Case Study-The NotPetya Cyberattack (2017)

The destructive wiper more than ransomware - Billions-Dollar Deception.

Attack Type

Destructive Wiper Malware

NotPetya masqueraded as ransomware but was primarily designed for irreversible data destruction, not financial gain.

M.E.Doc

The primary infection vector was a compromised software update for the Ukrainian accounting program, M.E.Doc.

MBR Corruption for SMB exploit

NotPetya mimicked Petya ransomware, targeting Windows systems by corrupting the Master Boot Record (MBR). It propagated rapidly using SMB exploits for lateral movement, causing widespread data destruction.

Threat Actors

Russian Military Intelligence

Numerous governments and cybersecurity experts have formally attributed the NotPetya cyberattack to Russian military intelligence operations.

Primary Actor: Sandworm Team (Unit 74455)

The incident is widely classified as state-sponsored cyberwarfare, primarily targeting Ukrainian critical infrastructure.

NotPetya: Technical Overview

EternalBlue Exploit

Exploited the MS17-010 vulnerability in the SMBv1 protocol, enabling unauthenticated remote code execution and initial network compromise.

Mimikatz Credential Theft

Mimikatz is a tool that steals stored passwords and password codes from a computer's memory to allow an attacker to jump between machines on a network.

Master Boot Record infection

System Lockout

File System Encryption

Unrecoverable Data Destruction

NotPetya: Impact Analysis

10B
Economic Losses

300+
Organizations Affected

65
Countries Impacted

- False Ransom Demand - Financial Loss
- Irrecoverable Data Loss - Operational Loss
- Reputation Damage
- Customer Trust Lost

NotPetya: Detection & Response

Detection

Actively monitor network traffic for anomalous Server Message Block (SMB) activity and scrutinize attempts to access Local Security Authority Subsystem Service (LSASS) memory, indicative of potential credential dumping.

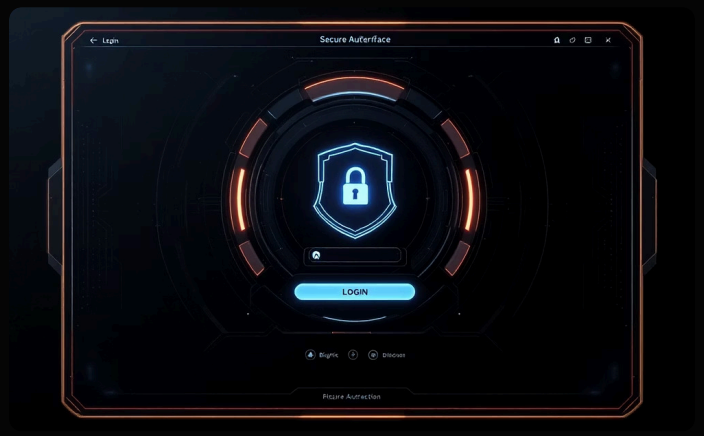
Response

Establish clear incident response plans, isolation protocols, and forensic capabilities to mitigate impact and recover swiftly.

NotPetya: Mitigation Strategies

Patch & Disable

Promptly apply the MS17-010 security update. Furthermore, disable the deprecated and vulnerable SMBv1 protocol across all endpoints and servers to mitigate known exploits and reduce the attack surface.



Protect Credentials

Enforce the principle of least privilege by removing excessive administrative rights. Implement robust credential protection mechanisms such as Credential Guard and Local Administrator Password Solution to prevent credential theft and lateral movement.

Segment & Backup

Implement network segmentation to logically isolate critical assets and restrict lateral movement of threats within the network. Establish and regularly verify DR backup systems to ensure data recoverability and resilience against ransomware attacks.

My Viewpoint

Estimating cyber infrastructure and making plan B with plan A!

Thank You

Remember, cybersecurity is a continuous commitment to vigilance and resilience. Let's build a more secure digital future together.