QUADRANT

CASE STUDY

Quadrant helps Private Equity firm investigate Business Email Compromise event and harden security posture.

THE **SNAPSHOT**

Customer: Private Equity firm, East Coast U.S.

Incident: Spearphishing / Business Email Compromise

Service: Incident Response / Compromise Assessment

Outcome: Mitigated impact; Deployed monitoring

TAKEAWAYS AT-A-GLANCE

- No one is immune to cyber attacks.
- Employee awareness is critical.
- Rapid response mitigates damages.
- Collaborative efforts enhance security.

THE **BACKGROUND**

As an East Coast Private Equity firm ('the Firm') that invests in middle-market businesses and has raised capital from a multitude of investors throughout the United States, this particular customer understands how important data protection and security visibility is. The firm worked with an MSP, however they had not deployed 24x7x365 security monitoring across all of their endpoints.

Housing a considerable amount of personal and financial information within their systems and contact tree, ransomware and data exfiltration remain a perennial threat. Like many organizations of their size, the Firm is supported by a small managed IT services staff and knows the value of cybersecurity protocols when it comes to a complex, changing threat landscape. Even being security conscious is not always enough, however.

"There is nothing scarier than finding out that someone is impersonating you to ask your trusted contacts to wire money to a fraudulent account. The Quadrant team understood the urgency of the situation and acted quickly to remove the attackers from our systems and keep them out. I only wish we had found these guys sooner."

-Partner, PE Firm

THE **INCIDENT:** A SPEARPHISHING ATTACK

On an average Wednesday afternoon, an Executive Assistant at the Firm received an email to their inbox from a trusted M&A advisory firm that looked like many they had seen before, from an account they recognized, containing a seemingly benign link to what looked like a data room (common shared storage space).

They ***clicked...***

THE **INCIDENT** (Continued)

Unbeknownst to them, the individual sending the email was not who they appeared to be, and the link was not to a data room. Rather, a malicious link that compromised their session token and allowed unauthorized access to their account and global admin privileges.

The Executive Assistant had fallen victim to a "spearphish"; a highly-targeted phishing technique that attempts to trick even security-aware users into trusting the content and sender. In this case, the sender's account had also been compromised up-stream, leaving our victim at the Firm with few red-flags to identify the spearphish.

The Threat Actors went to work, first by establishing a foothold, strategically adding multiple seemingly innocuous accounts as a backup to maintain access in case the compromised account was detected and locked. They then implemented inbox rules and email forwarding to conceal their activities within the environment. Leveraging the compromised, over-privileged account, they expanded their reach, targeting other accounts within the firm, including those belonging to the partners.

Using a similar but adapted playbook to the one that had successfully compromised the Executive Assistant, they began sending fraudulent but convincing emails from the Partners' accounts to other known contacts in the Private Equity space for financial gain.

THE **RESPONSE**

A user downstream, receiving a spearphish impersonating a Partner at the Firm, reported the email to his security team after questioning the tone and timing of the email. Verifying the link was malicious, the security team alerted the Firm that they had an active incident unfolding. the firm contacted their outside counsel, who brought in Quadrant, knowing that their response would be expert and immediate.

Quadrant Security is well-known in the Private Equity space as a security partner acutely aware of the unique dynamics in the world of alternative prviate investments. Quadrant immediately launched into Incident Response mode, teaming with the Firm's MSP to evict the threat actors by signing out all users, revoking MFA tokens, and resetting passwords. Thereafter, they began auditing the sign-in and admin logs to discover the root cause and confirm that the compromise had been thwarted.

THE FINAL **TAKEAWAYS**

Quadrant worked in close collaboration with both outside counsel and an MSP to reduce the Firm's associated legal liability/risk, while taking measures to secure the Firm's environment and monitor additional attacks, which it was able to thwart. It's important to remember:

No One Is Immune to Cyber Attacks. Even vigilant organizations can be targeted by sophisticated spearphishing campaigns. Small companies handling large sums with less mature security infrastructures are prime targets.

Limit Account Privileges. Implementing the principle of least privilege reduces the impact of compromised accounts.

Employee Awareness Is Key. Regular training helps staff identify and report suspicious activities promptly.

Verify Financial Requests Independently. Always confirm unusual or significant transactions through a secondary method, like a direct phone call.

Rapid Response Mitigates Damage. Immediate action, enabled through 24x7 monitoring by security experts can significantly reduce the impact of a breach.

Collaborative Efforts Enhance Security. Open communication between organizations aids in early detection and prevntion of attacks.