SOPHOS

Security made simple.

Security Threat Report 2014
Smarter, Shadier, Stealthier Malware

Contents

To find additional resources and
tools referenced in the report, visit

sophos.com/threatreport

Foreword

Reflecting on the security and threat landscape of 2013, one trend that stands out is the growing ability of malware authors to camouflage their attacks. Widespread dissemination of advanced botnet and exploit kit source code allows more malware authors to create innovative and diverse new attacks.

Cybercriminals have started to leverage online marketing as a way to promote and sell their services on the black market. In 2012, the Blackhole exploit kit broke new ground. But in 2013, Blackhole was replaced by several new exploit kits that grew out of it, borrowing some of its code. The resulting botnets are responsible for a sharp increase in ransomware attacks, with Cryptolocker being the prime malice.

Modern malware is all about stealth. Advanced persistent threats (APTs), one of the most vicious examples of a stealth threat, precisely target individuals, businesses, governments and their data. APTs are a sophisticated weapon to carry out targeted missions in cyber space. Data leaks—including espionage and exposure of corporate data—was a primary theme this past year.

APT attacks in 2013 were well-planned and well-funded; carried out by highly-motivated, technologically advanced, and skilled adversaries. Even after successfully accomplishing the mission, the APT continues to live on to gather additional information. Defending against the stealthy and persistent nature of APTs is a complex undertaking, and requires a coordinated approach on the systems as well as the network level.

Security is no longer a "nice to have," but a must-have. Businesses and governments rightfully concerned about privacy and protecting sensitive data now have to be more aware of troublesome security issues that could be found in critical infrastructure systems. As we fly in airplanes,

draw cash from a nearby ATM, or rely on a steady supply of electricity and water, we can no longer assume the security of these systems. Incidents of attacks on these critical network infrastructure and control systems demonstrate vulnerabilities in the essential infrastructure of our society. Systems including the smart grid infrastructure could become more of a focus for cybercriminals in the coming year.

The growing popularity of the "Internet of Things" (e.g., mobile devices, applications, social networks, and interconnected gadgets and devices) makes the threat landscape a moving target. New threats arise with emerging technologies like near field communications (NFC) being integrated into mobile platforms. Innovative uses of GPS services to connect our digital and physical lives present new opportunities for cybercriminals to compromise our security and privacy.

Such systems could yield attacks that have a very personal impact on each of us. In 2014 we need to start watching not just the evolution of existing attacks, but new types emerging that we haven't previously dealt with.

Best wishes,

Gerhard Eschelbeck
CTO, Sophos
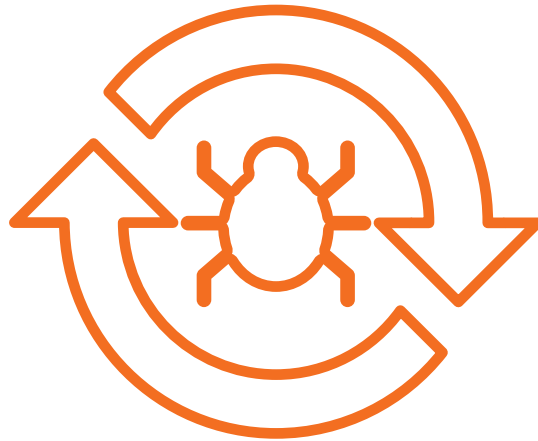
Introduction: Malware Evolves in 2013

Since our last Security Threat Report, malware and related IT security threats have grown and matured, and the developers and publishers of malicious code and websites have become far more creative in camouflaging their work.

In 2013, botnet and exploit kit innovations that were once restricted to the cutting edge have proliferated, as new malware authors learn from the experiences and released source code of their predecessors. Cybercriminals have become more adept at eluding identification, relying more heavily on cryptography and increasingly placing their servers in the darknet—closed, anonymous areas of the Internet designed to resist surveillance.

As users continue to focus on mobile devices and web services, so have malware authors. Android attacks grew in complexity and maturity this year; and well-hidden attacks like Darkleech placed thousands of web servers under malicious control. Meanwhile, legacy Windows users are bracing for Microsoft's April 8, 2014 deadline to end security updates for Windows XP and Office 2003—and wondering what dangerous "zero-day-forever" attacks may follow it.

