SOPHOS

simple + secure

Security Threat Report

Mid-Year 2011

Assessing the Threatscape

Table of Contents

** Note: all currency is in US dollars*

Malware is complex and seemingly everywhere and is often difficult to stop. It knows how to find your data—even on your mobile device and Mac. You can't ignore your "safe" devices any longer: you need to recognize and stop the threats before they do harm.

Hacking attacks against high-profile organizations were in the spotlight during the first half of 2011. News stories highlighted damaging data loss and exposure of sensitive information and businesses remain on high alert. Meanwhile, web threats—such as fake antivirus and SEO poisoning—continue to be the top vehicle for malware attacks this year. Mac users, once safe from malware, fall victim to attack in 2011. As smartphone adoption skyrockets and social networking explodes, IT departments struggle with decisions regarding security versus the need to collaboratively share information. The blurring line between professional and personal use of technology means that mobile platforms and social networking continue to pose threats to your business data. Email spam also continues to evolve, as spearphishing has turned into an art.

Since the start of 2011, we've seen 150,000 malware samples every day. That's a unique file almost every half second, and a 60% increase as compared to malware analyzed in 2010. We've also seen 19,000 new malicious URLs each day in the first half of this year. And, 80% of those URLs are legitimate websites that were hacked or compromised.

As always, we continue to track—and where possible, thwart—the latest attack techniques. To stay secure, it's vital to understand how recent threats work. This way you can build the proper defenses to keep malware out and keep your business operations safe and productive.

Threatscape: First Half of 2011

To understand how threats work is to know where they hide, who they target and why. Here are some of the notable statistics that represent the Threatscape in the first half of 2011.

150,000

malware samples

SophosLabs analyzed this number every day in the first half of 2011—an increase of almost 60% compared to malware analyzed in 2010.

59%

decline in email use

A recent comScore report shows a whopping 59% decline in the use of email among 12–17 year-olds, and a 34% decline for the 25–34 year-olds. Facebook, text messaging and tweets are now the preferred communication methods for many people.

4.5

A new web threat is detected every 4.5 seconds

SophosLabs saw an average of 19,000 new malicious URLs every day in the first half of 2011– that's one every 4.5 seconds.

1 Million

people duped

The FBI estimates that a cybergang tricked nearly a million people into buying its fraudulent software. With a price point from $50 to $130 (depending on how many "extras" the victim gets talked into), this netted them over $72,000,000.

99.999%

people on the Internet are people you don't know

Remember not to share your information with every "friend" you meet online.

81%

social network security risk

Sophos asked approximately 1,700 computer users which social network they felt posed the biggest security risk and Facebook at 81% "won" by a landslide. A significant rise from the 60% who felt Facebook was the riskiest when we asked the question a year ago.

85%

of organizations have established an acceptable use policy

But only 69% of these organizations have specific policies for company-owned mobile device users. And, this number further decreases when you consider policy for employee-owned mobile devices (31%), reinforcing the need for establishing AUPs for all mobile devices.

68,593,657

people viewed "Chocolate Rain" on YouTube to date

If your friends ask you to view this video on Facebook, do not click. It may be a clickjacking scam.

Note: Data presented in this graphic reflects the most recent information at the time this report was going to press. These figures may increase or decrease over time.

What's New in Malware

Malicious software can take the form of a computer virus or worm and disrupt or deny computer operations, steal private or sensitive information or gain unauthorized access to system resources. Since January 2011, serious malware attacks have hit many high-profile organizations who suffered damaging data loss. Some attacks were for kicks, some for money, some for political hacktivist reasons and some for reasons unknown.

Targeted Attacks: The rationale grows

Targeted attacks involve patient, skilled and usually well-funded attackers whose motivation is fueled by large financial gain.

These cybercriminals bypass network security controls and do so over time. By working stealthily and patiently, they can breach networks and steal data. Some of the most high-profile targeted attacks during the first six months of the year included the RSA hack, and subsequent attacks on Lockheed Martin and the International Monetary Fund (IMF).

Hacktivists, on the other hand, often conduct attacks to prove a point rather than to make money.

Hacking for Fun and Fame: Enter LulzSec

Hacktivists typically hack for political purposes. They attack corporations, organizations and websites for a cause. These groups may deface websites, redirect traffic, launch denial-of-service attacks and steal information to make their point.

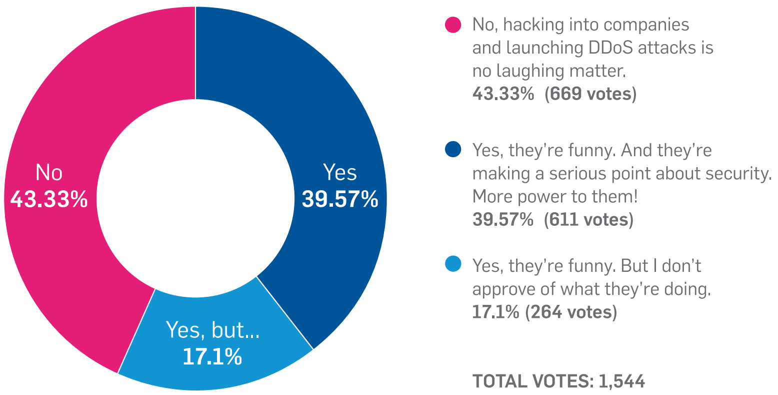
Notorious hacktivist group Lulz Security, or LulzSec, recently dominated headlines. LulzSec, also referred to just as Lulz, is the loosely conglomerated Internet group involved in the relentless hacker war on Sony, and attacks on PBS, the U.S. Senate, the CIA, FBI affiliate InfraGard and others. The group's name is derived from the Internet slang laughing out loud (LOL) and they claim to expose security vulnerabilities in websites and organizations for fun.

As this report was going to press, police arrested a 19-year old suspected hacker in Essex, UK, in connection with a series of hacks and denial-of-service attacks against a number of organizations. It's widely speculated that his arrest is in connection with the high-profile attacks by LulzSec, although unconfirmed.

LulzSec posted a press release announcing that its 50-day "cruise" has expired, and it must now sail into the distance. Shortly after, another hacker group A-Team, published a document that it claims reveals identities of some of LulzSec's members.

Although some people think hacking is a game that can help point out security vulnerabilities, hacktivists can expose the personal data of companies and individuals. In the U.S., the Obama administration seeks to increase sentences for those who break into government computer networks or potentially endanger the country's national security.

Do you find LulzSec's activities amusing?



TOTAL VOTES: 1,544

Source: Sophos poll

How Malware Reaches Us

Hackers can distribute malicious software through the links we click on when we surf the web, through the operating systems and through the software we run on desktops and laptops, and through the email messages and attachments we send. Even the mobile devices and social networking sites we use are targeted. So, as you're navigating the cyber terrain, check your tires, fasten your seatbelts and make sure your airbag is working.

Web Threats: A new threat every 4.5 seconds

Cybercriminals take advantage of our almost constant use of the web to launch malicious attacks. As a result, the web remains the biggest way cybercriminals distribute their malicious goods. During the first half of 2011, we saw an average of 19,000 new malicious URLs every day—that's one every 4.5 seconds.

