Incident Summary

Target Corp Data Breach

What we, the Industry, know (or think we know)

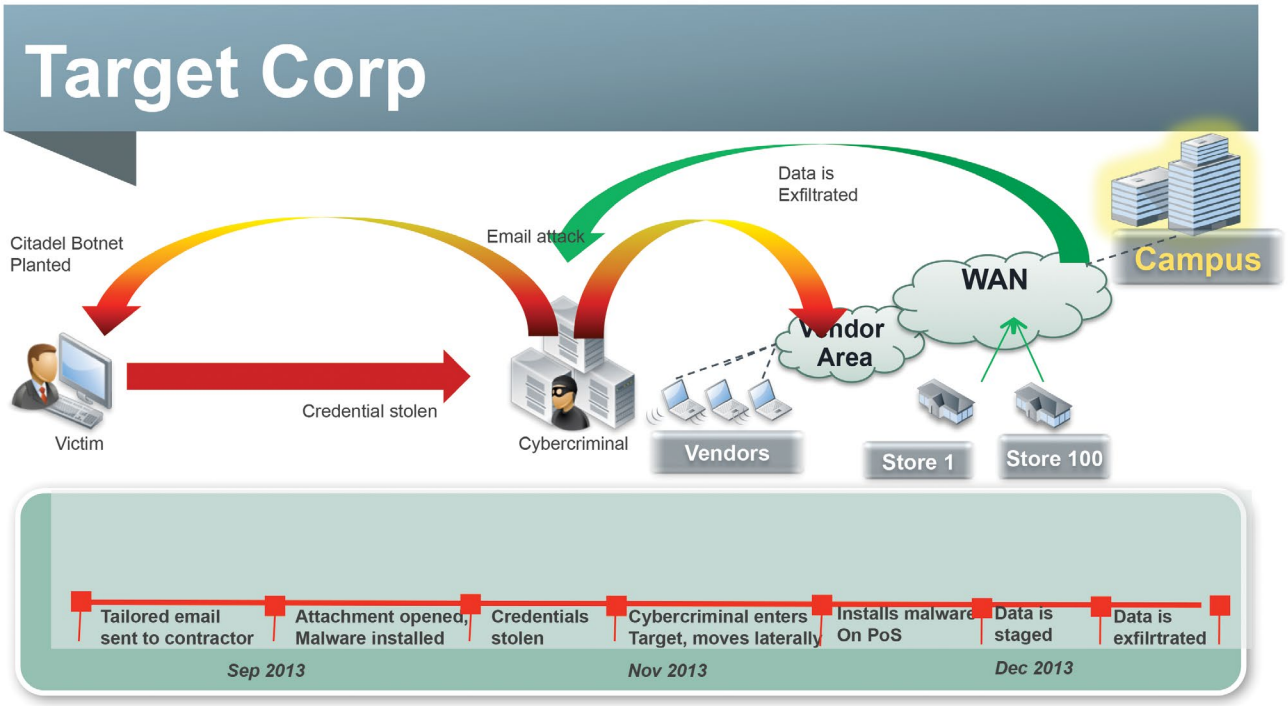
Around September, a Target Corp Contractor (Fazio Mechanical, HVAC), was infiltrated using email borne malware (Citadel Trojan) and credentials used to access Target's online billing system were stolen. While Fazio cites security "in full compliance with industry practices" it seems that their primary antimalware software was the free version of malwarebytes. Also, it is reported that the system used to access the Target Corporation network did not use Strong (two-factor) Authentication.

From that point, it is believed that access to the Target network allowed them to move laterally access PoS systems and install subsequent malware. The exact method and sequence is unclear at this time.

Note: early reports suspected that a web server had been compromised for the initial entry and/or later that a systems management server (from BMC) had been leveraged to gain access to the PoS, but that is now believed not to be the case.