Like others in the security industry, at Sophos we're observing more targeted threats aimed at specific companies, industries, or government agencies. In certain cases, threats targeted at financial accounts and transactions—which were once limited to Eastern Europe—have begun to appear more widely.

Some threats continue to be cyclical, returning for encores after fading for several years. For example, we saw the return of pump-and-dump email stock scams that had been nearly wiped out by the U.S. Securities and Exchange Commission several years ago.

In 2013 we also saw a vicious new version of ransomware called Cryptolocker. While ransomware has been around for nearly a quarter-century, the latest version uses very strong encryption to make users' files inaccessible and extort cash from them.

Fortunately, as a few data points will attest, the news wasn't all bad. The apparent creator of the Blackhole exploit kit—a global scourge in 2012—was arrested in October: evidence of progress in holding criminal malware organizations to account. Google made progress in 2013 in securing its Android platform from a technical standpoint, and in tightening its rules to restrict many aggressive potentially unwanted apps.

Meanwhile, the advanced researchers at our worldwide SophosLabs are pioneering important new approaches to detection and remediation, leveraging today's most powerful cloud and big data technologies.

Whether you're a large or small business, a school or government agency, or an individual user, our shared battle against malware continues. And so does our commitment to keeping you armed and protected.
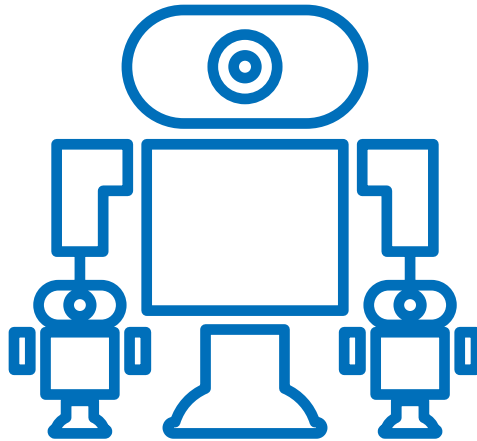
Botnets Grow in Size and Stealth

In the past 12 months, botnets have become more widespread, resilient and camouflaged—and they seem to be finding some dangerous new targets.

Botnet source code has traditionally been tightly protected by its owners. Even when cybercriminals choose to retire from running botnets, they can often sell their code at high prices. But in recent years, working botnet source code has been leaked. This allows imitators to create their own new botnets, and then evolve them to behave in ways the original coders never imagined.

For instance, the leaking of Zeus source code a few years ago led others to develop Gameover, which replaces Zeus's traditional centralized command and control (C&C) link with a peer-to-peer network of infected devices. Gameover added backup communications mechanisms; made greater use of encryption; and gave the botmasters more flexibility in setting rules for the botnet's behavior such as the ability to participate in widespread DDoS (distributed denial-of-service) attacks.[1]

Botnets are more resilient

Botnets are now integrating multiple backup forms of command and control. For example, if a botnet-infected client such as Gameover can't connect to addresses of other infected machines on the network, it runs built-in "domain generation" algorithms. If these algorithms discover even one of the new C&C servers that have been established, the client can restore its active role on the botnet.[2]

Botnet operators are also faster and more effective at responding to countermeasures. One antivirus company took control of part of the ZeroAccess botnet, redirecting traffic from 500,000 infected clients to a server controlled by the antivirus company (what we call sinkholing).[3] In response, working with affiliate networks, the botnet's owners quickly ramped up the number of new droppers they were placing on clients. Within weeks, they had replaced those that were lost—and the new versions aren't vulnerable to the same countermeasure.

Botnets delivering more dangerous ransomware

As users grow more resistant to fake alerts and antivirus scams, more botnets are delivering ransomware instead. Now, users are faced with an absolute demand to pay exorbitant sums in order to restore access to their own data.

Perhaps the most dangerous and widespread current example is Cryptolocker. This ransomware adds itself to the list of Windows programs that run at startup, tracks down an infected server, uploads a small ID file from your computer, retrieves a public key from that server (which stores a matching private key), and then encrypts all the data and image files it can find on your computer.

