SOPHOS

Security Threat Report 2013

New Platforms and Changing Threats

Table of contents

Graphics

Videos

Adware

Adware is software that displays advertisements on your computer

Foreword

Reflecting on a very busy year for cyber security, I would like to highlight some key observations for 2012. No doubt, the increasing mobility of data in corporate environments is one of the biggest challenges we faced in the past year. Users are fully embracing the power to access data from anywhere. The rapid adoption of bring your own device (BYOD) and cloud are really accelerating this trend, and providing new vectors of attack.

Another trend we are seeing is the changing nature of the endpoint device, transforming organizations from a traditional homogeneous world of Windows systems to an environment of diverse platforms. Modern malware is effective at attacking new platforms and we are seeing rapid growth of malware targeting mobile devices. While malware for Android was just a lab example a few years ago, it has become a serious and growing threat.

BYOD is a rapidly evolving trend, and many of our customers and users actively embrace this trend. Employees are looking to use their smartphone, tablet, or next generation notebook to connect to corporate networks. That means IT departments are being asked to secure sensitive data on devices they have very little control over. BYOD can be a win-win for users and employers, but the security challenges are real while boundaries between business and private use are blurring. It raises questions on who owns, manages and secures devices and the data on them.

Finally, 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. For example, malware kits like Blackhole are a potent cocktail of a dozen or more exploits that target the tiniest security holes and take advantage of missing patches.

Cybercriminals tend to focus where the weak spots are and use a technique until it becomes less effective, and then move on to the next frontier. Security is at the heart of this revolution of BYOD and cloud. Protecting data in a world where systems are changing rapidly, and information flows freely, requires a coordinated ecosystem of security technologies at the endpoint, gateway, mobile devices and in the cloud.

IT security is evolving from a device-centric to a user-centric view, and the security requirements are many. A modern security strategy must focus on all the key components—enforcement of use policies, data encryption, secure access to corporate networks, productivity and content filtering, vulnerability and patch management, and of course threat and malware protection.

Best wishes,

Gerhard Eschelbeck CTO, Sophos

2012 in review: New platforms and changing threats

In 2012, we saw attackers extend their reach to more platforms, from social networks and cloud services to Android mobile devices. We saw them respond to new security research findings more rapidly, and leverage zero-day exploits more effectively.

In the past year the most sophisticated malware authors upped the stakes with new business models and software paradigms to build more dangerous and sustained attacks. For instance, the creators of Blackhole, an underground malware toolkit delivered through Software-as-a-Service rental arrangements (aka crime packs), announced a new version. They acknowledged the success of antivirus companies in thwarting their activities, and promised to raise their game in 2012.

Private cybercriminals were apparently joined by state-based actors and allies capable of delivering advanced attacks against strategic targets. We saw reports of malware attacks against energy sector infrastructure throughout the Middle East, major distributed denial-of-service attacks against global banks, and targeted spearphishing attacks against key facilities.

More conventionally, attackers continued to target thousands of badly-configured websites and databases to expose passwords and deliver malware—yet again demonstrating the need for increased vigilance in applying security updates and reducing attack surfaces. Meanwhile, a new generation of victims found themselves on the wrong end of payment demands from cybercriminals, as social engineering attacks such as fake antivirus and ransomware continued unabated.

In the wake of these growing risks, 2012 also saw good news. This year, IT organizations and other defenders increasingly recognized the importance of layered defenses. Many organizations began to address the security challenges of smartphones, tablets, and bring your own device (BYOD) programs. Enterprises moved to reduce their exposure to vulnerabilities in platforms such as Java and Flash; and to demand faster fixes from their platform and software suppliers.

Not least, law enforcement authorities achieved significant victories against malware networks—including the arrest of a Russian cybercriminal charged with infecting 4.5 million computers with the goal of compromising bank accounts; and the sentencing in Armenia of the individual responsible for the massive Bredolab botnet. Yet another good sign: Microsoft's aggressive lawsuit against a China-based Dynamic DNS service that enabled widespread cyber crime, including operation of the Nitol botnet[1]. The lawsuit's filing and settlement demonstrated those who facilitate cyber crime can be held as accountable as the criminals themselves.

In 2013, as computing increasingly shifts to virtualized cloud services and mobile platforms, attackers will follow, just as they always have. This means IT organizations and users will need to ask tough new questions of their IT service providers and partners; become more systematic about protecting diverse devices and network infrastructure; and become more agile about responding to new threats. We'll be there to help—every minute of every day.

Widening attacks related to Facebook and other social media platforms

Throughout 2012, hundreds of millions of users flocked to social networks—and so did attackers. They built creative new social engineering attacks based on key user concerns such as widespread skepticism about Facebook's new Timeline interface,[2] or users' natural worries about newly posted images of themselves. Attackers also moved beyond Facebook to attack maturing platforms such as Twitter, and fast-growing services such as the Pinterest social content sharing network.

In September 2012, Sophos reported the widespread delivery of Twitter direct messages (DMs) from newly-compromised accounts. Purportedly from online friends, these DMs claim you have been captured in a video that has just been posted on Facebook. If you click the link in the DM, you're taken to a website telling you to upgrade your "YouTube player" to view the video. If you go any further, you'll be infected with the Troj/Mdrop-EML backdoor Trojan.[3]

September also saw the first widespread account takeovers on Pinterest. These attacks spilled image spam onto other social networks such as Twitter and Facebook. Victimized users who had linked their Pinterest accounts to these networks found themselves blasting out tweets and wall posts encouraging their friends to participate in disreputable work-at-home schemes.[4]

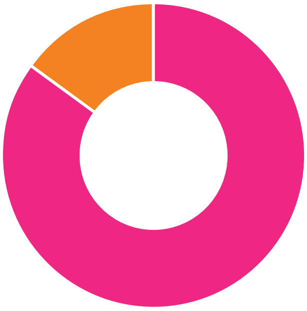
Learn more about attacks related to social media platforms

Four Data Threats in a Post-PC World

Beth Jones of SophosLabs explains social engineering

Naked Security Survey

Should businesses fool employees into opening inappropriate emails with the aim of education?



● Yes	85.21%
● No	14.79%

Based on 933 respondents voting

Source: Naked Security

With 1 billion users, Facebook remains the number one social network—and hence, the top target. In April, Sophos teamed with Facebook and other security vendors to help improve Facebook's resistance to malware. Facebook now draws on our massive, up-to-the-minute lists of malicious links and scam sites to reduce the risk that it will send its users into danger.[5] Of course, this is only one component of the solution. Researchers at Sophos and elsewhere are working to find new approaches to protecting users against social network attacks.

For example, Dark Reading reported that computer scientists at the University of California, Riverside have created an experimental Facebook app that is claimed to accurately identify 97% of social malware and scams in users' news feeds.[6] Innovations such as social authentication—in which Facebook shows you photos of your friends, and asks you to identify them, something that many hackers presumably can't do—may also prove helpful.[7]

Emerging risks to cloud services

In 2012, the financial and management advantages of cloud services attracted many IT organizations. In addition to expanding their reliance on hosted enterprise software and more informal services such as the Dropbox storage site, companies have also begun investing more heavily in private clouds built with virtualization technology. This move raises more questions about what cloud users can and should do to keep the organization secure and compliant.

Cloud security drew attention in 2012 with Dropbox's admission that usernames and passwords stolen from other websites had been used to sign into a small number of its accounts. A Dropbox employee had used the same password for all his accounts, including his work account with access to sensitive data. When that password was stolen elsewhere, the attacker discovered that it could be used against Dropbox. This was a powerful reminder that users should rely on different passwords for each secure site and service.

Dropbox is no stranger to cloud authentication problems, having accidentally removed all password protection from all its users' files in 2011 for nearly four hours.[8]

Also, VentureBeat reported that the company's iOS app was storing user login credentials in unencrypted text files—where they would be visible to anyone who had physical access to the phone.

Learn more about cloud services

Adopting Cloud Services With Persistent Encryption

Fixing Your Dropbox Problem

CTO Gerhard Eschelbeck explains cloud storage and BYOD

Dropbox has since improved security by introducing optional two-factor authentication,[9] but its problems raise broader issues. In May 2012, the Fraunhofer Institute for Secure Information Technology reported on vulnerabilities associated with registration, login, encryption, and shared data access on seven cloud storage sites.[10]

It's worth noting that Dropbox and some other sites already encrypt data in storage and transit, but this only protects data that has not been accessed using a legitimate user ID and password. Data stored on public cloud systems is subject to the surveillance and interception laws of any of the jurisdictions in which those cloud systems have servers.

Dropbox's difficulties have called greater attention to cloud security in general. With public cloud services and infrastructure beyond the control of the IT organization, how should companies approach security and compliance? Two-factor (or multi-factor) authentication is a must. But is it enough? Consider issues such as these:

- How will you manage "information leakage"? Specifically, how do you know if malicious insiders are forwarding sensitive information to themselves, where it will remain available even if they're fired?[11]

- How are you vetting suppliers and the administrators who operate their systems? Are you applying the same strict standards and contractual requirements you demand from other business-critical partners who see confidential or strategic data?[12]

- Can you prevent snapshotting of virtual servers that capture current operating memory images—including all working encryption keys? Some experts, such as Mel Beckman or System iNEWS, believe this rules the public cloud off-limits in environments where legal compliance requires physical control of hardware, e.g., HIPAA.[13]

It's a cloudy world, but when and if you decide to use cloud services, the following three steps can help you protect your data:

1. Apply web-based policies using URL filtering, controlling access to public cloud storage websites and preventing users from browsing to sites you've declared off-limits.

2. Use application controls to block or allow particular applications, either for the entire company or for specific groups.

