UNITED STATES SENATE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION

A "Kill Chain" Analysis of the 2013 Target Data Breach

MAJORITY STAFF REPORT FOR CHAIRMAN ROCKEFELLER
MARCH 26, 2014

Executive Summary

In November and December 2013, cyber thieves executed a successful cyber attack against Target, one of the largest retail companies in the United States. The attackers surreptitiously gained access to Target's computer network, stole the financial and personal information of as many as 110 million Target customers, and then removed this sensitive information from Target's network to a server in Eastern Europe.

This report presents an explanation of how the Target breach occurred, based on media reports and expert analyses that have been published since Target publicly acknowledged this breach on December 19, 2013. Although the complete story of how this breach took place may not be known until Target completes its forensic examination of the breach, facts already available in the public record provide a great deal of useful information about the attackers' methods and Target's defenses.

This report analyzes what has been reported to date about the Target data breach, using the "intrusion kill chain" framework, an analytical tool introduced by Lockheed Martin security researchers in 2011, and today widely used by information security professionals in both the public and the private sectors. This analysis suggests that Target missed a number of opportunities along the kill chain to stop the attackers and prevent the massive data breach. Key points at which Target apparently failed to detect and stop the attack include, but are not limited to, the following:

- Target gave network access to a third-party vendor, a small Pennsylvania HVAC company, which did not appear to follow broadly accepted information security practices. The vendor's weak security allowed the attackers to gain a foothold in Target's network.

- Target appears to have failed to respond to multiple automated warnings from the company's anti-intrusion software that the attackers were installing malware on Target's system.

- Attackers who infiltrated Target's network with a vendor credential appear to have successfully moved from less sensitive areas of Target's network to areas storing consumer data, suggesting that Target failed to properly isolate its most sensitive network assets.

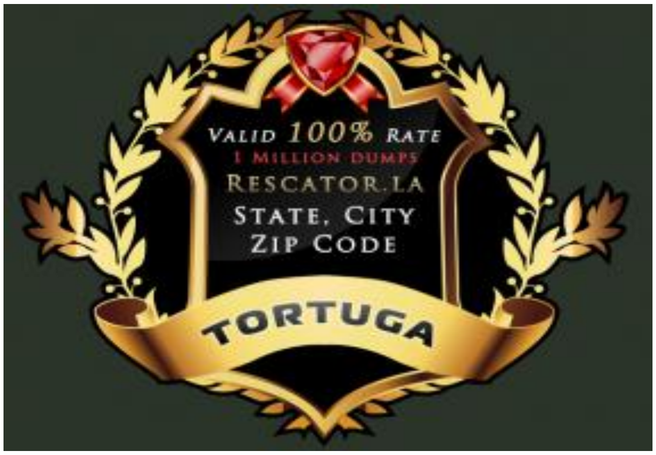
- Target appears to have failed to respond to multiple warnings from the company's anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target's network.

A. The Target Data Breach

1. The Stolen Data

On December 19, 2013, Target publicly confirmed that some 40 million credit and debit card accounts were exposed in a breach of its network.[1] The Target press release was published after the breach was first reported on December 18 by Brian Krebs, an independent Internet security news and investigative reporter.[2] Target officials have testified before Congress that they were not aware of the breach until contacted by the Department of Justice on December 12.[3] The data breach affected cards used in U.S. Target stores between November 27 and December 18, 2013.[4]

Figure 1 - Advertisement for Stolen Target Cards



Source: Krebsonsecurity.com

Thieves were able to sell information from these cards via online black market forums known as "card shops."[5] These websites list card information including the card type, expiration date, track data (account information stored on a card's magnetic stripe), country of origin, issuing bank, and successful use rate for card batches over time. The newer the batch, the higher the price, as issuing banks often have not had sufficient time to identify and cancel compromised

[1] Target, *Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores* (Dec. 19, 2013) (online at http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores).

[2] Brian Krebs, *Sources: Target Investigating Data Breach*, KrebsOnSecurity (Dec. 18, 2013) (online at http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/).

[3] Testimony of John Mulligan, Target Executive Vice President and Chief Financial Officer, before the Senate Committee on the Judiciary, at 2 (Feb. 4, 2014) (online at http://www.judiciary.senate.gov/pdf/02-04-14MulliganTestimony.pdf).

[4] *Id*. at 2-3.

[5] Brian Krebs, *Cards Stolen in Target Breach Flood Underground Markets* (Dec. 20, 2013) (online at http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/).

cards. A seller, nicknamed "Rescator," at a notorious card shop even offered a money-back guarantee for immediately cancelled cards.[6] Those purchasing the information can then create and use counterfeit cards with the track data and PIN numbers[7] stolen from credit and debit card magnetic stripes. Fraudsters often use these cards to purchase high-dollar items and fence them for cash, and if PIN numbers are available, a thief can extract a victim's money directly from an ATM. Based on a reading of underground forums, hackers may be attempting to decrypt the stolen Target PIN numbers.[8]

On January 10, 2014, Target disclosed that non-financial personal information, including names, addresses, phone numbers, and email addresses, for up to 70 million customers was also stolen during the data breach.[9]

2. The Attack

On January 12, Target CEO Gregg Steinhafel confirmed that malware installed on point of sale (POS) terminals[10] at U.S.-based Target stores enabled the theft of financial information from 40 million credit and debit cards.[11] This malware utilized a so-called "RAM scraping" attack, which allowed for the collection of unencrypted, plaintext data as it passed through the infected POS machine's memory before transfer to the company's payment processing provider. According to reports by Brian Krebs, a tailored version of the "BlackPOS" malware – available on black market cyber crime forums for between $1,800 and $2,300 – was installed on Target's POS machines.[12] This malware has been described by McAfee Director of Threat Intelligence Operations as "absolutely unsophisticated and uninteresting."[13] This assessment is in contrast

[6] *Id*.

[7] Target initially denied that debit card PIN numbers had been stolen, but reports confirmed that encrypted PIN numbers had indeed been stolen. *See* Jim Finkle and David Henry, *Exclusive: Target Hackers Stole Encrypted Bank PINs – Source*, Reuters (Dec. 25, 2013) (online at http://www.reuters.com/article/2013/12/25/us-target-databreach-idUSBRE9BN0L220131225).

[8] Adam Greenberg, *Hackers Seek to Decrypt PIN Codes Likely Stolen in Target Breach*, SC Magazine (Jan. 8, 2014) (online at http://www.scmagazine.com/hackers-seek-to-decrypt-pin-codes-likely-stolen-in-target-breach/article/328529/).

