

# CYBER SECURITY CASE STUDIES

Presented By: Sajjad Ahmed



# COURSE TOPICS RECAP

**THREAT MODELING**

**CYBER KILL CHAIN**

**PHISHING ATTACKS**

**WEB SECURITY (OWASP  
TOP 10)**

**ENCRYPTION**

**PASSWORDS AND  
AUTHENTICATION**



# WHY CASE STUDIES?

- **DEPEND HEAVILY ON DIGITAL SYSTEMS**
- **LEARN FROM REAL FAILURES**
- **CONNECT THEORY WITH PRACTICE**
- **IDENTIFY COMMON PATTERNS**
- **IMPROVE RISK AWARENESS**





# CASE STUDY 1

## WannaCry Ransomware

## OVERVIEW

- GLOBAL CYBER ATTACK
- OVER 150 COUNTRIES
- MANY COMPANIES VICTIMIZED

## MALICIOUS PROGRAM

- LOCKED ALL FILES USING ENCRYPTION
- A MESSAGE ASKING FOR MONEY

## HOW SPREAD?

- OLD
- NOT UPDATED
- MISSING SECURITY PATCHES
- SPREAD AUTOMATICALLY ACROSS NETWORKS

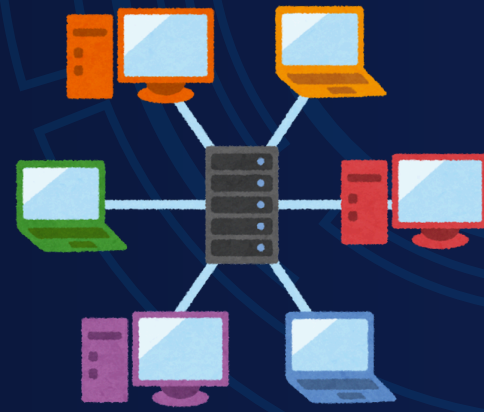
## HOW IT STOPED?

- WEBSITE: IUQERFSODP9IFJAPOSDFJHGOSURIJFAEWRWERGWEA.COM
- BOUGHT DOMAIN
- ACITIVATED HIDDEN KILL SWITCH

# PREVENTION



**Regular Software Updates**



**Network Segmentation**



**Strong Backup Strategy**



**Threat Modeling**



**Cyber Kill Chain**



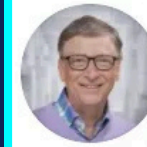
# CASE STUDY 2





# TWITTER HACK OVERVIEW

★ Pinned Tweet



**Bill Gates** ✓  
@BillGates

Everyone is asking me to give back, and now is the time.

I am doubling all payments sent to my BTC address for the next 30 minutes. You send \$1,000, I send you back \$2,000.



**Barack Obama** ✓ @BarackObama · 3m

I am giving back to my community due to Covid-19!

All Bitcoin sent to my address below will be sent back double. You send \$1,000, I will send back \$2,000!

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only doing this for the next 30 minutes! Enjoy.

💬 1.1K

↻ 2.6K

❤️ 3.3K



- **CONTROL ON HIGH-PROFILE ACCOUNTS**
- **PUBLIC TRUST**
- **FINANCIAL SCAMS**
- **FAKE MESSAGES FROM POPULAR ACCOUNTS**



# HOW THE ATTACK ESCALATED AND STOPPED

- SEARCHED LINKEDIN AND PUBLIC SOURCES
- IDENTIFIED TWITTER EMPLOYEES
- TARGETED EMPLOYEES WITH INTERNAL ACCESS

- CALLED EMPLOYEES PRETENDING TO BE IT SUPPORT
- SAID THERE WAS A VPN PROBLEM
- TRICKED EMPLOYEES INTO ENTERING CREDENTIALS

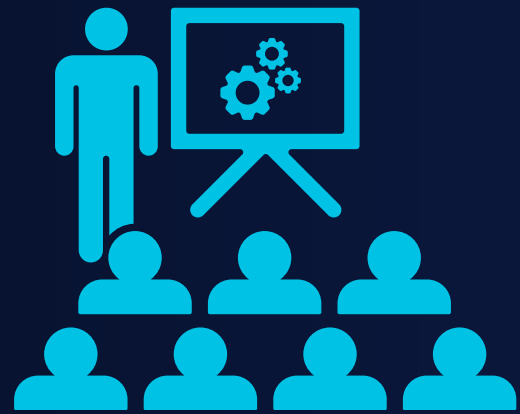
- ATTACKERS LOGGED INTO INTERNAL NETWORK
- ACCESSED ADMIN TOOLS
- CHANGED ACCOUNT SETTINGS

- LEARNED INTERNAL PROCESSES
- TARGETED EMPLOYEES WITH HIGHER PRIVILEGES
- EXPAND MORE CONTROL

- TOOK OVER FAMOUS ACCOUNTS
- POSTED BITCOIN SCAM MESSAGES
- DOUBLE RETURNS.