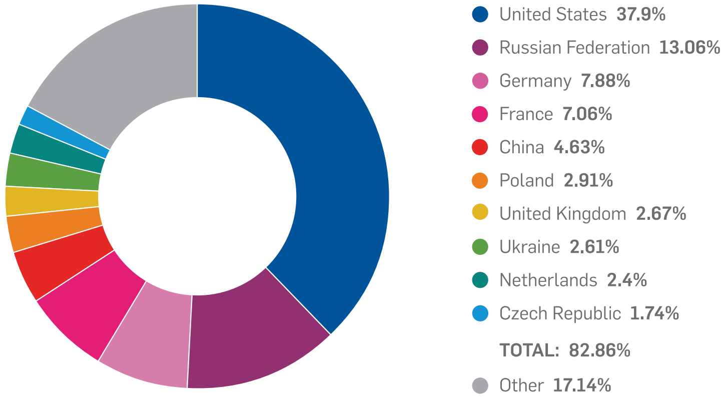
Many computer users still don't realize that something nasty can infect their computer when they visit a seemingly legitimate website. Yet more than 80% of the malicious URLs we found are legitimate websites hacked by cybercriminals. These thieves operate round the world to access the data on legitimate sites and subvert it for their own purposes. They achieve this by exploiting vulnerabilities in the software that power the sites or by stealing access credentials from malware infected machines.

The U.S. still holds the top spot on the list of countries hosting malware, although the total percentage of malware hosted by the U.S. declined slightly during the first half of 2011, down 1.4 points from 39.39% in 2010. The Russian Federation now claims the number two spot, a position held by France last year.

Two of the most common and persistent web threats are fake antivirus security software, also known as rogueware, or scareware, and Search Engine Optimization (SEO) poisoning. Cybercrimals can use these attack techniques separately or combined to take over your machine.

Top 10 countries hosting malware (via infected web pages)

January 1 – June 22, 2011



Source: SophosLabs

Fake Antivirus: Security scams reap millions

In 2010, fake antivirus was one of the more persistent threats of the year. In the first half of 2011, fake antivirus remained a threat, and these attacks are now actively targeting Mac users.

Here's how it works. A fake antivirus message warns users that their system has a virus, usually via a pop-up notification. These notifications appear authentic, right down to logos and certifications that the scammers stole from legitimate antivirus vendors.

The scam succeeds by convincing users that their computer has been infected by a virus. A pop-up urges users to get rid of the virus by purchasing antivirus software to remove the threat. Of course, paying for this software doesn't protect you—it only pays the bad guys. And in many cases, the cybercriminals are installing additional malware on your machine, and taking your credit card information. Recently, the FBI busted a cybergang that tricked nearly a million people into buying its fraudulent software. With a price point ranging from $50 to $130 the scam netted more than $72 million.

Many fake antivirus scams still target Windows users, and we see Mac fake antivirus software spreading in greater numbers than ever before. In some cases, scammers infect Macs to automatically open pornographic websites periodically—as further incentive to have users purchase the so-called "fix."

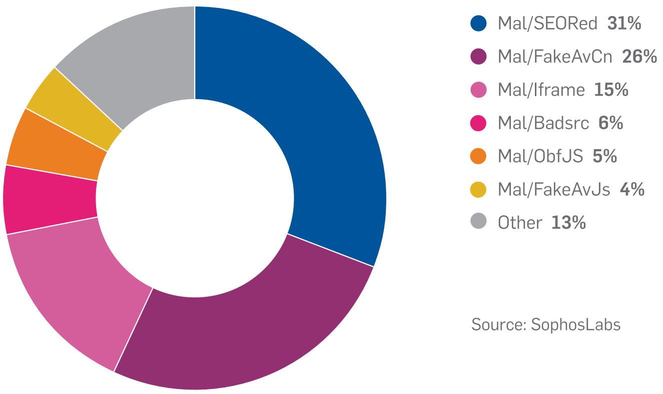
However, it's just another clever piece of social engineering, enticing you to hand over your credit card by making you believe that your Mac is compromised.

SEO Poisoning: Gateway for malicious behavior

The search engine is our gateway to the web. That's why cybercriminals manipulate search results from sites such as Google, Bing and Yahoo to lure victims to their malicious pages. Search engine optimization, or SEO, is a standard Internet marketing technique used by most companies to draw people to their sites. But it can also be abused. When the bad guys exploit SEO, it's known as SEO poisoning, or Black Hat SEO.

Black Hat SEO attacks

Snapshot of SWA detections May 20 – 25, 2011



Source: SophosLabs

Attackers use SEO poisoning techniques to rank their sites highly in search engine results and to redirect users to malicious sites. To maximize the number of victims, the crooks jump on search terms likely to generate a lot of traffic, including terms related to rapidly breaking news stories and popular "trending" topics. However, they also hijack mundane terms and target people searching for information on anything from burglar alarm wiring to diagrams of the heart.

When you inadvertently visit these malicious sites, malware such as viruses, worms or fake antivirus Trojans can load onto your computer. When hackers redirect you to their site, code on that site can load malicious PDF and Java components to exploit potential vulnerabilities in your computer software. Known as a "drive-by download," if the attempted exploits succeed, the malware will install on your machine.

Recently we've been tracking a fresh burst of SEO attacks that successfully capture user traffic. Black Hat SEO techniques stuff legitimate websites with content designed to rank highly in search engine results and then silently redirect users to malicious sites. The compromised results appear not just on regular web searches, but also on image searches.

Black Hat SEO attacks are extremely effective. A snapshot of the top malware we block on our customer web appliances shows that Black Hat SEO accounts for more than 30% of all detections.

The Worm That Won't Go Away: Stuxnet lingers

The Microsoft Windows worm Stuxnet, which security experts describe as extremely sophisticated malware that acts as a "dual warhead," continues to linger in 2011.

Some experts fear that the attack constitutes a new form of industrial warfare to which the United States and other nations are highly vulnerable. Others propose that the U.S. government was responsible for the worm, a question that Deputy Defense Secretary William Lynn sidestepped in a recent CNBC interview.

Whatever the source, Stuxnet has ushered in an era of threats that go beyond scammers trying to get money, to stealing information of importance to national security or causing disruptions to infrastructure. Partly in response to Stuxnet, the U.K. beefed up the country's cyber defenses.

Protection Strategies for Web Threats

To reduce risk, web use must be screened by quality protection technologies that can detect malware on hacked sites and respond quickly to emerging malware domains and URLs. Those tempted to bypass protection should be educated about its value and access to web proxies should be carefully monitored and controlled.

We also advise users to download and use antivirus software on and PCs and Macs.

Operating Systems: Mac malware is now real

Mac: The dream is over

Just when you thought no malware could take a bite out of Apple... malware threats on the Mac are now a reality. Malware makers have discovered a new business in Macs and they're not going to give up easily.

