جامعة الملك سعود
King Saud University

كلية علوم الحاسب والمعلومات

CSC 429: Computer Security

Course Project: Comprehensive Analysis of a Major Cybersecurity Incident

Group Member:

Abdulrahman Alateeq [redacted]

Mohammed Aljalajil

Abdulrahman Almayman

Introduction: Overview of the Incident and the Entities Affected

In May 2017, the WannaCry ransomware attack became one of the biggest cyber threats the world had ever seen. It targeted computers running Microsoft Windows, locking users out of their files and demanding a ransom in Bitcoin to get them back. The attack spread quickly by exploiting a weakness in the Windows operating system, especially on computers that hadn't installed a security update that could have stopped it. This allowed the malware to affect organizations all over the world, causing serious problems.

One of the worst-hit organizations was the National Health Service (NHS) in England. The attack infected many of its computers, encrypting important data and shutting down key systems. Hospitals had to turn away ambulances, cancel appointments, and delay surgeries. This directly affected patient care and showed how dangerous these types of attacks can be, especially in sectors like healthcare that people rely on every day.

The WannaCry attack taught an important lesson about the risks of using old, unprotected systems. It showed how failing to update software on time can lead to major problems. The attack was a wake-up call for everyone to take cybersecurity more seriously and to make sure critical systems are better protected against future threats.

Timeline of Events:

• **In March 2017**, Microsoft found a serious weakness in the SMB protocol, which is part of the Windows operating system. They released an important update (MS17-010) to fix the problem and prevent hackers from taking control of computers. Unfortunately, many systems didn't get this update on time.

• **On the 14th of April 2017**, a group of hackers called The Shadow Brokers leaked several hacking tools on the internet. One of these tools, called EternalBlue, was reportedly created by the U.S. National Security Agency (NSA). It was designed to take advantage of the SMB flaw in Windows, which made it easy for WannaCry to spread later on

• I**n the morning of the 12th of May 2017**, WannaCry ransomware started spreading across the world. It locked files on computers and demanded payment in Bitcoin to unlock them. It used the EternalBlue tool to jump quickly from one unprotected system to another, causing massive infections.

• **In the afternoon of the 12th of May 2017**, the attack caused significant disruption, most notably in the UK's National Health Service (NHS). Hospitals were forced to cancel appointments, delay surgeries, and divert ambulances due to compromised systems.

• **On the 13th of May 2017**, Microsoft released emergency patches for unsupported systems like Windows XP, Windows 8, and Windows Server 2003. This unusual step was taken to help mitigate the impact on older systems that were still in use.

• **On the 14th of May 2017**, The Cybersecurity and Infrastructure Security Agency (CISA) issued a public alert advising organizations to update their systems immediately, disable SMBv1 if unnecessary, and maintain proper backups to prevent similar attacks in the future.

• **In the weeks following the attack**, CISA's ICS-CERT released a detailed fact sheet summarizing the WannaCry incident. The document provided insights into the malware's propagation via EternalBlue and highlighted best practices for preventing similar attacks in the future.

Attack Methodology:

The WannaCry ransomware attack used several clever tactics to spread quickly and cause chaos. First, the attackers took advantage of a security flaw in the Windows operating system called MS17-010. This flaw, found in a part of Windows called the SMB protocol, allowed the attackers to take control of computers that hadn't been updated with a security fix.

To exploit this flaw, the attackers used a hacking tool called EternalBlue, which was originally created by the U.S. National Security Agency (NSA). However, this tool was leaked online by a group called the Shadow Brokers. EternalBlue made it possible for WannaCry to move from one

unprotected computer to another, spreading through networks without the need for anyone to click on anything.

The attackers also used another tool called DoublePulsar, which acted like a secret backdoor into the system. This backdoor allowed the ransomware to install itself without being stopped by security software or detected by users.

Once WannaCry infected a computer, it worked like a worm. It automatically looked for other computers on the same network or even across the internet that had the same flaw. This allowed it to spread rapidly and infect thousands of systems in a very short time.

Finally, after gaining access to a system, WannaCry locked important files by encrypting them. It then displayed a ransom note, demanding payment in Bitcoin to unlock the files. If the ransom wasn't paid within a certain time, the attackers threatened to delete the files forever.

