From Air Conditioner to Data Breach

G. Markowsky and L. Markowsky
School of Computing & Information Science, University of Maine, Orono, Maine, USA

Abstract— *This paper examines the 2013 Target Data Breach in detail with the intent of developing some lessons learned that can serve security educators. The Target Data Breach originated in the network of a trusted vendor and then spread to Target's network. The rush to put more objects on the Internet is introducing many vulnerabilities into networks, so Target's experience of being attacked from a "trusted" source is likely to be repeated from many new sources. This paper then discusses the concept of a "kill chain" and how it could be of use to defenders. Finally, it discusses the relevance of the cyber castle metaphor to the design of hybrid networks and some approaches to building secure hybrid networks.*

Keywords: Target Data Breach, Internet of Things, IoT, Cyber Castle, hybrid network

1. Introduction

On December 18, 2013, Brian Krebs posted [1] an item in his blog about Target investigating a data breach. On December 19, 2013, the giant retailer released a statement [2] confirming that they were indeed investigating a massive data breach. Target's statement included the following section.

> Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts. Among other actions, Target is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident.

The Target Data Breach inspired many news articles such as Goodin [3], Mick [4] and Kreft [5]. Mick [4] traces the source of the attack to an HVAC (heating, ventilation and air conditioning) company, Fazio Mechanical Systems, located in Sharpsburg, Pennsylvania. He notes that among Fazio's clients are Walmart, Costco, Exxon Mobil, and many other companies. Kreft [5] notes that the breach was caused by the loss of one of Fazio's employee's credentials and that Target gave Fazio access so they could remotely login and perform efficiency updates.

Yang and Jayakumar [6] report that in addition to the 40 million stolen credit cards, personal data for up to 70 million Target customers was also stolen, and that some customers might be in both groups. Although the Target Data Breach was large, it is not the largest known breach [7], [8]. See [7] for an interactive visualization.

2. Details of the Target Data Breech

On March 26 a U. S. Senate Committee released a report [9] about the Target Data Breach. Figure 1 from that report shows many interesting details about this breach. First, the attack took place over almost three months beginning in September 2013 and ending on December 15, 2013. Thus the attack was not some spur of the moment event carried out by a teenage hacker. It shows a great deal of planning and patience. Ironically, the attack began about the same time that Target was certified as PCI-DSS [10] compliant. The attack began with the theft of credentials from one or more Fazio employees. As noted in [4], Fazio has a number of large retailers as clients, and we do not know whether the attackers were specifically interested in exploiting Target or just discovered that Target was an easier "target" than other retailers.

According to [9], the attackers first breached Target's network on November 12, 2013. They spent nearly two weeks (11/15-11/28) testing malware on Target's point-of-sale (POS) system. Interestingly more than two weeks passed before Symantec and FireEye software detected the intrusions and alerted Target. At this point, no damage had been done and no data had been stolen. So far no one has come up with an explanation as to why Target chose to ignore the warnings that it received from its own systems.

Riley [11] contains some additional information about how Target was compromised. Six months before the data breach, Target purchased a computer security system called FireEye for $1.6 million. On multiple occasions FireEye warned Target about the presence of intruders in its networks and about some of their activities. These warnings were reviewed by Target's security staff and ignored. Finally, on December 12, 2013, the U. S. Department of Justice notified Target that its network had been breached and data stolen. It took Target another three days to remove the malware and attackers from its system.

Riley [11] contains many additional details about the malware and how it was installed on Target's network. It also includes a discussion of how the stolen credit card numbers were offered for sale and the fact that one of the websites that sold the stolen credit card numbers, Rescator.so, was broken into and the logins, passwords and payment information of carders were posted online.