3. Automatically encrypt files before they are uploaded to the cloud from any managed endpoint. An encryption solution allows users to choose their preferred cloud storage services, because the files are always encrypted and the keys are always your own. And because encryption takes place on the client before any data is synchronized, you have full control of the safety of your data. You won't have to worry if the security of your cloud storage provider is breached. Central keys give authorized users or groups access to files and keep these files encrypted for everyone else. Should your web key go missing for some reason—maybe the user simply forgot the password—the security officer inside the enterprise would have access to the keys in order to make sure the correct people have access to that file.

Blackhole: Today's malware market leader

Featuring research by SophosLabs

A close inspection of Blackhole reveals just how sophisticated malware authors have become. Blackhole is now the world's most popular and notorious malware exploit kit. It combines remarkable technical dexterity with a business model that could have come straight from a Harvard Business School MBA case study. And, barring a takedown by law enforcement, security vendors and IT organizations are likely to be battling it for years to come.

An exploit kit is a pre-packaged software tool that can be used on a malicious web server to sneak malware onto your computers without you realizing it. By identifying and making use of vulnerabilities (bugs or security holes) in software running on your computer, an exploit kit can automatically pull off what's called a drive-by install. This is where the content of a web page tricks software—such as your browser, PDF reader or other online content viewer—into downloading and running malware silently, without producing any of the warnings or dialogs you would usually expect. Like other exploit kits, Blackhole can be used to deliver a wide variety of payloads. Its authors profit by delivering payloads for others, and they have delivered everything from fake antivirus and ransomware to Zeus and the infamous TDSS and ZeroAccess rootkits. Blackhole can attack Windows, OS X, and Linux. It is an equal-opportunity victimizer.

Between October 2011 and March 2012, nearly 30% of the threats detected by SophosLabs either came from Blackhole directly, or were redirects to Blackhole kits from compromised legitimate sites. Blackhole is distinguished not only by its success, but by its Software-as-a-Service rental model, similar to much of today's cloud-based software. Weekly rental rates are specified (in Russian) right in the kit's accompanying read me file, along with surcharges for additional domain services. Like legitimate vendors of rental software, Blackhole's authors offer updates free for the life of the subscription.

Customers who want to run their own Blackhole servers can purchase longer licences. But the version of the Blackhole kit that these customers receive is extensively obfuscated. This is one of several steps that Blackhole's authors have taken to keep control over their product. We haven't yet seen Blackhole spin-offs from unrelated authors, though Blackhole has been aggressively updated, and other authors are borrowing its techniques.

Four stages of the Blackhole life cycle

1. Sending users to a Blackhole exploit site

The attackers hack into legitimate websites and add malicious content (usually snippets of JavaScript) that generate links to the pages on their Blackhole site. When unsuspecting users visit the legitimate site, their browsers also automatically pull down the exploit kit code from the Blackhole server.[14]

Blackhole host sites change quickly. Freshly registered domains are normally used to host Blackhole, typically acquired through the abuse of dynamic DNS services such as ddns., 1dumb.com, and dlinkddns.com. These hosts often disappear within one day. Blackhole's ability to consistently send traffic to the correct new hosts shows an impressive level of centralized control.

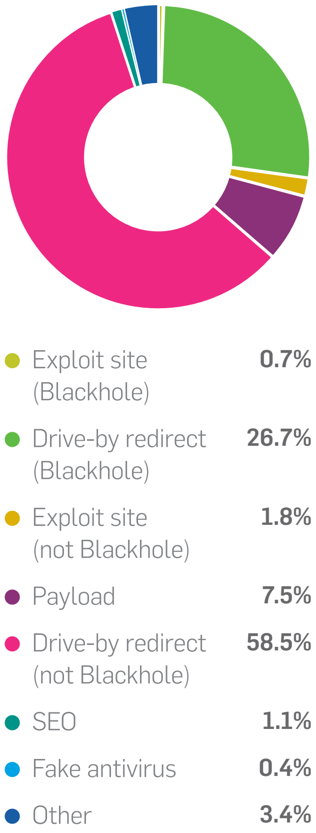
Blackhole has multiple strategies to control user traffic. We've recently seen its owners abuse affiliate schemes. Web hosts voluntarily add Blackhole code in exchange for a small payment, perhaps without realizing what the code will do. We've also seen Blackhole use old-fashioned spammed email links and attachments. For example, links that indicate problems with a bank account, or claim to provide a scanned document.

2. Loading infected code from the landing page

Once your browser sucks in the exploit kit content from the Blackhole server, the attack begins. The exploit code, usually JavaScript, first works out and records how your browser arrived at

Blackhole represents 27% of exploit sites and redirects

In 2012 more than 80% of the threats we saw were redirects, mostly from legitimate sites that have been hacked. A powerful warning to keep your site secure and your server scripts and applications up to date.



Source: SophosLabs

the Blackhole server. This identifies the affiliates who generate the traffic in the first place, so they can be paid just like affiliates in the legitimate economy. Then the exploit code fingerprints, or profiles, your browser to identify what operating system you are using, which browser version you have, and whether you have plugins installed for Flash, PDF files, Java applets and more.

While we've seen attacks based on many types of vulnerabilities, security holes in Java appear to be the leading cause of Blackhole infections. Here, again, Blackhole uses legitimate code wherever possible. For example, it loads its exploit code through the Java Open Business Engine, which has been used to support a wide variety of workflow applications and systems, including the U.S. president's daily Terrorist Threat Matrix report.[15]

3. Delivering the payload

Once a victim's system has been cracked, Blackhole can deliver the payload it's been directed to send. Payloads are typically polymorphic—they vary with each new system that's been infected. Blackhole's authors have been aggressive about using advanced server-side polymorphism and code obfuscation. Since they maintain tight central control, they can deploy updates with exceptional speed. Compared with other exploit kits that attackers purchase and host, we see rapid shifts in Blackhole's behavior and effectiveness. Blackhole payloads also typically use custom encryption tools designed to evade antivirus detection. Those tools are added by Blackhole's customers, and Blackhole contributes with an optional service that actively checks antivirus functionality on each system it attempts to attack.

4.Tracking, learning and improving

Blackhole keeps a record of which exploits worked with what combination of browser, operating system and plugins. This way, Blackhole's authors can measure which exploits are most effective against each combination of browser, plugin, and underlying operating system. This tracking technique isn't uncommon, but Blackhole's authors have been diligent in updating their kit to reflect what they discover.

Blackhole is equally good attaking advantage of new zero-day vulnerabilities. For example, in August 2012 it targeted a highly-publicized vulnerability in Microsoft Help and Support Center to deliver poisoned VBS scripts. Blackhole launched a new attack based on a dangerous new Java 7 vulnerability (CVE-2012-4681) that allows infected code to compromise Java's permission checking system.[16] Remarkably, 12 hours after a proof-of-concept for this Java attack went public, it was already included in Blackhole.[17] Oracle, in turn, delivered an emergency patch by the end of August, but many systems remain unpatched.

Given the level of sophistication and agility shown by Blackhole's authors, we have been surprised that they've left some portions of their kit essentially stagnant. For example, URL paths, filenames, and query string structure. SophosLabs expects this to change in the future, opening new opportunities for Blackhole's authors to improve their attacks.

Learn more about Blackhole

Malware B-Z: Inside the Threat From Blackhole to ZeroAccess

Mark Harris introduces SophosLabs

Fraser Howard of SophosLabs explains Blackhole

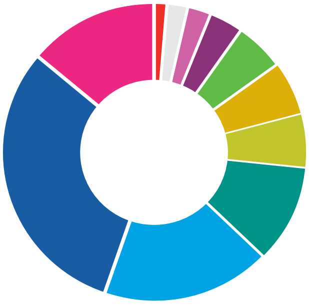
What we're doing about Blackhole, and what you can do

At SophosLabs, we track Blackhole 24/7, making sure that our generic detection and reputation filtering keep up with this changing exploit kit. Whenever Blackhole learns how to counter them, we rapidly roll out updates as needed via the cloud. We also apply cutting-edge techniques for identifying and analyzing server-side polymorphic attacks such as Blackhole.

On your end, the best defense against Blackhole is a defense in depth.

1. Quickly patching operating systems and applications is always important, and it's best to automate your patching process.
2. To reduce the attack surface, disable vulnerable systems such as Java and Flash wherever you don't need them.
3. Block compromised legitimate websites and exploit sites through a combination of reputation filtering and content detection technologies, and use content detection to block payloads. Note that reputation filtering can often block exploit sites before content detection occurs, but it is not foolproof by itself.
4. Deter or reduce social engineering attacks that originate with spam with up-to-date spam filters and more active user education.
5. If your endpoint security product has HIPS (host intrusion prevention system) features, use them for added protection against new or modified exploits.

Where are Blackhole exploit sites being hosted?



Countries hosting Blackhole exploit sites (2012)

● Brazil	**1.49%**	● Italy	**5.75%**
● Great Britain	**2.24%**	● Chile	**10.77%**
● Netherlands	**2.55%**	● Russia	**17.88%**
● Germany	**3.68%**	● United States	**30.81%**
● China	**5.22%**	● Other	**13.88%**
● Turkey	**5.74%**		

Source: SophosLabs

Java attacks reach critical mass

This was a rough year for Java in the browser. Major new vulnerabilities repeatedly battered Java browser plugins, encouraging many organizations to get rid of Java in the browser if possible.

In April, more than 600,000 Mac users found themselves recruited into the global Flashback, or Flashplayer botnet, courtesy of a Java vulnerability left unpatched on OS X for far too long. After Apple issued a removal tool and a Java patch, Oracle assumed direct responsibility for publishing Java for OS X in the future, and promised to deliver Java patches for OS X and Windows and to release OS X Java patches at the same time as those for Windows.[18]

Oracle's Java developers were soon called upon to deliver prompt patches. Within days of the discovery of a new zero-day vulnerability affecting Java 7 on all platforms and operating systems, the flaw was already being exploited in targeted attacks, was integrated into the widely used Blackhole exploit kit,[19] and had even shown up in a bogus Microsoft Services Agreement phishing email.[20] According to one detailed analysis, this exploit enabled untrusted code to access classes that should be off-limits, and even disabled the Java security manager.[21]

As Oracle had promised, it released an out-of-band fix more rapidly than some observers had expected. But, within weeks, more major Java flaws surfaced. Security Explorations, the same researchers who discovered the first flaw, found another way to bypass Java's secure application sandbox—this time, not just on Java 7, but also on Java 5 and 6,[22] and in all leading browsers. The new exploit put 1 billion devices at risk.

