THE UNIVERSITY OF WINNIPEG

ACS-2821-001

Information Security in Business

Target Data Breach Post Mortem

DISCOVER • ACHIEVE • BELONG

Target Data Breach Post Mortem

Overview

- The attack started on November 27, 2013.
- Target personnel discovered the breach by December 13th and the U.S. Justice Department was notified
- December 15th, Target had a third-party forensic team in place and the attack mitigated
- December 18th, security blogger Brian Krebs broke the story that

  "Nationwide retail giant Target is investigating a data breach potentially involving millions of customer credit and debit card records“
- Target informed about 110 million credit/debit-card together with their personal and financial information had been compromised
- Amounting to 11 gigabytes of data were pilfered.

Target Data Breach Post Mortem

1. Preliminary survey

- Attackers performed reconnaissance on Target's network prior to the attack
- The reconnaissance would show how Target uses Microsoft virtualization software, centralized name resolution, and Microsoft System Center Configuration Manager to deploy security patches and system updates
- Additional clues show that a simple Google search turns up Target's Supplier Portal, which includes a wealth of information for new and existing vendors and how interact with the company
- Drilling down list show names of HVAC and refrigeration companies use by Target

Target Data Breach Post Mortem

2. Compromise third-party vendor

- The attackers backed their way into Target's corporate network by compromising a third-party vendor
- It was unknown how many vendors targeted but only took one. Fazio Mechanical, a refrigeration contractor.
- A phishing email was use to duped at least one Fazio employee
- Citadel, a variant of the Zeus banking Trojan installed on Fazio computers
- With Citadel in place waiting for Fazio Mechanical's login credentials
- All major versions of enterprise anti-malware detected the Citadel Malware at the time of the breach

Target Data Breach Post Mortem

2. Compromise third-party vendor cont.

- Unsubstantiated sources mentioned Fazio used the free version of Malwarebytes anti-malware that does not offered real-time protection being an on-demand scanner
- Note that Malwarebytes anti-malware is highly regarded by experts when used in the correct manner
- Chris Poulin, a research strategist for IBM, suggested that Target
- should have demanded all vendors accessing their systems use appropriate anti-malware software. Or at least mandate two-factor authentication to contractors who have internal access to sensitive information

Target Data Breach Post Mortem

3. Leveraging Target's vendor-portal access

- Citadel used login credentials for the portals used by Fazio Mechanical
- The attackers figuring out which portal to subvert and use as a staging point into Target's internal network.
- Target hasn't officially said which system was the entry point, but Ariba portal was a prime candidate.
- The Ariba portal at Target used Active Directory (AD) credentials
- and the vendor had AD credentials, but internal administrators would use their AD logins to access the system from inside
- This means the server had access to the rest of the corporate network in some form or another

Target Data Breach Post Mortem

3. Leveraging Target's vendor-portal access cont.

- The attackers may have abused a vulnerability in the web application, such as SQL injection, XSS, or possibly a 0-day, to gain a point of presence, escalate privileges, then attack internal systems
- If IPS/IDS systems were in place it may have sense the
- inappropriate attack traffic and notifying Target staff of the unusual behavior
- According to this Bloomberg Business article, a malware detection tool made by the computer security firm FireEye was in place and sent an alarm, but the warning went unheeded.

Target Data Breach Post Mortem

4. Gain control of Target servers

- Speculation has it that the criminals used the attack cycle described in Mandiant's APT1 report to find vulnerabilities on the Target’s network
- The malware move laterally through the network and other vulnerable systems using SQL-injection attacks

5. Next stop, Target's point of sale (POS) systems

- Trojan.POSRAM used to infect Target's POS system
- A RAM-scraping portion of the POS malware grabs credit/debit card information from the memory of POS-devices as cards are swiped
- Every seven hours the Trojan checks to see if the local time is between the hours of 10 AM and 5 PM, and will attempts to send winxml.dll over a temporary NetBIOS share to an internal host (dump server) inside the compromised network over TCP port 139, 443 or 80
- This allowed the attackers to steal data from POS terminals that lacked internet access

Target Data Breach Post Mortem

5. Next stop, Target's point of sale (POS) systems Cont.

- Once the credit/debit card information was secure on the dump server, the POS malware sent a special ICMP (ping) packet to a remote server
- The packet indicated that data resided on the dump server and the attackers can moved the stolen data to off-site FTP servers and sold their booty on the digital black market.

