The Invisible Battlefield of Ransomware, Data Breaches, and AI-Powered Attacks

Vaibhavi Tiwari
April 2025

Not a Bedtime Story

One weak password

One click

100GB of critical data

Halting of 2.5 million barrels

$4.4 million Ransom in Bitcoin

Panic Buying

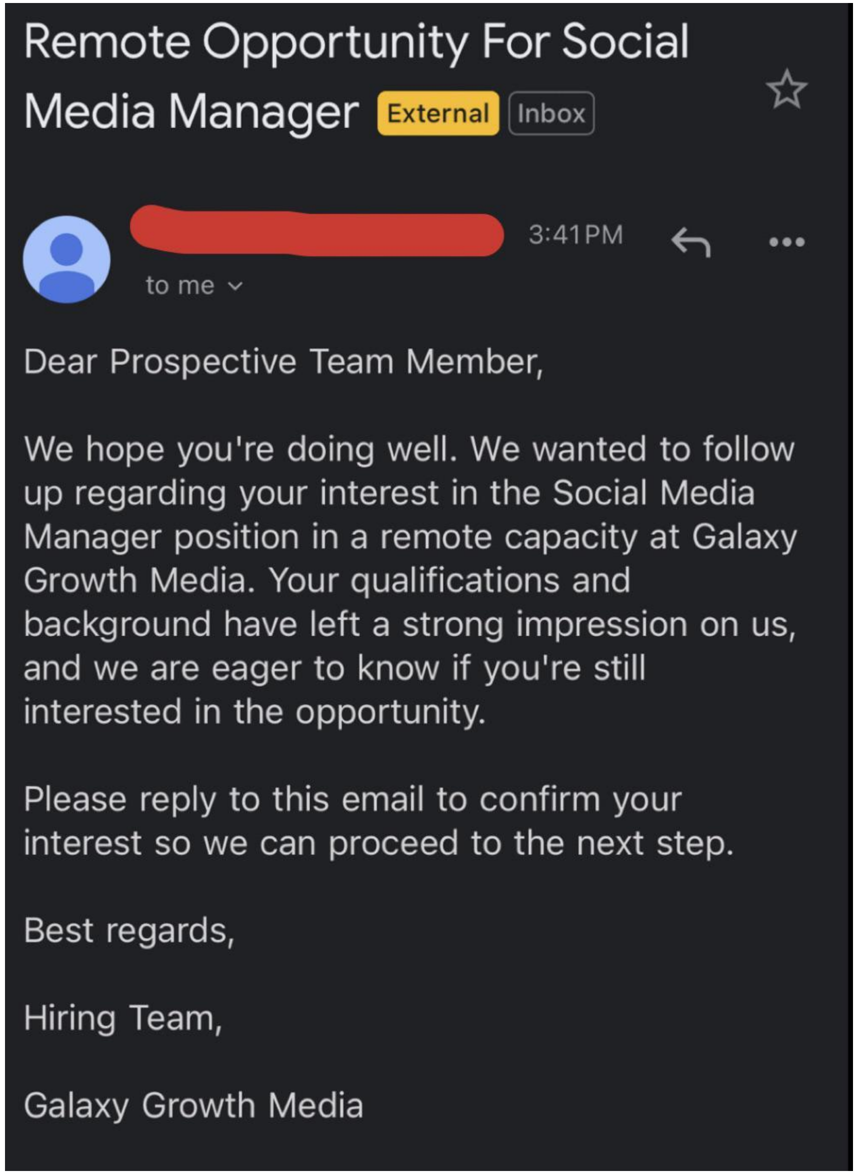
Gas Price Spike

Airlines Reroute Flights

Crisis across 17 States

Invisible Battlefield

- Cyber threats are unseen
- Every device and user is a target
- We’re all defenders now



Remote Opportunity For Social Media Manager

[redacted] 3:41PM

to me

Dear Prospective Team Member,

We hope you're doing well. We wanted to follow up regarding your interest in the Social Media Manager position in a remote capacity at Galaxy Growth Media. Your qualifications and background have left a strong impression on us, and we are eager to know if you're still interested in the opportunity.

Please reply to this email to confirm your interest so we can proceed to the next step.

