IBM Security

Security trends in the retail industry

Attackers are shopping for low-hanging fruit

IBM X-Force® Research

IBM

Click here to start ►

Contents

Executive overview

Despite some widely publicized attacks against major retailers, 2015 saw cybercriminals shifting their aim away from large retailers towards smaller businesses. We suspect that such was still the case in 2016, but industry analysts had difficulty assessing the true magnitude of the problem because many smaller retailers might not have reported compromises. The trend should concern large businesses because attackers may be viewing smaller businesses as routes into larger-business targets via the supply chain or payment portals.

IBM® Managed Security Services (IBM MSS) data shows that Shellshock attacks are high this year, making up more than a quarter of the threat activity observed across IBM MSS client networks, with notable activity spikes around the time of Shellshock's two-year anniversary in September[1] and again in October[2]. SQL injection and brute force attacks, long popular with cybercriminals for their proven success rate, are the second and third most frequently observed attack types.

Fingerprinting, a pre-attack technique for passively gathering information about a target system to identify weaknesses, accounts for nearly 11 percent of attack activity.

The Ponemon 2016 Cost of Data Breach Study: Global Analysis shows the financial damage to retailers continuing to escalate. In 2015, the retail sector experienced a significant increase in the cost of data, from $105 per record in 2014 to $165 in 2015. In 2016, that amount rose to $172 per record in retail, substantially above the cross-industry average of $158.

With the shopping season in full swing, we also assessed attack data from the Black Friday/Cyber Monday weekend. That might seem a good time for increased attacks, but historically we haven't seen a sharp uptick in threat activity across IBM MSS client networks. This year fared no differently, with the daily average number of attacks targeting retailers slightly lower than the daily average for the year.

Contents

It is important to note that this trend in attack activity is not a reflection of the amount of credit card fraud occurring. In fact, one report indicated that online retail credit card fraud on Black Friday through Cyber Monday was 20 percent higher in 2016 than in 2015.[3] Last year's IBM retail report highlighted the secureness of chip-and-PIN card versus chip-and-signature cards, but it's evident that the advent of the chip card hasn't solved the problem of card fraud. It has even introduced some legal murkiness, with several major US retailers filing lawsuits against credit card companies that are requiring them to allow the use of chip-and-signature cards.[4] With all the concerns plaguing the retail industry, organizations need to understand the trends and make the security investments that best apply to them. Our recommendations are meant to optimize security programs to stop advanced threats and protect retail's "crown jewels."

About X-Force

The IBM X-Force research team studies and monitors the latest threat trends including vulnerabilities, exploits, active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising customers and the general public about emerging and critical threats, IBM X-Force also delivers security content to help protect IBM customers from these threats. Threat intelligence content is delivered directly via the IBM X-Force Exchange collaborative platform, available at xforce.ibmcloud.com

Contents

The intersection of personalization, privacy and security

Consumers often seek more personalization and greater privacy of their retail accounts simultaneously, while sometimes also confusing privacy with security. Personalization cannot be delivered without some loss of privacy, and privacy and security are not the same.

In terms of data collection, privacy refers to the safe collection of information and its appropriate storage and use by the company. This collection of information allows for the personalization of the consumer's account. For instance, a consumer may provide demographic information in order to receive advertisements and coupons appropriate to their age, gender and so on. More people than not are willing to supply such details; a global survey released last year found that 54 percent of consumers are likely to share information with retailers.[5]

As retailers seek to fully implement personalization by tracking and integrating data from various devices such as smartphones, tablets and point-of-sale systems, the customer experience becomes more seamless and pleasing. However, the more data a retailer collects and integrates, the more vulnerable it becomes. Retail is already a prime target, and as its data repositories grow, it offers a data-rich environment ever more attractive to the cybercriminal.

To tackle the privacy issue, retailers should be transparent by providing an easily understood privacy policy, and consumers should be given the option of choosing when and how their data is collected and used. Consumers should also understand that many of their digital interactions leave data trails, and that finding the right balance between personalization and privacy is partly their own responsibility, not just the retailer's.

