CLEARNETWORK
YOUR CYBERSECURITY EXPERTS

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Manufacturing Industry

For matters of confidentiality, the identities in this case study have been obfuscated.

Employees
400

Annual Revenue
200 million dollars

Locations
United States & England

Company Background:

A radio manufacturing company in the United States has been in business for over 60 years. Starting from the company's mission is to manufacture and provide radio components to the commercial consumers and military/defense markets. The company prides itself on their intellectual property in consistently keeping a competitive edge, year over year. While the company itself is small to mid-market with approximately 400 employees, the annual revenue far surpasses this size at a healthy 200 million dollars per annum. Most of this revenue is due to the large government contracts that the company holds. The company supports 2 main locations, within the continental United States and one overseas location in England.

Technology Background:

The company's digital infrastructure is on-par with the standards for most manufacturing companies within the United States.

- **Domain:** Microsoft Active Directory
- **Email:** Microsoft Exchange
- **Remote:** VPN, Remote Desktop Server, FTP, Customer Portal
- **Firewall:** Cisco ASA
- **Virtualization:** VMware
- **Servers:** Microsoft Windows Server 2012R2, 2008R2, 2003
- **Workstations:** Microsoft Windows 7 & 10.
- **Manufacturing:** Linux-based, Windows XP, & Vista
- **Security:** Kaspersky Antivirus
- **SIEM:** None

The technological environment of the organization supported all locations through a federated system and enables sites to share work across the networks with ease through pre-configured site-to-site VPN's. Workers could collaborate through network file shares that had been mapped to each workstation and user to facilitate the business processes. The engineering departments could design new specifications for products, share with the appropriate personnel, and deliver to the manufacturing lines with no delays. Such streamlined processes ensured expedited workflows and swift product manufacturing.

The Breach:

One morning, in August of 2018 at approximately 8:45 a.m., the IT department received a complaint from a user. The employee was experiencing some odd symptoms of frequent account lockouts and strange icons appearing on her desktop. An IT technician unlocked her account and removed the unwanted desktop icons and resumed working on a larger infrastructure project to implement a new storage server to support the increase in data from a complete redesign on the radio specifications. The ticket was logged, and the user resumed working on her daily tasks.

- **9:05 a.m.:** 2nd call to IT department. Another user complaint of account lockout.
- **9:09 a.m.:** 3rd call to IT department. Another user complaint of account lockout.
- **9:20 a.m.:** 4th call to IT department. A senior business development manager is claiming that he can no longer gain access to the VPN and is receiving 'invalid credentials' messages when attempting to log in.
- **9:50 a.m.:** The company CFO entered the IT department's office and is visibly distraught. He is claiming that unauthorized funds have been transferred from the corporate bank accounts to a company that has no affiliation with the organization.
- **10:00 a.m.:** A meeting is called with the CFO, IT Director, and IT Department Staff Members. The morning calls are analyzed for common themes and trends. Frequent account lockouts are still being reported by multiple users. In the course of 15 minutes, over 30 calls have been received by the IT Department of account lockouts, strange desktop behavior, and Antivirus warnings. Additionally, a customer has contacted a sales agent and stated that the company's website appears to be 'different' and they cannot log into the customer portal. The CFO has contacted the CEO and has decided to contact law enforcement due to the unauthorized financial transactions that have occurred. The IT department has decided to not unlock any accounts that have been locked out until the root cause has been determined. Any systems that have Antivirus warnings are being quarantined and investigated.
- **10:35 a.m.:** During the staff meeting, the lead systems administrator noticed that the servers hosting the network shares have reached peak computing levels. The CPU graphs are at maximum levels and network shares are extremely latent. Upon further investigation, it is noticed that files within the shares are appended with a '.lock' at the end of each filename. The situation has turned critical, as this is a telltale symptom of a ransomware infection.

