2012 Trends, Volume 18, Published April 2013

Symantec

ISTR

INTERNET SECURITY THREAT REPORT 2013

CONTENTS

Introduction

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of approximately 69 million attack sensors and records thousands of events per second. This network monitors threat activity in over 157 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services and Norton™ consumer products, and other third-party data sources.

In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 51,644 recorded vulnerabilities (spanning more than two decades) from over 16,687 vendors representing over 43,391 products.

Spam, phishing, and malware data is captured through a variety of sources, including the Symantec Probe Network, a system of more than 5 million decoy accounts; Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology, is able to detect new and sophisticated targeted threats before reaching customers' networks. Over 3 billion email messages and more than 1.4 billion Web requests are processed each day across 14 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

Symantec Trust Services provides 100 percent availability and processes over 4.5 billion Online Certificate Status Protocol (OCSP) look-ups per day, which are used for obtaining the revocation status of X.509 digital certificates around the world.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report, which gives enterprises, small businesses, and consumers the essential information to secure their systems effectively now and into the future.

Executive Summary

Threats to online security have grown and evolved considerably in 2012. From the threats of cyberespionage and industrial espionage to the widespread, chronic problems of malware and phishing, we have seen constant innovation from malware authors.

We have also seen an expansion of traditional threats into new forums. In particular, social media and mobile devices have come under increasing attack in 2012, even as spam and phishing attacks via traditional routes have fallen. Online criminals are following users onto these new platforms.

The most important trends in 2012 were:

Small Businesses Are the Path of Least Resistance for Attackers

Last year's data made it clear that any business, no matter its size, was a potential target for attackers. This was not a fluke. In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees. In fact, the largest growth area for targeted attacks in 2012 was businesses with fewer than 250 employees; 31 percent of all attacks targeted them.

This is especially bad news because based on surveys conducted by Symantec, small businesses believe they are immune to attacks targeted at them. However, money stolen from a small business is as easy to spend as money stolen from a large business. And while small businesses may assume that they have nothing a targeted attacker would want to steal, they forget that they retain customer information, create intellectual property, and keep money in the bank. While it can be argued that the rewards of attacking a small business are less than what can be gained from a large enterprise, this is more than compensated by the fact that many small companies are typically less careful in their cyberdefenses. Criminal activity is often driven by crimes of opportunity. With cybercrimes, that opportunity appears to be with small businesses.

Even worse, the lack of adequate security practices by small businesses threatens all of us. Attackers deterred by a large company's defenses often choose to breach the lesser defenses of a small business that has a business relationship with the attacker's ultimate target, using the smaller company to leap frog into the larger one.

Additionally, small businesses and organizations can become pawns in more sophisticated attacks. Driven by attack toolkits, in 2012 the number of Web-based attacks increased by one third and many of these attacks originated from the compromised websites of small businesses. These massive attacks increase the risk of infection for all of us. But even more nefariously, as reported in our Elderwood white paper last year, the websites of small businesses and organizations are even being used in targeted attacks. Supplementing their phishing attacks, cyberespionage gangs now hijack these websites, lying in wait for their targets to visit so that they can infect them. This type of attack, called a watering hole, is another way attackers leverage weak security of one entity to defeat the strong security of another.

Malware Authors Act as Big Brother

If you think someone is violating your privacy online, you are probably right. Fifty percent of mobile malware created in 2012 attempted to steal our information or track our movements. Whether they are attacking our computers, mobile phones or social networks, Cyber-criminals are looking to profit by spying on us. Their ultimate goal is to make money. Their method is to learn our banking information, the phone numbers and email addresses of our friends and business associates, our personal information, and even how to become us by stealing our identity.

But the most ominous example of malware authors knowing all about us is in targeted attacks. Creating successful targeted attacks requires attackers to learn about us. They will research our email addresses, our job, our professional interests, and even the conferences we attend and the websites we frequent. All of this information is compiled to launch a successful targeted attack. Once on our devices, the attacker's tools are designed to pull as much data as possible. Undiscovered targeted attacks can collect years of our email, files, and contact information. These tools also contain the ability to log our keystrokes, view our computer screens, and turn on our computers' microphones and cameras. Targeted attackers truly act as an Orwellian incarnation of Big Brother.

Those jobs most targeted for attack in 2012 were knowledge workers who create the intellectual property that attackers want (27 percent of all targets in 2012) and those in sales (24 percent in 2012). Interest in targeting the CEO of an organization waned in 2012; those attacks decreased by 8 percent.

With Mobile, It's Not the Vulnerability that Will Get You

As expected, the amount of mobile malware in 2012 continues to rise. 2012 saw a 58 percent increase in mobile malware families compared to 2011. The year's total now accounts for 59 percent of all malware to-date. With a 32 percent increase in the number of vulnerabilities reported in mobile operating systems, it might be tempting to blame them for the increase. However, this would be wrong. In the PC space, a vulnerability drives attacks as new vulnerabilities are incorporated into commonly available toolkits. The more they're used, the faster they spread. This is not occurring in the mobile space. Today, mobile vulnerabilities have little or no correlation to mobile malware. In fact, while Apple's iOS had the most documented vulnerabilities in 2012, there was only one threat created for the platform. Compare this to the Android OS; although only thirteen vulnerabilities were reported, it led all mobile operating systems in the amount of malware written for the platform.

Vulnerabilities likely will become a factor in mobile malware, but today Android's market share, the openness of the platform, and the multiple distribution methods available to applications embedded with malware make it the go-to platform of malware authors.

Zero-day Vulnerabilities Available When Attackers Need Them

Zero-day vulnerabilities continue to trend upward; 14 were reported in 2012. In the last three years much of the growth in zero-day vulnerabilities used in attacks can be attributed to two groups; the authors of Stuxnet and the Elderwood Gang. In 2010, Stuxnet was responsible for 4 of the 14 discovered zero-day vulnerabilities. The Elderwood Gang was responsible for 4 of the 14 discovered in 2012. The Elderwood Gang also used zero-day threats in 2010 and 2011, and they've used at least one so far in 2013.

Attackers use as many zero-day vulnerabilities as they need, not as many as they have. And Stuxnet and Elderwood make for an interesting contrast in the strategy of their use. Stuxnet remains the aberration, using multiple zero-day exploits in one attack. From what we know today, it was a single attack that was directed at a single target. Multiple zero-day exploits were used to ensure success so they would not need to attack a second time.

By contrast the Elderwood Gang has used one zero-day exploit in each attack, using it continually until that exploit becomes public. Once that occurs they move on to a new exploit. This makes it seem that the Elderwood Gang has a limitless supply of zero-day vulnerabilities and is able to move to a new exploit as soon as one is needed. It is our hope that this is not the case.

Attribution Is Never Easy

Some targeted attacks make no attempt to stay undetected. A piece of malware named Shamoon was discovered in August. Its purpose was to wipe computer hard drives of energy companies in the Middle East. A group calling itself the "Cutting Sword of Justice" claimed responsibility. Throughout 2012, DDoS attacks were launched against financial institutions. A group called Izz ad-Din al-Qassam Cyber Fighters claimed responsibility.

These attacks and others appear to be classic cases of hacktivism. However, proving attribution and motive are not easy, even when someone claims responsibility. There has been much speculation, some reportedly from the intelligence community, that the Cutting Sword of Justice and the Qassam Cyber Fighters are fronts for a nation state. Complicating what appeared to be simple hactivism even further is the FBI's warning to financial institutions that some DDoS attacks are actually being used as a "distraction." These attacks are launched before or after cybercriminals engage in an unauthorized transaction, and are an attempt to avoid discovery of the fraud and prevent attempts to stop it.

2012 SECURITY TIMELINE

2012 Security Timeline

01 January

Data breach:

24 million identities stolen in data breach at Zappos apparel company.

Malcode:

A scam involving malicious browser plug-ins for Firefox and Chrome is discovered.

02 February

Botnet:

Kelihos botnet returns, four months after being taken down.

Mobile:

Google announces Google Bouncer, an app scanner for the Google Play market.

03 March

Botnet:

Researchers take down new variant of the Kelihos botnet, which reappears in a new form later in the month.

Hacks:

Six individuals are arrested as alleged members of the hacking collective LulzSec.

Botnet:

Security researchers take down key servers for the Zeus botnet.

Data breach:

A payment processor for a number of well-known credit card companies, including Visa and MasterCard was compromised, exposing details of 1.5 million accounts.[1]

Mobile:

A non-malware-based scam involving the Opfake gang is found that targets iPhone users.

04 April

Mac:

Over 600,000 Mac computers are infected by the OSX.Flashback Trojan through an unpatched Java exploit.

Mac:

A second Mac Trojan is discovered, OSX.Sabpab, which also uses Java exploits to compromise a computer.

05 May

Social networking:

Scammers are discovered leveraging social networks Tumblr and Pinterest.

Malware:

The cyberespionage threat W32.Flamer is discovered.

Certificate Authorities:

Comodo, a large Certificate Authority, authenticated and issued a legitimate code-signing certificate to a fictitious organization run by cybercriminals. This was not discovered until August.

06 June

Data breach:

LinkedIn suffers data breach, exposing millions of accounts.

Malware:

A Trojan by the name of Trojan.Milicenso is discovered, which causes networked printers to print large print jobs containing illegible characters.

07 July

Botnet:

Security researchers disable the Grum botnet.

Malware:

Windows malware is discovered in Apple's App Store, embedded in an application.

Mac:

A new Mac threat called OSX.Crisis opens a back door on compromised computers.

Botnet:

DNS servers, maintained by the FBI in order to keep computers previously infected with the DNSChanger Trojan safe, are shut off.

Malware:

A Trojan used to steal information from the Japanese government is discovered after being in operation for two years.

Malware:

A second printer-related threat called W32.Printlove, which causes large print jobs to print garbage, is discovered.

08 August

Hacks:

Reuters news service suffers a series of hacks resulting in fake news stories posted on its website and Twitter account.

Malware:

Crisis malware is discovered targeting VMware® virtual machine images.

Malware:

W32.Gauss is discovered. The scope of the threat is concentrated in the Middle East, in a similar way to W32.Flamer.

Certificate Authorities:

Comodo incident from May discovered and details published.

09 September

Malware:

A new version of the Blackhole attack toolkit, dubbed Blackhole 2.0, is discovered.

Botnet:

Security researchers disable an up-and-coming botnet known as "Nitol."

Mobile:

A vulnerability is discovered in Samsung's version of Android™ that allows a phone to be remotely wiped.

DDoS:

FBI issues warning about possible DDoS attacks against financial institutions as part of a "distraction" technique.[2]

10 October

Malware:

A ransomware threat distributed through Skype IM is discovered.

Data breach:

Customer data is stolen from Barnes & Noble payment keypads.

Attackers are discovered using a DDoS attack as a distraction in order to gather information that allowed them to later steal money from a targeted bank.

11 November

Hacks:

Burglars found using a known exploit in a brand of hotel locks to break into hotel rooms.

12 December

Malware:

Infostealer.Dexter Trojan horse discovered targeting point-of-sale systems.

Hacks:

Attackers exploit a vulnerability in Tumblr, spreading spam throughout the social network.

2012 IN NUMBERS

2012 in Numbers

Targeted Attacks in 2012

42% INCREASE

New Vulnerabilities

2010	2011	2012
6,253	4,989	5,291

Average Number of Identities Exposed Per Breach in 2012

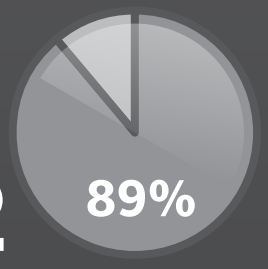
604,826

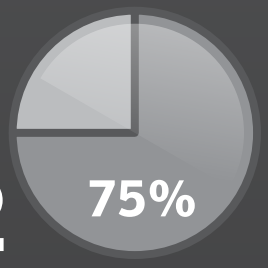
Mobile Vulnerabilities

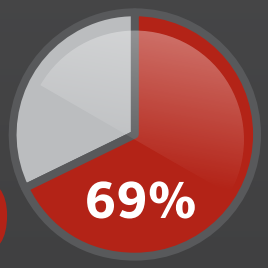
2012	415
2011	315
2010	163

Estimated Global Email Spam Per Day (in billions)

OVERALL SPAM RATE







% of All Spam with Dating & Sexual

3% 2010

15% 2011

55% 2012

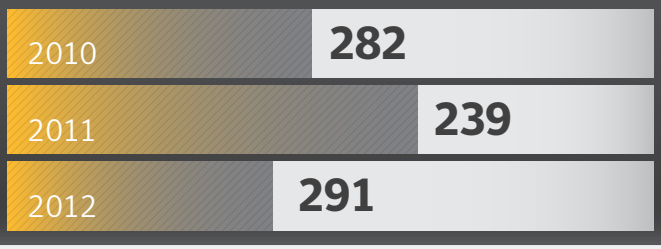
% of All Email Malware as URL

24% 2010

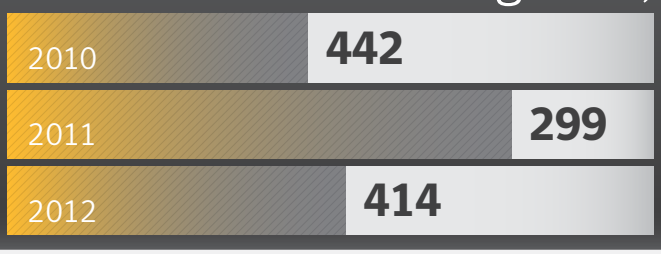
39% 2011

23% 2012

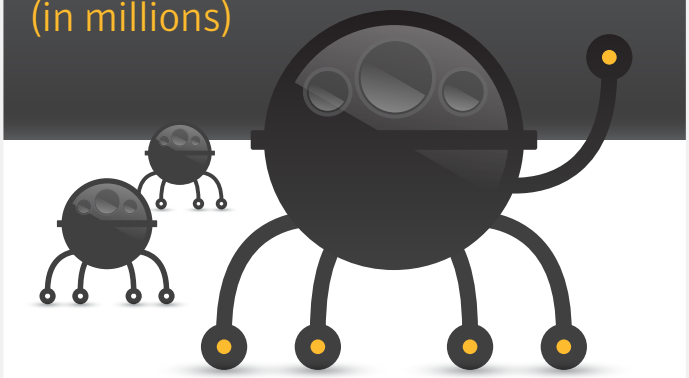
Overall Email Virus Rate, 1 In:



Overall Email Phishing Rate, 1 In:



Bot Zombies
(in millions)



2010	4.5
2011	3.1
2012	3.4

New Zero-Day Vulnerabilities

2010	2011	2012
14	8	14

Web Attacks Blocked Per Day

2011	190,370
2012	247,350

Mobile Malware Families Increase
2011–2012

58%

New Unique Malicious Web Domains

2010	43,000
2011	55,000
2012	74,000

TARGETED ATTACKS, HACKTIVISM AND DATA BREACHES

Introduction

"Just as nuclear was the strategic warfare of the industrial era, cyberwarfare has become the strategic war of the information era," says U.S. Secretary of Defense Leon Panetta.[3] Cyberespionage and cybersabotage are already a reality.

Outside the realm of states and their proxies, corporate spies are using increasingly advanced techniques to steal company secrets or customer data for profit. Hactivists with political and antibusiness agendas are also busy.

The string of media revelations about security breaches this year suggests that the business world is just as vulnerable to attack as ever.

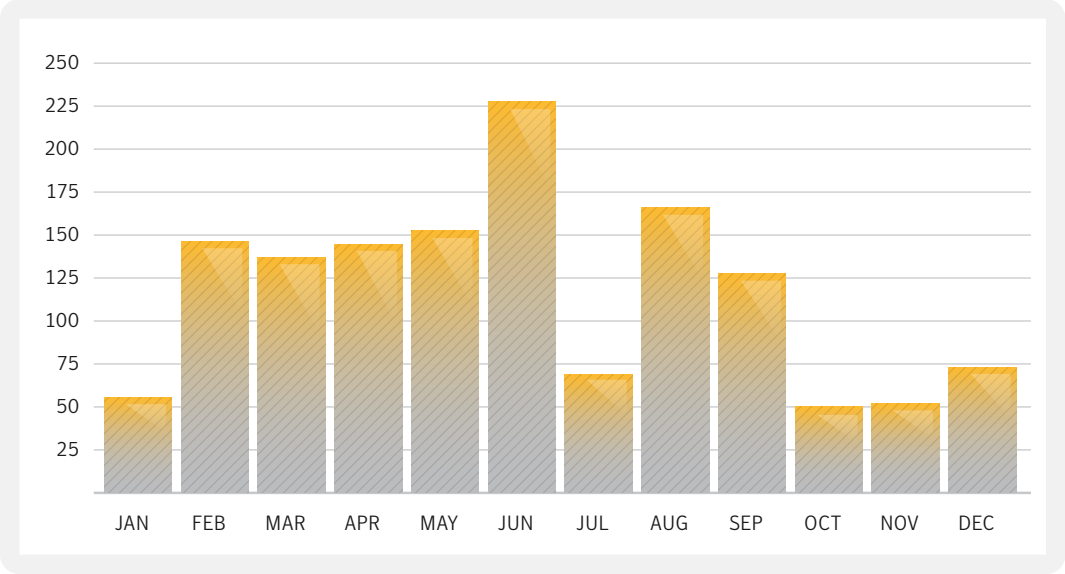
At a Glance

- Targeted attack global average per day: 116.
- Increasing levels of industrial espionage and data theft.
- More insidious targeted attacks, with new "watering hole" attacks and sophisticated social engineering.
- Fewer big data breaches, but the median number of identities stolen per breach has increased by 3.5 times.