Best regards,

Hiring Team,

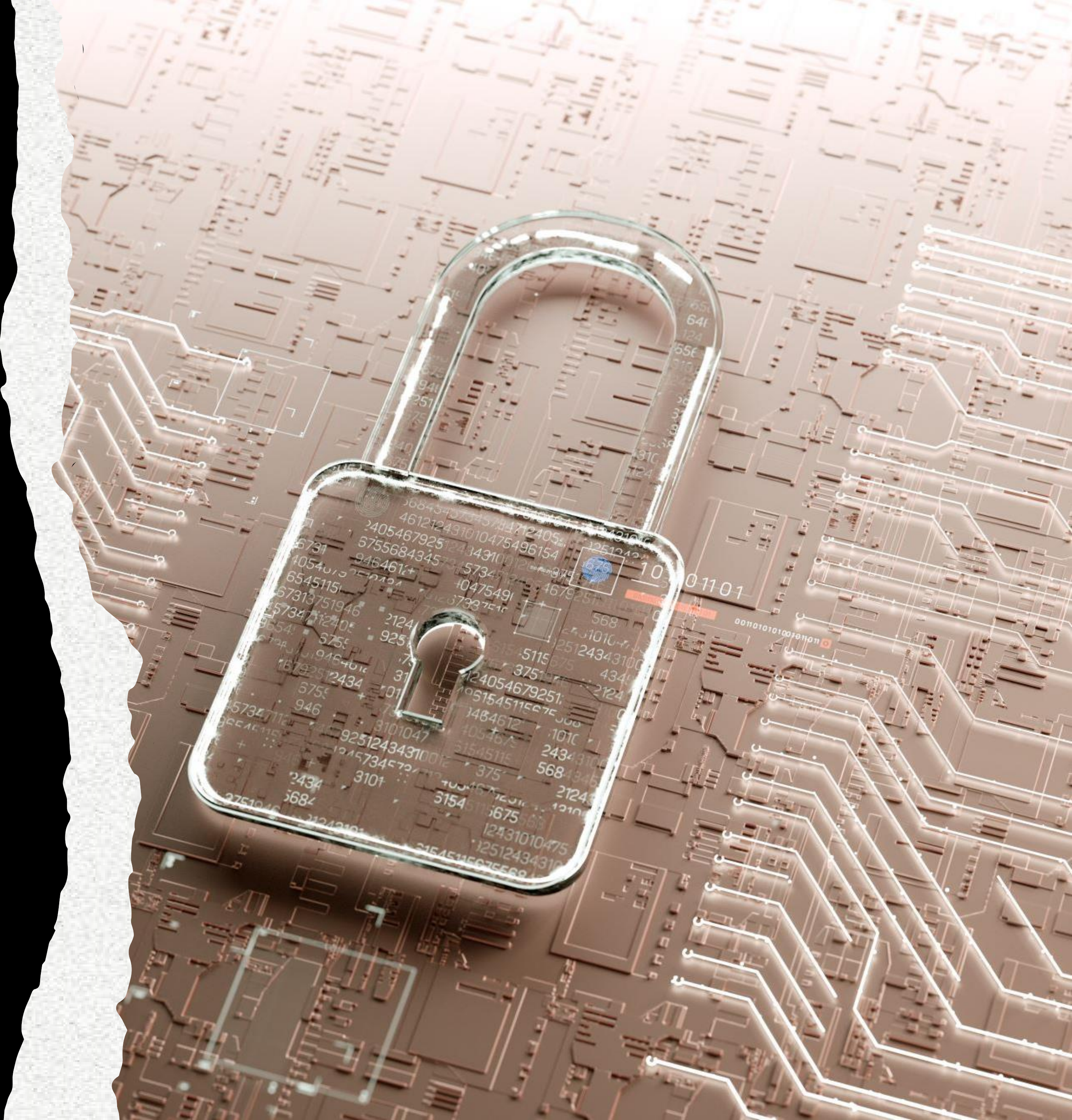
Galaxy Growth Media

Why people do that?

- Financial Gain
- Targeted Espionage
- Data Theft
- Psychological Manipulation
- Low Cost, High Impact
- Testing Security Boundaries
- Malicious Intent or Revenge

SILENT LOCKDOWN

Ransomware is a type of malicious software that **locks or encrypts your files**, then demands **payment** (a ransom) to restore access.



Why Is It So Dangerous?

