CLEARNETWORK
YOUR CYBERSECURITY EXPERTS

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Law Firm

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

Company Background:

A law firm, based in the Western United States, consisting of over 25 full-time attorneys and in business for over 50 years. The firm specializes in corporate litigation for white-collar crimes. For over 50 years, the law firm has served clients throughout North and Central America and has been the leading firm for many cases in the public limelight. The organization also employs over 40 people throughout other departments, such as information technology, paralegal, and administrative positions. The firm has a main location in the Western United States with attorneys throughout North and Central America (Canada, U.S., and Mexico)

Technology Background:

The firm has a data center at the main location. The data center consists of 10-15 servers in a traditional environment, boasting a document management system for case files, corporate file servers, patch management and orchestration server, domain controller, and DHCP server. Approximately 15 attorneys and 30 other employees reside at the corporate offices. 10 other (remote) attorneys are spread across the U.S., Canada, and Mexico and 10 support professionals and paralegals are geographically dispersed as well. The company leverages an onsite email server, VPN gateway, and cloud-based file sharing system via Dropbox.

- **Domain:** Microsoft Active Directory (on-premise)
- **Cloud Storage/Sharing:** Dropbox
- **Email:** Microsoft Exchange 2013
- **Remote:** Corporate VPN
- **Firewall:** Cisco ASA
- **Virtualization:** None (All Physical)
- **Servers:** Microsoft Windows Server 2016
- **Workstations:** Microsoft Windows 10 & Apple Mac OS
- **Security:** Kaspersky Antivirus
- **SIEM:** None

The law firm was recently engaged in a high-profile case, involving corporate executives in the oil and gas industry throughout the Middle East. The ongoing case was predicated on charges of white-collar crimes allegedly conducted by several executives in this industry. The defense team included 2 of the partner attorneys, 3 junior counselors, and several paralegals and assistants. The case was a multi-million-dollar deal that had placed the organization in a 24/7 state of operations to get ready for the defense. Attention was drawn to the organization from the press and other parties.

While the organization boasted a relatively mature cybersecurity posture, a SIEM platform was not purchased the prior year. Several SIEM proposals were presented to the firm but the information technology budget was spent on a recent upgrade of all corporate workstations and servers. Additionally, the company had recently purchased a new VoIP system that was an added expense on the information technology card for the year.

Attackers on the Edge

After a year of litigation, the case was finally coming to an end and an attorney on the case team received an email from an unknown source. The sender had stated that “we have full access to your company. Your cases, files, and secrets belong to us. We recommend that you drop your current client in the petroleum industry. They deserve to defend themselves. If you do not, we will expose the case to the public, including all confidential files on this case and every other case for the past 10 years.” This email was directly followed by emails from legitimate internal employees. The emails from over 15 internal employees stated “This is proof that we have access to everything. We have already downloaded all of the artifacts that we need so please feel free to lock us out now…”

Needless to say, the law firm was now in the middle of an unexpected situation in which client data had likely been stolen. Additionally, during the course of this case, several attorneys reported that files had “gone missing” and were not able to be recovered for court appearances and judgement summons. It was suspected that the attackers had motives to skew the results of this case and in the favor of the prosecution. Several other emails persisted after the originals had been sent. Proof of case information was presented by the attackers in the form of the missing documents and information lost during the case.

The attackers were apparently part of a self-righteous hacktivist group and had learned of the charges brought against the executives in the petroleum industry. The group had been targeting the executives for over 3 years throughout several accusations of corporate fraud, bid-rigging, theft, and corruption involving foreign politicians.

CLEARNETWORK
YOUR CYBERSECURITY EXPERTS

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Law Firm

Breach Anatomy

› The Exchange Server has been sitting on the edge of the network, exposed to the internet. This common practice is generally required for email servers and are usually exposed in some manner. However, the lack of vulnerability scanning had left the email server open to several gaps. The attackers had scanned performed scans on the system and found an exploitable vulnerability that granted a remote access shell on the system.

› From this gap, the attackers now had control over a system on the local environment. Lateral exploitation was performed on several internal servers. Once the attackers had compromised the internal active directory server, the attackers performed a password database dump. Once this password database had been dumped, the attackers cracked many of the internal employee passwords and began to login to internal workstations. They had collected files, removed sensitive documentation, and whitelisted malware on the internal Kaspersky Antivirus. The malware was dropped to gain remote access at a later time, if the initial routes were closed.

› Once the attackers had gained the Active Directory credentials, they moved outwards to email web access. The threat-actors logged into email accounts of several attorneys, partners, and administrative employees. Mass downloads of emails and auto-forwarding rules were set on all email accounts that were compromised.

› The firm had also leveraged Dropbox and DocuSign for file sharing with clients and signature processes. The attackers had simply requested new passwords on Dropbox and DocuSign after setting rules in the employee's inboxes to hide the responses from Dropbox and DocuSign. Once the attackers had quickly stolen all files within Dropbox and DocuSign, the email rules were removed, and the employees reset their passwords. Several trouble tickets were submitted on this issue, but no incident response investigation was opened at that time.