[9] Target, *Target Provides Update on Data Breach and Financial Performance* (Jan. 10, 2014) (online at http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance).

[10] A Point of Sale (POS) terminal is a physical device used by a merchant to process payments for goods and services purchased by a customer. Customized hardware and software is often used at a POS terminal, or cash register, part of which is used to swipe and process credit and debit card information.

[11] Becky Quick, *Target CEO Defends 4-Day Wait to Disclose Massive Data Hack*, CNBC (Jan. 12, 2014) (online at http://www.cnbc.com/id/101329300).

[12] Brian Krebs, *A First Look at the Target Intrusion, Malware*, KrebsOnSecurity (Jan. 15, 2014) (online at http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/).

[13] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg Businessweek (Mar. 13, 2014) (online at http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data).

with the statement of Lawrence Zelvin, Director of the Department of Homeland Security's National Cybersecurity and Communications Integration Center, who describes the malware used in the attack as "incredibly sophisticated."[14]

According to unnamed investigators, the attackers first installed their malware on a small number of POS terminals between November 15 and November 28, with the majority of Target's POS system infected by November 30.[15] A report by *The New York Times* states that the attackers first gained access to Target's internal network on November 12.[16]

A Dell SecureWorks report shows that the attackers also installed malware, designed to move stolen data through Target's network and the company's firewall, on a Target server.[17] The Dell SecureWorks team was able to analyze a sample of the actual malware used in the Target attack. The attackers reportedly first installed three variants of this malware on November 30 and updated it twice more, just before midnight on December 2 and just after midnight on December 3.[18] According to a *Bloomberg Businessweek* report, Target's FireEye malware intrusion detection system triggered urgent alerts with each installation of the data exfiltration malware.[19] However, Target's security team neither reacted to the alarms nor allowed the FireEye software to automatically delete the malware in question. Target's Symantec antivirus software also detected malicious behavior around November 28, implicating the same server flagged by FireEye's software.[20]

According to Seculert, a security company focused on advanced cyber threats, the malware started to send the stolen data to an external file transfer protocol (FTP) server via another compromised Target server on December 2, 2013.[21] Over the next two weeks, the

[14] House Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, *Protecting Consumer Information: Can Data Breaches Be Prevented?,* 113th Cong. (Feb. 5, 2014).

[15] Brian Krebs, *Target Hackers Broke in Via HVAC Company*, KrebsOnSecurity (Feb. 5, 2014) (online at http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/).

[16] Elizabeth A. Harris, Nicole Perlroth, Nathaniel Popper, and Hilary Stout, *A Sneaky Path Into Target Customers' Wallets* (Jan. 17, 2014) (online at http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html).

[17] A third type of malware was installed on intermediate servers which presumably stored stolen data inside Target's network before the next exfiltration step. However, this malware has thus far not been analyzed publicly. *See* Keith Jarvis and Jason Milletary, *Inside a Targeted Point-of-Sale Data Breach*, Dell SecureWorks, at 5 (Jan. 24, 2014) (online at http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf).

[18] *Id*.

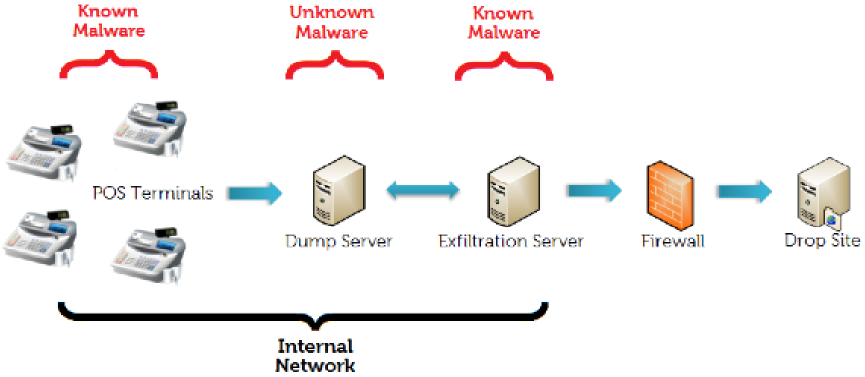
[19] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg Businessweek (Mar. 13, 2014) (online at http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data).

[20] *Id*.

[21] Aviv Raff, *PoS Malware Targeted Target*, Seculert (Jan. 16, 2014) (online at http://www.seculert.com/blog/2014/01/pos-malware-targeted-target.html).

attackers collected 11 GB of stolen information using a Russia-based server.[22] Analysis of the malware by Dell SecureWorks found that the attackers exfiltrated data between 10:00 a.m. and 6:00 p.m. Central Standard Time, presumably to obscure their work during Target's busier shopping hours.[23] Other sources describe a variety of external data drop locations, including compromised servers in Miami and Brazil.[24] The 70 million records of non-financial data were included in this theft, but public reports do not make clear how the attackers accessed this separate data set.

Figure 2 - Diagram of Data Exfiltration



Source: Dell SecureWorks

The attackers reportedly first gained access to Target's system by stealing credentials from an HVAC and refrigeration company, Fazio Mechanical Services, based in Sharpsburg, Pennsylvania.[25] This company specializes as a refrigeration contractor for supermarkets in the mid-Atlantic region[26] and had remote access to Target's network for electronic billing, contract submission, and project management purposes.[27]

Reports indicate that at least two months before the Target data breach began, attackers stole Fazio Mechanical's credentials for accessing Target's network via emails infected with

[22] *Id.*

[23] Keith Jarvis and Jason Milletary, *Inside a Targeted Point-of-Sale Data Breach*, Dell SecureWorks, at 6, 11 (Jan. 24, 2014) (online at http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf).

[24] Brian Krebs, *Target Hackers Broke in Via HVAC Company*, KrebsOnSecurity (Feb. 5, 2014) (online at http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/).

