Famous Cyber Attacks **Worldwide**

The world of cybersecurity is increasingly complex and often suffers from significant attacks, impacting both individuals and organizations.

WannaCry Ransomware Attack

The Attack

WannaCry was a global ransomware attack that affected over 200,000 computers in 150 countries in 2017.

It targeted computers using Microsoft Windows and exploited a vulnerability known as "EternalBlue", leaked from the National Security Agency by a team Called Shadow Brokers.

Impact

The attack disrupted critical infrastructure, including hospitals, businesses, and government agencies.

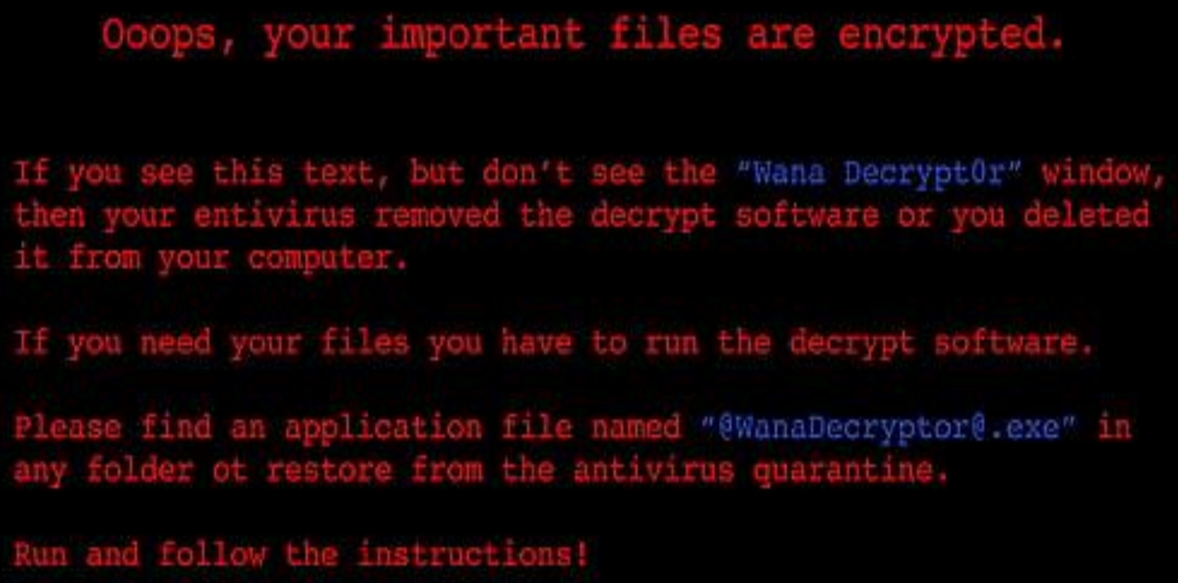
It encrypted files and demanded a ransom payment in Bitcoin to unlock them.

Consequences

The attack highlighted the vulnerability of critical infrastructure and the potential for significant damage.

It also led to increased awareness and investment in cybersecurity measures.

Data Breaches Associated with the Attack



```
    Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window,
then your entivirus removed the decrypt software or you deleted
it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in
any folder ot restore from the antivirus quarantine.

Run and follow the instructions!
```

1 Healthcare Records

Hospitals and healthcare providers were heavily affected, with patient data being compromised, including personal information, medical records, and financial details.