Once access to PoS systems was gained, a RAM scaper – or software that captures encrypted data when it appears in clear text within system memory – was installed. The malware seeks out Track 1 and Track 2 data stored on the magnetic strip of a card, which together contain the cardholder's name, account number, credit card number and expiry date. It is believed that a variant of BlackPOS, sold on the black market and subsequently modified to bypass AV detection, was installed on the systems.

From late November 27th to December 15th, the malware captured the cardholder data but still need to find a way to deliver it outside the company. Reports suggest data was staged within Target starting 6 days later (December 3rd) and exfiltrated using another compromised system within the target network to an FTP server. It is further suspected that it would only transmit the information in smaller batches, 3 times a day within normal business hours. Lastly, the receiving FTP server is believed to have been part of another legitimate but compromised party where it could ultimately be downloaded by Cybercriminals via a virtual private server.



And at some point, in addition to the credit card information of shoppers during the holiday period, the Cybercriminals also gained access to personal information about others in the company databases.

All of this data is believed to be flooding the black market as the initial thieves look to monetize their haul.

The Impact

All told, reports indicate that 40 million credit and debit card records, as well as personal information for 70 million others was stolen. It is believed that this was not an isolated incident, but may have been tied to 6 other retail breaches around the same period. However it is possible that the other incidents, while similar, may not be linked.

In addition to the data loss and required notification, Target Corp now has to deal with consumer class action lawsuits, as well as those from financial institutions who issued cards whose data was among the breach. Further, Target Corp execs have spent time dealing with the press and even Congress. In fact, in March of 2014 the CIO resigned at the same time that the information security and compliance group was being overhauled.

Longer-term, Target Corp has indicated they plan to move to new "chip and P.I.N" cards in the U.S. which will certainly carry a cost. Although that plan seems to have been underway, it is being accelerated and may include unforeseen costs.

Whether the industry as a whole moves to the new system, near term card issuers have to bear the cost of reissuing 40m new credit and debit cards, currently estimated at $200m. But some believe, for now, that fraud monitoring systems of their own limit their risk and cost.

While most consumers are believed to be protected, as fraudulent use of their card information is usually the responsibility of the card issuer, there are some initial and potentially longer term impacts. For example, some of the cards stolen and being replaced were used to provide unemployment benefits, which are delayed until new cards arrive. Further, identity theft beyond the card data (specifically if any of the 70 million records are used to establish phony accounts) can be more difficult to unravel should it occur. And while credit monitoring service is generally provided for 1 year following a breach like this we don't have enough history yet to tell us what may occur 12-18 months later.

Reducing Your Risk

While most companies are probably protected by now from this specific malware, going forward there are a number of security measures to consider (many may already be in place but it's a good idea to be sure) in order to reduce the risk of compromise from targeted attacks of this type.

At the highest level, there were two aspects to this breach- compromise of a vendor and then compromise of Target Corporate itself. This suggests a broader scope for security considerations.

First, even though it can be challenging, continued effort must be made to ensure appropriate security of vendors/ partners/contractors are in place. You are only as strong as your weakest link.

- Insist on industry standard security practices including commercial endpoint, email and web security. Single vendor suites and/or consolidated network security appliances make this viable even for smaller organizations.) Consider this as a vendor selection criteria or at least a contractual obligation that can be audited. *In this case, an email security solution that could "sandbox" the malicious attachment may have stopped the vendor compromise and identity theft, closing off that avenue into Target.*

- Require "strong" (two-factor) authentication for vendors to reduce risk in the event their credentials are stolen. *In this case, requiring dynamic, one-time authentication methods may have prevented Cybercriminals from leveraging the stolen credentials to gain access.*

- Ensure limited vendor access with proper firewall segmentation and inspection of traffic (Intrusion Prevention and Antimalware at a minimum, some form of Advanced Threat Protection- sandboxing, network monitoring, etc. – if you can) between the vendor area and the remainder of your network. *In this case, deeper inspection of traffic between vendor accessible area and PoS systems may have detected and/or prevented the access or installation of malware on the PoS systems. In particular, sandboxing of the malware may have identified the compromise before weeks passed and millions of records were stolen.*