[25] *Id.*

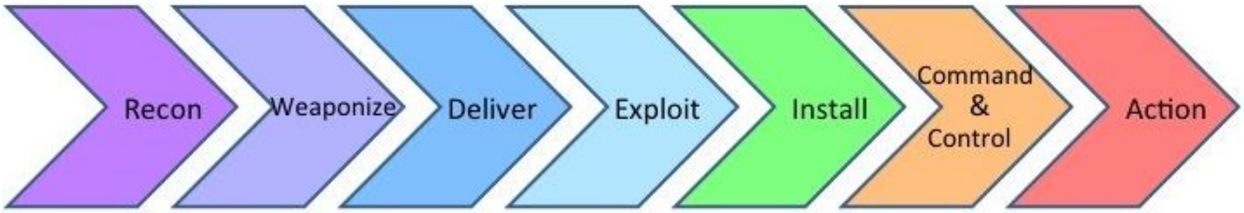
[26] Fazio Mechanical Services, *About Us* (accessed Mar. 12, 2014) (online at http://faziomechanical.com/about-us.html).

[27] Fazio Mechanical Services, *Statement on Target Data Breach* (accessed Mar. 12, 2014) (online at http://faziomechanical.com/Target-Breach-Statement.pdf).

malware.[28] According to a former Target security team member, Fazio would more than likely have had access to Target's Ariba external billing system;[29] however, reports do not make clear how the attackers gained access to Target's POS terminals from this initial foothold on the edge of Target's network. According to the same source, it is likely the outside portal was not fully isolated from the rest of Target's network.[30] Once inside, the attackers may have exploited a default account name used by an IT management software product by BMC Software to move within Target's network.[31] The attackers also disguised their data exfiltration malware as a legitimate BMC Software product.[32]

B. The Kill Chain

Figure 3 – Diagram of the Intrusion Kill Chain



Source: Lockheed Martin

1. The "Kill Chain" as a Cybersecurity Defense Tool

The conventional model of information security relies on static defense (e.g. intrusion detection systems and antivirus software) and assumes that attackers have an inherent advantage over defenders given ever-shifting technologies and undiscovered software vulnerabilities. In 2011, the Lockheed Martin Computer Incident Response Team staff published a white paper explaining how these conventional defenses were not sufficient to protect organizations from sophisticated "advanced persistent threats" (APTs).[33] The paper proposed an "intelligence-

[28] Sources have identified malware known as "Citadel," which steals passwords on compromised machines. However, this has not been confirmed. *See* Brian Krebs, *Email Attack on Vendor Set Up Breach at Target*, KrebsOnSecurity (Feb. 12, 2014) (online at http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/).

[29] *Id*.

[30] *Id*.

[31] Brian Krebs, *New Clues in the Target Breach*, KrebsOnSecurity (Jan. 29, 2014) (online at http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/).

[32] Keith Jarvis and Jason Milletary, *Inside a Targeted Point-of-Sale Data Breach*, Dell SecureWorks, at 6 (Jan. 24, 2014) (online at http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf).

[33] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lockheed Martin (2011) (online at http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf).

driven, threat-focused approach to study intrusions from the adversaries' perspective" that could give network defenders the upper hand in fighting cyber attackers.[34]

Instead of installing static defense tools and waiting for the next attack, the paper argued, network defenders should continuously monitor their systems for evidence that attackers are trying to gain access to their systems. Any intrusion attempt reveals important information about an attacker's tactics and methodology. Defenders can use the intelligence they gather about an attacker's playbook to "anticipate and mitigate future intrusions based on knowledge of the threat."[35] When a defender analyzes the actions of attackers, finds patterns, and musters resources to address capability gaps, "it raises the costs an adversary must expend to achieve their objectives . . . [and] such aggressors have no inherent advantage over defenders."[36]

To illustrate how network defenders can act on their knowledge of their adversaries' tactics, the paper lays out the multiple steps an attacker must proceed through to plan and execute an attack. These steps are the "kill chain." While the attacker must complete all of these steps to execute a successful attack, the defender only has to stop the attacker from completing any one of these steps to thwart the attack.

Analyzing past attacks, utilizing threat intelligence, and improving defenses at all phases of the kill chain allow a defender to detect and deny future attacks earlier and earlier in the kill chain. This requires constant vigilance, but it can theoretically defend against even APTs using so-called "zero-day" exploits, which utilize previously unknown vulnerabilities and attack signatures that defense tools cannot detect.[37]

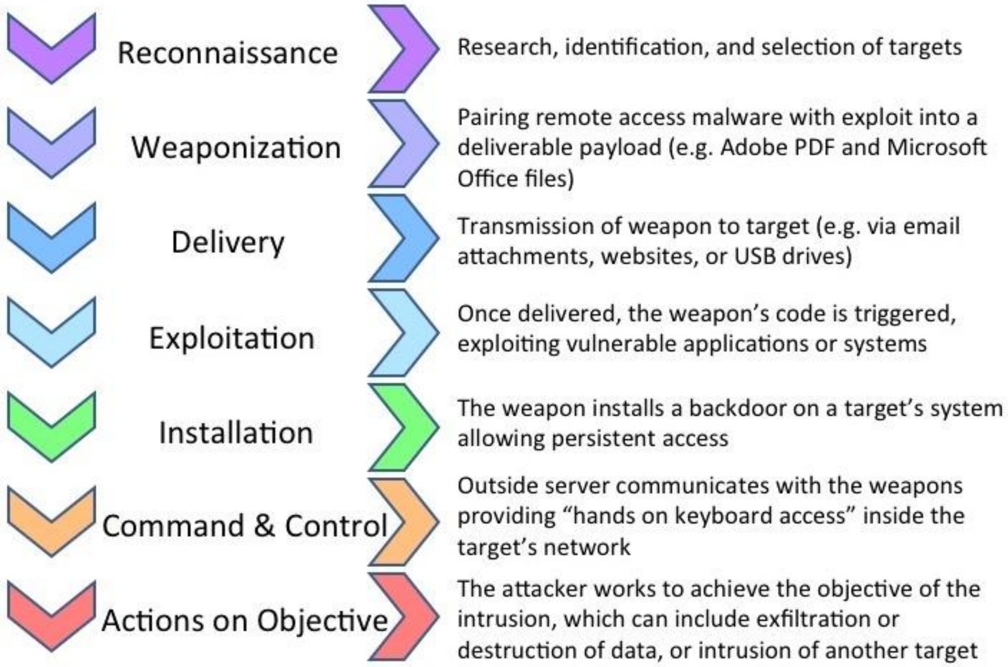
[34] *Id*. at 2.

[35] *Id*.

[36] *Id*. at 3.

[37] *Id*. at 4-5.