Many users today have little or no need for browser-based Java programs, known as applets. JavaScript and other technologies have largely taken over from applets inside the browser. Unless you genuinely need, and know you need, Java in your browser, Sophos recommends that you turn it off.

Our website offers detailed instructions for doing so within Internet Explorer, Firefox, Google Chrome, Safari, and Opera.[23]

If you do rely on websites that require Java, consider installing a second browser and turning Java on in that browser only. Use it for your Java-based websites only, and stick to your Java-disabled main browser for everything else.

Java isn't the only plugin platform that's caused security headaches. In previous years, Adobe's Flash has also been victimized by high-profile exploits. Fortunately, the need for browser plugins such as Flash is diminishing. HTML5-enabled browsers have capabilities such as playing audio and video built in, making customary plugins obsolete.

Major organizations still leave users' passwords vulnerable

Password vulnerabilities ought to be a rarity. Well-known and easily-followed techniques exist for generating, using and storing passwords that should keep both individuals and organizations safe. Yet in 2012 we saw one massive password breach after another, at a slew of high profile organizations.

- Russian cybercriminals posted nearly 6.5 million LinkedIn passwords on the Internet. Teams of hackers rapidly went to work attacking those passwords, and cracked more than 60% within days. That task was made simpler by the fact that LinkedIn hadn't "salted" its password database with random data before encrypting it.[24]

- Dating website eHarmony quickly reported that some 1.5 million of its own passwords were uploaded to the web following the same attack that hit LinkedIn.[25]

- Formspring discovered that the passwords of 420,000 of its users had been compromised and posted online, and instructed all 28 million of the site's members to change their passwords as a precaution.[26]

- Yahoo Voices admitted that nearly 500,000 of its own emails and passwords had been stolen.[27]

- Multinational technology firm Philips was attacked by the r00tbeer gang. The gang walked away with thousands of names, telephone numbers, addresses and unencrypted passwords.[28]

- IEEE, the world's largest professional association for the advancement of technology, left a log file of nearly 400 million web requests in a world-readable directory. Those requests included the usernames and plain text passwords of nearly 100,000 unique users.[29]

Learn more about modern threats

Train your employees to steer clear of trouble with our free toolkit.

Five Tips to Reduce Risk From Modern Web Threats

So, what can you learn from data loss—beyond that you don't want it to happen to you?

If you're a user:

- Use stronger passwords—and use a different one for each site that stores information you care about.
- Use password management software, such as 1Password, KeePass, or LastPass. Some of these tools will even generate hard-to-crack passwords for you.[30]

If you're responsible for password databases:

- Don't ever store passwords in clear text.
- Always apply a randomly-generated salt to each password before hashing and encrypting it for storage.
- Don't just hash your salted password once and store it. Hash multiple times to increase the complexity of testing each password during an attack. It's best to use a recognized password crunching algorithm such as bcrypt, scrypt or PBKDF2.
- Compare your site's potential vulnerabilities to the OWASP Top Ten security risks, especially potential password vulnerabilities associated with broken authentication and session management.[31]
- Finally, protect your password database, network and servers with layered defenses.

Android: Today's biggest target

Featuring research by SophosLabs

Over 100 million Android phones shipped in the second quarter of 2012 alone.[32] In the U.S., a September 2012 survey of smartphone users gave Android a whopping 52.2% market share.[33] Targets this large are difficult for malware authors to resist. And they aren't resisting—attacks against Android are increasing rapidly. In these pages, we'll share some examples, and offer some perspective. We'll ask: How serious are these attacks? Are they likely to widen or worsen? And what reasonable steps should IT organizations and individuals take to protect themselves?

Unsophisticated, but profitable: Fake software, unauthorized SMS messages

Today, the most common business model for Android malware attacks is to install fake apps that secretly send expensive messages to premium rate SMS services. Recent examples have included phony versions of Angry Birds Space, Instagram, and fake Android antivirus products.[34] In May 2012, UK's mobile phone industry regulator discovered that 1,391 UK Android users had been stung by one of these scams. The regulator fined the firm that operated the payment system involved, halted fund transfers, and demanded refunds for those who'd already paid. However, UK users represented only about 10% of this malware's apparent victims—it has been seen in at least 18 countries.

Currently, one family of Android malware, Andr/Boxer, accounts for the largest number of Android malware samples we see, roughly one third of the total. Linked to .ru domains hosted in the Ukraine, Andr/Boxer presents messages in Russian and has disproportionately attacked Eastern European Android users who visit sites where they've been promised photos of attractive women.

When they arrive at these sites, users see a webpage that is carefully crafted to entice them to download and install a malicious app. For example, the user might be prompted (in Russian) to install a fake update for products such as Opera or Skype. Or, in some cases, a fake antivirus scan is run, reports false infections, and recommends the installation of a fake antivirus program. Once installed, the new app begins sending expensive SMS messages. Many of these Trojans install with what Android calls the INSTALL_PACKAGES permission. That means they can download and install additional malware in the future.

Learn more about mobile device management

Free tool: Mobile Security for Android

Mobile Security Toolkit

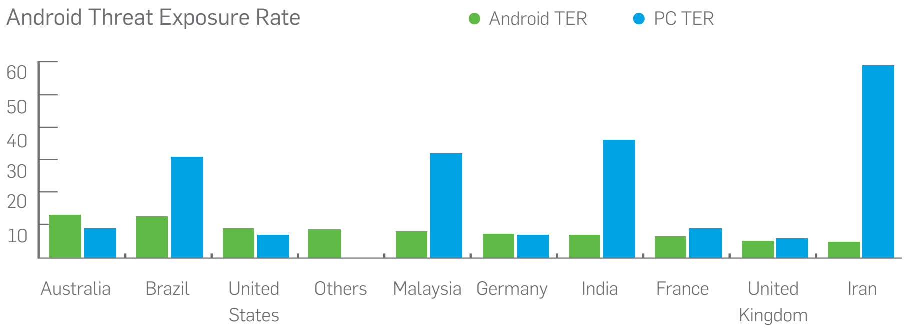
Mobile Device Management Buyers Guide

When Malware Goes Mobile

Vanja Svajcer of SophosLabs explains Android malware

Android threats accelerate

In Australia and the U.S., Sophos is now reporting Android threat exposure rates exceeding those of PCs.



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

Source: SophosLabs

Joining the botnet

Until recently, most fake software attacks we've seen on Android have been relatively unsophisticated. For example, some use primitive polymorphic methods that involve randomizing images, thereby changing checksums to avoid detection. Leading security companies learned how to defeat this tactic many years ago.

But the attackers are making headway. For example, consider the malware-infected editions of Angry Birds Space we saw in April 2012 (Andr/KongFu-L). Again, available only through unofficial Android app markets, these Trojans play like the real game. But they also use a software trick known as the GingerBreak exploit to gain root access, install malicious code, and communicate with a remote website to download and install additional malware. This allows these Trojans to avoid detection and removal, while recruiting the device into a global botnet.

Capturing your messages and your bank account

We have also begun to see Android malware that eavesdrops on incoming SMS messages and forwards them to another SMS number or server. This sort of data leakage represents a significant risk, both to individuals and to organizations.

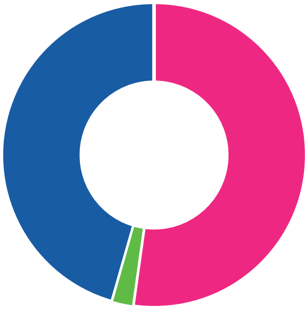
The potential exists for attacks like these to target Internet banking services that send mobile transaction authentication numbers via SMS. Many banks send authentication codes to your phone via SMS each time you do an online transaction. This means that just stealing a login password is no longer enough for criminals to raid your account. But malware on your phone, such as the Zeus-based Andr/Zitmo (and similar versions targeting BlackBerry) are capable of intercepting those SMS messages.

Consider the following hypothetical scenario. Through a conventional phishing attack, a victim gives criminals sufficient information to allow them to sign in to your mobile banking account and also port your phone number (this has happened). They can now log in to your online bank account while also receiving an SMS containing the second-factor authentication token needed to complete a transaction.

Through the use of a malicious Android app that harvests SMS messages in real time and in concert with a social engineering attack, attackers open a brief window of opportunity to steal this token and use it before you can stop them.

Naked Security Survey

Is smartphone SMS/TXT spam a problem for you?



● Yes 43.78%

● It was, but I downloaded an app and it is sorted now 2.36%

● No—I rarely/never received an SMS text spam on my phone 45.29%

Based on 552 votes

Source: Naked Security

PUAs: Not quite malware, but still risky

It's worth mentioning the widespread presence of potentially unwanted applications (PUA). PUAs are Android apps that may not strictly qualify as malware, but may nevertheless introduce security or other risks.

First, many users have installed apps that link to aggressive advertising networks, can track their devices and locations, and may even capture contact data. These apps earn their profits simply by serving pornographic advertising. Many companies may wish to eliminate them due to the information they expose, or because they may have a duty of care to protect employees from inappropriate content and a potentially hostile work environment.

Second, some sophisticated Android users have chosen to install Andr/DrSheep-A on their own devices. Similar to the well-known desktop tool Firesheep, Andr/DrSheep-A can sniff wireless traffic and intercept unencrypted cookies from sites like Facebook and Twitter. The legitimate use for this tool is to test your own network. However, it is often used to impersonate nearby users without their knowledge. We currently find Andr/DrSheep-A on 2.6% of the Android devices protected by Sophos Mobile Security. Corporate IT departments are unlikely to countenance the installation, let alone the use, of such tools.

If you "root" your device, it means you enable software to acquire full Android administrator privileges. The name comes from the administrator account, known as "root" on UNIX-like operating systems such as Android. Rooting is popular because it allows you greater control over your device—notably to remove unwanted software add-ons included by your service provider, and to replace them with alternatives of your own choosing.

Rooting bypasses the built-in Android security model that limits each app's access to data from other apps. It's easier for malware to gain full privileges on rooted devices, and to avoid detection and removal. For the IT organization supporting BYOD network access, rooted Android devices increase risk.

Mitigating the risks while they're still manageable

In most business environments, the risks from Android are modest at this point. But those risks are growing. Even as Google makes improvements that secure the platform against more obvious threats, new threats emerge. For example, some security experts have recently expressed concern about risks from new near field communications (NFC) features intended to allow advanced Android devices to function like credit cards.

Even today, Android malware can place a company's future at risk by exposing strategic information or stealing passwords. With this in mind, IT organizations should secure their Android devices against malware, data loss, and other threats. We recommend the following steps to bring down the level of risk. Remember, none of these tips are foolproof or sufficient in isolation. But in most environments, they will go a long way.

- Extend your IT security and acceptable use policies to Android devices, if you haven't done so already.
- Refuse access to rooted Android devices.
- Consider full device encryption to protect against data loss, and provide for remote wipe of lost or stolen devices. If you choose to encrypt, make sure your solution can also encrypt optional SD cards that may contain sensitive data, even if those SD cards are formatted differently.
- Where possible, establish automated processes for updating Android devices to reflect security fixes. Keep your Android devices up to date with the security patches provided by the manufacturer and by the vendors of any additional software you've intalled.
- Consider restricting Android devices to apps from Google's official Play Store. Malware has turned up in the Play Store, but much less frequently than in many of the other unregulated, unofficial app markets, notably those in Eastern Europe and Asia.

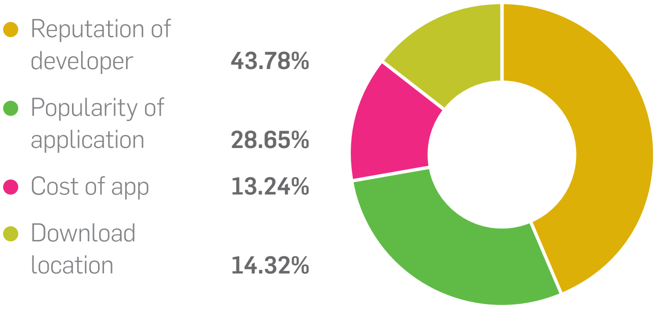
- When you authorize app stores, limit users to apps with a positive history and a strong rating.

- Avoid social engineering attacks, and help your colleagues avoid them. This means carefully checking the permissions that an app requests when it's installed. For example, if you can't think of a specific credible reason why an app wants to send SMS messages, don't let it. And pause for a moment to consider whether you still want to install it.[35]

- Finally, consider using an anti-malware and mobile device management solution on your Android devices. We recommend Sophos Mobile Control. But whatever solution you choose, get it from a company that has extensive experience with both antivirus and broader security challenges. Why? First, because attack techniques are beginning to migrate to Android from other platforms. Your solution provider should already know how to handle these. Second, because attacks are emerging and mutating more rapidly. Your provider should have the 24/7 global infrastructure to identify threats, and the cloud-based infrastructure to respond immediately. Third, and most importantly, because today's complex infrastructures require an integrated mobile security response that goes beyond antivirus alone to encompass multiple issues, ranging from networking to encryption.

Naked Security Survey

What is the most important consideration when you install an app on your Android device?



Based on 370 respondents
Source: Naked Security

Diverse platforms and technologies widen opportunities for attack

Once, almost everyone ran Windows. Attackers attacked Windows. Defenders defended Windows. Those days are gone.

In 2012 we saw plenty of Windows-specific holes and vulnerabilities. For instance, the Windows Sidebar and Gadgets in Windows Vista and Windows 7 were revealed to be so insecure that Microsoft immediately eliminated them, and gave customers tools to disable them.

Windows Sidebar had hosted mini-programs (gadgets) such as news, stocks, and weather reports. Together, these were Microsoft's answer to Apple's popular Dashboard and Widgets. However, security researchers Mickey Shkatov and Toby Kohlenberg announced that they could demonstrate multiple attack vectors against gadgets, show how to create malicious gadgets, and identify flaws in published gadgets.[36] Already planning a new approach to these miniature applications in Windows 8, Microsoft dropped Sidebar and Gadgets like a rock.

While most computer users still work with Windows, far more development now takes place elsewhere—on the web and mobile platforms. This means companies and individual users must worry about security risks in new and untraditional environments such as Android.

Here is a sampling of security breaches in 2012, offering a taste of what we all must deal with—and why our defenses must become increasingly layered, proactive and comprehensive.

- In February 2012, a hacker identified cross-site scripting (XSS) holes in 25 UK online stores that had been certified as safe by VeriSign, Visa, or MasterCard.[37] Criminals can exploit XSS flaws to steal authentication credentials or customer billing information, placing customers at risk of identity theft. The holes arose from a common source: a poorly written script for filtering user searches. It's another reminder to users that security isn't just a matter of words and icons. Simply seeing https://, a padlock, or a VeriSign Trusted logo doesn't mean you can get careless online. And it's a huge reminder to web professionals to keep all their applications and scripts up to date, including scripts made publicly available by other authors.
- Thousands of self-hosted WordPress sites were hosting the dangerous Blackhole malware attack.[38] In August 2012, Sophos discovered a major malware campaign which attempts to infect computers using the notorious Blackhole exploit kit. Users receive “order verification” emails containing links to legitimate WordPress blogs that have been poisoned to download malware. Users of the hosted WordPress.com service aren't vulnerable: the service provider, Automattic, looks after the security of the WordPress.com servers for them.
- Hackers have been demonstrating at least theoretical attacks against everything from transit fare cards to the newest near field communication (NFC) enabled smartphones.[39]

Ransomware returns for an encore

Certain attacks seem cyclical. Even when defeated for years, they're too easy and tempting for cybercriminals to abandon forever. For example, in 2012, Sophos saw a resurgence in ransomware attacks that lock users out of their computers, and demand payment to restore access.

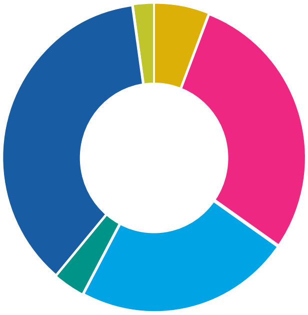
Ransomware is far from new. Way back in 1989, primitive ransomware was distributed on floppy disks by postal mail. Users were promised advanced software to advise them about HIV/AIDS, but instead found their hard drives scrambled. Users were told to pay $189 to an address in Panama via bankers draft, cashier's check, or international money order.[40]

Today's ransomware arrives via more modern techniques, such as social engineered email and poisoned webpages. One sort of ransomware merely freezes your PC and asks for money. This leaves your underlying files intact. Although an infection is disruptive, it can usually be repaired. The other sort of ransomware scrambles your files, so it is as catastrophic as losing your laptop altogether or suffering a complete disk failure.

As of this writing, the most widespread ransomware is of the first type. Reveton, for example, also known as Citadel or Troj/Ransom, hides the Windows desktop, locks you out of all programs, and displays a full screen window with an FBI (or other national police) logo. You see an urgent claim that illegally downloaded copyrighted material has been found on your computer, and that you must pay a fine (typically $200) to restore access.

Naked Security Survey

Which web browser do you recommend?



●	Internet Explorer	5.95%
●	Chrome	28.9%
●	Firefox	23.09%
●	Safari	3.25%
●	Opera	36.75%
●	No preference	2.06%

Based on 370 respondents

Source: Naked Security

This attack can be defeated by rebooting to an antivirus tool that contains its own operating system, bypassing Windows (for example, Sophos Bootable Anti-Virus). Once this tool is running, users can scan their systems, remove the infection, and restore their systems.[41]

Unfortunately, we've also seen growing numbers of infections that fully encrypt users' hard drives using strong encryption, and securely forward the only key to the attackers. In July 2012, we saw a variant that threatened to contact police with a "special password" that would reveal child pornographic files on the victim's computer.[42]

In nearly every case, updated antivirus software can prevent ransomware from installing and running on your computer. But if you've left your computer unprotected and you get hit by encryption-based ransomware, it's probably too late. Some ransomware encryptions can be reversed (Sophos has free tools which may be able to help), but only if the criminals have made cryptographic mistakes. There may be no cure, so prevention is always better.

Learn more about ransomware

Top 5 Myths of Safe Web Browsing

Director of Technology Strategy, James Lyne, explains ransomware

OS X and the Mac: More users, emerging risks

Featuring research by SophosLabs

Most malware developers have found it more profitable to attack Windows than to learn new skills needed to target the smaller OS X user community. But Macs are finding a new home in thousands of businesses and government agencies, and malware authors are paying attention.

Forrester Research analyst Frank Gillette recently reported that “almost half of enterprises (1,000 employees or more) are issuing Macs to at least some employees—and they plan a 52% increase in the number of Macs they issue in 2012.”[43] Even more Macs are arriving unofficially through bring your own device arrangements, where they are often an executive’s device of choice for accessing web or cloud applications. Growing Mac usage means many IT organizations must objectively assess, mitigate, and anticipate Mac-related malware threats for the first time. And the risks are clearly increasing.