2 Financial Data

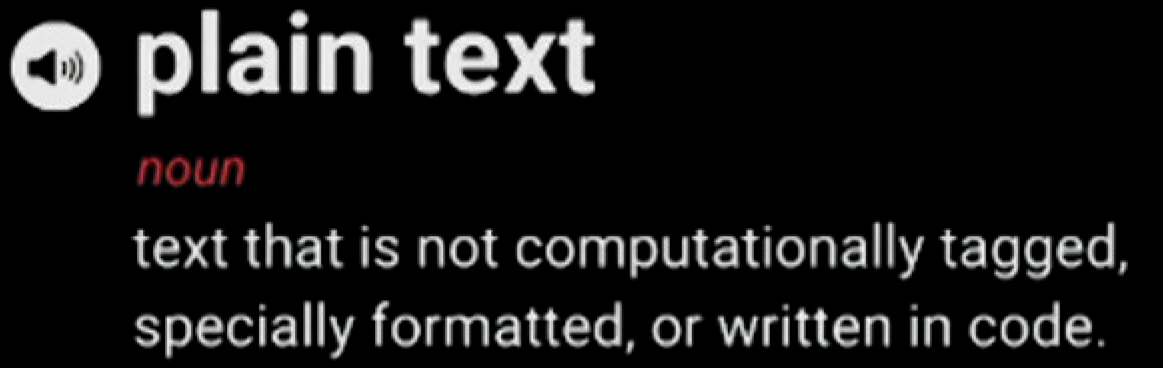
Banks and financial institutions were also targeted, with attackers gaining access to sensitive financial data, including account numbers, credit card information, and transaction details.

3 Personal Information

The attack affected individuals across various sectors, resulting in the theft of personal data such as names, addresses, social security numbers, and email addresses.

4 Business Records

Businesses were also affected, with attackers gaining access to proprietary data, financial information, and customer data, potentially impacting operations and reputation.



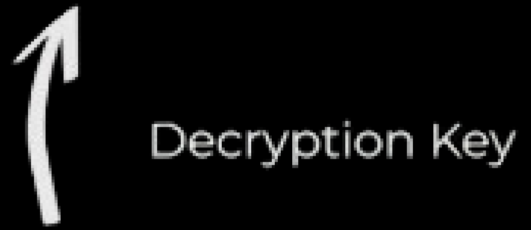
plain text

noun

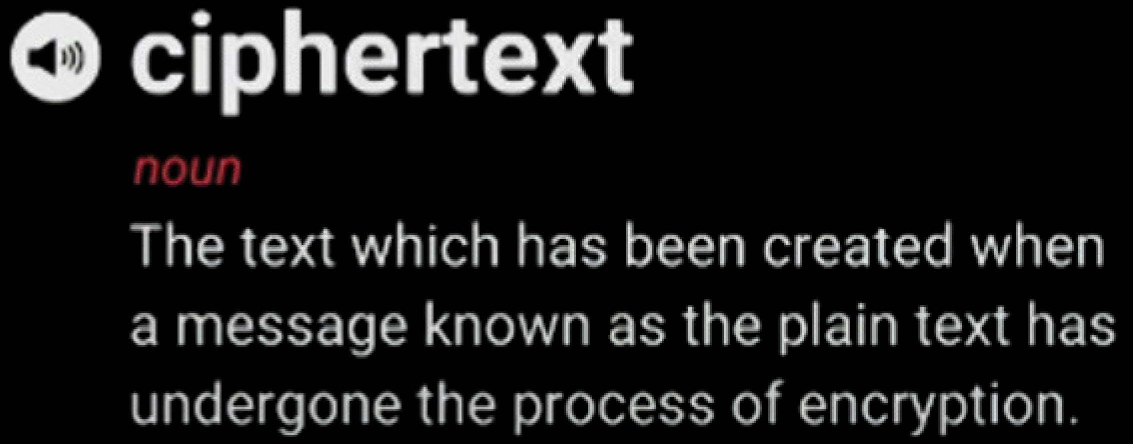
text that is not computationally tagged, specially formatted, or written in code.

example

The quick brown fox jumps over the lazy dog.