🔒 **Paralyzes entire systems** —When ransomware strikes, it doesn't just lock a few files — it can bring down **entire operations**. Hospitals can't access patient charts. Airports can't process flights. Cities can't provide basic services. Everything grinds to a halt.

📂 **Data is held hostage** —Attackers **encrypt critical data** and then go after backups to prevent recovery. This means even disaster recovery plans may fail unless isolated properly. The only way out? Pay — or lose everything.

💸 **No guarantee of recovery** — Many victims **never regain full access**, even after sending cryptocurrency to attackers. Some decryption keys fail. Others demand more money. It's a **high-stakes gamble with no safety net**.

🌐 **Spreads rapidly across networks** —Once inside, ransomware can **move laterally** through shared drives, servers, and cloud systems, infecting hundreds or thousands of machines in minutes. The result? **Massive disruption** across every department.

🏥 **High financial and human cost** — In healthcare, ransomware can delay **life-saving procedures**, cause **patient deaths**, and expose **confidential health records**. The financial damage can exceed millions — not just in ransom, but in downtime, lawsuits, and lost trust.

🔐 **Encrypted using military-grade algorithms** - Attackers use **strong encryption** (like AES-256), which is **impossible to crack without the decryption key**. Traditional IT tools can't reverse it. That's what makes ransomware so potent — it's not just a virus, it's a vault.

Locker

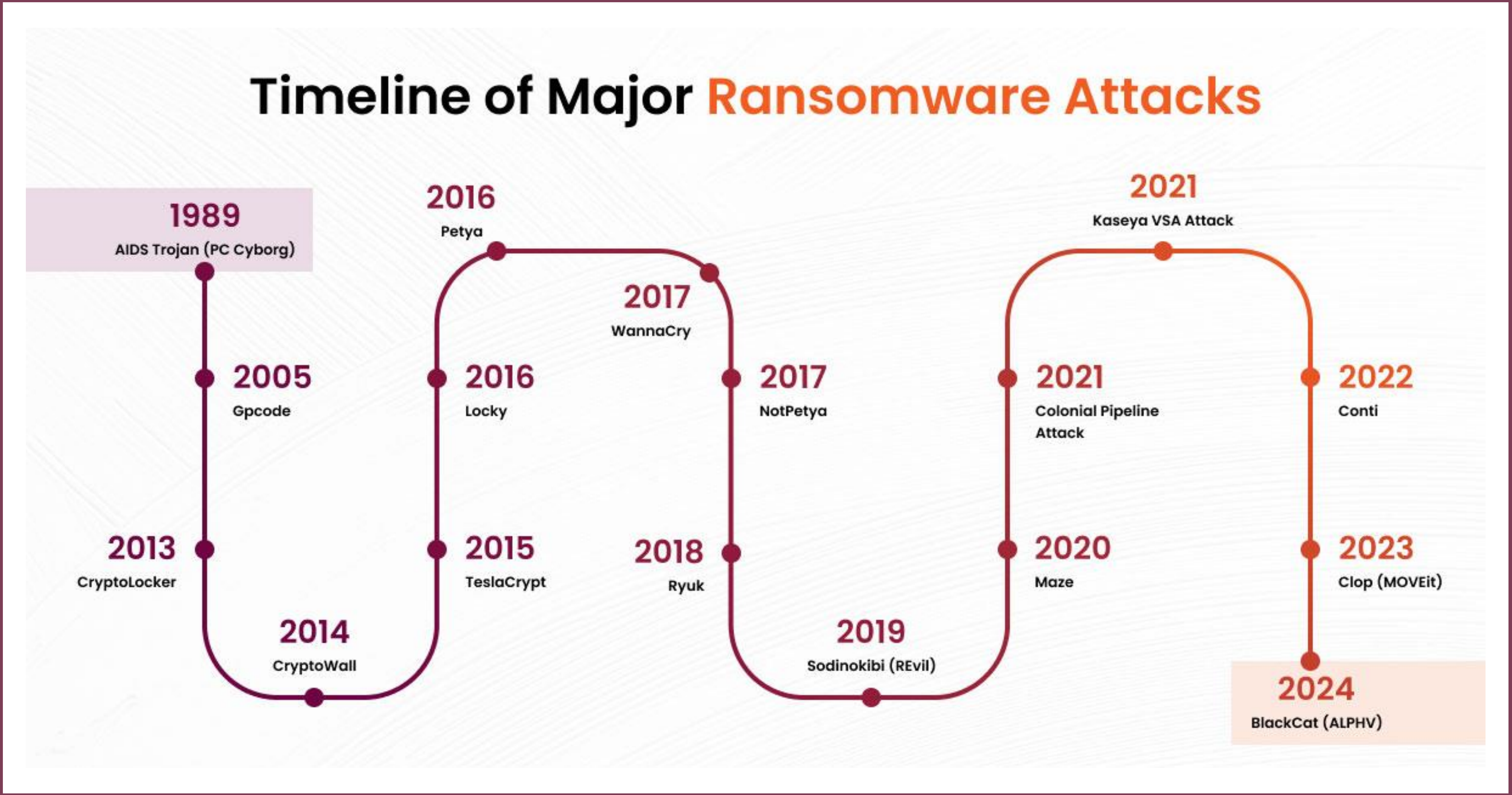
This type of ransomware locks the victim out of their computer or mobile device, preventing access to files, applications, or even the operating system.