Data

Targeted Attacks Per Day in 2012

Source: Symantec

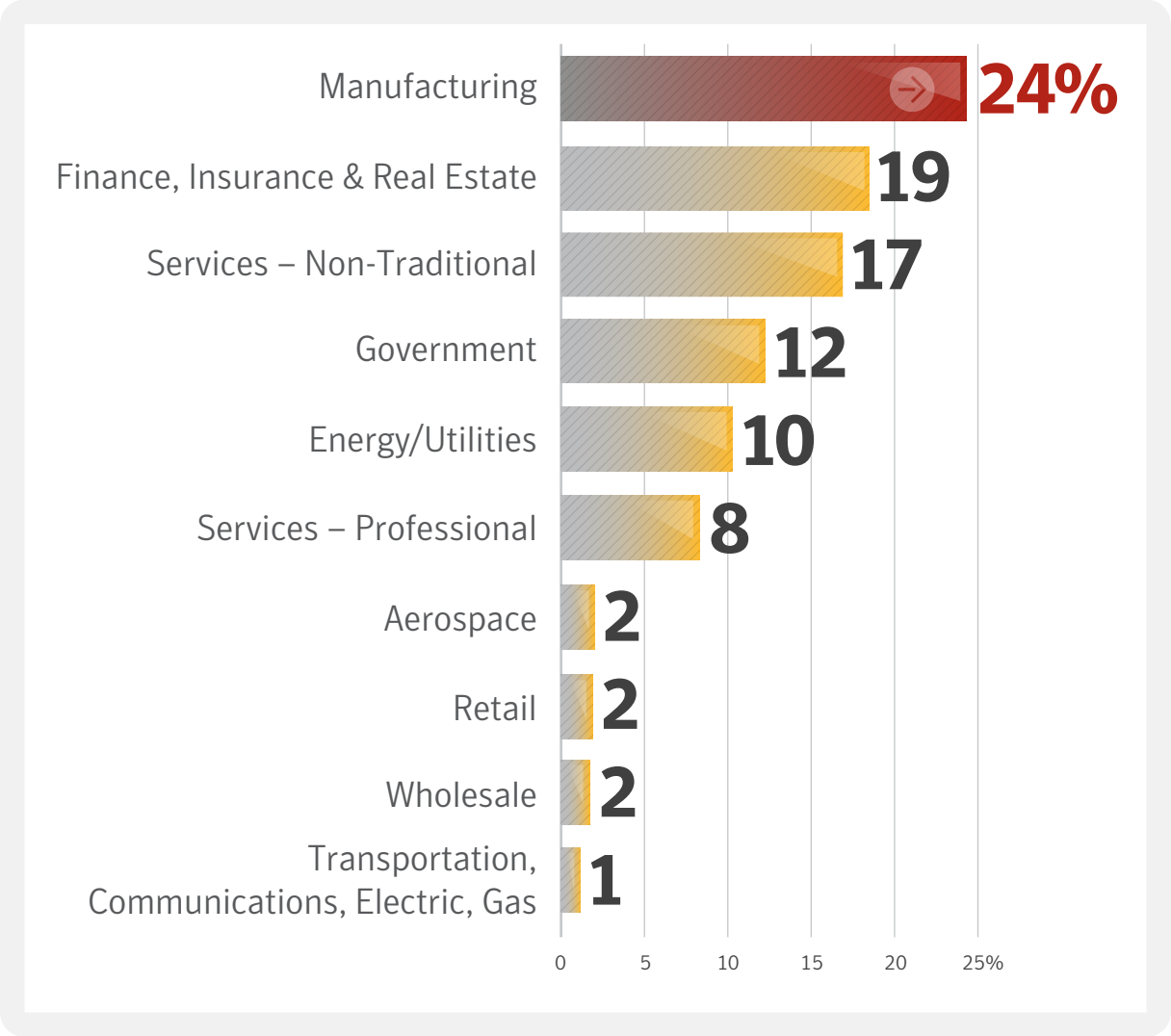


The global average number of attacks per day in 2012 was 116, compared with 82 in 2011 and 77 in 2010. We witnessed one large attack in April, and while events like this are extremely rare, it resulted in a large jump for that month. Without accounting for this, the global average would be nearer to 143 per day with this company included.

This client was a large banking organization, who had not previously been a Symantec customer, and approached Symantec for help to remove an existing infection. The infection was removed; however, a large wave of targeted attacks followed as the attackers sought to regain access, ultimately failing.

Top 10 Industries Attacked in 2012

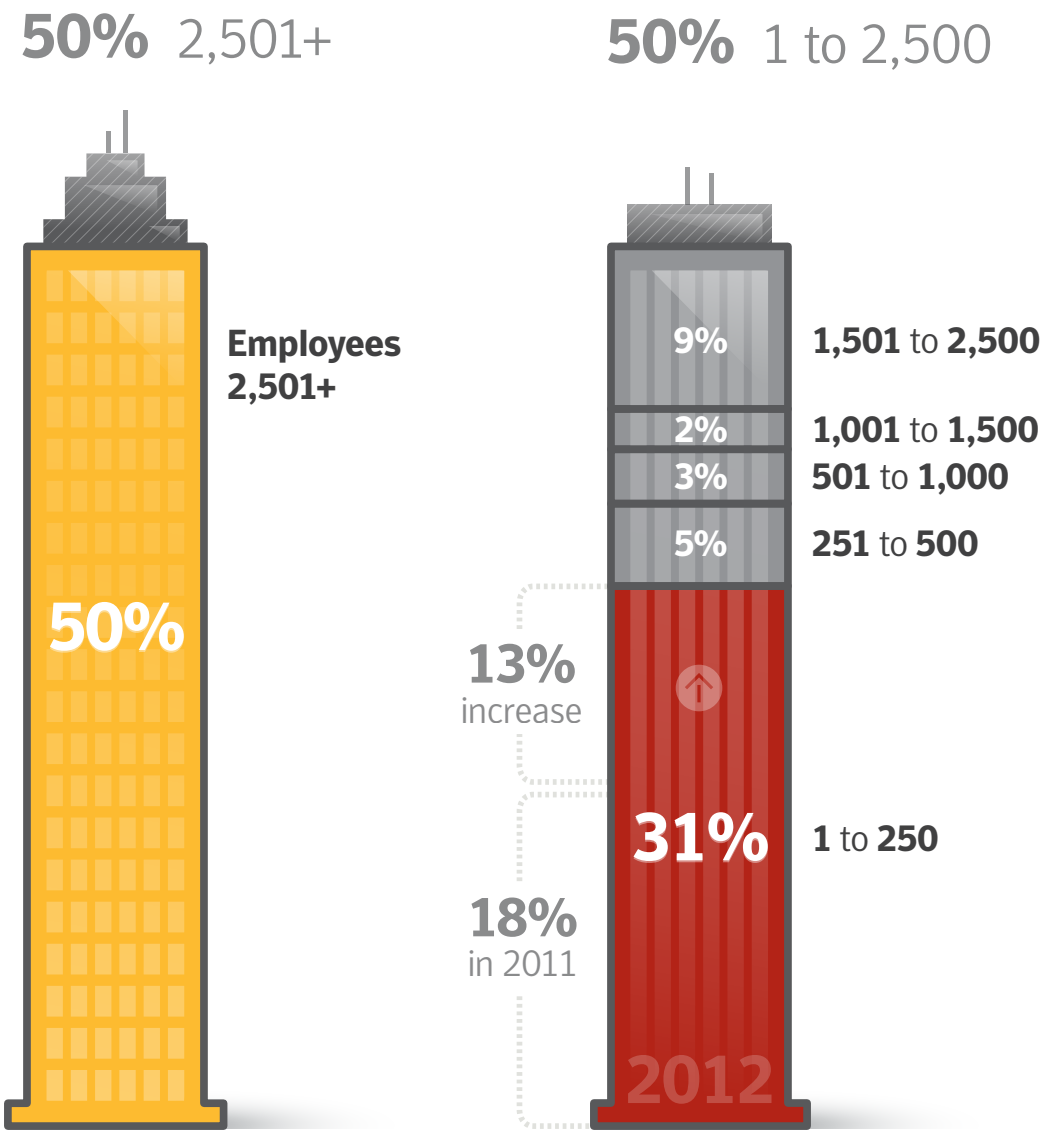
Source: Symantec



Manufacturing was the most-targeted sector in 2012, with 24 percent of targeted attacks destined for this sector, compared with 15 percent in 2011. Attacks against government and public sector organizations fell from 25 percent in 2011, when it was the most targeted sector, to 12 percent in 2012. It's likely the frontline attacks are moving down the supply chain, particularly for small to medium-sized businesses. (Categories based on Standard Industrial Classification codes.)

Attacks by Size of Targeted Organization

Source: Symantec

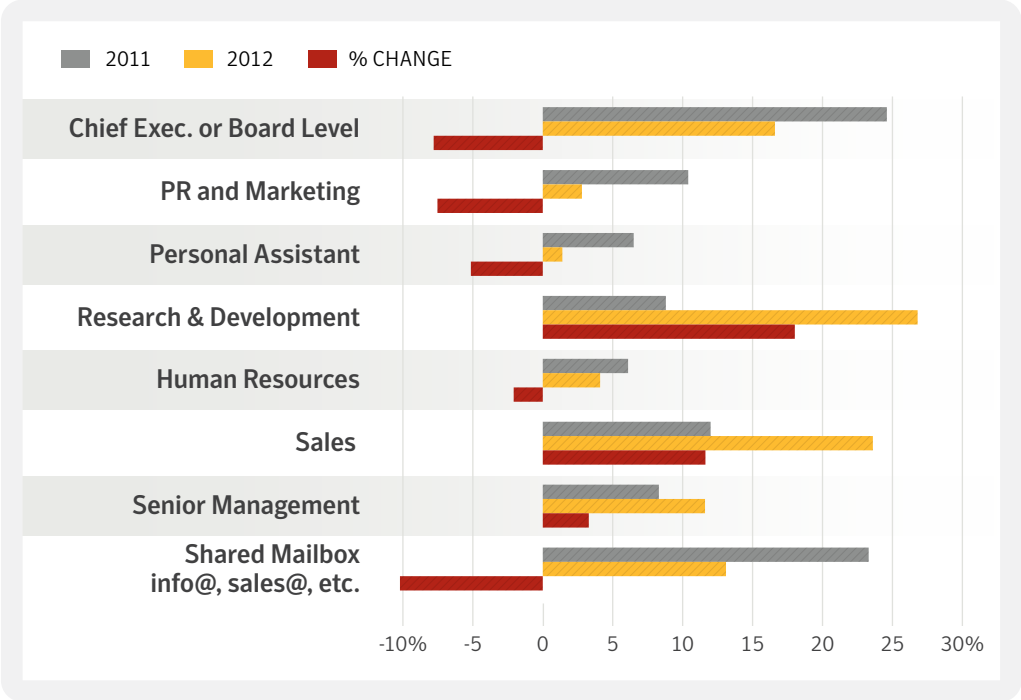


Organizations with 2,501+ employees were the most targeted with 50 percent of targeted attacks destined for this size of organization, almost exactly the same percentage as in 2011.

Targeted attacks destined for Small Business (1 to 250 employees) accounted for 31 percent of all attacks, compared with 18 percent in 2011, an increase of 13 percent.

Targeted Attack Recipients by Role in 2012

Source: Symantec



In 2012, the most frequently targeted job role was in R&D, which accounted for 27 percent of attacks (9 percent in 2011). The second most notable increase was against sales representatives, probably because their contact details are more widely available in the public domain, with 24 percent of attacks in 2012 versus 12 percent in 2011. In 2011, C-level executives were the most targeted, with 25 percent, but this number fell to 17 percent in 2012.

DDoS Used as a Diversion

In September, the FBI issued a warning to financial institutions that some DDoS attacks are actually being used as a "distraction." These attacks are launched before or after cybercriminals engage in an unauthorized transaction and are an attempt to avoid discovery of the fraud and prevent attempts to stop it.

In these scenarios, attackers target a company's website with a DDoS attack. They may or may not bring the website down, but that's not the main focus of such an attack; the real goal is to divert the attention of the company's IT staff towards the DDoS attack. Meanwhile, the hackers attempt to break into the company's network using any number of other methods that may go unnoticed as the DDoS attack continues in the background.[4]

Data Breaches

The overall number of data breaches is down by 26 percent, according to the Norton Cybercrime Index,[5] though over 93 million identities were exposed during the year, a decrease of 60 percent over last year. The average number of identities stolen is also down this year: at 604,826 per breach, this is significantly smaller than the 1.1 million per breach in 2011.

So why are the number of breaches and identities stolen down in 2012? For starters, there were five attacks in which more than 10 million identities were stolen in 2011. In 2012 there was only one, which results in a much smaller spread from the smallest to the largest data breach. However, the median number—the midpoint of the data set—increased by 3.5 times in 2012, from 2,400 to 8,350 per breach. Using the median is a useful measure because it ignores the extremes, the rare events that resulted in large numbers of identities being exposed, and is more representative of the underlying trend.

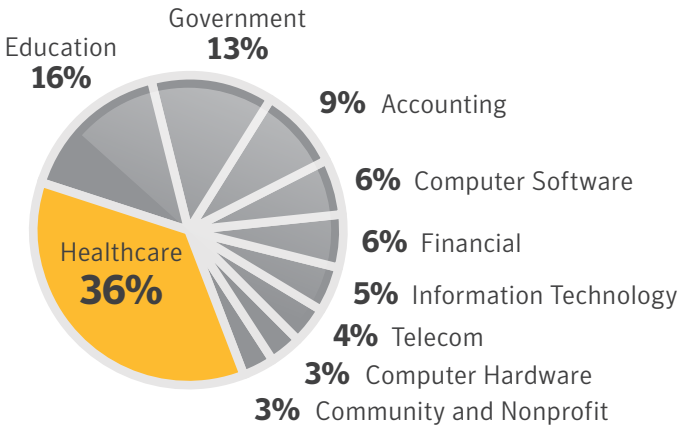
Part of the wide difference between data breaches in 2011 and 2012 is likely down due to a concerted effort by the notorious hacker groups Anonymous and LulzSec to publicize hacks during 2011—something that was not seen to the same extent in 2012. It's possible that companies are paying more attention to protecting customer databases or that hackers have found other, more valuable targets, or that they are still stealing the data but not being detected.

Healthcare, education, and government accounted for nearly two-thirds of all identities breached in 2012. This suggests that the public sector should further increase efforts to protect personal information, particularly considering how these organizations are often looked upon as the custodians of information for the most vulnerable in society. Alternatively, this could indicate that the private sector may not be reporting all data breaches, given how many public sector organizations are required by law to report breaches.

The vast majority (88 percent) of reported data breaches were due to attacks by outsiders. But it is safe to assume that unreported data breaches outnumber reported ones. Whether it is lost laptops, misplaced memory sticks, deliberate data theft by employees or accidents, the insider threat also remains high. To illustrate this point, the UK Information Commissioner's Office fined and prosecuted more businesses because of insider slipups than because of outsider attacks. Most SMBs should worry about someone in accounts just as much as they should worry about an anonymous hacker.

Data Breaches by Sector in 2012

Source: Symantec



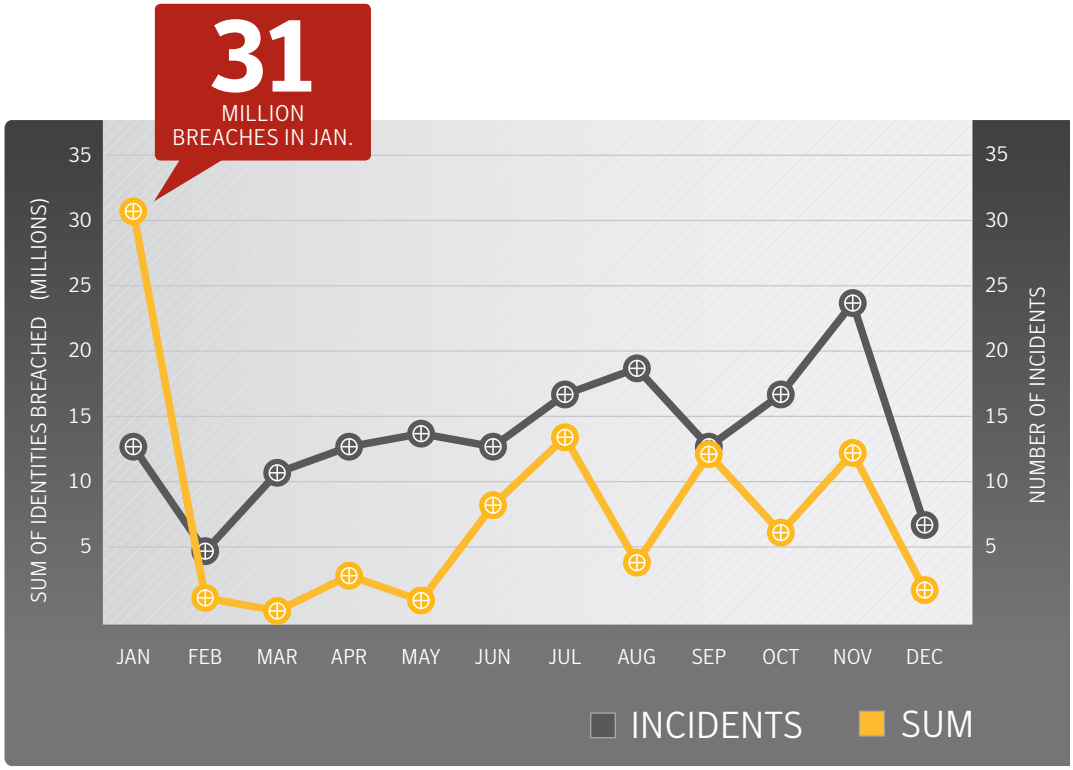
At 36 percent, the healthcare industry continues to be the sector responsible for the largest percentage of disclosed data breaches by industry.

Timeline of Data Breaches

Source: Symantec

January saw the largest number of identities stolen in 2012, due to one breach of over 24 million identities, while the numbers of the rest of the year mostly fluctuated between one and 12 million identities stolen per month.

The average number of breaches for the first half of the year was 11, and rose to 15 in the second half of the year– a 44 percent increase.