Retailers are tasked with protecting their consumers' sensitive information from the standpoint of both privacy and security. Even if businesses are collecting, storing and using information properly, they must concern themselves with the types of attacks discussed in the next section and seek ways to mitigate the exfiltration of their consumers' data.

Contents

Prevalent attacks targeting the retail industry

IBM Managed Security Services, which monitors billions of events reported every year by client devices in over 100 countries, analyzed the aggregate data we accumulated between January 1, 2016 and November 30, 2016. This data provides insight into the daily cyber experience facing the retail industry.

In this section we define an attack as a security event observed in a system or network that has been identified by correlation and analytics tools as malicious activity attempting to collect, disrupt, deny, degrade, falsify or destroy information system resources or the information itself.

The top five attack vectors, Shellshock, SQL injection, brute force, fingerprinting, and backdoors, accounted for around 74 percent of attack activity targeting the retail sector. Figure 1 breaks down the most prevalent attack vectors.

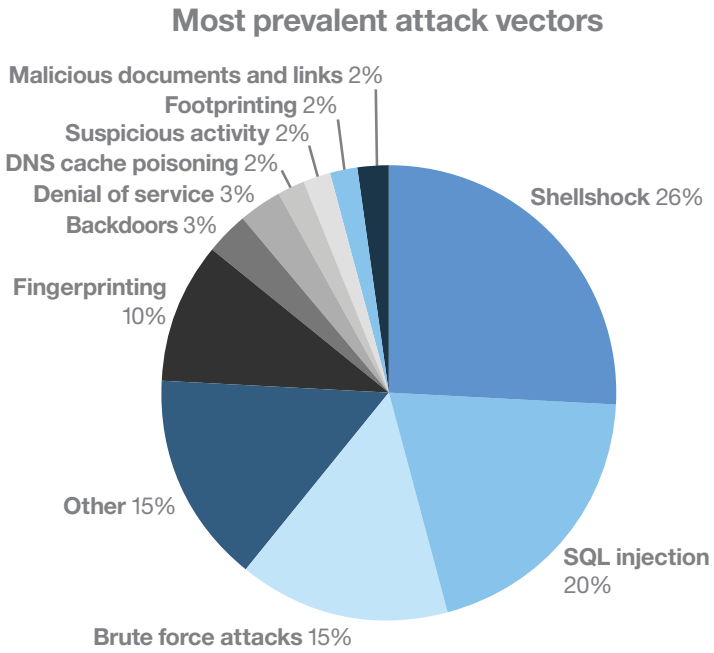

Figure 1. Most prevalent attack vectors in the retail industry. (January 1, 2016 – November 30, 2016). Source: IBM Managed Security Services data.

Contents

Shellshock

Shocking no more, Shellshock ranks as the number one attack vector, with 26 percent of all attacks. Shellshock is a vulnerability in the GNU Bash shell widely used on Linux, Solaris and Mac OS systems. September 24, 2016 marked the two-year anniversary of this threat, one of 2014's biggest headline makers in the information security sphere. As though in anticipation of its anniversary, Shellshock attack activity surged in September to levels not seen since 2015. A second wave of increased attacks was observed again in October.[6] Given such a surge, it is not surprising that in 2016 the retail industry experienced nearly twice as many Shellshock attacks as in 2015, with 60 percent of them occurring in September.

SQL injection

SQL injection is the number two attack vector targeting retailers, at 20 percent of attacks. Weak SQL database security policy is a common denominator in successful attacks. Ironically, data from the IBM X-Force Vulnerability Database shows that while attacks utilizing this threat are still widespread, the last few years have seen a substantial decline in the number of SQL injection vulnerabilities disclosed and the associated exploit code made publicly available. In fact, from 2011 to 2015 there was a 54 percent drop in the number of SQL injection vulnerabilities disclosed. The ratio of vulnerability to publicly available exploit code has also been declining. This means that attackers are carrying out successful attacks on older, unpatched SQL injection vulnerabilities.