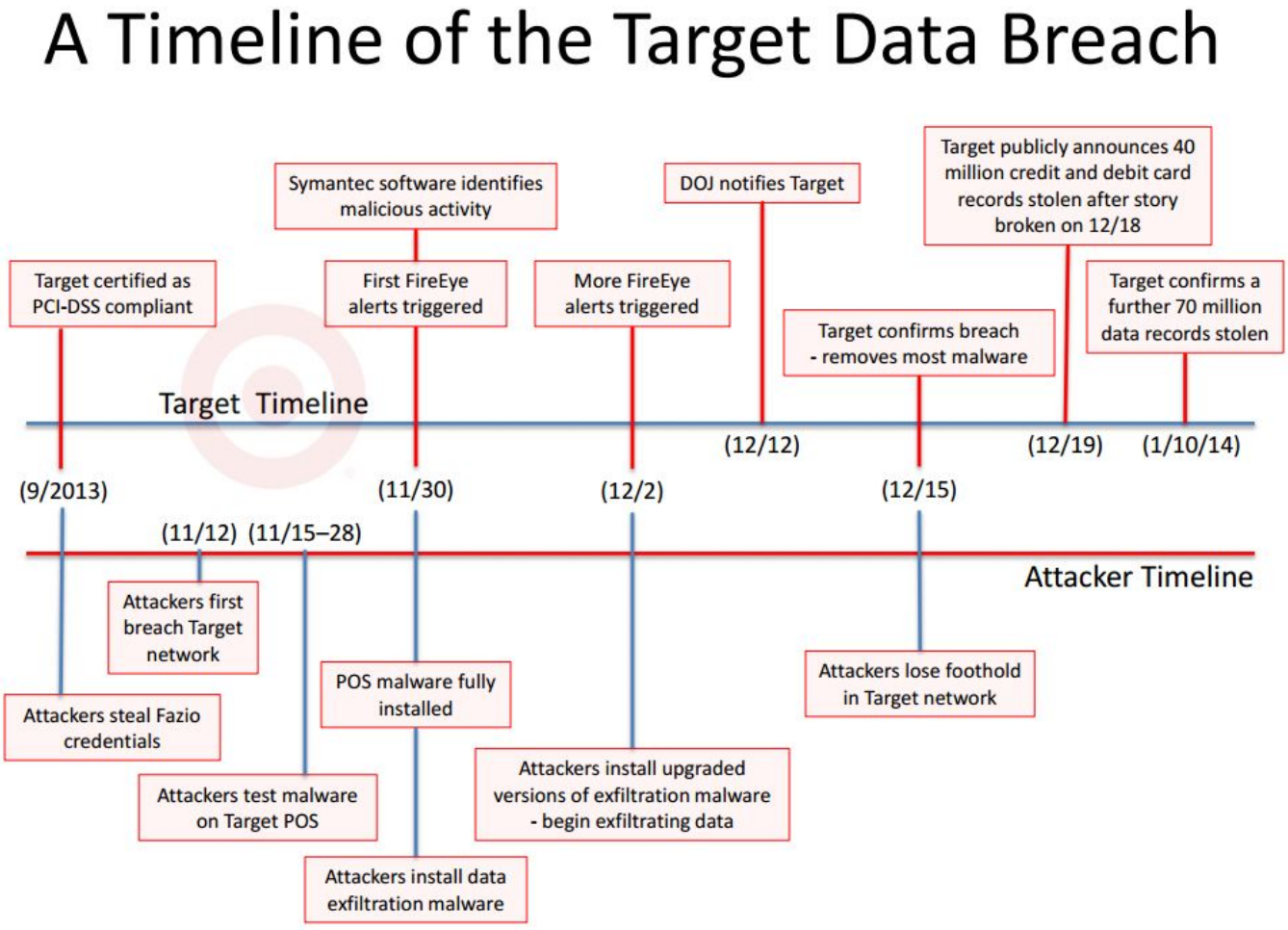


Fig. 1: Timeline from the Senate Report [9]

This data breach was very costly to Target and its staff. Target's profits fell 46% during the holiday season. In addition, several lawsuits were brought against Target, which will likely result in additional losses and legal fees. The data breach led to the resignation of Beth M. Jacob [12], its Chief Information Officer and Executive Vice President for Technology Services in March 2014. Ms. Jacob had no training in computer science or cybersecurity and it is unclear how much of a factor this was in the Target Data Breach. Her resignation was followed by the resignation of Target's CEO, Gregg Steinhafel, in May 2014 [13].