- LOCKED AFFECTED ACCOUNTS
- REMOVED ATTACKER ACCESS
- RESTRICTED INTERNAL TOOLS
- DISABLED TWEETING TEMPORARILY

# PREVENTION



**Employee Security  
Awareness Training**



**Strong  
Authentication**

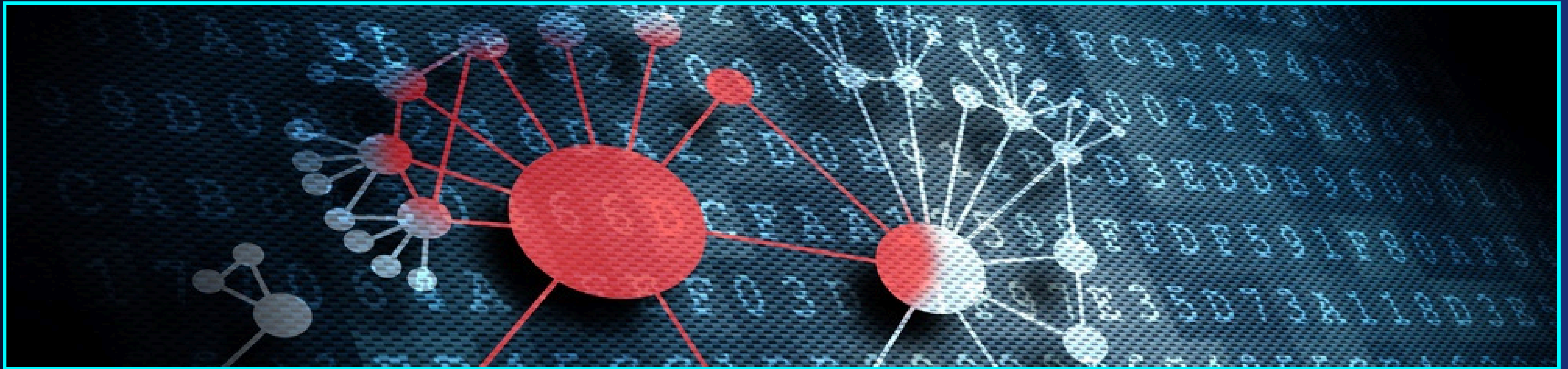


**Least Privilege  
Access**



**Monitoring and  
Detection**





# COMMON PATTERNS

- HUMAN MISTAKES
- UNPATCHED SYSTEMS
- POOR SECURITY MANAGEMENT
- WEAK GOVERNANCE
- PREDICTABLE ATTACKER STEPS

# REFERENCES

- Cloudflare, 2026 , WannaCry ransomware attack, URL: <https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/>, Accessed: 21 February 2026.
- Tero karvinen, 2026, URL: <https://terokarvinen.com/information-security/#homework>, Accessed: 21 February 2026.
- Suraj Srinivasan and Mark Rennella, Harvard.edu, 2019, Cybersecurity: Why All Business Disciplines Need to Teach It—and How, URL: <https://hbsp.harvard.edu/inspiring-minds/cybersecurity-why-all-business-disciplines-need-to-teach-it-and-how>, Accessed: 21 February 2026.
- kaspersky, What is WannaCry ransomware? URL: <https://www.kaspersky.com/resource-center/threats/ransomware-wannacry>, Accessed: 22 February 2026.
- X blog, 2020, An update on our security incident, URL: [https://blog.x.com/en\\_us/topics/company/2020/an-update-on-our-security-incident](https://blog.x.com/en_us/topics/company/2020/an-update-on-our-security-incident), Accessed: 23 February 2026.
- Mitnicksecurity blog, 2020, The 2020 Twitter Bitcoin Scam, URL: <https://www.mitnicksecurity.com/blog/2020-twitter-bitcoin-scam>, Accessed: 23 February 2026.
- Fortinet blog, Does WannaCry Still Exist?, URL: <https://www.fortinet.com/resources/cyberglossary/wannacry-ransomware-attack>, Accessed: 21 February 2026.





**THANK  
YOU**