

# Security Threat Report 2012



Seeing the Threats Through the Hype

## Table of contents

<b>Foreword</b> .....	1
<b>2011 in review: Hype about hacktivism</b> .....	2
<b>Under attack</b> .....	4
Hacktivism takes center stage .....	4
Protection strategies for hacktivism .....	4
Data theft and loss .....	5
Conficker remains widespread despite patch .....	6
Malware .....	6
Protection strategies for malware .....	6
The fall of fake antivirus .....	7
Targeted and stealth attacks are not just for defense contractors .....	7
Botnet takedowns momentarily knock out spam .....	8
Origins of spam .....	9
Protection strategies for phishing and spam .....	9
<b>Online threats</b> .....	10
Anatomy of an attack: Drive-by downloads and Blackhole .....	11
How Blackhole works .....	11
Stat snapshot: How web threats spread .....	12
Protection strategies for Blackhole .....	12
Protecting against network threats: Secure gateways .....	13
Protection strategies for networks .....	13
<b>Systems and software threats</b> .....	14
Operating systems: The rise of Mac malware .....	14
Protection strategies for operating systems .....	14
Software patching: More than Microsoft .....	15
Protection strategies for software .....	15
Removable media: Preventable data loss .....	16
6 tips to mitigate risk of data loss .....	16
Protection strategies for removable media .....	16

## Videos

Mark Harris of SophosLabs explains fake antivirus .....	7
Principal Researcher Fraser Howard explains web vulnerabilities .....	11
Director of Technology Strategy James Lyne explains mobile security .....	18
CTO Gerhard Eschelbeck explains cloud security .....	20
Graham Cluley of NakedSecurity.sophos.com explains social networking threats .....	23
Chester Wisniewski of NakedSecurity.sophos.com explains complete security .....	24

<b>Risk in the way we work .....</b>	<b>17</b>
Consumerization of IT .....	17
Mobile malware .....	18
Protection strategies for mobile devices .....	18
Mobile operating system security .....	19
Mobile data loss case study: Healthcare .....	20
Cloud computing .....	20
Cloud insecurity .....	20
Leaks from the cloud .....	21
Protection strategies for cloud computing .....	21
Social networks .....	22
Relaxed restrictions and risk to brands .....	22
Protection strategies for social networks .....	23
The erosion of privacy policies .....	23
<b>Sophos Complete Security .....</b>	<b>24</b>
<b>What's new in 2012: 10 trends .....</b>	<b>25</b>
<b>The last word .....</b>	<b>26</b>
<b>Sources .....</b>	<b>27</b>

## Graphics

Threat exposure risk .....	8
Spam dirty dozen countries .....	9
Spam sources by continent .....	9
Today's landscape for web threats ..	10
How web threats spread .....	12
Mac malware 1982-2011 .....	14
Survey: Mobile security .....	19
Survey: Social networking security ..	22

## Symbols

-  Watch a video
-  Download a free trial
-  Read a whitepaper

# Foreword

Over the past year we in the IT security industry have seen a growing awareness of the work we do. In 2011, a number of highly visible cyberattacks made news headlines around the world, but the underlying problem affects us all. It seems that the cybercriminals are getting bolder in their attacks as the availability of commercial tools makes mass generation of new malicious code campaigns and exploits easier. The net result has been significant growth in volume of malware and infections.

And for 2012, I anticipate growing sophistication in web-borne attacks, even broader use of mobile and smart devices, and rapid adoption of cloud computing bringing new security challenges.

The web will undoubtedly continue to be the most prominent vector of attack. Cybercriminals tend to focus where the weak spots are and use a technique until it becomes far less effective. We saw this with spam email, which is still present but less popular with cybercriminals as people deploy highly effective gateways. The web remains the dominant source of distribution for malware—in particular malware using social engineering, or targeting the browser and associated applications with exploits. Social media platforms and similar web applications have become hugely popular with the bad guys, a trend that is only set to continue.

The rapid inflow of consumer-owned smartphones and tablets is causing significant security challenges for many organizations. IT departments are being asked to connect devices to corporate networks and secure data on these devices, which they have very little control over. Due to the high degree of mobility, security requirements are plentiful, including enforcement of use policies, corporate data encryption, access to corporate networks, productivity/content filtering, and of course malware protection. The unique nature of modern form factors (in terms of processing power, memory, battery life) requires rethinking of security and defense mechanisms.

Cloud computing is one of the most significant revolutions in delivering software applications to users, and can significantly improve the effectiveness and manageability of security solutions—web security, data protection, or even endpoint and mobile security managed via the cloud are great examples. The service model takes the burden of managing applications away from the user, but introduces new issues of security and privacy for data at rest and in transit.

Protecting data in a world where systems are changing rapidly and information flows freely introduces a whole new set of people, process and technology challenges, reinforced by enhanced scrutiny by compliance and regulatory bodies. As we all radically reform the way we communicate and share data, we can expect cybercriminals to hook themselves into these systems to tout their nasty malicious code.

With this edition of the Sophos Security Threat Report, we want to share our latest research on hacktivism, online threats, mobile malware, cloud computing, and social network security. And we offer a look ahead to the coming year.

Best wishes,



**Gerhard Eschelbeck** CTO, Sophos

# 2011 in review: Hype about hacktivism

The year 2011 was characterized by major data breaches and targeted attacks on high-profile companies and agencies. Cybercriminals diversified their targets to include new platforms, as business use of mobile devices accelerated. And we saw a number of politically motivated “hacktivist” groups take the media spotlight, even as the more common threats to our cyber security grew.

Security experts and the media liked talking about hacktivist groups Lulz Security (LulzSec) and Anonymous as they sowed chaos by leaking documents and attacking websites. And we watched with interest and concern as targeted attacks hit high-profile organizations like RSA and defense contractors.

Cybercriminals are becoming more professionalized through the availability of commercial crimeware kits like the increasingly popular Blackhole kit. The result is mass generation of new malicious code and exploits, and a significant increase in the volume of malware. In the coming year, businesses will be challenged to manage these threats alongside new ways of accessing applications and data, like mobile and cloud services.



Even as we witnessed governments and organizations placing a heavy focus on the importance of cyber security, the volume of malware attacks and compromised websites steadily grew. In the second half of the year we saw an average of approximately 30,000 new malicious URLs every day, an increase of more than 50% since our mid-year 2011 report.

Meanwhile, traditional threats demonstrated how basics like good password management and patching are still a significant challenge to IT security. Infections from hacked legitimate websites and drive-by downloads, brought about by a failure to patch vulnerabilities in applications or the browser, remained common and costly to businesses.

In 2012 we'll need to be ready for attacks on new platforms and devices—all the places we use data for work and our personal lives. We'll need to upgrade our security tools to solve more of these problems. But before we can face the threats of tomorrow we have to learn the lessons of our past mistakes. We can't afford to forget the security basics.



# Under attack

For many years cybercriminals have been motivated by the promise of financial gain. But in 2011, the emergence of LulzSec and Anonymous marked a shift from hacking for money to hacking as a form of protest or to prove a point.

## Hacktivism takes center stage

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

Hacktivist group LulzSec dominated headlines in the first half of the year with attacks on Sony, PBS, the U.S. Senate, the CIA, FBI affiliate InfraGard and others, and then disbanded after 50 days.<sup>1</sup> Anonymous, a loosely-affiliated international hacking group, claims that its tactics initiate civil disobedience. Recently, Anonymous has been suspected of taking down sites in El Salvador, Israel and the city of Toronto through distributed denial-of-service attacks. Hackers affiliated with the group also released 90,000 email addresses of U.S. military personnel in an attack on Booz Allen Hamilton.