Locker ransomware displays a message claiming that the victim has violated a law or committed some other offense and demands payment for device unlocking.

Crypto

This type of ransomware encrypts a victim's files or entire hard drive, rendering them inaccessible until a ransom is paid.

Attackers often demand payment in cryptocurrency, such as Bitcoin, in exchange for a decryption key



Timeline of Major Ransomware Attacks

1989
AIDS Trojan (PC Cyborg)

2005
Gpcode

2013
CryptoLocker

2014
CryptoWall

2015
TeslaCrypt

2016
Locky

2016
Petya

2017
WannaCry

2017
NotPetya

2018
Ryuk

2019
Sodinokibi (REvil)

2020
Maze

2021
Colonial Pipeline Attack

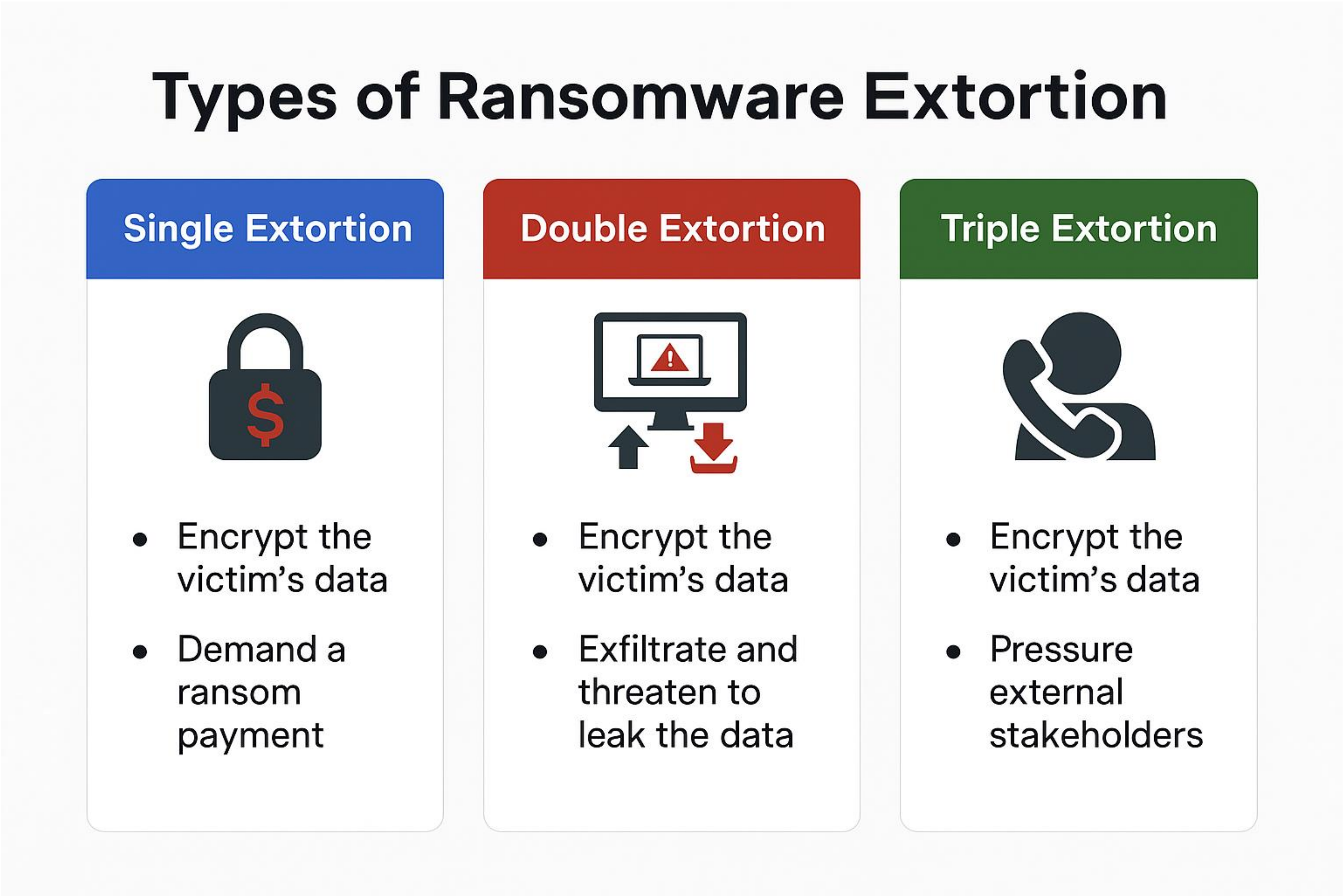
2021
Kaseya VSA Attack

2022
Conti

2023
Clop (MOVEit)

2024
BlackCat (ALPHV)

Credits - Parablu



Types of Ransomware Extortion

Single Extortion

- Encrypt the victim’s data
- Demand a ransom payment

Double Extortion

- Encrypt the victim’s data
- Exfiltrate and threaten to leak the data

Triple Extortion

- Encrypt the victim’s data
- Pressure external stakeholders

STAKES

🧩 **Impact Area**	📌 **Consequence**	**Real-World Example**
🏥 **Patient Care**	Delays, emergency diversions, cancelled surgeries	**WannaCry (2017)** – UK NHS hospitals canceled 19,000+ appointments
⚠️ **Human Safety**	Potential fatalities, medical errors due to system downtime	**Düsseldorf University Hospital (2020)** – Ransomware rerouted a patient who later died
