© Neil Daswani and Moudy Elbayadi 2021
N. Daswani, M. Elbayadi*Big Breaches*https://doi.org/10.1007/978-1-4842-6655-7_8

8. The Target and JPMorgan Chase Breaches of 2013 and 2014

Neil Daswani[1] and Moudy Elbayadi[2]
(1)
Pleasanton, CA, USA
(2)
Carlsbad, CA, USA

In this chapter, we cover the 2013 Target breach when hackers exfiltrated over 40 million credit card numbers and the JPMorgan Chase (JPMC) breach of 2014 when attackers stole the names and email addresses of over 70 million customers. We cover these two mega-breaches together because, in part, both were caused by third-party compromises. Organizations work with many third parties, including developers (as Cambridge Analytica was to Facebook), acquisitions (Marriott acquiring Starwood Hotels), and customers (Dun & Bradstreet providing customers data on businesses). As business models evolve to support more open “platforms,” we can expect to see the reliance on third parties “ecosystems” to increase, which makes the lessons from this chapter relevant and applicable. In the case of Target and JPMC, both were initially breached through a third-party supplier. The Target and JPMorgan Chase breaches were also significant because they were the first two mega-breaches, in which tens of millions of records were stolen in one shot, that took place starting in 2013 and 2014.

Target, the eighth largest American retailer, was breached in late 2013. Ukrainian hackers breached Target through third-party Fazio Mechanical Services, which ran the heating, ventilation, and air conditioning (HVAC) for 1800 Target stores nationwide (in addition to quite a few other retail chains). Hackers stole over 40 million customer credit card numbers through the point-of-sale registers and 70 million customers’ other personal information.

JPMorgan Chase (JPMC), one of the largest banks in the United States, was breached the following year in 2014. The FBI linked the JPMC breach to Israeli and Russian hackers who accessed over 90 bank servers and stole names, emails, phone numbers, and addresses of over 83 million customers. The attack began with a JPMC third-party website vendor, Simmco, that hosted the bank’s Corporate Challenge online platform which was used to organize charitable races.

The proverb “you are only as strong as your weakest link” applies well to managing third parties. Third parties should be treated as an extension of the organization itself that can ideally be secured at the same level of rigor as the organization itself. Third-party suppliers were the initial point of compromise for Target and JPMC, and both of their third-party suppliers were compromised due to phishing, malware, and inadvertent employee mistakes.

Why Target? Why the HVAC Supplier?

Before we dive into how this cyberattack occurred, let’s look at what made Target such an attractive victim and how the attackers infiltrated Target[1] through Fazio Mechanical Services.

Target, as a large retailer, works with many vendors to keep its supply chain running. Customers can go to www.target.com and access information such as the catalog of what Target sells, how to contact customer support, and other services. In addition to providing customers information on its website, Target provided information to its suppliers and potential suppliers on its public website, including how to send invoices, create work orders, and get paid for their services. Target provided a plethora of internal documentation for new and existing vendors on public-facing websites that did not require a login—no authentication or authorization allowed anyone from anywhere in the world to access the sensitive data. Anyone who did a Google search for "target vendor portal" could quickly come across Target's Supplier Portal[2] and browse through the plethora of documentation Target publicly hosts for its suppliers. The Target Supplier Portal also led to other Target pages such as the Target Facilities Management page, which included the Suppliers Download page, from which anyone could download a full list of all of the vendors that Target used.

If you were to download the list of Target HVAC vendors from the FM_HVAC_Oct_2011_Summary.xlsx Excel file on the Target Supplier[3] Portal, you would find in the metadata[4] of this file that it was created in June 2011 with a Microsoft Office 2007 license. The metadata also included the last user to edit the file, Windows user Daleso.Yadetta, and that HVAC file was last printed on Target's network at the Windows domain \\TCMPSPRINT04P\. From a simple Google search, one could discover that Daleso Yadetta was an employee who worked at Target for eight years. There is much data and metadata that could be gleaned from a single file, so one can imagine the information the hackers were able to piece together from all of the publicly hosted Target pages. For those who are familiar with the field of digital forensics, it is no surprise that so much information can be extracted. Target left itself vulnerable with all this publicly accessible data.

