IBM Security
Managed Security Services

IBM 2015 Cyber Security Intelligence Index

Analysis of cyber attack and incident data from IBM's worldwide security services operations

Research Report

IBM

Contents

About this report

IBM Managed Security Services continuously monitors billions of events per year, as reported by more than 8,000 client devices in over 100 countries. This report is based on data IBM collected between 1 January 2014 and 31 December 2014 in the course of monitoring client security devices as well as data derived from responding to and performing analysis on cyber attack incidents. Because our client profiles can differ significantly across industries and company size, we have normalized the data for this report to describe an average client organization as having between 1,000 and 5,000 employees, with approximately 500 security devices deployed within its network.

The annual Cyber Security Intelligence Index offers a high-level overview of the major threats to businesses worldwide over the past year. Our goal is to help you better understand the current threat landscape by offering a detailed look at the volume of attacks, the industries most affected, the most prevalent types of attacks and attackers, and the key factors enabling them. We provide insights into where and how successful attacks can impact today's technology-dependent organizations and discuss how the threat landscape is evolving from year to year, as companies work to better detect and insulate themselves from future attacks.

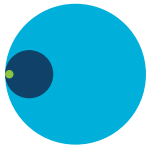
The year the Internet fell apart

By just about anyone's standards, 2014 was an eventful year for the cyber security industry. Significant threats and massive breaches made front-page news on a regular basis, leaving businesses and consumers wondering whether their data could ever be considered safe again.

Major vulnerabilities were found lurking in well-known applications, many of which had been dormant for more than 10 years. Once discovered—and subsequently exploited—they left virtually every industry vulnerable to serious threats, including the possibility of intruders gaining full remote access to critical systems. IT departments often found themselves unprepared to patch and mitigate these threats, leaving the window for exploitation wide open and leading to a "perfect storm" of zero-day attacks, system infiltration and subsequent data loss for many organizations.

Learn more:
Events, attacks and incidents defined

Many of the notable data breaches that occurred in 2014—some of which significantly impacted the affected organizations—were the result of attacks that exposed healthcare records, credit card data and volumes of personally identifiable information. They potentially compromised the safety of these organizations and endangering the security of millions of individuals who could now be exposed to the possibility of identity theft.



Get the picture: Annual security events, attacks and incidents

The numbers tell a new story

In 2014, the average organization monitored by IBM Security Services experienced approximately 81 million security events (see Figure 1). Continual policy tuning allowed IBM security analysts to filter out 11 percent of the security events, leading to greater efficiency on all levels and making it possible for them to shift their attention to those events meriting further analysis. But despite the resulting reduction of "noise" at the event level, the average number of incidents held fast to 2013 levels at 2.10 per week. In other words, while IBM has become more proficient at weeding out ineffective attacks, the incident-to-attack ratio rose from .65 percent to .91 percent.

Get the picture: Incident rates across monitored industries

Over 62 percent of incidents targeted just three industries

The data for 2014 shows a marked departure from the trends reported for both 2012 and 2013. While the finance and insurance category remains in its top spot as the most targeted industry, the information and communications category took over second place from manufacturing. And although retail held onto fourth place in the rankings, that industry experienced 3.2 percent more incidents in 2014 than it did in the previous year (see Figure 2). That represents the largest percentage change among the four industries remaining from the previous year's top five. As noted earlier, 2014 saw the compromise of a significant number of retail records. And as reported last September, point-of-sale malware was responsible for one of the largest retail security breaches ever reported. Clearly, point-of-sale systems have become extremely attractive as network entry points

for criminals—a trend that's expected to continue to grow in 2015. In another change from 2013 to 2014, the electric and utilities category took over fifth place in the rankings, edging out sixth-place health services by a small margin. Unauthorized access and malicious code incidents made up nearly half of the incidents targeting this year's number five industry. And attacks against the utility sector are a growing concern for governments globally. The Industrial Control Systems Computer Emergency Response Team's (ICS-CERT) January–April 2014 Monitor report disclosed the compromise of a public utility via unauthorized access to its control system network.[2] The administrative software was remotely accessible and configured with a simple password mechanism, making it susceptible to compromise via brute force.

Learn more:
Three potentially system-crippling threats

Taking one more look at the 2014 top industry list, it may be interesting to note that all industries, with the exception of manufacturing, saw an increase in their percentage of total incidents over 2013. This might prompt further investigation into what the manufacturing industry is or isn't doing differently from the other industries.

Unauthorized access spurs nearly twice as many incidents in 2014

In both 2012 and 2013, malicious code and sustained probes or scans dominated our clients' security incident landscape (see Figure 3). But all that changed in 2014 when certain types of unauthorized access incidents rocketed to the top, accounting for 37 percent of the total—nearly doubling from 19 percent in 2013. ShellShock and Heartbleed (see "Three potentially system-crippling threats") were the game changers here. These findings prove that anyone who thinks they know what to expect when it comes to cyber threats had better think again. Organizations that have developed a dynamic and flexible security posture will almost always find themselves better equipped to handle dramatic shifts like this.