🔐 **Data Privacy**	Leaked records, HIPAA violations, reputational damage	**Eskenazi Health (2021)** – Sensitive patient data published on dark web
💰 **Financial Cost**	Ransom payments, lawsuits, recovery expenses, insurance issues	**Change Healthcare (2024)** – Ransomware attack caused billing outages, cost estimated **$872M**+
⚙️ **Operations**	Paper-based workarounds, halted communication, EHR inaccessibility	**UHS (2020)** – 400+ hospitals went manual for days, impacting care
🚚 **Supply Chain**	Disrupted delivery of meds, lab results, and critical equipment	**Fresenius (2020)** – Global healthcare supplier hit, affecting dialysis services
🧠 **Mental Health**	Burnout among staff, stress and anxiety among patients	**Vastaamo Clinic (Finland, 2020)** – Therapy notes leaked; patients blackmailed
🔬 **Research**	Loss or theft of clinical trials, disrupted pharma/biotech innovation	**Hammersmith Medicines Research (2020)** – COVID-19 trial data stolen

Symmetric Key

Same key is used for both **encryption and decryption**.

Think: 🔑 → lock and unlock with the **same** key.

Asymmetric Key

Uses a **key pair**

Public key – used to encrypt

Private key – used to decrypt

One Step Deeper

The adversary generates a (public, private) key pair using an asymmetric encryption scheme and embeds the public key in the malware.

The malware encrypts the victim's data using a random symmetric key sk and the malware's public key.

