Task:5 - Research 3 malware incidents

-Maheshwar Anup

The **AIIMS ransomware attack** was a direct assault on critical healthcare infrastructure using encryption, the **Target data breach** was a sophisticated point-of-sale intrusion originating from a third-party vendor, and the **SolarWinds attack** was a widespread supply-chain compromise that affected thousands of organizations.

Malware Incident Reports

This report details three significant malware incidents: the AIIMS ransomware attack, the Target Corporation data breach, and the SolarWinds supply chain attack. Each section outlines the attack methodology and the subsequent mitigation and resolution efforts.

1. AIIMS, New Delhi Ransomware Attack (2022)

The cyberattack on the All India Institute of Medical Sciences (AIIMS) was a major incident that crippled the hospital's digital infrastructure, forcing it to operate manually for weeks.

Attack Method

The attackers deployed a ransomware variant, likely through a **phishing email** or by exploiting an **unpatched vulnerability** in the hospital's network. Once inside, the malware encrypted files on multiple servers, including the electronic health record (EHR) system, patient registration, and billing. This effectively locked staff out of critical patient data and administrative systems. The attackers demanded a ransom, reportedly in cryptocurrency, to provide the decryption keys.

Mitigation and Resolution

AIIMS and Indian government agencies, including the National Informatics Centre (NIC) and CERT-In, chose **not to pay the ransom**. Instead, they focused on recovery and strengthening their defenses.

- **System Restoration**: The primary effort involved restoring data from backups. The IT team worked to clean infected systems and rebuild the server infrastructure from scratch. This was a slow, painstaking process.
- **Manual Operation**: For nearly two weeks, the hospital reverted to manual mode for all operations, from patient registration to report generation, which caused significant delays.
- **Security Overhaul**: Following the incident, AIIMS implemented a comprehensive security upgrade. This included strengthening its firewall, deploying a new antivirus solution, segmenting the network to isolate critical systems, and mandating stronger password policies and multi-factor authentication (MFA).

2. Target Corporation Data Breach (2013)

One of the most infamous retail data breaches, the Target incident exposed the payment card and personal information of millions of customers during the holiday shopping season.

Attack Method

The attack was a multi-stage intrusion that began with a third-party vendor.

1. **Initial Compromise**: The hackers first stole network credentials from a third-party HVAC and refrigeration company that worked with Target. They gained this access through a phishing email sent to an employee of the vendor.
2. **Network Intrusion**: Using the stolen credentials, the attackers gained a foothold in Target's corporate network. They then moved laterally through the network, escalating their privileges until they reached the point-of-sale (POS) systems.
3. **Malware Deployment**: The attackers installed a custom piece of memory-scraping malware, later nicknamed "BlackPOS," on Target's checkout terminals. This malware was designed to capture unencrypted credit and debit card data (track data) from the POS system's RAM at the moment a card was swiped.
4. **Data Exfiltration**: The stolen data was periodically moved from the POS systems to a central staging server within Target's network and then exfiltrated to the attackers' external servers.

Mitigation and Resolution

The response involved immediate containment, public notification, and long-term security enhancements.

- **Containment**: Once the breach was identified, Target's security team worked with law enforcement and forensic experts to remove the malware from all POS devices and servers and close the network backdoors used by the attackers.
- **Customer Support**: Target publicly disclosed the breach, offered free credit monitoring and identity theft protection to affected customers, and faced numerous lawsuits and federal investigations.
- **Security Upgrades**: The breach was a massive catalyst for change. Target invested heavily in overhauling its security, including hiring a new CISO, implementing chip-and-PIN card technology (EMV) across its stores, enhancing network monitoring and segmentation, and tightening controls over third-party vendor access.

---

3. SolarWinds "SUNBURST" Supply Chain Attack (2020)

The SolarWinds attack was a highly sophisticated and widespread cyberespionage campaign that compromised thousands of organizations worldwide, including parts of the U.S. government.

Attack Method

This was a classic **supply chain attack**, where the attackers targeted a software provider to distribute malware to its customers.

1. **Initial Intrusion**: Nation-state actors breached SolarWinds' internal network.

2. **Code Tampering**: The attackers accessed the software development pipeline for SolarWinds' Orion Platform, a popular IT management software. They carefully inserted a malicious backdoor, dubbed "SUNBURST," into a legitimate Orion software update.
3. **Trojanized Distribution**: SolarWinds digitally signed and distributed this compromised update to its customers. Since the update came from a trusted source, it was installed by approximately 18,000 organizations, unknowingly creating a backdoor into their networks.
4. **Secondary Payload**: The SUNBURST backdoor would lay dormant for a couple of weeks before contacting a command-and-control (C2) server. For high-value targets, the attackers would then deploy a second, more potent malware (like "TEARDROP") to escalate privileges, move laterally, and exfiltrate data.

Mitigation and Resolution

The resolution was a complex, collaborative effort across the cybersecurity industry and government agencies.

- **Discovery and Disclosure**: The breach was discovered by the cybersecurity firm FireEye when they detected a suspicious login on their own network and traced it back to the compromised Orion update. They promptly notified SolarWinds and the public.
- **Sinkholing**: A "killswitch" was collaboratively developed by security researchers. They discovered that if the SUNBURST malware tried to contact a C2 domain that didn't exist but was under the control of security teams (a process called sinkholing), it would terminate itself. This helped neutralize the backdoor on many infected systems.
- **Remediation Guidance**: SolarWinds and government agencies like CISA issued detailed guidance for affected organizations, which included isolating compromised servers, patching the Orion platform, and hunting for any secondary malware or attacker persistence within their networks. This led to a massive, industry-wide incident response effort.
- **Improved Supply Chain Security**: The attack highlighted the critical vulnerabilities in software supply chains, leading to a global push for more rigorous software development security, code verification, and the adoption of "zero trust" security architectures.