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Manufacturing Industry

› **11:00 a.m.:** The IT Director, CFO, and CEO have decided to call an incident response company for help. Multiple issues have arisen and appear to be related.
› **11:15 a.m.:** The manufacturing floor manager entered the IT Department and stated that almost every manufacturing system has a message on the screen stating "Your files have all been locked by military-grade encryption. To recover your files, you must pay 50 Bitcoin. At the time of this incident, the price per Bitcoin was approximately $4,000 USD. This equated to approximately $200,000 USD.

Breach Anatomy:

Following the triage, containment, eradication, and recovery of the organization, the root causes and cyber kill chain of this attack were quite complex. The first attack had originated over 6 months prior to this fateful day when the IP-Camera system was hacked. An attacker had compromised the IP-Camera system from a remote location by leveraging a set of default credentials that had not been changed by the systems administrator that had implemented them.
Following the successful compromise of the IP-based security cameras, the network now had a mark and curious cyber-actors could peer into the live feeds of the company. Following this, the attention of other attackers grew exponentially. Live video feeds of manufacturing lines created a more attractive and lucrative endeavor; attacking the company where it hurt. Within the first 30 days of the IP-based camera system compromise, more attackers honed into the network and began a campaign to compromise the other systems from the outside. A lone Remote Desktop Protocol Server was externally-facing and was attacked several times. The domain password policy only supported 8 characters and a successful brute force password attack gave the criminals remote access as a legitimate user. Once inside, the attackers moved laterally to discover more assets on the network, since no network segmentation had been implemented. The reconnaissance took place for another 4-5 months in which attackers would come and go. They would map out the network, sniff passwords, and collect information on the manufacturing operations. The databases for the engineering specifications was accessed multiple times by the attackers during this phase.

Endgame:

› **Phase I:** On that fateful morning in August, the attackers had kicked off their ultimate campaign; the grand finale. They had already siphoned the intellectual property from the network and used the environment as a staging point for many other outward-facing attacks. Now it was time to collect and move on. The first calls to the IT Department between 9:05 a.m. and 9:20 a.m. were distractions. The attackers had purposefully locked accounts out to draw attention away from anyone that may be watching. At the same time of this attack, multiple other attackers were underway.
› **Phase II:** While the sleight of hand performance was in full-motion, the attackers had already sniffed the CFO's passwords, to everything. Banking credentials were leveraged to manually initiate a wire transfer of $99,000 USD. Since the organization had a different process for transferring anything over $100,000 USD, the attackers did not want to raise suspicion. However, they performed 2 wire transfers before the bank had contacted the manufacturing company, equating to $198,000.
› **Phase III:** The calls to the sales agents, regarding the customer portal were a direct result of a spoofed webpage. Since the attackers had access to modify anything on the network, they had decided to redirect customers from the company's customer portal to a spoofed version of the site. They had collected customer credentials and logged in as legitimate users. The information within the customer portal was lifted in this phase. Social security numbers, Taxpayer ID's, ACH numbers, routing numbers, birthday's, and other intellectual property were all stolen.
› **Phase IV:** The calls regarding suspicious changes to desktops, server resources, and manufacturing floor workstations were due to the last phase of the attack; Ransomware. A particularly nasty variant of ransomware was executed on servers, workstations, manufacturing systems, and anything else that hosted this vulnerability. File shares were also affected in this attack. Unlike many ransomware attacks, a large amount of bitcoin was requested due to the homework that the attackers had performed prior to execution. They understood that the value of this company resided in its ability to maintain manufacturing operations. When the manufacturing lines came to a screeching halt, the wire transfers and customer portal were the least of the company's worries. $200,000 USD was being requested or the company operations would not proceed. No decryption key was available unless the ransom was paid.

The Aftermath:

A company that had been in business for over 60 years was brought to its knees in a matter of hours. Operations were halted, reputations were at-stake, and the company was bleeding money. The company had no formal incident response plan, nor disaster recovery capability and was simply unprepared for this type of attack. The total monetary cost of the breach was over **2.5 million USD**. Aside from the $400,000 between the wire transfers and the ransomware payments, for every hour that the company could not continue manufacturing operations, the cost was over $10,000. The company had no Bitcoin account and hesitated to pay the ransom while the incident response team attempted to decrypt the files. This set the company back 10 days until operations were fully restored.