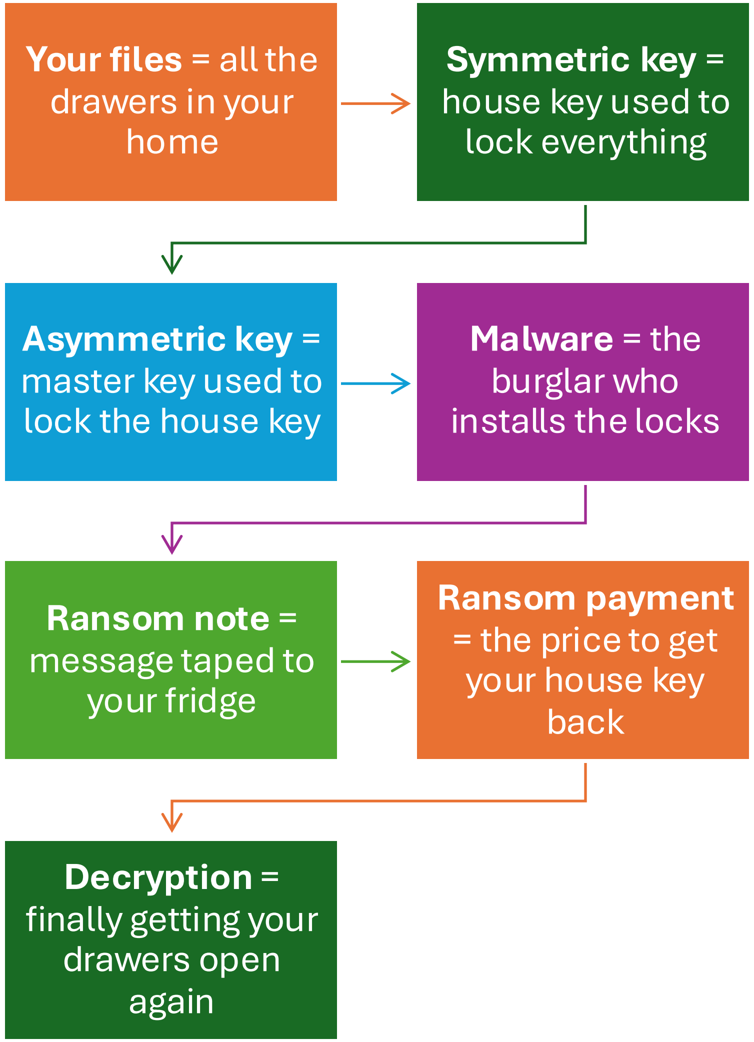
This produces two encrypted data components: (i) asymmetric encryption of the symmetric key sk (A) and (ii) symmetric encryption of the victim's data (B).

The malware sends (A) to the attacker and displays a ransom message to the user.

The victim pays the ransom, and the attacker decrypts A to obtain the symmetric key sk.

The attacker delivers sk to the victim, who then decrypts B using sk to recover the data and complete the attack.

One Step Easier



Your files = all the drawers in your home

Symmetric key = house key used to lock everything

Asymmetric key = master key used to lock the house key

Malware = the burglar who installs the locks

Ransom note = message taped to your fridge

Ransom payment = the price to get your house key back

Decryption = finally getting your drawers open again

Data Breaches

A breach doesn’t happen in one moment.

It’s a **domino effect** — one small crack leads to a data disaster.

Entry Point

How it happens?

Phishing emails

Exposed credentials

Unpatched software

Cloud misconfigurations

"Most attackers don’t break in — they log in."

Lateral Movement

What happens next?

Once inside, attackers **move sideways**, hopping from one system to another, gathering more credentials and mapping out the environment.

“It’s like walking through unlocked doors in a hotel, room to room, until you reach the vault.”

Data Exfiltration

The final blow:

Sensitive data is compressed, encrypted, and **silently exported** to an external server.

Victims often don’t notice for weeks or even months.

"By the time you find out, the data is long gone."

Breaches impact more than balance sheets — they hit reputation, trust, and careers.

Cost Beyond Dollars

💼 **Marriott (2018)**	**Impact:** 500 million guest records stolen	**Root Cause:** Long-term undetected breach after acquisition	**Aftermath:** Fines, lawsuits, reputation loss, customer anxiety	“Would you book again with a hotel that lost your passport data?”
📃 **Equifax (2017)**	**Impact:** 147 million SSNs, addresses, and DOBs leaked	**Cause:** Missed patch for known vulnerability	**Aftermath:** $700M+ in settlements, CEO resigned, massive trust erosion	“A single missed update became a national security risk.”
🚗 **Uber (2016/2017)**	**Impact:** 57 million user records stolen	**Cause:** Hackers accessed GitHub, used hardcoded credentials	**Aftermath:** Uber paid hush money, execs were criminally charged in 2022	“They tried to hide the breach — and paid for it later.”

“The real cost of a breach isn’t the ransom or the fine — it’s the **trust you lose**, and the time it takes to earn it back.”