In December Anonymous shut down the Florida Family Association (FFA) website in response to the FFA's opposition to a new

television show called *All-American Muslim* and requests to advertisers to pull support from the show. Anonymous reportedly defaced the FFA homepage with a message stating the site "destroys free speech." The hackers also exposed the email and IP addresses of more than 30 FFA newsletter subscribers and donors and listed credit card information for a dozen more.<sup>2</sup>

The variety of targets seems to show that almost any institution could be at risk, although only a tiny minority is affected by hacktivist attacks. Significantly, law enforcement organizations have made a series of arrests of members of both LulzSec and Anonymous.

In June, New Scotland Yard arrested a 19-year-old suspected LulzSec member in Essex, UK. Law enforcement in the UK and U.S. have arrested several other suspects. Turkish police detained 32 alleged members of Anonymous in June. And in July dozens more people were investigated for Anonymous connections in Italy and Switzerland.

## Protection strategies for hacktivism

Encryption is the best way to protect against hackers and unauthorized access of sensitive data.

## Data theft and loss

Data breaches are constantly in the news—in fact, since 2005 security breaches have compromised more than 500 million U.S. records alone.<sup>3</sup> Plus, lost data due to human error or negligence is just as much of a threat.

Risks arise when personal information is leaked, improperly discarded or gets into the wrong hands. Data can leave your network and your control in many ways, including through unprotected servers, desktop computers, laptops, mobile devices and email messages. And cybercriminals may use malware to get onto your network to destroy or steal your company's valuable information.

Identity theft, and consequently credit card theft, has major financial and reputation consequences for both the individual whose identity is stolen and the company from which the data was obtained. Organizations need to be vigilant about the way they handle, use and safeguard personal information to minimize their risks.

The Ponemon Institute's most recent U.S. Cost of a Data Breach report shows that costs continue to rise. In 2010, the costs of a data breach reached \$214 per compromised record and averaged \$7.2 million per data breach event.<sup>4</sup> This includes direct costs of a data breach—such as notification and legal defense costs—but also indirect costs like loss of trust and lost customer business.

---

### Learn more about data loss

 [The State of Data Security](#)

 [2011 Gartner Magic Quadrant for Mobile Data Protection](#)

## Conficker remains widespread despite patch

More than three years after its initial release, the Conficker worm is still the most commonly encountered piece of malicious software, representing 14.8% of all infection attempts seen by Sophos customers in the last six months. Evidently, plenty of infected PCs are still trying to spread this old worm.

Conficker began to spread to millions of unpatched PCs in 2008. It's estimated that at its peak Conficker infected more than 11 million PCs globally. By the end of 2011, Conficker was still the largest network threat in the world.<sup>5</sup> Last year Conficker dominated the cloud lookups from Sophos customers with more than 4 million queries from more than 1 million unique computers.

Security patching is still an important strategy for preventing infection. Although Microsoft patched this flaw more than three years ago, the current rate of Conficker infection is a shining example of how bad many of us are at patching our systems.

With a consistent security patching strategy, most people are well-protected against Conficker. However, the constant noise of Conficker rebounding off network defenses can hide some of the quieter and more targeted threats.

### Protection strategies for malware

To reduce risk of malware infection, screen web use on your network with quality protection technologies that can detect malware on hacked sites and respond quickly to emerging malware domains and URLs.

### Learn more about malware

 [Eight Threats Your Antivirus Won't Stop](#)

### Free Conficker Removal Tool

 [Download now](#)

## Malware

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It can include viruses, worms, spyware, adware and Trojans.

With some types of malware, you may not even know you're infected. Many web malware attacks are designed to steal personal information and passwords or use your machine for distributing spam, more malware or inappropriate content without your knowledge. We've highlighted some of the significant malware issues of 2011.

To counter the malware threat, Sophos uses proactive detection technologies. In the last six months of 2011, 80% of the unique malware seen by our customers (over 5.5 million different files) was detected by just 93 proactive detections. Proactive detections are designed to detect not just the millions of existing malware, but future malware before it's even been created. It's better to be proactive than reactive, responding to threats individually as they emerge.

## The fall of fake antivirus

Fake antivirus software is still one of the more common types of malware, although that began to change in 2011. This malware pretends to find dangerous security threats such as viruses on your computer. The initial scan is free, but if you want to clean up the fraudulently-reported threats, you need to pay. The fake antivirus warnings scare the victim into purchasing the junk software that will supposedly fix the problem.

Interestingly, six months ago fake antivirus software was everywhere. It was by far the most visible threat on PCs and was moving into the Mac arena. Since then, we've seen a sharp decline in fake antivirus creation by cybercriminals.

Although it's difficult to pinpoint the exact cause of the decline, international law enforcement cooperation is having an effect. In June of 2011, the FBI busted a cybergang that tricked nearly a million people into buying its fraudulent software. The fake antivirus software ranged from \$49.95 to \$129 apiece, and the scam netted more than \$72 million.<sup>6</sup>

Just a day later, Russian authorities arrested Pavel Vrublevsky, co-founder of a Russian company called ChronoPay, the country's largest processor of online payments.<sup>7</sup> It turns out that ChronoPay also processed the credit card payments and handled customer calls for the fake antivirus scammers.

Despite the recent fall-off, fake antivirus is still a big problem, responsible for 5.5% of infections in the last six months of 2011.

## Targeted and stealth attacks are not just for defense contractors

In 2011, companies such as Mitsubishi Heavy Industries, Lockheed Martin, L-3 Communications and Northrup Grumman were all hit by targeted cyberattacks. Experts speculate that these organizations may have been hacked to gain classified information on weapons systems.<sup>8</sup>

While attacks against governments or defense companies grab news headlines, these same types of attacks also affect ordinary businesses. Motives include financial gain as well as cyber espionage to uncover important corporate secrets. In addition, exploits used in a targeted attack may find their way into exploit packs that are sold in the cybercrime underground.

These attacks often leverage social engineering, such as making an email appear to come from a friend or colleague, to entice a user to open an email. With a targeted delivery mechanism, hackers can use malicious documents to exploit security flaws and install malware.

### Learn more about fake antivirus

 [Stopping Fake Antivirus: How to Keep Scareware Off Your Network](#)

 [Mark Harris of SophosLabs explains fake antivirus](#)

## Under attack

For example, PDF files or images embedded in the HTML code can compromise the browser extensions that handle them. If the objects themselves are malicious, examination of the HTML code will not reveal anything other than the presence of the object. Without attack signatures from the plugin vendors, it may be difficult to identify malicious components. In this case we recommend that you question all tags related to object embedding to make sure that they are legitimate.

