Clearwater

Chasing a Cyber Attacker out of an Organization

A play-by-play recount of threat detection and response and the lessons to learn about improving cyber resiliency

Intro

This paper reveals the various ways a real-life attack played out within the environment of a healthcare business associate. It documents how the attack happened and the moves and countermeasures that took place, including verifying that no access to sensitive data occurred, blocking the attacker's movement, and confirming that the organization was rid of any lingering exposure. The information is based on the work of Clearwater's Managed Security Services providing 24x7x365 threat detection, firewall and vulnerability management, log management, incident response, and other functions needed to achieve cyber resiliency.

Section 1

Industry Target Practice

The attackers were not likely maliciously targeting this organization specifically at first. However, they probably knew that this organization provided services for patient engagement and billing for healthcare, in addition to other industries.

Most attack exploits are opportunistic, looking for common and easy ways to breach organizations. Technology and people are not infallible, and attackers have automation and even databases helping them focus on likely profitable targets.

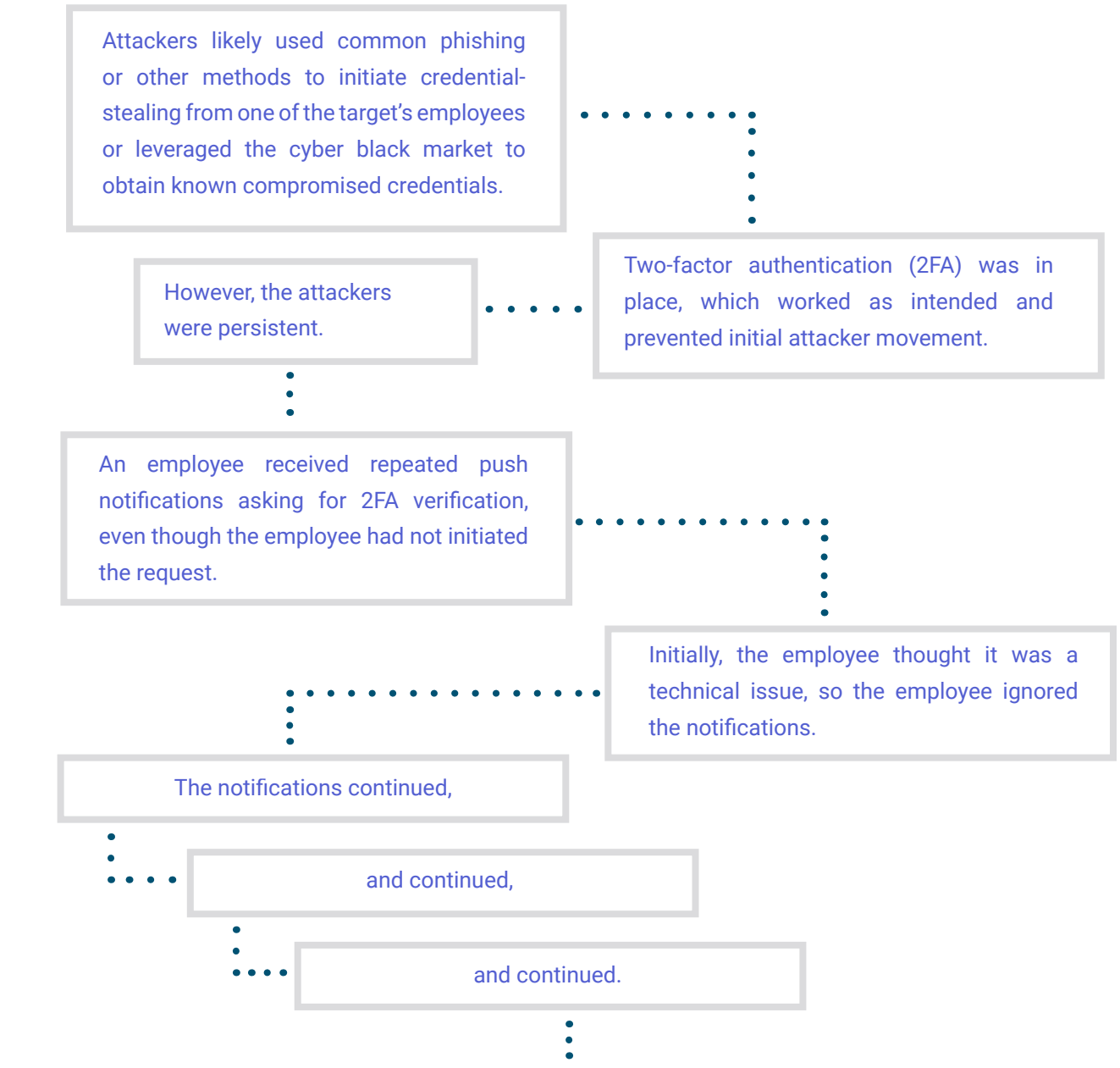
In this case, the attack tactics progressed to focusing on employees within this organization.

