WAR STORY

PHISHING & ADVANCED PERSISTENT THREAT (APT)

ATTACK DETAILS

A company in the manufacturing space realized that $700,000 was missing from its bank account. It also noticed that it had been a while since it received payments from some of its regular customers. Eventually, they realized that someone was intercepting its client payment emails and rerouting the money into a different bank account. The company frantically determined it was under attack. Unbeknownst to the organization, the attacker had been in its network for many months and was now deeply embedded in the company's infrastructure.

AT A GLANCE

Industry

- Manufacturing

Company size

- 2,000 employees

WHAT WE DID

Blue Team Alpha's elite cybersecurity team went "head-to-head" with the attacker and was eventually able to evict them. Due to the company's insufficient logging information and the attacker's keen ability to cover their tracks, we could not determine a specific initial point of entry. Statistically speaking, though, access likely came from a phishing email or an externally-accessible server that was poorly managed and vulnerable.

The company relied on several outdated systems and applications. Many of these contained known vulnerabilities that make it easy for attackers to gain network access.

Emergency | 612-399-9680 | 911@blueteamalpha.com
Email | sales@blueteamalpha.com
Web | blueteamalpha.com

WAR STORY

PHISHING & ADVANCED PERSISTENT THREAT (APT)

In this situation, the company's systems were too outdated and improperly managed to provide "full containment," so we delivered what we call "reasonable containment," which allowed us to move to the next and most crucial phase of the response - eradication. Our team quickly and completely evicted the attacker from the company's environment. We also contacted the FBI to recover the $700,000 missing from the company's account. However, the attacker dwelled within the company's network for so long that the FBI could not help.

Blue Team Alpha offered its expert remediation recommendations, and as of the writing of this case study, more than 12 months post-incident, the company has not had any additional cybersecurity issues.

LESSONS LEARNED

Relying on outdated servers and applications with known vulnerabilities dramatically increases the chances of falling victim to a cyberattack. It also makes it more challenging, if not impossible, to fully remediate an attack, potentially leaving your company at risk for future threats. We recommend taking a proactive approach to cybersecurity to shore up your defenses before an attack occurs.

Looking for help with proactive cybersecurity? Blue Team Alpha's virtual chief information security officer (vCISO) services make certified, top-tier security experts available to organizations who need security guidance and expertise. Our experts have decades of experience building security programs that show measurable improvement in security posture.