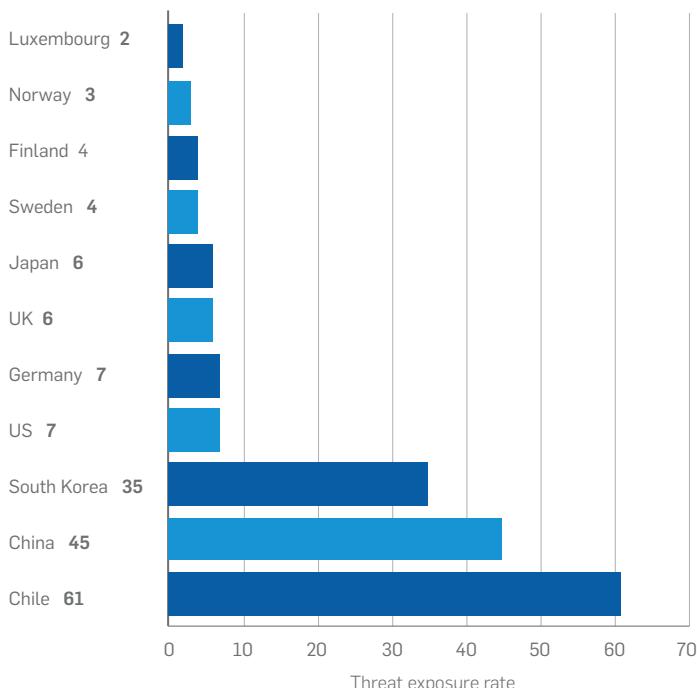
Stealth tactics such as the TDL family of rootkits are also becoming increasingly common. A rootkit hides the presence of other items of malware and may also hide itself. Recent versions of TDL are particularly sneaky—they don't need any files on your C drive. They store their files in a secret, encrypted partition at the end of your hard disk, launching before Windows itself.

According to data from SophosLabs, the average number of infected computers on a network compromised by the Conficker worm is 32.8. A more stealthy threat such as the TDL rootkit affects an average of 1.7 computers. When a piece of malware infects only a few PCs on a network, it's harder to find and clean up, giving it a longer lifespan.

## Botnet takedowns momentarily knock out spam

On March 16, 2011 a coordinated effort known as Operation b107 between Microsoft, FireEye, U.S. federal law enforcement agents and the University of Washington knocked Rustock offline. The highest volume botnet with a spam capacity of 30 billion spam messages a day, Rustock was best known for its Pharmacy Express emails touting Viagra and other pharmaceuticals. The result of the Rustock shutdown was an immediate drop of about 30% in global spam volumes, which decreased even further in the summer of 2011.<sup>9</sup>

Relative risk of running computer networks around the world



Threat exposure rate (TER): Measured as the percentage of PCs that experienced a malware attack, whether successful or failed, over a three month period.

The safest countries were Luxembourg with a TER of just 2, closely followed by Norway at 3 and Finland and Sweden both with a TER of 4. At the other end of the scale lies Chile with a TER of 61. Other notable scores: Japan 6, UK 6, U.S. 7, Germany 7, South Korea 35, China 45.

Source: SophosLabs, Q3 2011 data

Unfortunately, when one threat is diminished, others rise to take its place. SophosLabs has seen an increase in the volume of spam with attached malware. This started shortly after the Rustock takedown, with even higher spikes during August and September of 2011.

Spearphishing attacks are also on the rise. Over the past year, SophosLabs has noticed an increase in the number of targeted attacks attempting to phish users for credentials, as well as to push malware. Spearphishing uses customization methods to make the email seem legitimate—whether it appears to come from a

colleague or contain some personal information that pertains to a user's job or company. This results in higher user open and conversion rates, making spearphishing more successful for cybercriminals.

With spearphishing, the average theft per victim can be 40 times that of a mass attack, according to Cisco. It's estimated that the total cybercriminal benefit resulting from spearphishing attacks in 2011 amounted to \$150 million, a figure that tripled from \$50 million in 2010.<sup>10</sup>

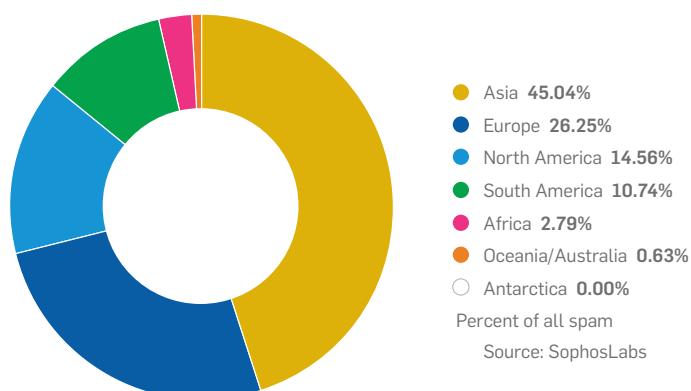
## Origins of spam

The very first email spam message was sent in May of 1978. It was a mass email sent by a DEC marketer to 600 ARPANET users advertising a new DEC computer and operating system with ARPANET support. Modern day spam is often more than just a nuisance. Spam may trick people into buying non-existent products or spread computer viruses, Trojans and other malicious software. The vast majority of today's email spam is sent by botnets, networks of compromised computers connected to the Internet.

## Spam dirty dozen countries

1. United States	<b>11.43%</b>	7. Vietnam	<b>3.07%</b>
2. India	<b>8.02%</b>	8. Indonesia	<b>2.88%</b>
3. Korea, Republic of	<b>7.94%</b>	9. Taiwan	<b>2.85%</b>
4. Russian Federation	<b>7.52%</b>	10. Ukraine	<b>2.82%</b>
5. Brazil	<b>5.62%</b>	11. Romania	<b>2.64%</b>
6. Italy	<b>3.37%</b>	12. France	<b>2.25%</b>

Spam sources by continent



## Protection strategies for phishing and spam

Anti-spam software is a must for capturing non-targeted spam. Spearphishing is much harder to detect. It helps to limit what personal information you share online, such as on social networks.

# Online threats

Cybercriminals constantly launch attacks designed to penetrate your digital defenses and steal sensitive data. And almost no online portal is immune to threat or harm.

According to SophosLabs more than 30,000 websites are infected every day and 80% of those infected sites are legitimate. Eighty-five percent of all malware, including viruses, worms, spyware, adware and Trojans, comes from the web.<sup>11</sup> Today, drive-by downloads have become the top web threat. And in 2011, we saw one drive-by malware rise to number one, known as Blackhole.

---

Learn more about  
web protection

 Endpoint Buyers Guide

## Today's landscape for web threats

Here are just a few of the techniques cybercriminals commonly use to distribute malware on the web:



**Blackhat search engine optimization (SEO)** ranks malware pages highly in search results.



**Social engineered click-jacking** tricks users into clicking on innocent-looking webpages.



**Spearphishing sites** mimic legitimate institutions, such as banks, in an attempt to steal account login credentials.



**Malvertising** embeds malware in ad networks that display across hundreds of legitimate, high-traffic sites.



**Compromised legitimate websites** host embedded malware that spreads to unsuspecting visitors.



**Drive-by downloads** exploit flaws in browser software to install malware just by visiting a webpage.

Malicious code typically installs spyware or malware by exploiting known vulnerabilities in your browser or associated plugins. These malware threats include:



**Fake antivirus** to extort money from the victim.



**Keyloggers** to capture personal information and account passwords for identity or financial theft.



**Botnet software** to subvert the system into silently joining a network that distributes spam, hosts illegal content or serves malware.

## Anatomy of an attack: Drive-by downloads and Blackhole

Drive-by downloads are nothing new—they've been around for a number of years. These attacks exploit multiple unpatched vulnerabilities in the user's browser, browser plugin, application or operating system. Hackers can either lure users to malicious sites they have injected with malicious code or hack legitimate sites to host the malware. Because legitimate sites are generally trusted and may be popular, high-traffic venues, they can be very successful for distributing malware to unsuspecting visitors through the browser.

