ALDRIDGE

CYBERATTACK CASEFILES

Healthcare Provider Gets Compromised, Defrauded, & Faces HIPAA Consequences

How Cyberattacks Work

Before we jump into this specific case, here's a quick overview of how cyberattacks work. Or, you can click here to jump to the case directly.

Step 1 Identify Target

There are two main approaches cybercriminals use to select their victims:

- Targeted – Attacker goes after a specific organization, conducting research on their tools, vendors, and people to construct a highly targeted spear phishing campaign or exploit identified vulnerabilities in their IT.
- Shotgun – Attacker launches a mass phishing email campaign on thousands of companies, only needing one or two people to fall for it and give up their credentials – providing the attacker access into the victim's email and organization.

Step 2 Gain Foothold

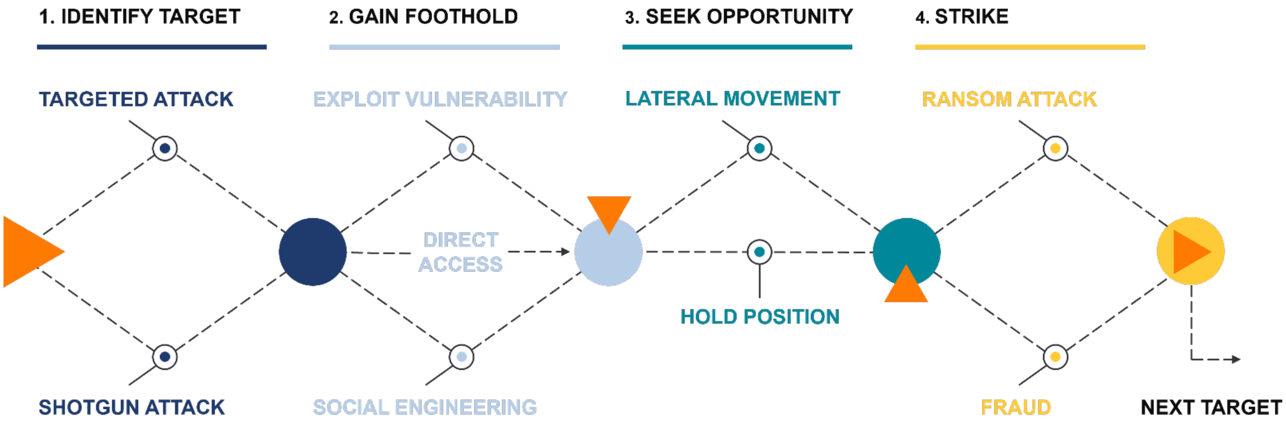
The threat actor has successfully breached an email/account or exploited a technical vulnerability to gain access inside their targeted organization's IT environment. This initial access point is crucial as it provides the attacker with a starting point from which they can further explore the target environment, expand their control, and carry out their intended objectives.

Step 3 Seek Opportunity

The attacker will use the visibility and access they gain from their initial foothold to identify how they can extract the maximum amount of value from their attack. This is referred to as a **lateral movement** - using their initial privileges and newfound access to information to further exploit their target organization.

Step 4 Strike

An attacker may hold their position for months, waiting for a good opportunity to escalate the attack and strike. Maybe the attacker has access to an employees' email and identified an exploitable financial conversation, such as renewing an expensive tool or service. The attacker will wait for an email containing an invoice to come through that they can intercept and alter, tricking the employee to wire money to the attacker's bank instead of the vendor.



The Attack

A respected healthcare provider fell victim to a **spear phishing** campaign targeted at their finance team. The victim organization was doing everything right – they had implemented industry recommended security tools and processes and their team was enrolled in ongoing security awareness training. Unfortunately, a sophisticated attacker can breach any organization with enough persistence.

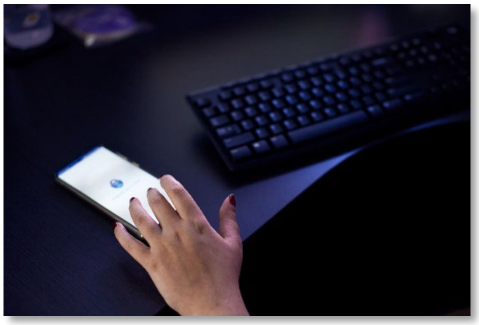
[Identify] Why Was This Organization Targeted?

Cybercriminals target healthcare organizations because the critical nature of healthcare services makes these organizations more likely to pay ransoms, while complex networks provide opportunities for unauthorized access and malicious activities. We know that this was a targeted attack based on the amount of research that went into creating a personalized phishing campaign that was designed for the victim organization's finance team.

