. Retrieved November 7, 2024, from <https://www.balbix.com/insights/addressing-iot-security-challenges/>
- Merchant, N. (n.d.). *IoT Technologies Explained: History, Examples, Risks & Future*. Vision of Humanity. Retrieved November 7, 2024, from <https://www.visionofhumanity.org/what-is-the-internet-of-things/>
- Matthews, L. (2017, July 27). *Criminals Hacked A Fish Tank To Steal Data From A Casino*. Forbes. Retrieved November 7, 2024, from