The most popular drive-by malware we've seen recently is called Blackhole. It's marketed and sold to cybercriminals in a typical professional crimeware kit that provides web administration capabilities. Blackhole offers sophisticated techniques to generate malicious code. And it's very aggressive in its use of server-side polymorphism and heavily obfuscated scripts to evade antivirus detection. The end result is that Blackhole is particularly insidious.

### How Blackhole works

Blackhole mainly spreads malware through compromised websites that redirect to an exploit site, although we've also seen cybercriminals use spam to redirect users to these sites. This year we've seen numerous waves of attacks against thousands of legitimate sites.

We've also noticed cybercriminals abusing a number of free hosting sites to set up new sites specifically to host Blackhole.

Just like the Blackhole kit itself, the code injected into the legitimate sites is heavily obfuscated and polymorphic, making it harder to detect. The typical payloads we see from Blackhole exploit sites include:

- Bot-type malware such as Zbot (aka Zeus)
- Rootkit droppers (for example TDL and ZeroAccess)
- Fake antivirus

Typically, the malware on these sites target Java, Flash and PDF vulnerabilities. At SophosLabs we saw a continual bombardment of new PDF, Flash, Java and JavaScript components each day for several months at the end of 2011. We've seen a huge rise in the volume of malicious Java files, virtually all of it from exploit sites such as Blackhole.

The dark genius of crimeware kits like Blackhole is that they continuously update as new vulnerabilities are discovered. However, many computers will continue to be infected by older Java vulnerabilities because they aren't up to date with the latest patches. The system for patching plugins and third party applications like Java is not nearly as mature as that of Microsoft's monthly Patch Tuesday process.

---

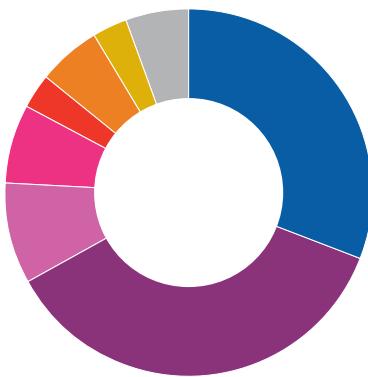
### Learn more about web threats

 Principal Researcher  
Fraser Howard explains  
web vulnerabilities

### Stat snapshot: How web threats spread

In 2011 we saw some major changes in the way malware spreads on the web. While fake antivirus is on the decline (5.5% of detections in the past six months), drive-by downloads from exploit sites like Blackhole are on the rise. About 10% of detections are exploit sites, about two-thirds of which are Blackhole sites. In the second half of the year, 67% of detections were redirections on compromised legitimate sites. Of these, approximately half are believed to be redirections to Blackhole exploit sites.

#### How web threats spread



- Drive-by redirect (Blackhole) 31%
- Drive-by redirect (not Blackhole) 36%
- Payload (not fake antivirus) 9%
- Exploit site (Blackhole) 7%
- Exploit site (not Blackhole) 3%
- Fake antivirus 5.5%
- Search engine poisoning 3%
- Other 5.5%

Percent of malware detections (July-Dec. 2011)

Source: SophosLabs

### Protection strategies for Blackhole

By tracking Blackhole detections with data from customers and partners, we have good visibility into where the exploit sites are hosted. We continually track, monitor and blacklist new sites. But because everything is continually moving—the code is polymorphic, and the exploit sites move to new URLs—it's important to have layers of protection.

We not only detect the malware payload, but provide detection for Blackhole exploit sites at all possible levels:

- JavaScript used in the core exploit site page (Mal/ExpJS-N)
- Java exploit components (various detections)
- Flash exploit components (Troj/SWFExp-AI)
- PDF exploit components (Troj/PDFEX-ET)

### Learn more about web protection

 [2012 Buyers Guide to Web Protection](#)

### Try our Sophos Virtual Web Appliance

 [Get a free trial](#)



## Protecting against network threats: Secure gateways

We see network gateways coming into greater use in the areas of education and healthcare, among many organizations that need to establish secure connections between their headquarters, branch locations and data centers.

As young people come to communicate more through sites like Facebook, Twitter and other online social networks, striking the right balance between acceptable and unacceptable use in schools is a challenge for school administrators.

Technologies designed for network security can help schools provide only appropriate access to these sites. With gateway technology, schools can block student access to social networking sites on campus, while allowing faculty and staff to use these tools. Or schools can limit student access to these sites to acceptable times of day, such as before or after school hours. Since social networking sites can also host malicious content, content filtering technologies can block access to malicious URLs.

Technology is rapidly changing the delivery of healthcare. Deploying IT for telehealth services allows organizations to support long-distance clinical healthcare, patient and professional health-related education, public health and health administration.<sup>12</sup> These efficient services link doctors to patients, improve access and lower costs. Doctors "visit" patients remotely and specialists consult with local healthcare workers to answer their questions about their patients' conditions.

However, HIPAA and other patient privacy regulations make secure connections a requirement. Secure telehealth is changing the face of healthcare for underserved and rural communities. Gateway technology keeps remote connections secure, guaranteeing safe access to patients and physicians in remote locations.

---

[Learn more about network security](#)

 [Simplifying Branch Office Security](#)

[Try our Astaro Secure Gateway](#)

 [Get a free trial](#)

---

## Protection strategies for networks

Simple, unified threat management protection with a secure gateway offers complete network security, including firewall and intrusion prevention with centralized control. It eliminates the complexity of deploying and managing a variety of point solutions to secure your network.

# Systems and software threats

Microsoft Windows has traditionally been the major target for hackers. As a result, today's operating systems are more securely coded and systematically patched than the applications that run on them. Hackers are becoming less interested in exploiting vulnerabilities in operating systems and are focusing on applications.

## Operating systems: The rise of Mac malware

In 2011, the emergence of malware for the Mac upstaged Windows malware. There's no doubt that the Windows malware problem is much larger than the Mac threat, but the events of 2011 show Mac users that the malware threat is genuine. Fake antivirus schemes such as MacDefender, Mac Security, MacProtector and MacGuard all came to light this year, and we're seeing scammers use techniques such as fake antivirus and SEO poisoning to infect Macs, as they've been doing for years with Windows.

Apple's Mac OS X 10.7, called Lion, claims to protect you against malware. However, it currently only detects a limited number of specific malicious downloads from about 10 different types of Mac malware. We recommend you run additional Mac antivirus protection as well.

---

Learn more about  
operating systems  
 [Three Simple Steps to Better Patch Security](#)

---

## Protection strategies for operating systems

The simplest way to reduce malware infection is to apply patches in a timely manner to fix newly discovered vulnerabilities. Check out our [endpoint security products](#) and [antivirus protection for Windows](#) to protect your company. You can also download our free [Anti-Virus for Mac Home Edition](#).

