SPEARTIP A company of ZURICH

SHADOWSPEAR® CLOUD MONITORING CASE STUDY

Protect cloud applications from cyber threats

COMPANY PROFILE

INDUSTRY

Construction

SIZE

0 - 5000 Users

REGION

Western United States

REVENUE

Industry Revenue, 2023: $1.8 T
U.S. Employee Count: 8.0 M
Revenue per Employee: 225k

PROTECT

- Google Workspace
- Microsoft Tenant
- Salesforce

DEFEND AGAINST

- Business Email Compromise
- Data Theft
- Wire Transfer Fraud
- User Account Takeover
- Multi Factor Authentication Bypass

Sources:
www.bls.gov/iag/tgs/iag23.htm
www.statista.com/topics/974/construction/#topicOverview

BACKGROUND

The victim, a construction management firm, was tricked into wire transferring over $800,000 to threat actors posing as the victim's vendor, an engineering company they were working with.

To initiate this cyber crime, threat actors gained access to the victim company's computer networks, including their email servers and accounts, through phishing attacks. From there, the threat actors allegedly identified employees responsible for financial obligations and their contacts with other companies.

The perpetrators created a spoofed email address, posed as a vendor to which the company owed money, and tricked them into wiring funds to an account the fraudsters controlled. The fraud was not detected until it was too late to respond.

SPEARTIP'S SOLUTION

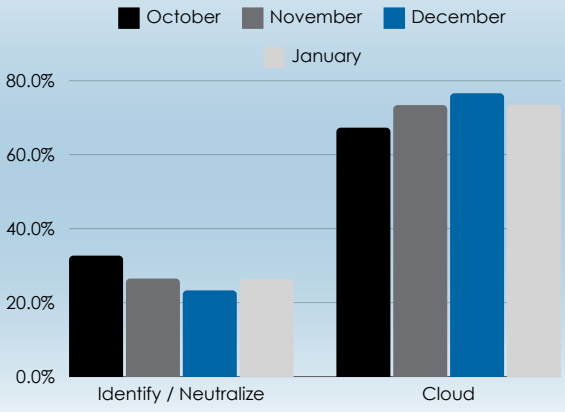
SpearTip's Security Operations Center (SOC) stands in as your defense against cyber threats, including account takeover and wire transfer fraud. Although, you cannot predict every incident or attack on your business, having a 24/7/365 team with vision into your environment can drastically improve your ability to respond to malicious intrusion attempts.

WHY CONSTRUCTION IS TARGETED

• Large-scale projects often include numerous vendors and require the transfer of large payments

• Construction projects are time sensitive and the care to thoroughly review every email is not always taken

• Contact information, bid data, or project costs can be collected by threat actors from public and private sources



Over the last year, threat actors have moved away from Ransomware operations. Ransomware campaigns are challenged by EDR tools and the availability of backups, often resulting in threat actors investing a lot of time, for marginal gain. Instead, threat actors focus on email environments. Data ingested by the SpearTip SOC suggests cloud application alerts make up a majority of all alerts our SOC is receiving, which indicates a necessary proactive approach to identifying risk in cloud applications.

Your organization may be vulnerable, but without vision, it can be difficult to gauge. That's why we are currently offering a 30-day trial of this service, offering absolutely free. To get started, visit speartip.com/shadowspear-cloud-monitoring or email us at info@speartip.com.

SPEARTIP A company of ZURICH

SHADOWSPEAR® CLOUD MONITORING CASE STUDY

Protect cloud applications from cyber threats

CONCLUSION

This incident demonstrates the immense need for a security services like SpearTip's 24/7/365 SOC paired with ShadowSpear Cloud Monitoring.

The work Zurich Resilience Solutions (ZRS) and SpearTip has engaged in with construction organizations has allowed our teams to address the repetitive presence of business email compromise, data theft, and fraudulent wire transfer. You may be familiar, but what are the next steps to protect your organization against these threats?

Executives must understand today's threats and what they mean for their business. Protecting brand image and revenue, maintaining critical operations, and fortifying sensitive data from threat actors are always top of mind, so establishing a framework and working toward cyber maturity is crucial for construction firms.

Construction requires numerous digital communication channels and has yet to be heavily regulated like some other industries. Aggressive threat actors will identify this trend and continue to look for organizational weaknesses.

*NEW FEATURES INCLUDED IN CLOUD MONITORING

- See the security scores of Microsoft tenants
- Reviews the Microsoft recommended actions that will improve the security score
- Provides recommended security actions across tenant
- Benchmarks your security scores against industry peers to ensure scores are on par
- Receives alerts if a security score regresses so we can act to keep security scores within acceptable levels

SPEARTIP.COM
800.236.6550
INFO@SPEARTIP.COM

SPEARTIP DEFENDS YOU