THE HOLISTIC APPROACH TO PREVENTING TARGETED ATTACKS.

Applied Intelligence

BAE SYSTEMS
INSPIRED WORK

EXECUTIVE SUMMARY

The news has been full of attacks on retailers. Target, which lost the data of more than 100 million customers, is just the highest profile example. Although tiny in comparison to Target, the attacks on Neiman Marcus and Michael's Stores also affected about four million customers.

In the Target case, wily attackers located unguarded vulnerabilities, found entry points where no one was looking, and even used the internal network to hide the payloads until they were ready to make off with their quarry. Perhaps intentionally, they did this all at the busiest time of they year for retailers - the all important holiday season. Maybe, in addition to having some good luck as they made their way through the defenses, the attackers counted on retailers being too occupied with other things to even notice.

In this white paper, we look beyond the headlines and focus on the roots of the Target attack and we investigate what Target could have done to prevent it. Finally, we propose a holistic approach to security that all companies can adopt to increase their security

WHAT WENT WRONG AT TARGET?

The Target attack dominated the security and mainstream technology press for weeks. It resulted in hundreds of front-page headlines, sparked thousands of water-cooler conversations and panicked millions of consumers. In the weeks and months following the disclosure of the attack, the circumstances of the compromise have become clearer. The Target attackers succeeded because of a combination of good luck and poor practices by the defenders.

Target CFO John Mulligan provided the gruesome details in testimony to the Senate Judiciary Committee in February 2014. Here's how it went: On November 30, 2013, the attack commenced when the wily hackers placed their malware on the Target network.

According to reporting by KrebsOnSecurity[1], the attackers were able to gain Target account credentials after a shotgun email phishing campaign hit a Target contractor. Mulligan told the Senate committee the hackers stole the credentials of an employee of Fazio Mechanical Services, one of Target's contractors for refrigeration and HVAC systems. As a Target contractor, Fazio staff had accounts on Target systems.

The attackers then placed malicious software on the Target network. This software copied and removed the stolen records to destination servers controlled by the attackers. Target's malware detection spotted the malicious software and the company's security team got an alert. But instead of moving alert status to "DEFCON 5" immediately to isolate the attack and minimize the damage, the Target teams did nothing.

Put simply: the warning signs - very clear warning signs - were there, but Target staffers ignored them.

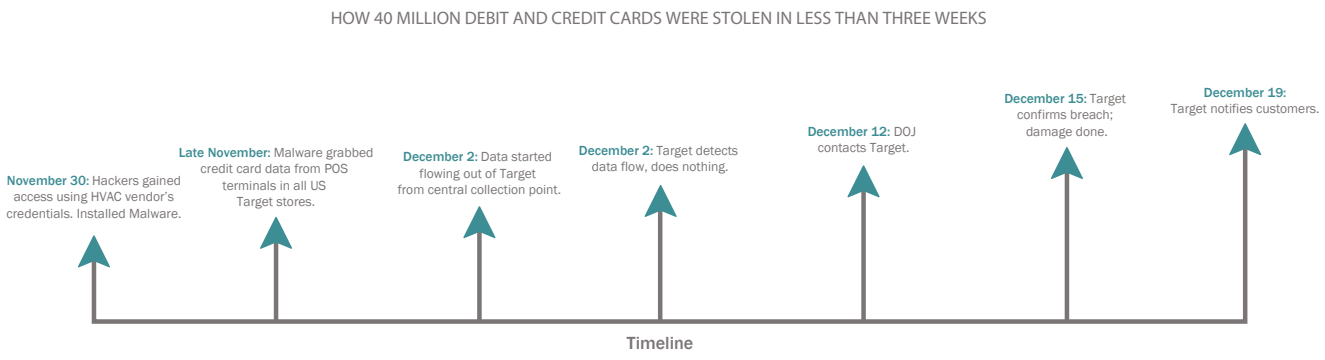


Figure 1: Monthly Incidents and Historical Data

[1] http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

It wasn't until the US Justice Department contacted Target on December 12, 2013, to tell the company of the data breach that the security team went back to work to find out what happened. Target then took three days to confirm that hackers had been able to compromise its point-of-sale network and install malware that had access to all card terminals in its US stores. Target notified customers on the December 19 - seven days after being alerted by the DOJ and nearly three weeks after it first detected a problem.