Fake antivirus and Flashback: Learning from Windows malware, gaining agility

In 2011, we saw a sustained attack on Mac users by a malware family called MacDefender. This malware, a fake antivirus, was the first significant Mac attack to be distributed via search result pages that attracted users to legitimate sites that had been poisoned with malware.

MacDefender is worth discussing today because it shows how Mac malware often follows in the footsteps of older Windows attacks. One sensible way to anticipate the future of Mac malware is to see what's happening now to Windows users. For instance, Mac admins might reasonably expect new customized attacks relying on server-side polymorphism.

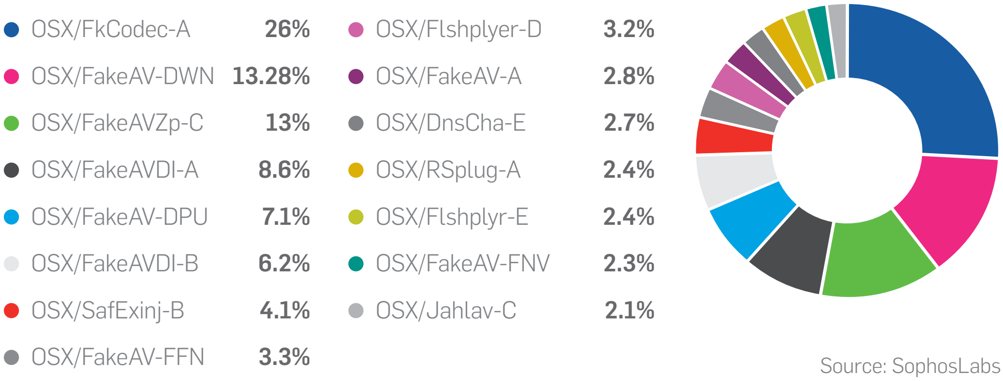
Borrowing from MacDefender while applying important innovations of their own, the creators of the notorious Flashback botnet (aka, OSX/Flshplyr) infected more than 600,000 Macs in the spring of 2012.

Flashback first surfaced as a fake Adobe Flash installer late in 2011. In April 2012, Flashback began to install itself as a drive-by download, exploiting a Java vulnerability left unpatched on OS X weeks after Microsoft had provided a fix to Windows users. Apple ultimately patched OS X 10.7 and 10.6, but not previous versions. At the infection's peak, Sophos' free Mac antivirus product identified Flashback-related malware on approximately 2.1% of the Macs it protected.

While both MacDefender and Flashback have been beaten back, they each show Mac malware authors becoming more agile. We've seen the authors changing the delivery mechanisms of existing malware and pursuing new zero-day exploits.

Mac OS X malware snapshot

In a typical week, SophosLabs detects 4,900 pieces of OS X malware on Mac computers. This chart shows a snapshot of Mac malware detected in the week of August 1-6, 2012.



Source: SophosLabs

Morcut/Crisis: More sophisticated and potentially more dangerous

Fake antivirus software typically makes money for cybercriminals by convincing users to provide personal credit card information for software they don't need. For most enterprises, the downside risks of fake antivirus have been modest. But malware such as OSX/Morcut-A (aka Crisis), first discovered in late July 2012, presents greater risks.

Designed for spying, Morcut can remotely monitor virtually every way a user communicates: mouse coordinates, IM, Skype call data, location information, the Mac's webcam and microphone, clipboard contents, keystrokes, running apps, web URLs, screenshots, calendar and address book contents, alerts, device information, and even file system metadata.

Morcut appears as a Java Archive file (JAR) claiming to be digitally signed by VeriSign. If installed by the user, Morcut deploys kernel driver components to hide and run without administrator's authentication;[44] a backdoor component which opens the Mac to other network users; command and control to accept remote instructions and adapt its behavior; and, most importantly, code for stealing user data.

If Morcut spreads, it will represent a serious threat to internal corporate security and compliance. Its capabilities especially lend themselves to targeted attacks aimed at capturing information about specific known Mac users in pivotal organizational roles. In contrast to most earlier Mac malware, it also reflects an extremely thorough understanding of Mac programming techniques, capabilities, and potential weaknesses.

Similar backdoor techniques are already appearing elsewhere. For instance, we recently saw them embedded in a kit for the first time. The kit, OSX/NetWrdRC-A, is primitive, flawed, and easily halted.[45] But it's a harbinger of more sophisticated and dangerous attacks to come.

Learn more about emerging OS X risks

Free tool: Sophos Anti-Virus for Mac

Andrew Ludgate of SophosLabs explains Mac malware

Windows malware hiding quietly on Macs

Much of the malware found on Macs is Windows malware. Traditionally, many Mac users have been indifferent about this—they assume that it won't damage their systems, and may not consider the harm to Windows-using colleagues they might place at risk. But IT administrators running cross-platform environments (or working with partners and customers who use Windows) are likely to see things differently. Moreover, the Windows partitions of dual-boot Macs can indeed be infected, as can virtualized Windows sessions running under Parallels, VMware, VirtualBox, or even the open source WINE program.

Mac users who need occasional access to a Windows program sometimes decide to download it from third parties, and may illegally create a license key using a downloadable generator. By doing so, they often encounter malware such as Mal/KeyGen-M, a family of trojanized license key generators that we've identified on approximately 7% of the Macs running Sophos Anti-Virus software.

Another common source of Windows malware on Macs today is fake Windows Media movie or TV files. These files contain auto-forwarding web links promising the codec needed to view the video, but deliver zero-day malware instead. Windows Media files generally won't run on Macs, but Mac users often torrent these files to improve their "ratios" on private tracker sites, without realizing the contents are malicious. Windows users then attempt to play the videos and become infected.

Recent OS X security improvements and their limitations

Mac OS X, originally built on BSD UNIX, has a strong security model. In 2009, with the release of OS X 10.6 Snow Leopard, Apple added limited malware scanning through the Launch Services Quarantine (LSQuarantine) system and XProtect technology. In mid-2011, XProtect became a dynamic push update service with more power to detect and clean up files fingerprinted as malicious.

In mid-2012, with OS X 10.8 Mountain Lion, Apple introduced Gatekeeper, which manages code execution permissions for code obtained through approved software. By default, Gatekeeper pre-authorizes all software signed with an official Apple developer key that has not been blocked due to previous abuse.

Gatekeeper is a significant and welcome improvement in Mac security, but it is only a partial solution. Software copied from USB, already on the computer, copied directly between computers, or transferred by non-standard file transfer systems such as BitTorrent will evade it. Individual users with administrator credentials can change Gatekeeper's default settings to allow unsigned apps to install without any alert.[46]

Users or running processes can still strip the LSQuarantine flag from files. Unsigned programs can be authorized and launched simply by right-clicking on them in the Finder and selecting Open, instead of just double-clicking on the icon. Versions of OS X older than 10.8 don't include Gatekeeper.

Finally, the runtime interpreters for Java, Flash, and OS X shell scripts are all pre-authorized by Apple. These interpreters are free to run whatever code they wish. Java and Flash have been major attack vectors on the Mac platform. This may gradually become less of a problem—the Mac version of Java was recently hardened, and Adobe Flash is gradually being replaced by HTML5.

Implementing a comprehensive Mac anti-malware solution

If Gatekeeper, LSQuarantine and XProtect offer only a partial solution, what does a complete Mac anti-malware solution look like? It will have these components:

- **User education.** Work with Mac users to help them understand that significant threats to Macs do exist. More will arrive as Macs become increasingly popular in business, and social engineering attacks are as likely to victimize Mac users as Windows users.

- **Layered protection.** Constantly updated Mac endpoint protection is now essential—but so is protection for servers, mail and web gateways, and network infrastructure. Note that server applications such as WordPress and Drupal have been heavily exploited by malware capable of targeting Mac clients. Be aware that many lightweight virus scanners, especially those on integrated gateway and firewall devices, do not scan for Mac malware and exploits, leaving them essentially unprotected at this layer.

- **Mac-specific expertise.** Either hire Mac specialists or train existing staff on the platform's unique characteristics. For instance, heuristic firewall and router policies may need to reflect differences in Mac traffic associated with Safari web browser pre-caching or network discovery broadcasts generated by the Mac's Bonjour services. Knowledgeable file system configuration choices can harden dual-boot Mac/Windows systems against attack.

  Where Mac users rely on Mail.app or other UNIX-style back-end mail clients, careful decisions about mail storage can make it less likely that Windows users will inadvertently open infected .zip files. While the Mac's underpinning is based on BSD UNIX, its user interface is not. Therefore, generic UNIX knowledge is very helpful, but not necessarily sufficient.

- **Strong IT processes and policies.** Wherever possible, extend ITIL-type best practice policies to Macs as well as PCs. Provide for rapid and automated patching of Macs as well as Windows devices. And, of course, patch Java, Flash, and applications as well as OS X itself. If possible, control users' ability to install new software. Make sure your internal developers digitally sign their own OS X software. Finally, manage your logs. Macs log virtually everything in real time, making it possible to identify new security threats and halt them via firewall policy changes or by isolating portions of the network.

- **Realism.** Since Macs are often used by senior executives and creative teams who need maximum control over their computers, you may need to accept that some Macs will be untrusted. But untrusted should not mean unprotected. You should still offer users whatever protection is practical. And organizations can't forget legal requirements associated with security and breach notification. These requirements may be especially important to enforce where senior executives are involved. Many security experts argue that perimeters are becoming less defensible, and conclude that all systems should be treated as untrusted, not just Macs.

Authorities make high-profile malware arrests and takedowns

Learn more about malware

Exposing the Money Behind the Malware

Security professionals will always have to rely on themselves first and foremost to protect their own systems and assets. But in 2012, we received more help from the authorities—and that was a welcome relief.