Figure 4 – Phases of the Intrusion Kill Chain



Reconnaissance – Research, identification, and selection of targets

Weaponization – Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

Delivery – Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

Exploitation – Once delivered, the weapon’s code is triggered, exploiting vulnerable applications or systems

Installation – The weapon installs a backdoor on a target’s system allowing persistent access

Command & Control – Outside server communicates with the weapons providing “hands on keyboard access” inside the target’s network

Actions on Objective – The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Source: Lockheed Martin

2. Analysis of the Target Data Breach Using the Kill Chain

John Mulligan, Target’s Executive Vice President and Chief Financial Officer, testified that his company “had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection and prevention capabilities and data loss prevention tools.”[38] He further stated that Target had been certified in September 2013 as compliant with the Payment Card Industry Data Security Standards (PCI-DSS),[39] which credit card companies require before allowing merchants to process credit and debit card payments.

These steps were obviously not sufficient to prevent the breach. Based on public information about Target’s breach reviewed in the previous section, this section walks through the steps of the kill chain and analyzes what actions Target and its contractor, Fazio Mechanical Services, did or did not take to defend themselves.

A. Reconnaissance – Attacker Quietly Gathers Information About Victim

As discussed above, the attacker may have sent malware-laden emails to Fazio at least two months before the Target data breach began. According to analysis by Brian Krebs, the attacker may have found information on Target’s third-party vendors through simple Internet searches, which, at the time of his writing, displayed Target’s supplier portal and facilities

[38] Testimony of John Mulligan, Target Executive Vice President and Chief Financial Officer, before the Senate Committee on the Judiciary, at 4-5 (Feb. 4, 2014) (online at http://www.judiciary.senate.gov/pdf/02-04-14MulliganTestimony.pdf).

[39] *Id*. at 5.

management pages.[40] Files available on these sites provided information for HVAC vendors and, through a metadata analysis, allowed the attacker to map Target's internal network prior to the breach. To disrupt this step in the kill chain, Target could have limited the amount of publicly available vendor information. Target could have also shared threat information with its suppliers and vendors and encouraged collaboration on security within the community.

B. Weaponization – Attacker Prepares Attack Payload to Deliver to Victim

While unconfirmed, the attacker likely weaponized its malware targeting Fazio in an email attachment, likely a PDF or Microsoft Office document. Fazio could have disrupted this step in the kill chain through the use of broadly accepted real-time monitoring and anti-malware software. However, according to investigators familiar with the case, Fazio used the free version of Malwarebytes Anti-Malware, which does not provide real-time protection and is intended only for individual consumer use.[41]

C. Delivery – Attacker Sends Payload to Victim

The attacker sent infected emails to Fazio in a so-called phishing attack. Phishing, or "spear phishing," when an attacker customizes email messages using social engineering techniques (e.g. checking Facebook or LinkedIn for a potential victim's business associates and relationships), is a well-known attack method. Fazio could have disrupted this step in the kill chain by training its staff to recognize and report phishing emails. Real-time monitoring and anti-malware software could have also potentially detected the infected file(s).

While reports are unconfirmed, the malware on Fazio's systems may have recorded passwords and provided the attackers with their key to Target's Ariba external billing system. In this phase of the kill chain, Target could have potentially disrupted the attack by requiring two-factor authentication for its vendors. Two-factor authentication includes a regular password system augmented by a second step, such as providing a code sent to the vendor's mobile phone or answering extra security questions. According to a former Target vendor manager, Target rarely required two-factor authentication from its low-level contractors.[42] PCI-DSS require two-factor authentication for remote access to payment networks and access controls for all users,[43] although the Ariba system is not technically related to Target's POS system.

However the attackers actually leveraged their access to this vendor's system to enter Target's network, less security at the perimeter of Target's network may have contributed to the attackers' success in breaching the most sensitive area of Target's network containing cardholder

[40] Brian Krebs, *Email Attack on Vendor Set Up Breach at Target*, KrebsOnSecurity (Feb. 12, 2014) (online at http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/).

[41] *Id*.

[42] *Id*.

[43] Standard 7.2 and 8.3 are most relevant to this discussion. Version 3.0 of the standard was released in November 2013, after the Target breach. As such, this report references the previous version 2.0. *See* Payment Card Industry Security Standards Council, *Payment Card Industry (PCI) Data Security Standard Version 2.0*, at 44, 47 (Oct. 2010) (online at https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf).

data. Using the Fazio credentials to gain access to Target's inner network, it appears the attackers then directly uploaded their RAM scraping malware to POS terminals.

D. Exploitation – Attackers Payload Deployed in Victim's Network

Once delivered, the RAM scraping malware and exfiltration malware began recording millions of card swipes and storing the stolen data for later exfiltration. Target could have potentially blocked the effect of the exfiltration malware on its servers by either allowing its FireEye software to delete any detected malware, or, if not choosing the automatic option, by following up on the several alerts that were triggered at the time of malware delivery. According to *Businessweek*, the FireEye software sent an alert with the generic name "malware.binary" to Target security staff.[44] It is possible that Target staff could have viewed this alert as a false positive if the system was frequently alarming.

Another protective step could have been paying greater attention to industry and government intelligence analyses. According to an FBI industry notification, RAM scraping malware has been observed since 2011.[45] Furthermore, a *Reuters* report stated that Visa published in April and August of 2013 two warnings about the use of RAM scraping malware in attacks targeting retailers.[46] These warnings apparently included recommendations for reducing the risk of a successful attack. According to the *Wall Street Journal*, Target's security staff made their misgivings known about vulnerabilities on the company's POS system; however, it is unclear if Target took any action to address vulnerabilities before the attack.[47]

E. Installation – Attacker Establishes Foothold in Victim's Network

Reports suggest that the attacker maintained access to Fazio's systems for some time while attempting to further breach Target's network. It is unclear exactly how the attacker could have escalated its access from the Ariba external billing system to deeper layers of Target's internal network. But given the installation of the BlackPOS malware on Target's POS terminals, the compromise of 70 million records of non-financial data, and the compromise of the internal Target servers used to gather stolen data, it appears that the attackers succeeded in moving through various key Target systems.

[44] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg Businessweek (Mar. 13, 2014) (online at http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data).

[45] FBI Cyber Division, *Recent Cyber Intrusion Events Directed Toward Retail Firms* (Jan. 17, 2014) (online at http://krebsonsecurity.com/wp-content/uploads/2014/01/FBI-CYD-PIN-140117-001.pdf).

[46] Jim Finkle and Mark Hosenball, *Exclusive: More Well-Known U.S. Retailers Victims of Cyber Attacks – Sources*, Reuters (Jan 12, 2014) (online at http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112).