Cybercriminal Action	Security Measures to Consider
Email with malware attached	Sandboxing of attachments
Credentials captured	Enterprise class content security suite
Credentials exfiltrated	Any layer of DLP
Stolen credentials used for access	Strong authentication
Lateral movement to PoS and delivery of malware	Additional inspection (IPS, AV, Sandboxing)
Install and run malware on PoS	Application control, behavior monitoring
Move captured data to staging server	DLP, at least for structured data
Exfiltrate data	DLP and/or Network Behavioral Analysis
Other considerations	WAF, IPS and vulnerability management

Second, within your organization, beyond the segmentation noted above, also consider the following:

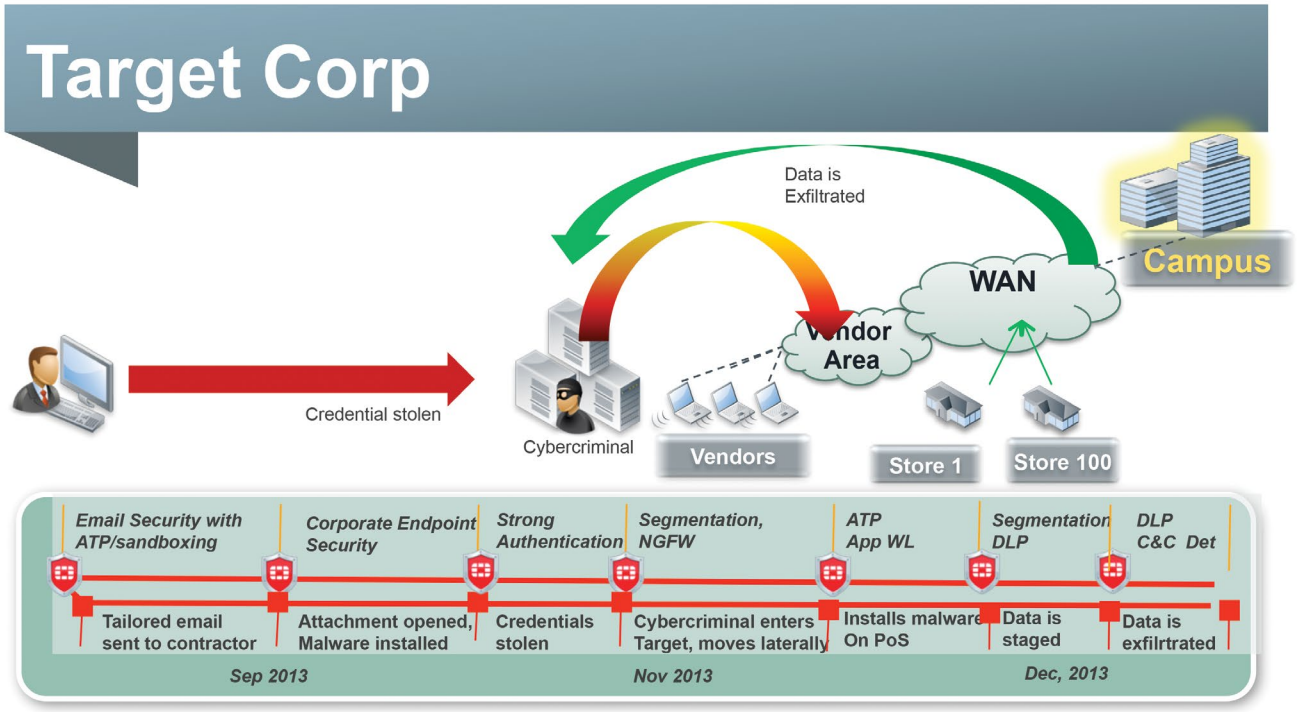
- Segment systems containing sensitive information not just from 3rd party accessible areas but also as much as you can from externally accessible systems. Ensure deeper inspection- intrusion prevention, antimalware, data loss prevention and advanced threat protection- of traffic in and out of that sensitive area.
  In this case, walling off PoS systems as much as possible both from the area accessed by the vendor credentials as well as from systems capable of transmitting the data externally may have helped, but if nothing else, sandboxing to examine the activity of code passing into the segmented area and ultimately being installed on the PoS system would have had the greatest chance to detect the modified malware early on.