It's almost certain that if it had taken swifter action, the attack would have been minimized. But the damage was done: the hackers stole 40 million debit and credit cards from shoppers during the holiday season along with personal data of about 70 million customers.

To make the situation even more embarrassing for Target, according to Krebs[1], the hackers used publicly accessible information on Target's supplier portal. Attackers exploited information found on Target's facilities management and supplier pages to help design their attack. One of the documents the attackers downloaded contained metadata that might have helped the attackers gain critical information about Target's internal network. Using knowledge gained from the publicly accessible document, attackers were able to design malware to collect data from the infected cash registers.

It appears that this was more than a breakdown of software or hardware; it was a broad breakdown of communication, accountability and common sense.

EMAIL IS THE KILLER APP

The most insecure parts of any security infrastructure are the living, breathing human beings tapping on keyboards. Intentionally or not, we all make mistakes now and then - mistakes we'd like to "do-over" if we could. And it's almost certain the poor HVAC contractor employed by Fazio Mechanical Services, whose account was compromised, made one of these mistakes. Fazio would, no doubt, give just about anything to get that click back. One innocent click, of the thousands we all do every day, made the difference between just another day at the office and a $100 million (and counting) debacle for a huge company.

The vector used for the initial attack on Fazio was email. It was a phishing attack. So why is email so often the cause of these kinds of problems? Why does it so often provide the starting point for attacks?

The short answer is that email is the most common egress and ingress point for information within most companies. Everyone has an email account. We all use email every hour of the day to communicate with colleagues and friends. We exchange files, send important messages and receive promotional emails from businesses. Email is the essential communications medium of the modern age.

Phishing attacks are the high-tech equivalent of a confidence game, conducted over the essential medium. Phishing emails can masquerade as friends, or as a popular retailer or businesses. Phishing emails cloak their origins by using masked URLs that only show the true URL if you hover your mouse over it. Ultimately, phishing emails are designed to induce recipients to "click" and visit malicious destinations controlled by the attackers.

Phishing emails are hard to stop unless recipients are vigilant. Defenders must be nearly perfect. While there are numerous tipoffs a user can employ to detect a phishing scam, not all employees are trained to recognize them. In the Target case, a shotgun phishing email, clicked on by that innocent HVAC contractor, was the point of failure.

HOW TO SPOT A PHISH

It's not always straightforward, but there are a few steps you can take to avoid being drawn in by a phish.

- **Look for misspelled words and lousy grammar:** Hackers are notoriously bad spellers. Some marketers are too, so it's not always the case that that a typo-laden email is a phish, but it's a good tipoff.
- **Look before you click:** Before clicking, hover over a link to make sure it goes to the site you think it does. Often, a phishing email will spoof the URL of a well-known brand - or just camouflage a nasty IP address under that URL.
- **Only open the familiar:** If you receive emails form people you don't know, or offers from companies you never subscribed to, don't open them. And if you do open them, don't click any links.
- **Pay attention to linkbait:** Attackers want victims to click on their links and will exploit every human failing to get them to do it. The more strongly an email appeals to your curiosity, charity, urgency, prurience or vanity, the more likely it is to be a phishing attack.

WHAT WAS THE BREAKDOWN?

In the Target breach, the key breakdown was not the click by an employee of Fazio Mechanical Services. The real breakdown was upstream, at Target - granting an outside vendor account privileges on a potentially sensitive service, in this case an account on Target's Active Directory servers. We could argue at length about why an ordinary and unsophisticated HVAC contractor needed Active Directory access. But even these two breakdowns - the simple act of granting Active Directory access, and clicking on the link that caused the damage - were not sufficient to explain why the Target hack became so infamous.[2]

To understand it all, we must add a third breakdown, which sits squarely in Target's lap: the failure to put the pieces together afterward.