[47] Danny Yadron, Paul Ziobro, Devlin Barrett, *Target Warned of Vulnerabilities Before Data Breach*, The Wall Street Journal (Feb. 14, 2014) (online at http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690).

Brian Krebs and Dell SecureWorks posit that the attackers may have exploited a default account name used in a BMC Software information technology management system;[48] however, it is unclear exactly how the attackers found the account password. If the theory is true, a protective step at this phase of the kill chain could have included the elimination or alteration of unneeded default accounts, as called for in PCI-DSS 2.1.[49]

In its recently filed 10K, Target states that in the fall of 2013, "an independent third-party assessor found the portion of our network that handles payment card information to be compliant with applicable data security standards."[50] One of those standards would have been PCI-DSS 11.5, which requires vendors to monitor the integrity of critical system files.[51] To achieve this standard, Target could have used a technique called "white listing," whereby only approved processes are allowed to run on a machine.

F. Command and Control (C2) – Attacker Has "Hands on the Keyboard" Remote Access to Victim's Network

Based on the reported timeline of the breach, the attackers had access to Target's internal network for over a month and compromised internal servers with exfiltration malware by November 30. While the exact method by which the attackers maintained command and control is unknown, it is clear the attackers were able to maintain a line of communication between the outside Internet and Target's cardholder network.

In this phase of the kill chain, one protective step includes analysis of the location of credentialed users in the network. For example, if the attackers were still using Fazio's stolen credentials, an analyst would have reason to be concerned if that credential was being used in an unrelated area of the Target network. That the attackers were still using Fazio's credentials when installing malware or moving through the Target network is unlikely, but the analysis could have still proven useful.

Another protective step at this phase would have been strong firewalls between Target's internal systems and the outside Internet (e.g., routing traffic through a proxy) to help disrupt the attacker's command and control. Target could also have filtered or blocked certain Internet connections commonly used for command and control.

[48] Brian Krebs, *New Clues in the Target Breach*, KrebsOnSecurity (Jan. 29, 2014) (online at http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/); Keith Jarvis and Jason Milletary, *Inside a Targeted Point-of-Sale Data Breach*, Dell SecureWorks, at 5 (Jan. 24, 2014) (online at http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf).

[49] Payment Card Industry Security Standards Council, *Payment Card Industry (PCI) Data Security Standard Version 2.0*, at 24 (Oct. 2010) (online at https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf).

[50] Target Corporation, SEC Form 10-K, at 17, 47 (Mar. 14, 2014) (online at http://www.sec.gov/Archives/edgar/data/27419/000002741914000014/tgt-20140201x10k.htm).

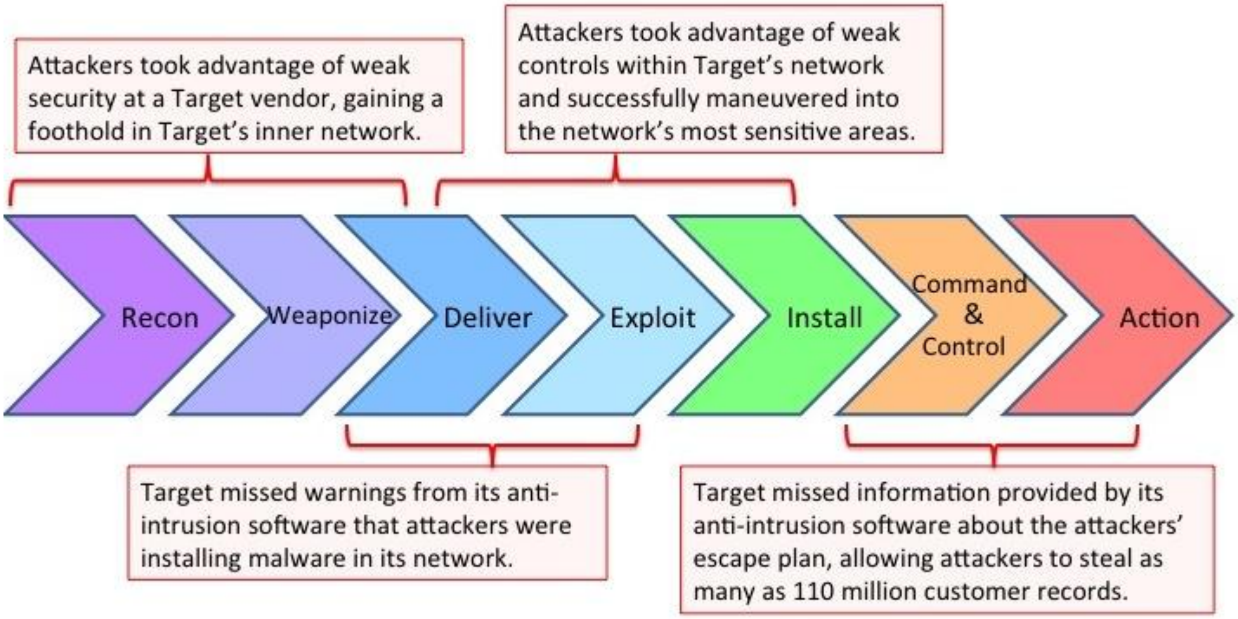
[51] Payment Card Industry Security Standards Council, *Payment Card Industry (PCI) Data Security Standard Version 2.0*, at 63 (Oct. 2010) (online at https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf).

G. Actions on Objectives – Attacker Acts to Accomplish Data Exfiltration

The attackers transmitted the stolen data to outside servers – at least one of which was located in Russia – in plain text via FTP[52] (a standard method for transferring files) over the course of two weeks. At this phase of the kill chain, protective defensive steps could have included white listing approved FTP servers to which Target's network is allowed to upload data. For example, a white list could have dismissed connections between Target's network and Russia-based Internet servers. An analysis of data transmissions on Target's busy network may be like searching for a needle in a haystack, but an upload to a server in Russia presumably would have been flagged as suspicious if discovered.

