Case Study

BINARY DEFENSE

Binary Defense Counterintelligence helps financial institution thwart cyber attack

Business

Savings bank with $50 million+ in assets, serving customers in five states

Challenges

Financial institutions are frequently in the crosshairs of hacking organizations or individuals

Existing solution was not providing 24-hour monitoring

Needed to expand the team's current skillset with counterintelligence expertise

Results

Binary Defense Counterintelligence Team detected an impending DDoS attack

Bank cybersecurity team took advanced precautions to thwart the attack

Avoided disruption of service due to preventative measures

"With the notifications and pre-warnings that Binary Defense provides, we are able to take as much precaution as possible."
- Cybersecurity Manager at financial institution

The customer

A long-established New York City-based savings bank with over 250 branches and 5000 employees.

The bank has a Cybersecurity Manager, responsible for all aspects of cybersecurity across the company, including vulnerability review, incident response, risk management, penetration testing and policy creation.

Highly targeted for cybersecurity threats

The financial industry as a whole is the most highly-targeted industry for cyberattacks–with banks facing 2000 attacks every minute of the day[1]. In addition, the financial industry is highly regulated to ensure that the crucial customer data they hold is secure. As a result, banks need to have strong cybersecurity programs in place to safeguard their customers' data against breaches and stay compliant with regulations.

Bringing the bank's security to the next level

Because of its location in New York City, and the number of branch offices the company has, this institution faces the threat of cyberattacks all the time. Prior to choosing Binary Defense, the Cybersecurity Manager and his team were using a Network Operations Sensor to monitor their assets. But, they couldn't do 24 hour-a-day monitoring. His staff monitored and managed the alarms from the sensor, but they needed a solution to help his team look for patterns, and begin to take action on them. "We needed someone who could take our systems and bring them up to the next level," said the cybersecurity manager.

In addition to selecting Binary Defense's Security Operations Center (SOC) to monitor their Security Information and Event Management (SIEM), the bank also purchased the Counterintelligence (CI) solution. Counterintelligence from Binary Defense is proactive monitoring of the darknet, Clearnet and social media for threats against a company's people, data and brand. The Binary Defense CI team is comprised of experts formerly employed in security in the military, government and private sector. "With the notifications and prewarnings that Binary Defense provides, we are able to take as much precaution as possible," the cybersecurity manager said. "When we get the potential for an attack, it allows us to make arrangements to mitigate it."

1 https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#3dcde30f6e90

Binary Defense Counterintelligence

Proactive, advanced threat hunting

Skilled and experienced intelligence specialists

"Eyes on glass" monitoring for physical, cyber and public image threats

We are an extension of your team

"Binary Defense gives me peace of mind because I know they're watching our network 24/7 ... We've put excellent procedures in place." - Cybersecurity Manager

DDoS attack proactively avoided

The Binary Defense CI team proactively searches 24/7 for threats against the bank and alerts the Cybersecurity Manager and his team when they see any suspicious activity that merits further investigation. At one point, the Binary Defense team noticed some chatter by a threat actor group regarding a planned Distributed Denial of Service (DDoS) attack on the bank. With this information, Binary Defense was able to give the bank a two week advance warning that an attack was coming.

Had the hackers succeeded with the attack, several systems could have been impacted, including the the bank's mobile banking site and company website, effectively preventing customers from accessing their banking information and bringing business to a halt. Having a heads up from Binary Defense allowed the bank's cybersecurity team to take action. "We could notify our service providers that something could happen, as well as internet scrubbing services that we subscribe to through third parties to look out and keep and eye on things," the Cybersecurity Manager said. The more knowledge you have, the more you can look for patterns."

"Banks are a common target for DDoS attacks. Our Counterintelligence team monitors threat actor groups to ensure that we are able to get out in front of the attack before the attacks hit our customers," said Dan McNemar, Binary Defense Director of Counterintelligence. "Any time we can prevent or mitigate an attack, it's a good day for us."

Security posture tightened up with help of Binary Defense

The bank has never suffered a major breach, largely in part to the Binary Defense CI team and the 24/7 SIEM monitoring. In addition, the bank's security team has tightened their security posture over the years with the guidance of Binary Defense, as well as sister company, TrustedSec. "Binary Defense gives me peace of mind because I know they're watching our network 24/7. I know that if alerts happen, we will get notifications. We've put excellent procedures in place. It definitely takes a lot of pressure off," said the Cybersecurity Manager.

600 Alpha Parkway, Stow, OH 44224

+1 800-246-2792

info@BinaryDefense.com

BINARY DEFENSE™

Learn more about us
www.BinaryDefense.com