Once your data has been encrypted by the bad guys, the only way to retrieve it is with the private key stored on their server—for which you have to pay the criminals (which we do not recommend).[4]

While Cryptolocker is sometimes delivered through email spam, it often arrives through botnets that have already infected you. In those cases, the bots are simply responding to an upgrade command that allows the crooks to update, replace, or add to the malware they've already dropped onto your PC—and you won't know until it's too late.[5]

Banking malware botnets appear to be growing

The source code of Carberp, a banking-oriented, credential-stealing botnet kit used to steal over $250 million from financial institutions and their customers, was leaked in mid-2013.[6] Long centered in Russia, we have recently seen evidence of Carberp activity worldwide, and elements of the leaked software are beginning to appear in other botnets. These include code based on Power Loader, which includes some of the most sophisticated techniques yet created to avoid detection while dropping malware onto a computer.7

Meanwhile, throughout the UK and Europe, many users have recently encountered Shylock/Caphaw, botnet-delivered financial malware that specifically targets customers of many leading global financial institutions, from Barclays and Bank of America to Capital One, Citi Private Bank, and Wells Fargo.[8]

2013 ZeroAccess Trend: Damaged by sinkholing, but rebounded rapidly

Sinkholing by antivirus companies dramatically reduced the number of ZeroAccess infected endpoints detected by Sophos in July and August 2013. But the owners of ZeroAccess responded aggressively, and by September, we were identifying more infected endpoints than ever.

Source: SophosLabs

5
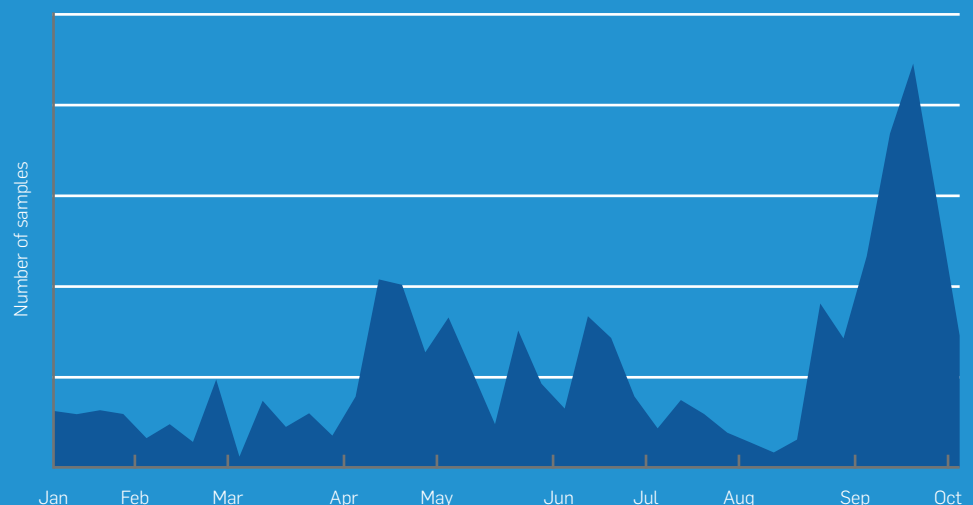
Botnets are more evasive

On some botnets, the first C&C check-in address an infected client tries to contact isn't part of a botnet: it's a legitimate (but compromised) domain that can't conveniently be blocked.

Often, the botnet client's first check-in is now a lightweight PPP server (a type of remote access server) in proxy mode, which in turn sends the connection somewhere else. When you target the first server for takedown, all you've disabled is a proxy: you haven't reached the botnet's actual command center.

Botnets are increasingly relying on the "darknet"

Botnets increasingly use hidden networks such as Tor that are designed to resist surveillance.[9] Tor has gained publicity as a key tool used by Wikileaks and others to protect their sources; and as host for the Silk Road online black market recently accused of facilitating illegal transactions.

Botnets can store C&C servers as hidden services on the Tor network, making them far more difficult to track down. Enterprises often respond by making an executive decision that their employees should not use Tor, and using application control technology to prevent use of the Tor browser client software.
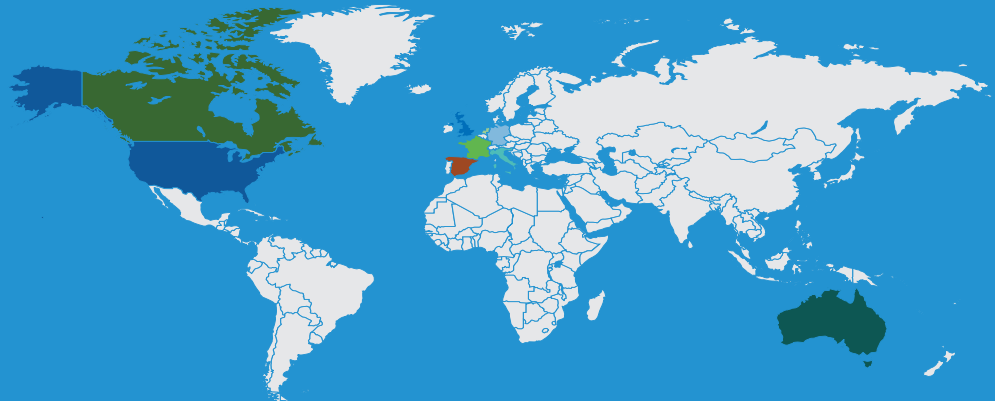
ZeroAccess Detections by Country