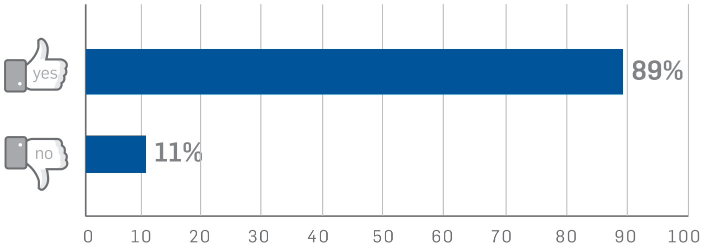
It's the biggest news on the Mac malware front in the past decade: Real, in-the-wild malware is infecting Mac users. Scammers use the same techniques (such as fake antivirus and SEO poisoning previously described) to infect Macs.

In response to one scheme, the "MacDefender" fake antivirus, Apple reportedly received more than 60,000 tech support calls. This caught Apple in a reactive position and it responded slowly.

This scam was followed by two others—"Mac Protector" and "Mac Guard." Mac Guard is particularly worrisome because it can install itself automatically without requiring an administrator password. In response, Apple has now instituted knowledge-based authentication (KBA) to prove user identity and regularly updates Xprotect, the anti-malware system built into recent releases of Mac OS X.

We ran a poll on the Sophos Facebook page asking folks if they would now recommend that friends and family install antivirus software on their Macs. Of the 968 people who answered the poll, 89% said yes.

Would you now recommend that your friends and family using Macs install antivirus software?



n = 968
Source: Sophos poll

Microsoft Windows: Malware targeting Windows XP still dominates

As we've seen, malware can infect machines regardless of platform. Microsoft Windows is notorious for malware, but cybercriminals choose to target Windows because of its huge installed base.

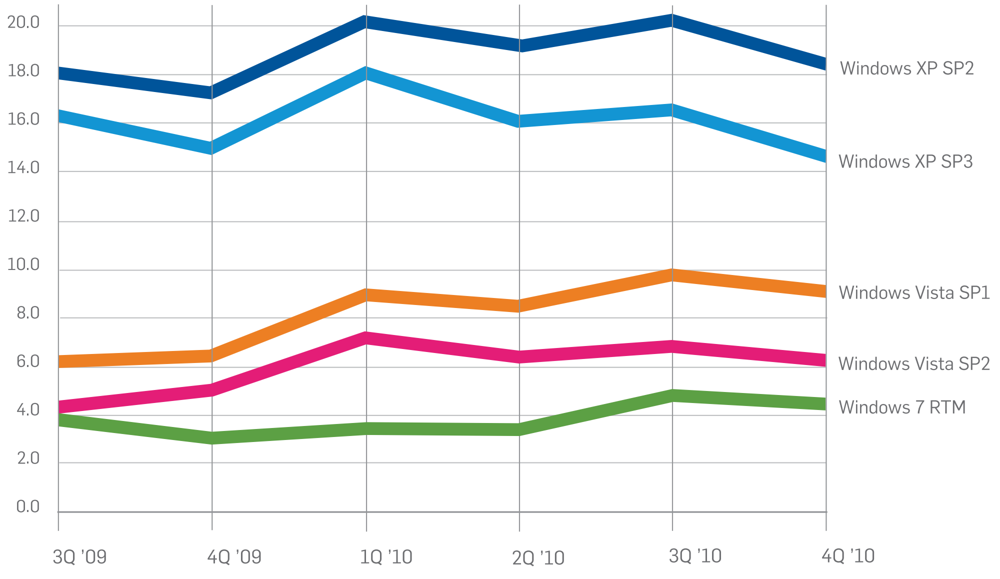
Microsoft collects data from about 600 million computers, which gives us good insight into how malware affects Windows. The most recent report, Microsoft's tenth Security Intelligence Report, shows an increase in malware targeting Windows 7, which is now installed in about a quarter of all Windows computers. Although there was a drop-off in new malware targeting XP, used by about half of all Windows users, Windows XP malware still accounts for the majority of malware written for Windows to date.

Protection Strategies for Operating Systems

The simplest way to put an end to malware is to keep abreast of security issues and Mac and Windows vulnerabilities. It's a good precaution to open your web browser's preferences menu and uncheck the box that says, "Open 'safe' files after downloading." This will prevent anything you download from automatically installing on your computer.

And it's important to apply patches in a timely manner. This way, you benefit from the developer's fixes to newly discovered vulnerabilities. You can also protect your company with endpoint security products and antivirus protection for Windows.

Malware continues to target Windows



Source: CRN

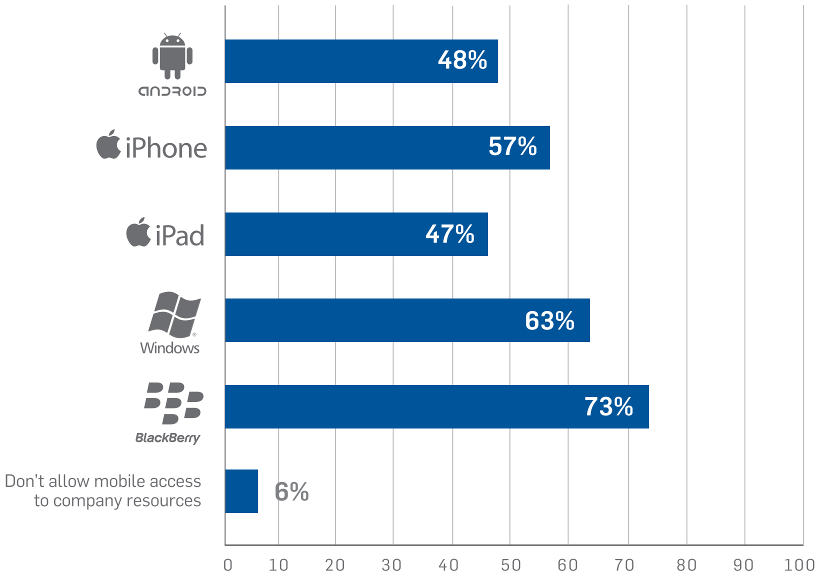
Mobile: Mini computers in your pocket

Mobile devices, including smartphones and tablets, are introduced into the corporate network each day. And, as these devices reach critical mass, it's vital that companies understand they act as a PC in your pocket and are similarly vulnerable. That's because they run operating system software and provide access to the web. Yet protecting mobile devices and communicating the need for protection remains a challenge.

A recent Sophos survey asked IT security professionals across multiple countries about mobile device use and access to corporate resources. Out of more than 240 responses, all but 6% said that they allow mobile devices to access corporate resources. Access for BlackBerry and Windows mobile phone OS ranked highest.