Average Cost Per Capita of a Data Breach [6]

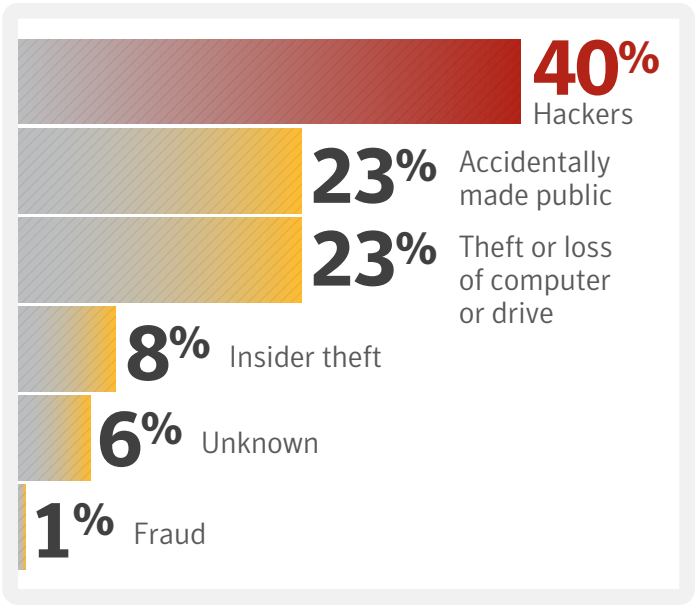
Source: Symantec

Country	Average Cost Per Capita
U.S.	$194
Denmark	$191
France	$159
Australia	$145
Japan	$132
UK	$124
Italy	$102
Indonesia	$42

At US$194, the United States is the country with highest in cost per capita, with Denmark a close second at $191 per capita.

Top Causes of Data Breaches in 2012

Source: Symantec



Hackers continue to be responsible for the largest number of data breaches, making up 40 percent of all breaches.

Analysis

Cyberwarfare, Cybersabotage, and Industrial Espionage

Targeted attacks have become an established part of the threat landscape and safeguarding against them has become one of the main concerns of CISOs and IT managers. Targeted attacks are commonly used for the purposes of industrial espionage to gain access to the confidential information on a compromised computer system or network. They are rare but potentially the most difficult attacks to defend against.

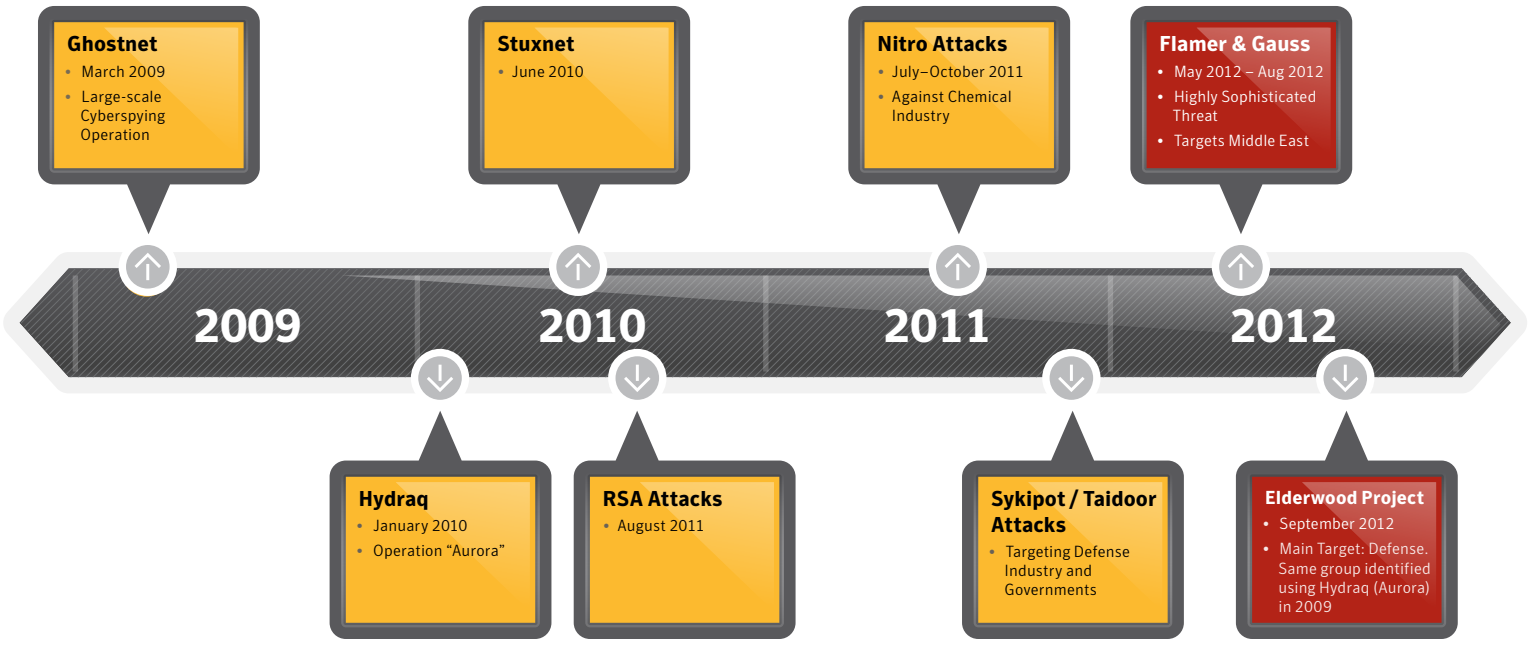
It is difficult to attribute an attack to a specific group or a government without sufficient evidence. The motivation and the resources of the attacker sometimes hint to the possibility that the attacker could be state sponsored, but finding clear evidence is difficult. Attacks that could be state sponsored, but appear to be rare in comparison with regular cybercrime, though they have often gained more notoriety. They can be among the most sophisticated and damaging of these types of threats. Governments are undoubtedly devoting more resources to defensive and offensive cyberwarfare capabilities. In 2012, it was still unlikely that most businesses would encounter such an attack, and the greatest risk comes from the more prevalent targeted attacks that are created for the purposes of industrial espionage. Increasingly, small to medium-sized businesses (SMB) are finding themselves on the frontline of these targeted attacks as they have fewer resources to combat the threat and a successful attack here may subsequently be used as the springboard to further attacks against a larger organization to which they may be a supplier.

Malware such as Stuxnet in 2010, Duqu in 2011, and Flamer and Disttrack in 2012 show increasing levels of sophistication and danger. For example, the malware used in the Shamoon attacks on a Saudi oil firm had the ability to wipe hard drives.[7]

The same techniques used by cybercriminals for industrial espionage, may also be used by states and state proxies for cyber attacks and political espionage. Sophisticated attacks may be reverse-engineered and copied so that the same or similar

Timeline of Targeted Attacks [8]

Source: Symantec



techniques can be used in less discriminate attacks. A further risk is that malware developed for cybersabotage may spread beyond its intended target and infect other computers in a kind of collateral damage.

Advanced Persistent Threats and Targeted Attacks

Targeted attacks combine social engineering and malware to target individuals in specific companies with the objective of stealing confidential information such as trade secrets or customer data. They often use custom-written malware and sometimes exploit zero-day vulnerabilities, which makes them harder to detect and potentially more infective.

Targeted attacks use a variety of vectors as their main delivery mechanism, such as malware delivered in an email, or drive-by downloads from an infected website the intended recipient is known to frequent, a technique known as a "watering hole" attack.

APTs are often highly sophisticated and more insidious than traditional attacks, relying on highly customized intrusion techniques. While targeted attacks are growing increasingly more common, the resources required to launch an advanced persistent threat campaign means they are limited to well-funded groups attacking high-value targets.

Symantec saw a 42 percent increase in the targeted attack rate in 2012 compared with the preceding 12 months. While the manufacturing industry has become the main target accounting for 24 percent of attacks, we also saw a wide range of companies coming under attack, not only large businesses, but increasingly SMBs as well. In 2011, 18 percent of targeted attacks were aimed at companies with fewer than 250 employees, but by the end of 2012, they accounted for 31 percent.

Social Engineering and Indirect Attacks

Attackers may be targeting smaller businesses in the supply chain because they are more vulnerable, have access to important intellectual property, and offer a stepping stone into larger organizations. In addition, they are also targeted in their own right. They are more numerous than enterprises, have valuable data, and are often less well-protected than larger companies. For example, an attacker may infiltrate a small supplier in order to use it as a spring board into a larger company. They might use personal information, emails, and files from an individual in such a smaller company to create a well-

Web Injection Process Used in Watering Hole Attacks [9]

Source: Symantec

crafted email aimed at someone in a target company.

In 2012, we saw a big increase in attacks on people in R&D and sales roles compared to the previous year. This suggests that attackers are casting a wider net and targeting less senior positions below the executive level in order to gain access to companies. The increase in attacks has been particularly high overall in these two areas. Still, attacks in other areas, such as back-office roles, are still a significant threat.

Attackers continue to use social engineering techniques in targeted attacks. For example, messages impersonating EU officials, messages that appear to come from security agencies in the United States and target other government officials, or messages that piggyback announcements about new procurement plans from potential government clients such as the U.S. Air Force. This shows extensive research, a sophisticated understanding of the motivation of recipients, and makes it much more likely that victims will open attachments that contain malware.

Watering Hole Attacks

The biggest innovation in targeted attacks was the emergence of watering hole attacks. This involves compromising a legitimate website that a targeted victim might visit and using it to install malware on their computer. For example, this year we saw a line of code in a tracking script[10] on a human rights organization's website with the potential to compromise a computer. It exploited a new, zero-day vulnerability in Internet Explorer® to infect visitors. Our data showed that within 24 hours, people in 500 different large companies and government organizations visited the site and ran the risk of infection. The attackers in this case, known as the Elderwood Gang, used sophisticated tools and exploited zero-day vulnerabilities in their attacks, pointing to a well-resourced team backed by a large criminal organization or a nation state.[11]

Recommendations

Assume You're a Target.

Small size and relative anonymity are not defenses against the most sophisticated attacks. Targeted attacks threaten small companies as well as large ones. Attackers could also use your website as a way to attack other people. If you assume you are a potential target and improve your defenses against the most serious threats, you will automatically improve your protection against other threats.

Defense in Depth.

Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network. Endpoints must be secured by more than signature-based antivirus technology.

Educate Employees.

Raise employees' awareness about the risks of social engineering and counter it with staff training. Similarly, good training and procedures can reduce the risk of accidental data loss and other insider risks. Train staff about the value of data and how to protect it.

Data Loss Prevention.

Prevent data loss and exfiltration with data loss protection software on your network. Use encryption to protect data in transit, whether online or via removable storage.

VULNERABILITIES, EXPLOITS, AND TOOLKITS

Introduction

Recent research by the Ponemon Institute suggests that the cost of cybercrime rose by six percent in 2012 with a 42 percent increase in the number of cyberattacks. The cost is significant with businesses incurring an average cost of $591,780.[12] Given the increase availability of vulnerabilities and exploits it comes as no surprise that the cybercriminals have increased their ability to make a profit.

Quite a few diverse skills are needed to find vulnerabilities, create ways to exploit them, and then run attacks using them. Fortunately for the cybercriminal, a black market exists where these skills can be purchased in the form of toolkits. Hackers find and exploit and or sell vulnerabilities. Toolkit authors find or buy exploit code and incorporate it into their "products." Cybercriminals in turn buy or steal the latest versions of toolkits which allow them to run massive attacks without the trouble of learning the skills needed to run the whole operation.

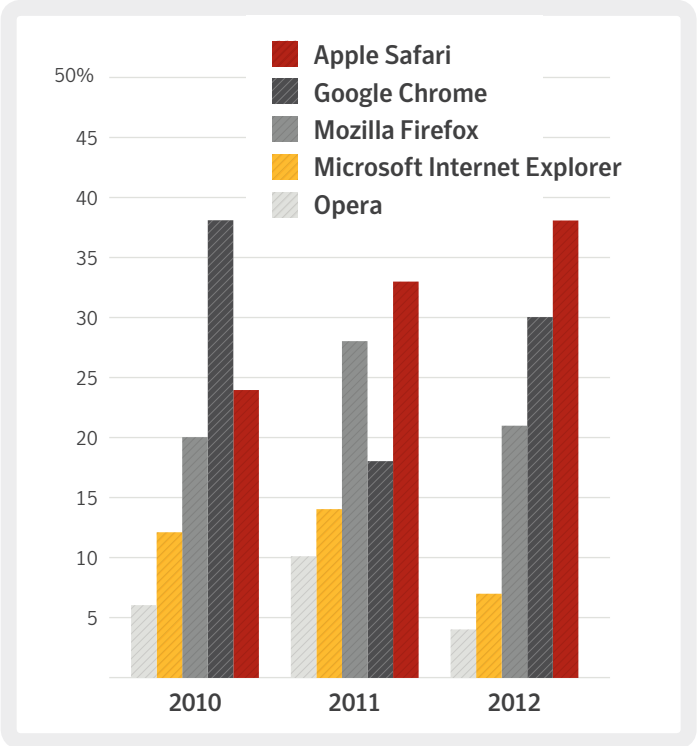
At a Glance

- Usage of zero-day vulnerabilities is up, from 8 to 14 in 2012.
- There is an increasingly sophisticated black market serving a multi-billion dollar online crime industry.
- These vulnerabilities are later commercialized and added to Web-attack toolkits, usually after they become published publicly.
- In 2012, drive-by Web attacks increased by one third, possibly driven by malvertising.
- Around 600,000 Macs were infected with Flashback malware this year.
- The Sakura toolkit, which had little impact in 2011, now accounts for approximately 22 percent of Web-based toolkit attacks, overtaking Blackhole during some points of the year.

Data

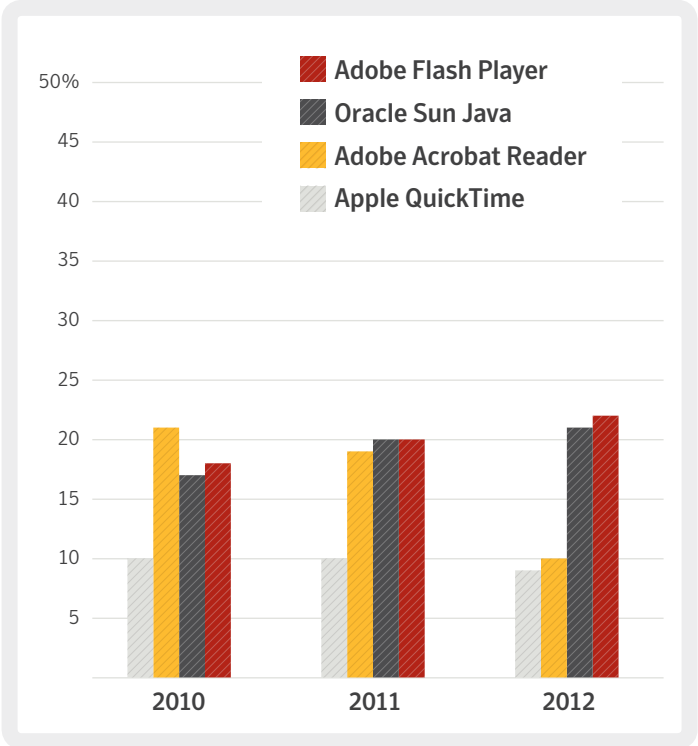
Browser Vulnerabilities 2010 – 2012

Source: Symantec



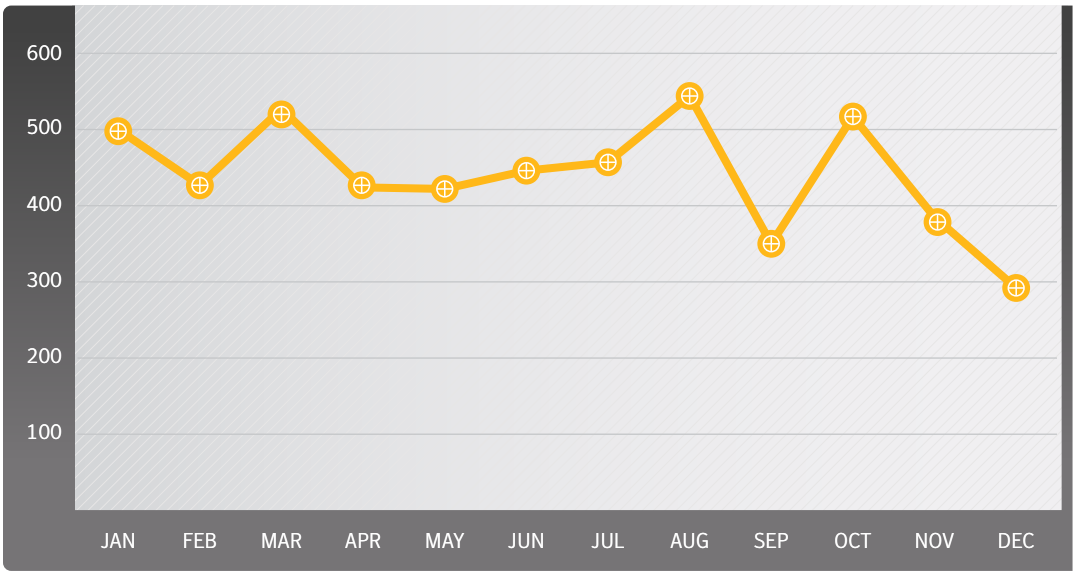
Plug-in Vulnerabilities 2010 – 2012

Source: Symantec



Total Vulnerabilities

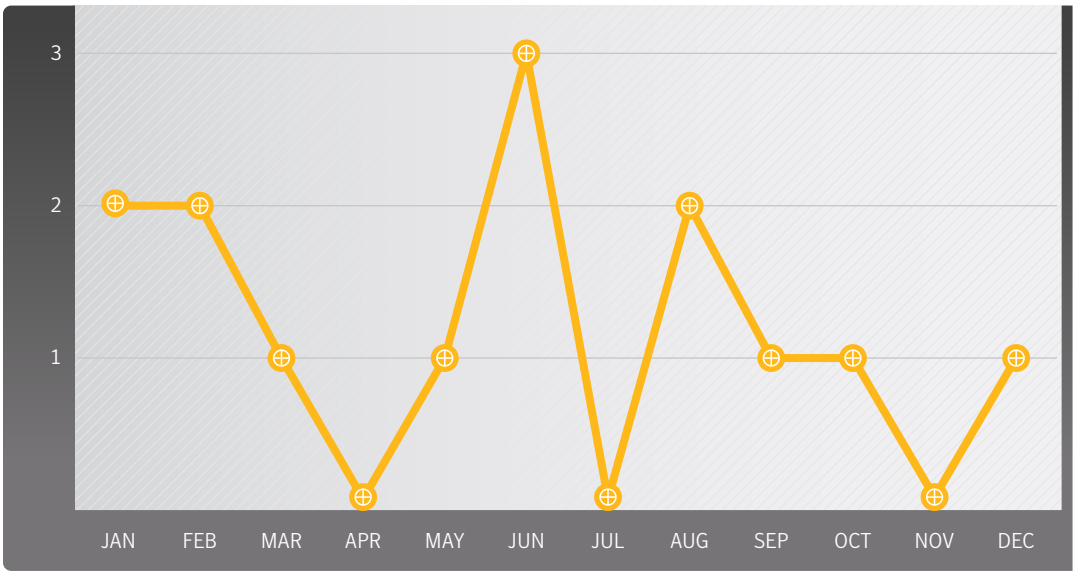
Source: Symantec



- *There were 5,291 vulnerabilities reported in 2012, compared with 4,989 in 2011.*
- *Reported vulnerabilities per month in 2012 fluctuated roughly between 300 and 500 per month.*
- *In 2012, there were 85 public SCADA (Supervisory Control and Data Acquisition) vulnerabilities, a massive decrease over the 129 vulnerabilities in 2011.*
- *There were 415 mobile vulnerabilities identified in 2012, compared with 315 in 2011.*

Zero-day Vulnerabilities

Source: Symantec



- *A zero-day vulnerability is one that is reported to have been exploited in the wild before the vulnerability is public knowledge and prior to a patch being publicly available.*
- *There were 14 zero-day vulnerabilities reported in 2012.*
- *There were up to 3 zero-day vulnerabilities reported each month.*

Analysis

Web-based Attacks on the Rise

We have seen the number of Web-based attacks increase by almost a third. These attacks silently infect enterprise and consumer users when they visit a compromised website. In other words, you can be infected simply by visiting a legitimate website. Typically, attackers infiltrate the website to install their attack toolkits and malware payloads, unbeknown to the site owner or the potential victims.