Failing to put the pieces together was not for lack of money or resources. Target had many security defenses in place. According to Bloomberg Businessweek[3], in the summer of 2013 the company installed a $1.6 million malware detection tool from FireEye and also had a security team in Bangalore monitoring its computer systems around the clock. Target was also PCI-compliant prior to the breach, which meant that - by definition - it also owned and operated anti-virus software, firewalls, intrusion detection systems (IDS) and log management software. All of these items are mandated by PCI-DSS and are required to be installed on systems that processed cardholder data. In addition, the retailer also operated a security operations center (SOC) in Minnesota.

Let's emphasize one fact: FireEye did its job on December 2. It detected the data outflow and alerted the Bangalore team, which, in turn, alerted the SOC in Minnesota. We can also reasonably assume that at least one of the other security technologies Target owned picked up traces of the attack. But then nothing happened for 13 days - as millions of customer records streamed out of Target to collection points in the US and subsequently to their final stop in Russia.

[2] http://money.cnn.com/2014/02/04/technology/security/target-senate/

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

WHAT ABOUT PCI DSS?

The credit card industry and the retailers it serves have certain standards in place to minimize data breaches. Retailers and other organizations that handle information for the major card organizations are supposed to adhere the proprietary Payment Card Industry Data Security Standard (PCI DSS). PCI DSS has at its core a standard to reduce credit card fraud that results from breaches like the one Target fell victim to.

But, as important as the standards may be, in many cases they are merely a way for a company to limit liability. And they are a single ingredient in protecting data. Other factors contribute to successful attacks. Target's vendor management was amateurish at best (Why did an HVAC contractor need Active Directory access?). And, without a doubt, the offending email should have been stopped in its tracks before an innocent person was able to ensnare an entire company in this mess.

How could this have happened, even after FireEye detected it and the security team in India and the US knew about it? We can make some educated guesses. Target's failure comes down to something fairly simple: the various silos of security information did not talk to each other. The information Target's staff received was not presented in a relevant or timely way. They did not arrive at the conclusions they needed to act fast enough. In short, the tragedy of Target was due to the failure to think of the many data sources, security systems, directories, suppliers and point-of-sale devices as a single, interconnected system.

A system, in the broad definition, is a set of connected technologies or processes that form a greater, more complex whole. And that's where Target's problem lies. It thought it had a system in place, but it's clear it only had silos: FireEye, the Bangalore team, the SOC in Minnesota, and many individual security technologies. When needed the most, they acted (or didn't act) separately.

In any crisis, it's systems thinking that saves the day. Consider the case of US Airways Flight 1549, which landed in the Hudson River under emergency conditions in early 2009. It was a successful water landing because of the systems in place. Captain and crew communicated smoothly. Passengers cooperated. Safety equipment deployed reliably. A complex interaction of people, processes, and technology - working together as an integrated whole - saved the day. The individual expertise of the captain, co-pilot and crew were critical to the safe landing, but if any of them had performed their duties in isolation, a heroic moment could have easily gone bad. That's systems thinking.

At Target, the success of the breach arose from a core problem: the components were scattered and unfocused. A better-imagined environment - a system in the true sense of the word - that was easier to monitor, integrated information faster, was simpler to build and required less maintenance, would have had a better chance at finding the problem before it exploded on the scene.

HOW DO YOU AVOID BECOMING THE NEXT TARGET?

No company wants to see their name splashed across the front pages of the Wall Street Journal. No company wants to be the next Target. We suggest that there are two choices a company can make about how to protect its information assets: the old way — silos — and the new way: the systems approach.

THE OLD WAY: SILO THINKING

Over the years, companies have been stockpiling more and more security gear. Anti-virus and firewalls enjoy 100% penetration and have been "checkbox" purchase items since the early days of the Internet. Since the mid-2000s, companies have added technologies such as intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM).

PCI-DSS established log management software as a CISO priority. In the wake of concerns about industrial espionage, "targeted attack detection" has emerged as a new category. These technologies, among others, have been added to the CISO's purchasing shopping list. As a result, IT security spending has increased to record high levels — 17% of the typical 2014 IT budget, according to Computerworld.[4]

Stacking more and more gear onto the CISOs shopping list is essentially the "best-of-breed" strategy. It could also be called the "spend-more" strategy, or simply "spray and pray." Companies procure all the elements separately from different vendors, with different technologies at play and different vendor interests. These silos are cobbled together — or not — by the customer or by a preferred integrator.