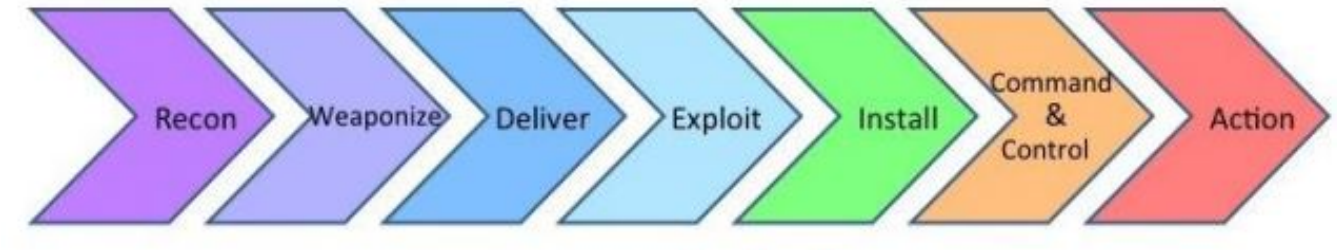
One consequence of the Target Data Breach is the acceleration in the adoption of chip-containing credit cards by Target and other retailers. For more details see [14].

3. Defending Against Target-Type Data Breaches

One of the reasons for studying data breaches is to figure out ways to reduce the likelihood of future data breaches. The Senate Report [9] mentioned in the previous section discusses the use of a "kill chain" in defending against Target-type data breaches. This concept was introduced by the Lockheed Martin Computer Incident Response Team in 2011 [15]. The goal of the kill chain approach is to redress the perceived imbalance between attackers and defenders. Typically, attackers need to only find one weak spot to proceed with exploitation, while defenders must protect all areas of a network. Users of kill chains try to mount an active defense and to model the attacker's steps by a kill chain of steps. The term kill chain comes from the fact that the attacker needs to carry out all the steps in the chain of steps to be successful, while the defender only needs to interrupt any one of the stages to prevent the attack. Kill chains are viewed as a defensive weapon against advanced persistent threats (APTs) such as the Target Data Breach.

The steps of the intrusion kill chain are shown in Figure 2. The following is a list of the steps and a brief explanation each.

1) *Reconnaissance.* This involves collecting as much information about the target as possible. This is done us-



Source: Lockheed Martin

Fig. 2: The Intrusion Kill Chain [9]

ing as many resources as possible. Amazing amounts of information can be collected from the Internet.

2) *Weaponization.* This involves putting together an exploitation package for the intended victim. This package is often built by combining a standard document such as a PDF file, a word processing document or a spreadsheet with some type of remote access trojan.
3) *Delivery.* This involves getting the payload to the intended victim. Three common methods for doing this are: email attachments, compromised websites and infected USB drives. Almost all these methods require some cooperation from the intended victim.
4) *Exploitation.* This involves getting the payload activated and getting a foothold on the target system. This step provides the first link between the attacker and the victim's system.
5) *Installation.* This involves expanding the bridgehead into a persistent presence on the victim's system.
6) *Command and Control (C2).* this involves setting up full control of the system and the escape path for such things as stolen data.
7) *Actions on Objectives.* This involves the attacker accomplishing whatever were the original goals of the attack.

The steps in the kill chain are familiar to cyber defenders. The novelty of using the concept of a kill chain is that it provides a strategy for an active defense that has the ability to disrupt many APTs. [15] provides a detailed case study of the use of this technique. We will follow the lead of the Senate Report [9] and apply this kill chain method to the Target Data Breach with the idea of suggesting how an active defense can thwart such attacks. The concept of a kill chain means that the attacker can be stopped at any point along the chain. Some steps in the chain might be easier to disrupt than other steps, and it is best to focus on those steps.

