GRA QUANTUM

CASE STUDY

Helping a world-leading credit card provider recover from a covert malware breach

Industry:

Finance and Banking

Goals:

- Determine source of costly data breach
- Achieve PCI Compliance

Service:

Remediation

Results:

- Determined source of data breach to be Russian criminal
- Became PCI Compliant to avoid total shutdown
- Developed standard employee training to mitigate future incidents

About GRA Quantum:

GRA Quantum is a pioneering information security firm with a mission to build close partnerships with our clients, serving them as trusted advisors in building effective, proactive plans. We believe in comprehensive strategies designed to harden networks, deflect attackers, and rapidly recover from any incidents.

A server in a data center of one of the world's largest white label credit card providers is covertly compromised by malware.

The Challenge

The breach leads to the theft of hundreds of temporary credit card account numbers and the siphoning off of millions of dollars into foreign bank accounts. Eventually, the financial damage resulting from these stolen assets and disruptions to normal business activities runs into the tens-of-millions of dollars.

The severity of the data breach then triggers a punitive response from the Payment Card Industry (PCI) Security Standards Council. In addition to a $100,000 fine, the company is given a short window of time to remediate the situation and submit proof of PCI security compliance or face total operational termination.

The Solution

The company's chief security officer (CSO) hired GRA Quantum to quickly and discretely investigate the situation and isolate the threat.

GRA Quantum's incident response team traveled to three different continents in order to conduct dozens of first-hand employee interviews and examine hundreds of pieces of evidence. The incident response team examined transactional records, log files, endpoint devices, and assessed the integrity of the physical security standards of the client's remote data centers.

Throughout the process, GRA Quantum maintained continuous communication with the client's board of directors in order to ensure PCI compliance was met as soon as possible.

The Outcome

GRA Quantum's investigative report determined the source of the breach to have originated from a Russian criminal element notorious for ransomware attacks. Our technicians traced the source of the breach to the computer of an unsuspecting employee who, while on a business trip, had inadvertently accessed an unsecure public network that was monitored by Russian hackers for potential victims. Through an access point made available by the employees computer, the hackers were able to work their way into one of the company's data centers.

GRA Quantum provided specific recommendations to help that client achieve full compliance with PCI's requirements, avoid a total shutdown of operations and ultimately save the company millions of dollars. The client subsequently sought out GRA Quantum's services again – this time to assist with the creation of a standardized cybersecurity education program for all current and future employees.

info@graquantum.com | 1(888) 610-6080