AI-Powered Attacks

When AI Attacks: Smarter, Faster, and More Deceptive

Deepfakes in Cybercrime

- Fake voice calls from CEOs asking for wire transfers
- Synthetic videos used in blackmail and disinformation
- **Real example:** Deepfake of European company exec used to steal $243K

Spot the Deep Fake

AI-Powered Attacks- Continues

AI-GENERATED TEXT (NLP) ATTACKS – PHISHING EMAILS, CHATBOT IMPERSONATION, MISINFORMATION CAMPAIGNS

AUTOMATED VULNERABILITY DISCOVERY – SOFTWARE VULNERABILITY

BIOMETRIC AND SURVEILLANCE ATTACKS - FACIAL RECOGNITION SPOOFING, VOICE BIOMETRIC BYPASS

AI-Powered Drone Attacks

1. Autonomous Surveillance & Reconnaissance

- Drones can autonomously navigate using AI (e.g., computer vision, SLAM).
- Malicious drones can spy on secure areas, gather intel, or track individuals.

2. Payload Delivery

- AI-controlled drones can carry explosives or malware-injecting devices to specific GPS coordinates.
- Facial or object recognition can trigger attacks only on target identification.

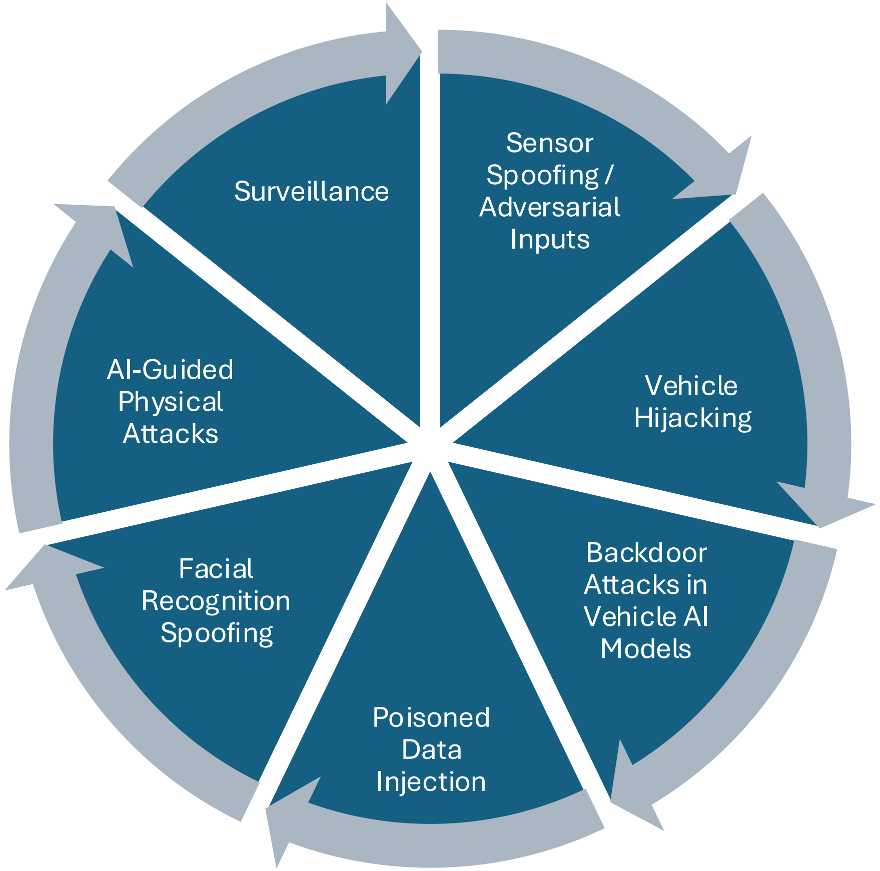
3. Swarm Attacks

- Multiple AI-powered drones acting as a swarm using decentralized decision-making.
- Hard to detect, defend against, or disable due to adaptive flight patterns.

4. Signal Jamming and GPS Spoofing

- AI-enabled drones can jam or spoof navigation systems, leading to operational chaos.