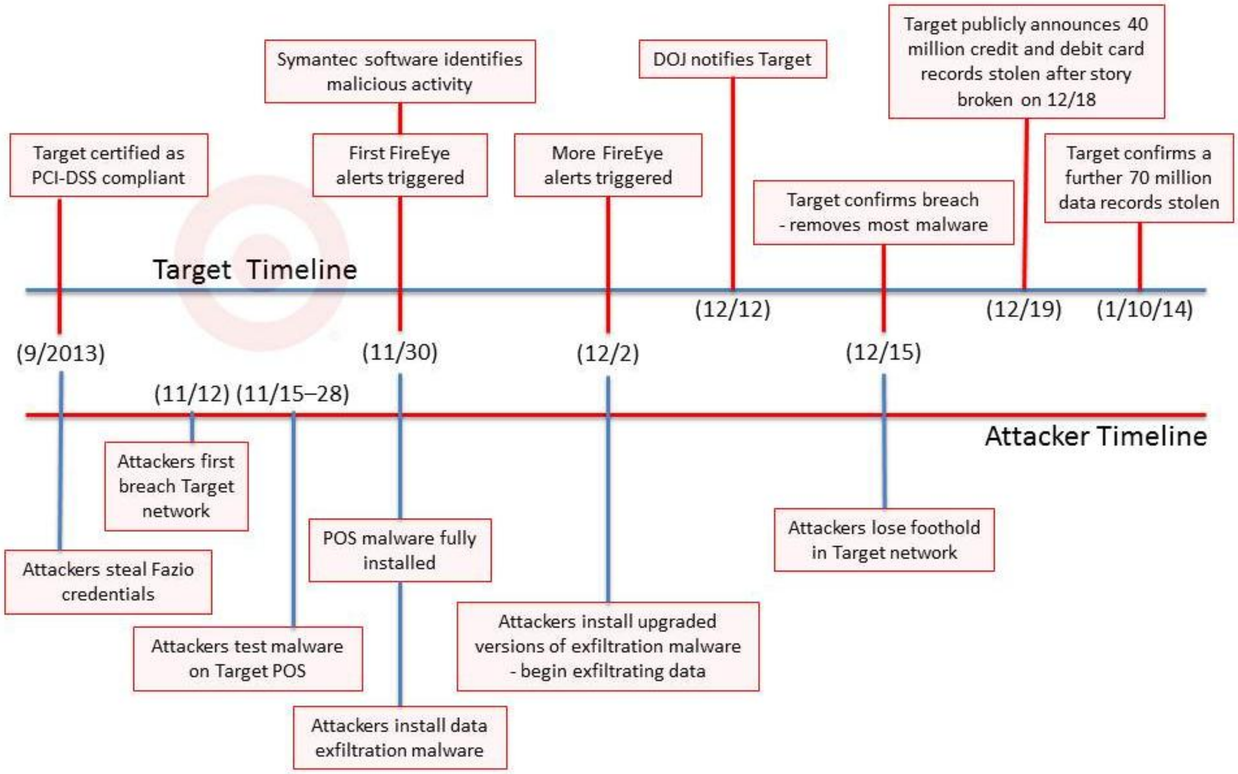
Target's FireEye software reportedly did detect the data exfiltration malware and decoded the destination of servers on which data for millions of stolen credit cards were stored for days at a time. Acting on this information could have stopped the exfiltration, not only at this last stage, but especially during the "delivery" step on the kill chain.

Figure 5 – Target's Possible Missed Opportunities

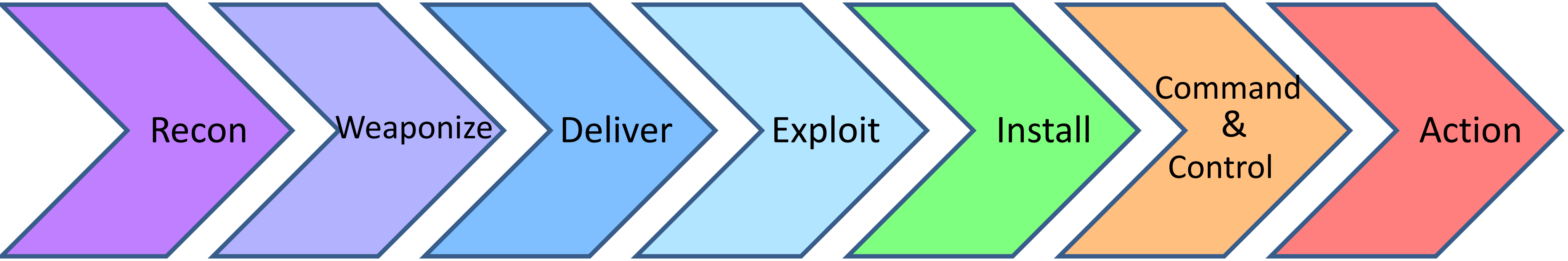

Attackers took advantage of weak security at a Target vendor, gaining a foothold in Target's inner network.
Attackers took advantage of weak controls within Target's network and successfully maneuvered into the network's most sensitive areas.
Recon
Weaponize
Deliver
Exploit
Install
Command & Control
Action
Target missed warnings from its anti-intrusion software that attackers were installing malware in its network.
Target missed information provided by its anti-intrusion software about the attackers' escape plan, allowing attackers to steal as many as 110 million customer records.

[52] McAfee, *McAfee Labs Threats Report Fourth Quarter 2013*, at 7 (2013) (online at http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2013.pdf).