### Mac malware 1982-2011

<b>1982</b>	Prehistory: Elk Cloner	<b>2004</b>	Renepo and Amphimix
<b>1987</b>	nVIR	<b>2006</b>	Leap, the first virus for Mac OS X
<b>1988</b>	HyperCard	<b>2007</b>	OpenOffice BadBunny and RSPlug financial malware
<b>1990</b>	MDEF	<b>2008</b>	Fake antivirus, backdoors and Jahlav
<b>1991</b>	German folk tunes	<b>2009</b>	Apple releases rudimentary virus protection
<b>1995</b>	Word macro viruses	<b>2010</b>	Backdoors, cross-platform attacks and free antivirus
<b>1996</b>	Laroux viruses for Excel	<b>2011</b>	MacDefender fake antivirus and SEO poisoning
<b>1996</b>	AutoStart 9805 and Sevendust		

Source: NakedSecurity.sophos.com

## Software patching: More than Microsoft

Windows may be the most attacked OS, but the primary vectors for hacking Windows have been through PDF or Flash.<sup>13</sup> Despite Microsoft's regular updates to patch Windows OS vulnerabilities, the content delivery systems remain the largest vulnerability on any OS.

Security researchers identify software vulnerabilities all the time. Unfortunately, software companies often have to play catch-up with the cybercriminals to counter zero-day attacks on previously unknown vulnerabilities. And while hackers often target Microsoft Office and Internet Explorer because of their widespread use, other commonly used software including Adobe and Mac programs are frequent targets.

To counter these threats, Adobe has adopted Microsoft's Patch Tuesday schedule to provide more frequent security updates. In early December, Adobe warned users of a new zero-day vulnerability being exploited in its Adobe Reader software. As of

December 2011 the company was working on fixing a flaw in Adobe Reader 9 for the release of Reader X in January 2012.

Experts in the security field have long urged software developers and vendors to integrate security into the development lifecycle. This includes scanning for common coding errors from the very start of development, rather than checking for potential security issues just before going to market. The U.S. National Institute of Standards and Technology recently expanded its database of software flaws to help developers avoid introducing bugs into their code.

Unfortunately, basic vulnerabilities such as SQL injection and cross-site scripting still account for a majority of security flaws in web applications. By exploiting these types of flaws, hacktivists operating under the Anonymous banner compromised several high-profile sites in 2011.<sup>14</sup>

## Learn more about software threats

 [Using Application Control to Reduce Risk](#)

## Protection strategies for software

The best protection is to keep software updates turned on, 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 plugins means lower risk.

To keep abreast of the latest vulnerabilities, read and review vendor sites and visit our [Threat Center](#) for information on the latest malware threats.



### Removable media: Preventable data loss

Removable media, such as USB flash drives (also known as USB keys, memory sticks or thumb drives) and CDs/DVDs, are so common we may not think of them as harboring security threats. Yet we've seen a number of significant data breaches this year caused by lost or stolen thumb drives carrying unencrypted information.

In a research experiment, our Sophos Australia office discovered a shocking lack of security precautions by users of USB flash drives. We purchased 50 USB flash drives from a lost property auction run by the transit authority in Sydney and discovered that 66% of the drives were infected with malware. And we uncovered information about many of the former owners of the devices, as well as their family, friends and colleagues. None of the owners had encrypted the drives to secure their files against unauthorized snoopers.

Fortunately, Microsoft effectively put an end to exploits of the Windows Autorun feature for removable media with an update in February 2011. Autorun is the technology that makes a program start automatically when you insert a CD or USB drive into your Windows PC. A large amount of malware, including the notorious Conficker worm, exploited the Autorun feature to infect computers via USB drives. As of May 2011, Microsoft reported 1.3 million fewer autorun infections on Windows Vista and XP—a drop of 68% as compared with 2010.<sup>15</sup>

### Protection strategies for removable media

Computer users should encrypt all personal and business data before storing it on USB drives, so it can't be accessed if devices are lost. Companies may also want to restrict how and where these devices are used. For instance, you may want to prohibit employees from using removable media devices that they bring in from home. Also, make sure your company scans corporate removable media devices for malware and sensitive data.

### 6 tips to mitigate risk of data loss

1. Keep your computer up to date with the latest security patches, not just Microsoft but Adobe, Firefox, etc.
2. Delete email with suspicious-looking content or attachments immediately. View email as plain text and disable JavaScript, Flash and preview features.
3. Manage your downloads folder at the end of each session. Delete what you don't need to keep and save the rest somewhere that makes sense on your computer.
4. Keep Flash, Java and JavaScript disabled in your web browser and PDF viewer, except for sites or documents that really need it.
5. Use security software that is up to date and that includes not just antivirus and firewall protection, but HIPS and web services too. And if your computer slows down as a result, don't turn off active scanning; instead, try different security software.
6. Purge your email and web browser caches from time to time. Some email programs give you the option to "rebuild archive" or "update database," to purge caches. Web browsers allow you to purge caches manually, or automatically when you exit the browser.

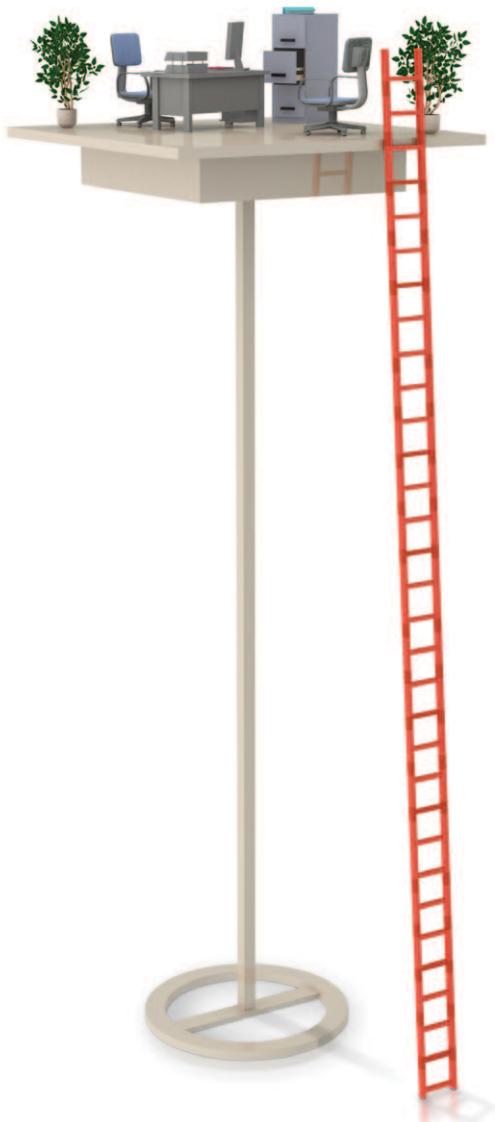
# Risk in the way we work

Increasingly, corporate users aren't just at home or at work, but somewhere else on the "everywhere network." And the consumerization of IT, sometimes called "bring your own device" or BYOD, is one of the newer causes of data vulnerability. Employees are accessing sensitive corporate information from their home computers, smartphones and tablets. Moreover, corporate-issued mobile devices increase risk, as does the rise of cloud services and the use of social media.

## Consumerization of IT

The market for smartphones and tablets continued to accelerate in 2011. According to market analyst International Data Corporation, tablet shipments rose more than 300% year-over-year in the second quarter of 2011 to 13.6 million units worldwide. Gartner reports that by 2016 at least 50% of enterprise email users will rely primarily on a browser, tablet or mobile client instead of a desktop client.<sup>16</sup>

Business expectations are also changing. Many companies now embrace these technologies when only a few years ago they blocked social media sites and non-standard unmanaged devices. These changes in technology and business expectations warrant a new proactive approach to information security.