Get the picture: Categories of incidents among top five industries

Learn more:
Three confidence-breaking breaches

Looking at the other major types of incidents we saw in 2014, malicious code dropped to second place, followed by sustained probes or scans in third place. Although lower on the list than in previous years, these threats are still significant; together they account for 40 percent of all the incidents observed. With an ever-expanding array of malware from which attackers may choose—including viruses, worms, Trojans, bots, backdoors, spyware and adware—it seems fairly certain that malicious code incidents will continue to wreak havoc for the foreseeable future. What's more, point-of-sale malware, such BlackPOS and Backoff, and ransomware such as CryptoWall and CryptoLocker, are gaining in popularity as a result of their effectiveness in compromising vulnerable targets. Attackers are typically interested in finding the path of least resistance. And these methods are capable of providing that.

Meanwhile, the number of denial of service attacks, which account for only four percent of the total, actually doubled over the previous year. Over 50 percent of these denial of service incidents were targeted at the retail industry—which may point to the possibility that an increased emphasis on thwarting more high-profile threats (such as point-of-sale malware) left a window open for attackers to exploit opportunities along a less-travelled path.

More than half of all attackers are "insiders"

There are plenty of reasons to assume that most attacks are the work of far-off "bad guys" with a political axe to grind or in search of fame and fortune. After all, we hear about them in news reports just about every day. But in 2014, 55 percent of all attacks were carried out by either malicious insiders or inadvertent actors (see Figure 4). In other words, the attacks were instigated by people you'd be likely to trust. And they can pose a significant threat, resulting in substantial financial and reputational losses.

Get the picture: Who are the "bad guys"?

What is an insider? An insider, in this case, is anyone who has physical or remote access to a company's assets. Those are tangible items—including hard copy documents, disks, electronic files and laptops—as well as non-physical assets, such as information in transit. Although the insider is often an employee of the company, he or she could also be a third party. Think about business partners, clients or maintenance contractors, for example. They're individuals you trust enough to allow them access to your systems.

Of course you might consider it awkward to think of your employees as a potential "threat." But that's just another reality of today's workplace. Even hundreds of years ago, there were spies carrying out business-related espionage all over the world. The truth is, individuals inside your organization may have an especially keen understanding of the company's weaknesses—or access to "insider-only" areas. That gives a maliciously-minded individuals an obvious advantage, since it's unlikely they need to bypass protection systems to obtain sensitive information. They already have access.

Still, it's important to note that breaches caused by insiders are often unintentional. In fact, over 95 percent of these breaches are caused by human error. That can mean accidentally posting confidential information on the company's public-facing website, sending confidential information to the wrong party via email, fax, or mail, or improperly disposing of clients' records.

But insiders who set out to take advantage of the company they work for can be much more dangerous. It's more difficult to thwart these insiders' malicious actions because they're willing to take extraordinary measures to circumvent access controls and are typically unconcerned with corporate policies or the potential consequences of their actions.

Case in point: Attackers use one attack as a smokescreen to hide others

Where is all this happening?

While it's important to understand who's behind today's cyber attacks, it's also useful to see where the majority of those attacks are coming from—and where they're landing. It is equally important to consider the size of each country involved and the availability of bandwidth within it. That goes a long way toward explaining why more than half of the attacks we saw in 2014 originated in the United States. And for many of the same reasons, the United States was also the most attacked country in 2014 (see Figure 5).

Get the picture: Where are these attacks coming from? And where are they taking place?

It's not about "if" you're going to be hacked; it's about "when"

When *The Wall Street Journal* held the annual meeting of its CIO Network earlier this year, it was clear from the outset that just about all the CIOs present were of similar thinking: that being hacked is inevitable. As the paper reported in February 2015: "Conversation during breaks gravitated to the remarkable destruction of Sony Pictures Entertainment's network and files that hackers caused in November [2014].

"This hack wasn't about stealing intellectual property and slinking away, or pranking a former employer. These hackers broke in and fired up the wrecking ball.

"The global chief information officers who gathered at the third annual CIO Network in San Diego … are a chastened crew. When asked who hasn't been hacked, just one hand went up in the audience, and that CIO got a lot of skeptical looks."[3]

Over the past few years it's become increasingly clear that the conversation has changed from talking about "if you will be hacked" to "when you will be hacked." And more importantly, the conversation then turns to what you should do about it.

Learn more:
A wolf in sheep's clothing

Put a halt to dangerous thinking

If you're asking, "Why would anyone want to come after us?" there's a good chance that you may already be in trouble. It's tempting to think that if your organization isn't that large or well known, or if you're not in one of the most frequently attacked industries, you may not have much to worry about. Unfortunately, that's dangerous thinking. Companies of all sizes are at risk, as are those in all industries. As we noted earlier, the average organization monitored by IBM Managed Security Services experienced approximately 81 million security events in 2014, which yielded two actual incidents each week. And yes, those two incidents could have happened to your company.

When it comes to cyber security, there are four key questions that every company should be asking its security team right now:

- How strong is my company's current security program—and how does it compare with other companies in my industry?
- What can we do to stop advanced threats from infiltrating our systems?
- Are we doing everything we can to protect our most valuable data?
- How can we adopt new technologies—such as mobile and cloud—without compromising our security?

The answers will help you understand where to turn next.

Why IBM Security?

Traditional security defenses are no match for today's unrelenting, well-funded attackers, while disruptive technologies introduce new vulnerabilities to exploit. Organizations must accelerate their ability to limit new risk and apply intelligence to stop attackers—regardless of how advanced or persistent they are. New analytics, innovation and a systematic approach to security are necessary. Yet there are very few companies able to meet those requirements on their own. Forrester Research has noted: "In order to be a true partner, [managed security services] providers need to demonstrate they can create business value as well as technical value for their clients. [They] are assuming more and more of an active role in defending their clients, which requires forward thinking, excellent execution, and an understanding of the client's security business drivers. These qualities will determine the ability of the managed security services provider to meet current and future demands that clients will ask of these service providers."[4]

Case in point: Stress testing can take some of the stress out of an attack

When you engage with IBM for managed security services, you gain access to a rich suite of capabilities that can help you extend protection from the back office to the front office. And we help ensure that it's integrated and coordinated across your enterprise. The IBM Managed Security Services Threat Research Group is staffed by an elite team of our most experienced and skilled threat analysts. Dedicated to delivering industry-leading cyber threat intelligence, the group provides up-to-date research on threats that could negatively impact IBM customers.

Case in point: A disgruntled employee creates a backdoor to steal company data

At IBM, our IT security services can cover your network, from infrastructure to applications to devices. We monitor, in near real time, some of the most complex corporate networks in the world. We develop some of the most sophisticated monitoring tools in the security industry, many of which are used by our competitors. And our team of highly skilled security professionals is constantly identifying and analyzing new threats, often before they are even known by the world at large. In fact, we maintain one of the largest databases of known cyber security threats in the world.

For more information

To learn more about how IBM can help you protect your organization from cyber threats and strengthen your IT security, contact your IBM representative or IBM Business Partner, or visit this website:
ibm.com/services/security

Follow us

Authors

Nicholas Bradley, Practice Lead, Threat Research Group, IBM Managed Security Services

Michelle Alvarez, Researcher/Editor, Threat Research Group, IBM Managed Security Services

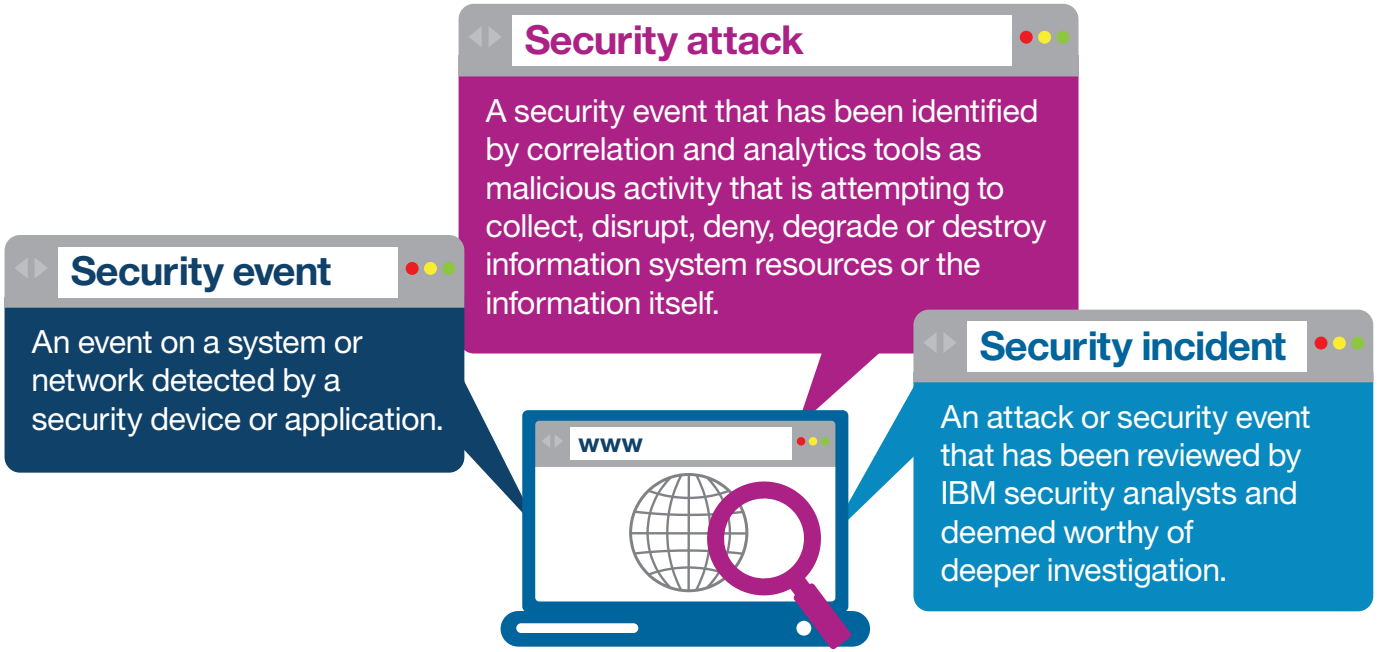
John Kuhn, Senior Threat Researcher, IBM Managed Security Services

David McMillen, Senior Threat Researcher, IBM Managed Security Services

Glossary

Term	Definition
Access or credentials abuse	Activity detected that violates the known use policy of that network or falls outside of what is considered typical usage.
Attacks	Security events that have been identified by correlation and analytics tools as malicious activity attempting to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. Security events such as SQL Injection, URL tampering, denial of service, and spear phishing fall into this category.
Breach or compromise	An incident that has successfully defeated security measures and accomplished its designated task.
Denial of service	Attempts to flood a server or network with such a large amount of traffic or malicious traffic that it renders the device unable to perform its designated functions.
Droppers	Malicious software designed to install other malicious software on a target.
Event	An event is an observable occurrence in a system or network.
Inadvertent actor	Any attack or suspicious activity sourcing from an IP address inside a customer network that is allegedly being executed without the knowledge of the user.
Incidents	Attacks and/or security events that have been reviewed by human security analysts and have been deemed a security incident worthy of deeper investigation.
Keyloggers	Software designed to record the keystrokes typed on a keyboard. This malicious software is primarily used to steal passwords.
Malicious code	A term used to describe software created for malicious use. It is usually designed to disrupt systems, gain unauthorized access, or gather information about the system or user being attacked. Third-party software, Trojan software, keyloggers, and droppers can fall into this category.
Outsiders	Any attacks that sourced from an IP address external to a customer's network.
Phishing	A term used to describe when users are tricked into opening an infected email attachment or browsing to a malicious website disguised as a trusted destination where they provide information that can be used to access a system or account or steal their identities.
Security event	An event on a system or network detected by a security device or application.
Security device	Any device or software designed specifically to detect malicious activity or protect a host or network. Such network-based devices are often referred to as intrusion detection and/or prevention systems (IDS, IPS or IDPS), while the host-based versions are often referred to as host-based intrusion detection and/or prevention systems (HIDS or HIPS).
Spear phishing	Phishing attempts with specific targets. These targets are usually chosen strategically in order to gain access to very specific devices or victims.
SQL injection	An attack that attempts to pass SQL commands through a website in order to elicit a desired response that the website is not designed to provide.
Suspicious activity	These are lower-priority attacks or suspicious traffic that could not be classified into one single type of category. These are usually detected over time by analyzing extended periods of data.
Sustained probe/ scan	Reconnaissance activity usually designed to gather information about the targeted systems such as operating systems, open ports, and running services.
Trojan software	Malicious software hidden inside another software package that appears safe.
Unauthorized access	This usually denotes suspicious activity on a system or failed attempts to access a system by a user who does not have permission.
Wiper	Malicious software designed to erase data and destroy the capability to restore it.
Zero-Day	An unknown vulnerability in an application or a computer operating system.

Events, attacks and incidents



According to the IBM Computer Security Incident Response Team, of all the security incidents they work through and analyze, only three percent actually reach a level of severity high enough to consider them "noteworthy"—with the most common impact being data disclosure or theft.

Return to text

Figure 1

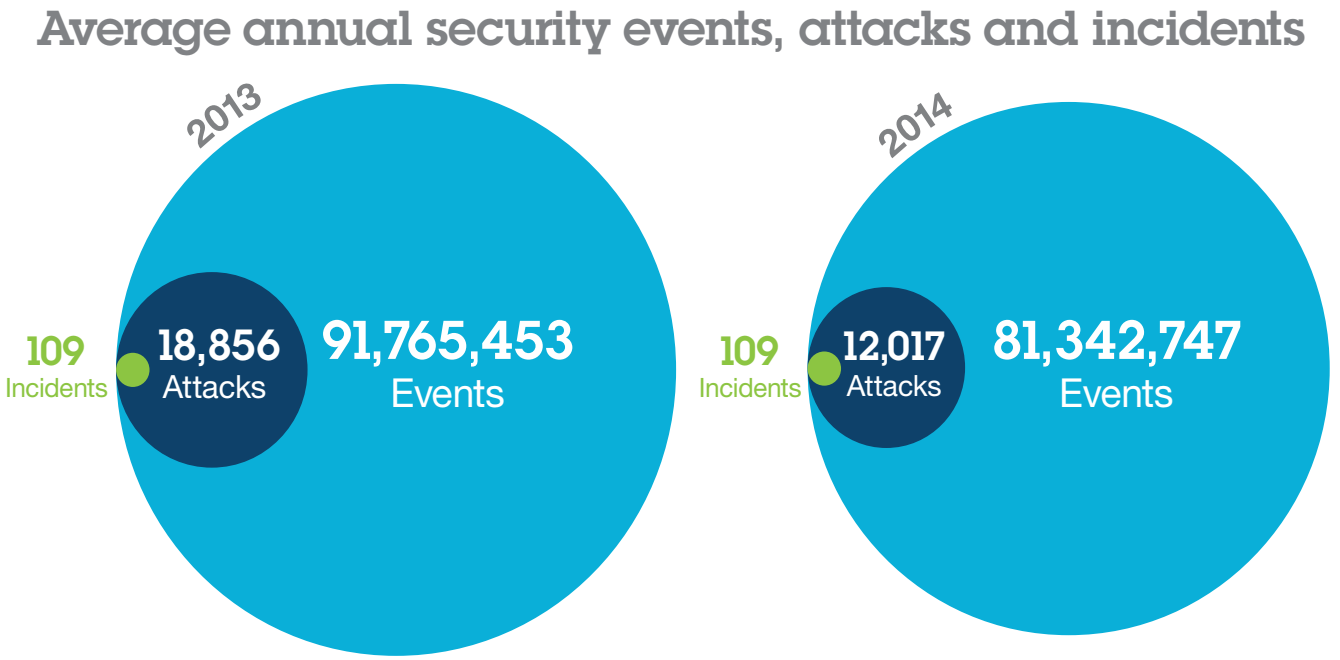


Figure 1. Security events appear in many guises and, in many cases, extremely high volume. IBM Managed Security Services' highly skilled intelligence and operations teams work to translate those ever-increasing event counts into actionable data and keep our clients from becoming overwhelmed.

Return to text

Figure 2

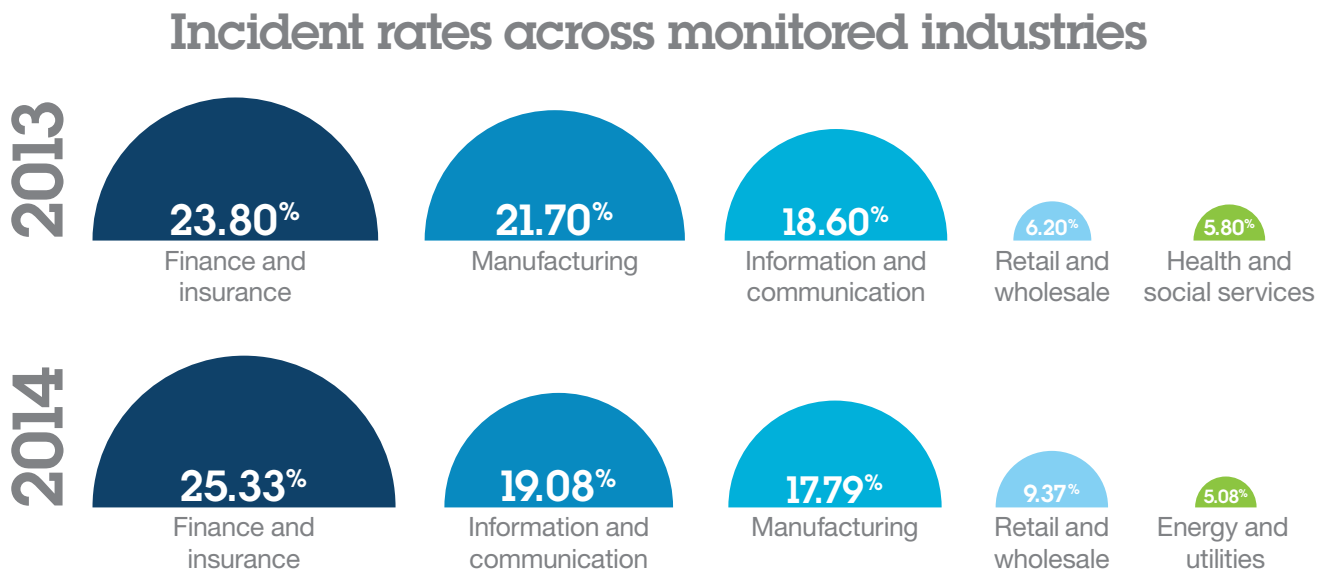


Figure 2. While the finance industry retained its spot at the top of the list from 2013 to 2014, the information and communication category switched places with manufacturing. Meanwhile, the energy and utilities category narrowly edged out the health and social service category for fifth place. Of this group, only manufacturing experienced fewer incidents in 2014 than in the previous year.

