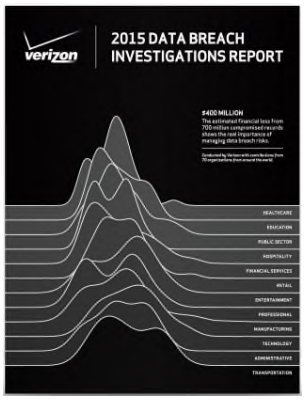
the Availability Digest

www.availabilitydigest.com
@availabilitydig

2015 Verizon Data Breach Investigations Report

August 2015



Every year for the last several years, Verizon has undertaken an extensive survey on data breaches and then published its findings in a detailed Data Breach Investigations Report (DBIR). We summarize their findings for the Year 2014 in this article. The full report can be found at http://www.verizonenterprise.com/DBIR/2015/.

The 2015 report includes input from 70 contributing organizations from around the world. Verizon distinguishes between security incidents and data breaches. A security incident is any event that compromises the confidentiality, integrity, or availability of an information asset. A data breach is an incident that results in confirmed disclosure (not just exposure) of data to an unauthorized party. The 2015 report is based on 79,790 security incidents and 2,122 confirmed data breaches.

The data is broken down into 20 different industry categories. The top three industries affected by security incidents are public services, information, and financial services.

Threat Actors

A threat actor is the entity that is engaging in an attack. About 85% of all threat actors were external. They include criminal organizations and state-sponsored attackers. About 15% were internal employees. A very small percentage were partners.

Verizon defines a “secondary” motive. With such a motive, a victim was targeted as a means to advance a different attack against another victim. One example is the hacking of a website to serve up malware to visitors in the hope that the true target of the actor will become infected. 70% of the attacks in 2014 were secondary attacks. A majority of them were denial-of-service attacks.

The major threat action was stolen credentials. This was followed by RAM scraping and phishing. The incidence of spyware and key logging was down significantly from prior years.

In 60% of the cases, attackers were able to compromise an organization in minutes. It took weeks or months for over 75% of the victims to discover the attacks.

Report Organization

The report is organized into eight major areas:

- Indicators of compromise
- Phishing

- Vulnerabilities
- Mobile
- Malware
- Industry profiles
- Impact
- Internet of Things

The report ends with a classification of incidence patterns.

Indicators of Compromise

There has been a great deal of work on attempting to find indicators that a compromise may occur. To date, this effort has had little success.

One attempt was to combine six months of daily updates from 54 different sources of IP addresses and domain names tagged as malicious by their feed aggregators. This included both inbound feeds (those feeds from which malicious code might be received) and outbound feeds (those feeds to which stolen data might be sent).

The result was that if threat intelligence indicators were really able to help an enterprise defense strategy, one would need to have access to all of the feeds from all of the providers, a Herculean task. There is a need for companies to be able to apply their threat intelligence to their environments in smarter ways.

One possibility is for companies to share their threat information with each other. However, this would have to be very fast and very efficient. Well over 90% of threats are active for only a day. 75% of attacks spread from one victim to another in less than a day – 40% in less than an hour. Clearly, the speed of sharing is key.

Phishing

Phishing uses social engineering to gain a foothold in someone's computer and then on to his network. Typically, an email is sent to an unsuspecting user with a link to a web site that seems innocuous but that is, in fact, malicious. By interacting with the site, the user can give up his credentials such as user names, passwords, bank account numbers, and credit/debit card information.

23% of email recipients open phishing emails, and 11% click on the attachments. Of these, 50% open phishing emails and click on links within the first hour. Phishing was associated with 95% of incidents attributed to state-sponsored attacks. It was associated with two-thirds of cyber-espionage incidents. Statistics show that a campaign of just 10 emails yields a 90% chance that at least one person will become the criminal's prey.

Departments such as Communications, Legal, and Customer Service were far more likely to open an email than all other departments.

Data from the Anti-Phishing Working Group suggests that the phishing infrastructure is quite extensive. Over 9,000 domains and nearly 50,000 phishing URLs are tracked each month.

