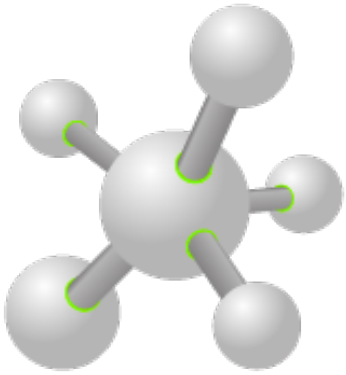
info@thinkst.com
research@thinkst.com
https://www.thinkst.com

ThinkstScapes Ad-hoc Information Update 2014 / AH2

The Target Breach & You



ThinkstScapes Ad-hoc Information Update

2014 / AH2

The Target Breach & You

Introduction

The American retail giant *Target* suffered a breach last year that yielded names, mailing addresses, phone numbers and email addresses for over 70 million clients. The initial disclosure revealed that approximately 40 million debit and credit card records were also stolen during the attack which appears to have hit Target hard. With nearly a hundred lawsuits related to the breach and an estimated $61 million dollars in direct incident response costs, analysts have estimated that the cost of the breach could run into billions[1].

This all makes for exciting headlines, so there has been no shortage of people documenting the breach. We feel however that there are some age-old lessons hidden in the incident that are worth paying attention to.

We hope you enjoy this update!

Background

On the 18th of December, independent security journalist Brian Krebs announced that *Target* was investigating a breach involving millions of customer debit and credit cards[2]. A day later, *Target* issued a statement confirming the breach: "*Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013*".

In an ironic twist the attack affected customers who shopped in retail stores exclusively (leaving online shoppers unaffected which is contrary to our usual view of technical attacks in online vs. offline risk). On January 12th, the Target CEO confirmed that malware installed on the Point of Sale machines was responsible for the theft.

In the days that followed, antivirus companies were quick to analyse samples of the malware and brought more details on the compromise to light (but details on the initial attack vector remained unknown). Analysis of the binaries at this point revealed that the malware operated in various stages, first grabbing sensitive

1 http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

2 https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

data, then copying it to an internal server where it was copied out of the network over the course of two weeks via FTP.

In February, officials revealed that the hackers managed to break into *Targets* payments network by first breaching a "data connection" between the U.S retailer and its heating and ventilation systems contractor (*Fazio Mechanical Services*). Fazio's official response was to proclaim that they were a "*victim of a sophisticated cyber attack operation*" while being "*in full compliance with industry practices.*"[3]

It would later emerge that the initial attack vector against Fazio was through Phishing.

Further investigations revealed that a common Active Directory environment was in use between various segments of the *Target* network, allowing an attack leveraged through *Fazio* to eventually target the payments network.

Lessons

Whitelisting vs. AntiVirus

The fact that "malware" was used to facilitate this attack has been used by several AntiVirus vendors to reiterate the importance of running their products. The truth, however, is that this was clearly a customized attack and the attackers could easily have modified their malware to evade detection (if needed).

Whether any antivirus vendor is able to make a credible (and honest) claim to have been able to stop the attack on the Point of Sale systems is doubtful, but there is a technology that would undoubtably have worked: application whitelisting. A Point of Sale terminal does not need to run multiple new binaries and a simple whitelisting program (and possibly the amount of pain required to deploy it) would have cost far less than the alternative.

Whitelisting applications and services on servers and single purpose machines is a no-brainer. While the initial deployment might require some overhead, its efficacy far outstrips all additional detection mechanisms.

Secure architecture trumps testing

Insufficient network segregation (or insufficient controls at network segmentation points) are a staple of security assessment reports. Although secure architecture is never as sexy as penetration testing or reverse engineering, it is a fundamental pillar of security that cannot be ignored. In far too many networks, one finds that a company's crown-jewels and end-users (or 3rd parties) are poorly kept separated by controls that can be trivially bypassed.

As company networks grow organically it is fairly common for filters between network segments to whittle down to nothing and, as time goes on, the probability of boxes being added that straddle both networks generally approaches 1.

We strongly suggest that architecture reviews are conducted periodically to ensure that attacks are contained in their zones by default.