By October 2013, ZeroAccess controlled thousands of endpoints throughout the U.S. and UK, and it was widely detected in Germany, Australia and Italy.

Unique Endpoints

United States	6,754
United Kingdom	1,625
Germany	747
Australia	622
Italy	458
Canada	360
France	340
Netherlands	170
Spain	110
Other	1,014

Source: SophosLabs

Botnet Bitcoin Mining: Another malware revenue stream

Botnet operators are constantly seeking new revenue streams. Bitcoin mining made big financial gains in 2013. Bitcoins are a purely digital currency not supported by any government. While the value of a bitcoin has fluctuated significantly, in recent months it typically ranged between $150 and $200 USD.[10]

New bitcoins are created by solving complex math problems that require massive computer processing power—the kind of power that huge global botnets can harness.

So, from May 2012 until February 2013, and then for three weeks in April 2013, infected clients on the ZeroAccess botnet were enslaved to mine new bitcoins.[11]

Even though the value of bitcoins rose dramatically during that period, ZeroAccess ultimately disabled this functionality. Why? We're not sure. Perhaps it was attracting too much attention. Perhaps they weren't making as much revenue as they could through click fraud. Some observers say that new, custom bitcoin-mining hardware is far more effective at the job than distributed botnets.[12]

While ZeroAccess is no longer mining bitcoins, other botnet owners haven't given up the dream. Leading security researcher Brian Krebs discovered the Russian FeodalCash botnet ramping up its bitcoin mining operations in May 2013.[13]

Android Malware: Mutating and Getting Smarter

Android malware continues to grow and evolve, following paths first blazed by Windows. But there is progress to report in securing the platform.

Since we first detected Android malware in August 2010, we have recorded well over 300 malware families. And we have seen the Android malware ecosystem follow in many of the paths first established years ago by Windows malware.

Sophisticated at avoiding detection and removal
Recently, we have seen great innovation in how Android malware seeks to avoid and counter detection methods. Ginmaster is a case in point. First discovered in China in August 2011, this Trojanized program is injected into many legitimate apps that are also distributed through third-party markets.

In 2012, Ginmaster began resisting detection by obfuscating class names, encrypting URLs and C&C instructions, and moving towards the polymorphism techniques that have become commonplace in Windows malware. In 2013, Ginmaster's developers implemented far more complex and subtle obfuscation and encryption, making this malware harder to detect or reverse engineer.[14] Meanwhile, with each quarter since early 2012, we have seen a steady growth in detections of Ginmaster, reaching more than 4,700 samples between February and April 2013.

New Android botnets
Recently, reports surfaced of a large-scale botnet controlling Android devices in much the same way botnets have controlled PCs. This botnet, which Sophos detects as Andr/GGSmart-A, thus far seems limited to China. It uses centralized command and control to instruct all of the mobile devices it has infected; for example, to send premium SMS messages that will be charged to the device owner. Unlike typical Android attacks, it can change and control premium SMS numbers, content, and even affiliate schemes across its entire large network. This makes it better organized, and potentially more dangerous, than much of the Android malware we've seen before.[15]

Ransomware comes to Android
Ransomware has a long and sordid history—the first versions were detected 25 years ago. For those unfamiliar with it, ransomware makes your files or device inaccessible, and then demands a payment to free them. In June 2013, Sophos researcher Rowland Yu discovered the first ransomware attack against Android devices. Called Android Defender, this hybrid fake antivirus/ransomware app demands a $99.99 payment to restore access to your Android device.

