Redpoint Cybersecurity LLC

BUSINESS E-MAIL COMPROMISE (BEC) USE CASE

THE PROBLEM

A major public relations and digital marketing agency faced a financially motivated Business Email Compromise (BEC). Redpoint Cybersecurity engineers provided agile response coupled with remediation and a planned penetration test (pentest) to additional vulnerabilities and indicators of compromise on the network.

- In the four-personnel finance department, attackers, in the span of two weeks, successfully compromised and exploited one account and attempted another; the attackers were able to spoof the domain and intercept email, resulting in a redirected ACH payment.
- The client, although using an MSP (Managed Security Provider) did not enforce the whitelisting of domains, SPF (Sender Policy Framework), or DMARC (Domain-based Message Authentication, Reporting and Conformance)/DKIM (DomainKeys Identified Mail), as means to authenticate and increase visibility on senders outside of the client enterprise.
- The client did not enforce a strong, complex password policy, deploy endpoint protection, or deploy Multi-Factor Authentication (MFA).

TOOLS & TECHNIQUES

- **BEC Investigation:** Redpoint engineers gained privileged accesses to the client's Microsoft Office365 instance. With those credentials, engineers deployed the following PowerShell modules to scour through the logs:
  - o Exchange Online PowerShell
  - o Azure AD PowerShell Module
  - o MSOnline Powershell Module
- **JQ, in conjunction with Microsoft Excel**, was used to verify if any mailboxes were illicitly used or if new mailboxes were created for redirection and successfully spoofed the domain to affect the client.

OUTCOMES

- Rapidly identified compromised accounts and source IPs upon commencing investigation, leading to the implementation of domain blocks and improved account hygiene
- An in-depth report highlighting vulnerabilities, proactive measures and next steps to increase situational awareness
- The IT team implemented new policies and procedures regarding increased procedure for client workstations statewide at all locations using the newly established infrastructure
- Leadership across the organization now has a better understanding of cyber security and how to better secure their network from future attacks. Redpoint has now commenced proactive services to hunt for additional vulnerabilities and indicators.

CONTACT US TODAY

TAB BRADSHAW

tab@redpointcyber.com
Principal
Redpoint Cybersecurity

RUSSELL SAFIRSTEIN

russell@redpointcyber.com
President
Redpoint Cybersecurity

This contains information which is general in nature and based on sources which are believed to be authoritative. Specific applications would require consideration of all facts and circumstances by qualified professionals familiar with a taxpayer and therefore we are not liable for the application of any information contained herein. No part of this correspondence may be reproduced or utilized in any form or by any means without written permission from Redpoint Cybersecurity.