More than half of the Shellshock attacks experienced by retailers in 2016 occurred in September, the anniversary of Shellshock's introduction.

Contents

Brute force attacks

Brute force attacks accounted for nearly 15 percent of the attacks. A brute-force password attack is a tactic in which an intruder tries to guess a username and password combination to gain unauthorized access to a system or data. Most of the attacks observed targeted the Secure Shell (SSH) service. Attackers favor SSH because it provides shell account access across the network.

Fingerprinting

Over ten percent of the attacks involved fingerprinting, often viewed as a kind of pre-attack to gather information on potential targets and discover existing weaknesses in them. Essentially, an attacker compares output from a target system to known "fingerprints" that uniquely identify specific details about the target, such as the type or version of its operating system or application. Attackers can use the information to exploit known vulnerabilities in the target organization's IT infrastructure.

Backdoors

Three percent of the attacks involved requests on certain TCP ports that indicate an attacker is running a backdoor on a compromised network. A backdoor allows someone to bypass security authentication mechanisms to gain access to a computer program. Most backdoors are placed on systems through a system compromise such as a virus or worm.

Contents

What's trending in retail?

Threat from POS malware ongoing despite some positive indicators

Point-of-sale (POS) malware, which is designed to extract customer payment card data and send it back to a command-and-control (C&C) server controlled by attackers, was seldom discussed in mainstream media until December 2013. Then, in one of the largest, most highly publicized data leaks of all time, over 100 million credit card numbers were stolen from a US retail chain.[7] The POS malware epidemic gained momentum throughout 2014 and 2015 with multiple card breaches damaging high-profile retail brands, and its capabilities continued to multiply: incorporating botnet capabilities, communicating with a central command-and-control server, deploying a keylogger on the infected systems and using creative exfiltration schemes to send data to the attackers.[8]

With this threat seemingly intensifying over the course of two years, we wanted to assess its impact during 2016. Interestingly, the IBM MSS data shows that last year's top attack vector, the use of malicious documents and sites, ranks far lower this year at only two percent of attack activity (see Figure 1). Attacks aimed at fooling victims into opening malicious documents or clicking on links to malicious sites are almost always intended to have the victim download malware. In the case of retailers, the malware is often POS-based.

This decrease in activity may indicate that more retailers are implementing best practices around protecting point-of-sale systems, such as restricting Internet access and keeping software up to date. Consequently, attackers are finding this threat vector less attractive.

As well as this observation revealed by the IBM MSS data, we see from another report[9] that in 2016 there have been fewer new malware variants targeting POS systems. Fewer new variants means security vendors can address threats in a timelier manner, reducing risk to the retailer.

Contents

Does this mean that POS malware is no longer a significant threat? No. Far from it. Although a drop-off in new malware variants and attacks using malicious documents and links is encouraging, the threat is still alive. This year several POS malware incidents have been reported, including one targeting a high-profile entertainment industry organization in which the malware went undetected for almost a year[10]—and that was just one of several 2016 incidents in which attackers were able to harvest data undetected for periods extending anywhere from three months to a whole year. And just in time for the holidays, we saw a new POS malware family, ScanPOS, distributed through a new phishing campaign.[11] Therefore we remain cautious, and we strongly advise applying the recommendations for protecting POS systems that we offer at the end of this report.

Extortion seeping into retail

The risk posed by ransomware and other extortion attacks is of growing concern across all industries. Retail is no exception. The past few years have seen a steady stream of retail ransomware incidents. In 2014, the personal data of 650,000 Belgian and French customers of an international pizza restaurant chain was leaked after a failed extortion attempt.[12] In one notable incident this year, a ransomware compromise at a US restaurant, the attackers demanded $10,000 to unlock encrypted files.[13] The FBI notified the restaurant that it was one of eight businesses targeted by overseas cybercriminals. In another extortion attack, the names, address and phone numbers of over ten million customers of a Korean e-commerce portal were stolen.[14] The ransomers demanded $2.66 million (USD) in Bitcoin for the return of the company's data.

Retail point-of-sale systems remain vulnerable as a vehicle for stealing credit card data, with a new POS malware family emerging at year end 2016.

Contents

Retail and IoT

Internet of Things (IoT) devices like smart watches and thermostats may be on consumers' holiday shopping lists this year, but attackers might have other plans for such devices. The recent record-shattering distributed denial of service (DDoS) attack against domain name provider Dyn, which used the Mirai IoT botnet, drew attention to IoT devices' increasing susceptibility to attack.[15]

Telecommunications is certainly not the only industry under attack. In June, security researchers found that over 25,000 CCTV cameras were used to carry out a days-long DDoS attack against the website of a small US-based jewelry shop.[16] Not only are retailers' websites susceptible to IoT botnets, then, but the CCTV cameras installed in their brick-and-mortar stores can be compromised and used in IoT botnets to attack other targets. Very often the IoT devices increasingly present in networks do not receive the level of security review given a new computer, so they can be easier targets for many types of attacks.

There are lots of excellent new uses for IoT in the retail space, for example detecting shoppers' location and behavior in stores.[17] Harnessing and analyzing that kind of information helps retailers deliver a smarter shopping experience to consumers. If we don't build security into these applications, however, they might well have a negative impact on both the retailer and customer. Also, IoT's presence in the supply chain creates the potential for almost complete visibility as data all the way from the manufacturer to the consumer is analyzed. Such increased visibility provides retailers with actionable information that improves efficiency, thereby reducing costs. The downside, though, is that IoT devices communicate through application programming interfaces (APIs) that are vulnerable to attack, so the attack surface grows. Breaching even one IoT device may allow an attacker to access the networks of multiple organizations and exfiltrate data or inject malware.

Contents

Attackers are shopping, not attacking

Attackers use the holiday season to their advantage via spam, phishing and compromised websites, and at this time of year we certainly see an increase in malicious holiday-themed activity. In one recent spam campaign, the emails were disguised as an official "Black Friday Deal" from a reputable site and attempted to deceive their victims with a gift card code. Another malicious campaign utilized the Locky ransomware and, at its peak, was responsible for 72 percent of all incoming spam emails analyzed by IBM Security.[18]

Surprisingly, though, IBM Security research in recent years has shown no significant uptick in attacks targeting the retail industry during the Black Friday/Cyber Monday period. This year, traffic appeared to spike on Black Friday and Cyber Monday, but over the four days of the extended weekend the attack count was actually lower than the daily average for the year (see Figure 2).