Third-party documentation may seem trivial, but such information is far from trivial—it can and was used to set up a successful attack. One of the themes that we will discuss in the second part of the book is the practice of "secure by design" philosophy. You should only provide information on a need-to-know basis and provide system access based on the principle of least privilege. That is, people should be given only the minimum access required for them to do their jobs. In the case of Target, there really was not a need for the entire Internet to know or be able to access the list of all of Target's suppliers.

The Attack: A Black Friday Nightmare

Two months before the Target breach, hackers launched an email malware scam against Fazio Mechanical Services, one of Target's less sophisticated suppliers. In an email malware scam, attackers send out emails to victims that contain links or attachments to malware. If the unsuspecting victim falls for the attack, malware is downloaded onto their computer and run.

At least one employee was duped, and once the malicious email was clicked, Citadel malware was downloaded onto the employee's computer. Citadel is a password-stealing bot program, and once the malware ran, hackers just had to wait for the employee to log in to the Target network once. By eavesdropping on the login, Citadel acquired the employee's Active Directory credentials.[5] Once the hackers acquired the credentials, they were able to log in to Target's network.

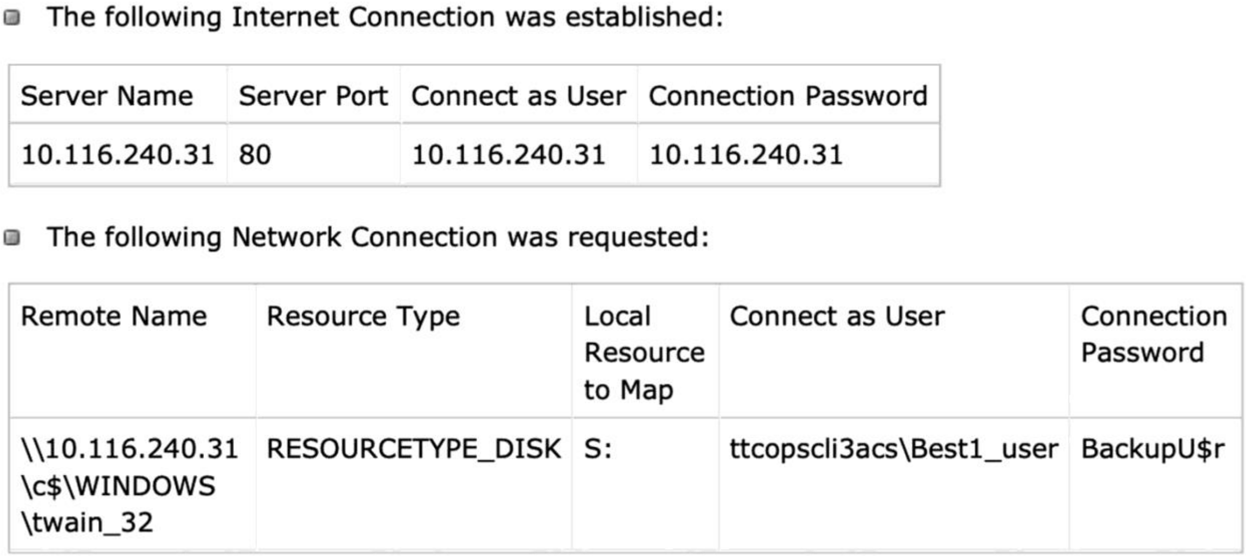
For this breach, it is important to know almost all Target contractors use an external billing system called Ariba. Ariba has functionality that allows contractors to upload invoices, for example, such that contractors can keep track of the work they do and then get paid by Target.

Aorato,[6] an Israeli hybrid cloud security startup, suggests that hackers were able to leverage a vulnerability in Ariba's web application and upload an executable PHP file. This executable file let hackers run commands of their choice. The hackers were able to query Target's active directory and probe Target's network. Aorato believes the hackers used a well-known technique called "Pass-the-Hash" to gain access to the hash token of an Active Directory administrator. Once logged in as an administrator, hackers created their own administrator account and were free to roam around Target's network. As will be discussed in the upcoming section on Verizon's audit of Target's network post the breach, auditors found that the Target network had almost no network segmentation.

Once a user—authorized or unauthorized—logged in to the system, they could access nearly every part of Target's network. Segmenting networks into zones with varying degrees of trust and data sensitivity is good practice, such that if one part of a network is compromised, it does not automatically allow attackers to access other parts of a network. Unfortunately, for Target, the point-of-sale registers and systems were connected to the same flat network where every employee had access.

