

Coast to Coast

Shawn Guins
CISSP, EnCE

Disclaimer:

The following is an account of an intrusion event that I handled many years ago. I am no longer involved with any of the parties mentioned in this article.

The client targeted was a financial institution and, here, will be called “the Bank.” Some techniques and details of this incident will be omitted, for obvious reasons. The names and specific locations have also been changed. There are different ways people conduct incident response and handling. That’s why there are 31 flavors of ice cream.

Tuesday morning started off like any other day. I was sitting in my office with my morning cup of coffee when my phone rang. My boss stated that he had received a call from a client, the Bank, stating that they were being attacked by hackers. Until that day, I had no working knowledge of the Bank’s infrastructure nor did I know if the staff had the experience or expertise to correctly identify an actual attack versus a port scan, probe, virus, etc. Through my experiences working in security, I have come to realize that a lot of people use buzz words like “hackers” to identify events that they do not thoroughly understand.

The initial information I had was sketchy at best. I learned that the Bank had a firewall on the front-end along with a NIDS and were in the process of implementing the ASA solution into the infrastructure. I contacted the Chief Information Officer of the Bank as I grabbed my laptop bag and headed to their corporate office. I wanted to get a first-hand assessment of their current situation. The information he provided told me they were experiencing something more than just a simple port scan or viral annoyance.

The CIO stated that they were having trouble with an attacker continually modifying the Bank's customer login portal. They believed this modified page was allowing the attackers to collect the Bank's customers ATM information in order to create duplicate ATM cards. Branch transactions reports showed that the attackers were successfully withdrawing customers' funds. The Bank was initially alerted to the attacks when customers started reporting unauthorized ATM withdrawals from their accounts. The CIO said he had a "band aid" solution in place, but they really needed to identify the method of entry and stop the attack. The temporary solution had decreased the frequency at which the page was being modified but had not stopped the attack completely. As I pulled into the corporate office, I knew the next several hours were going to be interesting.

During a quick meet and greet with the staff and management in the conference room, I needed to start the flow of information quickly and begin delegating collection tasks. Since the staff had not identified the point(s) of entry, I requested a network diagram of the infrastructure including all branches and especially all entry points into the network. Additionally, I requested a copy of the firewall logs and configuration, router configuration, access logs, IDS log, IIS log, event logs from the web server, and SQL logs. On the positive side, most of the logs appeared to be intact and the history of some spanned back several months. I asked for two copies of each log, the first copy containing the last 12 hours of activity and the second copy, the complete log.

While the reports were being generated, I questioned the staff about the information they knew for fact. Speculation during the information gathering phase can cause more trouble than good, leading to a wild goose chase and a loss of focus on the facts. The M.O. described by management and the staff suggested this was a fairly complex operation that consisted of a group or multiple persons being involved.

The staff stated that they had experienced an identical attack the previous year that resulted in a reported loss of around \$30,000 in unauthorized ATM withdrawals. This resulted in the staff making various changes to the firewall configurations, the introduction of IDS monitoring, and

changes to other system and network devices. The attacks ceased after these changes were made so the problem was thought to have been corrected. The current attack cycle had resulted in the loss of approximately \$25,000 and growing so time was a luxury that could not be afforded. The initial attack profile developed by the staff from the previous and current attacks showed that within 10-20 minutes of the customer's financial information being collected, the attackers were making an ATM withdrawal from their account. The withdrawals were in the amount of the maximum withdrawal limit set by the Bank of \$400 per day. In the event there were insufficient funds in that account, the attackers repeated the process on the next forged ATM card. This method was verified via the ATM surveillance cameras and transaction reports. In order to slow the attackers, the Bank suspended all ATM transactions city-wide in Anyplace, Florida, where the unauthorized transactions were occurring. The unauthorized transaction began again shortly afterward in Anywhere, California. ATM surveillance cameras and transaction reports confirmed the attacker at that location was using the same M.O. that was used in Florida.

The staff installed an automated webpage publishing program that would monitor the content of the customer login portal periodically and republish the original when the modified page was found. The stop-gap measure worked for a couple of hours until the attack frequency changed. At this is point, the Bank decided to seek outside help, and I was called.

Presented with these facts, I began to sift through the growing pile of logs, documents, and diagrams. As it stood, the source of the attack could be coming from the Internet but could also be internally based or backdoor method. Several infrastructural changes had been recently added, that had not been documented on the master diagram, and was being updated on the fly. A modem bank resided on the network but was ruled out because it was disabled and used for vendor remote access. The diagram showed that VPN tunnels connected each branch back to corporate. There were only two connections to the Internet, a primary and alternate for DR purposes. The backup connection was verified as being inaccessible externally. The web server was segregated on a network apart from the corporate network and fed by a SQL server located within the corporate network. Once all the requested logs were collected, I started a Nessus scan on the internal network to help locate any possible servers, services, or undocumented

communication devices that could be the source. Multitasking and efficiency is the name of the game.

The firewall logs did not show any signs of malicious traffic coming through. Review of the IDS logs did not provide any finger pointing either. The reason for this will be covered later. Additionally, the firewall configuration did not contain any "ANY" source/services rules or configuration errors. The router logs did not provide any useful information. Doing any type of event correlation was beginning to look bleak. The IIS logs were the largest and took the longest to acquire because they had to be burned to disc. I started searching through the web server logs looking for any instance where the customer login portal page was requested. Due to its function the search returned several thousand entries. Buried deep within the thousands of entries was a HTTP request containing "xp_cmdshell." Utilizing this SQL Extended stored procedure function, a FTP GET request was made to a remote server which published the modified page on the web server. This had to be addressed but it did not explain why the firewall or IDS did not log or alert on it. The source IP address of that HTTP request came from the external interface of the firewall. A follow-up status meeting was called to realign the response focus.

I disclosed my findings to the staff and was informed that one of the undocumented infrastructure changes made was that IIS and SQL resided on the same server. The SQL server was moved to the web server based on a recommendation made by their own "security" person, whom I later found out was fired for hosting a porn server on the Bank's network. (Go figure.) Now that the method had been identified, the next step was to see how bad the configuration was and fix it.

Reviewing the permissions on the IIS/SQL server revealed a host of default permissions both with system security, IIS, and SQL. Oddly enough, the permissions on the IIS log directory were set appropriately. I can only guess that either the attackers could not access the logs, did not know how, or did not care. I was able to separate the web server and SQL server fairly quickly using a secure build document and security checklist. There were also some required coding

changes made by their developers. Once everything looked good and tested out with both servers, I began investigating the mystery questions.

Why did the web server show the source address as the firewall when it was on a separate segment? Apparently the IIS server originally resided within the corporate network, and when it was moved, the table of the router was never updated. Traffic destined for the web server was forwarded to the firewall, which in turn forwarded it to the web server. It was one of those weird routing situations that you'd think wouldn't work, but it did. Long story short, the routing table was updated.

Why the IDS system did not alert on any of these attacks? The IDS system was implemented upstream between the firewall and the router, a choice location. However it was connected to a switch which did not support spanning. The staff incorrectly "proved" the IDS functionality by attacking the device directly. As a temporary solution to having a network tap, the switch was replaced with a hub until an upgraded solution could be implemented. It's not the cleanest of solutions, but it worked in the interim.

Why the firewall did not show any signs of this traffic? The firewall was not configured to log successful inbound connections. It did log successful outbound traffic and I was able to rule out the source of the attack originating from within the corporate network. Connection logging can fill log space on a device very quickly, and this was the case here. I mitigated this by configuring a remote syslog server for the firewall and router logs.

In summary, I located the source of the attacks later that day. It turned out to be a compromised server in Sweden owned by an excavation company. I notified them of the intrusion and asked if they would look into it. I tracked down the source of the modified customer login portal page, which was located on a "free hosting" site based in Tennessee. I sent them a similar request. The Bank stated that they were not going to pursue the attackers even though they had video from the ATM machines and lost over \$50,000. They felt that the negative PR was not worth it.

Management also said they had been told by the local FBI office in so many words that unless it was over \$100,000, the FBI really would not get involved. That statement was never verified.

This insecurity could have been identified more quickly if I had received the web server logs in the beginning, but that was the hand I was dealt at the time. Hindsight is always 20/20. On the days to follow, the attackers attempted the same exploit and many other variants, scans, and probes but were never successful. It would have been nice, if given the opportunity, to identify and catch this group. However, it did make for an interesting day, fighting the bad guys.