In perhaps their highest-profile victory, U.S. federal authorities followed up their 2011 arrests of the notorious LulzSec hackers by gaining extensive cooperation from one of the gang's key figures, Hector Xavier Monsegur ("Sabu"). As Sabu, Monsegur had long railed against the U.S. government—but he reportedly worked for months under cover, helping build cases against those behind hacking attacks on the CIA, Pentagon, U.S. Senate, the UK's Serious Organised Crime Agency (SOCA), and many other prominent organizations. Monsegur helped nab Jake Davis (aka "Topiary") in the Shetland Islands, where Davis reputedly held 750,000 stolen passwords in his possession. In August 2012, prosecutors requested a further six-month delay in Monsegur's sentencing to accommodate his further cooperation.[47]

LulzSec may have been the most widely publicized case of the year, but it was far from the only one. 2012 began with the extradition of suspected Russian cybercriminal Vladimir Zdorovenin to the U.S. Zdorovenin was charged with installing keyloggers on U.S. victims' computers to capture credit card numbers, using those accounts to make apparently legitimate purchases of goods from their own online businesses, and tapping into their victims' financial services accounts to manipulate stock prices.[48] He pled guilty to conspiracy and wire fraud.[49]

Then, in May, the mastermind of Bredolab—a botnet that captured 30 million computers in its heyday—was sentenced to four years in jail in Armenia. According to prosecutors, Georg Avanesov was earning 100,000 Euros (£80,000 or $125,000) a month from his Bredolab botnet business, renting access to criminals who wanted to mail spam and spread malware. At its peak, Avanesov's botnet was spewing out more than 3 billion infected emails every day—while he was jetting off to the Seychelles for luxury vacations.[50]

In June, the U.S. Federal Bureau of Investigation culminated a two-year international investigation into credit card fraud with 24 arrests of alleged cybercriminals from the U.S., UK, Bosnia, Bulgaria, Norway, Germany and beyond. These "carders" included several experts in creating remote access Trojans and defrauding Apple product warranties. The FBI estimated that it prevented more than $205 million in fraudulent transactions, identified 411,000 stolen cards, and notified 47 organizations that they had been compromised.[51]

Later the same month, Tokyo police arrested six men in connection with an app that infected Android smartphones, stole personal data, and demanded a fee. According to the police, 9,252 people had downloaded the malicious Android app, and 211 of them were convinced to pay up—more than $250,000 in all.[52]

Then, early in July, the UK's Police Central e-crime Unit (PCeU) reported the tough sentences meted out to three citizens of the Baltic states, after their conviction for using the SpyEye Trojan to steal from online bank accounts throughout the UK, Denmark, The Netherlands and New Zealand.[53]

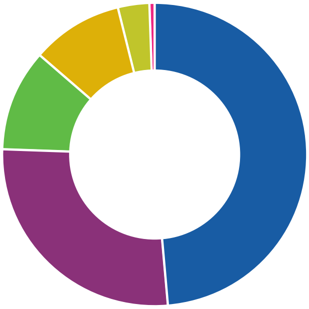
Later in July, Dutch police took down the secondary command and control (C&C) computers used by the huge Grum botnet, just a week after its existence was publicized.[54] Shortly thereafter, other authorities were able to disable the botnet's primary C&C computers in Panama and Russia, thereby dismantling a botnet that was responsible for an estimated 17% of the world's spam.[55]

Top 12 spam producing countries

1. India	12.19%	7. Russia	3.34%
2. United States	7.06%	8. France	3.04%
3. Italy	6.95%	9. Pakistan	2.95%
4. Korea	5.37%	10. Poland	2.77%
5. Brazil	4.17%	11. Indonesia	2.73%
6. Vietnam	4.16%	12. China	2.73%

Percent of all spam
Source: SophosLabs

Spam sources by continent



● Asia	48.66%
● Europe	27.07%
● South America	10.89%
● North America	9.68%
● Africa	3.20%
● Oceania	0.05%

Percent of all spam
Source: SophosLabs

Growth of dangerous targeted attacks

While law enforcement was becoming more effective against cybercriminals, 2012 also saw growing concern about state-sponsored cyber attacks, as well as exploits launched in apparent cooperation with states to achieve strategic objectives. To the extent that these attacks proliferate and are confirmed, high-value government and private targets will face worrisome new risks. Lower value targets will also need to increase vigilance in order to avoid becoming collateral damage. This will mean, among other things, strengthening their own network security efforts—and integrating them with other security services to detect and repel attacks more rapidly.[56]

In this category, the Flame attack got the most publicity in 2012, but its significance and effectiveness were far from clear. More recently, the destructive Shamoon Trojan (Troj/Mdrop-ELD) apparently caused significant damage throughout the Middle East's energy sector. According to the BBC and The Register,[57] it infected some 30,000 computers, taking Saudi Arabia's national oil company network offline.[58] Soon thereafter, Qatar's natural gas firm RasGas was attacked, taking its network and website offline as well, and leaving its office systems unusable.[59]

We saw hints of organized cyber attacks against the U.S. Late in September, U.S. Senator Joseph Lieberman pointed to massive recent DDoS attacks targeting Bank of America, JPMorgan Chase, Wells Fargo, Citigroup and PNC Bank, and alleging without public proof that these attacks were "done by Iran... [as] a response to increasingly strong economic sanctions the U.S. and its allies have put on Iranian financial institutions. It is, if you will, a counter attack..."[60]

According to Bloomberg, whatever their source, these new attacks "have breached some of the nation's most advanced computer defenses and exposed the vulnerability of its infrastructure."[61]

By their very nature, state-sponsored cyber attacks (and attacks by highly-sophisticated private teams closely allied with states) are difficult to track and prove—and equally susceptible to being overhyped. Nevertheless, more actors appear to be developing the capability to execute such attacks. And, once they possess such a capability, the temptation to use it will be substantial.

Is your country safe or risky?

Threat exposure rate by country

10 Safest Countries

	TER		TER
1. Norway	**1.81%**	6. U.S.	**3.82%**
2. Sweden	**2.59%**	7. Slovenia	**4.21%**
3. Japan	**2.63%**	8. Canada	**4.26%**
4. UK	**3.51%**	9. Austria	**4.27%**
5. Switzerland	**3.81%**	10. Netherlands	**4.28%**

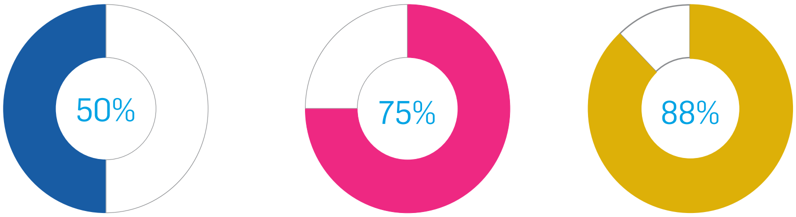
10 Riskiest Countries

	TER		TER
1. Indonesia	**23.54%**	6. India	**15.88%**
2. China	**21.26%**	7. Mexico	**15.66%**
3. Thailand	**20.78%**	8. UAE	**13.67%**
4. Philippines	**19.81%**	9. Taiwan	**12.66%**
5. Malaysia	**17.44%**	10. Hong Kong	**11.47%**

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

Source: SophosLabs

Welcome to the age of personalized malware



50% of our detections are based on only 19 malware identites.

75% of unique pieces of malware are seen in only one organization.

88% of malware found in fewer than 10 organizations.

Source: SophosLabs

Polymorphic and targeted attacks: The long tail

Learn more about long tail

▶ Richard Wang of SophosLabs explains the long tail

Featuring research by SophosLabs

The phrase "long tail" has become a popular way to describe events that don't fall within the conventional statistical distribution, but instead occur in ones or twos at the "tail end" of the distribution curve. That's the case in retail, where personalized products represent a growing percentage of sales—and it's increasingly true in malware too.

At Sophos, 75% of the malware files reported to us are only ever seen in one organization. This level of polymorphism is unprecedented. What's more, attackers have begun to develop and use far more sophisticated approaches to polymorphism to hide their attacks from security vendors and IT organizations. This battle has serious implications for IT, so it's important to understand what's happening, how Sophos is responding, and what you can do to protect yourself.

Polymorphism: Not new, but more troublesome

Polymorphism is not a new idea—malware authors have been using it for 20 years. Simply stated, polymorphic code changes its appearance in an attempt to avoid detection, without changing its behavior or goals. If a program looks different enough, attackers hope, antivirus software might miss it. Or the antivirus software might be forced to generate too many false positives, leading users to disable it.

In a polymorphic attack, code is typically encrypted to appear meaningless and paired with a decryptor that translates it back into a form that can be executed. Each time it's decrypted, a mutation engine changes its syntax, semantics, or both. For instance, Windows malware authors have often used structured exception handling to obfuscate control flow and make it tougher to perform static analysis of programs before they run.[62]

Traditional polymorphic viruses are self-contained and must contain the mutation engine in order to replicate. Sophos and other security companies have become adept at detecting these forms of malware. With access to the mutation engine, it's easier to analyze its behavior.

Today attackers are rapidly moving to web-distributed malware relying on server-side polymorphism (SSP). Now, the mutation engine and associated tools are hosted entirely on the server. Criminals can use these tools to create diverse file content on the fly. Recipients of this content (whether it is a Windows .exe, Adobe PDF, JavaScript, or anything else) see only one example of what the engine can create. They don't get to see the engine itself.

Security companies typically respond by obtaining many different examples of the engine's handiwork to gather information about how the engine works. They then write generic detection code.

Countering server-side polymorphism

At Sophos, we've used the analogy of genetics to become far more sophisticated in detecting SSP and other attacks. Sophos behavioral genotype technology identifies new malware by recognizing and extracting "genes" (or components of behavior). Using a finely tuned scoring system reflecting all the malware we've ever collected, we can identify combinations of genes (genotypes) that distinguish malware from legitimate code. We can compare this information with genes seen in known good files, minimizing false positives.