### Mobile malware

The incentive to attack mobile devices is growing along with our increasing reliance on these devices for banking and other transactions. And mobile applications and text messaging open devices up to attack.<sup>17</sup> We've seen mobile malware disguised as fake online banking applications to steal customer credentials, intercept banking authentication token code via short message service (SMS), and drain bank accounts. According to the Conficker Working Group, smartphone viruses are still fairly rare, but text-messaging attacks are becoming more common.

Some malicious apps automatically send text messages to premium phone numbers, racking up unauthorized charges. SMS toll fraud apps in the last few months have primarily targeted users in Europe. SMS scams are still more common outside the United States where it is easier to rent and set up premium rate numbers.<sup>18</sup>

Google removed more than 100 malicious apps from the Android Market in 2011, as hackers took advantage of the openness of the market. In December 2011, criminals published malicious apps offering free cloned copies of popular games such as Need for Speed and Angry Birds. Although Google removed the malicious apps after only a day on the market, users had already downloaded the apps at least 10,000 times.

Although users have become accustomed to better security practices when using their PCs, many aren't as cautious when using a mobile device. We suspect that this is because most users have experienced scams or malware on their PC, but not yet on their mobile device.

### Learn more about mobile security

 [Mobile Device Security: What's Coming Next?](#)

### Learn how to protect mobile devices

 [Mobile Security Toolkit](#)  
 [Director of Technology Strategy James Lyne explains mobile security](#)

### Protection strategies for mobile devices

Despite all the hype over hacking threats, basic security best practices can prevent most data loss—strong passwords, data encryption, patching and user education. Mobile device management solutions protect data everywhere and on any device. Your security solution should support a variety of mobile devices and operating systems and manage them from one web-based console. You can protect your data with a solution that can remotely locate, lock and wipe devices if they're lost or stolen.



## Mobile operating system security

It's hard to say which mobile operating system is the most secure. They all have improvements over the PC, but each has its own security flaws. And each vendor faces unique challenges for balancing security with usability, openness and functionality.

Research In Motion's (RIM) Blackberry is still the smartphone of choice for many enterprises because of greater security oversight by the manufacturer. RIM centrally controls all software and updates and has a very rigorous quality assurance process. Apple has similar security protocols with its central updating of the iOS operating system for iPhones, iPods and iPads, and tight controls on the manufacturing of iPhone handsets.

Apple also vets apps in its online app store according to some very strict rules. But Apple's scrutiny of the Apple App Store isn't perfect. We've seen some demonstrations of malicious apps through the app store that have raised questions about the rigorousness of Apple's vetting process. And various password/encryption attacks show that Apple's security isn't flawless.

Google Android is the most widespread mobile OS and its popularity is increasing, but security hasn't kept up. The openness of the platform and the availability of alternative markets for apps make Android-based devices more difficult to secure. As a result, Android has become the biggest target for malware attacks, surpassing Symbian.<sup>19</sup>

Microsoft's Windows Phone 7.5 offers somewhat better security than Android. Microsoft recently needledd Google with a campaign on Twitter, encouraging Android users to share stories with the hashtag

## Mobile security survey

520 participants

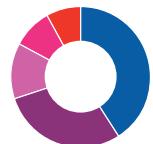
1. What phone OS does your company supply you with?

- None 29%
- Blackberry 26%
- iPhone 15%
- Android 14%
- Non-smartphone 9%
- Windows Mobile/Phone 7 7%



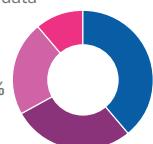
2. What phone OS do you wish your company supplied you with?

- Android 41%
- iPhone 29%
- Blackberry 13%
- Windows Mobile/Phone 7 9%
- I don't want a phone 8%



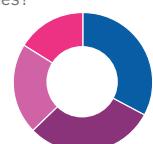
3. Would you be prepared to put up with additional security and management on your personal smartphone if you could access business data (e.g., your email, calendar, etc.)?

- Yes 39%
- Yes, but only if my company pays my monthly bill 28%
- No way—I like to keep it completely separate 22%
- I already have this feature 11%



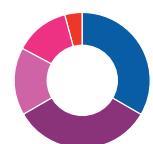
4. Do you have to enter a password to access your smartphones?

- No passwords on either phone 33%
- Yes on both my personal and company phones 30%
- Yes, on my personal phone 21%
- Yes, on my company phone 16%



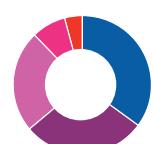
5. Which smartphone do you think offers the best security out of the box?

- Blackberry 33%
- Don't know 33%
- iPhone 16%
- Android 13%
- Windows Mobile/Phone 7 4%



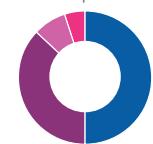
6. Which phone OS do you think will be most targeted by malware and hackers?

- iPhone 35%
- Android 29%
- Windows Mobile/Phone 7 24%
- Don't know 8%
- Blackberry 4%



7. Now be honest—have you ever misplaced or lost your business smartphone?

- No, I guard it with my life 50%
- I don't have a business smartphone 37%
- Yes, only once 8%
- Yes, several times 5%



Source: NakedSecurity.sophos.com

#droidrage about being hit with malware. However, Microsoft doesn't have as much security oversight as RIM or Apple. Although Microsoft has control over the distribution of updates for the platform, Windows Phones are manufactured by several device makers and have multiple carriers, opening potential security loopholes.

#### **Mobile data loss case study: Healthcare**

Mobile devices create risk for data loss because of their portability—they are easily lost or stolen. One field where data loss is increasingly costly is the healthcare industry.<sup>20</sup> Unfortunately, the widespread use of mobile devices puts patient data at risk.

Recent surveys by Manhattan Research found that more than 81% of physicians use a smartphone, up from 72% in 2010. At the same time, data breaches rose 32% in the past year, according to research released in December by the Ponemon Institute. Ponemon found that 96% of all healthcare organizations surveyed had experienced at least one data breach in the past two years.<sup>21</sup>

96% of healthcare organizations have experienced at least one data breach in the past two years.

## Cloud computing

Computation, software, data access and storage delivered as a service over the Internet—collectively known as cloud computing—creates scalability, flexibility and lower costs. But putting data in the cloud raises a unique set of security, compliance and privacy risks.

According to the Ernst & Young Global Information Security Survey, 61% of respondents would be using or evaluating cloud services within the next year. This will be a mix of public, private and hybrid cloud environments. However, 52% of organizations said they haven't implemented controls to mitigate data risk in the cloud. Our own informal poll of companies using cloud services found that only a few of them had cloud security policies in place.

Companies using cloud services need to ask questions about where their data is stored, who has access to it and whether it's stored on shared servers. You also need to assess cloud computing's impact on privacy; information security and data integrity; governance, risk management and assurance; and regulatory compliance.<sup>22</sup>

#### **Cloud insecurity**

Some well-publicized incidents in the past year emphasized that storing data in the cloud poses security and compliance risks. Added to the sense of cloud insecurity is the fact that companies and individuals may not know if their data is accessed under the banner of the U.S. law known as the Patriot Act. The law allows U.S. authorities to intercept and inspect any data housed, stored, or processed by a U.S. based or wholly owned company.<sup>23</sup>

---

### Learn more about cloud computing

 CTO Gerhard Eschelbeck explains cloud security

As a U.S. company, Microsoft admitted in June 2011 that it could be required to turn over data to U.S. authorities without informing customers, even in cases of data stored in the European Union. European companies and lawmakers have since raised concerns over this Patriot Act provision, given that the EU 1995 Data Protection Directive requires companies to notify customers when sharing their personal information. Microsoft's admission reportedly caused UK-based BAE Systems to pull out of a deal to store data with Microsoft's Office 365 cloud service, over fears defense secrets could end up in U.S. hands.<sup>24</sup>

#### Leaks from the cloud

While Anonymous and LulzSec dominated the data breach headlines in 2011, what became clear was that more and more organizations are collecting data about their customers and doing a poor job of protecting that information. Here are some of the biggest data breaches of 2011.

**Dropbox:** With 45 million users Dropbox is one of the more popular cloud file sharing services. But researchers discovered at least three different ways to hack into Dropbox and access data without authorization.<sup>25</sup> In June, a flawed update to the website left all user accounts open to access by anyone who typed in the email address associated with the account.<sup>26</sup>

**Epsilon:** A breach of the bulk email marketing company leaked millions of names and email addresses from the customer databases of some of its clients, including trusted brands like Best Buy, Marks & Spencer, Marriott Rewards, Walgreens and Chase Bank.<sup>27</sup>

**Sony:** Sony Corp.'s PlayStation Network and Sony Online Entertainment suffered a series of breaches that placed 100 million customer accounts at risk. It's been speculated that this is the most expensive data breach ever, costing the company up to \$2 billion.<sup>28</sup>

**Stratfor:** At year's end Stratfor, a subscription-based provider of geopolitical analysis, saw its servers breached by a group of individuals claiming to be affiliated with the hacktivist collective Anonymous. The stolen data included 75,000 credit card numbers and 860,000 user names and passwords, which the hackers then exposed online.<sup>29</sup>

#### Protection strategies for cloud computing

Always encrypt your data before storing it in the cloud. It's also important to select cloud services providers that are transparent about security measures, back-up and failover. Your standard security processes, such as access control and other data protection techniques, should include cloud services.



## Social networks

The explosive growth of social networks like Facebook, Twitter, LinkedIn and YouTube continued in 2011, and with it comes malware, spam and the continuing erosion in privacy. Employers are beginning to rethink bans and relax restrictions on employee access to social networks. And social media is now an integral part of the communication strategy for most corporations, leaving them susceptible to brand-damaging attacks from hacktivists and other cybercriminals.

### Relaxed restrictions and risk to brands

Social networking's growth has driven many companies to adopt social media strategies for marketing and corporate communications. Companies have Facebook pages, LinkedIn and YouTube profiles and Twitter accounts.

Companies are seeing the potential to tap new prospects via social networking, even in the highly regulated financial services industry. In a survey by Socialware, 84% of financial advisers said they use social networks for business purposes, up from 60% in 2010. The public sector, too, is lifting restrictions on access to social media. According to a Market Connections poll of federal, state and local government employees, just 19% said their agencies ban some or all social media websites, down from 55% in 2010.<sup>25</sup>

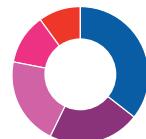
But social networking accounts can be hacked. In 2011, hackers compromised Microsoft's YouTube channel, defaced Pfizer's Facebook page, and replaced the content on Sesame Street's YouTube channel with hardcore pornographic movies.

## Social networking security survey

### 1. How often do you check Facebook at work?

- Never 36%
- Once a day 22%
- Once an hour 21%
- More than once an hour 12%
- Less than once a day 10%

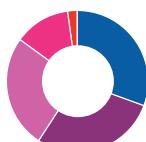
4,358 total count



### 2. Which social network do you consider to be the most secure?

- LinkedIn 31%
- Other 29%
- Facebook 26%
- Twitter 13%
- FourSquare 2%

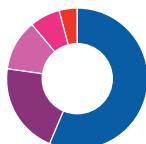
4,320 total count



### 3. Which social network do you consider to be the least secure?

- Facebook 57%
- Twitter 21%
- Other 12%
- FourSquare 7%
- LinkedIn 4%

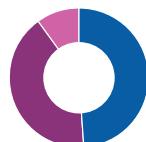
4,318 total count



### 4. Does your company allow you to use your personal laptop, desktop or phone for work?

- Yes 49%
- No 41%
- No, but I wish they did 10%

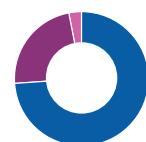
4,334 total count



### 5. Do you think using your own personal laptop or phone to access company resources

- Increases the risk of data loss 74%
- Doesn't affect data loss 23%
- Decreases the risk of data loss 3%

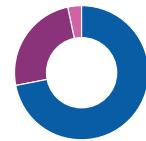
4,344 total count



### 6. Compared to last year, do you think the malware threat is

- On the rise 67%
- About the same 23%
- Less of an issue 3%

4,346 total count



Source: NakedSecurity.sophos.com

Hackers also took over the Twitter accounts of both *USA Today* and NBC News. In the NBC case, the hackers sent out fake tweets about an attack on Ground Zero on the anniversary weekend of 9/11. It appears that a spyware Trojan could have compromised the computer of NBC News' director of social media to steal passwords.

Sloppy password security is one reason brands are susceptible to hacking on social networks. Social networks themselves also need to be built with businesses in mind and offer a higher level of security for accounts which represent brand names. We're seeing some of these features in the Google Plus social network, which Google introduced in 2011. The network gained 25 million global unique visitors in less than a month, faster than any other social network in history.

Social networking is the most engaging online activity worldwide, accounting for one in every seven minutes spent on the web.<sup>30</sup>

### The erosion of privacy policies

People and businesses frequently share too much information and aren't doing enough to protect their accounts. It's important to remember that social networking sites like Facebook are in business to support advertising. This means they're more concerned with increasing users than putting sensible security defaults in place.

In 2011, Sophos published an [open letter to Facebook](#). It includes three steps we believe Facebook should take to better protect its users, including privacy by default, vetting of app developers and HTTPS for everything.

### Learn more about social networks

 Graham Cluley of [NakedSecurity.sophos.com](#) explains social networking threats

### Protection strategies for social networks

IT managers should educate their users about how to choose hard-to-crack passwords. If you're on Facebook, join over 150,000 people who like the [Sophos Facebook page](#), where we keep you updated on the latest scams and all the security news.



# Sophos Complete Security

We give you protection wherever you need it: computers, laptops, virtual desktops and servers, mobile devices, and your network, web and email gateway. Complete security means we don't just detect threats, we help you address every point in the security lifecycle.

- › **Reduce the attack surface:** We address the things that bring risk like vulnerabilities and applications.
- › **Protect everywhere:** We protect your users wherever they are and whatever devices they use.
- › **Stop attacks and breaches:** Detecting and preventing threats and data loss is our business. But we've moved beyond signatures with innovations like live protection, which means we can stop new threats instantly. And our mobile device management stops data loss from lost or stolen devices.
- › **Keep people working:** Both your users and the IT team are crucial to your company. We engineer our products to simplify the tasks that often take too much time, like cleaning up infections and recovering forgotten passwords.

We engineer our products to eliminate complexity. The result is you'll get advanced protection you can actually use. Security shouldn't get in the way, so we keep resource impact low. Plus, we work to make deployment, policy setting and clean-up easy.

Stopping threats and protecting your data is what we do. And we believe our job is to do that comprehensively, without making your job more complicated. This is our mantra. That's why we give you solutions for every part of your business.

## Learn more about complete security from Sophos

 Chester Wisniewski of NakedSecurity.sophos.com explains complete security

 The Four Rules of Complete Web Protection

### Endpoint



Our endpoint protection will keep data in and malware out, all within your antivirus budget.

