WHAT DID WE LEARN FROM THE MOST DESTRUCTIVE CYBER ATTACKS?

Understanding the past to secure our digital future

Diana Moldovan, ASOS, UK
moldovan.diana1987@gmail.com

Evolution and Impact of Cyberattacks



Evolution of Cyberattacks

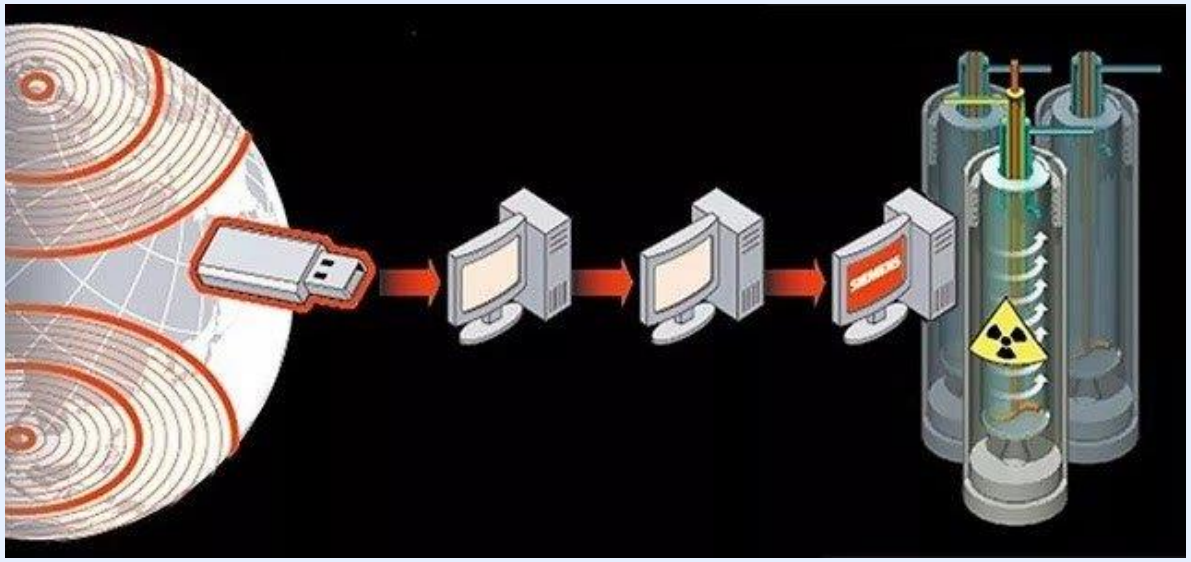
Cyberattacks evolved from isolated incidents to global crises over decades. They now target governments, businesses, and individuals.

Importance of Historical Analysis

Studying past cyberattacks helps improve defense strategies effectively.

Major Cybersecurity Incidents

Stuxnet (2010)



Cyber Weapon Innovation

Stuxnet was a groundbreaking cyber weapon causing physical damage via digital means.

Zero-Day Exploits

It exploited four zero-day vulnerabilities in Windows to infiltrate critical systems.