Figure 6 – A Timeline of the Target Data Breach

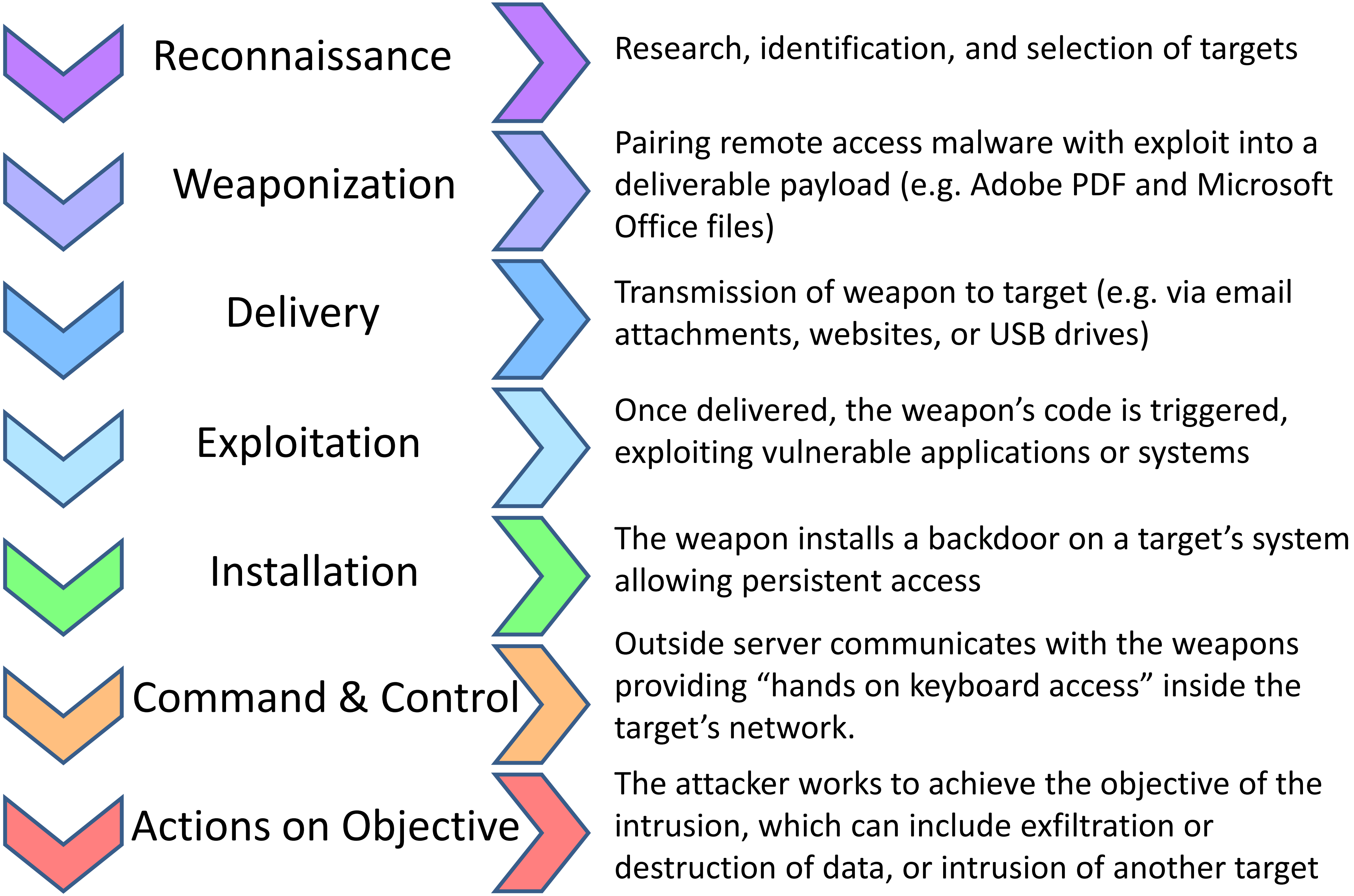

Symantec software identifies malicious activity
DOJ notifies Target
Target publicly announces 40 million credit and debit card records stolen after story broken on 12/18
Target certified as PCI-DSS compliant
First FireEye alerts triggered
More FireEye alerts triggered
Target confirms a further 70 million data records stolen
Target confirms breach - removes most malware
Target Timeline
(12/12)
(12/19)
(1/10/14)
(9/2013)
(11/30)
(12/2)
(12/15)
(11/12)
(11/15–28)
Attacker Timeline
Attackers first breach Target network
POS malware fully installed
Attackers lose foothold in Target network
Attackers steal Fazio credentials
Attackers install upgraded versions of exfiltration malware - begin exfiltrating data
Attackers test malware on Target POS
Attackers install data exfiltration malware

The Intrusion Kill Chain



Appendix I

Phases of the Intrusion Kill Chain



Reconnaissance

Research, identification, and selection of targets

Weaponization

Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

Delivery

Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

Exploitation

Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems

Installation

The weapon installs a backdoor on a target's system allowing persistent access

Command & Control

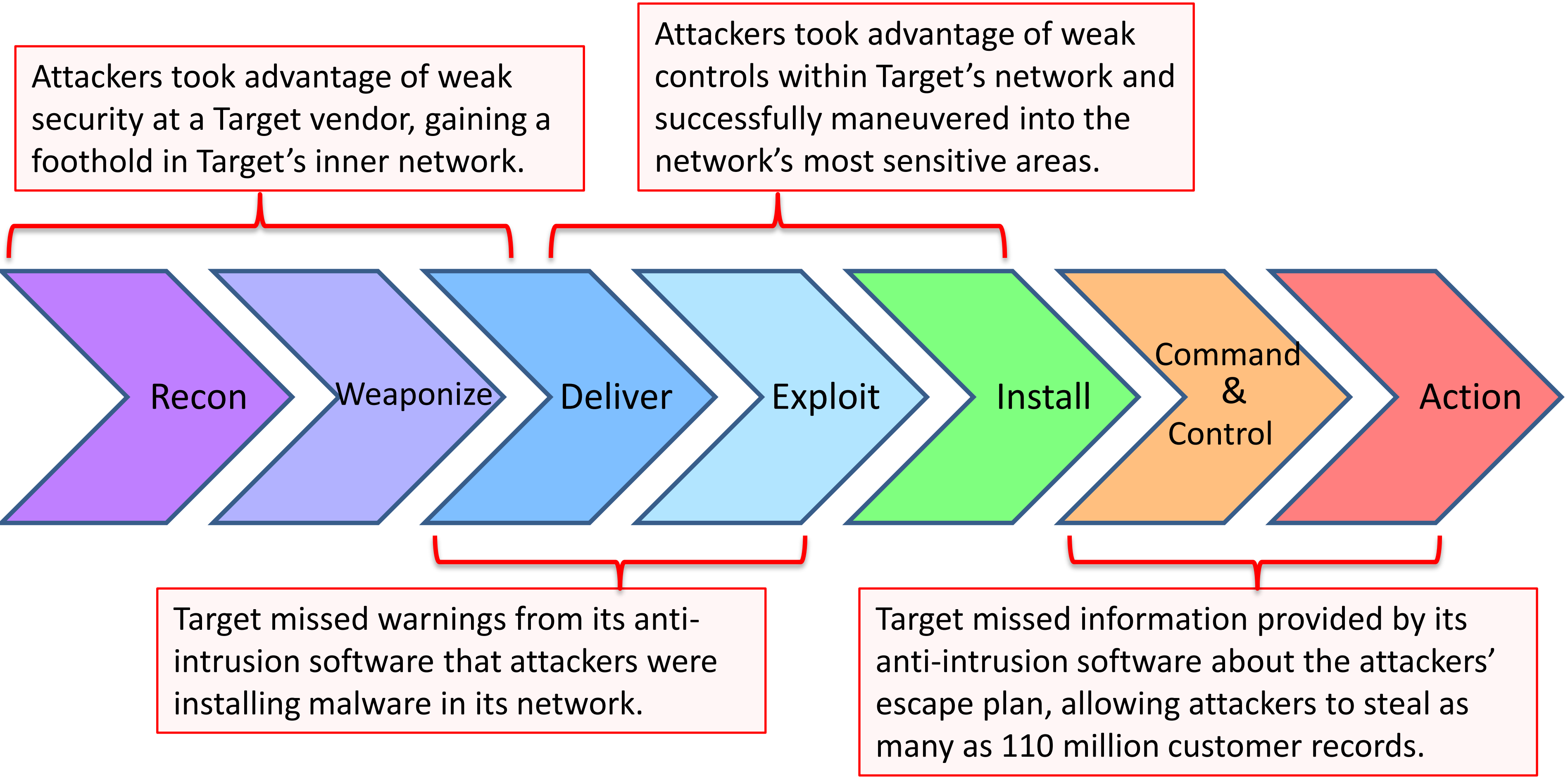
Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.