This gene-based approach is flexible and extensible. We can always add or modify genes reactively, or issue predictive genes to catch what the authors seem most likely to change next. We can also watch how they respond to detections by other security companies. Often, malware authors make changes which don't immediately impact our detection. By proactively adjusting our genetic profile to reflect these changes, we can make it less likely that further changes will render the attack invisible to us.

For certain SSP malware, the back-and-forth between security vendors and malware authors has accelerated dramatically. For example, sophisticated malware authors are constantly attempting to determine which portions of their code are being detected. We've seen attackers modify and replace compromised code within hours. Of course, we're also working non-stop to anticipate and respond.

SSP was pioneered on Windows systems, and has primarily been used on Windows executable files and JavaScript webpage content. In 2012, we saw it used for the first time in Android malware, and we believe it will spread to OS X in the near future. The notorious Blackhole exploit kit relies heavily on SSP, though it also has many other tricks up its sleeve.

Targeted attacks: narrow, focused and dangerous

Like most SSP attacks, Blackhole aims to deliver its payload widely and indiscriminately. But other forms of long tail attack are much more narrowly targeted. A malware author may intend to attack only a few organizations, seeking crucial financial data or banking credentials, and carefully preparing the attack with up-front research and reconnaissance. They may launch an attack with a spoofed email containing an infected document attachment crafted to tempt specific recipients.

For example, a financial decision-maker might receive an infected spreadsheet promising quarterly sales data. If the targeted person opens the infected document without it being flagged and the malware is installed, it may sit quietly until a user logs onto the company's online banking site. At this point, the malware may steal credentials through keystroke logging or by intercepting the second authentication factor in a two-factor authentication system. The attacker then can use the login for a future attack.

Criminals often launch targeted attacks against small and mid-sized businesses without a strong IT presence. And, since these pieces of malware are typically distributed to only a small number of targets, they may not be known by the organization's security provider and could slip through undetected, even without the use of advanced polymorphic techniques. This demonstrates another advantage of Sophos' gene-based approach. Our endpoint protection client can usually recognize new malware from its behavior and characteristics, even if we haven't seen it before.

The attackers may focus on compromising a single website they know their target organization's users will visit. Targets sometimes include small supply chain partners perceived as likely to have weaker IT security.[63]

Beyond using advanced endpoint protection, if you are a small or mid-sized business you can also reduce risk by setting aside a separate computer for online financial services: one that won't be used for general web browsing, email reading, or social networking.

Defense-in-depth against SSP

IT and security professionals need to be well-prepared to counter attacks based on SSP and narrowly targeted cybercrime attacks. First and foremost, you need layered defense-in-depth.

For example, the widespread ZeroAccess botnet and rootkit can often be spotted by the way it connects to its peer-to-peer botnet. Detecting this communication at your firewall would lead you back to the infected computer.

Security rules should combine static and dynamic analysis to identify a malicious program. For example, suspicious content noticed when a file is first analyzed (such as unusual encryption) can later be linked to suspicious activity (such as making an unexpected network connection).

IT professionals need to consider the risk of seemingly legitimate administration tools in targeted attacks. These tools won't be detected as malicious, but are actually quite powerful in an attacker's hands. Effective countermeasures include limiting the sorts of non-business applications that a user can run, a feature usually called application control.

Finally, IT professionals need to aggressively counter an attacker's best opportunities to find and exploit vulnerabilities by reducing network, software and user attack surfaces. Regular and automated patching has always been good practice, but it's become even more urgent in today's threat landscape.

Complete security

To stop evolving threats, protect data everywhere, manage your users needs for mobility, and ease the pressures on your IT team, you need a complete security strategy—covering the full security lifecycle. Complete security can be divided into four primary strategies:

- Reduce the attack surface. Take an active approach that monitors more than malware, including threats like vulnerabilities, applications, websites and spam.
- Protect everywhere. Make sure users are protected wherever they are and whatever device they're using and combines endpoint (including mobile), gateway and cloud technologies to share data and work together to provide better protection without impacting users and performance.
- Stop attacks and breaches. It's time to move beyond simply relying on antivirus signatures and look at layers of detection that stop threats at different stages of their execution. Make sure protection also looks at risky user behavior too—not just for malicious code.
- Keep people working. That includes your users and IT staff. Simplifying the tasks that take too much time today—by providing complete visibility and granular control of your security system—you can quickly see when something is wrong and then fix it.

Explore your two paths to complete security with Sophos

Sophos UTM

Integrates complete security software within a single appliance. Choose only the protection you need when you need it. And deploy it on the platform that best fits your business: software, hardware or virtual appliance. Each offers an identical feature set no matter if you protect 10 or 5,000 users. And our web-based management console enables easy, consolidated management of all your IT security.

Sophos EndUser Protection

Protects you everywhere, from your network to your servers, endpoints and mobile devices. And, because it's all from Sophos, it works better together. It's easier to use, saving you time and money, and it's backed by a vendor you trust.

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 to expect in 2013

By James Lyne, Director of Technology Strategy

At Sophos we pride ourselves in rapidly identifying, managing and responding to threats.

While cybercriminals are often opportunistic, we believe that in 2013 the ready availability of testing platforms—some with money back guarantees from their sponsors—make it all the more likely malware will continue to slip through single-tier traditional security systems. As a result we believe we will see more attacks where attackers hold long-term, high impact access to businesses. In response, a renewed focus on layered security and detection across the entire threat lifecycle, not just the point of initial entry, is likely to be a significant theme in the coming year. We also think the following five trends will factor into the IT security landscape in 2013.

Basic web server mistakes

In 2012 we saw an increase in SQL injection hacks of web servers and databases to steal large volumes of user names and passwords. Targets have ranged from small to large enterprises with motives both political and financial. With the uptick in these kinds of credential-based extractions, IT professionals will need to pay equal attention to protecting both their computers as well as their web server environment.

More “irreversible” malware

In 2012 we saw a surge in popularity and quality of ransomware malware, which encrypts your data and holds it for ransom. The availability of public key cryptography and clever command and control mechanisms has made it exceptionally hard, if not impossible to reverse the damage. Over the coming year we expect to see more attacks which, for IT professionals, will place a greater focus on behavioral protection mechanisms as well as system hardening and backup/restore procedures.

Attack toolkits with premium features

Over the past 12 months we have observed significant investment by cybercriminals in toolkits like the Blackhole exploit kit. They've built in features such as scriptable web services, APIs, malware quality assurance platforms, anti-forensics, slick reporting interfaces, and self protection mechanisms. In the coming year we will likely see a continued evolution in the maturation of these kits replete with premium features that appear to make access to high quality malicious code even simpler and comprehensive.

Better exploit mitigation

Even as the number of vulnerabilities appeared to increase in 2012—including every Java plugin released for the past eight years—exploiting them became more difficult as operating systems modernized and hardened. The ready availability of DEP, ASLR, sandboxing, more restricted mobile platforms and new trusted boot mechanisms (among others) made exploitation more challenging. While we're not expecting exploits to simply disappear, we could see this decrease in vulnerability exploits offset by a sharp rise in social engineering attacks across a wide array of platforms.

Integration, privacy and security challenges

In the past year mobile devices and applications like social media became more integrated. New technologies—like near field communication (NFC) being integrated in to these platforms—and increasingly creative use of GPS to connect our digital and physical lives means that there are new opportunities for cybercriminals to compromise our security or privacy. This trend is identifiable not just for mobile devices, but computing in general. In the coming year watch for new examples of attacks built on these technologies.

Learn more about mobile security

Mobile Device Security: What's Coming Next

The last word

Security really is about more than Microsoft. The PC remains the biggest target for malicious code today, yet criminals have created effective fake antivirus attacks for the Mac. Malware creators are also targeting mobile devices as we experience a whole new set of operating systems with different security models and attack vectors. Our efforts must focus on protecting and empowering end users—no matter what platform, device, or operating system they choose.