According to U.S. government data, the number of healthcare breaches in the first five months of 2022 has nearly doubled from the same period last year.

Section 2

Pushing the People Boundary

Here is how the breach happened.



Annoyed by the repeated requests, the employee ultimately relented and approved the request.

Section 3

Landing Inside

After utilizing the employee credentials, with authorization, the attackers began to conduct internal recon and attempted to gain additional access to other systems.

What worked in the organization's favor?

Clearwater's managed threat detection and response service provided security operations on the systems critical to the company's operations. Immediate detection of anomalous behavior triggered a security event and investigation.

What went wrong?

The company did not have protection on all of its assets or systems and only protected what the company considered "operational" assets. This attack quickly took advantage of Dev. systems outside threat detection and response service management. Initial detection was delayed, and it is unknown what reconnaissance details were obtained.

According to the HIPAA Journal, the top 10 security weaknesses attackers commonly exploit are:

- Slow software updates and patching
- Open ports and misconfigurations that expose services to the internet
- Failure to enforce multi-factor authentication
- Use of default credentials and configurations
- Insufficient controls for remote access
- Incorrectly applied privileges or permissions and errors within access control lists
- Poor password policies
- Unprotected cloud services
- Insufficient phishing defenses
- Poor endpoint detection and response

Section 4

Rattling Doors and Testing Tactics

As the attackers continued maneuvers, they repeatedly set off security events on the managed systems. While the attackers attempted lateral movements and tested their tactics, Clearwater security analysts also gained additional insight into what the attackers' next move might be.

How could they tell?

The analysts found code that was similar to what was used by a Russian-based advanced persistent threat (APT) group. In-depth research with threat intelligence into the tools and tactics being observed served as a calling card or fingerprint that helped identify the patterns and potential attack targets. The next step was to focus on setting up additional containment and response measures.

Fingerprinting patterns and potential attack maneuvers

Section 5

Risk Containment

It was time to declare a security incident to contain the risk as the team of responders actively combed through all likely system paths. Another necessary but difficult decision was made. The organization should halt operational services, resulting in downtime with their business processing.

It's important to note that when attacks like this happen, it's often difficult, if not impossible, for organizations to continue business as usual. In this case, the business function had the option to pause to ensure the security of patient data. However, for provider organizations that must always ensure system access for patient safety and wellness, making this type of decision is even harder to make. In most situations it is necessary in order to contain outside attackers that have a foothold within an environment.

Section 6

The Silent Manuevers

During the next week, the forensic investigation continued. The process put systems into quarantine and these steps were planned and deliberate as to not tip off the attackers that Clearwater analysts were aware of the intrusion.

Why? Because doing so could have increased the execution velocity increasing the chance of triggering a data exfiltration or worse a full blown ransomware attack.

This cautious approach provided responders more insight into the extent of the breach while they simultaneously took actions to reduce the potential attack surface limiting the tactics the adversary could take. More countermeasures were implemented as part of the kill chain process. Systems were scrutinized and even shut down for a full forensic investigation and when they were brought back up they were configured for the highest level of threat detection by the Clearwater security analysts. This was necessary to ensure that upon return to operations, there wouldn't be an exposure point that later could reopen doors for another attack.

MITRE ATT&CK® is a curated knowledge base and model for cyber adversary behavior. ATT&CK Tactics, which are outlined below, are unordered and may not all occur in a single intrusion because adversary tactical goals change throughout an operation.