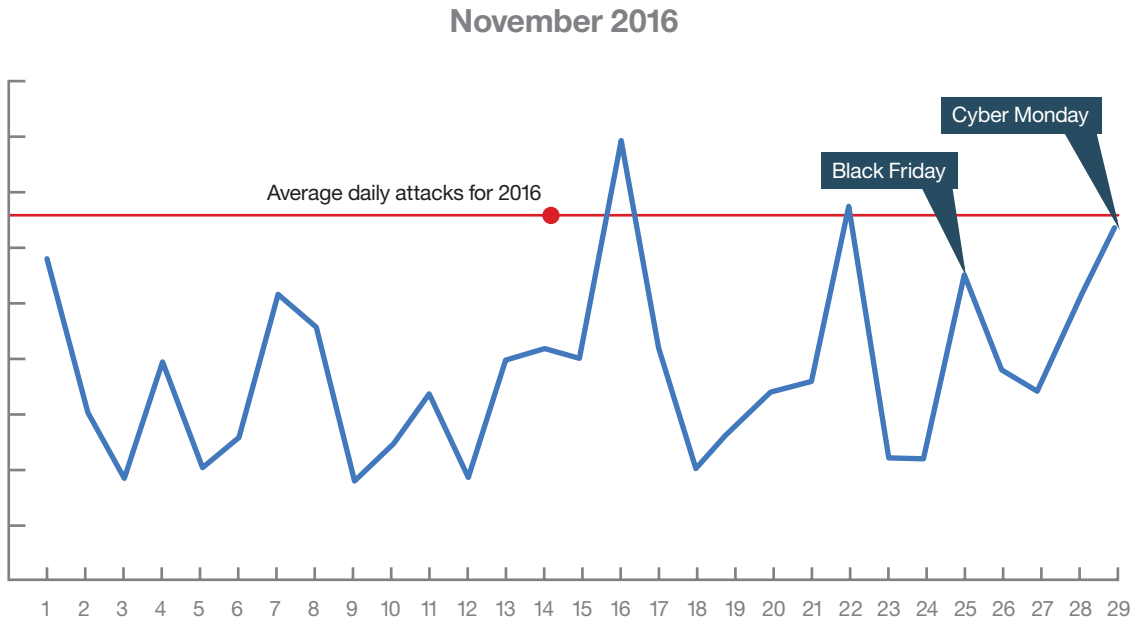

Figure 2. Daily average attack count for retailers over Black Friday through Cyber Monday was lower than the daily average for the year (November 1, 2016 – November 29, 2016). Source: IBM Managed Security Services data.

Contents

Serious compromises and attacks do of course happen during the holidays. Daily security attack volume might be lower than expected during this time because cybercriminals could be doing their dirty work earlier in the year, laying the groundwork to reap the benefits during the holiday shopping frenzy. Attackers often infiltrate systems and then spend months stealthily collecting data before any announcement is made or the target organization discovers the compromise.

It's also possible that user education has had a positive impact. There are so many warnings during the holiday season that users may actually be more wary than usual and are hesitating before they click on the dancing Santa in the holiday e-card that installs malware or the flashing "Discount" image that leads them to a malicious site. The extra seasonal vigilance may also be why there are fewer attack attempts. Why attack when everyone is watching?

Black Friday "deals," dancing Santas in ecards and flashing "Discount" images may be holiday-themed attempts to get users to click on a malicious link or download malware.

Contents

Recommendations

Attackers targeting the retail industry are less interested in taking down a site and more focused on obtaining valuable information such as credit card data. This is very different from attackers' motivations in other industries where disruption may play a bigger motivational role. Furthermore, retail industry attackers are using tried-and-true vectors like SQL injection and brute force attacks against which organizations need some basic protection.

Let's start with the basics: Identify, protect, detect and recover

While large retailers can certainly be susceptible to SQL injection and brute force attacks, smaller retailers are the more likely victims. The vulnerabilities targeted by such vectors can be characterized as low-hanging fruit and are common in smaller-business environments where the basic security measures—identify, protect, detect and recover—have not been performed. That should be of concern to large businesses because attackers may be viewing smaller businesses as routes into larger-business targets via the supply chain or payment portals. Often the problem is that small and medium-sized businesses may be unsure of where and how to begin addressing cyber security. In the US, help with that issue can be found in the National Institute of Standards and Technology (NIST) guide Small Business Information Security: The Fundamentals. Ideally, businesses and enterprises of all sizes should apply the following bare minimum recommendations.

Network visibility

Visibility into network incidents is vital. Security information and event management (SIEM) tools can give organizations of all sizes a powerful way to prevent, detect and respond to the latest threats before damage is done. Analyzing network traffic to identify security threats in real time is the key to prioritizing security incidents. Tools such as IBM QRadar® Security Intelligence Platform consolidate log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network.

Vulnerability patching

The top two attack vectors, Shellshock and SQL injection, exploit unpatched vulnerabilities, so timely patch management is critical for organizations of any size. With the analysis you gather from security intelligence and data analytics tools such as IBM QRadar and the IBM BigFix® Endpoint Management solution, you need to identify the greatest vulnerabilities in your sector and always—always!—keep your systems patched and up to date.

Contents

Mitigate brute force attacks

Many products and services today require strong passwords, but weak passwords are still helping criminals carry out successful brute force attacks. Enforce strong passwords that don't allow dictionary words or words that appear in common password lists. Lock an account after three to five failed login attempts. Make error messages returned for all types of failed logins identical so attackers can't tell whether a valid user ID has been used but a wrong password entered, or vice versa. Do not allow direct login to administrator accounts. Further recommendations can be found in the IBM Report Beware of older cyber attacks.