Decryption Key



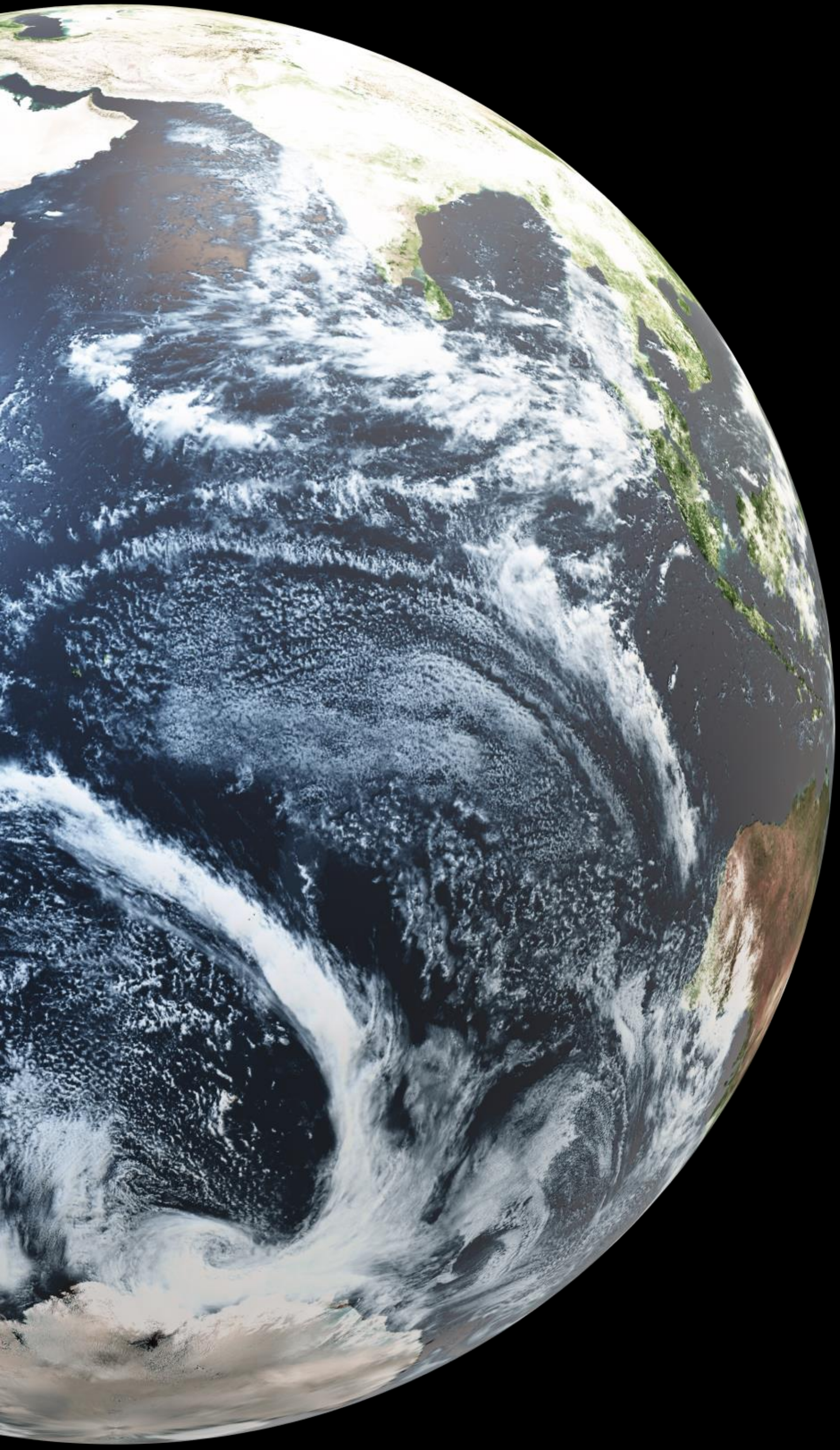
ciphertext

noun

The text which has been created when a message known as the plain text has undergone the process of encryption.

example

Aol xbpjr iyvdu mve qbtwz vcly aol shgf kvn.