1) *Reconnaissance.* It appears that the Target attackers carried out the their reconnaissance through Internet searches and by using Target's supplier portal and facilities, which were active as of February 12, 2014 [16]. In this step, the attackers identified Target's third-party vendors. Some of Target's vendor information sites continue to be active as of August 30, 2014 [17], [18]. This publicly available information permitted the attacker to map Target's internal network prior to the breach. One good defensive action for most organizations might be to limit the amount of publicly available information about themselves. This is difficult to do since no one has full control of the information available about them. For example, one does not need to have a Facebook page to have a Facebook presence: it is enough to have friends with Facebook accounts who choose to mention you. While security researchers tend to disparage "security through obscurity," making it difficult for an adversary to learn about your systems might encourage the adversary to search for an easier target. There is a reason why carnivores typically pick less vigorous animals when there is a choice. Organizations can help their defense by encouraging their employees and collaborators to expose as little information as possible to the public. As countries have learned in wartime, "loose lips, sink ships."
2) *Weaponization.* It is speculated that the weapon used to initiate the Target Data Breach was most likely a modified PDF or Microsoft Office document that was emailed to a Fazio employee. At that time Fazio was using the free version of Malwarebytes's Anti-Malware software, which does not provide real-time protection and is not licensed for commercial use. In general, organizations should invest in protective software. Although this protective software is not foolproof, it does catch many instances of malware and helps raise cybersecurity awareness among users. In some sense, it is hard for a defender to disrupt the weaponization stage since it is totally in the hands of the attacker. At best one can prepare for different sorts of weapons once they get delivered.
3) *Delivery.* The weapons appear to be delivered to Fazio via a phishing email. Once Fazio was compromised,

it was relatively easy for the attackers to get into Target's network. The PCI-DSS standard requires two-factor authentication for network access from outside the network as shown in the following quote [10, p. 47].

> 8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.

Organizations can disrupt the delivery or an exploit by getting their employees to recognize the dangers of phishing emails. One effective method is to send phishing-type emails to your own staff and display a "Gotcha" type of message when people click on links they shouldn't click on. Phishing is surprisingly successful even at security companies so it is important to take it seriously and to take steps to make it less effective. Similarly, use two-factor authentication as much as possible. It is obviously less convenient, but the consequences of security breaches are becoming quite severe. It is especially important not to ignore calls for two-factor authentication when one is supposedly adhering to some standard such as PCI-DSS.

4) *Exploitation.* To defeat exploitation one must make one's systems as secure as possible. Ironically, Target's FireEye software system had a feature that would automatically eradicate malware, but that feature was disabled at the time of the attack. Being aware of which attacks are likely to be deployed can help defeat exploitation. For example, in 2013 Visa issued warnings in April [19] and August [20] describing exactly the sort of attack that was used against Target. Had the Target security staff been on the lookout for such attacks, they would have likely responded earlier and more effectively to the attack launched against them. Organizations should seek to learn as much as possible about current threats. This can be through reading as widely as possible and attending conferences and workshops. The cyber threat landscape is constantly changing and one needs to stay current. In general, defenders will get better results if they are active defenders rather than first responders once a disaster has occurred. Of course, if one has defensive systems and they issue warnings, it is imperative that the defender understand exactly what is triggering the warnings. It is a bad idea to routinely dismiss warnings as false alarms. If one is indeed troubled by false alarms from a system, then either the system needs to be better configured or replaced.
5) *Installation.* It is not clear how the installation step was carried out by the attackers. There is some speculation that the attackers might have exploited a default account in a BMC Software information technology management system. In general, system security is increased by securing or removing all default accounts and making sure that all default passwords have been replaced with real passwords. This is a requirement of the PCI-DSS standard [10, p. 24].
6) *Command and Control.* Figure 1 shows that about a month passed between the time the Target network was first breached and the time that the Department of Justice notified Target that its systems had been breached. The details of how the attackers maintained their position in the network are not known; however it is known that the attackers seemed to be able to roam freely throughout Target's system. Target would have benefited from having strong firewalls between various systems. It would also have benefited from blocking or filtering Internet connections that are commonly used for command and control. Networks containing sensitive data should be very unfriendly landscapes for roaming by unauthorized users. There should be frequent barriers and challenges to all who traverse this landscape. We will revisit this point in our last section.
7) *Actions on Objectives.* The data stolen from Target's servers was exported by FTP in plain text to several servers, at least one of which was located in Russia. At a minimum, Target should have had network rules in place that prohibited connections to countries with which it had no business relations. This would have complicated the data exporting for the attackers. In general, it is important to watch outgoing traffic for suspicious activities. Many firewalls focus on filtering incoming traffic. While this is important, it is only part of the story. Sometimes outgoing traffic is easier to analyze for suspicious activities. In general it is good to have whitelists, graylists and blacklists to help interrupt malicious activities and to expedite benign activities.