One of the most effective ways to minimize the phishing threat is through employee awareness. Some companies purposefully send phishing email to their people. When the email is opened opened, the employee will read that he has just opened a phishing email.

Vulnerabilities

A study of 200 million successful exploitations across 500 Common Vulnerability and Exposures (CVE) reports from over 20,000 enterprises in 150 countries was used to create an aggregated picture of

exploited vulnerabilities over time. 99.9% of the exploited vulnerabilities were compromised more than a year after the CVE was published. For the overwhelming majority of attacks exploiting known vulnerabilities, the patch had been available for months prior to the breach. Just because a CVE gets old doesn't mean it goes out of style.

In 2014, ten CVEs accounted for almost 97% of the exploits observed. However, there were seven million other exploited vulnerabilities. Half of the CVEs were exploited within the first two weeks of their publication.

If a vulnerability gets a "cool" name such as Heartbleed, Poodle, or Sandworm, it probably falls within the definition of a critical vulnerability. The bottom line is that all security patches should be applied, some perhaps more quickly than the normal patch cycle.

Mobile

Mobile devices are not a preferred vector in data breaches. That being said, almost all malware attacked Android devices. iOS devices were fairly immune. The bulk of the Android malware can be categorized as *adnoyance-ware*, the receipt of unwanted ads. Over five billion downloaded Android apps are vulnerable to remote attacks.

Out of tens of millions of mobile devices, only 0.03% were infected with truly malicious exploits. 95% of these malware types showed up for less than a month. 80% lasted for less than a week.

Malware

The malware infections of nearly 10,000 organizations were studied in the 2015 DBIR. About five malware events occur every second. Among the top five industries suffering malware infections were:

- Education – 2,332 events/week
- Retail – 801 events/week
- Utilities – 772 events/week
- Insurance – 575 events/week
- Financial Services – 350 events/week

Half of all organizations discovered malware events during 35 or fewer days in 2014.

Malware is getting more varied. In 2005, seven families of malware represented 70% of all malcode activity. This malware focused on email worms. In 2014, 20 malware families represented 70% of all malcode and focused on botnets, credential theft, and fraud.

70% to 90% of malware samples are unique to an organization. This simply means that the signatures (specific code sequences) of a given piece of malware are changed from system to system to avoid detection by anti-virus utilities.

Financial services organizations fix most infections within one day. Insurance organizations fix about half in three days, and retail organizations fix half in about seven days. Utilities fix half of infections in about 10 days. It takes educational organizations about 50 days to fix half of all infections. This is probably to be expected given the regular influx of unmanaged devices as hordes of youth invade the halls of higher learning.

Industry Profiles

Various industries exhibit substantially different threat profiles and therefore cannot have the same remediation priorities. Security standards that treat all requirements as equal stepping stones on a path to 100% compliance are not effective. There is no "one size fits all" approach.

Even within industries, there are widely distributed clusters of attack vectors. For instance, financial services shows four distinct and widespread types of attacks. Information industries show seven clusters, while accommodation show two clusters. On the other hand, there are clusters of attack vectors containing several industries. Many subsectors in different industries share a closer threat profile than do subsectors in the same industry. For instance, two manufacturing subsectors have more in common with central banks than they have with each other.

These observations highlight the need for more thoughtful and thorough research into risk profiles across various types of organizations. Maybe cyber risk has more to do with business models or organizational structure or company policies than under which high-level industry a company falls. It follows that the standard practice of organizing information-sharing groups and activities according to broad industries as is the arrangement in this report is less than optimal and may even be counterproductive.

Impact

The cost of data breaches was studied using information from 191 insurance claims for loss of payment cards, personal information, and personal medical records.

The average cost for a lost record based on corporate estimates of the cost of lost data was USD $201 in 2014, up from $188 in 2013. However, based on insurance records, the actual average cost of a lost record was USD $0.58.

Part of this discrepancy is the exclusion of soft costs that don't show up in the insurance data. Another factor has to do with the extent of the loss. The larger the number of records lost, the less cost there was per record. For losses of under 100 records, the average cost was about USD $1,000 per record. For losses of 1,000 records, the average cost was $100 per record. For losses of 10,000 records, the average cost was $10 per record. For losses of 100,000 records, the average cost was $1.50 per record. For losses of one million records, the average loss was $1 per record. For losses of ten million records, the average cost was about $0.20 per record. For losses of 100 million records, the cost was about $0.10 per record.

Larger organizations had higher costs per breach because they typically lost more records than smaller organizations and thus had higher overall costs.

The Internet of Things (IoT)

No widely known IoT breaches have occurred. Most of the breaches reported in the media were proof of concept.

However, the industry expects exponential growth of IoT over the next five years. Verizon predicts that there will be over 5 billion IoT devices by the end of this decade.

Many of the devices will be simple unitaskers. When developing IoT devices aimed at millions of customers, cost is particularly important. Software to protect the device adds cost. It is fruitless to expect that security will have the same priority from developers as does device functionality.

Incidence Classification Patterns

96% of all incidences fell into one of nine categories. The frequency of incidences for different classifications for 2014 are summarized below:

- Miscellaneous errors – 29.4%
- Crimeware – 25.1%
- Insider misuse – 20.6%

- Physical theft/loss – 15.3%
- Web app attacks – 4.1%
- Denial of service – 3.9%
- Cyber-espionage – 0.8%
- POS intrusions – 0.7%
- Payment card skimmers – 0.1%

The common denominator across the top four categories – accounting for over 90% of all incidents – is people.

However, the above results are for incidences. The story on confirmed breaches is different. For instance, POS intrusions accounted for 0.7% of all incidences but 28.5% of all breaches. The frequency of breaches for the various categories follows. Included are the industries most affected by each.

- POS intrusions – 28.5% (accommodations, entertainment, retail)
- Crimeware – 18.8% (public, information, retail)
- Cyber-espionage – 18% (manufacturing, public, professional)
- Insider misuse – 10.6% (public, healthcare, financial services)
- Web app attacks – 9.4% (information, financial services, public)
- Miscellaneous errors – 8.1% (public, information, healthcare)
- Physical theft/loss – 3.3% (public, healthcare, financial services)
- Payment card skimmers – 3.1% (financial services, retail)
- Denial of service – 0.1% (public, retail, financial services)

Year in Review

The report lists the major malware infections for each month of 2015:

Month	Malware	Impact
January	Snapchat	4.5 million compromised names and phone numbers
February	Kickstarter	5.6 million victims
March	Korean Telecom	One of the year's largest breaches affecting 12 million customers
April	Heartbleed	First of three open-source vulnerabilities in 2014
May	eBay	Database of 145 million customers compromised
June	PF Chang's	Most high-profile data breach of the month
July	Energetic Bear	Cyber-spying operation directed at the energy industry
August	Cybervor	1.2 billion compromised credentials
September	iCloud	Celebrity accounts hacked
October	Sandworm	Attacked a Windows vulnerability
November	Sony Pictures	Highest-profile hack of the year
December	Inception Framework	Cyber-espionage attack targeted the public sector

Wrap-Up

The changes in the report for this year from the previous year are not statistically significant.

The report tallied the percentage of incidents in which a critical security control (CSC) could be applied as the recommended strategy. The results are shown in the table below.

Critical Security Control	Percentage	Category
Two-factor authentication	24%	Visibility/Attribution
Patching web services	24%	Quick Win
Internet-facing devices	7%	Visibility/Attribution

Proxy outbound traffic	7%	Visibility/Attribution
Web application testing	7%	Visibility/Attribution
User lockout after multiple failed attempts	5%	Quick Win
Block known file-transfer sites	5%	Advanced
Mail attachment filtering	5%	Quick Win
Limiting ports and services	2%	Quick Win
Segregation of networks	2%	Configuration/Hygiene
Password complexity	2%	Visibility/Attribution
Restrict ability to download software	2%	Quick Win
Anti-virus	2%	Quick Win
Vet security process of vendor	2%	Configuration/Hygiene

It is interesting to note that 40% of controls determined to be most effective were in the “Quick Win” category. These are controls that are the easiest to implement.