COUNTRIES AFFECTED (< 3 HOURS)

- GERMANY
- RUSSIA
- TURKEY
- KAZAKHSTAN
- INDONESIA
- VIETNAM
- JAPAN
- SPAIN

* DATA BREACH *** DATA BREACH *
!!! CYBER !!!
ATTACK
* DATA BREACH *** DATA BREACH *

Analyze the Types of **Data Compromised**

Type of Data	Examples
Personal Information	Names, addresses, social security numbers, email addresses, phone numbers
Financial Data	Credit card numbers, bank account details, transaction history
Medical Records	Patient names, diagnoses, treatment plans, medical history
Business Records	Financial statements, customer data, intellectual property
Government Data	Government documents, classified information, sensitive data

Attack Scenario

1

Exploiting Vulnerability

The attack leveraged the "EternalBlue" exploit, allowing attackers to remotely execute code on vulnerable computers.

2

Spreading the Malware

The malware quickly spread to other vulnerable machines through network connections, creating a chain reaction.

3

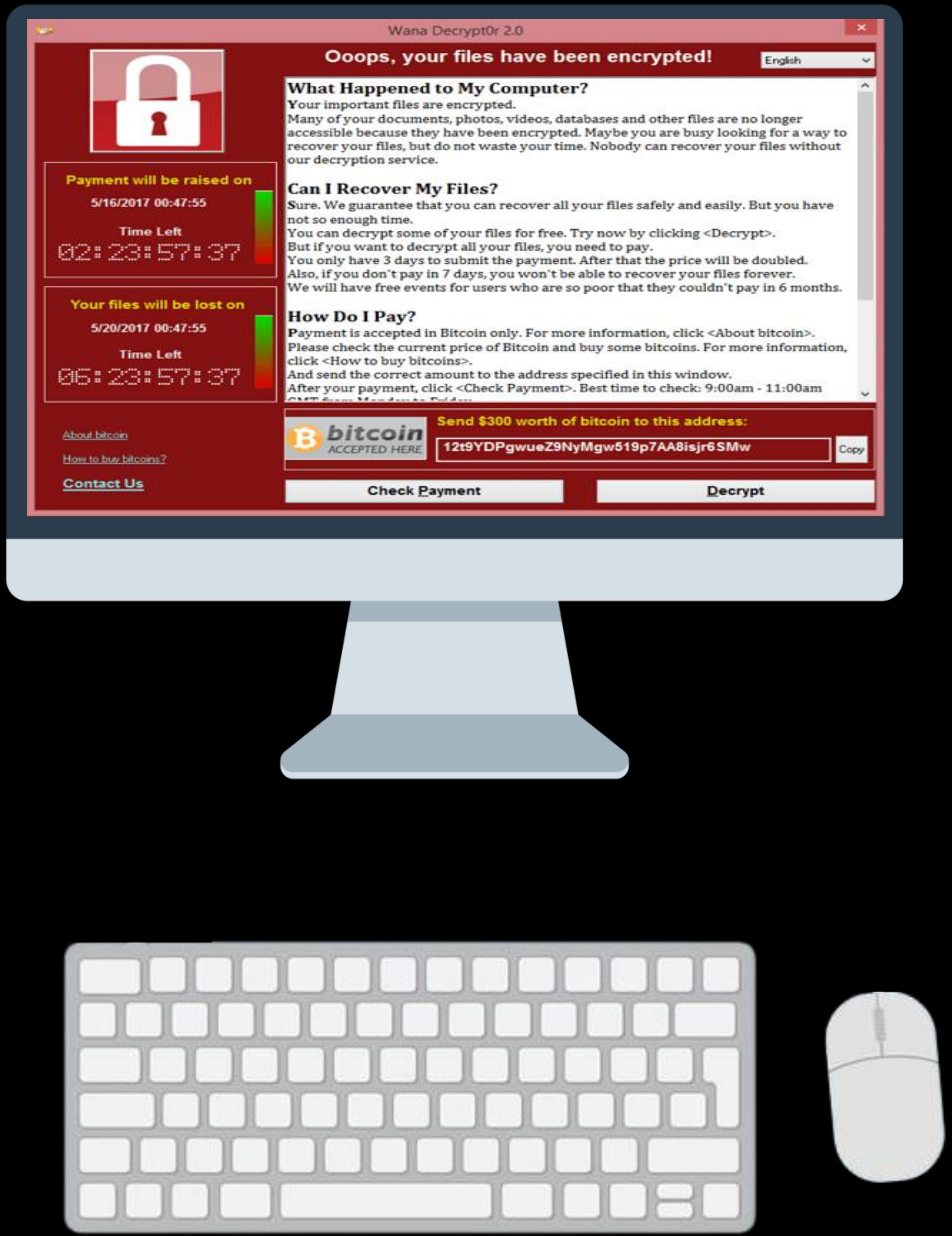
Encrypting Files

Once infected, WannaCry encrypted files on the infected computer, making them inaccessible to the user.

4

Ransom Demand