- If you are able to put additional control- antimalware, application control, behavior monitoring or other controls- on those systems containing sensitive information, great.
  Also, efforts to monitor and/or lock down the PoS systems/configurations may have also helped prevent or at least detect the installation of malware.

- Given that the attack is only successfully if the data is exfiltrated, consider data loss prevention technologies for outgoing traffic.
  While DLP can be a large project to undertake when trying to protect the wide range of structured (ie. credit card numbers whose numbering follows a well-defined pattern) and unstructured (ie. intellectual property which can take a wide range of forms) data in an enterprise, detecting structured data is a reasonably mature (if not so widely deployed) capability in many endpoint, email and web security products. In this case, checking outgoing traffic (if not encrypted) for structured data of credit and debit card numbers may have prevented the most harmful aspect of the data breach.

- Make sure that your own defenses against initial compromise are strong, including proper email security with ATP, web security and endpoint protection, as well as vulnerability management and WAF.
  Although the initial network intrusion in this case stemmed from a third party who was granted access, in many cases the intrusion (and possibly the lateral movement in this case) results from the exploit of an unpatched or unknown vulnerability. Vulnerability management and web application firewalls for web servers (in addition to IPS systems that offer virtual patching for all servers) can help reduce the risk of intrusion.

- Recognize that a breach can still happen and implement ATP such as payload and/or network anomaly detection technologies.
  Gartner has outlined 5 "styles" of advanced threat defense that have emerged in response to the rise of targeted attacks that are tailored to beat established defenses. These include network anomaly detection and forensics, endpoint behavior analysis and forensics plus payload analysis (aka sandboxing). Organizations should consider one or more of these messages for early detection and/or faster remediation in the event of a breach. tIn this case, the ability to detect and assess the previously unknown malware post installation but pre-exfiltration (something that occurred a week after the initial compromise of Target and months after the compromise of the vendor) may have reduced the scope of the breach dramatically.



Of course it is understood that all the measures above would be expensive and time consuming, without a 100% guarantee to prevent a breach, so first look at which controls are already deployed (and make sure they are deployed properly). Then consider what may be licensed but not yet deployed, or available from an existing vendor for a small/modest additional charge. After that explore additional technologies, especially for ATP, to complement what you already have in place.

Of note, most firewall vendors will also offer full stack next generation firewall capabilities of IPS, Application Control, AV, and even ATP and DLP, providing a quick and affordable way to put many of these protections in place internally and at the edge. Further, email security solutions with strong embedded URL inspection and sandboxing capability are quite common, so look to those vendors for easy extension of capability. In some vendor cases, it is even possible to select all of these components, including WAF and Strong Authentication, for those looking to make a single volume purchase due to tight budgets and/or a single centrally managed solution given small IT/Security teams. Regardless of who you buy from, raising security in each of these areas will reduce your risk of a breach. Each organization's risk tolerance, budget and staffing will dictate which measures make sense.

For Fortinet Customers

Fortinet customers have received updates to their antimalware, IPS and other threat prevention products. Fortinet's new FortiSandbox offering can also help detect sophisticated attacks that bypass traditional security measures. Finally, Fortinet recommends that organizations take a coordinated approach to addressing the challenge posed by sophisticated attacks and has introduced a cohesive Advanced Threat Protection Framework. More information on that framework can be found here – http://www.fortinet.com/solutions/advanced-threat-protection.html.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480