(Paper based red-team exercises can add tremendous value here by allowing a skilled attacker to identify beachheads and services that would allow one to easily jump between different zones of trust.)

FireEye and boxed solutions

It was recently reported that the Target breach took place despite a recent investment of nearly two million dollars (US) on cutting edge FireEye equipment[4]. FireEye, which is one of the "hottest" security products currently on the market were quick to point out that the tool did indeed raise an alert which, although detected by Target's Bangalore team, was not acted on by the team in the US.

For anyone who has worked on the security team of a large organization, this is hardly a surprise.

---

3 http://faziomechanical.com/Target-Breach-Statement.pdf

4 http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

While it is easy in retrospect to point fingers at teams that failed to respond, we are all aware that the number of malware alerts generated in an average enterprise are mirrored only by the number of IDS alerts that are routinely ignored by SoC teams worldwide. This is the norm, not the exception and for us to act differently is dishonest.

It is absolutely true that most of these tools can and should be tuned to obtain saner baselines, and to limit the number of false positives they emit but the most important change that is required is one of expectation management. If we expect such tools to be silver bullets, we are setting ourselves up to fail (and we will deserve it when we do!)

> *Despite advances in technology and lofty vendor claims there is still no sign of any sort of silver bullet boxed solution in sight. We need to make sure that we have a thorough understanding of the realistic benefits to be gained from new security technology purchases.*

The right technology, intelligently applied

It is interesting to note, that an examination of the reports around the attack tend to indicate that a DLP solution or even a customized IDS solution would have been likely to raise a flag during the attackers lateral movement phases of the breach. While both DLP solutions and IDS can be bypassed, both can be tuned to detect credit card numbers traversing network segments with little effort.

> *This is not meant to encourage the purchase of more equipment, but serves as a reminder that even "older", less fashionable technology, thoughtfully deployed can yield far better results than the shiniest technology currently dominating the headlines. We constantly speak of the importance of good sysadmins, and their value in thoughtful deployments cannot be overstated.*

Informed by Secret Service

Target were informed of the breach by the US Secret Service, and by an investigative reporter who discovered the spread of stolen credit cards on underground forums. It is a well cited fact that most of the companies in Verizon's annual data breach report only discover their breach when informed by third parties, but this is bad news for most of us.

The absence of credit card information from most of our networks does not by itself not leave attackers uninterested, but it does mean that we are less likely to bleed proof of our comprise into monitored underground networks. The absence of this canary in the coal mine leaves us prone to a false sense of security that will make the eventual surprise of discovery of compromise all the more painful.

> *It is not possible to secure your organization without complete visibility of your organization's networks. The lack of public compromises of a given network should not be taken as an indication of the security posture of that network.*

Security debt

The Target incident was used to raise the issue of EMV's low uptake in the US, with the suggestion that EMV would have prevented this attack. Such a claim is not clear for Target though, as EMV is primarily designed to ensure that the card owner is present when the card is used, and a compromised POS could have access to card data or even PINs depending on its construction. However, it is true that payment card protections have languished over the years (especially in the US), as industry players could not agree on how to share the costs of implementation. It is little wonder Target recently announced the acceleration of a project to implement EMV in their stores.

> *The broader point is that the payment card industry has been accumulating security debt and the debt collectors are starting to visit. In direct costs this amounts to tens of millions of dollars for Target plus the indirect costs. Incurring debt to grow a business is elementary, but it can't be rolled over indefinitely and the same applies to technical debt. As the threat landscape morphs, important security actions might be temporarily deferred but they are seldom permanently neglected without consequence.*

Conclusion

The press has been fairly merciless with its condemnation of Target and security vendors are quick to exploit such situations to increase revenue. Most honest security practitioners look at the breach and quote John Bradford: “There but for the grace of God, go I”.

We should use the incident to take honest stock of decisions made, and our current security posture and should take the opportunity while we are not in the headlines to make sure we don’t get there.

This update was written by haroon@thinkst.com. Please contact him if you have queries or comments relating either to this report, or the ThinkstScapes service.