[Foothold] How the Attacker Got Inside

The attacker got inside by using an **attacker-in-the middle attack**. They initiated their attack by sending phishing emails containing a link to a fraudulent Microsoft login page (set up by the attacker beforehand) to the target organization's finance team. One person fell for the phishing email and logged into the fraudulent page, giving the attacker their Microsoft credentials.

Defeating Multi-Factor Authentication (MFA)

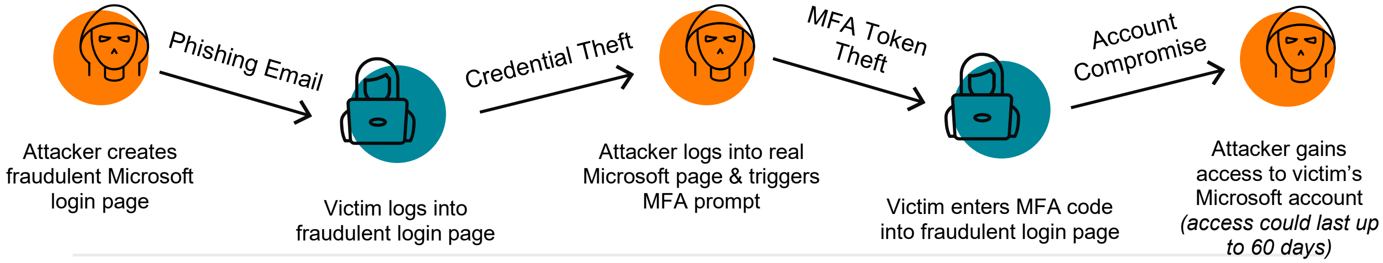


The attacker was monitoring their fraudulent login page. As soon as the victim employee entered their credentials into the fake page, the attacker copied their password and logged into the real Microsoft login page, triggering an MFA text code to be sent to the victim employee's phone.

The fraudulent Microsoft page also contained an MFA prompt, so the victim employee entered their real MFA code into the fake prompt. Again, the attacker was watching this all happen and as soon as the employee entered their MFA code, the attacker copied it into the real Microsoft login page – giving the attacker full access to the victim's Microsoft account and email. This entire sequence played out in less than 10 seconds.

When the employee entered the MFA code into the fake page, it may have just given them a login error and told them to try again later. It may have seemed odd to the employee, but not to the level where they felt the need to raise a flag and ask someone about it. They likely shrugged it off and got back to work, not realizing that they just had their account compromised.

Attacker-in-the-Middle Attack


Attacker creates fraudulent Microsoft login page
Phishing Email
Victim logs into fraudulent login page
Credential Theft
Attacker logs into real Microsoft page & triggers MFA prompt
MFA Token Theft
Victim enters MFA code into fraudulent login page
Account Compromise
Attacker gains access to victim's Microsoft account *(access could last up to 60 days)*

[Opportunity] What the Attacker Was Looking For

With full access to the victim employee’s Microsoft account, the attacker scanned their Outlook for correspondence with vendors to determine if the employee had any financial authority. The compromised employee was responsible for paying invoices, making them a high-value target. The attacker doesn’t need to seek further opportunity, they can camp out in their current position and wait for the right moment to strike.

Waiting For the Right Moment

The attacker slowed down the attack once they realized they were already where they needed to be, inside the inbox of someone with financial authority. They waited for 3 days, reading the victim employee’s emails; identifying vendor relationships to exploit.

The attacker identified a financial conversation that the compromised employee was having with a vendor. The attacker set up a fraudulent domain that looked like it belonged to that vendor and began emailing their target from that fake domain. The attacker emailed the victim for days using fraudulent domain to build trust before initiating the final phase of the attack.

[Strike] Defrauding the Victim

The attacker sent an email from the fraudulent vendor email domain with an invoice that fit with the conversation the victim was having with the actual vendor days prior. The email also mentioned that they have updated banking information and to please route the invoice payment to this new account.

To the victim’s credit, they did take a pause after they received new banking information. They looped in other members of their team to review the email and confirm that it was legitimate. Unfortunately, no one else on their team noticed anything wrong with the email and invoice – so the wire transfer to the attacker’s bank account was approved, completing the attack, and defrauding the victim organization out of $150k. Unfortunately, the damage extended beyond the wired money…

The Damage

$150K in wire fraud

3 Days Business Downtime & Disruption

The average cost of downtime in healthcare is **$7,900** per minute.
Source: What Are the Effects and Costs of Downtime to Healthcare Organizations?

HIPAA Ramifications

HIPAA fines can be civil or criminal, depending on the nature and severity of the violation. The civil fines range from **$100 to $25,000 per violation category, per calendar year**. The criminal fines range from $50,000 to $100,000 and imprisonment of up to one year to 10 years. A HIPAA violation can also result in civil liability in some cases. Required notification to affected persons incurs additional HIPAA violation costs.