Upon starting, Android Defender uses a variety of social engineering tactics and an unusually professional look and feel to repeatedly seek Device Administrator privileges. If given those privileges, it can restrict access to all other applications, making it impossible to make calls, change settings, kill tasks, uninstall apps, or even perform a factory reset. It presents a warning message about infection that is visible on screen, no matter what a user is doing. It can even disable Back/Home buttons and launch on reboot to resist removal. About the only thing it doesn't do is encrypt your content or personal data.[16] Frankly, we'll be surprised if we aren't reporting encrypting attacks in next year's Threat Report.

Bank account theft, delivered via smartphone
In September 2013, we detected a new form of banking malware that combines conventional Man-in-the-Browser attacks against Windows with social engineering designed to compromise Android devices and complete the theft via smartphone. Sometimes called Qadars, we detect it as Andr/Spy-ABN. While we are currently encountering relatively low levels of this malware, it has already targeted French, Dutch and Indian financial institutions.

Most Widespread Android Malware Detections, October 2013
While no single Android malware family is currently dominant, today's most widely detected Android malware is Andr/BBridge-A. This Trojan uses a privilege escalation exploit to install additional malicious apps on your device. Andr/BBridge-A has demonstrated real staying power—it was second on our list of Android infections way back in June 2012.[17]

Andr/BBridge-A	9%	Andr/Adop-A	2%	Andr/SmsSend-BE	2%
Andr/Fakeins-V	6%	Andr/Boxer-D	2%	Andr/MTK-B	2%
Andr/Generic-S	5%	Andr/SmsSend-BY	2%	Other	65%
Andr/Qdplugin-A	3%	Andr/DroidRt-A	2%		

Note: Percentages rounded to nearest whole percent
Source: SophosLabs
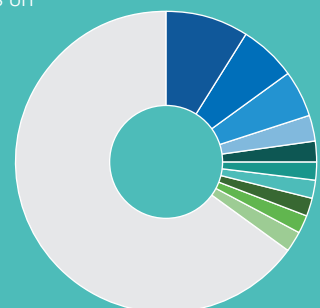
Like its predecessor Zeus, Andr/Spy-ABN begins on the Windows side, injecting code into Internet Explorer to intercept user information before it's encrypted and forwarded to financial institutions. It also captures browser personal certificates and cookies.

Once authenticated, users are told that their bank now requires the use of a new smartphone app as an anti-fraud measure (how ironic). The user is asked for his/her phone number and model, and an SMS is sent, linking to a download of the malicious app. If this isn't bad enough, the injected code even blocks users from accessing their accounts until the smartphone malware has been installed and provides an activation code.[18]
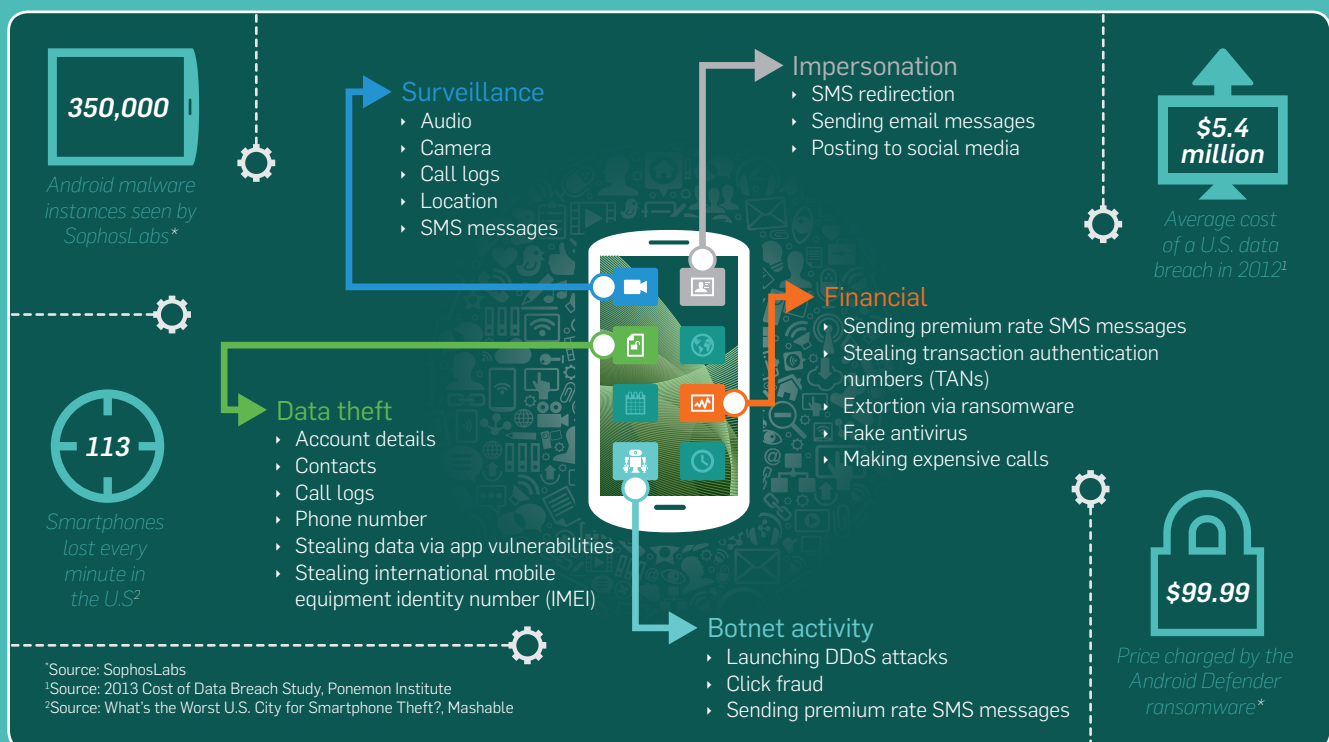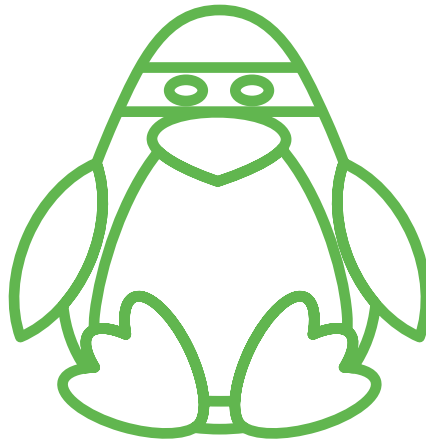
Securing Android