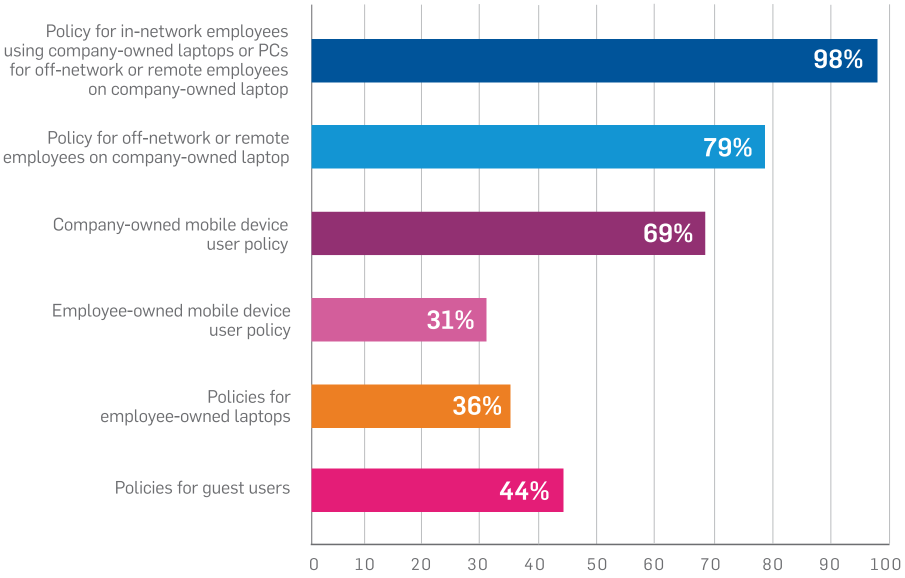
The survey also revealed that over 85% of organizations have already established an acceptable use policy (AUP) within their organizations, yet only 69% of these organizations have specific policies for company-owned mobile device users. And, this number further decreases when you consider policy for employee-owned mobile devices (31%), reinforcing the need for establishing AUPs for all mobile devices, whether corporate-issued or employee-owned.

Mobile device use and access to corporate resources



n = 242
Source: Sophos survey

Mobile device use and AUPs



n = 211
Source: Sophos survey

Notable Growth of Online Banking Malware Mandates AUPs

Forrester Research predicts that 20% of U.S. adults will do some form of banking transaction over their mobile phones by 2015, up from 12% today. It's increasingly important to maintain the integrity and privacy of networks, business data and personal information. Even more so, after learning that mobile application malware targeting online banking apps were discovered in 2011.

The first, which is named OddJob was discovered in February 2011. It keeps banking website sessions open even after users think they've logged off. By tapping into the session ID token—which banks use to identify a user's online banking session—cybercriminals can electronically impersonate a legitimate user and complete a range of banking operations. OddJob has targeted Symbian and BlackBerry smartphones and banking customers in the U.S., Poland and Denmark.

The second, which is called Zitmo or Zeus Mitmo (which is short for "Zeus in the Mobile" or Zeus "Man-in-the-Mobile"), aims to defeat the two-factor authentication used in online banking. The Trojan, which targets Android, Symbian, Windows Mobile and BlackBerry phones, will ask for details including cellphone number, type of device and a user's mTAN, which stands for mobile transaction authorization number. Once installed, the application will monitor incoming SMS messages for anything that resembles a banking transaction and will install a backdoor to receive commands via SMS. It also creates its own malicious database on the phone to capture financial information. With this information, a hacker can access your online banking platform and make fraudulent transactions by subverting the bank's security procedures. So far, this has successfully targeted Polish and Spanish banking customers.

Each mobile phone developer has its own strategy for security, some more effective than others. Understand how a smartphone's operating system can help protect you, or let malware attack.

Google's Android: Open platform difficult to secure

Android continues to gain market share in the U.S. with mobile analytics firm comScore reporting a 6% jump in the first quarter of 2011. (Interestingly, market share varies widely by country.) The openness of the platform and the availability of applications from alternative markets make Google's Android-based devices more difficult to secure.

While Google produces what you might call a "reference design" OS, it's up to the manufacturers to customize and test it on their devices. Many different companies produce Android phones for many different carriers. This means each device's OS is somewhat unique. Carriers also create their own customizations, further diversifying the variants of Android in the field. Perhaps because of this, it seems that the rate of new Android malware is increasing.

Cybercriminals infiltrated the Android Market with a host of malware during the first six months of the year, including a number of SMS-sending Trojans published by unknown attackers. In a more serious incident in March, the Droid Dream malware affected more than 50 Android apps. In June, Google removed at least 10 applications from the Android Market that hosted Plankton malware, which could be used to steal private data from the smartphone.

Another vulnerability found in a beta version of Skype for Android leaks sensitive data. However, Skype promised to fix the vulnerability.

Researchers at the University of Ulm publicized a security hole present in 99% of Android devices that allows unauthorized parties to snoop on your Google Calendar and Contacts. Google has plugged the hole, but concerns remain about how to fix more serious security vulnerabilities on the Android devices themselves. Because Google relies on manufacturers and carriers to push out OS updates, fixes might not be sent to Android users as soon as they are available. Unfortunately, this represents a real problem. Before you get the update on your phone, you must rely on Google to fix the bug, your device manufacturer to patch its custom OS and your carrier to decide to provide you with the fix.

Organizations should note that it's not only Android smartphones that are vulnerable. Tablets, such as Samsung's Galaxy Tab or HTC's Flyer, that run the operating system are also at risk, and this poses a risk to your data.

Pressure on Google is building on two fronts. On one side, users demand better security. On the other side, security vendors such as Sophos want Google to provide better OS interfaces so that security software can fight against the rising tide of Android malware.

RIM's BlackBerry: Rigorous QA

Despite waning investor confidence and a loss of market share to the iPhone, Research In Motion's (RIM) BlackBerry is still the device of choice for many enterprises.

RIM centrally controls all software and updates for BlackBerrys. Because no one else produces the handsets, the company has a very rigorous quality assurance (QA) process to find defects and ship fixes and updates to improve security on a more regular basis.

This doesn't mean vulnerabilities are non-existent. CanSecWest's PWN2OWN competition, which is run by HP, challenges ethical hackers to execute arbitrary code (PWN) on laptops or mobile phones through a previously undisclosed browser exploit. If you succeed, you can go home with a new mobile device (OWN).

Hackers at the competition successfully exploited a software flaw in Google's Chrome browser Webkit codebase to attack the BlackBerry. In a laudably quick response, Google almost immediately patched the offending code in Chrome.

And, in July 2011 RIM issued an advisory to address several issues in Adobe Flash, the most severe of which could result in remote code execution of any application that uses Adobe Flash, including its most recent product, the BlackBerry PlayBook. Although there are no known attacks at the time this report was going to press, RIM advised PlayBook users to update their software so they remain protected against applicable Flash vulnerabilities.

Apple's iOS: Security advantage with the App Store

iPhones and iPads have the same security advantage as RIM because Apple controls the handsets as well as the operating system.

It's estimated that there will be 150 million U.S. smartphone users in mid-2011, with 120 million people accessing the mobile web.

Source: Nielsen

They also benefit from the partial buffer of Apple's App Store, which vets apps according to some very strict rules, eliminating much of the risk of rogue apps. Users willing to pay for their apps remain relatively safe. But those who "jailbreak" their iPhones to alter iOS, compromise their security and are subsequently at risk of downloading maliciously modified apps.

There was also a backlash against Apple for a location-tracking bug that meant iPhones and iPads were collecting location-related data and archiving it on users' machines, which theoretically allowed someone with access to your machine to track your physical whereabouts. The company has since released an iOS update to address this vulnerability and hopefully regain some positive press within the Mac community.

Microsoft's Windows Phone 7: The security middle ground?

Similar to RIM and Apple, Microsoft centrally controls the distribution of updates for the Windows Phone platform. But unlike the BlackBerry and the iPhone, Windows phones are manufactured by several device makers and have multiple carriers.