Organizations need to create attack scenarios to give themselves an opportunity to critically review their own security posture. The analysis applied to the Target Data Breach in this section can be applied by organizations to their own systems.

4. Implications for The Internet of Things

The Internet of Things (IoT), sometimes referred to as the Cloud of Things (CoT) or even the Internet of Everything (IoE), is a term that refers to the growing interconnected ensemble of objects that use the Internet to provide connectivity. Some authors include computers and smartphones in the Internet of Things, while others exclude them.

The security threat introduced by the IoT, and the relevance of the Target Data Breach, is that now computers are

sharing the same cyberspace as thermostats, air conditioners and countless other "smart" devices. The growth of these smart Internet-connected devices promises to swamp the growth of computers, tablets and smartphones. If every appliance has some sort of connectivity, along with every TV, game box, burglar alarm, heating and ventilation system, fire alarm, etc., then it is easy to see that the average household might soon have more "things" devices connected to the Internet than traditional devices. As early as 2003 [21] many luxury cars had 100 or more processors. Even the run of the mill economy car in 2003 already had several dozen processors. Now with the development of the "connected car" [22], [23] all of these microprocessors will be vulnerable. It is not surprising that Gartner [24] estimates that there will be 26 billion devices in the IoT by 2020, and that ABI Research [25] estimates that there will be 30 billion devices in the IoT by 2020. Note that both estimates do not include computers and smartphones. Gartner [24] notes that "by 2020, component costs will have come down to the point that connectivity will become a standard feature, even for processors costing less than $1."

At least one think tank has declared the Internet of Things to be one of the major security threats for 2014 [26]. Studies by Norse [27] and Hewlett Packard [28], [29] identify many types of objects, including such things as printers, thermostats, and security systems, that can be and have been compromised.

One of the reasons that the Internet of Things is such a security threat is that security takes a backseat to innovation [30]. Two powerful forces driving the growth of the IoT are profit and convenience. Companies see the Internet of Things as a very lucrative market. The market for set top boxes grew to $20 billion in 2013 [31]. The markets for many other devices are also expanding rapidly. In addition, businesses expect that the "Big Data" generated by the armies of sensors and intelligent devices will help them develop new products and increase their profits [32].

5. Conclusions and Recommendations: The Castle Metaphor Revisited

It is clear from the analysis of the Target Data Breach and the growth of the Internet of Things that networks in organizations are going to be hybrids. For this hybrid environment, the castle metaphor [33] both conveys the concepts of cyberdefense and complements the concept of a kill chain. Castles inspire many people from an early age and provide a physical model for security that some people might relate to better than just a purely virtual model.

Applying the castle metaphor to the Target Data Breach , we conclude with the following observations:

1) Real castles were always part of an overall defensive strategy and were often constructed first, before the surrounding cities were built. This was not always possible in the case of older cities, but in many cases cities grew around castles that were able to provide local defense. Many computer networks grow in an arbitrary and unplanned manner, without a strategy to meet the organization's objectives and needs. Clearly, the Target network would have benefited from a better design.
2) Castles were subdivided into a number of subareas that could be defended even if some of the defenses were breached. Organizations need to run through various scenarios on the assumption that their defenses will be breached. In particular they should focus on information that they do not want attackers to get and think about how to protect it better. It is clear that sensitive data in Target's internal network was insufficiently protected.
3) Castle defenses were active and castle defenders thought hard about how to put as many obstacles in the path of attackers as possible. As noted earlier, kill chains are designed to work with an active defense.
4) Castle defenses had multiple walls constructed so that they supported each other. For example, some castles had two sets of walls. The inner walls were taller than the outer walls so that even if the enemy were to capture the outer walls, they would not be able to look down upon the defenders on the inner walls. This reinforces the idea that defenses need to be designed with proper separation and defense given to particular items.
5) Castles directed attackers in particular directions and made them work for every inch of territory. Since cyber crime has become a business, having defenses that require more time from an attacker to overcome will often encourage the attacker to go elsewhere. The FireEye system that Target installed forced the attackers to use its facilities and enabled it to spot the intrusion. Regretably, Target security personnel ignored the FireEye warnings.
6) Castles had removable bridges and narrow passages that made defense easier. The various restrictions proposed on FTP traffic function as narrow passages and removable bridges.
7) Castles used guile and deceit to redirect attackers and to confuse them. The FireEye system used by Target is an example of guile when used properly.
8) Castle defenders usually had a good idea of who would be likely to attack them and how. The Visa alerts [19] and [20] outlined exactly the sort of attack that Target might be subject to. Unfortunately, Target ignored these timely warnings.

