COALFIRE

CASE STUDY

Global merchant service provider hires Coalfire to investigate a breach and validate its cybersecurity infrastructure

AT A GLANCE

A cyber incident is a matter of *"when,"* not *"if."* A leading global merchant service provider experienced this firsthand. However, this breach resulted in the successful prosecution of an international hacking ring and a dramatic enhancement of the client's network security posture that has successfully prevented and countered intrusions.

CHALLENGE

A multinational merchant service provider was breached by a sophisticated international hacking ring that resulted in a $10M global ATM cash-out in 24 hours. To provide a definitive answer regarding the breach to its customers and board of directors, the organization immediately hired an outside entity to provide incident response, forensics, and remediation services. To minimize the risk of future breaches, the organization worked with the outside entity to reassess its network security posture, and then contracted with Coalfire to implement the necessary changes.

APPROACH

The outside entity partnered with the merchant service provider to provide emergency incident response services to help respond to the breach. Through these services, the outside entity appropriately triaged, contained, and eradicated the incident. Then, they successfully investigated the incident, and not only found the initial attack vector and intruder activity, but also tracked the attackers and provided evidence to law enforcement. The client received a short-term containment plan to resolve the incident and a long-term remediation plan to harden it against future attacks.

Shortly thereafter, Coalfire performed a security engineering assessment, where they evaluated the extensive Payment Card Industry (PCI) infrastructure and rearchitected it to not only comply with regulations but also exceed the standard's requirements. The new architecture enhanced security and performance, providing the client with operational and technical cost savings over the long-term upgrade and replacement

roadmap. After the new architecture was approved, Coalfire brought the client back into compliance with various security frameworks and standards, including the PCI Data Security Standard (PCI DSS). The breach highlighted several areas of non-compliance, and Coalfire provided control guidance, testing, and program management on an aggressive time schedule across the organization to meet the client's compliance mandate. To do this, Coalfire performed a comprehensive enterprise risk assessment. The risk assessment prioritized the remediation items, control design and testing, and an enterprise penetration test.

Coalfire offers clients a single point of contact and seamless expertise for end-to-end breach response and remediation.

"In a meeting with the U.S. Incident Response firms, the Director of the FBI Cyber Division cited the close working relationship among the outside breach response firm, Coalfire, and their investigators as key to the arrest and successful prosecution of the Russian attackers. He emphasized the successful teamwork as the model for future joint incident response operations."

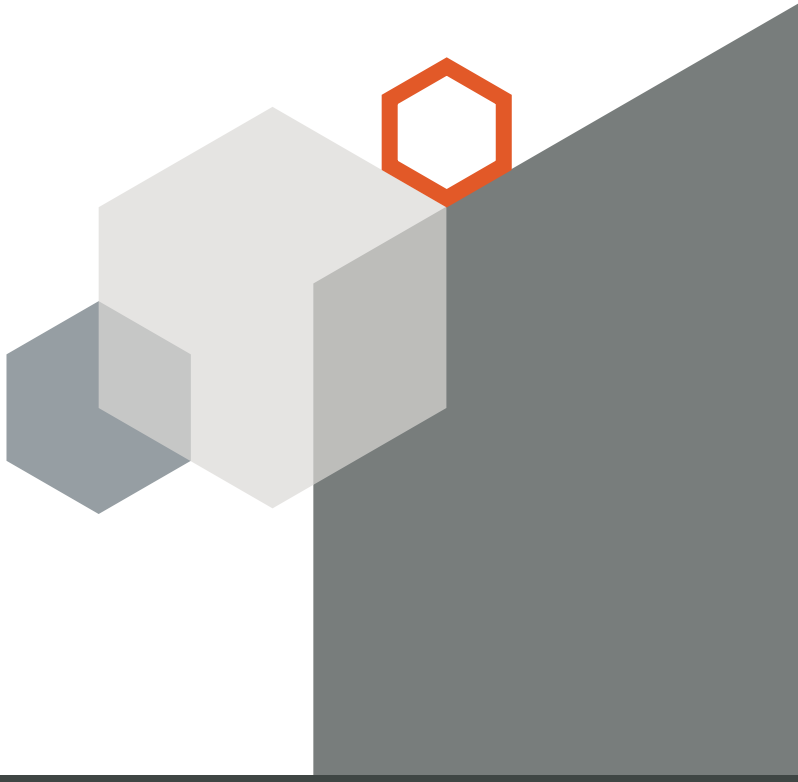
- BRIG. GEN. JIM JAEGER, USAF (RETIRED), CHIEF CYBER STRATEGIST, OUTSIDE BREACH RESPONSE FIRM

RESULTS

As a result of Coalfire's work, the global merchant service provider and international law enforcement authorities identified the attackers, brought them to justice, partially recovered the stolen funds, and implemented the lessons learned to avoid future breaches.

Coalfire effectively:

- Identified a sophisticated technique used by the hackers to attack ATM encryption systems.
- Provided crucial "lessons learned" to the organization, the PCI community, and U.S. and international regulatory agencies.
- Contributed directly to the arrest and successful prosecution of an international hacking ring.
- Defined and implemented long-term security strategies that have precluded subsequent breaches of the merchant service provider.



COALFIRE

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. **Coalfire.com**

CS_MerchSvcs_030419