ALERT LOGIC®

CLOUD SECURITY REPORT

The Changing State of Cloud Security

ALERT LOGIC®
Security. Compliance. Cloud.

2015

ALERT LOGIC®

CLOUD SECURITY REPORT 2015

INTRODUCTION 4

EXECUTIVE SUMMARY 5

THE METHODOLOGY 6

THE FINDINGS 9

- Environment Analysis 9
- Threat Vector Analysis 12
- Industry Analysis 16

CONCLUSION 22

APPENDIX 24

ALERT LOGIC®

INTRODUCTION

Alert Logic provides managed security and compliance solutions for over 3,000 customers around the globe.

As part of our cybersecurity research practice, we review threats and attacks against our vast customer base on a regular basis, looking for insight to share in our annual *Cloud Security Report*. Using the attack data we collect across thousands of organizations and a wide variety of industries—with IT infrastructure deployed across on-premises, hosting, and public cloud environments—our findings are representative of the current threats and attacks many organizations experience today.

For this report, we employed our big data security analytics engine to analyze over one billion events and identify over 800,000 security incidents. These incidents range in severity from "Review at your earliest convenience" to "You are under a targeted attack; deploy countermeasures immediately."

Unlike other security reports that offer a generalized analysis, our report is based on real data: our customers' data, our analysis, and our stories. We believe that this firsthand accounting of attacks against cloud environments can provide insight into how to better secure your IT environments, protect your customer data, and ultimately continue to grow your business.

We hope that you find this report informative and valuable, and that it bolsters your efforts for continually improving the security framework of your business.

- Alert Logic Research Team

EXECUTIVE SUMMARY

Cyber attacks are on the rise. Companies both large and small are targeted daily by hackers seeking valuable data to monetize in the cyber underground. Recent reports show that 87% of organizations are making use of cloud infrastructure[1], while analysts predict spending will exceed $200 billion[2] in 2016. This means: 1) Organizations are making use of public clouds now more than ever before, and 2) Hackers now have a larger attack surface to gain access to sensitive data. It is imperative for organizations to understand the attack methods being used to compromise their environments, so they can prepare a defense strategy when they become the target of an attack.

As cloud growth continues, our data is telling a familiar story. Our 2015 research not only reinforces our previous *Cloud Security Report* findings, it also uncovers new insights that can prove valuable to organizations when building out their security framework.

CLOUD ADOPTION REMAINS STRONG: In 2014, we continued to see an increase in attack frequency for organizations with infrastructure in the cloud. This is not surprising—production workloads, applications, and valuable data are shifting to cloud environments, and so are attacks. Hackers, like everyone else, have a limited amount of time to complete their "job." They want to invest their time and resources into attacks that will bear the most fruit: Businesses using cloud environments are largely considered that fruit-bearing jackpot. However, attackers are not abandoning attacks against on-premises data centers; they are simply applying more pressure to businesses with applications in the cloud. Their hypothesis, which in some cases may be true, is that businesses have a misconception about the security they need in the cloud. Some businesses, attackers have found, mistakenly assume cloud providers take care of all their security needs. The reality, however, is that security in the cloud is a shared responsibility.

INDUSTRY AND CUSTOMERS DRIVE YOUR THREAT PROFILE: This year we performed industry analysis, looking for trends in attack types. As the analysis progressed, we noted a distinct difference between businesses that primarily service their customers online, and those that do not. This indicates a new level of sophistication in the way attackers are approaching infiltration—a fact that perhaps appears obvious but is underrepresented in research. It is clear from our data that of the many factors influencing a business's threat profile, interaction with the customer plays a major role. Businesses with a significant online presence for customer interaction are the targets of application attacks far more than those businesses that interact with their customers by other means. For those businesses that have smaller online presences, we find attackers are using traditional means of infiltration, such as Brute Force and Trojan attacks. Understanding what drives your threat profile is key to determining the time and investment necessary for a successful security-in-depth strategy.

KILL CHAIN CONSTRUCT DRIVES UNDERSTANDING: Today's attackers are a sophisticated lot, using advanced techniques to infiltrate a businesses environment. Unlike in the past when hackers primarily worked alone using "smash-n-grab" techniques, today's attackers work in groups, each member bringing his or her own expertise to the team. With highly skilled players in place, these groups approach infiltration in a much more regimented way, following a defined process that enables them to evade detection and achieve their ultimate goal: turning sensitive, valuable data into profits. This year, we dive deep into the Cyber Kill Chain®[3], a construct developed by Lockheed Martin, to provide insight into an attacker's behavior, from initial reconnaissance activities to ultimate data exfiltration.

YOU CAN STAY AHEAD OF THE ATTACKERS: In this report, we also provide recommendations to help organizations improve their security posture—a handy checklist that you can share with your team to start the conversation of bolstering your security.

[1] http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2014-state-cloud-survey
[2] http://allthingsd.com/20120709/public-cloud-and-telecom-to-lead-3-6-trillion-in-it-spending-this-year-garner-says/
[3] http://cyber.lockheedmartin.com/cyber-kill-chain-lockheed-martin-poster

THE METHODOLOGY

HOW WE COLLECT & ANALYZE THE DATA

The Customers

We categorize our customer data into two groups: on-premises (formerly called enterprise data center) and cloud (formerly called cloud and hosting providers). On-premises data center customers invest in a dedicated, in-house IT infrastructure. Cloud customers consume Infrastructure-as-a-Service solutions from a cloud provider.

The Data

The data used in this report is real-world incident data detected in customer environments secured via Alert Logic's network intrusion detection, log management, and web application firewall products. To eliminate noise and false positives, Alert Logic® utilizes our patented correlation engine, Alert Logic® ActiveAnalytics™, which evaluates multiple factors to determine whether events are relevant security incidents. Finally, the ActiveWatch™ team, Alert Logic's in-house security analyst group, reviews each incident for validation, further reducing false positives.

This year, we expanded the scope of the report, including a full 12 months of event and incident data compared to previous reports, which were based on six-month intervals. While the amount of overall incidents is obviously greater in this full-year report, a comparison with past reported results provides an interesting trend analysis.

Event vs. Incident

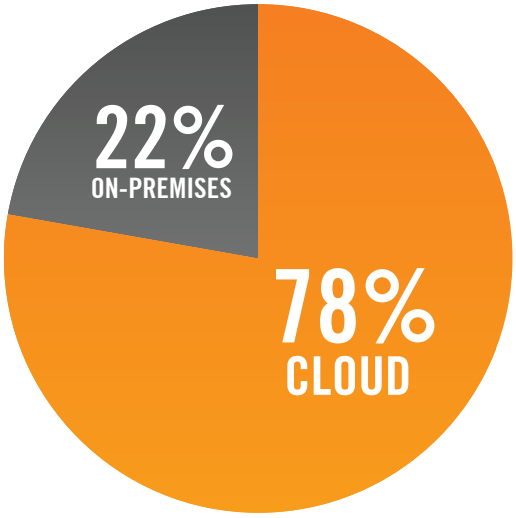
We categorize an event as evidence of suspicious behavior detected via an Intrusion Detection System (IDS) signature, log message, or web application request. We define an incident as an event or group of events that have been confirmed as valid threats based on correlation and advanced automated analysis by Alert Logic ActiveAnalytics, and verification by a certified ActiveWatch analyst.

ALERT LOGIC CUSTOMER DATA SET*

842,711 incidents over 365 days

(2308 actual attacks per day average)

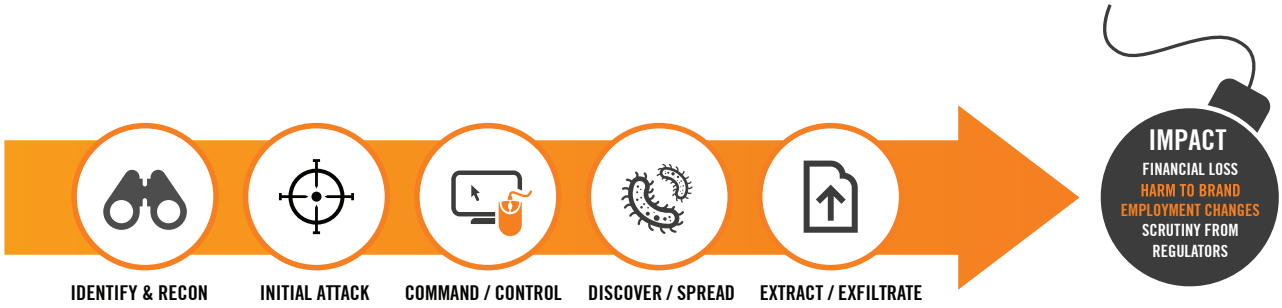
- 3,026 customers
  - 2387 Cloud**
  - 639 On-Prem
- 16 different industries (SIC codes)



* Customer data set (78/22) – Percentage of total customers by deployment

**Cloud customers include both customers whose applications and infrastructure are deployed in public cloud environments (such as AWS) and those who have applications and infrastructure in place with a hosting provider (such as Rackspace)

The Analysis: Cyber Kill Chain® Approach



The Alert Logic Security-as-a-Service solution is designed to identify threats at any point along the Cyber Kill Chain®. Lockheed Martin's Computer Incident Response Team developed the Cyber Kill Chain® to describe the different stages of an attack, from initial reconnaissance to objective completion. This representation of the attack flow has been widely adopted by organizations to help them approach their defense strategy in the same way attackers approach infiltrating their businesses. As malicious activity continues to threaten sensitive data—whether it is personal data or company-sensitive data—one certainty remains: Attackers will continue to infiltrate systems. The best opportunity to protect all types of sensitive data is to understand how attackers operate.

In order to better understand the 2014 data presented in this report, as well as how attacks operate, the following fictional case was created to map out an attack, categorizing each attack activity in the context of the Kill Chain. The fictitious company in this case is known as XYZ, Inc. XYZ sells its products to consumers in brick and mortar stores as well as online and via mobile apps. XYZ has experienced explosive growth since the introduction of its latest product, and has expanded its data center footprint into the cloud to make ordering products easier for customers.

The hacker group, EchoBravo (EB), has been tracking XYZ for quite a while. XYZ's growth and significant online presence makes the company a desirable target for EB, with valuable data that could net a sizable profit from its sales in the cyber underground.

EXAMPLE ATTACK: HOW ECHOBRAVO TAKES DOWN XYZ, INC.

STEP 1: IDENTIFY AND RECON EB begins by scanning XYZ's public-facing websites, gathering as much information about the sites as possible. Simultaneously, EB performs scans against the XYZ internal network, looking for possible vulnerabilities and/or holes in its perimeter protection. Lastly, EB scours popular social media networks, learning as much as possible about XYZ's employees, partners, suppliers, and employees' families and friends, which can be utilized for the purpose of social engineering. After several months of monitoring, EB has identified multiple potential entry points into the XYZ network and is now primed to initiate the attack.

STEP 2: INITIAL ATTACK EB will be using several attack vectors, deployed from different regions of the world to gain access to the XYZ network. Based on the reconnaissance findings, EB will attempt to execute a targeted, sophisticated attack against XYZ's e-commerce site. EB will also attempt to distribute malware via phishing emails and social engineering with the intent of misleading an employee to click a link that permits malware to enter the network. Finally, EB will attempt a Brute Force attack to gain access to the XYZ network. Using different IP addresses and a significant number of computers, EB hackers will kick off an automated dictionary attack. After only a few short days, EB's campaign is successful and malware is installed on the victim's computer.

STEP 3: COMMAND & CONTROL With the malware in place, EB now begins a "low and slow" in-depth recon against the internal network. With command and control over the victim's computer, EB disables several security controls on the machine, attempts to escalate privileges on the victim's account, and creates a new user account with privileged access.

STEP 4: DISCOVER AND SPREAD With unfettered access to the network, EB begins to spread malware across XYZ's environment through network shares, unsecured servers, USBs, and network devices, while simultaneously creating a detailed map of the company's network, security controls, and new public cloud data center. EB now has a significant presence in XYZ's network. So EB waits, making detailed asset maps, noting employee patterns and other information that can assist in the data theft.

STEP 5: EXTRACT AND EXFILTRATE After a suitable amount of time has passed, EB begins to siphon data out of the XYZ environment. EB moves the targeted data to a remote server, taking additional steps to prevent a trace of the data's location. After several months of siphoning data, EB ends the campaign. However, before exiting, EB makes several network modifications that will enable the group to return at any time in the future.

The final step not represented in the Kill Chain—but a significant step nonetheless—is when XYZ finally discovers the compromise. Recent reports show that on average it takes more than 200 days to detect a breach[1], and the majority of breach notifications come from an outside party. This is exactly what occurs for XYZ. Several months after EB's campaign is completed and XYZ's data is converted to cash—or Bitcoin—XYZ is notified by government officials that some data linked to the company was purchased by an undercover operative on a popular dark website. XYZ then goes into recovery mode, kicking off many costly (both in terms of real dollars and reputation) actions to restore its network security posture and protect its customer data.

In this example, XYZ did not have the tools, technology, or expertise in place to detect EB's activities at any point across the Kill Chain. Fortunately, many organizations do have at least some form of defense. While some defense is better than none, it's imperative that organizations approach securing their environments with the mindset of the attacker. This perspective will help uncover the weak spots in any framework and keep organizations one step ahead of attackers.

[1] M-Trends® 2015: A View from the Front Lines

THE FINDINGS

Environment Analysis

This report generates insights based on over 800,000 verified security incidents, derived from over one billion events observed between January 1 and December 31, 2014. This data was collected from over 3,000 organizations across multiple industries from around the world. For a full list of the partners included in this report, see Appendix Figure D.

Cloud vs. On-Premises

For the calendar year of 2014, we analyzed customer data across cloud and on-premises environments, and the overall trends determined from this data tell a familiar story. As we continue to see organizations take advantage of new options for housing their most sensitive data, attack vectors are continuing to converge. As is evident with the growth reported by public cloud providers—such as Amazon Web Services (AWS)—it is clear that organizations of all shapes and sizes are making use of the more affordable and efficient cloud infrastructure. Attackers are seeing this trend as well and are making concerted efforts to infiltrate businesses making use of cloud environments, just as they previously did with physical data centers.

ABOUT APPLICATION ATTACKS IN ON-PREMISES ENVIRONMENTS

Stephen Coty, Chief Security Evangelist

Internal applications (ERP, CRM, Databases, etc.) are the backbone of most organizations, making them desirable targets for the motivated attacker. Attackers will resort to virtually anything to take control of an asset that:

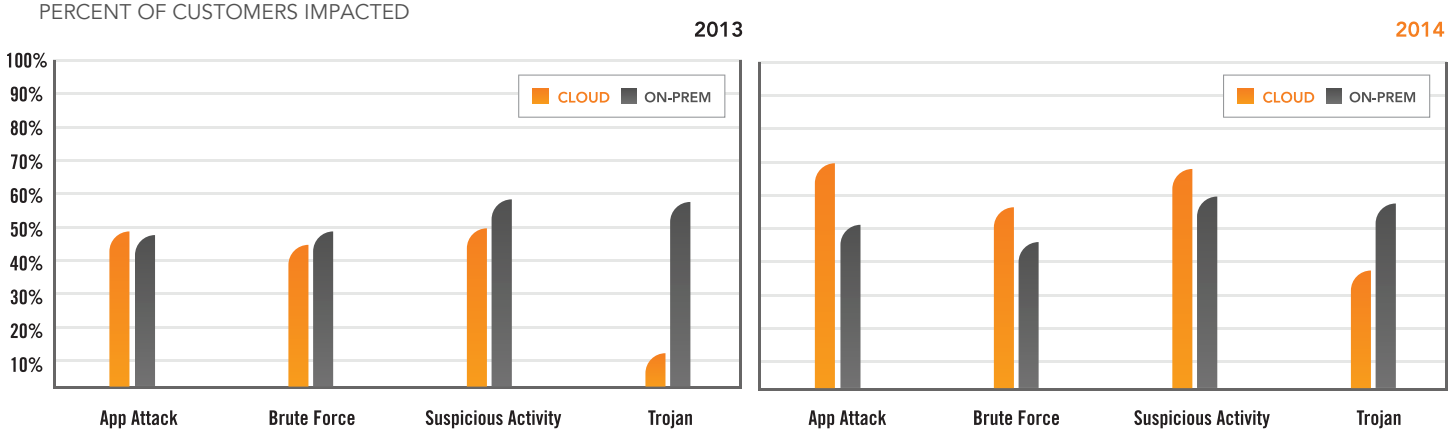
- Has been integrated into many other applications for support, data, and notifications
- Is typically used for many years with very little maintenance or patching of known vulnerabilities
- Is accessed by all employees, providing a rich set of credentials that can be comprised

If an attacker penetrates a network and installs a key logger, the attacker can then capture the keys to the kingdom: user credentials. With credentials in hand, the attacker has unfettered access to an organization's application and the valuable data it can access. The attacker, understanding the security framework, can then work to evade detection and slowly siphon sensitive data for days, weeks, months, or even years. The end result, unfortunately, could be significant long-term damage to the business's reputation, resulting in a costly investment to determine the extent of the breach and protective measures.

It is vitally important to secure and monitor internal applications for malicious activity, similar to securing a customer-facing application. It is imperative to not be lulled into a false sense of security simply because internal applications are not intended for customer interactions. Internal applications require the same level of protection as external applications.

INCIDENT OCCURRENCE

PERCENT OF CUSTOMERS IMPACTED



TOP THREE INCIDENT CLASSES

YEAR-OVER-YEAR COMPARISONS

CLOUD ENVIRONMENTS

App Attack

45% INCREASE

Suspicious Activity

36% INCREASE

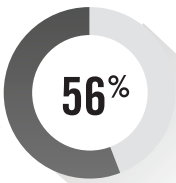
Brute Force

27% INCREASE

ON-PREMISES DATA CENTER

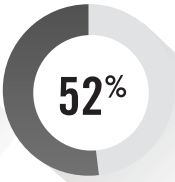
Suspicious Activity

3% INCREASE



Trojan

1% INCREASE

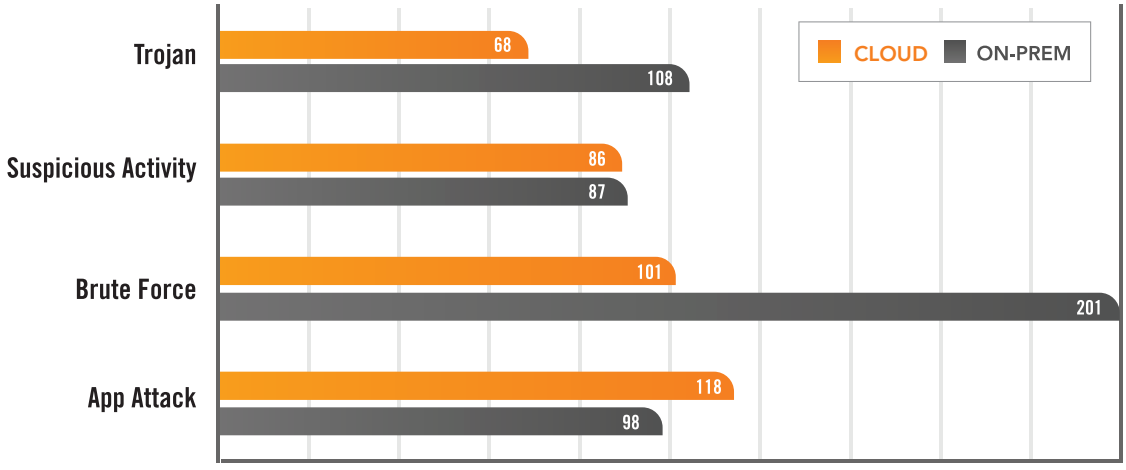


App Attack

6% INCREASE

INCIDENT FREQUENCY

AVERAGE NUMBER OF INCIDENTS PER IMPACTED CUSTOMER



On-Premises

Overall, the attacks we detected for our on-premises customers did not vary materially from previous years, with applications remaining a high-value target for attackers. Brute Force attacks in on-premises environments were less frequent than in 2013. Of this incident type, the top three attack vectors were WordPress, SSH and SMB, together comprising 79% of the total Brute Force attacks. (WordPress, in particular, is a popular open source content management system that, according to Forbes, is used by more than 60 million bloggers sites[1].)

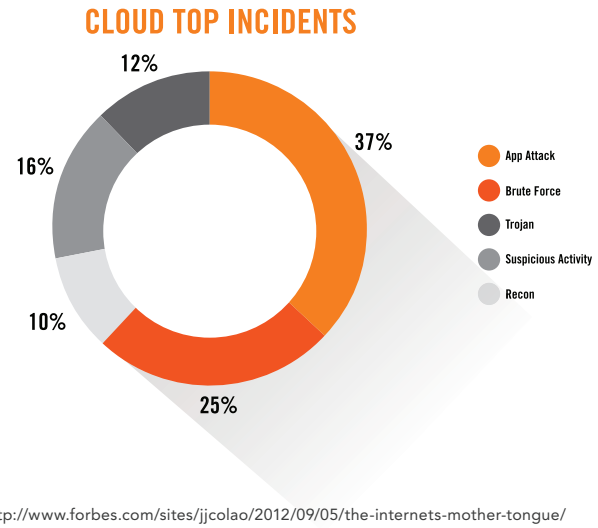
Most of these failed attempts to log into devices came from scripts running on other compromised devices. The majority of these exploitations occur through vulnerable plugins and themes.

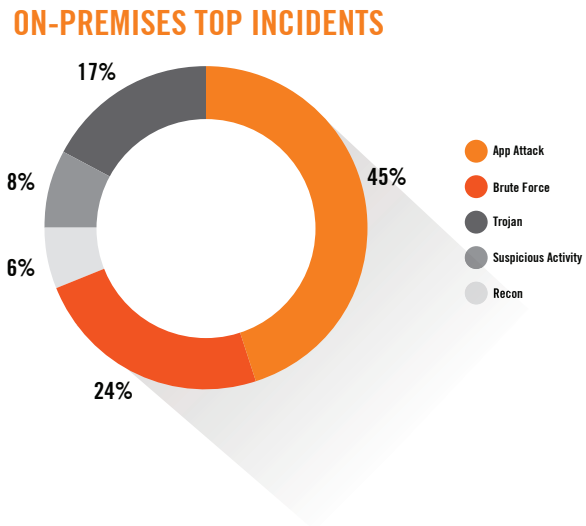
Our data also revealed a downturn in the various forms of Trojan activity in the on-premises environment. Redkit—a popular but not widely distributed exploit kit that efficiently allows you to distribute malware—was the most utilized malware in Trojan incidents. This particular malware usually redirects targets to the malware kit when browsing compromised sites. In the last year, several media sites were compromised to deliver variants of the malware kits, which in turn delivered more malicious code, such as credential stealers or remote access Trojans. This relatively flat 2014 trend, in regards to on-premises data center attacks, is not surprising. Attackers understand how to penetrate these environments and continue to use what they perceive to be effective attack vectors. Since on-premises data centers are certainly not becoming obsolete in the foreseeable future, it is important that organizations continue to invest in their security framework for all of their physical data centers, applications, and mission-critical infrastructure.

Cloud Environments

2014 was quite a year for public clouds. Competition between the major providers heated up, leading to a wide array of affordable options for businesses taking advantage of cloud. With such attractive options, we saw a continued increase in infrastructure migration to the cloud, resulting in a direct increase in attack percentages detected for our customers using cloud environments. Application attacks remain the prevalent mode of attack for organizations using the cloud.

Reconnaissance increased significantly in 2014. Some of the most common scans we detected included ZmEu, Morfeus, VNCScan, and Nessus scans, as well as multiple generic scans. Suspicious activity increased slightly as well, indicating more unknown or unfamiliar activity around our customers' environments. While some of this activity included legitimate penetration testing and security audit tasks, there was certainly more activity by suspicious actors in search of an effective means for compromising our customer environments.





[1] Source: http://www.forbes.com/sites/jjcolao/2012/09/05/the-internets-mother-tongue/

INFOCUS: APT17

Cybercrime Research Team, ActiveIntelligence

Crackers. Hackers. Bad Actors. You wouldn't invite any of them into your home. But they often show up uninvited. Every day, we observe targeted attacks. Some are relatively sophisticated, while others employ a combination of commercial malware with a cleverly crafted email. One recent, more sophisticated attack leveraged seemingly benign public posts through Microsoft TechNet forums. APT17 used crafted malware to poll these posts and searched for the specific tags "@MICR0S0FT" and "C0RP0RATI0N," which they used to publish the attackers' Command & Control [C2] addresses. The collected data was then encapsulated within an image file and delivered to the specific C2 resource. This method was previously employed on Twitter and Facebook; it allows public-facing infrastructure to be repurposed for malicious use, generally unbeknownst to the victim.

APT17 is a group of Chinese actors tasked with what we believe to be specific targeting and intelligence-gathering missions. This group often relies on the end user to create the initial infection vector; this is generally achieved through phishing or spear phishing emails. Once an attacker has cemented access into a compromised environment, he/she will begin to monitor and analyze the environment, perform lateral movements, and then ultimately carry out the exfiltration of data. This supports the attacker in various ways—credential harvesting, information leakage, confidential data theft, and personal data theft. Attackers can then move on to the marketing element: Advertise the data, sell the data, and reap the financial gains.

End users should always be wary of opening email attachments from unexpected senders, clicking links on unknown websites, and using software, codecs, and programs from unknown sources. Where possible, users should review access requirements with IT to ensure they are secure. As with most malware, we can seek out specific information to aid us in detecting attacks. This is normally linked to the C2 addresses, the type of malware, the email sender, the connecting infrastructure, or even hard-coded information within the malware. However, detection and protection against the most sophisticated attacks can be troublesome, so users should ensure they are up to date with vendor patches for their operating system and software. They should also consider whitelisting connectivity requirements and adhere to a least-privilege method of access to decrease opportunities for malware to take control. It could be the difference between a successful and unsuccessful exploit.

Threat Vector Analysis

Among the one billion events and 800,000 security incidents identified in 2014, we detected almost every type of attack imaginable. A holistic review of the data revealed the prevalence of particular attack types, which we examine below.

Reconnaissance

As mentioned, the first step in a well-coordinated attack is reconnaissance—the process of building a picture of the business's environment an attacker plans to infiltrate. This reconnaissance process allows the attacker to determine which applications, services, and vulnerable products may exist before launching an attack.

Reconnaissance, as this year's data reveals, has become more prevalent across all industries. This change speaks volumes to the motives and objectives of today's threat actors. Today, attackers are not interested in a smash-and-grab approach to compromise. Rather, they are playing the "long con" game. When attackers identify their targets, they work to gather as much knowledge as possible before launching an assault.

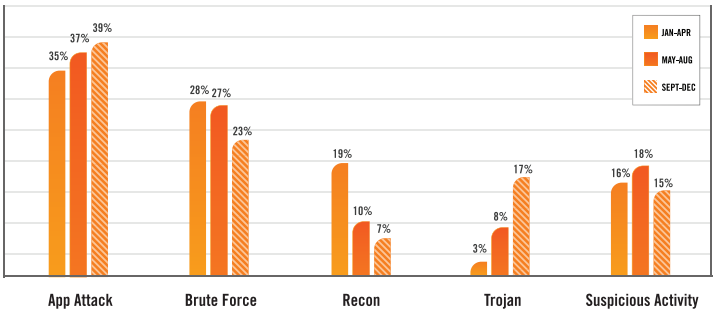
To gain a full picture of an organization's environment they intend to exploit, attackers must invest time and effort into "casing the joint." Not unlike the bank robbers of the past who frequently visited their targeted banks for days, weeks, even months before the actual robbery, attackers will monitor a targeted organization's environment for extended periods of time. The thorough attacker will take note of all external-facing websites and applications, the ports accessible via the Internet, and any vulnerability that may exist in the network infrastructure. With this information, the attacker can construct a plan to quietly infiltrate the environment.

Detecting recon activity is a first line of defense and is essential to staying ahead of an attacker. Every industry is susceptible to recon activity. According to our data, no single industry was more susceptible than another. It is only after recon is complete that attack vector variances from industry to industry can be identified.

After comprehensive recon is complete, an attacker will know which type of attack vector will be the most effective. From our data, there are three primary attack vectors seen across many industries: application, Trojan, and Brute Force attacks.

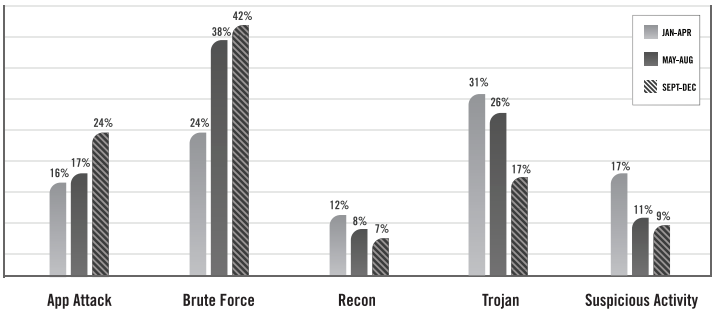
INCIDENT OCCURRENCE OVER TIME

CLOUD ENVIRONMENTS



INCIDENT OCCURRENCE OVER TIME

ON-PREMISES



Application Attack: Tried and True for a Reason

Application attacks are by far the most common threat we detect in our customer environments. This isn't necessarily surprising, since applications—whether internally or externally facing—provide the gateway to sensitive data. That said, an industry-by-industry analysis shows application attack frequency varies by industry sector. For instance, application attacks are frequently detected in Transportation & Public Utilities sector customers. In fact, over 80% of all attacks detected for these customers are application attacks. Conversely, application attacks account for only a small portion of attacks against our Mining, Oil & Gas customers, due to the limited customer-facing applications deployed in that industry.

These results reinforce the conclusion that customer interaction dictates attack type. The vast majority of our Transportation & Public Utilities sector customers have extensive external-facing application deployments. The applications vary from traditional websites to mobile applications and everything in between. Attackers are aware of this and take every opportunity to uncover vulnerable applications that will provide access to a wealth of customer data.

The Real Estate industry, which historically thrived on paper, postal service, and telephones, has now moved many of its services and applications to the cloud, providing easier access for their customers. Today, everything from conducting an initial home search to finalizing a home purchase can be completed online, largely due to the industry's recent embrace of new Software-as-a-Service (SaaS) applications. This is clearly reflected in the Real Estate industry attack profile; over half of the malicious activity we uncovered was comprised of application attacks.

Real Estate and its associated businesses offer enticing data for attackers, which can be sold in underground markets to facilitate identity theft and fraud. Consumers purchasing homes provide a variety of personally identifiable information (PII), such as name, address, phone number, government-issued identification, email, and financial information (both earnings and spending habits), which represents a windfall for attackers. This information, purchased in the underground, allows someone to establish fraudulent credit and run up large

APPLICATION ATTACK

An attempt to exploit an application to harm, destroy, or access the data stored in the application. Examples of application attacks include SQL Injection and the HeartBleed exploit.

sums of debt that will never be repaid. The impact on these fraud victims can be far-reaching and long lasting, requiring consumers to complete extra verification steps each time they need to establish new credit.

Looking at the industry verticals as a whole within our cloud customer environments, we see that almost all sectors are experiencing application attacks. This confirms the reality that the demand for public-facing infrastructure, such as web services or applications, continues to grow. Regardless if it is online banking, shopping, review research, health, or insurance, the public wants easily accessible services and applications. Malicious actors know this, and will carry out premeditated attacks to specifically compromise these applications.

Trojan

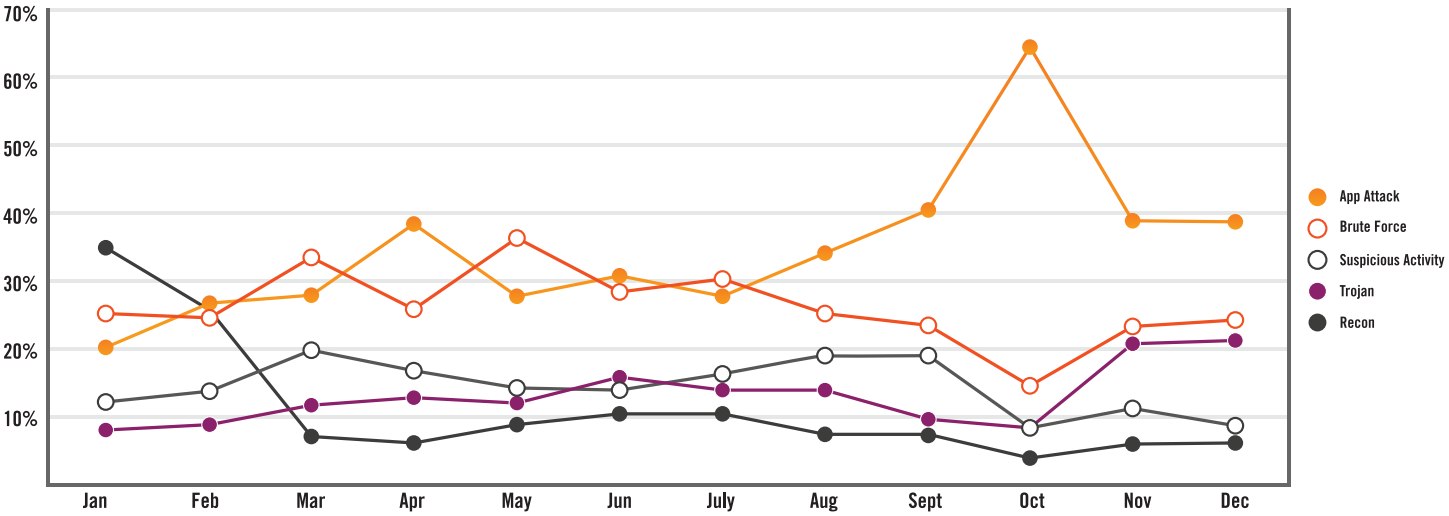
Trojan malware, or non-replicating malicious code that executes a specific task, can be inadvertently downloaded from compromised legitimate websites, or sent by emails applying social engineering techniques. This makes the Trojan attack an effective option for intrusion by malicious actors.

With the varied means by which they can be injected into an environment, as well as the damage they can cause once they penetrate and execute, the Trojan infection and subsequent rogue activities it initiates can leave an organization in shambles. We detect numerous Trojan attacks daily across many industries, particularly with our Agriculture, Forestry, & Fishing industry customers. Since there is little customer interaction required online, our customers in this sector deploy few public-facing applications, making application attacks a poor choice for the attackers. However, the distributed nature of the Agriculture, Forestry, & Fishing industry—with its many remote outposts and employees accessing high-value information—makes it a perfect target for a Trojan attack.

In a global industry like Agriculture, with so many cost pressures, knowledge of innovative techniques to reduce costs and increase yields, as well as indicators of future price changes, are extremely valuable to competitors. Trojan malware is an ideal technique for attackers to gain a foothold in an organization, allowing them to take control of the infected system and reach their ultimate goal: turning your data into profits in the underground.

MONTH-TO-MONTH ATTACK SPREAD

% OF ATTACKS OVER 2014



Potentially any industry is at risk of this attack type, but the presence of valuable information to steal, and the difficulties ensuring security across distributed organizations, leaves industries like Agriculture at a particularly high risk.

Brute Force Attacks

A Brute Force attack can be an effective way to compromise a network, given the ease at which it can be executed by attackers. With simple tools and computing power, an attacker can bombard a network with username/password combinations from different IP addresses. Unfortunately for organizations, the IP addresses constantly change, making it difficult—if not impossible—to block this type of attack. Additionally, businesses are sometimes unable to simply lock out usernames after failed login attempts, since doing so could wreak havoc on normal business operations. If a Brute Force attack is successful, the attacker will gain access to the network, application, or other asset. With this access, the attacker can begin making lateral moves within the network to establish a footprint for continuing and ultimately completing the attack campaign.

BRUTE FORCE

An attempt to gain access to a system by repeatedly trying different users names and passwords or cryptographic keys until the correct username/password combination or correct key is found. An example would be a dictionary attack against an ftp or email server.

We see Brute Force attacks across most of our customers; however, the highest occurrence of this attack type is within Computer Services, Transportation & Public Utilities, and Service Businesses. This makes sense, because our customers in these industries have a significant number of employees who work exclusively on computers, meaning these businesses employ large numbers of applications, servers, and systems. These are target-rich environments for attackers.

INDUSTRY ANALYSIS

INDUSTRY MATTERS, BUT ONLINE PRESENCE REALLY MATTERS

While reviewing attacks by network type revealed certain trends in 2014, we also uncovered an even wider divergence of threats—as compared to previous reports—when categorizing incidents by industry type. The result: Threats vary greatly on a variety of industry-specific factors, including:

- Online Presence
- Customer Interactions
- Employee Activities
- Security Controls and Effectiveness
- Business Sector

The largest influencers in attacker threat vectors are a business's online presence and how it interacts with customers. Taking a closer look, we reached a conclusion: The amount of online interaction a business has with customers determines the attack vectors that were most widely used against it, more so than the type of IT infrastructure they use. This makes perfect sense, once you examine the evidence behind this statement.

Consider a business that sells to consumers online (e-commerce). To be successful, that company would ensure multiple routes for online customer interactions via mobile devices. The business would also process thousands of transactions a day, making it an enticing target for attackers in search of credit card data to sell on the cyber underground.

Conversely, consider a business that has limited online customer interactions, such as a heavy equipment manufacturer. These businesses engage in significantly fewer online transactions—many of their sales come after a number of person-to-person interactions. In some instances, where the industry's products are large and take multiple months to deliver, there may be very little data of value accessible via external web applications. Because of this, attackers targeting this industry would search for ways to infiltrate the organization's network to capture company-sensitive data, such as product designs, financials, and proposal information. This data, while not desirable to the identity thief seeking information in the cyber underground, would be very valuable to the company's competitors.

The takeaway here is simple: Businesses with a large volume of online customer interactions are targets for web application attacks to gain access to customer data. Businesses with few online customer interactions are more likely to be targeted for their proprietary company data, not their customer data, using vectors such as Brute Force or phishing attacks.

With customer data from dozens of industries at our disposal, we selected three industries for a detailed analysis: Mining, Oil/Gas & Energy, Retail, and Financial Services. These industries exhibit interesting attack profiles that can provide insight into the state of cloud security today, not only for those in these industries, but for everyone.

TOP TEN INDUSTRY ATTACKS

54% **ADVERTISING**
APP ATTACKS

48% **COMPUTER SERVICES**
APP ATTACKS

33% **FINANCIAL**
BRUTE FORCE

39% **HEALTHCARE**
BRUTE FORCE

46% **MANUFACTURING**
APP ATTACKS

37% **ACCOUNTING / MGMT**
BRUTE FORCE

79% **MINING**
TROJAN

55% **REAL ESTATE**
APP ATTACKS

45% **RETAIL**
APP ATTACKS

71% **TRANSPORTATION**
APP ATTACKS

ALERT LOGIC®

Mining Analysis

The Mining, Oil/Gas & Energy industry is a prime target for cyber attacks primarily due to the value of its data in the world market. Protected information includes valuable geophysical data, like measurements of the earth's gravity and magnetic fields to determine the geometry and depth of subsurface areas where oil and gas are located. Companies spend significant sums to gather this research, and their findings typically dictate their strategy for years to come. It is understandable why attackers seek this information. There are those willing to purchase this valuable data in the underground to gain a competitive advantage.

It is no coincidence that the vast majority of attacks against the Mining, Oil/Gas & Energy industry were related to Trojan activity. Most Trojans create backdoors that contact offsite servers to send stolen information or collect victims' keystrokes using key logger software. Trojans are not easily detected and indicators of compromise are not always the same. Remote access Trojans (RATs), built for espionage and intellectual property theft, are comprised of highly destructive malicious code.

Brute Force attacks account for a small number of the incidents we observed against this industry in 2014. As discussed, given the relatively low number of "computer workers" and external web applications in this industry, attackers do not frequently use this vector in this particular industry.

In April 2014, the Apache Software Foundation (ASF) (http://www.apache.org) released a warning to its customer base that a patch issued in March for a zero day vulnerability in Apache Struts up to version 2.3.16.1 did not fully patch the vulnerability, which may result in Remote Code Execution via ClassLoader manipulation (CVE-2014-0094), or DoS attacks (CVE-2014-0050).

The least frequent types of attacks we identified within this industry were application attacks and reconnaissance. Of the application attacks, a commonly used target was Apache Struts. This is an open source web application framework for developing java applications; multiple vulnerabilities have been uncovered throughout its lifespan. Looking forward, Apache Struts will continue to rely on the community for future patches.

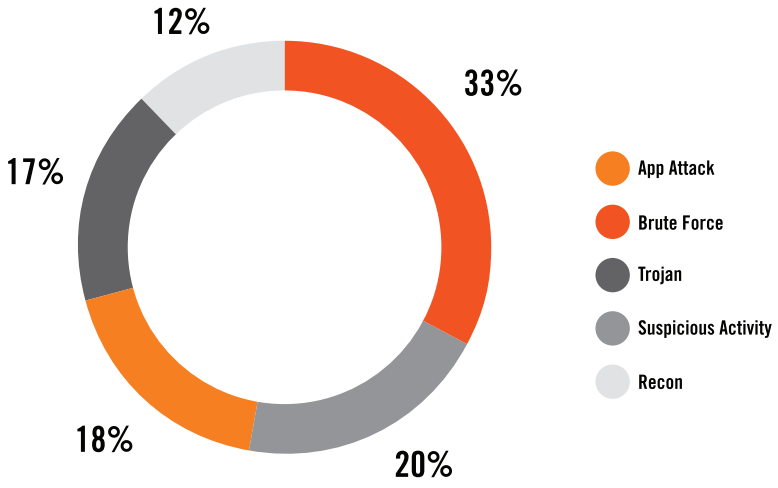
Financial Analysis

With the growing demand for consumer applications that provide ease of use and access, the Financial Services industry has engaged in the widespread adoption of Internet-enabled financial services. These now include website access, mobile banking via applications, SMS/Text message banking, and numerous email-based services.

Adding these new delivery models to their cloud environments resulted in an increase of attackers attempting to steal financial data—credit card numbers as well as personal information to fuel financial fraud and insider information to facilitate insider trading. For example, the FIN4 group used their attacks on the financial industry to gain confidential information related to the pharmaceutical and healthcare industries. This insider knowledge allowed FIN4 to successfully trade on the stock market and earn millions of dollars.

Application and Brute Force attacks comprise the majority of malicious activity within our Financial Services industry customer base, signaling a clear determination of attackers to gain access to these organizations' valuable data. These attack types are indicators of the intent to obtain data—application attacks will allow the leaking of information from databases and backend systems, and Brute Force attacks will grant access to internal systems, usually resulting in lateral movement within the organization to build a starting ground for a more sophisticated attack. Coupled with reconnaissance activity, 70% of attack types

FINANCIAL SECTOR ATTACKS



INFOCUS: FINANCIAL ATTACK

Art Ehuan, Managing Director, Alvarez & Marsal

COMPANY PROFILE

Alvarez & Marsal (A&M) provided incident response support for a Financial Services executive who was targeted by cyber attackers through a family member.

THE ATTACK

A Financial Services company—where the executive was employed—contacted A&M and requested incident response assistance in order to determine if the cyber attack on the executive's home network (which consisted of bundled Cable, VOIP, and Internet services) had impacted the corporate network.

The response by A&M was to determine if the cyber attack originated through a phishing email to the corporate executive's teenage son containing an offer to beta test a new game. The son's system was compromised through malware installed on the home computer, as the result of the phishing email. Once the cyber attackers had access to the home network, they were able to breach the corporate executive's computer. The cyber attackers identified and captured the executive's credentials attached to his personal banking account. The attackers used this information to log into the executive's account and change his email contact notification. They then initiated a wire transfer from the executive's personal account.

Interestingly, the bank had a notification requirement: To complete a wire transfer over a defined amount, the bank must first contact the authorized user of an account to confirm the transfer of funds. While the cyber attackers intercepted the bank call to the executive's home and routed it to their own phone number, the bank teller that placed the call realized that the person authorizing the transfer was not the executive. The teller terminated the wire transfer and notified the executive via an alternate method. The executive was concerned that the cyber attackers might also gain access to his corporate network through the breach, so he notified his company of the event. Social engineering cyber attacks continue to be successful due to the resourcefulness of criminal groups. The negative impact of the breach could have been prevented or mitigated if the following best practices had been in use:

- Be cognizant of the personal information that is posted on social media sites.
- Dependent on users on a home network, consider the possibility of segmenting the network to protect information where sensitive data is managed or processed.