Based on the lack of network segmentation and security in general (as discussed later on), there are many ways hackers could have breached the Target network. Once they gained access to Target's PoS systems, the attackers installed a "RAM scraper" on the PoS registers. A RAM scraper is a malware program that can copy sensitive data out of the memory of a device. A RAM scraper by the name of BlackPOS on the black market was used in the attack against Target. The attackers customized their BlackPOS RAM scraper to run undetected in specific environments. BlackPOS recorded the credit card numbers from the memory of Target's PoS register. Days after Target realized the breach someone uploaded a copy of the customized BlackPOS used on Target's PoS registers to threatexpert.com, a malware scanning service owned by the cybersecurity company Symantec.

From the report in Figure 8-1, you can see that hackers (username: Best1_user, password: BackupU$r) established a connection with Target's network (ttcopscli3as) in Brooklyn Park, Minnesota. The ttc in the domain name ttcopscli3as is probably an acronym for Target Technology Center, aka the name of Target's Minnesota campus.



The following Internet Connection was established:

Server Name	Server Port	Connect as User	Connection Password
10.116.240.31	80	10.116.240.31	10.116.240.31

The following Network Connection was requested:

Remote Name	Resource Type	Local Resource to Map	Connect as User	Connection Password
\\10.116.240.31 \c$\WINDOWS \twain_32	RESOURCETYPE_DISK	S:	ttcopscli3acs\Best1_user	BackupU$r

Figure 8-1

This image shows that hackers (username: Best1_user, password: BackupU$r) connected with Target's network (ttcopscli3as)[7]

Target's Real-Time Attack Response

As one of the largest American retailers, Target did have several defensive mechanisms in place. For instance, Target had multiple anti-malware tools in place to protect itself. Six months before the data breach, Target spent $1.6 million on anti-malware software products from FireEye. In addition to the newly deployed FireEye software, Target also had deployed Symantec Endpoint Protection (SEP) and had a team of FireEye security specialists in Bangalore monitoring Target's network and security 24/7.

Early Warnings

The anti-malware countermeasures sounded the alarm. The Bangalore team that monitored FireEye alerts noticed the malware and informed Target headquarters in Minneapolis. Target's deployment of SEP software also raised alarms and pointed to possible compromised servers—the same servers FireEye software was flagging. FireEye software has a feature that automatically removes malware as it is detected. That feature was unfortunately turned off, as false positive alerts sometimes cause business disruption when files are automatically removed or quarantined.

The specific malware classification the FireEye software provided Target to describe the malware was malware.binary. This categorization is fairly generic, and a large company like Target gets hundreds of these warnings every day. These warnings also came during the busiest shopping day of the year, Black Friday (the day after the US Thanksgiving holiday). Molly Snyder, a Target spokesperson, commented vaguely saying:

Through our investigation, we learned that after these criminals entered our network, a small amount of their activity was logged and surfaced to our team. That activity was evaluated and acted upon. Based on their interpretation and evaluation of that activity, the team determined that it did not warrant immediate follow up.[8]

The facts indicated that Target knew about the malware infections, had the opportunity to act, but having good anti-malware countermeasures was not enough. The malware classification was too generic and not specific enough that Target personnel felt they should be acted upon. In addition, there were so many generic alerts being generated that there was not enough "signal" compared to the "noise" being generated. A successful deployment of anti-malware countermeasures should result in a scenario in which each alert is high fidelity enough that it makes sense to act upon each alert. Else, if so many alerts are generated that one cannot have enough confidence in each alert, all the alerts stand to be ignored, leaving an open window for a breach to occur despite detections.

A Timeline and the Stolen Data

Target's network was first breached in mid-November 2013. Between mid- and late November 2013, attackers successfully uploaded their malicious software to a select number of PoS registers for testing. By the end of November, attackers successfully launched their fully functioning malicious software to the majority of Target stores nationwide. The attackers were able to collect records of all transactions, including credit card numbers, between the end of November and mid-December, during the busiest shopping weeks for Americans, including Black Friday and the bulk of Christmas shopping. On December 15, 2013, Target realized its network was breached, and three days later, the breach was exposed by Brian Krebs via his KrebsOnSecurity blog. Target came forward with news of the breach on the same day.