Sources

1. Microsoft Settles Lawsuit Against 3322 dot org, Reveals Scale of Nitol Botnet in China, http://nakedsecurity.sophos.com/2012/10/05/microsoft-settles-lawsuit-against-3322-dot-org/
2. Beware Remove Your Facebook Timeline Scams, Naked Security, http://nakedsecurity.sophos.com/2012/05/29/beware-remove-your-facebook-timeline-scams/; 'Remove Facebook Timeline' Themed Scam Circulating on Facebook, ZDNet, http://www.zdnet.com/blog/security/remove-facebook-timeline-themed-scam-circulating-on-facebook/9989
3. Twitter DMs From Your Friends Can Lead to Facebook Video Malware Attack, Naked Security, http://nakedsecurity.sophos.com/2012/09/24/twitter-facebook-video-malware/
4. OMG This Is So Cool! Pinterest Hack Feeds Spam to Twitter and Facebook, Naked Security, http://nakedsecurity.sophos.com/2012/09/12/omg-this-is-so-cool-pinterest-hack-feeds-spam-to-twitter-and-facebook/
5. Facebook Teams Up With Sophos and Other Security Vendors, Naked Security, http://nakedsecurity.sophos.com/2012/04/25/facebook-teams-up-sophos-other-vendors/
6. Application Detects Social Network Spam, Malware, Dark Reading, http://www.darkreading.com/security-monitoring/167901086/security/vulnerabilities/240006232/application-detects-social-network-spam-malware.html
7. A Continued Commitment to Security, The Facebook Blog, http://www.facebook.com/blog/blog.php?post=486790652130
8. Latest Black Eye For Dropbox Shines Spotlight On Larger Problem, Dark Reading, http://www.darkreading.com/blog/240004868/latest-black-eye-for-dropbox-shines-spotlight-on-larger-problem.html
9. Another Layer of Security for Your Dropbox Account, Dropbox Blog, 8/27/12, https://blog.dropbox.com/index.php/another-layer-of-security-for-your-dropbox-account
10. Fraunhofer Institute Finds Security Vulnerabilites in Cloud Storage Services, The H Security, http://www.h-online.com/security/news/item/Fraunhofer-Institute-finds-security-vulnerabilites-in-cloud-storage-services-1575935.html
11. 5 Dropbox Security Warnings for Businesses, InformationWeek, http://www.informationweek.com/security/management/5-dropbox-security-warnings-for-business/240005413?pgno=2
12. As you move forward with cloud computing, you may find it valuable to read Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, available from the Cloud Security Alliance at https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
13. Cloud Security: Top 5 Vulnerabilities of the Public Cloud, iPro Developer, http://www.iprodeveloper.com/article/security/public-cloud-security-698785
14. Sophos Technical Paper: Exploring the Blackhole Exploit Kit, http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/exploring-the-blackhole-exploit-kit.aspx
15. The Open Business Engine, http://obe.sourceforge.net/
16. ImmunityProducts.Blogspot.com, http://immunityproducts.blogspot.com/2012/08/java-0day-analysis-cve-2012-4681.html
17. Java Flaws Already Included in Blackhole Exploit Kit Oracle Was Informed of Vulnerabilities in April, Naked Security, http://nakedsecurity.sophos.com/2012/08/30/java-flaws-already-included-in-blackhole-exploit-kit-oracle-was-informed-of-vulnerabilities-in-april/
18. Oracle Updates Java, Supports OS X, Claims Full and Timely Updates for Apple Users, Naked Security, http://nakedsecurity.sophos.com/2012/08/15/oracle-updates-java-claims-full-and-timely-updates-for-apple-users/
19. Unpatched Java Exploit Spreads Like Wildfire, Naked Security, 8/28/12, http://nakedsecurity.sophos.com/2012/08/28/unpatched-java-exploit-spreads-like-wildfire/
20. Attacks on Java Security Hole Hidden in Bogus Microsoft Services Agreement Email, Naked Security, http://nakedsecurity.sophos.com/2012/09/03/java-security-hole-microsoft/
21. CVE-2012-4681 Java 7 0-Day vulnerability analysis, Deep End Research, http://www.deependresearch.org/2012/08/java-7-vulnerability-analysis.html
22. New Security Hole Found in Multiple Java Versions, Naked Security, http://nakedsecurity.sophos.com/2012/09/26/new-security-hole-multiple-java-versions/
23. Visit: http://www.sophos.com/en-us/security-news-trends/security-trends/java-zero-day-exploit-disable-browser.aspx
24. New Security Hole Found in Multiple Java Versions, Naked Security, http://nakedsecurity.sophos.com/2012/09/26/new-security-hole-multiple-java-versions/
25. Philips Hacked as R00tbeer Gang Strikes Again, Naked Security, http://nakedsecurity.sophos.com/2012/08/21/r00tbeer-returns-philips-hacked-poor-passwords/
26. Security Spill at the IEEE, Naked Security, http://nakedsecurity.sophos.com/2012/09/26/ieee-squirms-after-sensational-security-spill/
27. The Worst Passwords You Could Ever Choose Exposed by Yahoo Voices Hack, Naked Security, 7/13/12, http://nakedsecurity.sophos.com/2012/07/13/yahoo-voices-poor-passwords/
28. Philips Hacked as R00tbeer Gang Strikes Again, Naked Security, http://nakedsecurity.sophos.com/2012/08/21/r00tbeer-returns-philips-hacked-poor-passwords/
29. Security Spill at the IEEE, Naked Security, http://nakedsecurity.sophos.com/2012/09/26/ieee-squirms-after-sensational-security-spill/
30. The Worst Passwords You Could Ever Choose Exposed by Yahoo Voices Hack, Naked Security, 7/13/12, http://nakedsecurity.sophos.com/2012/07/13/yahoo-voices-poor-passwords/
31. OWASP Top Ten 2010: The Ten Most Critical Web Application Security Risks, The Open Web Application Security Project (OWASP), http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf
32. Source: IDC. http://money.cnn.com/2012/08/08/technology/smartphone-market-share/index.html
33. Source: ComScore. http://www.comscore.com/Press_Events/Press_Releases/2012/9/comScore_Reports_July_2012_U.S._Mobile_Subscriber_Market_Share

34. Angry Birds Malware Firm Fined £50,000 for Profiting From Fake Android Apps, Naked Security, http://nakedsecurity.sophos.com/2012/05/24/angry-birds-malware-fine/

35. Reading this, you might be curious why Sophos Anti-Virus requests permission to send SMS messages. When you do a remote lock or locate, it wants to send you an SMS with latitude/longitude or confirmation that the lock was successful.

36. Disable Windows Sidebar and Gadgets Now on Vista and Windows 7. Microsoft Warns of Security Risk, Naked Security, http://nakedsecurity.sophos.com/2012/07/12/disable-windows-sidebar-gadgets/

37. 25 VeriSign Trusted Shops Found to Have XSS Holes, Naked Security, http://nakedsecurity.sophos.com/2012/02/28/verisign-xss-holes/

38. Insecure WordPress Blogs Unwittingly Host Blackhole Malware Attack, Naked Security, http://nakedsecurity.sophos.com/2012/08/10/blackhole-malware-attack/

39. Android NFC Hack Lets Subway Riders Evade Fares, Naked Security, http://nakedsecurity.sophos.com/2012/09/24/android-nfc-hack-lets-subway-riders-evade-fares/

40. Ransomware: Would You Pay Up? Naked Security, http://nakedsecurity.sophos.com/2012/09/25/ransomware-would-you-pay-up/

41. Reveton/FBI Ransomware: Exposed, Explained and Eliminated, Naked Security, http://nakedsecurity.sophos.com/2012/08/29/reveton-ransomware-exposed-explained-and-eliminated/

42. Ransomware Makes Child Porn Menaces in Broken English, Naked Security, http://nakedsecurity.sophos.com/2012/07/04/ransomware-menaces/

43. Apple Infiltrates the Enterprise: 1/5 of Global Info Workers Use Apple Products for Work, http://blogs.forrester.com/frank_gillett/12-01-26-apple_infiltrates_the_enterprise_15_of_global_info_workers_use_apple_products_for_work_0

44. Mac Malware Spies on Email, Survives Reboots, http://www.informationweek.com/security/attacks/mac-malware-spies-on-email-survives-rebo/240004583

45. Apple Zombie Malware "NetWeird" Rummages for Browser and Email Passwords, http://nakedsecurity.sophos.com/2012/08/24/apple-zombie-malware-netweird-rummages-for-browser-and-email-passwords/

46. Mountain Lion: Hands on With Gatekeeper, http://www.macworld.com/article/1165408/mountain_lion_hands_on_with_gatekeeper.html

47. LulzSec Informant Sabu Rewarded With Six Months Freedom for Helping Feds, Naked Security, http://nakedsecurity.sophos.com/2012/08/23/sabu-lulzsec-freedom/

48. Alleged Russian Cybercriminal Extradited to the US, Naked Security, http://nakedsecurity.sophos.com/2012/01/19/alleged-cybercriminal-extradited-usa/

49. Russian Man Pleads Guilty to Cyber-Fraud Conspiracy in U.S., Bloomberg, http://www.bloomberg.com/news/2012-02-24/russian-national-pleads-guilty-to-cyber-fraud-conspiracy-in-u-s-.html

50. Bredolab: Jail for Man Who Masterminded Botnet of 30 Million Computers, Naked Security, http://nakedsecurity.sophos.com/2012/05/23/bredolab-jail-botnet/

51. FBI Arrests 24 in Internet Credit Card Fraud Ring, Naked Security, http://nakedsecurity.sophos.com/2012/06/27/fbi-arrests-24-in-internet-credit-card-fraud-ring/

52. Android Porn Malware Leads to Arrests in Japan, Naked Security, http://nakedsecurity.sophos.com/2012/06/18/android-porn-malware/

53. Baltic SpyEye Malware Trio Sent to Prison, Naked Security, http://nakedsecurity.sophos.com/2012/07/01/uk-cops-announce-sentencing-of-baltic-malware-trio/

54. Dutch Police Takedown C&Cs Used by Grum Botnet, Security Week, http://www.securityweek.com/dutch-police-takedown-ccs-used-grum-botnet

55. Top Spam Botnet 'Grum' Unplugged, Krebs on Security, http://krebsonsecurity.com/2012/07/top-spam-botnet-grum-unplugged/

56. Midyear Security Predictions: What You Should Know and Look Out For, Dark Reading, http://www.darkreading.com/blog/240002287/midyear-security-predictions-what-you-should-know-and-look-out-for.html

57. 30,000 Machines Infected in Targeted Attack on Saudi Aramco, The Register, http://www.theregister.co.uk/2012/08/30/rasgas_malware_outbreak/

58. Shamoon Virus Targets Energy Sector Infrastructure, BBC, http://www.bbc.com/news/technology-19293797

59. More Dangerous Attacks Against Major Energy Providers: Mystery Virus Attack Blows Qatari Gas Giant RasGas Offline, Cyberseecure, http://cyberseecure.com/2012/08/mystery-virus-attack-blows-qatari-gas-giant-rasgas-offline-the-register/

60. U.S. Senator Blames Iran for Cyber Attacks on Banks, Naked Security, http://nakedsecurity.sophos.com/2012/09/26/us-iran-banks/

61. Cyber Attacks on U.S. Banks Expose Computer Vulnerability, Bloomberg, http://www.bloomberg.com/news/2012-09-28/cyber-attacks-on-u-s-banks-expose-computer-vulnerability.html

62. Taxonomy of Malware Polymorphism, http://www.foocodechu.com/?q=node/54

63. European Aeronautical Supplier's Website Infected With "State-Sponsored" Zero-Day Exploit], http://nakedsecurity.sophos.com/2012/06/20/aeronautical-state-sponsored-exploit/

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

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

Australia and New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales:
Tel : +65 62244168
Email : salesasia@sophos.co

Boston, USA | Oxford, UK