Silo thinking has a key weakness. By requiring the monitoring of multiple, disparate systems, the best-of-breed strategy splits the attention of already-busy IT staff, and inevitably leaves a few vectors unwatched.

THE HOLISTIC APPROACH: SYSTEMS THINKING

The alternative to silo thinking is systems thinking: re-imagining security processes as an integrated whole. In the case of attack prevention, that means selecting vendors that integrate all the elements - email, web filtering and SIEM. The components don't all have to be from the same company, but they need to be integrated in such a way that the information flows seamlessly. Crucially, the information needs to be filtered and packaged into a format in which it can be rapidly assessed, evaluated and acted on by human analysts.

If one component detects something, it alerts the other components. Putting everything under the same watchful eyes protects assets and helps a company understand the risks more acutely. Connecting the systems on the back end begins to break down the individual siloes.

[4] http://www.computerworld.com/s/article/9242536/Forecast_2014_How_to_wring_value_from_your_IT_budget

The goal of systems thinking is to interrupt an attack at every critical point in its lifecycle. This lifecycle is often called the Kill Chain. As described by Lockheed Martin, these phases include:

1. **Reconnaissance:** Research, identification and selection of targets.
2. **Weaponization:** Coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (i.e., the weaponizer).
3. **Delivery:** Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors are email attachments, websites, and USB removable media.
4. **Exploitation:** After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability.
5. **Installation:** Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
6. **Command and Control:** Compromised hosts beacon to an Internet controller server to establish a command and control channel. Once the C2 channel establishes, intruders have "hands on the keyboard" access inside the target environment.
7. **Actions on Objectives:** Intruders take actions to achieve their original objectives. Typically, this objective is data theft, which involves collecting, encrypting and extracting information from the victim environment. Alternatively, the intruders may access the initial victim box for use as a hop point to compromise additional systems.

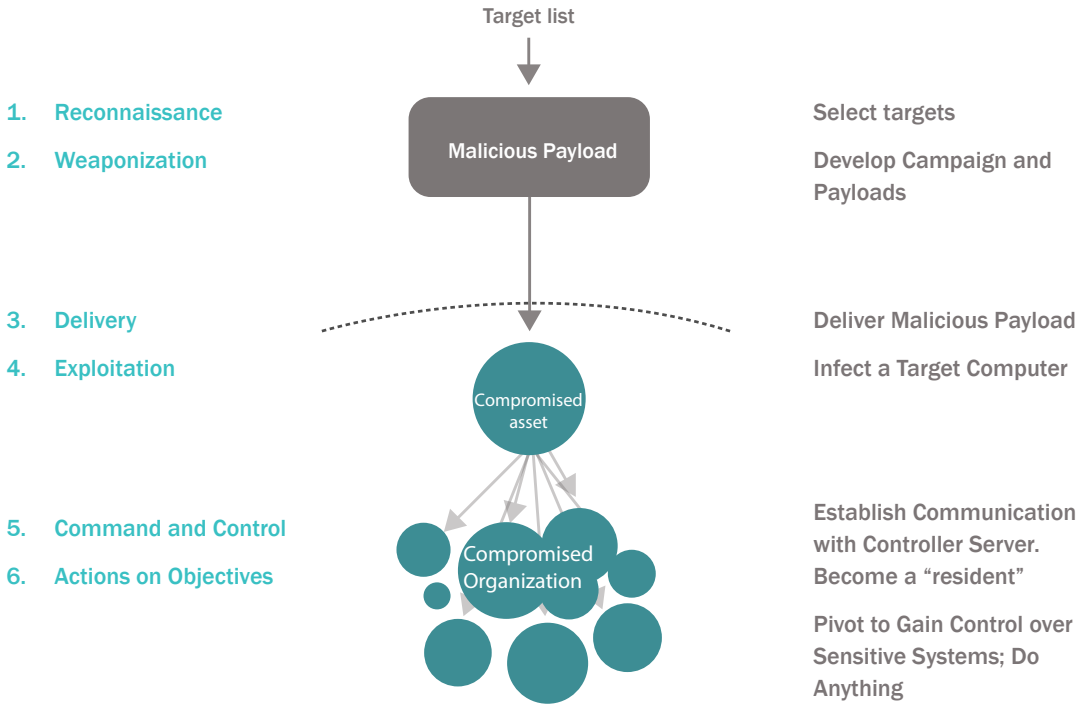
Adapted from Hutchins, Cloppert and AminBy employing systems thinking, enterprises can construct cooperative, compensating controls that prevent an adversary from moving from one phase to the next.[5]