Attackers demanded a ransom payment in Bitcoin to decrypt the files, threatening to permanently delete them if the ransom wasn't paid.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Agencies Related to the Attack

National Security Agency (NSA)

The NSA developed the "EternalBlue" exploit, which was later leaked and used by the WannaCry attackers.

Microsoft

Microsoft released security patches to address the "EternalBlue" vulnerability, but many organizations were slow to apply them.

UK's National Cyber Security Centre (NCSC)

The NCSC played a crucial role in identifying and mitigating the WannaCry attack, including releasing a "kill switch" that helped stop the spread of the malware.

Europol

Europol coordinated international efforts to investigate the attack and track down the perpetrators.

Resulting Losses

Financial Losses

The attack caused significant financial losses, including the cost of restoring systems, paying ransom demands, and dealing with the aftermath of data breaches.

Reputational Damage

The attack damaged the reputation of affected organizations, impacting public trust and customer confidence.

Impact on CIA Triad

1 Confidentiality

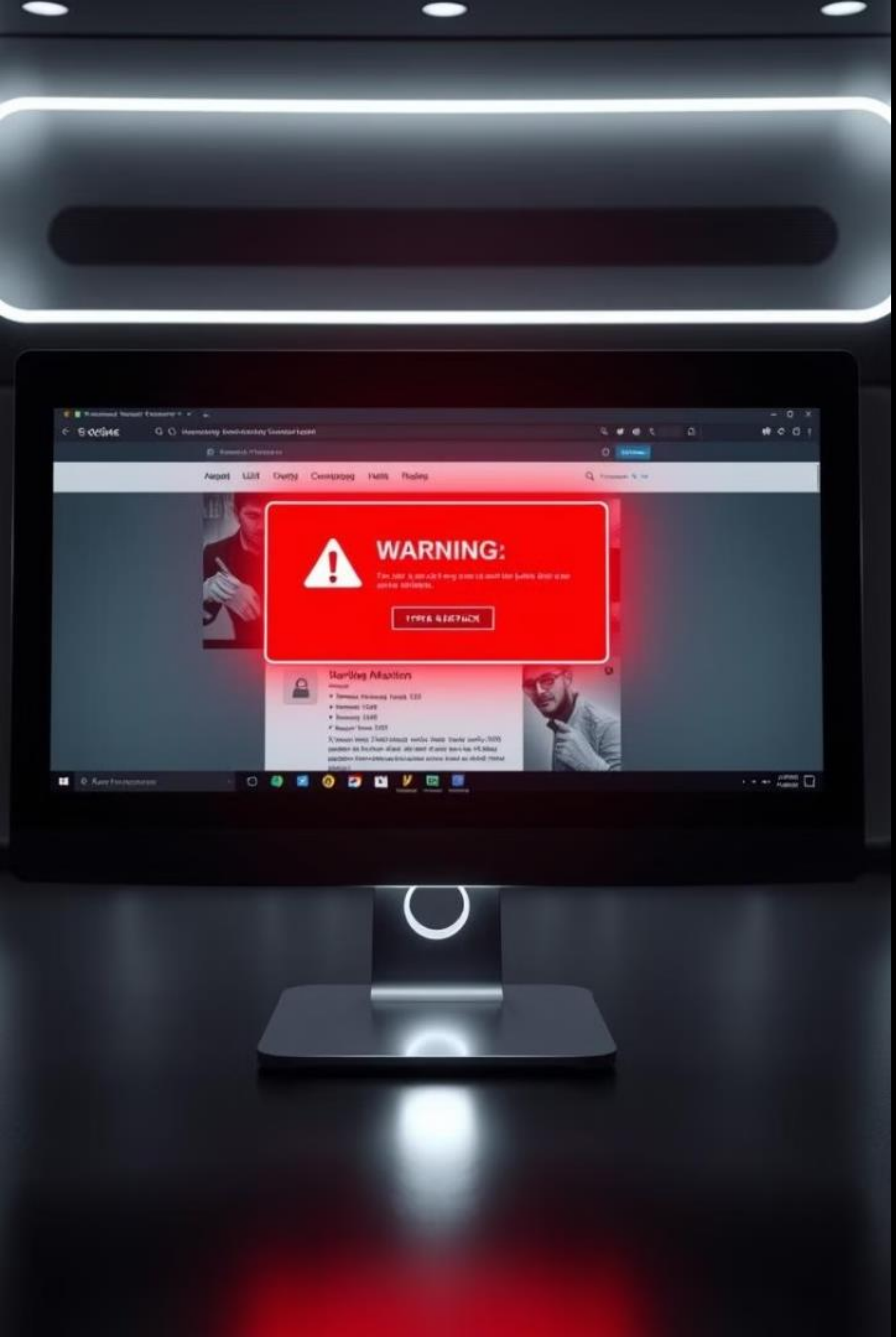
The attack compromised the confidentiality of sensitive data, exposing personal information, financial details, and proprietary business data.