Actions on Objective

The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Appendix II

Target's Possible Missed Opportunities



Attackers took advantage of weak security at a Target vendor, gaining a foothold in Target's inner network.

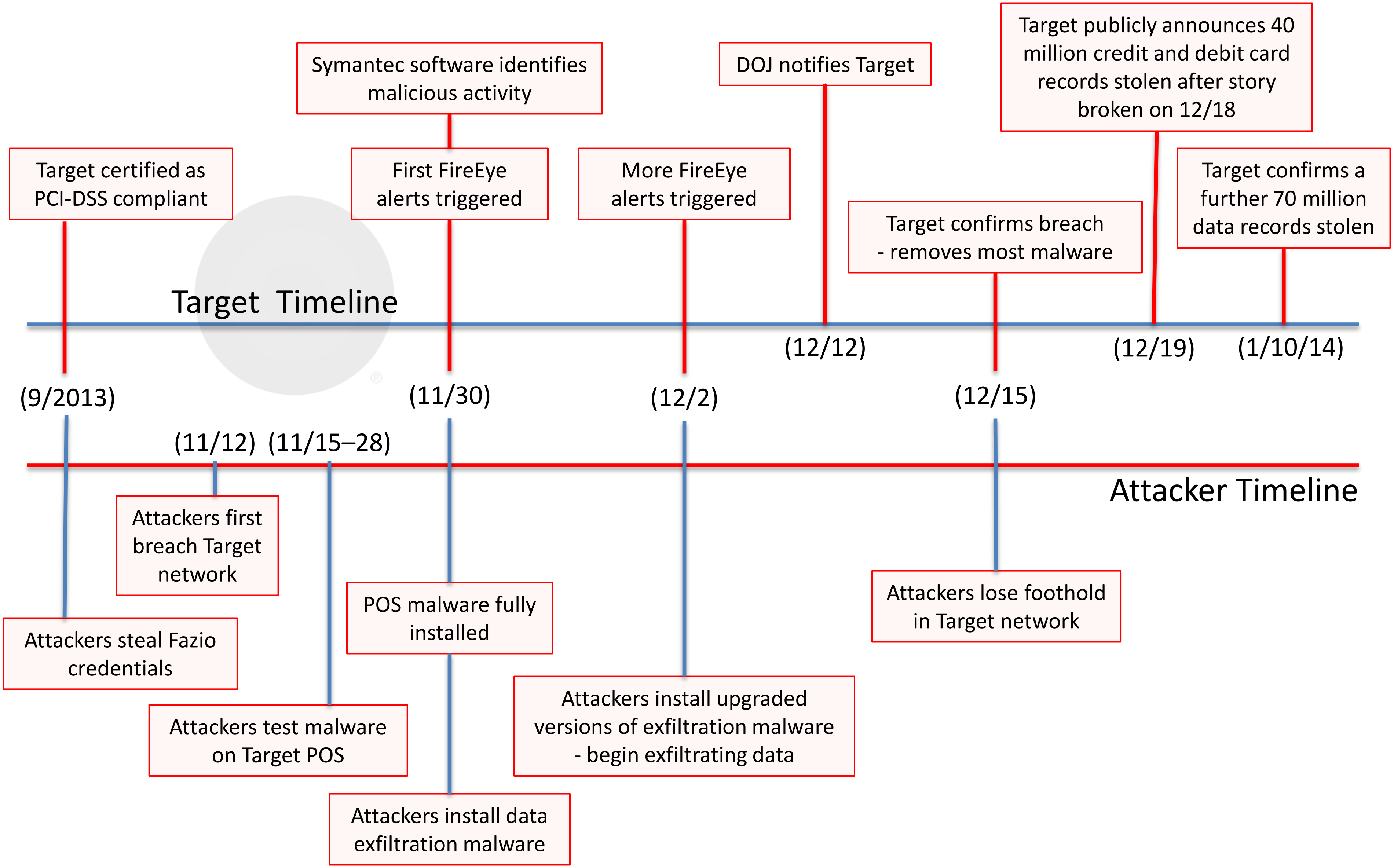
Attackers took advantage of weak controls within Target's network and successfully maneuvered into the network's most sensitive areas.

Target missed warnings from its anti-intrusion software that attackers were installing malware in its network.

Target missed information provided by its anti-intrusion software about the attackers' escape plan, allowing attackers to steal as many as 110 million customer records.

Appendix III

A Timeline of the Target Data Breach



Target Timeline

(9/2013) Target certified as PCI-DSS compliant

(11/30) First FireEye alerts triggered

Symantec software identifies malicious activity

(12/2) More FireEye alerts triggered

(12/12) DOJ notifies Target

(12/15) Target confirms breach - removes most malware

(12/19) Target publicly announces 40 million credit and debit card records stolen after story broken on 12/18

(1/10/14) Target confirms a further 70 million data records stolen

Attacker Timeline

(9/2013) Attackers steal Fazio credentials

(11/12) Attackers first breach Target network

(11/15–28) Attackers test malware on Target POS

(11/30) POS malware fully installed

Attackers install data exfiltration malware

(12/2) Attackers install upgraded versions of exfiltration malware - begin exfiltrating data

(12/15) Attackers lose foothold in Target network

Appendix IV