The Target data breach resulted in 40 million credit card numbers and the personally identifiable information (PII) of over 70 million customers being stolen. PII exposed in this breach included customer names, emails, phone numbers, and more. Customers were finding out their credit card information was compromised when banks notified them that they made a $900 purchase for oil in Russia, or their debit card had been drained and was in overdraft (true stories!). About one in three, or 110 million Americans, were affected by this data breach in one way or another in 2013.

Fazio Paid for Not Paying for Anti-virus

Understanding the security vulnerabilities of both Fazio Mechanical and Target paints a clear picture of what flaws in the two security systems allowed the attackers to penetrate the systems and what preventative measures could have been taken to create a more secure and robust network. Fazio Mechanical was using a free version of the Malwarebytes anti-malware software as its primary way to detect malware on its systems. Due to its use of Malwarebytes' free version, and its configuration, it took Fazio a long time to discover the email malware in its internal network. Malwarebytes anti-malware software is a very well-known and well-regarded anti-malware tool, but there are two concerns with the way Fazio was using the software:

1. 1.

The free version of the software does not scan software in real time and is an on-demand software scanner. Rather than continually scanning a system, the free version will scan a system when an input is triggered, such as clicking a button that says *Scan System Now*. The professional version of the software, which was not deployed at Fazio Mechanical Services, does scan a system in real time.

2. 2.
   The free version of this software was made specifically for individuals, and its license prohibits corporate use. Malwarebytes has specific software for businesses to protect from attacks such as the one to which Fazio fell victim.

The Verizon Auditors

Within days of discovering the breach, Target hired Verizon security experts to audit Target’s network. KrebsOnSecurity obtained a copy of Verizon’s confidential investigation report in late 2015. Verizon auditors state in the report that once in the Target network, there were “no controls limiting their access to any system, including devices within stores such as point-of-sale (PoS) registers and servers.”[9]

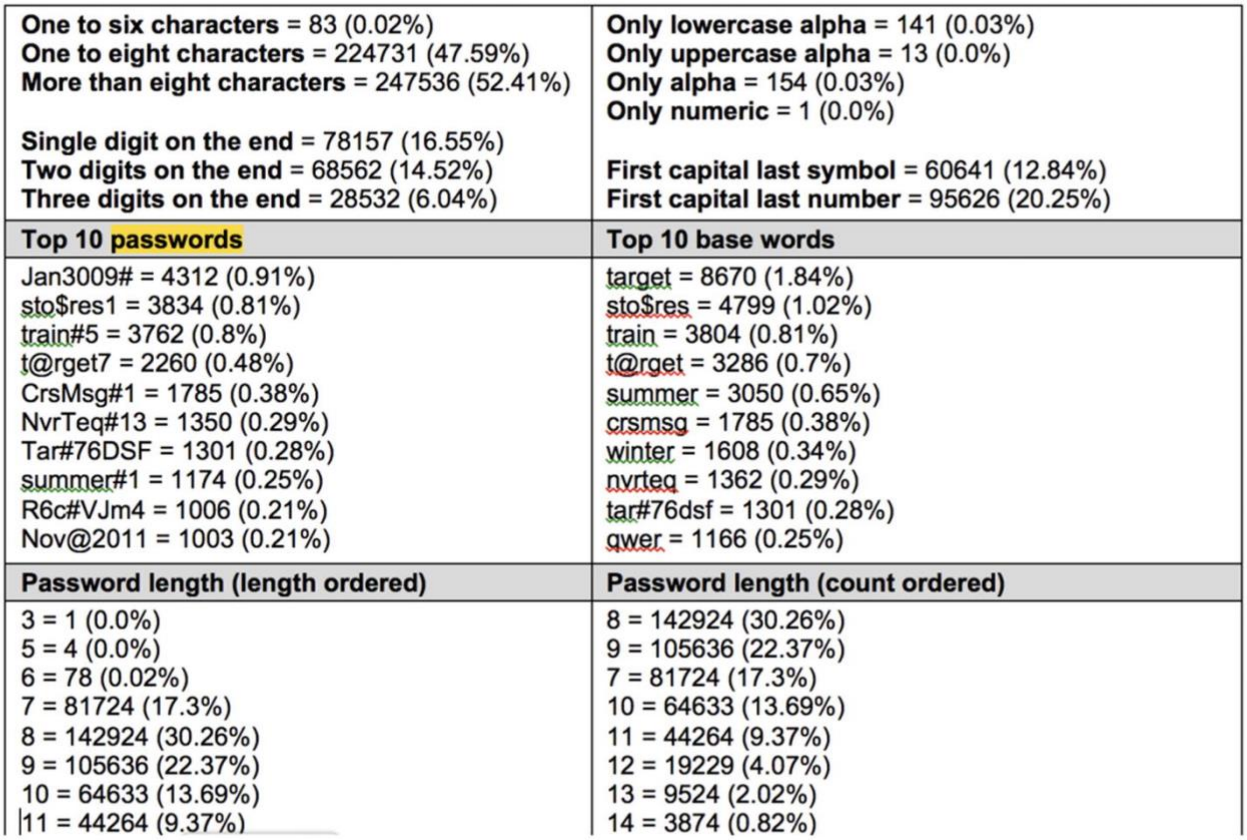
Verizon security experts found a slew of vulnerabilities that made the Target network extremely susceptible to an attack. At one point, Verizon consultants were able to communicate directly with Target’s PoS registers after they compromised a network-enabled deli meat scale in a different store. Each of the vulnerabilities Verizon consultants found is listed as follows:

1. 1.
   Lack of network segmentation: A lack of segmentation played a crucial role in hackers being able to access the PoS registers using stolen third-party credentials.

2. 2.
   Weak and default passwords: Verizon security experts found that Target had a password policy that was not enforced and therefore not followed by all employees. Consultants found files on multiple servers in the Target network that contained valid network credentials. Many systems were also using weak or default passwords, and the Verizon team gained access to these systems quickly. Default and weak passwords allowed the consultants to escalate their privilege to administrators, which allowed them to move freely around Target’s entire network. Within a week, security consultants cracked 86% of Target’s network credentials (472,308 of 547,470 passwords), and the Verizon team had almost full control of everything in Target. Figure 8-2 shows some of the top passwords Verizon cracked during their week at Target. Over 5% of the passwords were some version of the word Target, stores, train, or summer.

3. 3.
   Misconfigured services: Verizon experts also found that Target was using misconfigured Microsoft SQL servers and Apache Tomcat servers. The misconfigured servers initially allowed consultants to access the Target network. The default password on the servers was another way for consultants to escalate their privilege and gain control of the Target network. This is an additional network vulnerability that was not used by the attackers.

4. 4.
   Outdated software: Lastly, experts found that Target had not updated its server software for security patches. Just like we update our laptops or cell phones, servers receive updates that, in many cases, patch, or fix, security vulnerabilities found. Verizon consultants were able to exploit the known vulnerabilities in the old software and control Target’s network without any authentication credentials.



One to six characters = 83 (0.02%) **One to eight characters** = 224731 (47.59%) **More than eight characters** = 247536 (52.41%) **Single digit on the end** = 78157 (16.55%) **Two digits on the end** = 68562 (14.52%) **Three digits on the end** = 28532 (6.04%)	**Only lowercase alpha** = 141 (0.03%) **Only uppercase alpha** = 13 (0.0%) **Only alpha** = 154 (0.03%) **Only numeric** = 1 (0.0%) **First capital last symbol** = 60641 (12.84%) **First capital last number** = 95626 (20.25%)
Top 10 passwords	**Top 10 base words**
Jan3009# = 4312 (0.91%)	target = 8670 (1.84%)
sto$res1 = 3834 (0.81%)	sto$res = 4799 (1.02%)
train#5 = 3762 (0.8%)	train = 3804 (0.81%)
t@rget7 = 2260 (0.48%)	t@rget = 3286 (0.7%)
CrsMsg#1 = 1785 (0.38%)	summer = 3050 (0.65%)
NvrTeq#13 = 1350 (0.29%)	crsmsg = 1785 (0.38%)
Tar#76DSF = 1301 (0.28%)	winter = 1608 (0.34%)
summer#1 = 1174 (0.25%)	nvrteq = 1362 (0.29%)
R6c#VJm4 = 1006 (0.21%)	tar#76dsf = 1301 (0.28%)
Nov@2011 = 1003 (0.21%)	qwer = 1166 (0.25%)
Password length (length ordered)	**Password length (count ordered)**
3 = 1 (0.0%)	8 = 142924 (30.26%)
5 = 4 (0.0%)	9 = 105636 (22.37%)
6 = 78 (0.02%)	7 = 81724 (17.3%)
7 = 81724 (17.3%)	10 = 64633 (13.69%)
8 = 142924 (30.26%)	11 = 44264 (9.37%)
9 = 105636 (22.37%)	12 = 19229 (4.07%)
10 = 64633 (13.69%)	13 = 9524 (2.02%)
11 = 44264 (9.37%)	14 = 3874 (0.82%)

