

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.

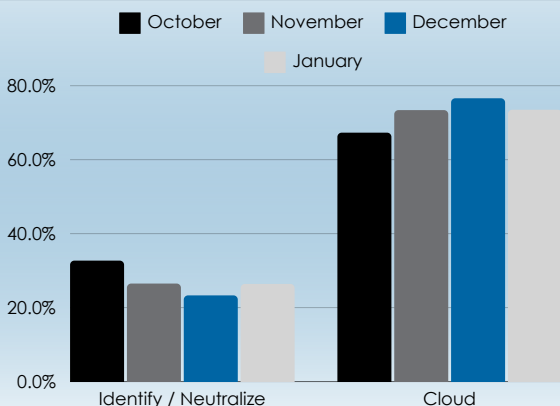
The perpetrators created a spoofed email address, posed as a vendor to which the company owed money, and tricked them into wiring funds to an account the fraudsters controlled. The fraud was not detected until it was too late to respond.

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.

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

This is intended as a general description of certain types of managed security services, including incident response, continuous security monitoring, and advisory services available to qualified customers through SpearTip, LLC, as part of Zurich Resilience Solutions, which is part of the Commercial Insurance Business of Zurich Insurance Group. SpearTip, LLC does not guarantee any particular outcome. The opinions expressed herein are those of SpearTip, LLC as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any of its affiliated companies (collectively, Zurich Insurance Group) as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group. Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product nor will it ensure coverage under any insurance policy. No member of Zurich Insurance Group accepts any liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.