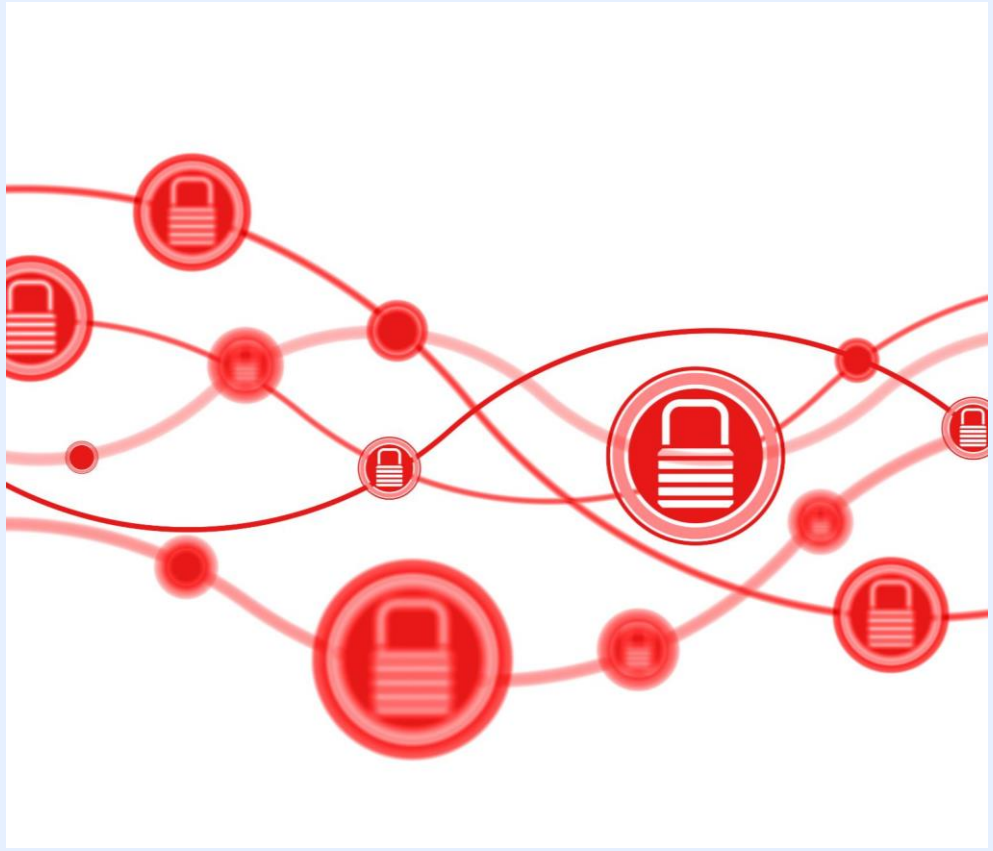
Industrial Control Disruption

Stuxnet manipulated PLCs and SCADA to alter centrifuge operations and mask status.

Lessons learnt

Highlights securing OT and IT, protecting air-gapped systems, and layered defenses.

SolarWinds Supply Chain Attack (2020)



Malicious Code Injection

Attackers inserted harmful code into Orion software updates affecting thousand of organisations globally.

Advanced Hacking Techniques

Attackers altered sealed code, used domain targeting, and mimicked communication to avoid detection.

Nation-State Cyber Espionage

The breach was attributed to Russian's Foreign Intelligence Service, targeting sensitive US government agencies and organisational data.

Lessons Learnt

Highlights need for secure supply chains, zero trust, continuous monitoring, and vendor control.

Equifax Data Breach (2017)



Massive Data Exposure

Personal information of 147 million individuals was exposed, causing huge trust loss , financial penalties and $700m in settlements.

Cause of Breach

Attackers exploited an unpatched Apache Struts vulnerability to access Equifax's data systems.

Lessons learnt

Regular audits, timely patching, and strong threat management are essential for data protection.

WannaCry Ransomware Attack (2017)



Global Impact

WannaCry affected over 200,000 computers in 150 countries worldwide, with losses estimated at $4-8 billion.

Exploitation method

The attack used the EternalBlue Windows vulnerability leaked by Shadow Brokers.

Critical Infrastructure Disruption

Hospitals, telecom, and transport sectors faced major disruptions from the ransomware.

Lessons learnt

Timely patching, network segmentation, backups, and training are vital defenses.

NotPetya Malware Attack (2017)



Cyber weapon

NotPetya was a destructive malware disguised as ransomware, causing global disruption and losses of over $10b.

Propagation Mechanisms

It exploited EternalBlue vulnerability and credential theft to spread rapidly across networks (Mimikatz).

Impact

The attack caused billions in damages, affecting major corporations worldwide.

Lessons learnt

Lessons include network segmentation, reliable backups, and thorough employee training.

Comparative Analysis

WannaCry vs NotPetya

⚙️ Purpose

• WannaCry – Financial ransomware aiming for ransom payments.

• NotPetya – Disguised as ransomware but actually a destructive wiper.

🌍 Impact

• WannaCry hit 200,000+ systems in 150+ countries. Financial ransomware aiming for ransom payments.

• NotPetya caused $10B+ in damages, crippling major corporations.

⚒️ Technical Details

• Both used EternalBlue exploit (Windows SMBv1 vulnerability).

• WannaCry encrypted files; NotPetya wiped the Master File Table (MFT).

💡 Key Difference

• WannaCry sought money.

• NotPetya sought chaos and disruption.

Key Takeaways

Conclusions and Best Practices

- **Shared Responsibility -** Cybersecurity requires vigilance across all organizational levels to effectively mitigate risks.
- **Regular Updates -** Applying patches and software updates closes vulnerabilities preventing potential attacks.
- **Data Protection -** Backups and encryption safeguard sensitive information from unauthorized access or loss.
- **Zero Trust Architecture -** Continuous access verification reduces risks of unauthorized entry in the network.
- **Third-Party Risk Management -** Monitoring vendor vulnerabilities prevents supply chain attacks and enhances security.
- **User Education -** Training reduces human error, the weakest link in cybersecurity defense.