INFOCUS: STEALING PUBLIC CLOUD CREDENTIALS

Sean Jones, Cybercrime Researcher, ActiveIntelligence

Disclosure of sensitive data—such as cloud credentials, security keys, and API keys—is a growing problem. As cloud-based tool development for storing, building, and deploying services increases, so will accidental disclosure of sensitive data. Hackers are aware of these disclosures and are always on the lookout for this sensitive data.

Hackers might employ bots specifically written to scan for this sensitive data in public code repositories such as GitHub and Bitbucket. Bots perform automated and repeatable tasks over the Internet at a much faster rate than any manual activity.

Once a malicious actor is able to obtain a user's sensitive data, like cloud credentials, the attacker can perform any manner of activity in the context of the user. The elastic nature of cloud computing means that attackers have access to large amounts of resources from compromised accounts, far more than the account may normally use. For instance, an attacker could steal computing resources to mine Bitcoin, or use compromised storage to store and distribute illegal content. It is also possible that attacks may be conducted against third parties by stealing network resources and launching denial of service attacks.

It is extremely important that all sensitive data is kept in a secure location and never stored in a public forum or code repository. Additionally, if any credentials, security keys, or access tokens are accidentally publicized, they should be considered compromised. Any compromised credentials must be removed and replaced on all systems. This is a critical rule to follow, because data from honeypots shows that attackers are continuously conducting Brute Force attacks against cloud services in order to guess usernames and passwords, and search for default passwords that have not been updated.

Administrators can use cloud identity and access management tools to control access to their cloud services. Tools that collect and report activity within environments should be included in the security-in-depth strategy for cloud deployments. Any recorded activity can facilitate the reviewing of logs to find and report on suspicious activity.

we identified in the Financial Services industry are focused on either gaining access or obtaining data.

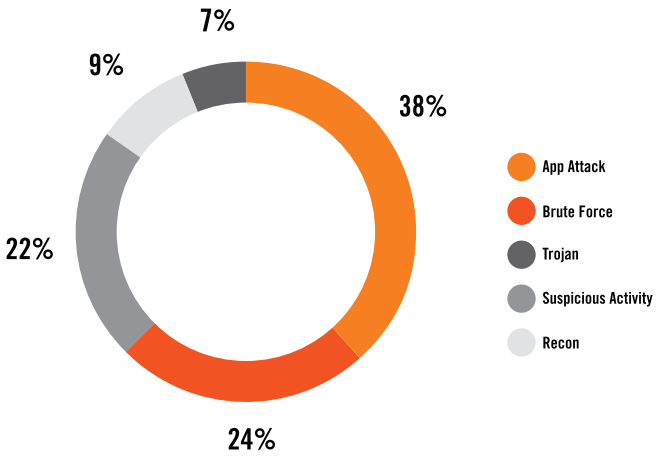
Unsurprisingly, Trojan activity was also used to further attackers' quests for internal access. Generally using spear phishing with malicious links and attachments, this technique is used to lure in less technically minded employees in order to gain a foothold within the environment, typically an on-premises data center. Cloud-based systems suffer less with this type of activity due to the nature of deployment, reducing the threat opportunity to these systems. Financial organizations are often viewed by malicious actors as challenging targets, due to the industry's large budgets, strong compliance and regulatory concerns, and heavily appointed security teams dedicated to focusing on day-to-day activities. In spite of these challenges, however, sophisticated attack groups still focus on the exploitation of these organizations, due to the financial return that could result in the event of a successful breach.

Retail Industry

The Retail industry is a favorite target for attackers. Customer financial information held by retailers—like credit card data—can be obtained and sold by attackers through a readily available secondary market of criminals specializing in credit card fraud. Retailers have heavily invested in digital systems to reduce costs at the point of sale. However, security budgets have often failed to keep track with the deployment of digital point of sale (POS) systems, giving attackers the ability to exploit vulnerabilities discovered on these systems. This environment has led to many high-profile breaches where attackers have been able to infiltrate networks, install specialized malware on POS, and steal tens of thousands of individuals' financial data.

Retail customers were targeted by a significant number of application attacks. Legacy e-commerce systems may be missing modern security features, and even recent systems may not be fully resistant to all application attack techniques. Attackers launch multiple probes against these systems, searching for weaknesses that can be exploited to gain access. Access to systems serves as a point of ingress for further attacks, giving attackers a means of stealing financial information, or as a way to obtain goods without payment.

RETAIL SECTOR ATTACKS



Developing e-commerce applications is resource intensive. Ensuring the security of the application is often a low priority, compared to delivering a positive customer experience. This lack of attention to security features coupled with an increase in investment by attackers means that application attacks are likely to remain a significant risk for the Retail industry in the future.

Brute Force attacks are likely evidence of similar activity, where attackers attempt to guess system usernames and passwords. All too often, systems are deployed with default usernames and passwords, or replaced with insecure passwords that offer little protection against systematic password guessing programs. Reconnaissance and suspicious activity attacks are evidence of attackers probing systems and networks, searching for potential vulnerabilities that can be exploited to gain access. Once an attacker gains access to a system, he can launch further attacks to escalate privileges until he obtains full control of the system to plunder information at will.

Trojan activity detected within the Retail industry encompasses malware that has infiltrated networks and is attempting to spread, or seeking to communicate with attackers to obtain further instructions. The Retail industry faces a challenging threat environment. By processing large amounts of financial data, the Retail industry will continue to attract the attention of malicious actors. Investing in and maintaining security systems to combat attackers and their continued innovations are vital to protecting systems and the valuable information they hold.

CONCLUSION

HOW THE GOOD GUYS CAN WIN

2014 was a banner year for high-profile breaches. More than 85 million records were lost via data breach, both from internal and external attackers. Whether you were an entertainment company releasing a controversial movie or a big box retailer whose POS systems were vulnerable to compromise, attackers had a virtual field day swiping sensitive data and converting that data into millions of dollars, euros, and pounds, causing significant brand impact. The good news for those responsible for securing IT infrastructure: Boardrooms around the world can no longer turn a blind eye to their aging security framework, especially when moving to the cloud. Increases in security tool and technology investments are expected to continue, giving organizations a more proactive stance in the ongoing battle to secure their data and protect their business.

WHAT TO CONSIDER WHEN ADDRESSING YOUR SECURITY FRAMEWORK

Cloud security means different things to different people, but an inclusive approach to securing your environment will be the most successful one. When thinking about security, there are many dimensions to consider. First among them is user-based security specific to Software-as-a-Service (SaaS) versus securing Infrastructure-as-a-Service (IaaS) and its associated applications and data. Both are important, but for different reasons: User-based security centers on visibility—knowing which SaaS applications your employees access, and the governance of those applications, as well as what data is being shared and how to control the flow of that data in SaaS applications. Securing IaaS is what protects you from the attacks we outlined in this report. You are securing the applications and underlying infrastructure in order to defend against today's threat landscape. Respecting both of these security dimensions, and considering the best approach to address both, will result in the most effective security posture.

Understand the shared security model.

While not a mystery, many companies are still learning where the lines of demarcation are drawn between what areas cloud providers address and what areas are a customer's responsibility. Cloud providers such as AWS, Microsoft Azure, IBM SoftLayer, Google, and Rackspace all provide security controls that typically include physical, perimeter network, and the hypervisor layer. They invest heavily in their areas of responsibility to ensure that they are fully secure and hardened.

