Solutionary Case Study

SOLUTIONARY
AN NTT GROUP SECURITY COMPANY

INDUSTRY
Banking

COUNTRY
United States

BUSINESS CHALLENGE
ABC Bank (ABC) identified unauthorized wire transfers from their environment. They needed to know when and how it happened quickly, in order to mitigate future attacks and notify affected customers.

SOLUTION
ABC hired a specialized incident response team to manage the incident, including daily briefings with technical staff, executive management and board of directors.

SERVICES
On-Demand Critical Incident Response from the Solutionary Security Engineering Research Team (SERT), including:

- Incident management by seasoned incident response team members.
- Malware analysis and reverse engineering.
- Forensic analysis of incident artifacts.

RESULTS

- Identified attack methodology.
- Discovered indicators of compromise.
- Determined scope of impact quickly, limiting notification to only affected clients.
- Provided detailed reporting with full analysis of the attack, attack timeline, tactical and strategic recommendations, and executive summary.
- Enabled technical staff to focus on operations while trained incident response experts supported the response effort.

CLIENT OVERVIEW
ABC is a regional bank with assets of more than $12 billion. With a long history delivering business and consumer services, the bank operates over 30 branches in the three state region the bank serves.

ABC Bank* gets the right answers the fastest way possible, avoiding the wrong publicity.

Business Challenge

ABC Bank (ABC) has a skilled team of network and information technology specialists. They manage a large network, provide reliable services to internal and external clients and contribute to the bank's high operational efficiency rating.

When faced with an information security incident, however, the team was not well prepared to detect, investigate and respond to the incident. Responding to day-to-day operational incidents is one thing, but responding to a targeted data breach is another thing altogether.

While the technology team attempted to understand and mitigate the attack, they were not aware of the techniques being used by the attackers to facilitate the fraudulent wire transfers. The team realized they were dealing with something more advanced than an everyday security incident, but a very focused attack.

The attacker gained complete control of the systems used to initiate, approve and track wire transfers. The attack was initiated via spear phishing, allowing the attacker to escalate system privileges, install remote administration tools, increase authorized maximum wire transfer limits and perform a series of wire transfers.

All of these activities went undetected until an upstream provider identified three suspicious transfers, totaling over $5 million dollars, being sent to a pet grooming service in Idaho. Realizing the attacker was still in the network and time was critical, ABC decided they needed specialized outside expertise to contain and mitigate the breach.

Services Provided

ABC engaged the Solutionary Security Engineering Research Team (SERT) to provide on-demand Critical Incident Response services. SERT includes certified security professionals with specific expertise in:

- Incident coordination and management.
- Incident mitigation and containment.
- Forensic image acquisition (including maintenance, storage, chain of custody and destruction).
- Network and system forensic analysis.
- Malware reverse engineering and analysis.
- Federal and local law enforcement coordination.

** The bank name and some identifying details have been changed for this case study.*

About Solutionary

Solutionary, an NTT Group security company, is the next generation managed security service provider (MSSP), focused on delivering managed security services, security consulting services and global threat intelligence. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs. The patented, cloud-based ActiveGuard® service platform uses multiple detection technologies and advanced analytics to protect against advanced threats. The Solutionary Security Engineering Research Team (SERT) researches the global threat landscape, providing actionable threat intelligence, enhanced threat detection and mitigating controls. Experienced, certified Solutionary security experts act as an extension of clients' internal teams, providing industry-leading client service to global enterprise and mid-market clients in a wide range of industries, including financial services, healthcare, retail and government. Services are delivered 24/7 through multiple state-of-the-art Security Operations Centers (SOCs).

Value Derived

Incident Response:

SERT provided forensic findings so ABC could quickly notify only those customers affected by the attacks, avoiding the need for a broader public disclosure of the incident. Doing so reduced the overall cost of the incident and helped to preserve ABC's reputation with customers not affected. Quick action also helped ABC to prevent additional fraudulent wire transfers from occurring.

SERT provided a detailed description of the attack vector and methodology to ABC, including tactical and strategic recommendations in order to remediate the immediate threat and also prevent future attacks. Rapid action from SERT enabled ABC to regain control of their wire transfer systems and fully evaluate their controls, while meeting all required reporting guidelines.

Forensic and Malware Analysis:

SERT identified and provided a list of compromise indicators to ABC and assisted with investigations of their network infrastructure to identify additional unauthorized remote administration or other attacker tools. Because the attacker used the cloud to mask the attack, SERT wrote special tools to analyze the mult-host command and control the attacker used.

While reverse engineering malware identified during the attack, SERT experts pieced together the precise methods the attacker used to obtain an initial foothold into the ABC protected network. Analysis revealed not only findings from the current incident, but also aspects of security and process recommedations ABC should consider improving to prevent and detect future attacks. SERT works with both internal and external resources when conducting an incident response engagement. In this case, SERT also found a SQL injection attack within a cloud application used by ABC Bank that allowed controls to be bypassed. SERT advised the SAAS vendor of the attack.

Incident Management:

During the initial hours of the incident, many stakeholders asked critical questions that could not be answered by internal staff. Using a calm, practiced process, with daily communications briefings led by a SERT Incident Response Team Leader, accurate and timely information was provided at regular intervals. This enabled the entire ABC team to not only be more effective in their response, but also save many hours of ineffective incident management.

SOLUTIONARY

9420 Underwood Avenue
Omaha, NE 68114
(866) 333 2133
www.solutionary.com

Solutionary, an NTT Group security company, is the next generation managed security services provider (MSSP), focused on delivering managed security services and global threat intelligence.