



FIND EVIL. SOLVE CRIME: HOW USING MANDIANT INTELLIGENT RESPONSE THWARTED A BANK HEIST

This case study demonstrates how MANDIANT Intelligent Response (MIR) helped one of our customers stop a bank robbery in progress — by accelerating their response to an information security incident.

WHERE MONEY GOES, CRIME FOLLOWS.

In late January 2008, MANDIANT's client — a mid-size bank with over \$1 billion in assets — received two alerts of a potential problem on their network. The first alert was from a Federal law enforcement agency who received a tip that the bank was targeted for a breach. The second from numerous customers who noticed irregular activity in their accounts.

Like most banks in the internet age, the bank offers its customers the convenience and ease of on-line banking. Like many banking infrastructures, the front-end application servers are part of a larger network containing consumer card data¹ and automated teller machine (ATM) systems. Attackers target these application servers in hopes of reaching the crown jewels — consumer card data.

Upon initial inspection, the bank suspected the breach involved systems that process card data, including ATM transactions. The breach may also have compromised the hardware security modules that perform the encryption of the PIN entry devices.

MANDIANT sent a team to the client site to work with the bank's personnel and diagnose the cause and extent of the incident. The objective of the investigation was to identify what the hackers had stolen; what systems they had compromised; and where all their tools were planted.

THE CASE

The compromise was the result of a Structured Query Language (SQL) injection attack conducted on the system that hosted the bank's public website. This attack provided the attackers direct access to the bank's back-end databases and over 700 systems behind the corporate firewall.

Once on the network, the perpetrators were able to push malicious software (malware) to the bank's systems and then spread laterally throughout the network. Although their prime target was credit card numbers, the attackers also installed key-loggers and monitoring software on an unknown number of systems.

Firewall logs could verify that data left the bank's network, but because the hackers deleted all temporary files with harvested card data after extracting them from the network, there was no way to

¹Consumer card data refers to bank card, credit card and debit card numbers.

determine *what* data left. Computer forensics would have to be performed on every system in which the attackers were active in order to retrieve those deleted files.

The firewall logs could also identify active backdoors on the network, but every system would need to be verified as “clean” before the bank could resume normal operations.

THE RESPONSE — (FIND EVIL)

As part of the response, the team deployed MANDIANT Intelligent Response™ (MIR). Using MIR allowed them to collect data from over 550 systems throughout the bank’s infrastructure and understand the scope of the incident within three hours.

MIR gave the team the capability to list running processes, search for files and extract suspect binaries from compromised systems without having to send a person to the systems in question. This saved a lot of time and resources, allowing the team to cover more systems in a much shorter time than they would have been able to do with traditional incident response techniques. Moreover, MIR gave the team the ability to search for and retrieve deleted files, allowing them to better determine the amount and type of data that was stolen.

Perhaps most importantly, MIR was able to identify several pieces of dormant malware that the attackers had left behind... but not yet activated. This malware, in the form of key-loggers, would not have been found if not for MIR’s ability to search every system on the network. Had the key-loggers not been found, it would have been possible for the attackers to re-enter the bank’s network at a later date when the tools were activated.

CONCLUSION — (SOLVE CRIME)

Using MANDIANT Intelligent Response™ enabled the bank to ascertain quickly which systems were compromised within its network and to determine what data had been stolen. MIR was also able to help the response team ensure the attackers were extricated from the bank’s network, so they could safely resume normal operations.

The speed and accuracy of MIR meant that the response team was able to perform in hours work that would normally take days. Because MIR saved the team time, they were able to ultimately save the bank money by responding rapidly to the incident and implement a successful remediation plan that prevented the loss of customer assets maintained by the bank.

ABOUT MANDIANT

MANDIANT is a company of consultants, authors, instructors and security experts. We have chased bad guys through the computer networks of the *Fortune 500*, the defense industry, and the banks of the world. We have testified in court and helped bring many of these criminals to justice.

We can help you find evil and solve crime — through our products, services and skills. We can also help you avoid it, through proactive services and education.

To learn more about how MANDIANT Intelligent Response can save your organization time and money, contact us at info@mandiant.com or 1.800.647.7020.