2 Integrity

The attack compromised the integrity of data by encrypting files and altering their content, rendering them unusable.

3 Availability

The attack severely impacted the availability of systems and data, preventing users from accessing critical information and services.



SpyEye Botnet : A Notorious Cyberattack

The SpyEye botnet was a sophisticated and highly destructive malware campaign that wreaked havoc across the globe in the late 2000s and early 2010s. It posed a serious threat to individuals and businesses alike, leading to numerous data breaches and financial losses.

Data Breaches Associated with the Cyber Attack

1 Financial Institutions

SpyEye targeted banks and financial institutions, stealing sensitive customer information and financial data.

2 E-Commerce Businesses

Online retailers were another primary target, as SpyEye aimed to steal customer credit card information and payment details.

3 Government Agencies

SpyEye also targeted government agencies, potentially compromising sensitive data related to national security or public safety.

4 Individual Users

Individual users were also victims of SpyEye, with their personal data, including passwords and bank account information, being compromised.

Types of **Data Compromised**

Credit Card Numbers	Usernames	Passwords
Bank Account Information	Social Security Numbers	Personal Identification Documents
Medical Records	Financial Statements	Confidential Business Data

Attack Scenario

1

Infection

The SpyEye botnet spread through malicious emails, infected websites, and vulnerabilities in software.

2

Data Theft

Once infected, the botnet would steal sensitive information from the victim's computer and send it to the attackers' servers.

3

Command and Control

The attackers used a command and control network to manage the botnet and issue commands to infected computers.

4

Financial Gains

The stolen information was then used to commit financial crimes, such as identity theft and online fraud.

Agencies Related to the Attack

Federal Bureau of Investigation (FBI)

The FBI led the investigation into SpyEye, working with international law enforcement agencies to dismantle the botnet.

Europol

Europol, the European Union's law enforcement agency, collaborated with the FBI to coordinate the international response to the SpyEye threat.

National Cyber Security Alliance (NCSA)

The NCSA played a vital role in raising awareness about the SpyEye botnet and providing guidance to individuals and businesses on how to protect themselves.