Few doubt that providing secure cyber services is becoming more challenging. It will require all of us to devote more attention to cybersecurity in order to prevent future Target-like data breaches.

References

[1] Brian Krebs, "Sources: Target Investigating Data Breach," Krebs on Security, December 18, 2013, http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.

[2] Target Press Release, "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," Minneapolis, December 19, 2013, http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores.

[3] Dan Goodin, "Point-of-sale malware infecting Target found hiding in plain sight," *ars technica*, January 15, 2014, http://arstechnica.com/security/2014/01/point-of-sale-malware-infecting-target-found-hiding-in-plain-sight/.

[4] Jason Mick, "HVAC Firm at Center of Target Data Breach Also Counts Wal-Mart, Costco as Customers," *Daily Tech*, February 5, 2014, http://www.dailytech.com/HVAC+Firm+at+Center+of+Target+Data+Breach+Also+Counts+WalMart+Costco+as+Customers/article34278.htm.

[5] Elizabeth Kreft, "How One HVAC Worker May Have Led to the Entire Target Data Breach," *The Blaze*, February 6, 2014, http://www.theblaze.com/stories/2014/02/06/how-one-hvac-worker-may-have-caused-the-entire-target-data-breach/.

[6] Jia Lynn Yang and Amrita Jayakumar, "Target says up to 70 million more customers were hit by December data breach," The Washington Post, January 10, 2014, http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html.

[7] Information is Beautiful Website, July 1, 2014, an interactive visual display of data breaches, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[8] Information is Beautiful Dataset, July 1, 2014, a spreadsheet that lists many data breaches that occurred prior to the Target Data Breach, https://docs.google.com/spreadsheet/ccc?key=0Aqe2P9sYhZ2ndFpGb0pHeEdKVndwTHFyT3BHS0dLN1E#gid=1

[9] "A 'Kill Chain' Analysis of the 2013 Target Data Breach, "*Majority Staff Report for Chairman Rockefeller*, March 26, 2014, http://www.commerce.senate.gov/public/?a=Files.Serve\&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883.

[10] Payment Card Industry (PCI) Data Security Standard, version 2.0, October 2010, https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

[11] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack,"Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," Bllomberg Businessweek, March 13, 2014, http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data. A video presenting this information can be viewed at http://www.cbsnews.com/news/target-ignored-systems-hacking-warnings-report-says/.

[12] Elizabeth A. Harris, "Target Executive Resigns After Breach," New York Times, March 5, 2014, http://www.nytimes.com/2014/03/06/business/a-top-target-executive-resigns.html?_r=0.

[13] Elizabeth A. Harris, "Faltering Target Parts Ways With Chief," New York Times, May 5, 2014, http://www.nytimes.com/2014/05/06/business/target-chief-executive-resigns.html.

[14] Megan Geuss, "Chip-based credit cards are a decade old; why doesn't the US rely on them yet?", Ars Technica, August 2, 2014, http://arstechnica.com/business/2014/08/chip-based-credit-cards-are-a-decade-old-why-doesnt-the-us-rely-on-them-yet/

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

[16] Brian Krebs, "Email Attack on Vendor Set Up Breach at Target," Krebs on Security, February 12, 2014, http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.