Return to text

Three potentially system-crippling threats

ShellShock: A more than 20-year-old vulnerability in the GNU Bash shell (widely used on Linux, Solaris and Mac OS systems) sparked the mobilization of attacks known as ShellShock beginning in late September 2014. This first vulnerability quickly gave way to the disclosure of several additional vulnerabilities affecting the UNIX shell. IBM Managed Security Services (MSS) observed a significant increase in focused attacks targeting these vulnerabilities within 24 hours of their disclosure. The attacks came in waves, from different source IPs and originating countries. In the two weeks following the disclosure, the US was on the receiving end of more recorded attacks than any other country. This threat is a good example of a growing trend on the attacker front called "malware-less" attacks. Attackers are looking to exploit existing functionality in applications rather than risking malware detection that would thwart their success.

Heartbleed: The Heartbleed vulnerability is a security bug in OpenSSL, a popular open source protocol used extensively on the Internet. It allows attackers to access and read the memory of systems thought to be protected. Vulnerable versions of OpenSSL allow the compromise of secret keys, user names, passwords and even actual content. It is believed that this vulnerability has been in existence for at least two years and has quite possibly been exploited for just as long. Many companies have issued statements claiming that they have now remedied the vulnerability in their environment, but there is truly no way of knowing how much data has fallen into the wrong hands through the exploitation of this bug. While the Heartbleed bug itself was introduced on the last day of 2011, it didn't make its first public appearance until April 2014, when it showed up as an OpenSSL advisory. By the end of that month, IBM MSS had tracked over 1.8 million attacks against customers. The three hardest hit countries were China, Russia and the United States.

Unicorn: Every release of Microsoft Internet Explorer (beginning with version 3.0) that's run on any Windows operating system (beginning with Windows 95) allows remote code execution via a data-only attack. In this type of attack, the attacker changes key data structures used by the program's logic, forcing the control flow into existing parts of the program that would be otherwise unreachable. Discovered in November 2014 by an IBM X-Force® researcher, this is a complex and rare vulnerability. Attackers can use it in "drive-by attacks" to run programs remotely and take over a user's machine—even sidestepping the Enhanced Protected Mode (EPM) sandbox in Internet Explorer 11 and the Enhanced Mitigation Experience Toolkit (EMET), a free Microsoft anti-exploitation tool.[1] The flaw is known to be at least 19 years old. Similar to ShellShock, it's yet another serious vulnerability going unnoticed for an extremely long time despite all the efforts of the security community.

Return to text

Figure 3

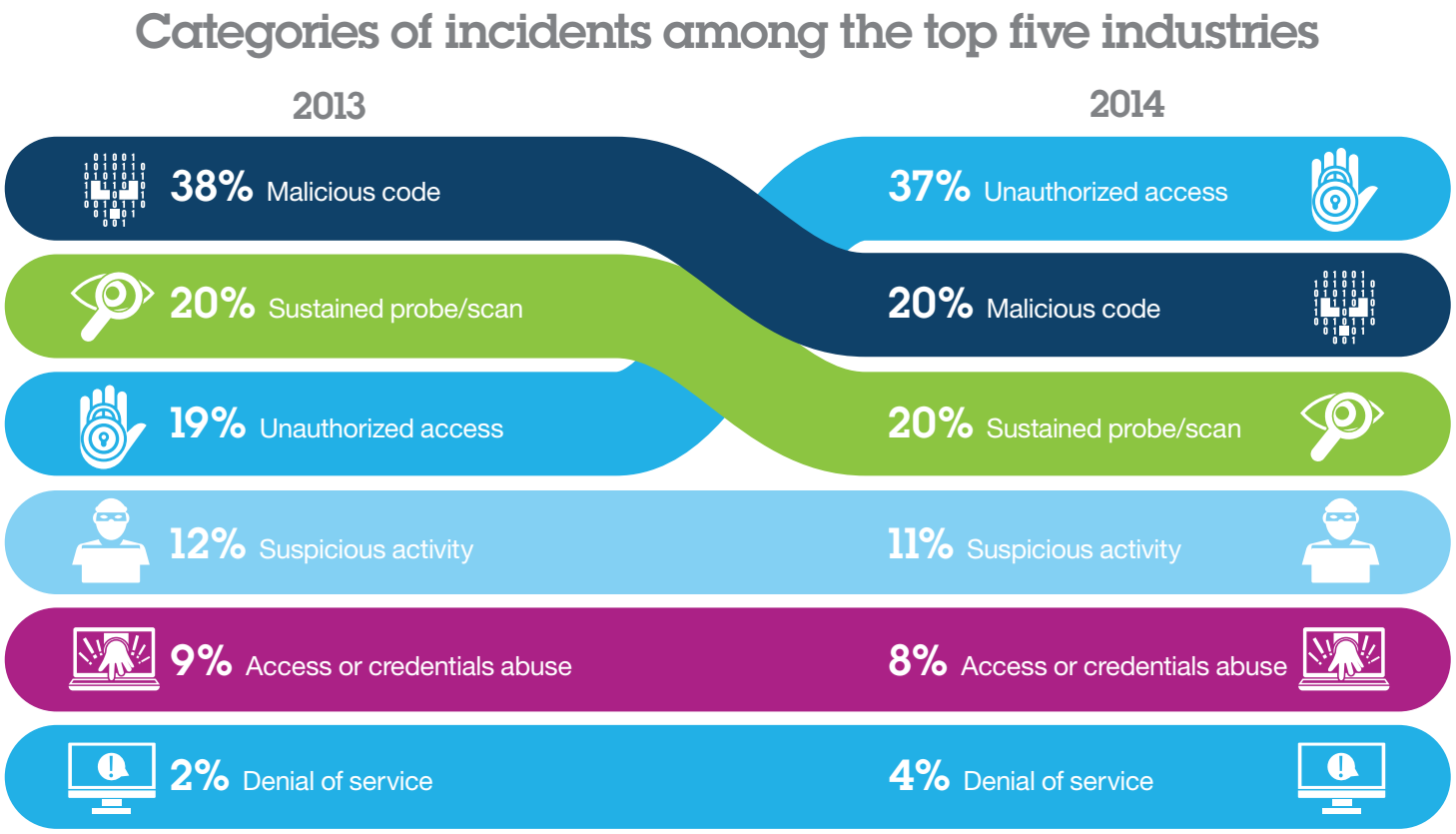


Figure 3. In 2014, unauthorized access topped the list of incident categories affecting the top five industries named in this report, replacing malicious code, which was the top category in 2013.

Return to text

Three confidence-breaking breaches

It was early 2014 when **one of the largest arts and crafts retailers** in North America told customers of possible fraudulent activity on some US payment cards that had been used at the chain's stores. The company later confirmed that a malware-related attack had resulted in a breach sometime between mid-2013 and February 2014, affecting certain systems that process payment cards, and may have affected more than 2.5 million cards. It also reported that an additional 400,000 cards may have been impacted at a subsidiary.

In one of the largest recorded retail breaches to date, **a major North American retailer of home improvement goods** fell victim to a point-of-sale attack that affected more than 2,000 stores. Confirmed by the company in the fall of 2014, the breach exposed over 55 million records of payment card data—a large quantity of which appeared to go up for sale immediately on underground cybercrime sites. The incident also resulted in the theft of more than 50 million email addresses. BlackPOS—a specific type of point-of-sale malware—was blamed for the breach.

A leading operator of general acute care hospitals in North American disclosed in the summer of 2014 that it had been the victim of one of the largest reported healthcare data breaches that year. The attack was credited to an Advanced Persistent Threat group based in East Asia. Sophisticated malware resulted in the compromise of Social Security numbers, names and addresses for some 4.5 million patients.

Return to text

Figure 4

Figure 4. While outsiders were found to be responsible for 45 percent of the attacks recorded in 2014, 55 percent of attacks were carried out by those who had insider access to organizations' systems.

Return to text

CASE POINT in Attackers use one attack as a smokescreen to hide others*

Approach: Attackers launched an attack to create additional traffic as a diversion to keep attention away from other targeted attacks.

How it happened: Attackers took advantage of a "low and slow" distributed denial of service (DDoS) attack tool to saturate the company's web server resources. Because the traffic appeared legitimate, it passed undetected and failed to set off any warnings that there might be a problem. By the time the company discovered the problem, the attackers had already begun to capitalize on malware previously installed on vulnerable systems. They proceeded to perform fraudulent wire transfers while all the company's IT resources were completely focused on the initial DDoS incident.

Impact: The company was exposed to potential financial damage on two levels. First, while the website was down, customers were unable to perform transactions, resulting in potential financial loss for the company. And second, the fraudulent wire transfers resulted in millions of dollars stolen from accounts. Brand reputation was also severely damaged and hundreds of customers moved their financial accounts elsewhere, having lost trust in the company and fearing future compromise.

Lessons learned: Traditional defenses such as firewalls and intrusion-prevention systems alone are no longer enough to protect against DDoS. A managed web defense service can help prevent these attacks by routing traffic away from an organization's infrastructure during an attack, keeping websites running without disrupting operations. What's more, by implementing an advanced malware solution, an organization could be able to prevent mass-distributed malware infections and detect legacy threats.

*This is a fictional account based on the collective experiences of multiple clients, as monitored by IBM Managed Security Services.

Return to text

Figure 5

Figure 5. The largest number of attacks both originated (50 percent) and took place (59 percent) in the United States in 2014. Next in line were China, where 16 percent of all attacks originated, and Japan, which was the target of 24 percent of the year's attacks. Germany and China were not in the group of top countries where attacks took place.