Resulting Losses

Financial Losses

SpyEye caused billions of dollars in financial losses, including stolen funds, credit card fraud, and identity theft.

Reputational Damage

Victims suffered reputational damage, as the theft of sensitive information could lead to loss of trust and confidence among customers and stakeholders.

Legal Consequences

The SpyEye botnet resulted in legal action against individuals and organizations involved in the attack, leading to fines, convictions, and other legal consequences.

Impact on **CIA Triad**

Confidentiality

SpyEye compromised the confidentiality of sensitive information, such as personal data and financial records.

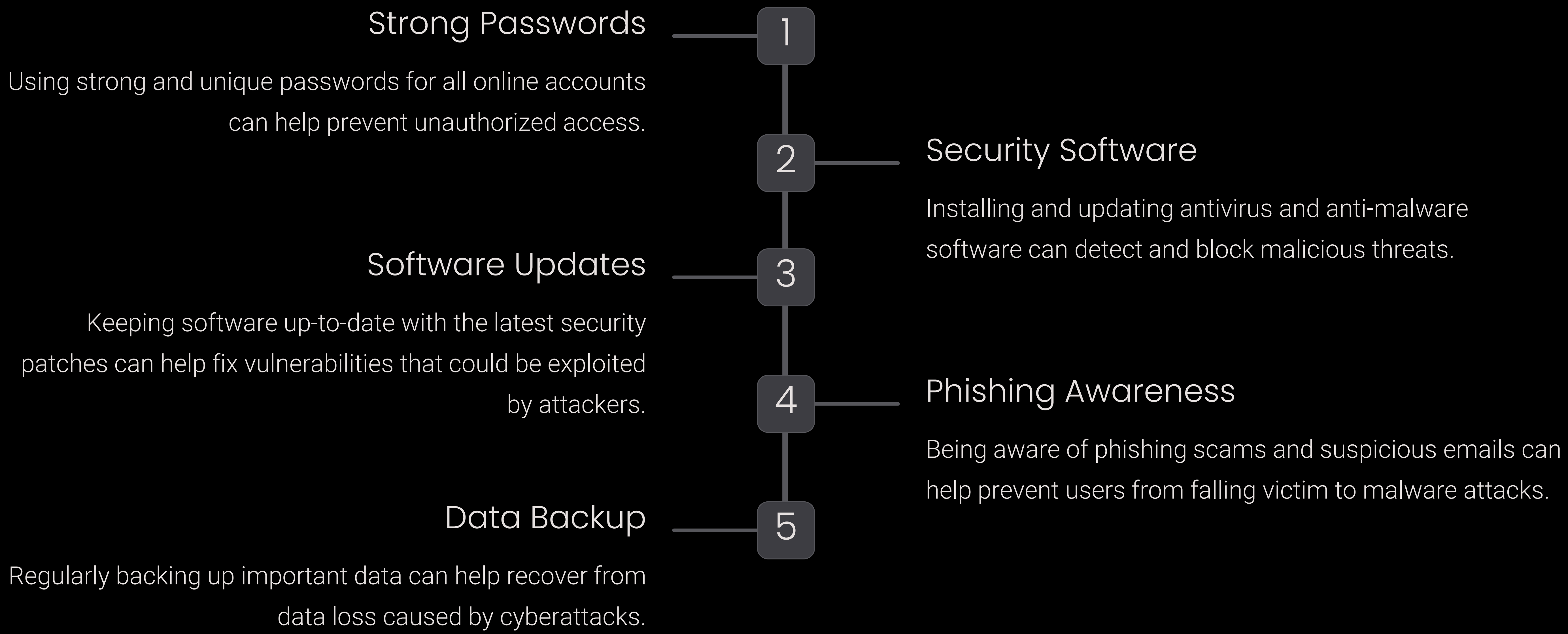
Integrity

The botnet could alter or manipulate data on infected computers, compromising the integrity of information and systems.