Attacks on/by Autonomous Vehicles



Surveillance

Sensor Spoofing / Adversarial Inputs

Vehicle Hijacking

Backdoor Attacks in Vehicle AI Models

Poisoned Data Injection

Facial Recognition Spoofing

AI-Guided Physical Attacks

AI for Defense

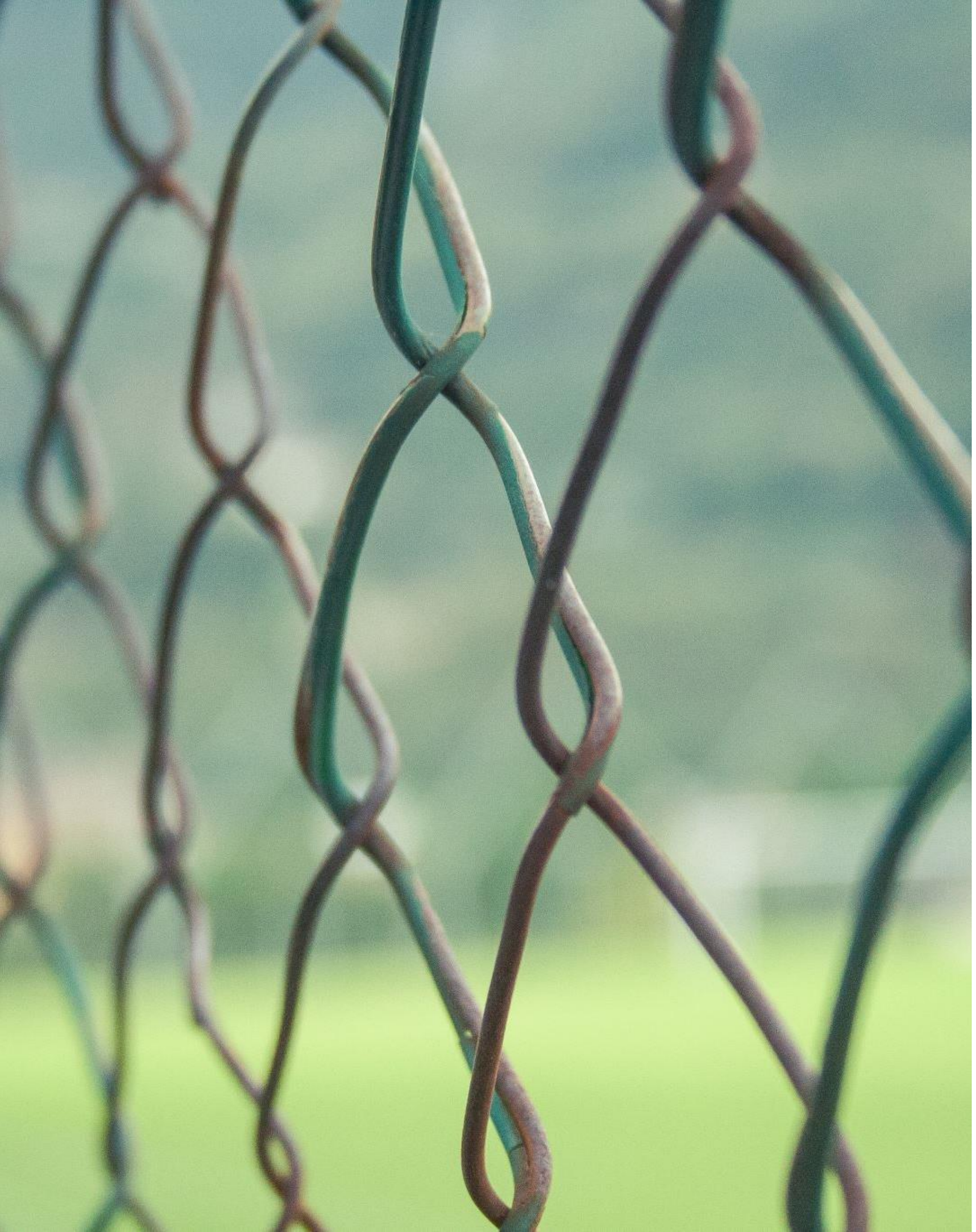
When AI Fights Back: Your Smartest Cybersecurity Ally

Use Cases

Behavioral Analytics

Anomaly/ Phishing Detection

Predictive Patching



Behind every click is a person. Behind every breach is a story.

Simple Actions, Big Impact

- Enabling multi-factor authentication
- Updating software regularly
- Using strong and unique passwords
- Being cautious with links and attachments
- Backing up data

In the age of AI and invisible threats, awareness is your superpower

“The best way to predict the future is to secure it”

THANK YOU

Q&A