Figure 8-2

Many Target employees were using weak or default passwords, and this table shows statistics of the passwords Verizon auditors were able to crack

The Aftermath

After the dust settled, Target was held accountable for the breach and paid reparations to affected parties. Although Target was certified compliant with the Payment Card Industry Data Security Standard (PCI DSS) at the time of its breach, it clearly was not secure against breach and made it clear that compliance does not ensure security.[10] Being compliant with PCI DSS also did not protect Target from financial accountability from the card brands in the aftermath of the breach. Target paid credit card issuers for the cost of reissuing cards to customers. Visa alone received $67 million from Target as part of a settlement agreement. Target also settled a class action lawsuit for $10 million. Victimized customers could be paid up to $10,000 in damages. Brian Yarbrough, a consumer research analyst with Edward Jones estimates that the average settlement was between $50 and $100.[11]

All in all, it is estimated that the data breach cost Target over $250 million, even accounting for the $90 million Target received from its insurance claims. Target's sales for December 2013 fell 3–4%. Within six months of the breach, Target's CEO and CISO were fired and replaced with new leadership. This was the first mega-breach where the CEO and CISO were both fired. Security is an issue for which the CEO was ultimately held accountable. As such, security is not just an IT problem. It is an issue that spans across many departments at a company, and the buck stops at the CEO.

Target took significant steps to improve its security following the breach. Target mentioned in an online blog post that since the attack the company[12]:

- **Enhanced monitoring and logging**: Implemented additional rules and alerts, centralized log feeds, and enabled additional logging capabilities.
- **Installed application whitelisting for point-of-sale systems**, including deployment to all registers, point-of-sale servers, and development of whitelisting rules. Whitelisting allows access for certain programs to run. If a program is not whitelisted ahead of time, it does not get to run. Whitelisting would prevent a non-authorized RAM scraper or Citadel malware from running. Even if the malware is not detected by an anti-malware program, it will not get to run because it is not whitelisted.
- **Implemented enhanced segmentation**: Developed point-of-sale management tools, reviewed and streamlined network firewall rules, and developed a comprehensive firewall governance process.
- **Reviewed and limited vendor access**: Decommissioned vendor access to the server impacted in the breach and disabled select vendor access points, including FTP and telnet protocol.
- **Enhanced security of accounts**: Coordinated a reset of 445,000 Target team member and contractor passwords, broadened the use of two-factor authentication, expanded password vaults, disabled multiple vendor accounts, reduced privileges for certain accounts, and developed additional training related to password rotation.

In addition to the additional security measures, Target invested hundreds of millions of dollars into a new Cyber Fusion Center, Target's new security headquarters. After Target implemented its new security protocols, Verizon performed another audit and external penetration test in February 2014. Verizon security experts then found Target's network to be much more robust and less susceptible to data breaches.

The Hackers

Despite the shortcomings of Target's and Fazio Mechanical's security, it is important to remember that both companies and their affected customers were victims of a cybercrime. Target worked closely with federal law enforcement agencies, including the US Secret Service, and the US Department of Justice to track down the perpetrators of this criminal act. Federal agents found a lead in the malware code that points to one Ukrainian official named Andrey Khodyrevskiy. Federal agents found the alias "Rescator" embedded in the malware code and found the same alias writing posts on the online forum vor.cc for Russian hackers. Rescator says he also went by the nickname Helkern. Federal agents were then able to find details such as photos posted online, email addresses, and places of employment linked between Andrey Khodyrevskiy and Helkern. There is no definite proof Khodyrevskiy attacked Target, but the 22-year-old was arrested two years earlier by the Ukrainian security police for being caught in a separate hack. It is believed that Khodyrevskiy is just one of a group of hackers who victimized Target and Fazio Mechanical.