Customers carry the responsibility of protecting the applications, data, and network infrastructure on which the applications and data reside. What this means for you: Your area of responsibility requires that you have technology, process, and expertise capable of delivering network threat detection, log analytics, application layer protection, and

access management, among other areas of security.

Understand your threat profile.

As discussed in this report, your industry, the applications you run, and the data you retain drive the attraction of attackers. Maintaining a solid understanding of the application types deployed, the type of data maintained, and the associated compliance mandates (such as PCI, HIPAA, SOX, etc.) will help to drive the types of security controls and solutions you need to deploy.

To fulfill your part of this shared security model, you must formulate a plan that includes technology, information, people, and processes.

WHERE TO BEGIN

- **IT'S ABOUT THE DATA:** When developing your security framework, do not start with technology selection. Take a step back and think about the type of data and applications you will be using in the cloud. There may be different approaches to security required for different types of data and applications.
- **BUILD THE PROCESS FIRST:** With an understanding of the data you are protecting, begin building your process playbook. This will include responsibilities, stakeholders, incident response plans, as well as contingency plans for when something goes wrong.
- **NOW BUILD YOUR SECURITY TOOLKIT:** No single piece of software is going to fulfill every security need. To prepare for the unexpected, it is crucial to have all of the necessary tools primed and ready within the security arsenal.
- **CREATE ACCESS MANAGEMENT POLICIES:** Logins are the keys to the kingdom and should be treated as such. Protecting these means putting in place a solid access management policy, especially for those who are granted access on a temporary basis. Integration of all applications into a corporate AD or LDAP centralized authentication model will help with this process.
- **ADOPT A PATCH MANAGEMENT APPROACH:** Unpatched software and systems can lead to major issues for any organization. Securing an environment includes outlining a process to update systems on a regular basis. All updates should be tested to confirm that they do not damage or create vulnerabilities before implementation into a live environment.
- **REVIEW LOGS REGULARLY:** Log review should be an essential component of any organization's security protocols. It is absolutely necessary to take the time to review logs—they might uncover something significant.
- **SECURE YOUR CODE:** Hackers are continually looking for ways to compromise applications. Code that has not been thoroughly tested and secure makes it easier to do harm. By testing libraries, scanning plugins, etc., organizations can take an offensive stance against future attacks.

Cyber attacks are going to happen. Vulnerabilities and exploits are going to be identified. Having a solid security-in-depth strategy, coupled with the right tools and people that understand how to respond, can ultimately put you in a position to minimize your exposure and risk.

APPENDIX: THE DATA

CLOUD VS. ON-PREMISES: INCIDENT OCCURRENCE AND FREQUENCY

Fig. A

Attack Type	Cloud		On-Premises	
	Occurrence	Frequency	Occurrence	Frequency
Application Attack	70%	118	52%	98
Brute Force	56%	101	47%	201
Recon	57%	40	48%	46
Suspicious Activity	53%	68	50%	60
Trojan Activity	37%	68	57%	108

INCIDENT METRICS

Incident Occurrence
Percentage of customers experiencing a specific class of incident at least once during the study period. Provides a view of the probability of attack.

Incident Frequency
Average number of incidents of each type per impacted customer. Provides an understanding of attacker persistence and tenacity.

INCIDENTS OVER TIME

Fig. B

Attack Type	Jan-Apr		May-Aug		Sept-Dec		Total	
	CLOUD	ON-PREM	CLOUD	ON-PREM	CLOUD	ON-PREM	CLOUD	ON-PREM
Application Attack	35%	16%	37%	17%	39%	24%	**37%**	**20%**
Brute Force	28%	24%	27%	38%	23%	42%	**25%**	**36%**
Recon	19%	12%	10%	8%	7%	7%	**10%**	**8%**
Suspicious Activity	16%	17%	18%	11%	15%	9%	**16%**	**12%**
Trojan Activity	3%	31%	8%	26%	17%	17%	**11%**	**24%**

MONTH-TO-MONTH ATTACK SPREAD

Fig. C

Attack Type	Jan	Feb	Mar	Apr	May	Jun	July	Aug	Sept	Oct	Nov	Dec	Total
Application Attack	20%	27%	28%	39%	28%	31%	28%	34%	41%	66%	39%	39%	**39%**
Brute Force	25%	25%	34%	26%	37%	29%	31%	25%	24%	14%	23%	24%	**25%**
Recon	12%	14%	20%	17%	14%	14%	17%	19%	19%	8%	11%	9%	**13%**
Suspicious Activity	8%	8%	11%	13%	12%	16%	14%	14%	9%	8%	21%	21%	**14%**
Trojan Activity	35%	26%	7%	6%	9%	10%	10%	7%	7%	3%	6%	6%	**9%**

PARTNERS INCLUDED IN STUDY*

Fig. D

PARTNER	WEBSITE	PARTNER	WEBSITE
2nd Watch	2ndwatch.com	**Microsoft Azure**	azure.microsoft.com
Amazon Web Services (AWS)	aws.amazon.com	**MegaPath Networks**	megapath.com
CyrusOne	cyrusone.com	**NaviSite**	navisite.com
Datapipe	datapipe.com	**OneNeck IT Solutions**	oneneck.com
Dimension Data Cloud Solutions	dimensiondata.com	**PEER 1 Dedicated Hosting**	peer1.com
Google Cloud Platform	cloud.google.com	**Pulsant**	pulsant.com
HOSTING	hosting.com	**Rackspace Managed Hosting**	rackspace.com
Hostway Services	hostway.com	**Sungard Availability Services**	sungardas.com
Internap	internap.com	**VMware vCloud Air**	vcloud.vmware.com
Latisys	latisys.com	**Windstream Communications**	windstreambusiness.com
Logicworks	logicworks.net		

*This partners list is representative of our top partners, but is not an exhaustive list of our entire partner network.

INCIDENT CLASSIFICATIONS

APPLICATION ATTACK

An attempt to exploit an application to harm, destroy, or access the application or data stored in the application. Examples of application attacks include SQL Injection and the HeartBleed exploit.

BRUTE FORCE

An attempt to gain access to a system by repeatedly trying different users names and passwords or cryptographic keys until the correct username/password combination or correct key is found. An example would be a dictionary attack against an ftp or email server.

SUSPICIOUS ACTIVITY

This activity has not been confirmed as malicious but it needs to be reviewed to confirm or invalidate malicious activity. The activity may include vulnerability scanning or some types of IRC activity.

RECON

This activity involves an attacker scanning for particular ports or searching for particular applications or vulnerabilities. This would include an attacker using a ZmEu to search for vulnerable PHP implementations or using NMAP to perform a port sweep.

TROJAN ACTIVITY

Unwanted and malicious code that is not self-replicating. This code may cause harm to the system, data to be lost or stolen or provide remote access to a malicious user. Some notable Trojans are Kazy and Superfish.

CONTRIBUTORS

Research
Alert Logic
ActiveIntelligence Team

Writers
Steve Salinas
Martin Lee
Stephen Coty
Art Ehuan
Sean Jones

Data Analyst
Dan Cellucci

Design
Sean Ferguson
Willie Blue

Editors
Sheridan Scott
Rahul Bakshi

CORPORATE HEADQUARTERS

Alert Logic, Inc.
1776 Yorktown, 7th Floor
Houston, TX 77056

UK OFFICE

Floor 5, 1 Capital Quarter
Cardiff
CF10 4BE
United Kingdom