### Encryption



We secure your confidential information and help you comply with regulations.

### Mobile



We help you easily protect, secure and manage your mobile devices and data.

### UTM



You get one appliance that eliminates the complexity of multiple point solutions.

### Network



Keep your network infrastructure safe with complete network security.

### Email



We encrypt your sensitive email, prevent data loss and block spam.

### Web



We make using the Internet safer and more productive.

# What's new in 2012: 10 trends

We're always looking to stay ahead of the threats. Here are 10 trends we think will be the main factors affecting the IT security landscape in 2012.

## 1. Social media and the web

We expect cybercriminals to continue their effective mass generation of malware, increasing the number of attacks using new social media platforms and integrated apps.

## 2. Security means more than Microsoft

Over the past 18 months the bad guys have increased attacks on platforms like Mac OS X and Adobe. We'll continue to see more targeted attacks on non-Windows platforms in 2012 and 2013.

## 3. Mobile devices in the spotlight

In 2011 we saw a greater volume of malicious attacks on key platforms such as Android. IT security professionals will need to deal with rapidly evolving mobile platforms, each with a unique set of risks.

## 4. New web and network technologies force us to learn some lessons

Web technologies are undergoing interesting changes, from HTML5 to IPv6. These new technologies introduce some impressive new capabilities, but they also introduce new attack vectors.

## 5. Casual consumerization causes backslicing

A casual shift to use of consumer devices without appropriate controls will cause backslicing in security capabilities. IT will once again struggle to deploy reliable security measures for the environment.

## 6. More hacktivism and targeted attacks

With rising awareness of cybercrime as a means of data theft, intelligence gathering, and political dirty tricks, it's likely we'll see more targeted attacks in 2012. These attacks will continue to be a priority issue for certain businesses and organizations.

## 7. Data regulations proliferate and penalties grow

New regulations and tougher penalties for data breaches will be major concerns for organizations. Proposed laws like the U.S. Stop Online Piracy Act (SOPA), and the European Union's Data Protection Directive, will have a major impact on data protection and privacy for businesses and private citizens alike.

## 8. Mobile payment technology may be new target

We're eagerly waiting for the widespread availability of convenient payment technologies like near field communication (NFC) in mobile devices. We expect cybercriminals are just as eager to target these integrated platforms that hold your life and your money.

## 9. Cloud services are back in vogue

Some companies were slow to adopt cloud services because of perceived insecurity. But many organizations are now starting to use these services. That means more focus on encrypting data wherever it flows, rather than just protecting the device or the network.

## 10. The basics still go wrong

Security basics like patching and password management will remain a significant challenge to IT security.

Keeping your devices healthy by identifying missing patches in areas commonly targeted by the bad guys will help significantly. Technologies like file and folder encryption will smooth the adoption of cloud services and new devices.

---

Try Sophos Endpoint Protection

 Get a free trial

# The last word

The big challenge for organizations in 2012 will be to keep security capabilities from backsliding as they adopt new technologies and as the cybercriminals expand their focus. As we continue to mobilize and access information in different ways and from different locations, security tools will need to keep up. But in our quest for security from the next threat, we can't forget what we learned from the last one. Cybercriminals will continue to stalk the easiest prey—those who don't follow the simple security measures we should have learned by now.



# Sources

1. Sophos Naked Security Blog, "The end of LulzSec?" by Graham Cluley, June 26, 2011
2. *Forbes*, "Hackers Take Down Anti-Muslim Website," by Janet Maragioglio, December 16, 2011
3. Privacy Rights Clearinghouse, "Chronology of Data Breaches"
4. Ponemon Institute, "Cost of a data breach climbs higher," Dr. Ponemon's blog
5. Sophos Naked Security Blog, "The Conficker worm, three years and counting," by Chester Wisniewski, November 24, 2011
6. Sophos Naked Security Blog, "FBI announces international cyberbusts: scareware peddlers and malvertisers taken down," by Paul Ducklin, June 23, 2011
7. Krebs on Security, "ChronoPay Co-Founder Arrested," by Brian Krebs, June 24, 2011
8. Sophos Naked Security Blog, "Hackers steal data on nuclear plants and fighter jets," by Graham Cluley, Oct. 25, 2011
9. Sophos Naked Security Blog, "One week later Rustock and Pharmacy Express still flat lined," by Brett Cove, March 24, 2011
10. Cisco, "Email Attacks: This Time It's Personal," June 2011
11. Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of US Companies," August 2011
12. HRSA, Health Resources and Services Administration, [Telehealth](#)
13. Channel Insider, "The Eight Riskiest Mobile Devices in Need of Protection," by Ericka Chickowski, October 24, 2011
14. eWeek Europe, "Common Coding Errors Added to NIST Database," by Fahmida Y. Rashid, November 29, 2011
15. cnet, "Microsoft declares a victory against autorun malware," by Lance Whitney, June 17, 2011
16. Sophos.com, "Sophos Releases Enhanced Mobile Device Management Platform," December 19, 2011
17. *Computerworld*, "Four rising threats from cybercriminals," by John Brandon, November 21, 2011
18. eWeek, "Google Removes Malicious Cloned Games from Android Market," by Fahmida Y. Rashid, December 13, 2011
19. Street Articles, "Is Mobile Internet Banking Safe?" by Taufan Surapati, August 26, 2011
20. amednews.com, "Smartphones blamed for increasing risk of health data breaches," by Pamela Lewis Dolany, December, 19, 2011
21. amednews.com, "Smartphones blamed for increasing risk of health data breaches," by Pamela Lewis Dolany, December, 19, 2011
22. CRN, "Cloud, Mobile, Social Creating Security Conundrums," by Andrew R. Hickey, November 2, 2011
23. ZDNet, "Microsoft admits Patriot Act can access EU-based cloud data," by Zach Whittaker, June 28, 2011
24. ZDNet, "Defense giant ditches Microsoft's cloud citing Patriot Act fears," by Zach Whittaker, December 7, 2011
25. FierceCIO Tech Watch, "Dropbox's multiple security problems," by Paul Mah, August 19, 2011
26. TUAW, "Dropbox security bug temporarily allowed logins without authentication," by Chris Rawson, June 20, 2011
27. Sophos Naked Security Blog, "Epsilon email address megaleak hands customers' customers to spammers," by Paul Ducklin, April 4, 2011
28. Sophos Naked Security Blog, "Sony admits breach larger than originally thought, 24.5 million SOE users also affected," by Chester Wisniewski, May 3, 2011
29. Sophos Naked Security Blog, "Data leaks at Stratfor and Care2 mark the end of a year riddled with data theft," by Chester Wisniewski, December 30, 2011
30. comScore, "It's a Social World," December 21, 2011

Copyright 2012 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 NakedSecurity.sophos.com. 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](mailto:sales@sophos.com)

North American Sales:  
Toll Free: 1-866-866-2802  
Email: [nasales@sophos.com](mailto:nasales@sophos.com)

Australia and New Zealand Sales:  
Tel: +61 2 9409 9100  
Email: [sales@sophos.com.au](mailto:sales@sophos.com.au)

Boston, USA | Oxford, UK  
© Copyright 2012. Sophos Ltd. All rights reserved.  
All trademarks are the property of their respective owners.

Sophos Security Threat Report 2012 1.12v1.dNA

**SOPHOS**