Return to text

A wolf in sheep's clothing

In April of this year, IBM announced it had uncovered a sophisticated—and unusually successful—campaign that had already stolen upwards of $1 million from large and medium-size companies in the US. Launched by a gang of cyber criminals using a combination of phishing, malware and phone calls, the scheme has been named "Dyre Wolf" by IBM researchers, making reference to the now-popular Dyre or Dyreza malware used in the attacks. And although other attacks may have made a bigger impact or gained wider notoriety, few have demonstrated the kind of sophistication that Dyre Wolf has displayed.

The attackers target individuals working in specific companies by sending spam email with unsafe attachments. That's how they get a variant of the Dyre malware into the companies' computers. Once installed, the malware then lies in wait until it becomes obvious that the user is trying to log onto a bank website. At that point, it immediately creates a fake screen telling the user that the bank's site is temporarily unavailable and offers instructions to call a specific phone number.

That's when social engineering techniques take over. A live, English-speaking "operator" answers the call with the name of the bank that the user expects. Unaware that they're participating in a fraud, users typically share their banking details, setting off a large wire transfer to withdraw funds from the relevant account.

After the transfer has been completed, the attackers quickly move the money from one bank to another to avoid detection. The attackers have even been known to initiate denial of service sprees against their victims, paralyzing their web capabilities and making it virtually impossible to discover the theft until many hours later.

The group behind this project has developed a complex campaign that's exceptionally effective at stealing large sums of money. Its infrastructure, manpower and knowledge of banking systems and websites clearly demonstrate that the group is well-funded, experienced and intelligent. And that's what makes Dyre Wolf a significant threat.

Return to text

CASE in POINT

Stress testing can take some of the stress out of an attack*

Approach: Hackers targeted a specific company with a tool known as "SQLninja," which is designed to allow an attacker to inject an SQL database and gain full administrator access.

How it happened: Once they gained control of the system, the attackers found the path to an unsecured data table containing privileged employee information, including Social Security numbers, dates of birth, residential addresses and email addresses. They were able to retrieve the entire table and then delete the master on the server. With the full list in their possession, they posted a snippet of the data to an online pastebin (a web application used to store plain text). Thus proving that their efforts were successful, they followed up with an email to the company's CEO demanding a monetary ransom for the return of the data. Then, as a final act of defiance, the attackers also found the path to the root web server and defaced it by posting an image of their cybercrime logo.

Impact: The data contained in the table was detailed enough to potentially allow cyber criminals to pose as the company's employees and attempt to gain credit in their names. In addition, the stolen data tables with the employee information were lost forever because the company hadn't developed or implemented data recovery or disaster plans. As a result, the website had to be completely rebuilt—at great expense—to bring the company back online and put it back in business.

Lessons learned: It's vital that organizations perform security stress tests and proper data validation on homegrown web-based applications that have access to back-end SQL databases. Creating redundant backups of all data and keeping them offline can lead to quick recovery, while subscribing to or creating a robust disaster recovery plan can limit the financial loss that comes with having to start over and rebuild lost assets.

*This is a fictional account based on the collective experiences of multiple clients, as monitored by IBM Managed Security Services.

Return to text

CASE POINT in

A disgruntled employee creates a backdoor to steal company data*

Approach: A disgruntled network administrator created a backdoor (or intentional flaw) on a server in order to bypass security mechanisms and continue to have unauthorized access after being dismissed.

How it happened: Unhappy with management and the lack of a pay increase following his annual review, a network administrator created a backdoor on the company's server. He gave the process a common system file name to disguise the malware and make it appear to be a widely used administration tool. The employee was eventually dismissed but retained unauthorized access to sensitive customer information and confidential documents for weeks afterward.

Impact: Thousands of customer records were compromised and hundreds of thousands of dollars were spent on notification and response, legal, investigative and administrative expenses, reputation management and credit monitoring subscriptions.

Lessons learned: Monitoring employee activity—and using applications designed for anomaly detection—is critical to identifying misuse and suspicious activities. Every user's access should be managed throughout his or her entire employment, not just when they leave the company. It's also important to ensure that hosts used by former employees are taken offline immediately, that a backup is made on an external storage device and the hosts are completely completely rebuilt from trusted media before being reconnected to the network and passed on to another employee.

*This is a fictional account based on the collective experiences of multiple clients, as monitored by IBM Managed Security Services.

Return to text

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

Please Recycle

[1] *IBM X-Force Researcher Finds Significant Vulnerability in Microsoft Windows*

[2] *ICS-CERT Monitor, January – April 2014*, page 1.

[3] *"Cybersecurity in the wake of Sony,"* The Wall Street Journal, February 10, 2015.

[4] The Forrester Wave™: Managed Security Services: North America, Q4 2014, Forrester Research, Inc., November 18, 2014.

SEW03073-USEN-01