Availability

SpyEye could disrupt the availability of systems and networks, making it difficult for individuals and businesses to access critical data and services.

Lessons Learned and Mitigation Strategies



1. **Strong Passwords**

   Using strong and unique passwords for all online accounts can help prevent unauthorized access.

2. **Security Software**

   Installing and updating antivirus and anti-malware software can detect and block malicious threats.

3. **Software Updates**

   Keeping software up-to-date with the latest security patches can help fix vulnerabilities that could be exploited by attackers.

4. **Phishing Awareness**

   Being aware of phishing scams and suspicious emails can help prevent users from falling victim to malware attacks.

5. **Data Backup**

   Regularly backing up important data can help recover from data loss caused by cyberattacks.

Target Data Breach : A Case Study in Cyber Security

In 2013, Target, a major American retailer, suffered a massive data breach that affected millions of customers. The attack exposed sensitive personal information and served as a wake-up call for businesses regarding cybersecurity.

Data Breached

1
Credit Card Information

The attackers stole credit card numbers, expiration dates, and CVV codes.

2
Personal Information

Names, addresses, phone numbers, and email addresses were also compromised.

3
Debit Card Information

Some debit card numbers were also stolen, putting customers at risk of financial loss.

4
Other Data

The attackers may have also accessed other sensitive information, such as purchase history and browsing activity.

Types of **Compromised Data**

Personal Identifiable Information (PII)	Names, addresses, phone numbers, email addresses
Financial Data	Credit card numbers, expiration dates, CVV codes, debit card numbers
Transaction Data	Purchase history, browsing activity

Attack Scenario

1

Initial Intrusion

The attackers gained access to Target's network through a third-party vendor.

2

Data Exfiltration

The attackers then stole customer data from Target's payment processing systems.

3

Discovery and Response

Target discovered the breach and alerted customers and law enforcement.

Agencies Involved

Federal Bureau of Investigation (FBI)

The FBI led the investigation into the Target data breach.

Secret Service

The Secret Service also assisted in the investigation, focusing on credit card fraud.

Target

Target cooperated with law enforcement and took steps to mitigate the damage.

Financial, Reputational, and Legal Losses

Financial Losses

Target incurred significant costs due to the breach, including legal fees, credit monitoring services for customers, and lost revenue.

Reputational Damage

The breach damaged Target's reputation, eroding customer trust and potentially impacting future sales.

Legal Consequences

Target faced numerous lawsuits from customers and regulators, resulting in substantial legal costs and settlements.

Impact on CIA Triad

1

Confidentiality

The breach compromised the confidentiality of customer data, exposing sensitive information to unauthorized parties.

2

Integrity

The integrity of Target's systems was compromised, as the attackers were able to modify data and potentially introduce malware.

3

Availability

The breach disrupted Target's operations, as systems had to be taken offline for investigation and remediation.

Lessons Learned and Recommendations

Strengthen Security

Businesses need to invest in robust security measures to protect against cyberattacks.

Third-Party Risk Management

Businesses need to carefully vet and manage third-party vendors to minimize the risk of breaches.

Incident Response Planning

Businesses need to develop a comprehensive incident response plan to quickly and effectively address security incidents.

Employee Training

Employees need to be trained on cybersecurity best practices to prevent phishing attacks and other threats.

Strategies for Mitigating Cyber Risks

1

Regular Updates

Install security updates promptly. Patches often address vulnerabilities that attackers exploit.

2

Strong Passwords

Use complex and unique passwords for each account. Avoid using easily guessable combinations.

3

Multi-Factor Authentication

Enable multi-factor authentication (MFA) whenever possible, adding an extra layer of security.

4

Backups

Regularly back up important data and store it offline. This allows recovery even if data is encrypted.

5

Employee Training

Educate employees about cybersecurity threats and best practices. Human error is a major vulnerability.

THANK YOU

- Group 8

- Namitha Raveendran
- Nanda Krishnan V
  Neeraj Jayesh
- Prathibha Pradeep
- Praveen N