Protect POS systems

The threat from POS malware appears to be diminishing slightly, but retail organizations should still secure their endpoint sales mechanisms against POS malware. At a minimum, we strongly recommend implementation of the best practices outlined in last year's retail report.

Protect your enterprise while reducing cost and complexity

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your company's critical assets. We protect some of the most sophisticated networks in the world and employ some of the best minds in the business.

IBM offers services to help you optimize your security program, stop advanced threats, protect data and safeguard cloud and mobile. Security intelligence Operations and Consulting Services can assess your security posture and maturity against best practices in security. With IBM X-Force Incident Response and Intelligence Services, IBM experts proactively hunt and respond to threats, and apply the latest threat intelligence before breaches occur. With IBM Managed Security Services, you can take advantage of industry-leading tools, security intelligence and expertise that will help you improve your security posture—often at a fraction of the cost of in-house security resources.

Contents

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world's broadest security research, development and delivery organizations, monitors billions of security events per day in more than 130 countries, and holds more than 3,500 security patents.

About the author

Michelle Alvarez, a Threat Researcher and Editor for IBM Managed Security Services, brings more than 10 years of industry experience to her role. Michelle is responsible for researching and analyzing security trends and developing and editing security and threat mitigation thought leadership papers. She joined IBM through the Internet Security Services (ISS) acquisition in 2006. At ISS she served as an analyst and contributed to the development of the X-Force Database, one of the world's most comprehensive threats and vulnerabilities database. For many years, Michelle played an important operational role within the Information Technology-Information Sharing and Analysis Center (IT-ISAC), a non-profit, limited liability corporation formed by members within the information technology sector. She is a regular contributor to the IBM-sponsored security blog, SecurityIntelligence.com, and has her master's degree in information technology.

Contributors

Scott Craig – Threat Researcher, IBM Security

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

For more information on security services, visit:
ibm.com/security/services

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog

Contents

References

[1] https://securityintelligence.com/shellshock-anniversary-major-security-flaw-still-going-strong/

[2] https://securityintelligence.com/researchers-detect-second-wave-shellshock-attacks-since-two-year-anniversary/

[3] http://www.darkreading.com/analytics/holiday-weekend-online-payment-card-fraud-20--higher-in-2016-/d/d-id/1327610

[4] http://www.bankrate.com/finance/credit-cards/how-lawsuits-over-chip-and-pin-affect-consumers.aspx

[5] https://www.sas.com/content/dam/SAS/en_us/doc/research1/balance-between-personalization-privacy-107399.pdf

[6] https://securityintelligence.com/researchers-detect-second-wave-shellshock-attacks-since-two-year-anniversary/

[7] http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

[8] https://securityintelligence.com/the-pos-malware-epidemic-the-most-dangerous-vulnerabilities-and-malware/

[9] http://www.eweek.com/security/pos-malware-declines-as-spam-volume-grows-sonicwall-reports.html

[10] http://notice.themadisonsquaregardencompany.com/customerupdate/

[11] http://www.morphick.com/resources/lab-blog/scanpos-new-pos-malware-being-distributed-kronos

[12] http://www.theguardian.com/technology/2014/jun/16/dominos-pizza-ransom-hack-data

[13] http://www.wusa9.com/news/local/rockville/scam-artists-hack-restaurant-computer-demand-10k/102424542

[14] http://www.koreatimes.co.kr/www/news/nation/2016/07/116_210566.html

[15] http://www.fiercetelecom.com/telecom/dyn-confirms-friday-ddos-attack-was-based-mirai-botnet

[16] https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html

[17] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=AB&infotype=PM&htmlfid=WWC12356USEN&attachment=WWC12356USEN.PDF

[18] https://exchange.xforce.ibmcloud.com/collection/Amazon-Cyber-Week-Spam-Campaigns-c2ad3c53d2e3a5432024a6a137ab233c

Contents

IBM Security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
December 2016

IBM

SEL03121-USEN-00