Root Causes and Vulnerabilities:

The WannaCry ransomware attack was successful because it took advantage of several security weaknesses in computer systems. The main problem was a flaw in the Windows operating system, known as MS17-010, in a part of the system called the SMB protocol. This flaw made it possible for attackers to take control of computers that hadn't been updated with a security patch.

Microsoft had actually released a fix for this problem two months before the attack, but many organizations didn't apply it. Without this update, their systems were left vulnerable, making it easy for WannaCry to infect them. The problem was worse for organizations using old versions of Windows, like Windows XP and Windows Server 2003, which didn't receive regular security updates anymore. These outdated systems were even more exposed to the attack.

The attackers also used a powerful hacking tool called EternalBlue, which exploited the MS17-010 flaw. EternalBlue allowed WannaCry to spread quickly between unprotected systems, turning a single infection into a network-wide problem in a matter of hours.

Impact Analysis of the WannaCry Ransomware Attack:

Financial Impacts

The WannaCry attack cost organizations a lot of money. Some tried paying the ransom to recover their data, but there was no guarantee they'd get their files back. Others spent huge amounts on fixing their systems, recovering data, and upgrading their cybersecurity. For example, the UK's National Health Service (NHS) had to spend a lot of money repairing the damage and updating its systems. In total, global losses from the attack were estimated at up to $4 billion, including immediate costs and longer-term losses caused by disrupted operations.

Reputational Impacts
Organizations hit by the attack suffered damage to their reputations. People lost trust in them because they felt these companies didn't do enough to protect their data. For example, the NHS faced public criticism for not being better prepared, especially since it provides critical services like healthcare. Rebuilding trust took a lot of time and effort. Companies had to show they were serious about improving their security to win back customers and stakeholders.

Operational Impacts
The attack caused massive disruptions to the daily operations of many organizations. WannaCry encrypted data, making systems unusable. This stopped businesses from functioning normally. The NHS had to cancel thousands of medical appointments and surgeries, affecting patients directly. Car manufacturers like Nissan and Renault had to stop production temporarily to contain the attack. These disruptions not only delayed services but also led to financial losses and operational backlogs.

Legal Impacts
The attack also raised serious legal issues. Organizations that didn't protect sensitive data properly faced fines or legal actions, especially in places with strict data protection laws like Europe's General Data Protection Regulation (GDPR). These legal consequences made it clear that ignoring cybersecurity responsibilities can lead to major problems. Many companies also had to deal with lawsuits from customers or partners who were affected by the attack

Lessons Learned

1. **Keep Software Updated**
   The ransomware used a vulnerability that Microsoft had already patched months earlier. Organizations that didn't install the update were left exposed. This shows why it's crucial to keep software up to date and have a solid process for applying patches quickly.

2. **Have Reliable Backups**
   Backing up data regularly is one of the best ways to reduce the impact of ransomware. If you have a secure backup, you don't need to pay the ransom, you can just restore your data. These backups should be stored separately from your main systems, so they aren't affected by an attack.

3. **Segment Your Network**
   Dividing your network into smaller sections can stop ransomware from spreading to the entire system. This way, even if one part of the network is hit, the damage is limited. Adding strict access controls between these sections can provide extra protection.

4. **Educate Employees**
   Most attacks start with human error, like someone clicking on a phishing email. Training employees to recognize suspicious emails and follow safe online practices can prevent many attacks. Regular awareness campaigns and testing can help reinforce these habits.

5. **Prepare for Attacks**
   Every organization should have an incident response plan. This is a step-by-step guide on what to do if there's an attack. It should include who does what, how to communicate during the crisis, and how to isolate and remove the threat quickly. Practicing these plans ensures everyone knows what to do when it counts.

6. **Work with Experts**
   Collaborating with cybersecurity organizations like the Cybersecurity and Infrastructure Security Agency (CISA) can give you access to the latest threat intelligence. Sharing information with others in your industry can also help everyone stay ahead of emerging threats.

References:

1. **Secureworks:** WCry (WannaCry) Ransomware Analysis
2. **CISA:** Indicators Associated with WannaCry Ransomware
3. **NHS England:** Lessons Learned Review of the WannaCry Ransomware Cyber Attack
4. **Kaspersky:** Ransomware WannaCry: All You Need to Know
5. **Security.com:** WannaCry Ransomware Attack
6. **UpGuard:** WannaCry