Arjun Chauhan

Professor Vroomen

TIM 50

1 June 2023

Case Study 4 - Maersk

1. **What Happened**
    a. A ransomware attack occurs by deploying malicious software onto target machines, generally intending to encrypt the user's files in their entirety to demand a ransom, hence the name ransomware. In most cases, malware is deployed via emails with links or attachments which deploy the malware payload. Once the malware is downloaded and installed in the background, it can either be activated immediately or wait dormant until receiving an activation command. Once activated, the malware proceeds to encrypt as many files as it can reach, often under the guise of a software update or computer "repair". This cover prevents users from disconnecting the power to their system, which is often the only way to stop an attack in progress. Once files are encrypted, the malware will often demand payment in the form of Bitcoin or other cryptocurrency in exchange for a decryption key.
    b. Unlike ransomware, NotPetya's demands for ransom were disingenuous, as "no means for the victims to pay the ransom or receive decryption keys" existed.[1] Rather, NotPetya was purely destructive, hiding behind the facade of ransomware and harnessing existing Windows exploits so that the program could run in the background without user input. In part because of this difference in intent,

NotPetya is also unlike ransomware because it has been attributed to a state-sponsored group aligned with Russia in their conflict against Ukraine.

c. The NotPetya ransomware was initially planted onto "More than 300 Ukranian companies, banks, and hospitals"[1]. However, Maersk utilized tax-filing software from MeDoc, a Ukranian company. An update to the MeDoc software was pushed through MeDoc's automatic update system which contained and ran NotPetya[2], spreading to the many firms which utilized the software, including Maersk.

2. Actions Taken To Recover

a. Domain controllers are a key aspect of Microsoft's Active Directory system, which is used to manage and control resources on a Windows-based network. Domain controllers are particularly important for user authentication[3], which was "The primary and key objective"[1] in Maersk's recovery efforts. The redundancy of domain controllers in a network typically makes them a low-risk component, but NotPetya attempted with almost total efficacy to hit all of these controllers simultaneously. However, Ghana's energy crisis at the time meant that Maersk's domain controller in the country had been offline during the attack, and was, therefore, the only unaffected system on Maersk's network. From this one system, Maersk could recreate the rest of its network. Due to bandwidth limitations, the physical hard drive from this server would have to be transported to the company's London command center, rather than having its contents sent to the command center over the internet.

b. Given that the domain controller in Ghana was the only remaining uncorrupted controller, the hard drive from this server had to be transported to Maersk's

command center in London, both to prevent potential infection and to avoid bandwidth limitations in Ghana. The drive was transported to Nigeria, where an employee with a travel visa for Britain would accompany the drive to London. In London, this drive could be duplicated to recreate all 149 other controllers.

c. Besides devices that were offline at the time of attack, every system connected to Maersk's network was infected and entirely encrypted by NotPetya. If Maersk elected to reimage all its systems, rather than replacing them, the process would take weeks, if not months.

Item	Quantity	Cost Per Unit	Total Cost (dollars)	
Servers	4000	$8,112.49	$32,449,960.00	Price estimated based on Dell PowerEdge R760xs
Routers	40	$3,157.00	$126,280.00	Price estimated based on Cisco ISR4331-SEC/K9
Switches	1800	$1,299.00	$2,338,200.00	Price estimated based on Ubiquiti Enterprise XG 24
PCs	45000	$2,369.00	$106,605,000.00	Price estimated based on Dell Precision 3460 Workstation
Applications	2500	$684.00	$1,710,000.00	Pricing based on Microsoft 365 E5 Annual License, though more specialized applications could certainly cost more
			$143,229,440.00	

3. Recommendations to Prevent such Attacks in Future

   a. IT Policy Changes:

      i. Frequent Software Upgrades - At the time of the attack in 2016, Maersk was still running Windows 2000, which was phased out by Microsoft on July 12, 2010[4]. In order to maintain protection against recently discovered vulnerabilities, Maersk must keep its systems up to date. This would also involve a restructuring of Maersk IT bonus structures, which discouraged the downtime required for these updates.

ii. Regular Systemwide Backups - Maersk was lucky that power was cut to its domain controller in Ghana, as this was the only system to survive the attack and could be used to rebuild the rest of the network. To prevent this situation in the future, Maersk should maintain regular offline backups of domain controllers, which were a key blindspot in Maersk backup practices, as well as individual systems in its numerous locations worldwide, whose local files were lost in the attack.

iii. Software validation prior to deployment - Maersk was collateral damage in an attack on a third-party target whose software Maersk utilized. Had this software been validated by Maersk staff before being deployed by an auto-update system, the attack could have been prevented.

b. Machine-learning-based intrusion detection can be harnessed to actively defend Maersk's network against attacks such as NotPetya by detecting anomalies and recognizing irregular network behavior, while simultaneously making centralized network monitoring far easier. XDR systems collect data from various network endpoints, consolidating and analyzing this data to detect and prioritize threats.[5] Such systems can pull data both from past attacks and internal patterns, providing greater insight than traditional malware detection systems. SEIM systems also analyze data from network activity, using "predetermined rules"[6] to fight threats. SEIM systems are particularly effective in pattern detection, providing similar centralization benefits to XDR systems. In tandem, these tools could help prevent attacks like NotPetya from ever taking root in Maersk's network.

References

1. Wesley, D., Dua, L., Roth, A. (2019). *Cyberattack: The Maersk Global Supply Chain Meltdown* W19132. Ivey Publishing.
2. Wakefield, J. (2017, June 28). *Tax software blamed for cyber-attack spread*. BBC News. https://www.bbc.com/news/technology-40428967
3. Worthington, D. (2023, May 11). *What is a domain controller?* JumpCloud. https://jumpcloud.com/blog/what-is-a-domain-controller
4. Emil Protalinski - Dec 8, 2009 4:41 pm UTC. (2009, December 8). *Support for windows 2000, windows XP SP2 ends Next July*. Ars Technica. https://arstechnica.com/information-technology/2009/12/support-for-windows-xp-sp2-windows-2000-ends-july-13-2010/
5. *What is XDR? Extended Detection & Response - Crowdstrike*. crowdstrike.com. (2023, May 15). https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/
6. *What is Siem?*. Microsoft Security. (n.d.). https://www.microsoft.com/en-us/security/business/security-101/what-is-siem