[5] See Hutchins, Cloppert and Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," ©2010 Lockheed Martin Corp

THE INTRUSION KILL CHAIN: AN ATTACK TEMPLATE

As noted in our 2H 2013 Financial Institution Threat Report, Blackhole-associated web activities had dropped significantly, and our findings indicate that it has practically disappeared at this point. Since the arrest of the creator of the Blackhole exploit kit in October 2013, different exploit kits have risen to compete for market share, but none have gained dominance like Blackhole did. As shown in Table 5, in 1H 2014, due to low incident volume, no exploit kit earned its way onto our Top 10 Threats list. Ransomware Cryptolocker jumped from number four to number one. Compared to 2H 2013, threats have diversified. The threats identified in Table 4 aggregately accounted for 28 percent of total incidents, and in 2H 2013, they accounted for 38 percent. This is also reflected in the Simpson diversity index, which increased to 0.85 from 0.46. This represents a significant increase in diversity.

Also of note: 4 of the top 10 threats on this list are new.



Broadly speaking, systems thinking requires looking at all the elements as part of a whole - including the technology you buy and install, the people you hire and what you can teach them, and the traits and behaviors you should encourage in the organization. These elements are all put into service with one goal: to interrupt the Kill Chain.

1. **Technology:** The things you can buy

- **Email security** is a more proactive measure than IDS/IPS. It can filter attacks that begin with email - the killer app - during the Delivery phase.
- **Intrusion detection and prevention (IDS/IPS) technologies** enable you to spot and detect command and control traffic patterns during the Exploitation phase or later.

2. **Zoning involves segmenting your network** - placing firewalls with rules in between the different security zones (i.e., between your production network and your corporate LAN and between your production network and your DMZ where your public-facing assets are stored). Proper zoning makes it harder for adversaries to achieve Actions on Objectives. Competencies: The skills an IT department must master

- **Compartmentalizing information** introduces the equivalent of locked gates between the various levels of information - along a scale from publicly available material to the most treasured company information. Everyone doesn't need to know everything about everything. Compartmentalizing information means that only those people who need to know something (or gain access to physical assets) can do so.
- **Network security monitoring** requires setting and recording a baseline for normal activity on your network, such as the normal traffic level and type. You should train IT to recognize anomalies and then have a process in place for taking action.
- **Incident response** means preparing for the worst, and doing what you must, when you've been breached.

3. **Traits:** The behaviors you can encourage in employees

- **Security awareness** teaches your employees to look for suspicious activities. Phishing campaigns have a formula to them and a rhythm - so there are very concrete things you can train your people to look for.
- **Phishing resistance** involves targeting your own employees with fake phishing campaigns to test their awareness. It ensures they're not susceptible to this kind of trickery.
- **Custodianship** encourages a sensibility and responsibility in employees to report something if it could threaten the security of customer data and company systems. There should be a straightforward reporting mechanism in place.

WHAT DOES A TRUE SECURITY SYSTEM LOOK LIKE?

A systems approach requires multiple layers of technology that help protect an enterprise at every phase in the Kill Chain. These components work together as cooperative, compensating controls to interrupt attackers as they attempt to move from one phase to the next. These technologies are appropriate before an attack succeeds (pre-exploitation) and afterward (post-exploitation).