Although Microsoft does not control its phones as closely as RIM or Apple, the updating process is not dependent on device makers and carriers, as with Android devices. This places Windows Phones in a sort of middle ground.

Microsoft's central control of updates means flaws can be patched as soon as fixes become available. But because device manufacturers and carriers have no control over which updates to install, this approach comes with some risk.

For instance, when Microsoft tried to push an update to the Windows Phone 7 early this year, the update accidentally "bricked" some Samsung Omnia handsets, rendering them unusable with no restoration data available.

Protection Strategies for Mobile

Today, most people use their mobile devices for a mix of personal and professional purposes. Although IT departments in traditional enterprise organizations have tried to keep work-related technology separate from personal consumer-based technology, the two are inevitably blending.

- This makes it even more important to have a mobile computing device security program in place, including promoting ongoing awareness and conducting training for users, and setting up policies, encryption, firewalls and login passwords. All smartphone users would be wise to use common sense with phone passwords. New research from Apple suggests that 15% of all iPhone owners use one of just 10 passwords on their lock screen.
- **For more practical guidance on securing mobile devices, download 7 Tips for Securing Mobile Workers.**
- **Learn more about Sophos Mobile Control, which delivers data protection, policy compliance and device control for mobile devices.**

Social Networking: Threats explode, so limit access to personal info

Social networking privacy issues dominated the headlines in the first half of 2011. With most social networks, the default settings share everything and users have to reset their options to make their accounts more private. This opens up a host of security issues because so many people—both friends and strangers—have access to your information.

And to see just how many security issues social networks pose, we recently conducted a social media poll that asked whether respondents' organizations have encountered spam, phishing or malware incidents. Of the nearly 2,000 people polled, 71% reported that they, or one of their colleagues, had been spammed on a social networking site, 46% had been phished and 45% were sent malware. The remaining respondents were divided—some were not victims, others were unsure.

Because of all the personal information readily available on social networks, cybercriminals can steal information about you and then tailor their attacks based on your interests and likes. This is known as "social engineering" and it makes security threats much more difficult to recognize.

Here's a closer look at some of the recent attacks and privacy issues plaguing three major social networking sites—Facebook, Twitter and LinkedIn—and a sneak peek at Google+:

Facebook: Self-XSS, clickjacking and survey scams abound

With so many users, Facebook is a target for scams; it can also expose your personal information far beyond your group of friends.

Users need to remember that Facebook makes money from its advertisers, not its users. Because advertisers want to get their message out to as many people as possible, Facebook shares your information to everyone, not just your "friends." And most recently, Facebook's facial recognition technology automatically suggests that friends tag you, unless you turn it off.

Scams on Facebook include cross-site scripting, clickjacking, survey scams and identity theft. One of the scammers' favorite methods of attack at the moment is known as cross-site scripting or "Self-XSS." Facebook messages such as "Why are you tagged in this video?" and the Facebook Dislike button take you to a webpage that tries to trick you into cutting and pasting malicious JavaScript code into your browser's address bar. Self-XSS attacks can also run hidden, or obfuscated, JavaScript on your computer allowing for malware installation without your knowledge.

Facebook scams also tap into your interest in the news, holiday activities and other topical events to get you to innocently reveal your personal information. Facebook posts asking you to create a Royal Wedding guest name and In honor of Mother's Day seem innocuous enough—until you realize that information such as your children's names and birthdates, pet's name and street name

facebook

Facebook security best practices:

- Adjust Facebook Privacy settings
- Read the Facebook Guide to Privacy
- Think carefully about choosing your friends
- Show "limited friends" a cut-down version of your profile
- Disable options, then open them one by one
- Read the complete guidelines

now reside permanently on the Internet. Because this information is often used for passwords or password challenge questions, it can lead to identity theft.

Other attacks on Facebook users include "clickjacking" or "likejacking," also known as "UI redressing." This malicious technique tricks web users into revealing confidential information or takes control of their computer when they click on seemingly innocuous webpages. Clickjacking takes the form of embedded code or script that can execute without the user's knowledge. One disguise is a button that appears to perform another function. Clicking the button sends out the attack to your contacts through status updates, which propagates the scam. Scammers try to pique your curiosity with messages like Baby Born Amazing Effects and The World Funniest Condom Commercial – LOL. Both clickjacking scams take users to a webpage urging them to watch a video. By viewing the video, it's posted that you "like" the link and it's shared with your friends, spreading it virally across Facebook.

Clickjacking also is often tied to "survey scams" that trick users into installing an application from a spammed link. Cybercriminals take advantage of news topics, such as the Osama bin Laden video scam, which takes you to a fake YouTube site in an effort to get you to complete a survey. Scammers earn commission for each person that completes it. Taking the survey also spreads the scam virally to your Facebook friends.

In theory, new Facebook security features provide protection against scams and spam—but unfortunately they're mainly ineffectual. Self-XSS, clickjacking and survey scams essentially did not exist just a few years ago, but they now appear on Facebook and other social networks on a daily basis.

Our recent social networking poll also asked computer users which social network they felt posed the biggest security risk. Facebook is clearly seen as the biggest risk with 81% of the votes, a significant rise from the 60% who felt Facebook was the riskiest when we first asked the question a year ago. Twitter and MySpace each received 8% of the votes this year, and LinkedIn only 3%.

Twitter: Beware of shortened URLs

Twitter is a valuable source of real-time information. During the devastating Japanese earthquake and tsunami in March, Twitter users shared information and helped raise funds. Unfortunately, as often happens, scammers try to channel that goodwill for their own gain. A Twitter scam impersonating the British Red Cross asked tweeters to send money through Moneybookers to a Yahoo email address in one Japanese tsunami charity scam. In another scam, emails resembling Twitter notifications included dangerous links disguised as a tsunami video. If you clicked on this link, malicious JavaScript could infect your computer.

Twitter users often shorten URLs via bit.ly and other services to keep tweets within their 140 character limit. Hackers can also create shortened URLs to easily redirect you to malicious sites, because the URL itself gives you no indication of the site name. Although most shortened URLs are legitimate, if a link brings you to another page that asks for a Twitter or Facebook password, leave immediately.

Similar to Facebook scams, Twitter messages promise such curiosities as the Banned Lady Gaga Video, which brings users to a fake YouTube page when followed. If you click the play button, a window pops up and seeks permission to access your Twitter account. If you grant access, you allow third parties to post messages using your account name. Another recent scam, TimeSpentHere, promises to tell you how many hours you've spent on Twitter. Because it appears to come from a Twitter friend, you may think about clicking on it. But this rogue application actually wants your email address, which could be used later for a phishing campaign or spam.