The Aftermath:

The law firm brought the situation to the attention of the district attorney. The case team was inclined to eventually forfeit the case, due to mishandling of confidential case information. The law firm had devoted nearly a year of work and thousands of hours to this case. The payout for the case would only come with a favorable decision or win. However, the case was dropped by the team and sent to another firm. An adversarial group had infiltrated the corporate structure of the law firm and had disrupted and destroyed a high profile and potentially profitable case. Furthermore, the law firm was compromised on several other fronts. Unrelated case information was also exposed that placed the firm in a state of emergency beyond the immediate case. All past clients were informed of the data breach, spanning several areas within the U.S., Mexico, and Canada. The following year of the firm's work consisted of reparations to reputation damage and bolstering of their cybersecurity defenses.

A Preventable Breach:

The law firm was vulnerable, surveilled, and exploited. While the final results of the breach did not reveal how much data was actually stolen, it was estimated that approximately 1,500 cases were potentially compromised. All parties were informed, and stringent controls were put against the law firm, in regard to cybersecurity due diligence. During the course of the attack and data theft, opportunities for responses were not relayed by any form of technology. The attackers had circumvented multiple controls, gained access, manipulated antivirus software, and breached cloud and internal systems. If the organization had been proactively monitoring the network's security with a managed Security Information and Event Management platform (SIEM) and other services offered by ClearNetwork, the devious activities would have likely been discovered and halted. In fact, the entire breach could have been prevented and halted with the following ClearNetwork solutions and SIEM capabilities:

› **Vulnerabilities:** The included vulnerability scanning capabilities of ClearNetwork's SIEM could have rapidly identified the external vulnerabilities on the exposed Exchange Server. If such vulnerabilities were identified quickly, pertinent patches and fixes could have been applied and prevented the exploitation of the email server.

› **Credential Database Theft:** When the attackers had compromised the internal Active Directory Server, they swiftly downloaded the SAM Database (credentials file). This suspicious behavior was not detected by any SIEM solution. Therefore, attackers were able to download that SAM database and perform password cracking, eventually compromising numerous accounts. This suspicious activity could have been detected and alerted on by the SIEM tool.

› **Password Cracking:** Once inside of the network, the attackers began to discover weak passwords via a set of hacking tools. The password hashes matched that of the less secure Lan Manager (LM) protocol. Such LM passwords could have been discovered on the network via a SIEM platform and reported on. However, even though the organization was leveraging NT Lan Manager (NTLM), some older hashed passwords still existed, leading to compromise of the credentials.

› **Antivirus Circumvention:** Software control is a critical aspect of any security posture. However, in the case of the law firm, the attackers were able to circumvent the built-in controls of the antivirus software. Once root access had been gained on the machines, the attackers merely whitelisted the malware signature and explicitly allow this program to run without intervention from the

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Law Firm

antivirus software. The SIEM tool could have been ingesting the logs from the antivirus clients and alerted the staff when modifications were being made.

› **Business Email Compromise:** Once the attackers had the credentials of the internal users from Active Directory, they moved to the outside and logged into the Microsoft Outlook Web Application (OWA). A SIEM tools could have been ingesting Microsoft Exchange logs and alerted staff members that nefarious logins were occurring from other countries. Several logins from Russia, China, Romania, and Nigeria were discovered during the investigation.

› **Data Exfiltration:** The attackers used several channels to exfiltrate data. The attackers had infiltrated Dropbox and DocuSign accounts several times to download data. If the organization had been leveraging Azure Active Directory single sign-on for Dropbox and DocuSign and sending logs to the SIEM, these activities could have generated critical alerts and warned staff members of abnormal activities. Additionally, the attackers used common channels such as Pastebin to upload files from the internal network to locations for later use. The attackers were also found to be leveraging encrypted communication channels to send files to offsite locations. None of these activities were noted in any alerts. The SIEM platform could have discovered the data exfiltration and brought valuable intelligence to the attention of the staff members.

› **Time to Respond:** During the course of the incident investigation, it was found that the attackers had access to the corporate environment, accounts, and information for several months. No detection had occurred at any point in time and the attackers were able to steal the information that they required without interruptions. When the incident response and forensics team engaged with the law firm, several tools were required to be deployed by the teams. Manual log searching, data indexing, and case management requires an enormous amount of time and slowed down the investigation dramatically. Furthermore, since the organization was not forwarding logs to a central location for storage and alerting, much of the information was simply not obtainable. The lack of information that was able to be collected presented several problems for the law firm when presenting to authorities. If ClearNetwork's SIEM platform had been implemented, logs could have been aggregated and correlated in a single location, dramatically expediting time to response and leaving a clear forensic trail for e-discovery.

Enhancing the Security Posture

From a single vulnerability, on an externally-facing server, a law firm was brought to a grinding halt. The initial attack vector and all subsequent attacker paths could have been easily identified and remediated prior to the attack, with the implementation of ClearNetwork's Managed SIEM solution. If the law firm had implemented the solution prior to the attack, the threats could have been neutralized before and/or during the attack. However, no signals or alerts were generated, and the attackers were able to conduct their nefarious activities without obstruction.

Making the decision to invest in security is one that is not recommended, but necessary. ClearNetwork's Managed SIEM solution is a paramount step for organizations that wish to be well-equipped and informed of their security posture. In this case, ClearNetwork's Managed SIEM solution could have identified the vulnerabilities, alerted on abnormal behavior, and facilitated incident responders before a catastrophic situation.

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