JPMorgan Chase: One of the Largest US Bank Breaches

Twelve months after the Target breach, JPMorgan Chase Bank (JPMC) discovered a breach in its network. Attackers compromised the personal information of over 76 million individual customers and 7 million business customers. Like Target, JPMC was, in part, compromised by a third party. At the time, JPMC was the largest American bank with $2.7 trillion in assets and had stringent security protocols to protect consumer accounts from theft or fraud. The remainder of this chapter will walk through how 83 million customers' PII were stolen from JPMC, despite the bank spending a quarter billion dollars on security annually.

The Annual Race

JPMC's breach started with the entity that organized the bank's annual charitable race. Since 2001, JPMC has hosted the JPMorgan Corporate Challenge across the world. Throughout the year in different cities, participants signed up to run or walk a 3.5-mile track with their colleagues. The revenue generated from the event was donated to local charities. In 2017 alone, the charitable event hosted a little less than 250,000 runners from over 7300 companies.

To sign up for this cause, participants registered on the JPMorgan Corporate Challenge website, hosted by Simmco Data Systems. Many of JPMC's employees participated in the annual race.

In April 2014, attackers compromised Simmco's website certificate.[13] With Simmco's website certificate compromised, hackers intercepted all traffic on the Corporate Challenge website, including the login credentials made by JPMorgan Chase employees. Unfortunately, many employees were using the same credentials for their corporate bank logins as they were using on the Simmco Corporate Challenge website.

Hold Security Identifies Stolen Credentials

Neither Simmco nor JPMC were aware of any breach in either system. Hold Security, a security firm based in Milwaukee, had uncovered an online repository of over one billion login credentials created by a group of Russian hackers. The repository credentials infiltrated more than 400,000 websites, including Simmco Data Systems. As Hold Security was sorting through the data, the firm contacted clients who were potentially breached. In early August 2014, Hold Security informed JPMC security consultants that the repository contained the usernames and passwords of participants of the Corporate Challenge in addition to the Simmco certificate. During this time, JPMC security consultants were aware that the bank's network was experiencing unusual network traffic.

JPMC Is Breached

For four months, between April 2014 and August 2014, attackers tested stolen credentials from the Simmco breach on numerous JPMC login portals. Prior to any attacker activities, JPMC performed a routine upgrade to its servers in which they had upgraded all the servers to require two-factor authentication.[14] Not all servers required two-factor authentication after the upgrade, though. Within the four months of the attacker's probing, JPMC found an outdated server that was not using two-factor authentication and used the stolen employee credentials to access JPMC's network. Attackers were tipped off that the credentials were valid when they unlocked access to an old server hosting employee benefits information. Attackers unfortunately only need to find one hole to get in, whereas information security defenders have the challenge of making sure as many holes as possible are closed.

The compromised servers contained the names, email addresses, addresses, and phone numbers of 83 million JPMC customers. JPMC stated that the breach was limited to personal information, and no financial information was compromised.

The Aftermath

JPMC's COO Matt Zames and CISO Greg Rattray led the investigation to trace the hackers' origins and attempt to identify the hackers who broke into the bank's network. The bank executives linked the Simmco website breach to 11 IP addresses overseas. The executives also found that those same IP addresses had been communicating with JPMC's network for months.

Furthermore, hackers deleted log files that would have tracked the attackers' movements through the bank's network, so it is unclear if even JPMC knows much about the hacker's movement through its network. After the breach, JPMC worked closely with the NSA and FBI to analyze the breach's extent and track down the attackers. JPMC closed all security loopholes concerning this breach. After the breach, JPMC CEO James Dimon committed to doubling the bank's security budget to half a billion dollars annually.

The Attackers

In 2015, law enforcement agencies were able to trace the JPMC breach to five hackers. Four of the hackers were identified and indicted for not only hacking JPMC but also E*Trade, Dow Jones, and Scottrade. Israeli and Russian nationals Gery Shalon, Andrei Tyurin, Joshua Samuel Aaron, and Ziv Orenstein have all been arrested and indicted on 23 counts, including but not limited to unauthorized access of computers, identity theft, securities and wire fraud, and money laundering. The indictment credits Shalon as the mastermind behind the group's illegal cyber activities. With the stolen data, including the JPMC data, the group scammed millions of people worldwide, earning hundreds of millions of dollars. The group's goal was to use the stolen data to start a brokerage firm set up as a copycat of the American brokerage firm Merrill Lynch.