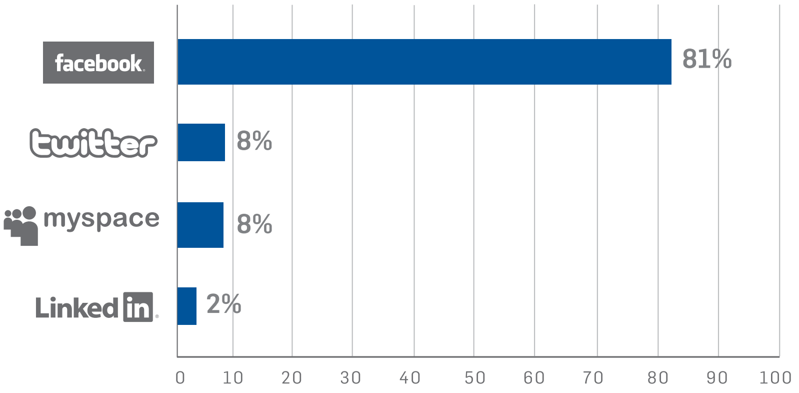
LinkedIn: Threats remain low

Although cybercriminals more frequently target users of Facebook and Twitter, the business networking site LinkedIn is also a target. The biggest threat with LinkedIn is data mining. Cybercriminals take information about companies and whom they employ, and then use that information to launch spearphishing attacks. Corporate directories also exist online, providing a wealth of information for spearphishers.

Malicious LinkedIn invitation reminders pose another threat. These links can redirect you to a webpage that installs a variant of the Zbot malware (also known as Zeus) onto your computer. If you click on the link, remote hackers can compromise your computer and potentially steal your confidential data.

Although most shortened URLs are legitimate, if a link brings you to another page that asks for a Twitter or Facebook password, leave immediately.

Which social network do you think poses the biggest security risk?



n = 1,699
Source: Sophos: Naked Security poll

Sophos asked over 1,200 computer users which social network they felt posed the biggest security risk; and Facebook won by a landslide with 82%. That's a significant rise from the 60% who felt Facebook was the riskiest when we first asked the question a year ago.

Google Plus: Early users demand privacy

Google Plus, a recently launched social network that aims to compete head-to-head with Facebook, is learning the ropes as far as privacy is concerned. Google currently restricts the social network to a "limited field trial" so it can gather feedback, patch bugs and identify privacy holes before making the site available to a mass audience. Privacy experts say that Google Plus is designed to let people have better control over privacy with respect to sharing with family,
co-workers and friends.

In response to initial user feedback, Google Plus recently changed its privacy options regarding gender, so that users do not have to reveal their gender online.

Protection Strategies for Social Networking

Facebook has its own Facebook Security page. But we also recommend reviewing the Sophos best practice guidelines for Facebook privacy settings with your organization's staff, and setting up ongoing security training and awareness programs. You can keep up to date with the real threats on Facebook by joining the Sophos Facebook page. And, you can learn how to clean up your Facebook profile after a survey scam in this Sophos YouTube video.

Twitter users can use its Safety Center and its blog posts to learn how to Avoid Phishing Scams. If you find a rogue Twitter application you can go to Twitter's Settings/Applications to revoke the offending app's rights. And you can also get regular status updates on Twitter by following @safety and @spam. **Follow @SophosLabs to get regular updates to protect your business.**

LinkedIn users should regularly review its blog that discusses security issues and includes posts such as Protecting yourself from hackers and Quick tips on Security and Privacy.

IT managers should also work with their communications team to **create and roll out a corporate social media policy** that includes not only how to communicate using social media, but also how use these sites, safely.

Finally, **keep your antivirus software up to date**, install the latest security patches and if you're looking for news, go to legitimate news websites, rather than clicking on a link that was sent by a friend.

Email Spam and Spearphishing: Still a threat

A recent comScore report shows a whopping 59% decline in the use of email among 12- to 17-year olds, and a 34% decline for the 25 to 34 age bracket. Facebook, text messaging and Twitter have taken over as preferred communication methods for many.

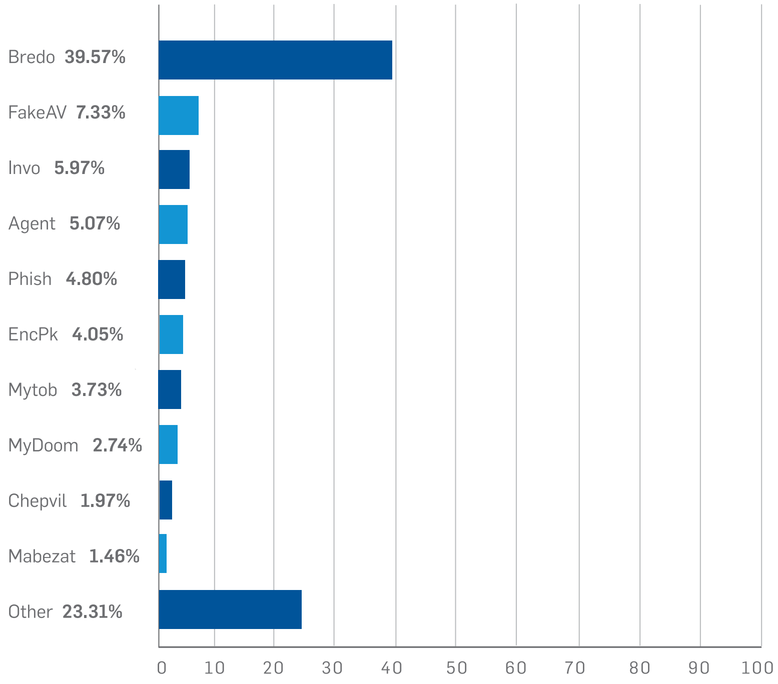
Dovetailing with a decline in email use, threats from email attachment malware are declining. As compared to 0.27% of email attachments containing threats in the first quarter of 2010, just 0.16% contained threats in the first quarter of 2011. Scammers now use more HTML attachments rather than just ".exe" executable files as vehicles to deliver malware.

More prevalent in the email world today, scammers employ "spearphishing" attacks, which use social engineering techniques to lure a specific target into divulging sensitive information, including logins and passwords. Hackers recently targeted Lockheed Martin, the world's biggest military contractor, using a spearphishing attack. Recognized as a high-value target in the world of cyber espionage and hacking, Lockheed Martin said it records a million probes against its network a day. Experts speculated that hackers sent an email to employees and used a spearphishing attack to plant a virus on the Lockheed Martin network. This enabled them to gain access to the corporate virtual private network (VPN), which was then compromised—possibly using information and materials stolen during the RSA hack in March. Although Lockheed Martin reported that no customer, program or employee personal data was compromised, this attack proved that email still delivers serious threats.

Although improvements to gateway, URL blocking and web-based protection contributed to a drop-off in traditional email, spam still exists and turns a profit.

The U.S. once again leads the field of spam-relaying countries, contributing approximately 13% of the world's spam traffic in the first half of 2011. India, Russia, South Korea and Brazil broke through the 6% barrier during the first six months of the year, with their massive online populations clearly lacking the protection needed to keep their systems free from spamming malware.

Top malware families in infected email



Source: SophosLabs

But mature major economic powers such as Italy, France and the U.K. also occupied the top 10, so it's clear that wealth and technological advancement don't guarantee safety.

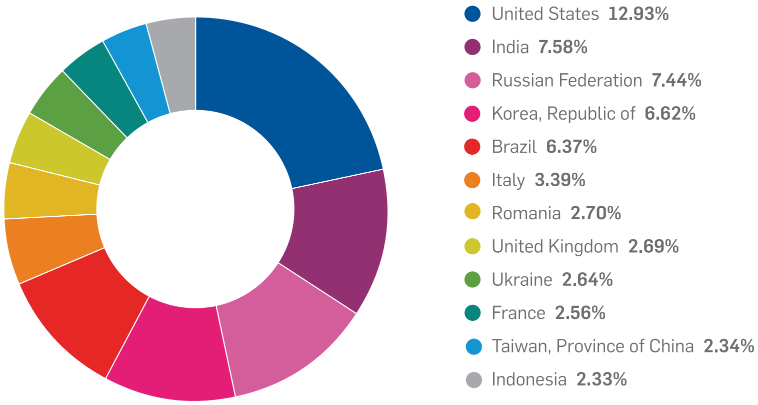
In global terms, Asia edged ahead of Europe in the first half of 2011 in spam production, growing from 33% of spam production in the first half of 2010 to 40%, while Europe dropped a couple of points to 29%. North America held on to third place, also dropping slightly.

Protection Strategies for Email Spam and Spearphishing

Anti-spam software is a must for capturing "traditional" spam. Spearphishing is much harder to detect. It helps to limit access to personal information on social networks, etc., in the first place. And as always, don't click on anything if you have doubts.

Dirty Dozen: Spam relaying countries

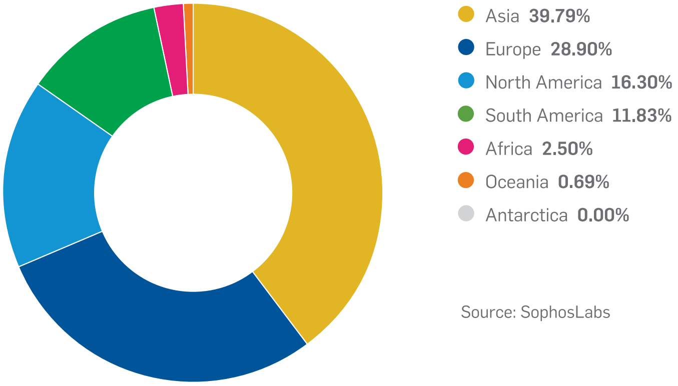
January – June 2011



Source: SophosLabs

Spam relaying by continent

January – June 2011



Source: SophosLabs

Software: Vulnerabilities abound

The software we use every day can contain insecure code and vulnerabilities that allow hackers to break into individual machines or networks to plant malware. Because of the ubiquity of Microsoft Office and Internet Explorer, hackers most often target Microsoft products, although other commonly used software including Adobe and Mac programs are also targets.

In June, Microsoft issued its second largest patch release to date in 2011, fixing 32 critical and important severity vulnerabilities, including flaws in Internet Explorer (IE) versions 6, 7 and 8 that could allow remote code execution. April's patch of 64 vulnerabilities in 17 bulletins included fixes for a flaw in IE 6, 7 and 8 that ethical hackers exploited in this year's PWN2OWN competition. Sophos detected malware exploiting this vulnerability as Troj/ExpJS-BV.

Meanwhile, Microsoft launched an effort in March to convince users to upgrade from IE 6 to a newer version (IE is now on version 9). Microsoft previously stopped supporting IE 6, meaning the company no longer issues security patches for the aging browser, leaving users vulnerable to hacker attacks.

In June, Microsoft reported that worldwide use of IE 6 had fallen to less than 11% and set a goal of reducing usage to less than 1% of all IE users.

Mac computers came under threat on a few occasions, due to security holes in non-Mac software running on the OS X. In June, Apple pushed out a security update to plug holes in Oracle's Java Platform that left users vulnerable to drive-by download attacks. Also in June, Apple released the latest version of its operating system, OS X 10.6.8, which fixed multiple flaws that could allow arbitrary code execution. The update also served to identify and remove known variants of the Mac Defender family of fake antivirus software.

So far this year, hackers have also exploited multiple zero-day flaws in popular Adobe software including Flash, Reader and Acrobat. Because Flash Player is so widely used and distributed, other applications that support Flash content could be exploited.

In 2010, scammers widely exploited Adobe's Reader software, but Adobe is taking steps to address this issue and now releases patches on a more predictable basis. Adobe also works with security vendors through the Microsoft Active Protections Program (MAPP). Members of MAPP receive security vulnerability information in advance of Microsoft's monthly security update to get an early start on building protections.

Protection Strategies for Software

Security researchers identify software vulnerabilities on a near-constant basis. Unfortunately, software companies often have to play catch-up with the cybercriminals to counter zero-day attacks—previously unknown flaws. Because software makers issue security patches frequently—with Microsoft issuing patches on the second Tuesday of each month—it's important to keep software up-to-date, install patches regularly and run antivirus programs. It also makes sense to use application control technologies to take control of what your users install and reduce the threat surface. Fewer programs and plug-ins means lower risk.

To keep abreast of the latest vulnerabilities, read and review authority sites and visit the SophosLabs Vulnerabilities Analysis page.

It also makes sense to use application control technologies to take control of what your users install and reduce the threat surface. Fewer programs and plug-ins means lower risk.

Removable Media: Beware of Autorun

Modern malware, such as the Conficker worm, exploits removable media such as USB flash drives and CDs/DVDs to automatically run when inserted into a target computer. But there's good news on this front.

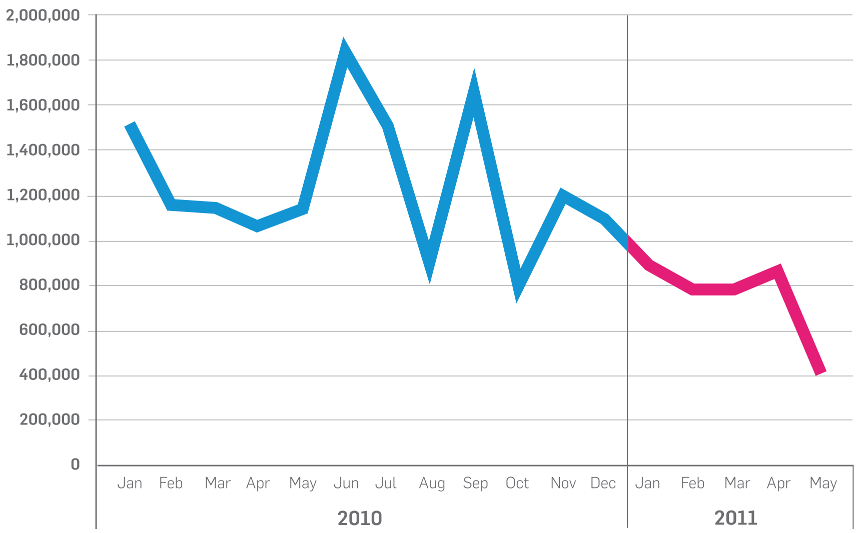
Between March and May of this year, there was a significant drop in the number of computers being infected by malware exploiting the Windows Autorun feature. Autorun infections dropped by 59% on XP machines and by 74% on computers running Windows Vista. It appears that Microsoft's decision earlier this year, to roll out an update preventing Autorun on removable media without a user's permission, paid off.