The malware payload that is dropped by Web-attack toolkits is often server-side polymorphic or dynamically generated, rendering enterprises that rely on signature-based antivirus protection unable to protect themselves against these silent attacks. A hidden piece of JavaScript™ or a few lines of code linking to another website can install malware that is very difficult to detect. It then checks the system of each visitor for browser or operating system vulnerabilities until it finds one that is likely to succeed and it uses that to install malware on the visitor's computer.

These attacks are successful because enterprise and consumer systems are not up to date with the latest patches for browser plug-ins, such as Adobe's Flash Player® and Acrobat Reader®, as well as Oracle's Java™ platform. While a lack of attentiveness can be blamed for consumers remaining out of date, often in larger companies, older versions of these plug-ins are required to run critical business systems, making it harder to upgrade to the latest versions. Such patch management predicaments, with slow patch deployment rates, make companies especially vulnerable to Web-based attacks.

It's important to note that the volume of vulnerabilities doesn't correlate to increased levels of risk. One single vulnerability in an application may present a critical risk to an organization, if exploited successfully. Analysis of risk from vulnerabilities exploited in Web-based attack toolkits is an area that Symantec will explore further in 2013.

The key is that it's not the latest zero-day vulnerability that is responsible for the widespread success of Web-based attacks. The rate of attacks from compromised websites has increased by 30 percent, while the rate of discovery of vulnerabilities has only increased by 6 percent. In a nutshell, it's older, non-patched vulnerabilities that cause most systems to get compromised.

The Arms Race to Exploit New Vulnerabilities

We have witnessed an increase in zero-day vulnerabilities this year. There were 14 unreported vulnerabilities first seen being used in the wild in 2012. This is up from 8 in 2011. Overall, reported vulnerabilities are up slightly in 2012, from 4,989 in 2011 to 5,291 in 2012. Mobile vulnerabilities are also up, from 315 in 2011 to 415 reported in 2012.

Organized groups, such as the team behind the Elderwood attacks, have worked to discover new weaknesses in everyday software such as Web browsers and browser plug-ins. When one vulnerability becomes public, they are able to quickly deploy a new one, which speaks to the sophistication of the groups creating vulnerabilities.

There is an arms race between Internet criminals and legitimate software developers. Criminals' ability to quickly find and exploit new vulnerabilities is not matched by software vendors' ability to fix and release patches. Some software companies only patch once a quarter; others are slow to acknowledge vulnerabilities. Even if they do a good job with updates, companies are often slow to deploy them.

While zero-day vulnerabilities present a serious security threat, known (and even patched) vulnerabilities are dangerous if ignored. Many companies and consumers fail to apply published updates in a timely way. Toolkits that target well-known vulnerabilities make it easy for criminals to target millions of PCs and find the ones that remain open to infection. In fact, the vulnerabilities that are exploited the most often are not the newest.

Malvertising and Website Hacking

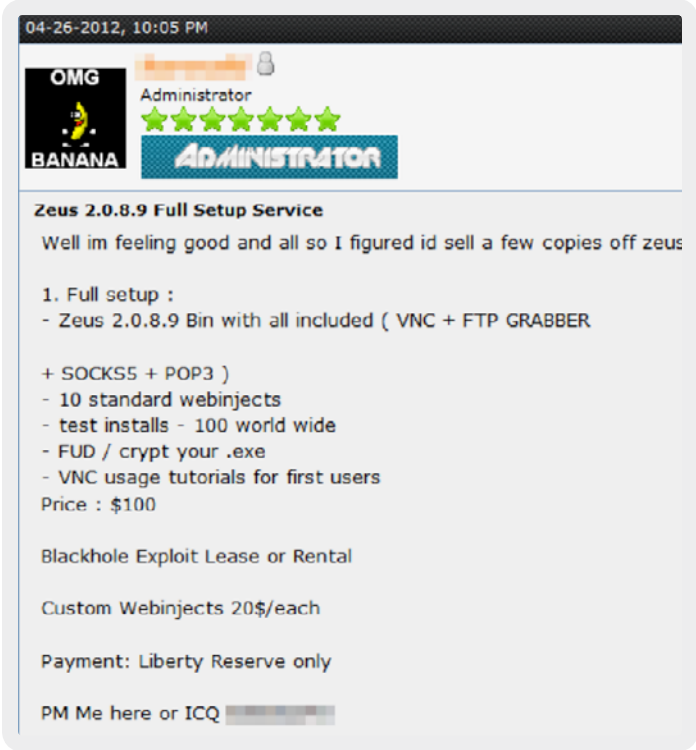
How does a hacker add his code to a legitimate website? Toolkits are available that make it easy. For example, in May 2012, the LizaMoon toolkit used a SQL injection technique to affect at least a million websites.[13] Other approaches include:

- Exploiting a known vulnerability in the website hosting or content management software
- Using phishing, spyware, or social engineering to get the webmaster's password
- Hacking through the Web server backend infrastructure, such as control panels or databases
- Paying to host an advertisement that contains the infection

This last technique, known as malvertising, means that legitimate websites can be impacted without even being compromised. This form of attack appears to be very common. Using experimental scanning software (see "Website Malware Scanning and Website Vulnerability Assessment" later in this section), Symantec found that half of the tested sites were infected by malvertising.

Malvertising opens an avenue of attack that hackers can use to compromise a website without having to directly hack the website itself. Using these malicious ads allows them to silently infect users, often installing dynamically created malware that antivirus alone is unable to detect.

A sign of the seriousness of the problem is that Google and other search engines scan for malware and blacklist sites that contain malware. There have been occasions when prominent advertising networks have fallen prey to malvertising, impacting some of the biggest names in online media.[14] Situations like this can have a serious impact on websites whose bottom line often depends on revenue, even diminishing their credibility in the eyes of their readers. With dozens of advertising networks and constantly rotating adverts, tracking malvertising and preventing it is a huge challenge.



Online advertisement for a malware toolkit.

Web Attack Toolkits

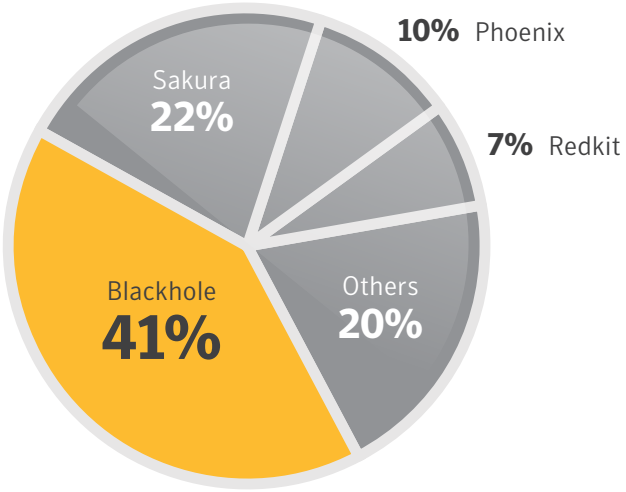
It's one thing to discover new vulnerabilities, but another matter to implement a way to exploit them. Criminal entrepreneurs turn them into toolkits that less sophisticated users can buy and use. Like commercial software, they even include support and warranties. Authors accept payments using online payment services with anonymous numbered accounts.

Attack toolkits exist for creating a variety of malware and for attacking websites. The popular Blackhole toolkit is a notorious example. This updating strategy suggests that it has a kind of brand loyalty and that the authors are building on that in the same way that legitimate software vendors do with their updates and new editions.

Blackhole continued to make its presence felt in 2012, making up for 41 percent of all Web-based attacks. We also saw the release of an updated version of the toolkit, dubbed Blackhole 2.0, back in September. However, Blackhole's overall dominance may have begun to decline, as another Web attack toolkit surpassed Blackhole during a few months in the latter half of 2012. Sakura, a new entrant to the market, at its peak made up as much of 60 percent of all toolkit activity, and 22 percent of overall toolkit usage in 2012.

Top Web Attack Toolkits by Percent

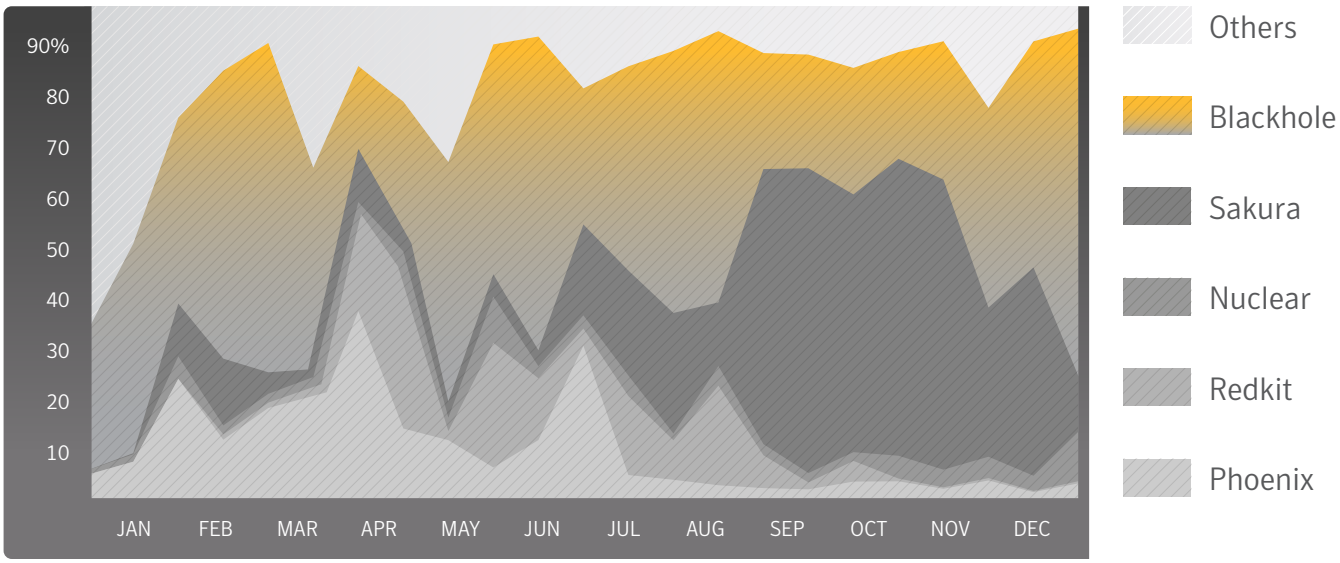
Source: Symantec



Approximately 41 percent of Web-based toolkit attacks in 2012 related to the Blackhole toolkit, compared with 44 percent in 2011. The Sakura toolkit was not in the top 10 for 2011, and now accounts for approximately 22 percent of Web-based toolkit attacks, overtaking Blackhole at some points in the year.

Web Attack Toolkits Over Time

Source: Symantec



Website Malware Scanning and Website Vulnerability Assessment

In 2012, Symantec's Trust Services (formerly VeriSign) technology scanned over 1.5 million websites as part of its Website Malware Scanning and Vulnerability Assessment services. Over 130,000 URLs were scanned for malware each day, with 1 in 532 of websites found to be infected with malware. The most common form of compromise was for the use of drive-by downloads.

Furthermore, in assessing potentially exploitable vulnerabilities on websites, over 1,400 vulnerability scans were performed each day. Approximately 53 percent of websites scanned were found to have unpatched, potentially exploitable vulnerabilities (36 percent in 2011), of which 24 percent were deemed to be critical (25 percent in 2011). The most common vulnerability found was for cross-site scripting vulnerabilities.

The Growth of Secured Connections

One of the ways to judge the growth of usage for SSL is to monitor the change in statistics for OCSP (Online Certificate Status Protocol, which is used for obtaining the revocation status of a digital certificate) and CRL (Certificate Revocation List) lookups. When an SSL secured connection is initiated, a revocation check is performed using OCSP or CRL and we track the number of lookups that go through our systems. This is a growth indicator for the number of SSL secured sessions that are performed online. This implies that more people are going online and using secured connections (for example, representing a growth of eCommerce transactions on the Web). It also may show the impact of the adoption of SSL more widely, in more places and for more uses, such as the growing use of Extended Validation SSL Certificates, which trigger browsers to indicate whether a user is on a secured site by turning the address bar green, and for "Always On SSL" (adopted heavily through 2012 by social networks, search services, and online email providers). Further, it may be a result of devices other than traditional desktops and laptops that enable online access; for example, smartphones and tablets.

In 2012, Symantec identified the average number of OCSP lookups grew by 31 percent year on year between 2011 and 2012, with more than 4.8 billion lookups performed each day in 2012. The high-water-mark of OCSP lookups was 5.8 billion in a single day in 2012. It is worth noting that OCSP is the modern revocation checking methodology.

Additionally, Symantec's CRL lookups increased by 45 percent year on year between 2011 and 2012, with approximately 1.4 billion per day, and a high-water-mark of 2.1 billion. CRL is the older lookup technology that OCSP supersedes.

Norton Secured Seal and Trust Marks

In 2012, more consumers were visiting websites with trust marks (such as the Norton Secured Seal) in 2012. Based on analysis of the statistics from Symantec's own trust marks, we saw an 8 percent increase in 2012. The Symantec trust mark was viewed up to 750 million times a day in 2012 as more online users are necessitating stronger security to safeguard their online activities.

Stolen Key-signing Certificates

2012 continued to show that organizations large and small were susceptible to becoming unwitting players in the global malware distribution network. We've seen increased activity of malware being signed with legitimate code-signing certificates. Since the malware code is signed, it appears to be legitimate, which make it easier to spread.

Malware developers often use stolen code-signing private keys. They attack Certificate Authorities and once inside their networks, they seek out and steal private keys. In other cases, poor security practices allow them to buy legitimate certificates with fake identities. For example, in May 2012, Comodo, a large Certificate Authority, authenticated and issued a legitimate code-signing certificate to a fictitious organization run by cybercriminals.[15]

Recommendations

Use a Full Range of Protection Technology.

If the threat landscape was less advanced, then file scanning technology (commonly called antivirus) would be sufficient to prevent malware infections. However, with toolkits for building malware-on-demand, polymorphic malware and zero-day exploits, antivirus is not enough. Network-based protection and reputation technology must be deployed on endpoints to help prevent attacks. And behavior blocking and scheduled file scanning must be used to help find malware that avoid preventative defense.

Protect Your Public-facing Websites.

Consider Always On SSL to encrypt visitors' interactions with your site across the whole site, not just on the checkout or sign-up pages. Make sure you update your content management system and Web server software just as you would a client PC. Run vulnerability and malware scanning tools on your websites to detect problems promptly. To protect these credentials against social engineering and phishing, use strong passwords for admin accounts and other services. Limit login access to important Web servers to users that need it.

Protect Code-signing Certificates.

Certificate owners should apply rigorous protection and security policies to safeguard keys. This means effective physical security, the use of cryptographic hardware security modules, and effective network and endpoint security, including data loss prevention on servers involved in signing code, and thorough security for applications used to sign code. In addition, Certificate Authorities need to ensure that they are using best practices in every step of the authentication process.

Adopting an Always On SSL approach helps to safeguard account information from unencrypted connections and thus render end users less vulnerable to a man-in-the-middle attack.

Be Aggressive on Your Software Updating and Review Your Patching Processes.

The majority of Web-based attacks exploit the top 20 most common vulnerabilities. Consequently, installing patches for known vulnerabilities will prevent the most common attacks. It's essential to update and patch all your software promptly. In particular, with risks like the Flashback attacks that used Java, it's important to run the latest version of that software or do without it altogether. This is equally true for CIOs managing thousands of users, small business owners with dozens of users, or individual users at home.

Update, patch, and migrate from outdated and insecure browsers, applications, and browser plug-ins to the latest available versions using the vendors' automatic update mechanisms, especially for the top software vulnerabilities being exploited. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Be wary of deploying standard corporate images containing older versions of browsers, applications, and browser plug-ins that are outdated and insecure. Consider removing vulnerable plug-ins from images for employees that have no need for that software. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

SOCIAL NETWORKING MOBILE AND THE CLOUD

Introduction

Online criminals and spammers are less interested in email as an infection vector than they were. Why? Because social media is becoming so popular and it gives them many new ways to steal people's identities or personal information and infect their computers with malware.

Social media combines two behaviors that are useful for criminals: social proof and sharing. Social proofing is the psychological mechanism that convinces people to do things because their friends are doing it. For example, if you get a message on your Facebook wall from a trusted friend, you're more likely to click on it.

Sharing is what people do with social networks: they share personal information such as their birthday, home address, and other contact details. This type of information is very useful for identity thieves. For example, your social media profile might contain clues to security questions a hacker would need to reset your password and take control of your account.

People are spending more time online, and the most popular activity is for social networking. Furthermore, younger users are more commonly using mobile devices to access the Internet and social media applications.[16]

Moreover, many mobile applications frequently rely on cloud-based storage, and without an Internet connection are often limited in their functionality. Many more people and businesses are routinely using cloud-based systems, sometimes without even realising it.

The bank robber Willie Sutton famously explained why he robbed banks: "Because that's where the money is." Online criminals target social media because that's where the victims are.

Facebook users can report potential Facebook phishing scams to the company through the following email address: phish@fb.com.

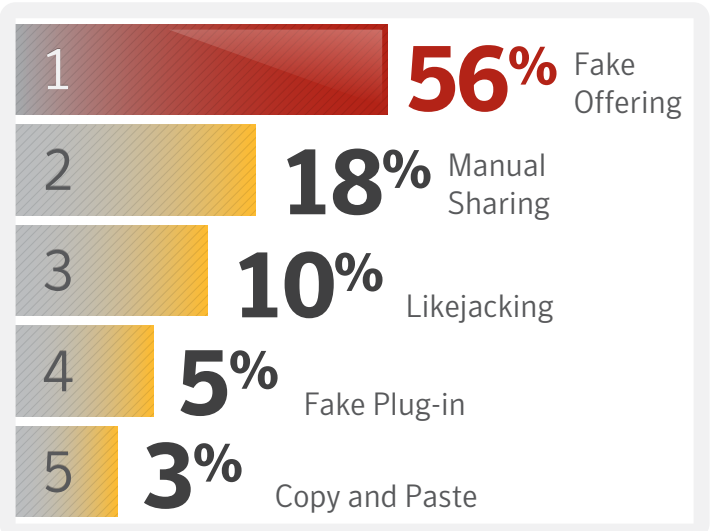
At a Glance

- Scammers continue to use social media as spam and phishing tools, including newer sites such as Pinterest and Instagram.
- Mobile malware has increased significantly in 2012 with new threats such as mobile botnets.
- Thirty-two percent of all mobile malware steals information from the compromised device.
- Fast-growing trends towards cloud computing, bring your own device, and consumerization create additional risks for businesses.

Data

Top 5 Social Media Attacks in 2012

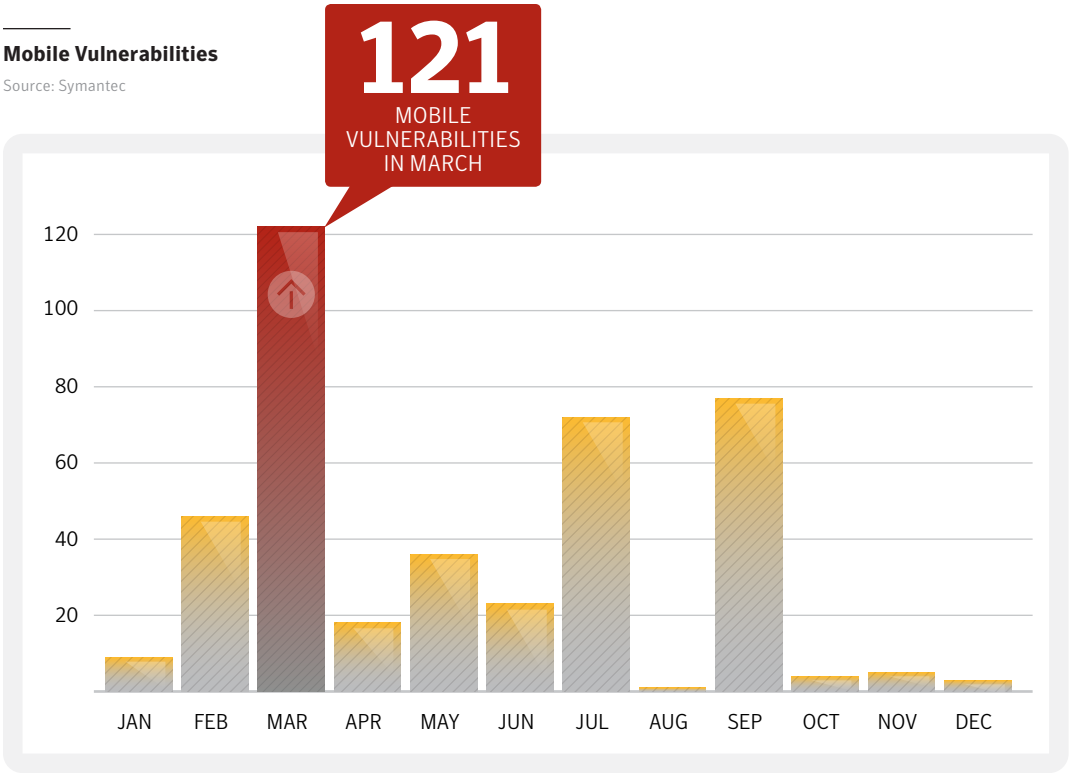
Source: Symantec



- **Fake Offering.** These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.
- **Manual Sharing Scams.** These rely on victims to actually do the hard work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends.
- **Likejacking.** Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.
- **Fake Plug-in Scams.** Users are tricked into downloading fake browser extensions on their machines. Rogue browser extensions can pose like legitimate extensions but when installed can steal sensitive information from the infected machine.
- **Copy and Paste Scams.** Users are invited to paste malicious JavaScript code directly into their browser's address bar in the hope of receiving a gift coupon in return.

Mobile Vulnerabilities

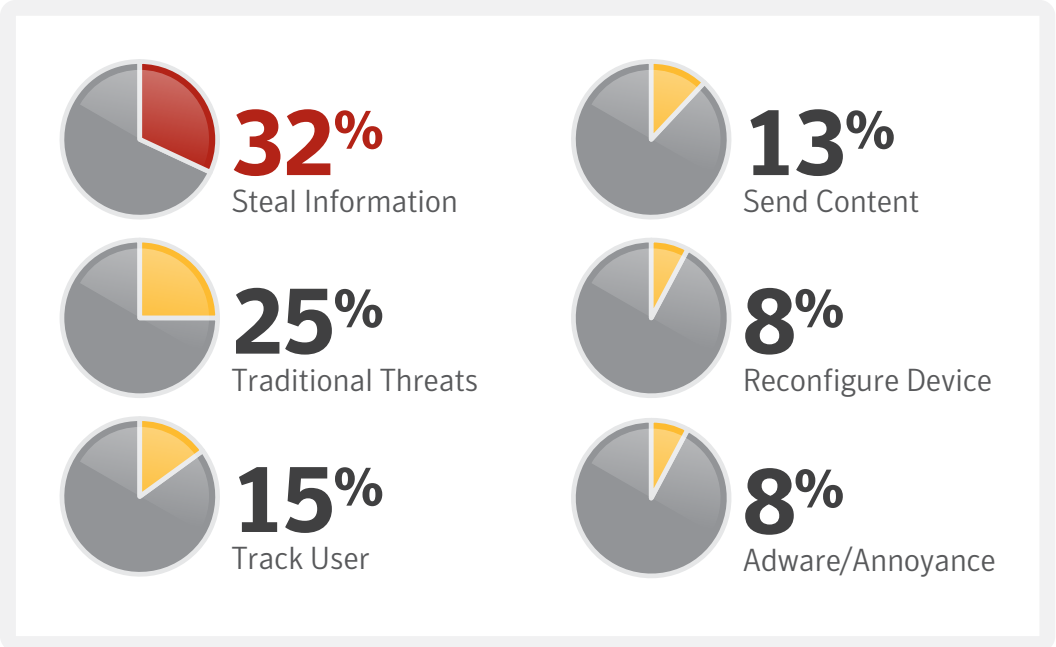
Source: Symantec



- *March was the most active month of 2012, with 121 vulnerabilities reported.*
- *There were 415 mobile vulnerabilities identified in 2012, compared with 315 in 2011.*

Mobile Threats in 2012

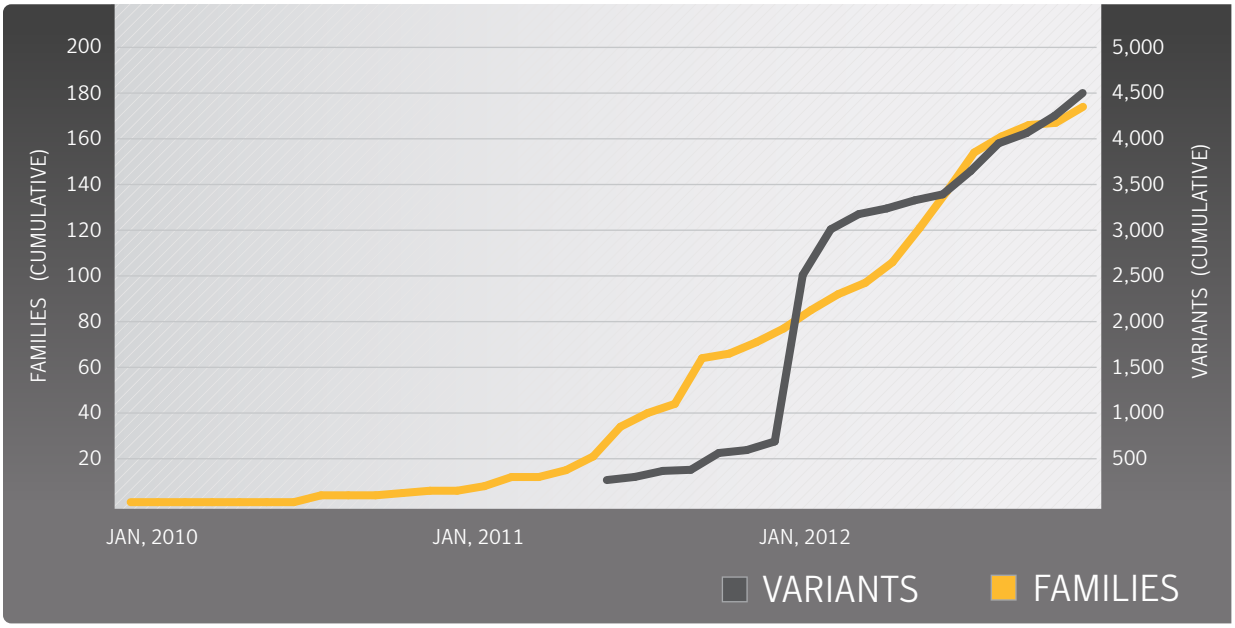
Source: Symantec



Information stealing tops the list of activities carried out by mobile malware, with 32 percent of all threats recording some sort of information in 2012.

Cumulative Mobile Android Malware, Families and Variants 2010 to 2012

Source: Symantec



- *2012 saw a 58 percent increase in mobile malware families compared to 2011. The year's total now accounts for 59 percent of all malware to-date.*
- *At the same time the number of variants within each family has increased dramatically, from an average ratio of variants per family of 5:1 in 2011 to 38:1 in 2012. This indicates that threat authors are spending more time repackaging or making minor changes to their threats, in order to spread them further and avoid detection.*

Mobile Threats by Device Type in 2012

Source: Symantec

Device Type	Number of Threats
Android malware	103
Symbian malware	3
Windows Mobile malware	1
iOS malware	1

In contrast to vulnerabilities, Android was by far the most commonly targeted mobile platform in 2012, comprising 103 out of 108 unique threats.

Mobile Vulnerabilities by OS

Source: Symantec

Platform	Documented Vulnerabilities
Apple iOS	387
Android	13
BlackBerry	13
Nokia	0
LG Electronics	0
Windows Mobile	2

The vast majority of vulnerabilities on mobile systems were on the iOS platform. However, the higher number of vulnerabilities is not indicative of a higher level of threat, because most mobile threats have not used software vulnerabilities.

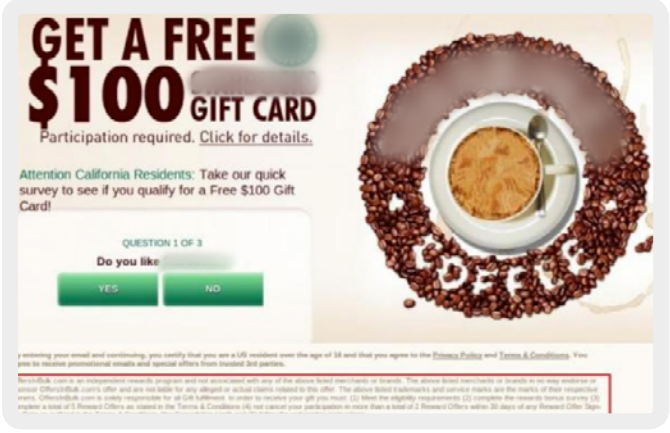
Analysis

Spam and Phishing Move to Social Media

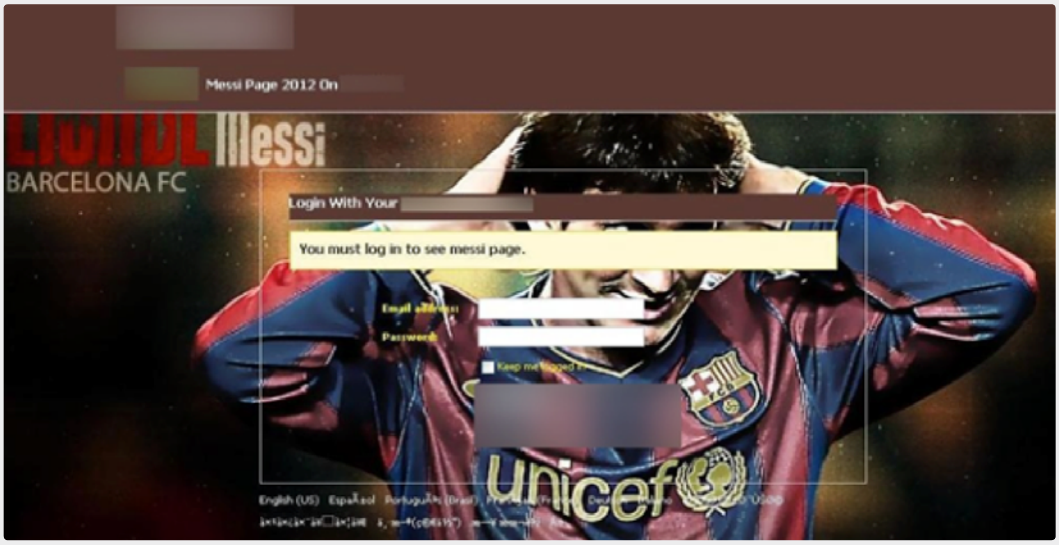
In the last few years, we've seen a significant increase in spam and phishing on social media sites. Criminals follow users to popular sites. As Facebook and Twitter have grown in popularity for users, they have also attracted more criminal activity. However, in the last year, online criminals have also started targeting newer, fast-growing sites such as Instagram, Pinterest, and Tumblr.

Typical threats include fake gift cards and survey scams. These kinds of fake offer scams account for more than half (56 percent) of all social media attacks. For example, in one scam the victim sees a post on somebody's Facebook wall or on their Pinterest feeds (where content appears from the people they follow or in specific categories) that says "Click here for a $100 gift card." When the user clicks on the link, they go to a website where they are asked to sign up for any number of offers, turning over personal details in the process. The spammers get a fee for each registration and, of course, there's no gift card at the end of the process.

Typical social media scam.



Fake website with bogus survey.



Phishing site spoofing a social networking site promoting soccer star Lionel Messi.

We also documented a similar spam campaign on the popular photo-sharing app Instagram.[17]

Another trick is to use a fake website to persuade a victim to reveal their personal details and passwords; for example, their Facebook or Twitter account information. These phishing scams are insidious and often exploit people's fascination with celebrities such as professional athletes, film stars, or singers. We have seen an increase in phishing scams that target specific countries and their celebrities.

In 2012, we have seen ever more threats targeted on social media websites as well as more and more new channels and platforms opening up, especially those that are available only as mobile applications. It is likely that these mobile social channels will become more targeted in 2013, especially those that are aimed specifically at teenagers and young adults, who may not know how to recognize such attacks and may be a little freer with their personal details.

Mobile Threats

In the last year, we have seen a further increase in mobile malware. This correlates with increasing numbers of Internet-connected mobile devices. Android has a 72 percent market share with Apple® iOS a distant second with 14 percent, according to Gartner.[18] As a result of its market share and more open development environment, Android is the main target for mobile threats.

Typically, people use phones to store personal information and contact information and increasingly they have high-speed Internet connections. The smartphone has become a powerful computer in its own right, and this makes these attractive devices to criminals. They also have the added advantage of being tied to a payment system—the owner's phone contract—which means that they offer additional ways for criminals to siphon off money from the victim.

We've seen a big rise in all kinds of mobile phone attacks:

- **Android threats** were more commonly found in Eastern Europe and Asia; however, during the last year, the number of Android threats in the rest of Europe and the United States has increased.
- **Privacy leaks** that disclose personal information, including the release of surveillance software designed to covertly transmit the owner's location.[19]
- **Premium number fraud** where malicious apps send expensive text messages. This is the quickest way to make money from mobile malware. One mobile botnet Symantec observed used fake mobile apps to infect users and by our calculation the botmaster is generating anywhere between $1,600 to $9,000 per day and $547,500 to $3,285,000 per year.[20]
- **Mobile botnets.** Just as spammers have linked networks of PCs into botnets to send out unwanted email, now criminals have begun using Android botnets the same way.[21] This suggests that attackers are adapting techniques used on PCs to work on smartphones.

Historically, malware infected smartphones through rogue app markets and users sideloading apps directly onto their devices. However, legitimate app stores are not immune. In 2012, we saw rogue software masquerading as popular games on the Google® Play market, having bypassed Google's automated screening process.[22]

Businesses are increasingly allowing staff to "bring your own device" (BYOD) to work, either by allowing them to use personal computers, tablets, or smartphones for work, even subsidizing their purchase. Even when companies provide their own equipment, the trend towards consumerization means that companies often turn to consumer technology, such as file-sharing websites, and devices, such as consumer laptops or tablets, to reduce costs. These two trends open the door to a greater risk to businesses from mobile devices because they often lack security features such as encryption, access control, and manageability.

We have seen far more vulnerabilities for the iOS platform, which makes up 93 percent of those published, than for Android in 2012, but yet Android dominates the malware landscape, with 97 percent of new threats.

While seemingly contradictory at first, there is a good reason for this: jailbreaking iOS devices. In order to install applications that are not available on the Apple App Store, a user must run an exploit against a vulnerability in the software. While not the safest approach from a security standpoint, this is the only way to install applications that are not available through the Apple App Store.

In contrast, the Android platform provides the option to install apps from unofficial markets by simply changing settings in the operating system. Since no exploit is needed, the same incentives aren't present as there are on iOS. Android users are vulnerable to a whole host of threats; however, very few have utilized vulnerabilities to spread threats.

While Android clocks in with 103 threats in 2012, this number may appear small compared to other estimates on the scope of the mobile threat landscape. Many estimates are larger because they provide a count of overall variants, as opposed to new, unique threats. While many of these variants simply undergone minor changes in an attempt to avoid antivirus scanners detecting them, Symantec counted at least 3,906 different mobile variants for the year.

There's an important distinction between old and new Android versions regarding security features. Google added a feature in Android version 4.x to allow users to block any particular app from pushing notifications into the status bar. This came in response to feedback from users of older versions, annoyed by ad platforms that push notifications to the status bar.

Also, due to the rise of threats that silently send premium text messages—Android.Opfake, Android.Premiumtext, Android.Positmob, and Android.Rufraud, for instance—Google added a feature in Android 4.2 to prompt the user to confirm sending such premium text messages. This can be very helpful in protecting most users.

However, at around 10 percent market penetration at the end of 2012,[23] Android 4.2 devices account only for a small percentage

of the total devices out there. The Android ecosystem makes it harder to keep everyone up to date. Google released the official platform that works out of the box only on Nexus devices—Google's own branded device. From there each manufacturer modifies and releases its own platform, which is in turn picked up by mobile network operators who also customize those platforms.

This makes it impossible for any change coming from Google to be quickly available to all in-field devices. Any change to the platform requires thorough testing by each manufacturer and then each operator, all adding to the time needed to reach users. Having so many device models also multiplies the amount of resources all these companies have to allocate for each update, leading to infrequently released updates or in some cases no updates for older devices.

For most exploits in the OS, Google released quick fixes; however, users still had long waits before they received the fix from their network operators. Some exploits are not in the original OS itself but in the custom modifications made by manufacturers, such as the exploit for Samsung models that appeared in 2012. Samsung was quick to fix it, but the fix still had to propagate through network operators to reach users.

Tighter control from Google over the platform can solve some of the "fragmentation" issues, but this could affect the relationship it has with manufacturers. A cut-off point for older Android users could help to mitigate the risk, but it is usually the manufacturers that do this.

Cloud Computing Risks

The cloud services market was expected to grow by 20 percent in 2012, according to Gartner.[24] Cloud computing promises businesses a way to enhance their IT without heavy upfront capital costs and, for smaller businesses, it offers access to enterprise-class business software at an affordable price. On a fundamental level, it offers huge and growing economies of scale as Internet bandwidth and processing power continue to increase rapidly.

Cloud computing offers some potential security benefits, especially for smaller companies without dedicated IT security staff. Well-run cloud applications are more likely to be patched and updated efficiently. They are also more likely to be resilient, secure, and backed up than on-premises systems.

However, cloud computing presents some security concerns, too:

- **Privacy.** Well-run cloud companies will have strong policies about who can access customer data (for example, for troubleshooting) and under what circumstances. Information should only be entrusted to a third party over the Internet where there is sufficient assurance as to how that data will be managed and accessed.
- **Data Liberation.** Cloud computing businesses make it easy to get started, and reputable companies make it easy to extract your data (for example, archived emails or customer records) if you want to change providers. Before entrusting their data to a cloud provider, potential users should fully evaluate the terms and conditions of extracting and recovering that data at a later date.
- **Eggs in One Basket.** As we have seen from large-scale data breaches in the last few years, attackers tend to go where they can score the most data for the least effort. If a cloud services provider stores confidential information for a large number of customers, it becomes a bigger target for attackers. A single breach at a cloud provider could be a gold mine of personal data for an attacker.
- **Consumerization.** Companies face a significant risk of accidental or deliberate data loss when their employees use unapproved cloud systems on an ad-hoc basis. For example, if company policies make it difficult to email large files to third parties, employees may decide to use free online file sharing applications instead. The risk is that these systems may fall short of company standards for security. For example, one popular file-sharing site left all its user accounts unlocked for four hours.[25] In addition, where employees use unauthorized cloud applications for their work, such as social networking sites for marketing purposes, they open up the company to attack from Web-based malware.
- **Infrastructure.** Although not in the wild, there is a theoretical risk that in a virtualized, multi-tenant architecture, a malicious user could rent a virtual machine and use it to launch an attack against the system by exploiting a vulnerability in the underlying hypervisor and use this to gain access to other virtual machines running in the same environment. Consideration should also be given to data encryption within the virtual machine to minimize the risk from unauthorized access to the physical hard disks.

Recommendations

Social Media Threats Are a Business Issue.

Companies are often unwilling to block access to social media sites altogether, but they need to find ways to protect themselves against Web-based malware on these and other sites. This means multi-layer security software at the gateway and on client PCs. It also requires aggressive patching and updating to reduce the risk of drive-by infections. Lastly, user education and clear policies are essential, especially regarding the amount of personal information users disclose online.

Cloud Security Advice.[26]

Carry out a full risk assessment before signing up. Secure your own information and identities. Implement a strong governance framework.

Protect Your Mobile Devices.

Consider installing security software on mobile devices. Also, users need to be educated about the risks of downloading rogue applications and how to use their privacy and permission settings. For company-provided devices, consider locking them down and preventing the installation of unapproved applications altogether.

MALWARE, SPAM AND PHISHING

Introduction

Malware, spam, and social engineering continue to be massive, chronic problems. Although they have been around for a long time, attacks continue to evolve and they still have the potential to do serious damage to consumers and businesses.

In addition, they hurt everyone by undermining confidence in the Internet. These chronic threats do not get much news coverage because they are "background noise" but that doesn't mean that they are unimportant. A useful comparison is the difference between plane crashes and car crashes. A single plane crash makes the national news, but the daily death toll on the roads goes unreported despite killing significantly more people each year.[27]

The popularity of ransomware is an example of all these themes. It permanently locks people out of their computer unless they pay a swinging "fine" to the perpetrators. It's corrosive to trust, expensive to remedy, and reveals a new level of ruthlessness and sophistication.

The numbers are telling. In one example, malware called Reveton (aka Trojan.Ransomlock.G), was detected attempting to infect 500,000 computers over a period of 18 days. According to a recent Symantec survey of 13,000 adults in 24 countries, average losses per cybercrime incident are $197.[28] In the last 12 months an estimated 556 million adults worldwide experienced some form of cybercrime.

At a Glance

- With ransomware, malware has become more vicious and more profitable.
- Email spam volumes fall again, down 29 percent in 2012, as spammers move to social media.
- Phishing becomes more sophisticated and targets social networking sites.

Irreversible ransomware locks people out of their computer unless they pay a "fine," which in most cases does not unlock the computer.

Data

Spam

Spam rates declined for a second year in a row, dropping from 75 percent in 2011 to 69 percent of all email in 2012. In 2011 we were reluctant to call this decrease in spam a permanent trend. Botnets can be rebuilt, new ones created. But several factors appear to be keeping spam rates lower than in previous years.

The takedowns of spam botnets continued in 2012. In March 2012 a resurrected Kelihos botnet was taken down for a second time. In July the Grum botnet was taken down. While both were significant spam botnets and contributed to the reduction in spam, undoubtedly email spammers are still feeling the pain of botnet takedowns from 2011.

Additionally, pharmaceutical spam continues to decline, apparently unable to recover from the loss of the major players in the online pharmaceutical business.[29] Given advancements in anti-spam technology, plus the migration of many users to social networks as a means of communication, spammers may be diversifying in order to stay in business.

This is not to say that the problem of spam has been solved. At 69 percent of all email, it still represents a significant amount of unwanted messages.

As email spam rates continue to decline, we see the same social engineering techniques that have been used in email spam campaigns increasingly being adopted in spam campaigns and being promoted through social networking channels.

Top 5 Activity for Spam Destination by Geography

Country	%
Saudi Arabia	79%
Bulgaria	76%
Chile	74%
Hungary	74%
China	73%

Top 5 Activity for Spam Destination by Industry

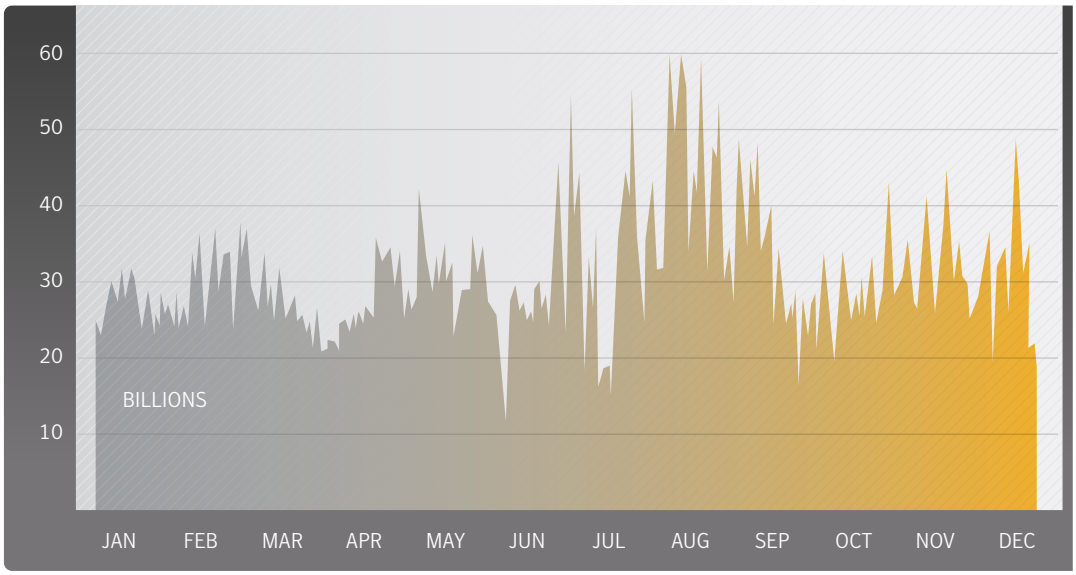
Industry	%
Marketing/Media	69%
Manufacturing	69%
Recreation	69%
Agriculture	69%
Chemical/Pharmaceutical	69%

Top 5 Activity for Spam Destination by Company Size

Organization Size	%
1-250	68%
251-500	68%
501-1,000	68%
1,001-1,500	69%
1,501-2,500	69%
2,501+	68%

Global Spam Volume Per Day in 2012

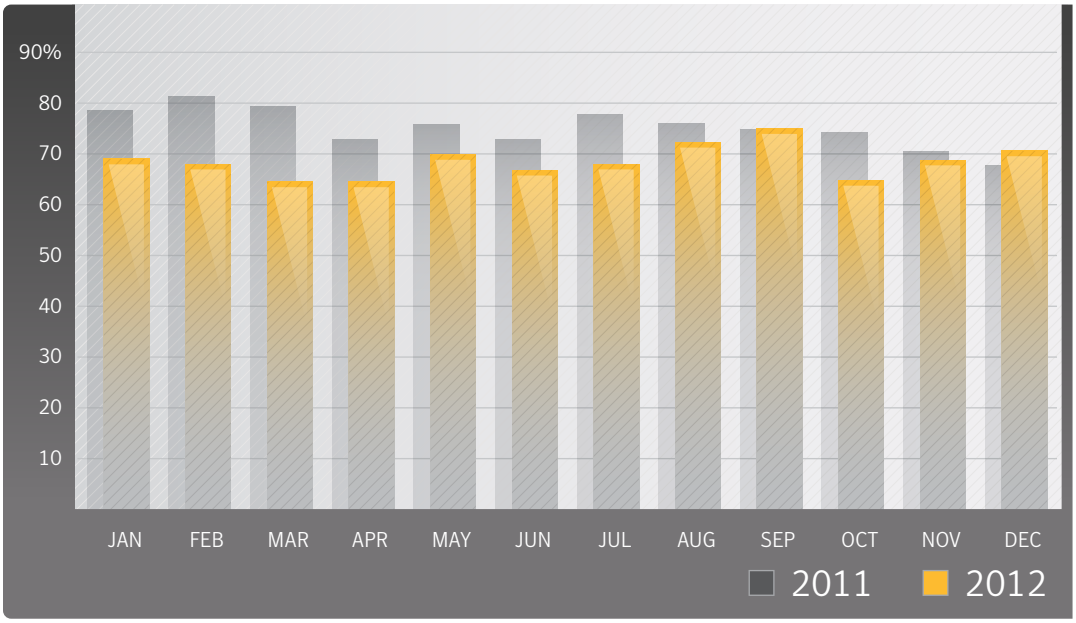
Source: Symantec



- *Spam volumes were highest in August.*
- *The estimated projection of global spam volumes decreased by 29 percent, from 42 billion spam emails per day in 2011, to 30 billion in 2012.*

Global Spam Rate – 2012 vs 2011

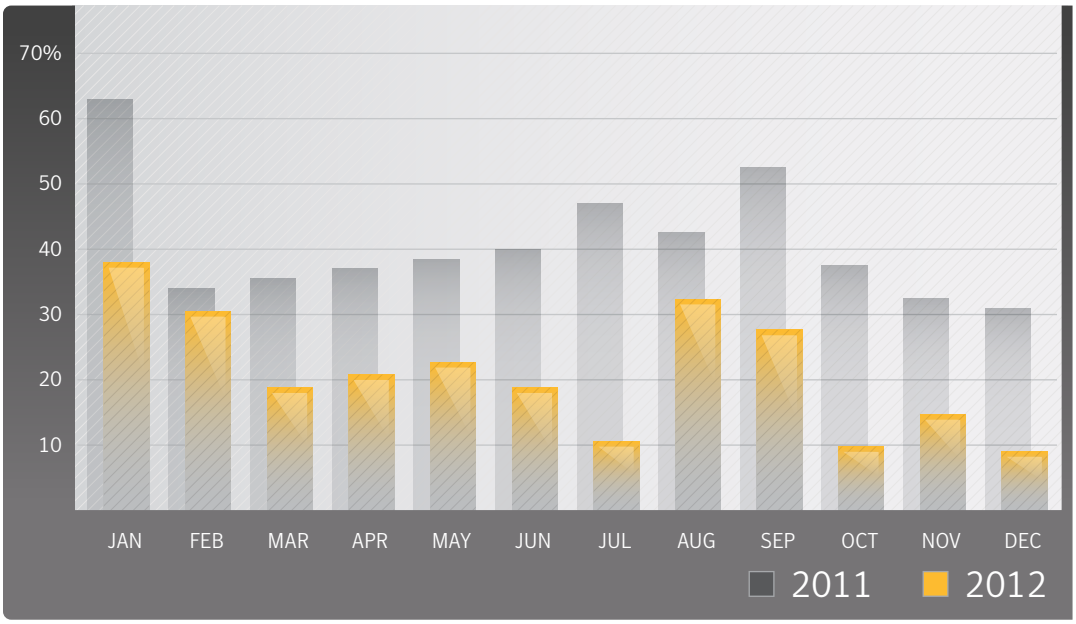
Source: Symantec



The overall average global spam rate for 2012 was 69 percent, compared with 75 percent in 2011.

Pharmaceutical Spam – 2012 vs 2011

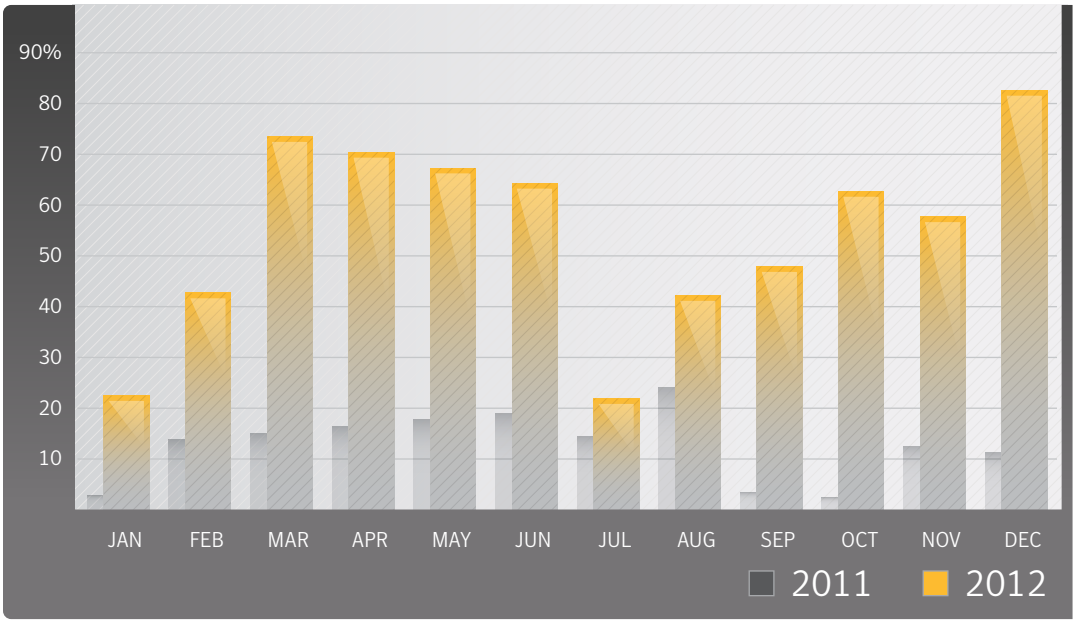
Source: Symantec



- *Pharmaceutical spam makes up 21 percent of all spam, but was overtaken by the Adult/Sex/Dating category, which now makes up 55 percent of spam.*
- *Pharmaceutical spam in 2012 declined by approximately 19 percentage points compared with 2011.*

Adult/Sex/Dating Spam – 2012 vs 2011

Source: Symantec



- *Adult/Dating spam in 2012 increased by approximately 40 percentage points compared with 2011.*
- *This suggests an almost direct correlation between the decline in pharmaceutical spam and the increase in dating spam.*
- *The proportion of adult/sex/dating spam was greater in 2012 than for pharmaceutical spam in 2011, but the actual volume of adult/sex/dating spam in 2012 was lower than for pharmaceutical spam in 2011, since overall spam volumes were lower in 2012 than in the previous year.*

Phishing

Email phishing rates are also down this year, from one in 299 emails in 2011 to one in 414 in 2012.

The decline in the use of email as a method to spread spam and carry out phishing attacks does not likely indicate a drop in activity by attackers. Rather, it appears that we are seeing a shift in activity from email to other forms of online communication, such as social networks.

Top 5 Activity for Phishing Destination by Industry

Industry	1 in
Public Sector	1 in 95
Finance	1 in 211
Education	1 in 223
Accommodation/Catering	1 in 297
Marketing/Media	1 in 355

Top 5 Activity for Phishing Destination by Geography

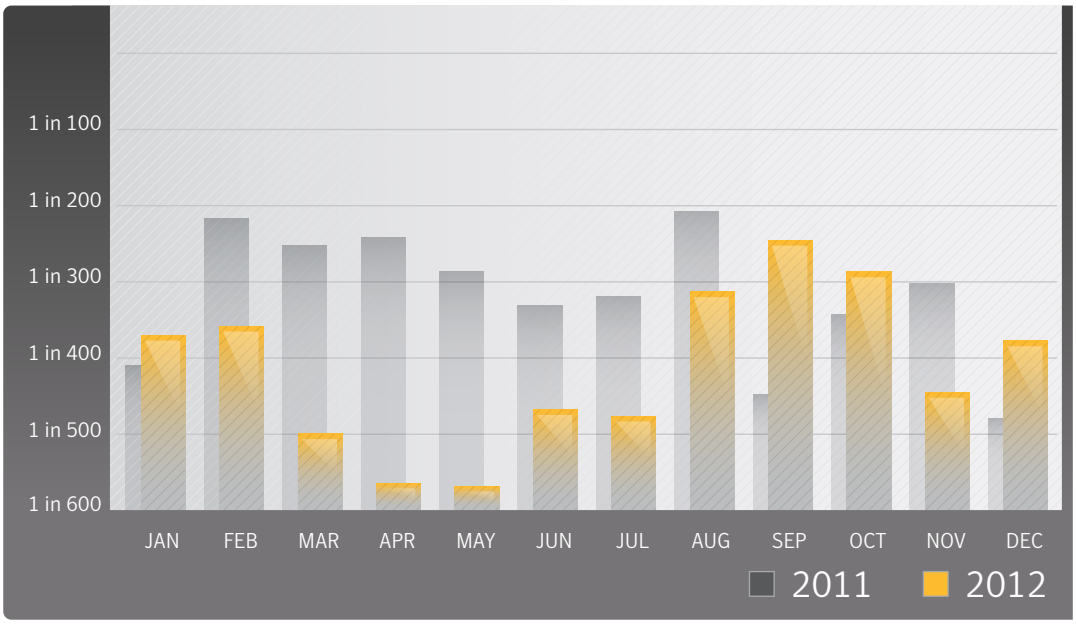
Country	1 in
Netherlands	1 in 123
South Africa	1 in 177
United Kingdom	1 in 191
Denmark	1 in 374
China	1 in 382

Top 5 Activity for Phishing Destination by Company Size

Company Size	1 in
1-250	1 in 294
251-500	1 in 501
501-1,000	1 in 671
1,001-1,500	1 in 607
1,501-2,500	1 in 739
2,501+	1 in 346

Phishing Rate – 2012 vs 2011

Source: Symantec



- *Phishing rates have dropped drastically in 2012, in many cases less than half the number for that month in the previous year.*
- *The overall average phishing rate for 2012 was 1 in 414 emails, compared with 1 in 299 in 2011.*

Malware

One in 291 emails contained a virus in 2012, which is down from one in 239 in 2011. Of that email-borne malware, 23 percent of it contained URLs that pointed to malicious websites. This is also down from 2011, where 39 percent of email-borne malware contained a link to a malicious website.

Much like the drop in spam and phishing rates, a drop in emails that contain viruses does not necessarily mean that attackers have stopped targeting users. Rather, it more likely points to a shift in tactics, targeting other online activities, such as social networking.

Top 5 Activity for Malware Destination by Geography

Country	1 in
Netherlands	1 in 108
Luxembourg	1 in 144
United Kingdom	1 in 163
South Africa	1 in 178
Germany	1 in 196

Top 5 Activity for Malware Destination by Industry

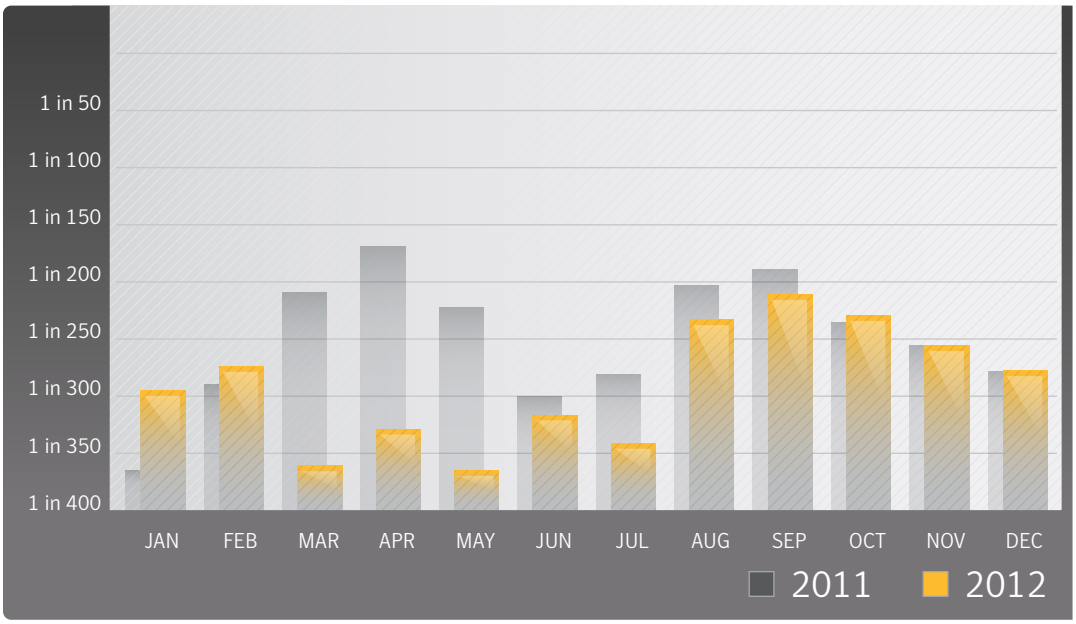
Industry	1 in
Public Sector	1 in 72
Education	1 in 163
Finance	1 in 218
Marketing/Media	1 in 235
Accommodation/Catering	1 in 236

Top 5 Activity for Malware Destination by Company Size

Company Size	1 in
1-250	1 in 299
251-500	1 in 325
501-1,000	1 in 314
1,001-1,500	1 in 295
1,501-2,500	1 in 42
2,501+	1 in 252

Proportion of Email Traffic in Which Virus Was Detected – 2012 vs 2011

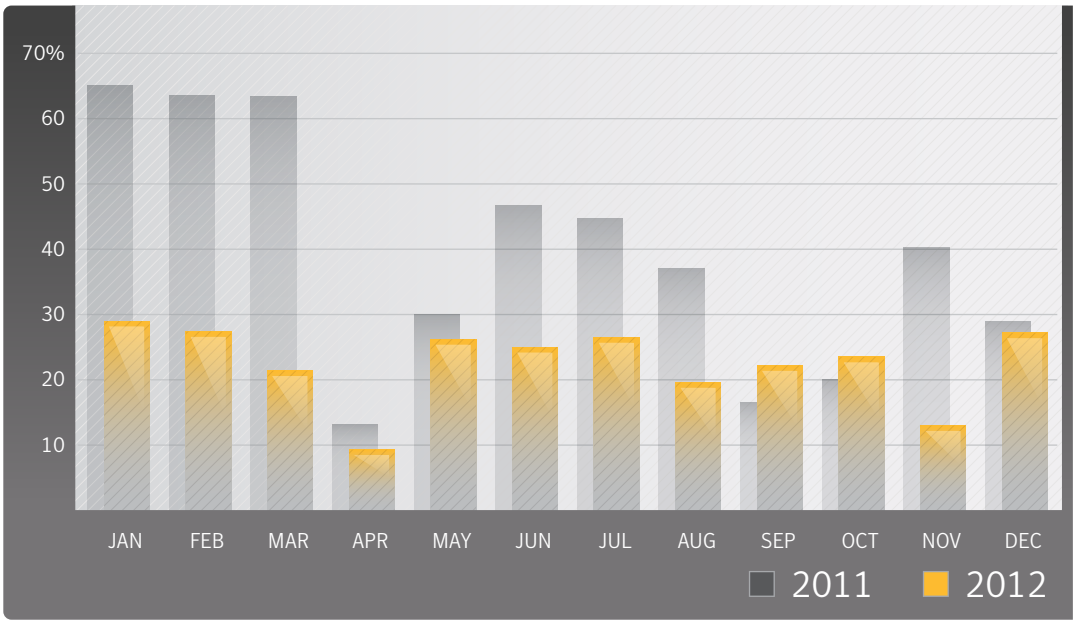
Source: Symantec



- *Overall numbers declined, with one in 291 emails containing a virus.*
- *In 2011, the average rate for email-borne malware was 1 in 239*

Proportion of Email Traffic Containing URL Malware – 2012 vs 2011

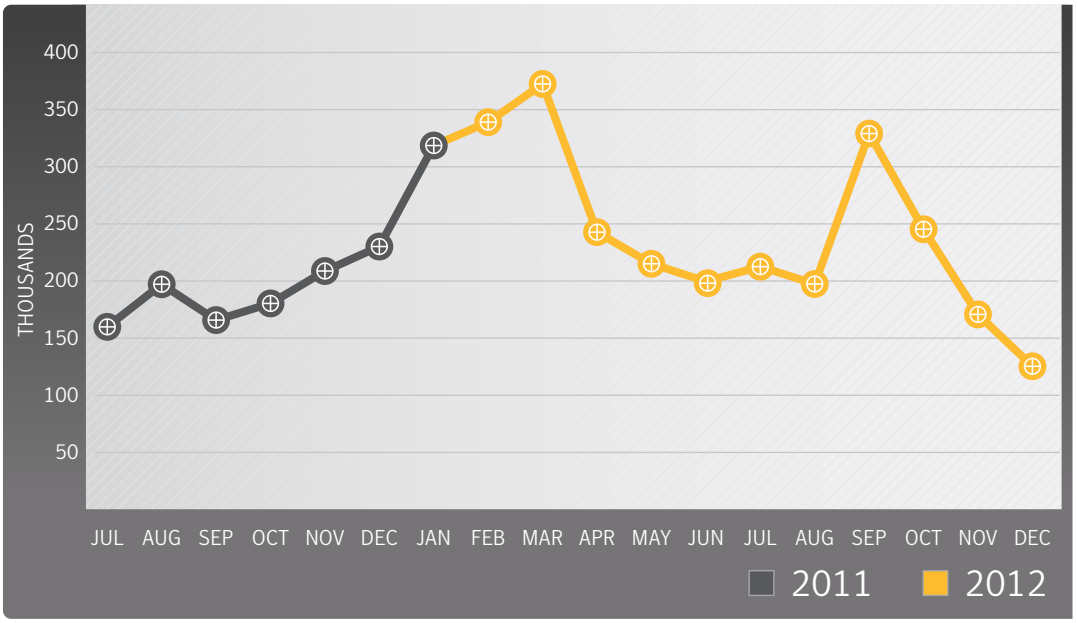
Source: Symantec



- *Emails that contained a malicious URL dropped significantly in 2012. In some months it was more than half the rate as it was that month in 2011.*
- *In 2012, approximately 23 percent of email malware contained a URL rather than an attachment, compared with 39 percent in 2011.*

Website Malware Blocked Per Day

Source: Symantec



- *In 2012, approximately 247,350 Web-based attacks were blocked each day.*
- *In 2011, this figure was approximately 190,370 per day. This represents an increase of 30 percent.*

Website Exploits by Type of Website

Based on Norton Safe Web data, the Symantec technology that scans the Web looking for websites hosting malware, we've determined that 61 percent of malicious sites are actually regular websites that have been compromised and infected with malicious code.

We see Business, which covers consumer and industrial goods and service sectors, listed at the forefront this year. This could be due to the contribution of compromised sites from many SMBs that do not invest in appropriate resources to protect them. Hacking, which includes sites that promote or provide the means to carry out hacking activities, jumped to second, though it didn't appear in the top 15 in 2011.

Although the Technology and Telecommunication category, which provides information pertaining to computers, the Internet and telecommunication, ranks third this year, it sees 5.7 percent of the total compromised sites, only a 1.2 percent drop from 2011. Shopping sites that provide the means to purchase products or services online remain in the top five, but Shopping sees a drop of 4.1 percent.

It is interesting to note that Hosting, which ranked second in 2011, has moved down to seventh this year. This covers services that provide individuals or organizations access to online systems for websites or storage. Due to this increase in reliable and free cloud-based hosting solutions, provided by the likes of Google, Dropbox and others, we see usage moving away from unreliable hosting solutions, which could have contributed towards the drop. Blogging has also experienced a significant drop in 2012, moving down to fourth position. This could support the theory that people are moving towards social networking and exchanging information through such networks. Malware developers find it easy to insert malicious code in such sites and spread them using various means.

Website Exploits by Type of Website

Source: Symantec

Rank	Top Domain Categories that Got Exploited by # of Sites	# of Infected Sites/Total # of Infected Sites
1	Business	7.7%
2	Hacking	7.6%
3	Technology and Telecommunication	5.7%
4	Blogging	4.5%
5	Shopping	3.6%
6	Known Malware Domain	2.6%
7	Hosting	2.3%
8	Automotive	1.9%
9	Health	1.7%
10	Educational	1.7%

Top 10 Malware in 2012

Source: Symantec

Rank	Malware Name	%
1	W32.Sality.AE	6.9%
2	W32.Ramnit.B	5.1%
3	W32.Downadup.B	4.4%
4	W32.Virut.CF	2.2%
5	W32.SillyFDC	1.1%
6	W32.Mabezat.B	1.1%
7	W32.Xpaj.B	0.6%
8	W32.Changeup	0.6%
9	W32.Downadup	0.5%
10	W32.Imaut	0.4%

Analysis

Macs Under Attack

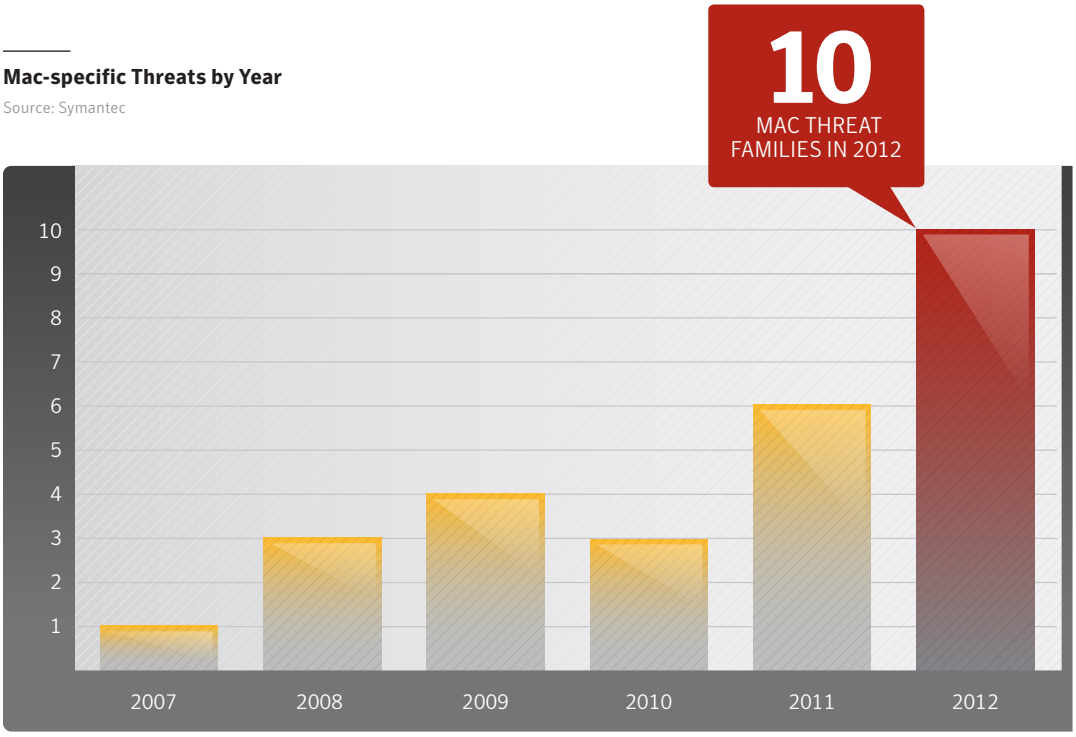
Historically, Mac users have felt less vulnerable to malware than PC users. As Apple has gained market share, Macs have become a more attractive target. In fact, 2012 saw the first significant Mac malware outbreak. The Flashback attack exploited a vulnerability in Java to create a cross-platform threat.[30] It was incorporated into the Blackhole attack toolkit and used by criminals to infect 600,000 Macs,[31] which is approximately one Mac in 100. Like more and more attacks in 2012, as discussed in the "Web Attack Toolkits" section, it spread when users visited infected websites. Although the Flashback malware was mainly used for advertising click fraud, it had other capabilities, such as giving hackers remote access to infected computers.[32] Because most Mac users do not have antivirus software, the chances of detection, once infected, were small.