- **Reconnaissance**
- **Resource Development**
- **Initial Access**
- **Execution**
- **Persistence**
- **Privilege Escalation**
- **Defense Evasion**
- **Credential Access**
- **Discovery**
- **Lateral Movement**
- **Collection**
- **Command and Control**
- **Exfiltration**

Section 7

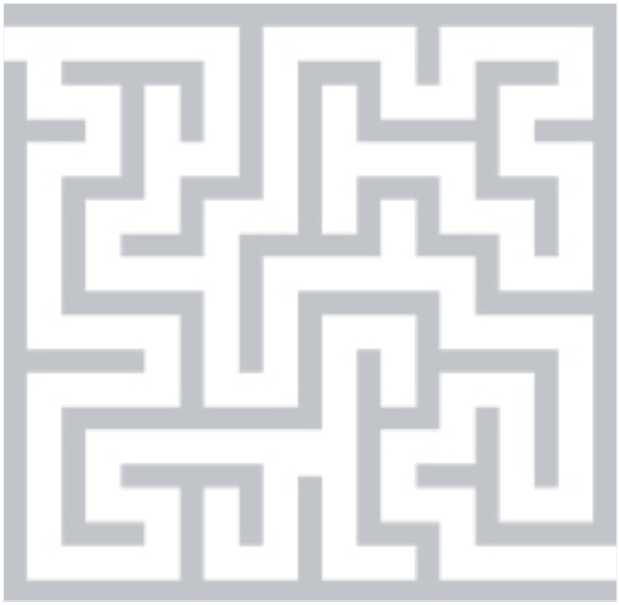
A New Path in the Shadows

Within 24 hours, the operational systems for this company were taken back and no longer exploitable by the attacker.

However, the bad actors didn't give up their persistence and found another path to exploit to again breach the organization. The attackers took advantage of the development assets that IT didn't routinely manage, so they did not have advanced endpoint detection or logging for these systems. The attack successfully exploited a shadow system and it's administration tool that enabled remote access. The attackers used this for the deployment of payloads to several other machines in this environment and then began their lateral movement.

Common lateral movement tactics:

- Exploitation of remote services
- Internal spear-phishing
- Lateral tool transfer
- Remote service session hijacking
- Remote services
- Replication through removable media
- Software deployment tools
- Tainting shared content
- Use of alternate authentication material



Section 8

Playing the Long Game

Over the next few days, the attackers played a game, making a move, while the security analysts countered. Eventually, about a week into it, the attackers went dark. They stopped triggering security events and setting off detection alarms.

It was likely the bad actors had gathered enough intel about the systems they accessed and were also aware the security team was on to them.

During this game of wait and see, Clearwater security opersations knew it wasn't time to stop response measures. They watched to see what the attackers would do next. Three days later, the attackers made their next move—the last push to execute their plan, which was an attempt to deploy ransomware to maintain the foothold they believed they had.

Fortunately for the client, Clearwater detected and stopped all the attackers' attempts and successfully contained the ransomware risk. With managed threat detection and response, actions were being monitored, and the endpoints and servers the adversaries targeted were immediately quarantined, blocking the ability to advance. In addition, orchestration across network devices and logs captured the active threat indicators and behavioral signatures. These were now part of the Clearwater security operations center (SOC) threat intlligence and ensured that any attack using these threats again, with this client, or across any other Clearwater managed security services client, would be thwarted and detected.

Response and Recovery Actions:

- Capturing forensic images
- Rebuilding machines
- Determining if backups are free of traces of the attackers
- Scouring logs for any associated anomolous activities

Section 9

After the Breach

This was a close call. As part of response and recovery, Clearwater security operations determined that the attackers had not exfiltrated or accessed client or sensitive data. However, the recovery processes was still underway, extending over the next several months and included the development of a post breach event action plan.

Based on the incident evaluation, additional plans to improve security measures across all areas were taken:

- Implement consistent advanced endpoint protection for all environments
- Modification to the multi-factor processes
- Implementation of geo-location logic
- Privilege account management
- Password policy and management improvements
- Additional security awareness training and authentication processes

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this ebook? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact