FEATURE

11 Steps Attackers Took to Crack Target

Aorato, a specialist in Active Directory monitoring and protection, delivers a step-by-step report on how attackers used the stolen credentials of an HVAC vendor to steal the data of 70 million customers and 40 million credit cards and debit cards from the retailer.

By Thor Olavsrud
Senior Writer, CIO
SEP 2, 2014 4:45 AM PT

Despite the massive scale of the theft of Personal Identifiable Information (PII) and credit card and debit card data resulting from last year's data breach of retail titan Target, the company's PCI compliance program may have significantly reduced the scope of the damage, according to new research by security firm Aorato, which specializes in Active Directory monitoring and protection.

Leveraging all the publicly available reports on the breach, Aorato Lead Researcher Tal Be'ery and his team catalogued all the tools the attackers used to compromise Target in an effort to create a step-by-step breakdown of how the attackers infiltrated the retailer, propagated within its network and ultimately seized credit card data from a Point of Sale (PoS) system not directly connected to the Internet.

Many of the details of how the breach occurred remain obscured, but Be'ery says it is essential to understand how the attack happened because the perpetrators are still active. Just last week, the Department of Homeland Security (DHS) and United States Secret Service released an advisory that the malware used to attack Target's PoS system has compromised numerous other PoS systems over the past year.

Tracing the Attack Is Like Cyber Paleontology

While Be'ery acknowledges that some of the details in Aorato's account may be incorrect, he feels confident that the reconstruction is largely accurate.

"I like to think of it as cyber paleontology," Be'ery says. "There were many reports on the tools that were found in this incident, but they didn't explain how the attackers used these tools. It's like having bones, but not knowing what the dinosaurs looked like. But we know what other dinosaurs looked like. With our knowledge we were able to reconstruct this dinosaur."

In December 2013, in the midst of the busiest shopping season of the year, word began trickling out about a data breach at Target.

Soon the trickle was a torrent, and it would eventually become clear that attackers had gotten the Personal Identifiable Information (PII) of 70 million customers as well as data for 40 million credit cards and debit cards. CIO Beth Jacob and Chairman, President and CEO Gregg Steinhafel resigned. Target's financial damages may reach $1 billion, according to analysts.

Most who have followed the Target story know that it began with the theft of credentials of Target's HVAC contractor. But how did the attackers get from that initial point of penetration, at the boundary of Target's network, to the very heart of its operations? Be'ery believes the attackers took 11 deliberate steps.

Step 1: Install Malware that Steals Credentials

It started with stealing the credentials of Target's HVAC vendor, Fazio Mechanical Services. According to KresonSecurity, which first broke the story of the breach, the attackers infected the vendor with general purpose malware known as Citadel through an email phishing campaign.

Step 2: Connect Using Stolen Credentials

Be'ery says the attackers used the stolen credentials to gain access to Target-hosted web services dedicated to vendors. In a public statement issued after the breach, Fazio Mechanical Services President and Owner Ross Fazio said the company "does not perform remote monitoring or control of heating, cooling or refrigeration systems for Target. Our data connection with Target was exclusively for electronic billing, contract submission and project management."

This web application was very limited, Be'ery says. While the attackers now had access to a Target internal web application hosted on Target's internal network, the application did not allow for arbitrary command execution, which would be necessary to compromise the machine.

Step 3: Exploit a Web Application Vulnerability

The attackers needed to find a vulnerability they could exploit. Be'ery points to one of the attack tools listed in public reports on the list, a file named "xmlrpc.php." According to Aorato's report, while all the other known attack tool files are Windows executables, this was a PHP file, which is used for running scripts within web applications.

"This file suggests that the attackers were able to upload a PHP file by leveraging a vulnerability within the web application," The Aorato report concludes. "The reason is that it is likely the web application has an upload functionality meant to upload legitimate documents (say, invoices). But as often happens in web applications, no security checks were performed in order to ensure that executable files are not uploaded."

The malicious script was probably a "web shell," a web-based backdoor that allowed the attackers to upload files and execute arbitrary operating system commands.

Be'ery notes that the attackers likely called the file "xmlrpc.php" to make it look like a popular PHP component — in other words the attackers disguised the malicious component as a legitimate one to hide it in plain sight. This "hiding in plain sight" tactic is a hallmark of these particular attackers, Be'ery says, noting that it was repeated multiple times throughout the attack.

"They know they're going to get noticed in the end because they're stealing credit cards, and the way to monetize credit cards is to use them," he explains. "As we saw, they sold the credit card numbers on the black market and pretty soon afterward Target was notified of the breach by the credit card companies. The attackers knew that this campaign would be short-lived, a one-off. They weren't going to invest in infrastructure and becoming invisible because in a few days this campaign would be gone. It was enough for them to hide in plain sight."

Step 4: Search Relevant Targets for Propagation

At this point, Be'ery says, the attackers had to slow down and do some reconnaissance. They had the capability to run arbitrary OS commands, but proceeding further would require intelligence on the layout of Target's internal network — they needed to find the servers that held customer information and (they hoped) credit card data.

The vector was Target's Active Directory, which contains the data on all members of the Domain: users, computers and services. They were able to query Active Directory with internal Windows tools using the standard LDAP protocol. Aorato believes the attackers simply retrieved all services that contained the string "MSSQLSvc" and then inferred the purpose of each service by looking at the name of the server (e.g., MSSQLvc/billingServer). This is likely also the process the attackers would later use to find PoS-related machines, according to Aorato.

With the names of their targets, Aorato says the attackers then obtained their IP addresses by querying the DNS server.

Step 5: Steal Access Token from Domain Admins

By this point, Be'ery says the attackers had identified their targets, but they needed access privileges to affect them — preferably Domain Admin privileges.

Based on information given to journalist Brian Krebs by a former member of Target's security team, as well as recommendations made by Visa in its report on the breach, Aorato believes the attackers used a well-known attack technique called "Pass-the-Hash" to gain access to an NT hash token that would allow them to impersonate the Active Directory administrator — at least until the actual administrator changed his or her password.

As further evidence of the use of this technique, Aorato points to the use of tools, including penetration test tools, whose purpose is to logon sessions and NTLM credentials from memory, extract domain accounts NT/LM hashes and history and dump password hashes from memory.

Step 6: Create a New Domain Admin Account Using the Stolen Token

The previous step would have allowed the attackers to masquerade as a Domain Admin, but would have become invalid if the victim changed their password, or when trying to access some services (like Remote Desktop) which require the explicit use of a password. The next step, then, was to create a new Domain Admin account.

The attackers were able to use their stolen privileges to create a new account and add it to the Domain Admins group, giving the account the privileges the attackers required while also giving the attackers control of the password.

This, Be'ery says, is another example of the attackers hiding in plain sight. The new username was "best1_user," the same username used by BMC's Bladelogic Server Automation product.

"This is a highly abnormal pattern," Be'ery says, noting that the simple step of monitoring the users list and flagging new additions for sensitive accounts like administrator accounts could go a long way toward stopping attackers in their tracks. "You have to monitor access patterns."

He also notes that the reconnaissance actions taken in step four are another example of abnormal usage that activity monitoring can detect.

"It's very important to monitor for reconnaissance," Be'ery says. "Every network looks different, has a different structure. Attackers have to learn about that structure through queries. That behavior is very different from the normal patterns of users."

1 | 2 | NEXT >

New! Download the CIO May/June Digital Magazine

YOU MIGHT LIKE

Copyright © 2017 IDG Communications, Inc.