Pre-exploitation: Interrupting the Delivery phase

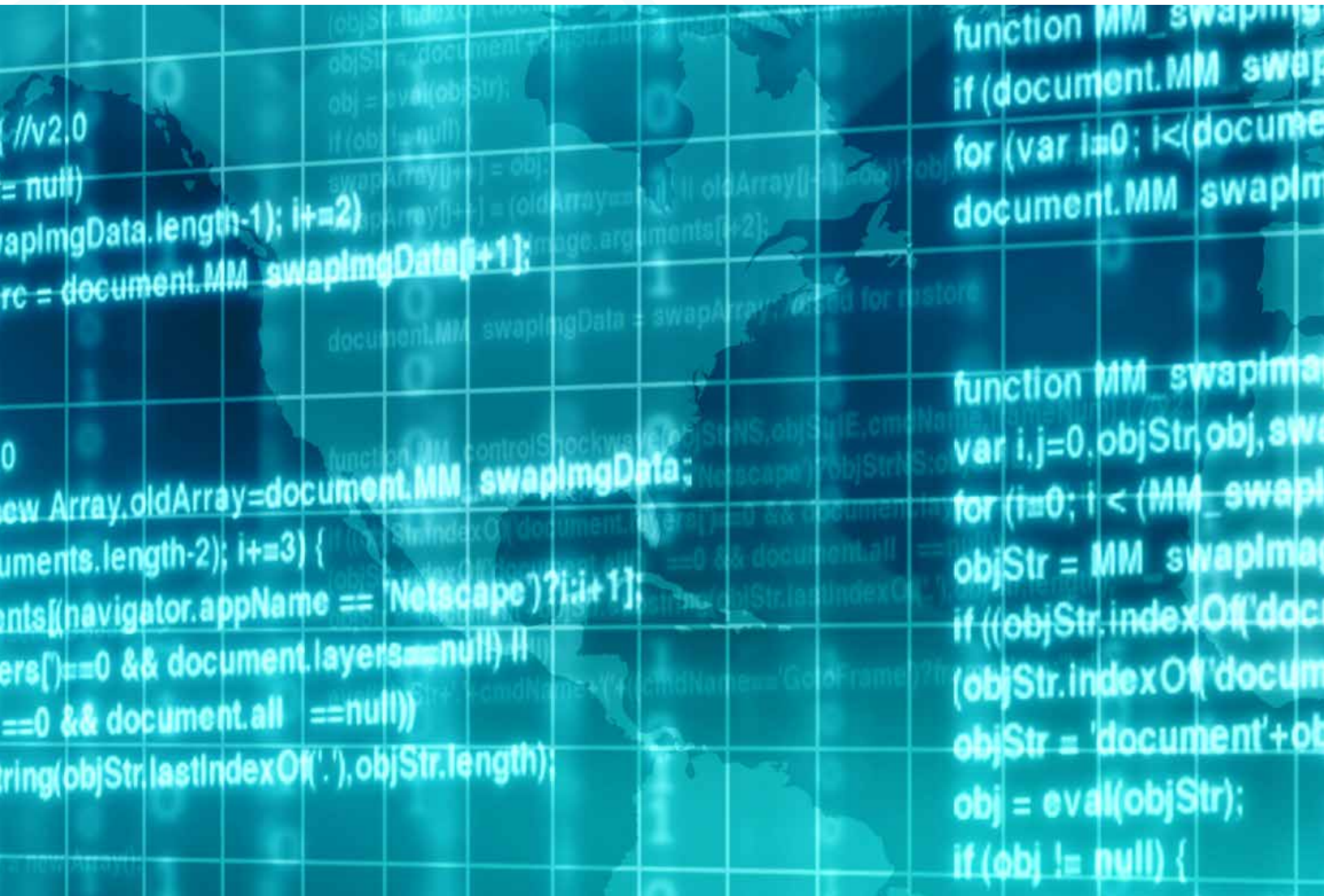
- **Email security:** Strong, redundant anti-virus and anti-spam engines, with controls to throttle high-volume senders and detect directory brute-forcing.
- **Web security:** Inline web security filters to prevent visits to sites that are known to or likely host malware used in attack campaigns.
- **Zero Day Prevention:** Heuristics, analytics and sandboxing to stop targeted attacks, spear phishing, "longline" phishing, and advanced zero-day exploits that anti-virus and anti-spam controls can't detect.