Attack Reaction

The fraud was quickly discovered, and the victim organization immediately engaged their cyber insurance and IT team. Their cyber insurance carrier called in their incident response team to assist the organization's IT team in:

1. Attack Investigation – when did the attack start, what did the attacker do with their access, and what systems and users were affected?
2. Returning IT a Healthy State – shutting down the attack and restoring IT to a state before the attack began.

Fortunately, this was a relatively quick cyberattack; the entire process took less than 30 days. The timeline is significant because the victim organization did not have a **Security Incident and Event Management** (SIEM) tool, meaning they didn't have event logs beyond 30 days. If the attacker had waited longer before escalating the attack, say 5 weeks instead of 3 days, the incident response team would not be able to see how the attack began and may assume the compromise was much deeper than it was. If you can't say for sure, you'd have to err on the side of caution, which would mean a far more disruptive (and expensive) investigation and recovery process.

Thanks to the victim organization's quick reaction, the immediate damage from the attack was minimized. There was some downtime and disruption from the investigation, but it was manageable. They even managed to recoup most of the funds that were wired to the attacker. If you catch wire fraud early enough, you can reach out to the FBI for help. The FBI works with banks to disrupt wire fraud and claw back as much money as they can.

Although the immediate damage from the attack was minimized, there could be long-term fallout from possible HIPAA violations. The attacker gained access to everything that was in the victim employees' inbox. Every time the attacker had a chance to read an email containing protected patient data, it could be a HIPAA violation. Sorting out the HIPAA ramifications from this attack will be an ongoing pain for this organization.

Lessons Learned

You can be doing *almost* everything right and still get breached

The victim organization had **Multi-Factor Authentication**, but it was defeated by a Attacker-in-the-Middle attack.

They had ongoing **Security Awareness Training & Testing**; the compromised employee never failed a phishing test.

They had a policy to **confirm banking changes by calling**, but the accounting team didn't follow process.

Effective security requires a security-minded culture

Without true buy-in from your team, the security tools, training, and policies you have can be bypassed by a creative attacker. If people don’t know why the security policies and procedures are important, they’ll ignore them and do what is convenient like they did in this case.

The basics aren’t cutting it anymore

If this organization had a SIEM solution that was monitored around-the-clock by a security team or, Security Operations Center (SOC) this attack could have been discovered and responded to sooner.

A good cyber insurance policy is critical

At the end of the day, the victim organization made it through the attack with only a few scrapes and bruises. They prepared for a successful attack ahead of time by purchasing a good cyber insurance policy. A “good” cyber insurance policy is typically a stand-alone policy with adequate limits and includes attack recovery services like an incident response team.

Timing is everything

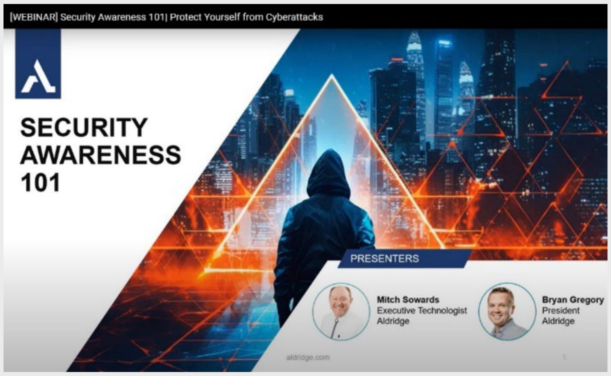
The victim organization’s quick reaction to the incident allowed their IT and response team to minimize the damage and even recoup most of their direct losses. In many cases like this, wire fraud is only discovered when the vendor shuts off services after months of non-payment. By that point, there is almost nothing you can do to recoup your losses.

Getting breached doesn’t have to be the end of the world

Going through a successful cyberattack, dealing with insurance, and navigating HIPAA violations is still painful; however, it is not catastrophic. The security elements and preparations this organization made ahead of time (even when imperfectly implemented) paid off and turned a potential catastrophe into something manageable.

Free Training - Security Awareness 101

This entire attack began with one person falling for a spear phishing email attack. Although security awareness training isn’t perfect, it is still the best way to educate your people on cybercrime and how they can defend themselves from it.



[WEBINAR] Security Awareness 101| Protect Yourself from Cyberattacks

SECURITY AWARENESS 101

PRESENTERS

Mitch Sowards
Executive Technologist
Aldridge

Bryan Gregory
President
Aldridge

aldridge.com

1

Take advantage of our free Security Awareness 101 training to **learn the fundamentals of cybersecurity and how to recognize and report spear phishing attacks in under 60 minutes**. If you are concerned about your teams’ security awareness, this training is for you.

WATCH NOW