Lessons learned for Target from this data breach

- Target has improve security posture with the following:
  - Improved monitoring and logging of system activity
  - Installed application whitelisting POS systems and
  - Implemented POS management tools
  - Improved firewall rules and policies
  - Limited or disabled vendor access to their network
  - Disabled, reset, or reduced privileges on over 445,000 Target personnel and contractor accounts
  - Expanded the use of two-factor authentication and password vaults
  - Trained individuals on password rotation

Target Data Breach Post Mortem

Target Data Breach Timeline

- Nov. 27 - Dec. 15, 2013
  - Personal information, including names, mailing addresses and phone numbers, of 40 million customers who used credit and debit cards at U.S. stores are exposed to fraud.
- Dec. 13, 2013
  - Target executives meet with the U.S. Justice Department.
- Dec. 14, 2013
  - Target hires a third-party forensics team to investigate the hack.
- Dec. 15, 2013
  - Target confirms that criminals had infiltrated its system, installed malware on its point-of-sale network, and potentially stolen guest payment and credit card data.
  - Target removes malware from "virtually all" registers in U.S. stores. The public remains unaware of the data breach.

Target Data Breach Post Mortem

Target Data Breach Timeline cont.

- Dec. 18, 2013
  - Data and security blog KrebsOnSecurity first reports the data breach. The Secret Service investigates.
- Dec. 19, 2013
  - Target publicly acknowledges the breach, saying it's under investigation
  - Information accessed by attacker included credit and debit card numbers and card expiration dates, with no indication that PIN numbers were impacted, according to a spokesperson.
  - Customers jam Target's website and customer service hotlines
- Dec. 20, 2013
  - Target says very few credit cards compromised by the breach have resulted in fraud and offers U.S. customers a 10 percent discount off in-store purchases for the last weekend before Christmas.
  - The retailer also announces it has no indication that birth dates or Social Security numbers were accessed in the breach

Target Data Breach Timeline cont.

- Dec. 21, 2013
  - JPMorgan Chase & Co. (NYSE:JPM) places daily limits on spending and withdrawals for its debit card customers affected by the Target breach, begins reissuing cards and opens some branches on a Sunday to help Target customers.
- Dec. 22, 2013
  - Transactions at Target fell 3 percent to 4 percent compared to the year earlier on the last weekend of holiday shopping before Christmas. Other retailers report strong results.
- Dec. 23, 2013
  - Target's general counsel Tim Baer hosts a 30-minute conference call with state attorneys general as the company works with the U.S. Department of Justice, Secret Service and others.

Target Data Breach Timeline cont.

- Dec. 27, 2013
  - An ongoing investigation by a third-party forensics unit finds that encrypted debit card PIN information was accessed during the breach, but Target says it believes PIN numbers remain secure.
- Jan. 10, 2014
  - Target says an additional 70 million customers had personal information stolen during the breach, including emails.
  - The company lowered its forecast for its fourth quarter, saying sales were meaningfully weaker than expected after news of the breach.
- Jan. 22, 2014
  - Target lays off 475 employees at its headquarters in Minneapolis and worldwide and leaves another 700 positions unfilled.

Target Data Breach Timeline cont.

- Feb. 4, 2014
  - Target CFO John Mulligan testifies before the U.S. Senate Judiciary Committee, mentioning the ongoing investigation but offering no new information on who might have hacked the data.
  - Mulligan says Target has invested hundreds of millions in data security and rejects claims that its systems weren't up to par.
  - Other witnesses discuss the benefits of chip-and-PIN technology, used widely in Europe but not in the U.S., where banks and retailers have balked at the expense.
- Feb. 18, 2014
  - Costs associated with the data breach topped $200 million, a report from the Consumer Bankers Association and Credit Union National Association finds.
- Mar. 7, 2014
  - Target lets its employees wear jeans and polos to work in an effort to boost morale after layoffs and the saleskilling data breach.

Target Data Breach Post Mortem

Target Data Breach Timeline cont.

- April 30, 2014
  - Target says it has committed $100 million to update technology and will introduce chip-and-PIN technology for its debit and credit cards by early 2015.
- May 5, 2014
  - Bob DeRodes, a former tech adviser in several federal government agencies, takes over as Target's chief information officer. Target CEO Gregg Steinhafel resigns.

ACS-2821-001 – Questions?