Post-exploitation: Interrupting the Command and Control and Actions on Objectives phases

- **IDS/IPS:** Monitoring and analysis of complex network traffic in real-time; blocking of malicious internal traffic and sophisticated attacks that cannot be prevented with firewalls alone.
- **Security information and event management (SIEM):** 24 x 7 monitoring of critical devices on the network by a trained security team. Log management: Regular reviews of security logs from critical devices to understand security events across the network, detect suspicious activity and respond quickly to prevent malicious attacks.
- **Insider Threat prevention:** Content aware policy filters to ensure that sensitive and protected information stay inside the organization - where they belong.

Additional components, such as archiving, device management and compliance software can help. But the key components to help a company avoid the kinds of headlines they don't want are in this list.

A systems approach connects the dots and those connections ensure that information gets in the hands of those who need it as quickly as possible - whether it's a system component or a human being.



TAKEAWAYS

The issues we outlined in this paper are not one-dimensional. They are a complex set of problems. But the key to solving, or at the very least understanding, these problems is to think of them as separate elements of an interconnected system.

We look at it as a matter of People, Process and Technology - with the goal of interrupting the attacker's Kill Chain.

PEOPLE

As we noted earlier, the weakest link can often be the person at the keyboard who clicks links, downloads payloads and generally wreaks havoc - however innocently. Often, this behavior arises from a simple lack of training on what to do and how to do it. Effective, regular training can minimize the risks, but it is only be part of the solution. Process organizes things and directs people on what to do and when.

PROCESS

Regardless of the technology in play, it's important that every company have ironclad processes in place. An effective process at Target and other companies might not have prevented the attack, but it could have shortened the mean time to incident discovery - a critical, if overlooked, metric. Often, the focus is simply on attack prevention. That remains important. But just as important is recognizing that no defenses are 100% impregnable - so having a process in place for dealing with successful attacks is must.

Target's initial technology defenses did their job once the attack started. But the process broke down at some point and the company moved too slowly. If Target had been even a little bit faster in responding to the attack, closing the breach, notifying the authorities and getting in touch with customers, at best, it could have slowed the flow of credit card data and might have prevented the problem from reaching the such a large scale. If it had contacted the authorities when the breach was first discovered (instead of waiting for them to come knocking), it's likely it would have notified its customers faster as well. That wouldn't have eliminated the problem, but it would have reflected better on the company and would have helped make its customers feel more at ease.

TECHNOLOGY

Security technology has evolved considerably in the past few years, and the point solutions currently available are better than ever. Integration and coordination of those solutions is crucial for interrupting the Kill Chain, whether it is before the initial attack succeeds (the Delivery Phase), or after (the Command and Control and Actions on Objectives phases). Significant reduction of risk - the goal of every company - will only come when companies can reimagine and integrate the siloed components they own into a coherent, cooperative and consistent security system.

ABOUT US

BAE Systems Email Protection Services is the expert cloud provider of information security solutions. We deliver the industry's only advanced Security-as-a-Service platform that's simple to deploy and transformational to use. For years, BAE Systems Applied Intelligence has been recognized as a leading managed service provider of business email and network security services. We have hosted, secured and monitored the information assets of thousands of large enterprises and regulated businesses utilizing our proprietary security software. By tirelessly safeguarding our customers' most important information, we enable growth-minded leaders to pursue their business ambitions without security worry.

If you would like to learn more, please do not hesitate to call at **800.234.2175** Option #2 or visit our web site at **baesystems.com/ai.**

Canadian Headquarters
BAE Systems Applied Intelligence
154 University Avenue, 2nd Floor
Toronto, ON, M5H 3Y9
Canada
T: +1 (647) 777 2000

US Headquarters
BAE Systems Applied Intelligence
120 West 45th Street
15th Floor
New York, NY 10036
T: +1800 234 2175

Global Headquarters
BAE Systems Applied Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

E: learn@baesystems.com
W: www.baesystems.com/ai

www.twitter.com/baesystems_ai

www.linkedin.com/company/baesystemsai