Does this indicate that hackers are going to start paying further attention to Macintosh computers as a platform to target? Not necessarily. While Mac users may encounter an occasional threat here or there, the vast majority of what they encounter is malware aimed at Windows computers. In fact, of all the threats encountered by Symantec customers who used Mac computers in the last quarter of 2012, only 2.5 percent of them were actually written specifically for Macs.

This isn't to say that Macs are a safer alternative to PCs; as we've seen, they're just as susceptible to attacks. There were more threats created specifically for the Mac in 2012 than in years past and the trend appears to be rising.

Mac-specific Threats by Year

Source: Symantec



There were more unique threats for OS X in 2012 than any year previously.

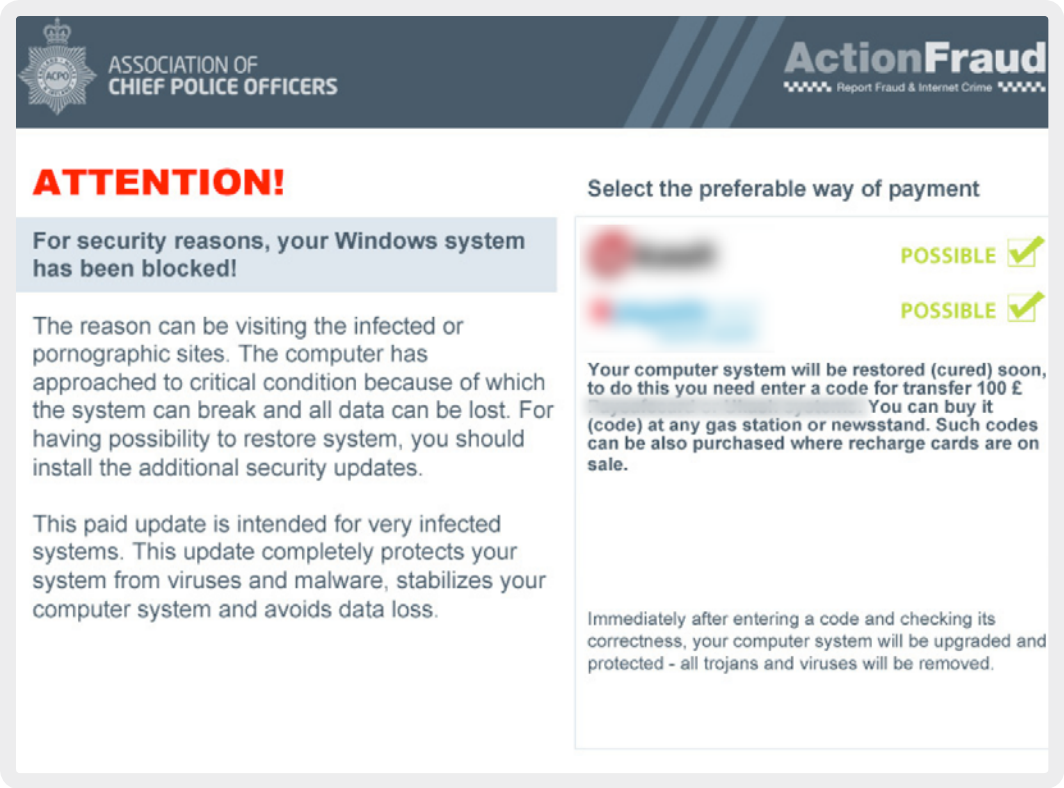
Rise of Ransomware

Ransomware became a bigger challenge in 2012 as its popularity among malware authors increased. Unlike scareware, which encouraged you to buy fake antivirus protection, ransomware just locks your computer and demands a release fee. The malware is often quite sophisticated, difficult to remove, and in some cases it persists in safe mode, blocking attempts at remote support.

Victims usually end up with ransomware from drive-by downloads when they are silently infected visiting websites that host Web attack toolkits. This ransomware is often from legitimate sites that have been compromised by hackers who insert the malicious download code. Another source of infection is malvertisements where criminals buy advertising space on legitimate websites and use it to hide their attack code, as discussed in the malvertisement section.

The perpetrators use social engineering to increase the chances of payment. The locking screen often contains a fake warning from local law enforcement and the ransom is presented as a fine for criminal activity online. In some cases, ransomware also takes a photo of the victim using a webcam and displays this image in the locking screen, which can be unnerving for victims.

Criminals use anonymous money transfer systems or prepaid credit cards to receive the payments. The ransom typically ranges between $50 and $400. In many cases, payment doesn't unlock the computer. Symantec monitored a ransomware command and control server and saw 5,300 computers infected. About three percent of victims paid the ransom, which netted the criminals about $30,000.



Typical ransomware locking screen showing a fake police warning.

Long-term Stealthy Malware

Internet criminals are also making money from malware that stays hidden on the victims' computers. Operating in botnets with many thousands of computers acting collectively, these stealthy programs send out spam or generate bogus clicks on website advertisements (which generate referral income for the site owners). These techniques don't generate rapid returns like ransomware; however, they are much less likely to be discovered and, thanks to clever coding, are more difficult to remove. Consequently, they can generate a constant stream of revenue over time.

Email Spam Volume Down

After decreases in 2011, this year saw a further reduction in the volume of email spam from 76 percent of all email messages to 69 percent. There are several reasons for this. First, law enforcement action has closed down several botnets, reducing the number of messages being sent.[33] Second, spammers are increasingly redirecting their efforts to social media sites instead of email. Lastly, spammers are improving the quality and targeting of their spam messages in an effort to bypass filters and this has led to a reduction in the overall numbers being sent.

Advanced Phishing

While spam has declined slightly in 2012, phishing attacks have increased. Phishers are using very sophisticated fake websites—in some cases, perfect replicas of real sites—to trick victims into revealing personal information, passwords, credit card details, and bank credentials. In the past they relied more on fake emails, but now those emails coupled with similar links posted on social media sites are used to lure the victim to these more advanced phishing websites.

Typical fake sites include banks and credit card companies, as you'd expect, but also popular social media sites. The number of phishing sites that spoofed social network sites increased 123 percent in 2012.

If criminals can capture your social media login details, they can use your account to send phishing emails to all your friends. A message that seems to come from a friend appears much more trustworthy. Another way to use a cracked social media account is to send out a fake message to someone's friends about some kind of emergency. For example, "Help! I'm stuck overseas and my wallet has been stolen. Please send $200 as soon as possible."

In an attempt to bypass security and filtering software, criminals use complex website addresses and nested URL shortening services. They also use social engineering to motivate victims to click on links. In the last year, they have focused their messages around celebrities, movies, sports personalities, and attractive gadgets such as smartphones and tablets. The number of phishing websites that used SSL certificates in an attempt to lull victims into a false sense of security increased by 46 percent in 2012 compared with the previous year.

We saw a significant (threefold) rise in non-English phishing in 2012. In particular, we saw a significant increase in South Korea. The non-English languages that had the highest number of phishing sites were French, Italian, Portuguese, Chinese, and Spanish.

Recommendations

Protect Yourself Against Social Engineering.

For individuals as well as for businesses, it's essential that people learn to spot the telltale signs of social engineering, which can include undue pressure, titillation or a false sense of urgency, an offer that is literally too good to be true, bogus "officialese" in an attempt to make something look authentic (for example, lengthy reference numbers), implausible pretexts (for example, a Microsoft "representative" calls to tell you that your computer has a virus), and false quid-pro-quo offers (for example, receive a free gift when you provide personal or confidential information).

Avoid Ransomware.

Avoid marginal websites and, in particular, pirate software and adult sites. Do not install unsolicited plug-ins or executables if prompted to do so, even on legitimate websites. Consider using advertising blocker software in your browser. Ensure that your computer is up to date with the latest patches and updates to increase your resistance to drive-by Web infections. Keep backups and recovery disks so you can unlock your computer in an emergency. And, of course, have effective, up-to-date security software.

Think Before You Click.

That unsolicited email from a known acquaintance, such as your mother or coworker, may not be legit. Their account may have been compromised, if they've fallen for a social engineering trick.

Antivirus on Endpoints Is Not Enough.

On endpoints (desktops/laptops), signature-based antivirus alone is not enough to protect against today's threats and Web-based attack toolkits. Deploy and use a comprehensive endpoint security product that includes additional layers of protection, including:

- Endpoint intrusion prevention that protects against unpatched vulnerabilities from being exploited, protects against social engineering attacks, and stops malware from ever making it onto endpoints;
- Browser protection for protection against obfuscated Web-based attacks;
- Heuristic file-based malware prevention to provide more intelligent protection against unknown threats;
- File and Web-based reputation solutions that provide a risk-and-reputation rating of any application and website to prevent rapidly mutating and polymorphic malware;
- Behavioral prevention capabilities that look at the behavior of applications and malware and prevent malware;
- Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;
- Device control settings that prevent and limit the types of USB devices to be used.

LOOKING AHEAD

Looking Ahead

"Never make predictions," said a wise man, "especially about the future." But we can extrapolate from this year's data to speculate on future trends in the hope that this will help organizations and individuals protect themselves more effectively. Looking ahead, here are our priorities and concerns for the coming year:

More State-sponsored Cyber Attacks

The last few years have seen increasingly sophisticated and widespread use of cyber attacks. In peacetime, they provide plausible deniability; in wartime, they could be an essential tool. Cyber attacks will continue to be an outlet where tensions between countries are played out. Moreover, in addition to state-sponsored attacks, non-state sponsored attacks, including attacks by nationalist activists against those whom they perceive to be acting against their country's interest, will continue. Security companies and businesses need to be prepared for blowback and collateral damage from these attacks and, as ever, they need to make strenuous efforts to protect themselves against targeted attacks of all kinds.

Sophisticated Attack Techniques Trickle Down

Know-how used for industrial espionage or cyberwarfare will be reverse-engineered by criminal hackers for commercial gain. For example, the zero-day exploits used by the Elderwood Gang will be exploited by other malware authors. Similarly the "open-sourcing" of malware toolkits such as Zeus (also known as Zbot), perhaps in an effort to throw law enforcement off the trail of the original authors, will make it easier for authors to create new malware.

Websites Will Become More Dangerous

Drive-by infections from websites will become even more common and even harder to block without advanced security software. Criminals will increasingly attack websites, using malvertising and website attack kits, as a means of infecting users. Software vendors will come under pressure to increase their efforts in fixing vulnerabilities promptly. Users and companies that employ them will need to be more proactive about maintaining their privacy and security in this new social media world.

Social Media Will Be a Major Security Battleground

Social media websites already combine elements of an operating system, a communications platform, and an advertising network. As they go mobile and add payment mechanisms, they will attract even more attention from online criminals with malware, phishing, spam, and scams. Traditional spam, phishing, and malware will hold steady or decline somewhat; however, social media attacks will grow enormously. As new social media tools emerge and become popular, criminals will target them. Further, we think that the intersection of smartphones and social media will become an important security battleground as criminals target teenagers, young adults, and other people who may be less guarded about their personal data and insufficiently security-minded to protect their devices and avoid scams.

Attacks Against Cloud Providers Will Increase

So far, the very big data breaches have occurred in businesses that collect a lot of personal data, such as healthcare providers, online retailers or games companies. In 2013 we expect to see a variety of attacks against cloud software providers.

Increasingly Vicious Malware

Malware has advanced from being predominantly about data theft and botnets (although both are still very common) through fake antivirus scams to increased ransomware attacks in 2012. We expect to see these attacks become harder to undo, more aggressive, and more professional over time. Once criminals see that they can get a high conversion rate from this kind of extortion, we may see other manifestations, such as malware that threatens to and then actually deletes the contents of your hard disk. This was the case of the Shamoon attacks that occurred in August and erased data from the infected computer. Essentially, if it is possible, someone will try it; if it is profitable, many people will do it.

Mobile Malware Comes of Age

Just as social media is becoming the new "operating system" for computers, mobile phones and tablets are becoming the new hardware platform. Tablet adoption and smartphone market penetration will continue and this will attract criminals. What has evolved over a decade on PCs is emerging more rapidly on smartphones and tablets. We'll see ransomware and drive-by website infections on these new platforms in the coming year. For businesses that use these new devices or allow employees to bring their own to work, this will present a serious security problem in 2013.

Persistent Phishing

Identities are valuable, so criminals will continue to try to steal them. Phishing attacks will continue to get smarter and more sophisticated. For example, we'll see more perfect site replicas and SSL-encryption phishing sites. Phishing will become more regional and it will appear in a wider variety of languages, making it harder to block and more effective. It will continue its spread on social media websites where it will exploit the medium's virality and trusted messaging.

Endnotes

01 See http://krebsonsecurity.com/2012/03/mastercard-visa-warn-of-processor-breach/.

02 See http://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf.

03 Aviation Week & Space Technology, October 22, 2012, 82.

04 See http://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf.

05 The data for the data breaches that could lead to identity theft is procured from the Norton Cybercrime Index (CCI). The Norton CCI is a statistical model that measures the levels of threats including malicious software, fraud, identity theft, spam, phishing, and social engineering daily. Data for the CCI is primarily derived from Symantec Global Intelligence Network and for certain data from ID Analytics. The majority of the Norton CCI's data comes from Symantec's Global Intelligence Network, one of the industry's most comprehensive sources of intelligence about online threats. The data breach section of the Norton CCI is derived from data breaches that have been reported by legitimate media sources and have exposed personal information, including name, address, Social Security numbers, credit card numbers, or medical history. Using publicly available data the Norton CCI determines the sectors that were most often affected by data breaches, as well as the most common causes of data loss.

06 See http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-global.en-us.pdf.

07 See http://www.symantec.com/connect/blogs/shamoon-attacks.

08 Internet Security Threat Report, April 2012, "Targeted Attacks," 16.

09 See http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf.

10 See http://www.symantec.com/connect/blogs/cve-2012-1875-exploited-wild-part-1-trojannaid.

11 See http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf.

12 See http://www.symantec.com/connect/blogs/cost-cybercrime-2012.

13 See http://www.symantec.com/connect/blogs/lizamoon-mass-sql-injection-tried-and-tested-formula.

14 See http://www.symantec.com/connect/blogs/danger-malware-ahead-please-not-my-site.

15 See http://www.securityweek.com/comodo-certificates-used-sign-banking-trojans-brazil.

16 See http://blog.nielsen.com/nielsenwire/social/2012/.

17 See http://www.symantec.com/connect/blogs/instaspam-instagram-users-receive-gift-card-spam.

18 See http://www.gartner.com/it/page.jsp?id=2237315.

19 See http://en.wikipedia.org/wiki/FinFisher and http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html?_r=1.

20 See http://www.symantec.com/connect/blogs/androidbmaster-million-dollar-mobile-botnet.

21 See http://www.symantec.com/connect/blogs/androidbmaster-million-dollar-mobile-botnet.

22 See http://news.cnet.com/8301-1009_3-57470729-83/malware-went-undiscovered-for-weeks-on-google-play.

23 See http://developer.android.com/about/dashboards/index.html.

24 See http://www.gartner.com/it/page.jsp?id=2163616.

25 See http://www.wired.com/threatlevel/2011/06/dropbox/.

26 For more advice about cloud adoption, see https://www4.symantec.com/mktginfo/.

27 In the United States, for example, the NTSB reports that 472 people died in aircraft accidents in 2010 compared with 32,885 in highway accidents. See http://www.ntsb.gov/data/index.html.

28 See http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02.

29 See http://www.npr.org/blogs/money/2013/01/15/169424047/episode-430-black-market-pharmacies-and-the-spam-empire-behind-them.

30 See http://www.symantec.com/security_response/writeup.jsp?docid=2012-041001-0020-99.

31 See http://www.symantec.com/connect/blogs/flashback-cleanup-still-underway-approximately-140000-infections.

32 See http://www.symantec.com/connect/blogs/both-mac-and-windows-are-targeted-once.

33 See http://krebsonsecurity.com/tag/planet-money/.

About Symantec

Symantec protects the world's information and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

More Information

- Symantec.cloud Global Threats: http://www.symanteccloud.com/en/gb/globalthreats/.
- Symantec Security Response: http://www.symantec.com/security_response/.
- Internet Security Threat Report Resource Page: http://www.symantec.com/threatreport/.
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/.
- Norton Cybercrime Index: http://us.norton.com/cybercrimeindex/.

Symantec. Confidence in a connected world.

For specific country offices and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

04/13 21284430