WAR STORY

PHISHING & RANSOMWARE

BLUE TEAM ALPHA

ATTACK DETAILS

AT A GLANCE

Industry

- Logisitics

Company size

- 600 employees

An attacker sent phishing emails to employees of a company in the logistics industry. One of the users opened the email, thought it was legitimate, and entered their username and password credentials. Knowing that many people sync their computer and email passwords at work, the attacker used the employee's login credentials to access the organization's VPN. Once inside, the attacker surveyed the environment, figured out “who’s who” in the organization and sent emails to targeted individuals from the compromised email account.

The attacker was inside the organization undetected for several months. They gained access to administrative accounts, deciphered the timing of invoices and expected payments, and obtained the company’s bank wiring details.

They wired approximately $300,000 from the company’s bank account into their personal account. Additionally, they sent several pending invoices with updated false payment information, so the money would go to their account when payment was made. If that wasn’t enough, the attackers also set off a ransomware attack, encrypting all of the company’s computer assets.

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

WAR STORY

PHISHING & RANSOMWARE

WHAT WE DID

A lot of cleanup work needed to be done because of this attack, but our team dug in and devoted more than 300 hours to get the job done. The company had 300 workstations, all of which needed to be reloaded due to the ransomware attack. We arrived on site and set up camp in a large conference room. We set up an imaging service to create copies of all of the computers. Fortunately, the company had encrypted backups and a SAN (Storage Area Network) snapshot, which truly saved it from irreparable damage.

We used the backups to start restoring services. Our team's expertise and the additional hardware we brought to help with remediation enabled us to get the business back up and running within three days. All of the workstations were reimaged within five days. Unfortunately, there was one site for which the company did not have quality backups, and it needed to pay the ransom for this data. We were, however, able to lower the ransom amount by $250,000, negotiating $850,000 to approximately $600,000. In these situations, companies are often powerless, as these ransomware attacks originate from non-extradition countries, leaving no options for recourse.

LESSONS LEARNED

Regular, encrypted, and "air-gapped" backups are a critical component of cybersecurity. Air gapping is the act of disconnecting the backup device from the network, so it can't be compromised if the entire network is attacked. Failure to take these proactive measures can cost you deeply if an attack occurs. Employees should be educated on phishing attacks, and companies should ensure login credentials are not duplicated across email and network access.

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