[17] Target's Partners Online Website, https://wamlogin.partnersonline.com/securitybrokerage/pub/login.htm?TYPE=33554433\&REALMOID=06-0fb16762-e63c-4dfe-a532-445551a2cc51\&GUID=\&SMAUTHREASON=0\&METHOD=GET\&SMAGENTNAME=\$SM\$cc00Zase4DnYh8i1ouaTStDOm1cY5nFYdGTFhrO4YJmPrPT7tLYI0Xo\%2bdoEIoCNJ\&TARGET=\$SM\$https\%3a\%2f\%2fwww\%2epartnersonline\%2ecom\%2f

[18] Target's Property Development Website, https://pdzone.target.com/portal-target/templates/html/login_new.jsp?TYPE=33554433\&REALMOID=06-f980003e-9313-4487-9ac0-98f792cd3f2f\&GUID=\&SMAUTHREASON=0\&METHOD=GET\&SMAGENTNAME=-SM-pE3oyZbm8QUgajXyF0U\%2bN90sEDwYJr1Uba9SdRrCZOl5LpIlHIpFKsYwdcu8cz5\%2f\&TARGET=-SM-HTTP\%3a\%2f\%2fpdzone\%2etarget\%2ecom\%2fportal--target\%2ftemplates\%2fhtml\%2fexternal_content_display\%2ejsp\%3fcontentid\%3dPRD02--035451.

[19] Visa Data Security Alert, "Preventing Memory-Parsing Malware Attacks on Grocery Merchants," April 11, 2013, http://usa.visa.com/download/merchants/alert-prevent-grocer-malware-attacks-04112013.pdf.

[20] Visa Data Security Alert, "Retail Merchants Targeted by Memory-Parsing Malware - UPDATE," August, 2013, http://usa.visa.com/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf.

[21] Jim Turley, "Motoring with microprocessors," August 11, 2003, http://www.embedded.com/electronics-blogs/significant-bits/4024611/Motoring-with-microprocessors.

[22] Wikipedia, "Connected car," August 15, 2014, http://en.wikipedia.org/wiki/Connected_car.

[23] Charlie Osborne, "Verizon on Internet of Things, the connected car: Location is key," ZDnet, July 22, 2014, http://www.zdnet.com/verizon-on-internet-of-things-the-connected-car-location-is-key-7000031860/

[24] Gartner Press Release, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020," December 12, 2013, http://www.gartner.com/newsroom/id/2636073.

[25] ABI Research Press Release, "More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020," May 9, 2013, https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne.

[26] Steve Durbin, "Security Think Tank: ISF's top security threats for 2014," *ComputerWeekly.com*, http://www.computerweekly.com/opinion/Security-Think-Tank-ISFs-top-security-threats-for-2014.

[27] Norse Blog, "Threat Thursday: Compromised Internet Connected Devices on Your Network," December 12, 2013, http://www.norse-corp.com/blog-thursday-devices-131212.html.

[28] HP Press Release, "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," July 29, 2014, http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.U-412vldXNk.

[29] HP Study, "Internet of Things Research Study," http://fortifyprotect.com/HP_IoT_Research_Study.pdf.

[30] Mohana Ravindranath, "Analyst: In 'Internet of Things,' security often takes a backseat to innovation," The Washington Post, November 21, 2013, http://www.washingtonpost.com/business/on-it/analyst-in-internet-of-things-security-often-takes-a-backseat-to-innovation/2013/11/21/b50db616-52ed-11e3-9e2c-e1d01116fd98_story.html.

[31] Riley Snyder, "Set-top box revenue grows to record $20 billion," Los Angeles Times, July 16, 2014, http://www.latimes.com/business/technology/la-fi-tn-set-top-box-sales-20140716-story.html.

[32] Kurt Marko, "How the Internet of Things Will Change Your Business,", Information Week, December 31, 2013, http://reports.informationweek.com/abstract/81/11996/Business-Intelligence-and-Information-Management/How-the-Internet-of-Things-Will-Change-Your-Business.html?cid=smartbox_techweb_analytics_7.300001221.

[33] George Markowsky and Linda Markowsky, "Using the Castle Metaphor to Communicate Basic Concepts in Cybersecurity Education, " Proceedings of the 2011 International Conference on Security & Management, July 18-21, 2011, Las Vegas, Nevada, USA, pp. 507-511, http://worldcomp-proceedings.com/proc/p2011/SAM5059.pdf.