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Manufacturing Industry

No SIEM:

6 months prior to this massive and disruptive attack, the company was hit with a menial attack by internet pranksters. A hack into the IP-based camera system was likely performed by a curious individual or group that had no intent of pulling off this Oceans Eleven-type attack. However, once inside the attackers opened pandora's box. This invited more serious and experienced threats into the game. If the organization had been proactively monitoring the network's security with a Security Information and Event Management platform (SIEM), the initial suspicious activities would have likely been discovered and halted expeditiously. In fact, the entire breach could have been stopped with the following capabilities of Clearnetwork:

- **Account Monitoring:** The suspicious activities from the reconnaissance would have been alerted on. Accounts were being leveraged at all hours of the day and night to move laterally. Suspicious account activity alerts would have sent alerts to security administrators and analysts and Clearnetwork would have quickly alerted their IT staff.
- **Anti-Exploitation Alerts:** When a network is under attack and the adversaries are launching exploitation code against workstations, laptops, and servers, alerts would have been generated and sent to the appropriate parties.
- **Vulnerabilities:** The ransomware was able to spread through SMB vulnerabilities over port 445. The Clearnetwork's vulnerability scanning integrations would have discovered such vulnerabilities prior and given the IT Department the intelligence to act swiftly to patch systems and shutdown ports, protocols, and services that were not required.
- **Suspicious System Activities:** The CFO's workstation had been compromised for over 45 days before the wire transfers took place. The attackers had been logging into this system with dummy accounts that they had created in the company's Microsoft Active Directory database. They had created multiple Domain and Local Administrator accounts that were used to log into the CFO's system and steal credentials.
- **Malware:** Multiple systems were found to be infected with various pieces of malware. Trojans, Spyware, Adware, File-less malware, and others could have been detected by the SIEM. No central console existed for the organization's antivirus software so therefore, no centralized alerting was enabled. Clearnetwork would have collected the antivirus information from each system and sent it to the SIEM so that the 'big-picture' could be analyzed proactively.
- **Malicious Redirects:** Customers were directed to a spoofed site that mimicked that of the customer portal. A SIEM could have detected this malicious redirect, based on a series of pre-defined criteria for ensuring legitimate site integrity through trusted certificates.

Time & Intelligence

The manufacturing company was breached for over 6 months in this attack. Post-attack and recovery, the company incurred massive financial losses. However, the intangible losses were far greater. The reputation of the company was tarnished. Clients, customers, and business affiliates all learned of the attack and the information compromised. The intellectual property of the company had been stolen as well. Technical information, product drawings and specifications, contracts, and internal communications were compromised. The attack could have likely been detected and prevented if a SIEM solution were implemented. The lack of monitoring capabilities ultimately led to an extremely complex breach of a company that had previously thought little of cyber-attacks. Large companies are not the only targets for attackers. Attackers understand that small and mid-market companies, such as this victim, are not likely equipped with the tools and capabilities to detect and thwart cyber-attacks. Investing in a SIEM has become one of the best and most proactive methods to effectively combat cyber-threats today.

Looking to protect yourself from this type of attack?

Clearnetwork USM would have caught this attack during its early stages. Our service utilizes SIEM and Log Management, Monthly or Bi-weekly Vulnerability Assessments, Intrusion Detection, Behavioral Analysis, Asset Discovery, Endpoint Detection and Response, File Integrity Monitoring and more. Everything is managed and watched by our expert security analysts each with years of experience in locating evasive threats. We also fully utilize your existing security investments like anti-virus and firewalls and over 200 other devices/services by constantly watching the logs for any sign of a threat and using that data with all our other collected data to paint a full picture of what's happening on the network. All of this offered by us in one solution, with no long term contract, and we offer a free 14 day proof of concept (POC) so we can demonstrate our value.

Please reach out to schedule a demo or talk in more detail.

sales@clearnetwork.com

800-463-7920 x3