Summary

Target was breached in 2013, exposing 40 million customer credit cards and 70 million customers' personal information. One year later, JPMorgan Chase Bank was breached, and hackers stole 83 million customers' personal information. The stolen credit card information from Target left customers susceptible to fraud, and the stolen personal information from JPMC left customers vulnerable to targeted phishing attacks. The following are the root causes and lessons learned from both of these breaches, in order of importance:

- **Third-party supplier compromise**: Target's network was initially breached because of a lack of third-party security. Hackers stole network credentials from Fazio Mechanical Services, and these stolen credentials gave attackers a foothold into Target's network. In the case of JPMC, Simmco Data Systems' website certificate was compromised, and hackers were able to intercept bank employees' recycled credentials. Third parties should be treated as an extension of an organization. Holding third parties to just as high a level of security as your own organization will help ensure that third parties do not become the weakest link in an organization's security.
- **Malware**: Hackers used malware in the attack against Target, both to infect user machines and steal credit card numbers out of the memory of PoS devices. Companies can invest in anti-virus software, and prioritize security, in addition to ensuring that the CISO and their team are adequately funded to protect against attacks and breaches. For instance, if the Target security team was resourced well, the team could have addressed all the security alerts generated. In addition, the team would be able to fine-tune its security tools to reduce the rate of false positives.
- **Inadvertent employee mistakes**: Weak passwords and passwords reused at multiple sites are a security vulnerability. Despite having a strong password policy, Target did not enforce this policy, and auditors easily cracked 86% of the company's network credentials. JPMC employees were using their corporate bank network credentials to create accounts on third-party websites like that of Simmco. Such recycled/reused passwords left the bank exposed. Having a strict and enforced password is an effective way to prevent credentials from being cracked. Two-factor authentication consistently deployed everywhere will also ensure security when sensitive credentials are stolen.

Footnotes

[1]
We cannot know for sure if the attack on Fazio Mechanical led attackers to victimize Target or whether Target was the initial mark. In the former case, attackers most likely cast a far and wide net when running an email malware scam to then see what victims look like promising leads. The second scenario is that attackers initially went after Target because it is a large retailer that had publicly exposed plenty of internal documentation.

[2]
Note that all of Target's public vendor pages have been taken down or are now privately hosted since the breach in 2013. Some of the URLs Target previously used are listed as follows. Spot a pattern?

[3]
Target's Supplier Portal: https://extpol.target.com/SupplierPortal/index.html

Target Facilities Management: https://extpol.target.com/SupplierPortal/facilitiesManagement.html

List of Target's Vendors: https://extpol.target.com/SupplierPortal/downloads.html

[4] Metadata is data that describes other data. For example, when you take a photo with your phone, the picture is saved along with metadata that includes the location where the photo was taken, the settings of the camera when the photo was taken, and the size and resolution of the photo. If you use Google Photos, you can see all this metadata by viewing the details of the photo. In the case of a Microsoft Excel file, metadata can include when the file was created, when it was last edited, and who last edited the file.

[5] An Active Directory is a live directory or database that stores information such as user accounts and other sensitive data. Active directory credentials would authenticate a user to access the said active directory.

[6] Aorato's analysis of the breach matches with details of the breach provided by Krebs on Security insider sources.

[7] Source: http://krebsonsecurity.com/wp-content/uploads/2014/01/POSWDS-ThreatExpert-Report.pdf

[8] Source: www.reuters.com/article/target-breach/target-says-it-declined-to-act-on-early-alert-of-cyber-breach-idINDEEA2C0LV20140313

[9] Source: https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

[10] https://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/#:~:text=Target%20and%20other%20breached%20entities,didn't%20stop%20their%20breaches

[11] Source: www.usatoday.com/story/money/2015/03/19/target-breach-settlement-details/25012949/

[12] Source: https://corporate.target.com/article/2014/04/updates-on-target-s-security-and-technology-enhanc

13
A website certificate verifies the identity of a website to its visitors. A valid website certificate also allows for a secure transfer of data between a website visitor and the website. Data is securely transferred using the HTTPS protocol, which you will see at the beginning of your URLs.

14
Two-factor authentication requires a user to authenticate themselves with not only their username and password but also a one-time second verification code. This could be a text message with a six-digit code or a notification on a trusted device that requires a user to click a button.