However, a recent study conducted by the U.S. Department of Homeland Security (DHS) discovered that the biggest risk from removable media might come from poor decision-making by users. According to a Bloomberg report, the DHS study found that government employees showed carelessness in using thumb drives and CDs that had been left in parking lots and offices, without verifying their authenticity. Of those who picked up the removable media, 60% plugged the devices into their office computers. That figure rose to 90% when the devices were marked with an official logo.

Reduction in infections by major autorun-abusing families

Reported by Microsoft Malicious Software Removal Tool

January 2010 – May 2011



Source: Microsoft

Protection Strategies for Removable Media

The first line of defense against removable media threats is restriction and control. Companies may want to restrict how and where these devices are used. Corporate use policies should clearly inform employees of proper and acceptable use. For instance, you may want to forbid employees to use removable media devices that they bring in from home. Also, make sure your company scans devices regularly for malware and sensitive data. You should also implement file encryption when using removable media.

Law & Order

So, what can governments do to protect us from cybercrime? Should governments be involved and create legislation around data breach notification? Are they effectively going after cybercriminals? Some companies that suffered data breaches, such as Sony and Citigroup, are criticized for failing to alert their customers in a timely manner about major data breaches that might expose personal data. But, legislation is emerging to help guide companies.

Legislation: A work in progress

A draft version of a data breach bill currently in the U.S. House of Representatives requires companies that experience a breach to tell law enforcement within 48 hours and to begin notifying consumers within 48 hours of when the company completes an assessment of the hack. The bill could be changed to give companies a limit of 60 days for notification. The draft bill would also require companies to begin erasing personal data once it is no longer needed, eliminating the possibility it could be stolen in a hacking attack. U.S. President Obama also proposed a more sensible disclosure law that would uniformly define Personally Identifiable Information (PII) and set new rules for notification that would supersede existing state laws.

Cracking Down on Cybercrime: Governments take action

Government agencies continually try to crack down on cybercrime. Nevertheless, there are limits to what they can do to counter hacker attacks, because cybercriminals may operate across several jurisdictions or in foreign countries. For instance, a crook in Belgium can defraud someone in Australia via a malicious advertisement served from China, which tricks the person into a credit card transaction in Canada processed by a server in Finland.

Police have made some headway in the battle against online hacktivist groups LulzSec and Anonymous. Authorities arrested suspected members of Anonymous after raids in Turkey and Spain. In addition, the FBI recently announced some important success against two international cybergangs based in the U.S. The FBI operation, codenamed "Trident Tribunal," led to several arrests and significant disruption of cybercriminal operations. The first cybergang was allegedly responsible for selling $72 million in fake antivirus software, as mentioned earlier. A second cybergang provided malvertising services; this technique lets scammers sneak advertisements for fraudulent services—notably, for fake antivirus—onto respectable websites. According to the FBI, just two people stole more than $2 million in that scam.

How to Stay Ahead of Threats

Training and awareness need to be integrated into your organization's security strategy along with technology tools to help you keep malware out and protect your data. Get users to think of online security in terms of the lessons they already know from the real world. This encourages critical thinking, rather than just applying "Band-Aid" solutions for specific issues. And then implement all of the tools you need to simplify the process for securing your organization from threats.

End-User Training and Awareness: Real life lessons translated

Here are some tried and true security lessons that work online too:

- "If it sounds too good to be true, it is."
- "Don't take candy from strangers." (99.999% of the people on the Internet are strangers.)
- "Your inbox is just like your mailbox, anyone can put anything in there. Just because they know your address doesn't mean you should trust them."
- "There is no such thing as a free lunch." Somebody somewhere is paying and whoever pays the piper calls the tune, such is the case with Facebook's advertisers.

What Tools Help Us Stay Secure?: A practical guide

While education and awareness provides one smart way to stay ahead of the bad guys and their malware attacks, a range of technologies can also help you to maintain security and privacy. They include:

Antivirus software for Windows and Macs
A must-have for just about any computer system; detects, blocks and removes malicious code; should cover rootkits, scripts in web pages, exploit attempts and other malicious activities, as well as traditional file-based threats. Local detection data is best supplemented by expanded online lookup systems to protect against the latest emerging threats. Use "allow" lists to minimize false positives.

Gateway malware and content filters
Watch for malware being downloaded at the gateway level. This should include blocking malicious URLs as well as file transfers, again using cloud lookups.

Quality web filtering solutions These solutions let companies enforce browsing policies, too. Management and reporting systems will help corporate admins monitor company networks for compliance with policies.

Anti-spam software
Another must, especially for businesses; filters email to remove spam, phishing scams and messages with malicious attachments, and links to malicious web pages. This must combine strong detection with vanishingly small false alarm rates. It should also provide traceability and archiving to ensure blocked messages can be retrieved in case of false positives.

Encryption software
Vital in any business working with sensitive customer data, or any place where internal data might be valuable or compromising if lost. Data should be kept in encrypted form whenever possible, particularly during transfer and on portable systems or devices. Fail-safe and administrator overrides can help in the case of lost passwords or abuse by rogue employees.

Patching and vulnerability monitoring
Keep software up to date with the latest security fixes. Some software may offer automatic updating; but in corporate environments, internal testing may be needed first. Employ solutions to coordinate and enforce patching policies across a network, and tools to scan for vulnerable and out-of-date software.

Device and network control
Enforcing rules on which systems and devices can connect to company networks is a necessity for network integrity. Isolate company networks from all potential sources of infection and protect them from methods of data theft.

Data loss prevention
Helps you monitor data transfer so you can control what users do with sensitive data.

In the first half of 2011, hackers attacked many high-profile companies and government agencies, in some cases stealing sensitive and confidential data. In other attacks, the hackers sent a warning shot as a signal that no one was secure. Mac users had to start worrying about malware, something that has not been a major issue since the introduction of OS X. Other trends, such as the blending of work and home lives and the sharing of information with online social networks, can put companies at risk. Continue to check our Security Trends page to get a sense of the new threats that continue to emerge.

Constant vigilance is necessary, but you don't need to go it alone. Sophos has the technology tools to help you combat security threats. Combine those with training and awareness programs, and you'll go a long way toward keeping your data safe. In our increasingly pressurized business environment, Sophos simplifies your day-to-day work by taking on the heavy lifting to help you prevent malware and protect your data.

Sources

Sophos.com

SophosLabs

Sophos: Naked Security

Associated Press

Bloomberg News

Business Insider

Channelnomics

Computerworld

comScore: The 2010 Digital Year in Review

comScore MobiLens

CRN

Fortune

Forrester Research

HeadlineBits.com

Huffington Post

Inc.

InformationWeek

L.A. Times

Nielsen

Network World

New York Times

PC World

Privacy Professor

ReadWrite Mobile

Reuters

Socialbakers

TechCrunch

TechTarget

TechWeb

The Guardian

Time: Techland

Vanity Fair

Wikipedia

ZDNet

Copyright 2011 Sophos Ltd. All rights reserved.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Ltd. and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

The information contained in the Security Threat Report is for general information purposes only. It's provided by Sophos and SophosLabs and Naked Security. While we keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the website or the information, products, services, or related graphics contained in this document for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK
© Copyright 2011. Sophos Ltd. All rights reserved.
All trademarks are the property of their respective owners.