We're pleased that Google has taken some significant steps to further secure the Android platform in recent months. First, Android 4.3 eliminates automatic app downloads that existed in previous versions. Second, Google has tightened its Developer's Agreement, especially as it relates to potentially unwanted apps (PUAs), which aren't unmistakably malware but tend to behave in ways far more intrusive than most users desire.

Google has identified several app and ad framework behaviors that will no longer be permitted. For example, developers can no longer place third-party advertising and links on the home screen, change the browser home page, or use the system notification area for purposes unrelated to their useful functionality.[19]

Anatomy of a Hacked Mobile Device: How a hacker can profit from your smartphone

Your Android smartphone may look innocent. But when compromised by malware, it can illegally watch and impersonate you, participate in dangerous botnet activities, capture your personal data, and even steal your money.[20]

350,000
Android malware instances seen by SophosLabs*

113
Smartphones lost every minute in the U.S[2]

Surveillance
› Audio
› Camera
› Call logs
› Location
› SMS messages

Data theft
› Account details
› Contacts
› Call logs
› Phone number
› Stealing data via app vulnerabilities
› Stealing international mobile equipment identity number (IMEI)

Impersonation
› SMS redirection
› Sending email messages
› Posting to social media

Financial
› Sending premium rate SMS messages
› Stealing transaction authentication numbers (TANs)
› Extortion via ransomware
› Fake antivirus
› Making expensive calls

Botnet activity
› Launching DDoS attacks
› Click fraud
› Sending premium rate SMS messages

$5.4 million
Average cost of a U.S. data breach in 2012[1]

$99.99
Price charged by the Android Defender ransomware*

*Source: SophosLabs
[1]Source: 2013 Cost of Data Breach Study, Ponemon Institute
[2]Source: What's the Worst U.S. City for Smartphone Theft?, Mashable

Linux: Pivotal Technology, Attracting Criminals

Linux is a targeted platform because Linux servers are so widely used to run websites and deliver web content.

While Linux sees a small fraction of the volume of malware targeted at Windows or Android, we see a modest but steady stream of malware executables and scripts attacking it. Moreover, we detect large numbers of samples targeting services that are designed to be platform independent, but often run on Linux servers.

For multiple reasons, Linux-based web servers have become obvious targets for criminals seeking to redirect traffic to their crime kits. First, Linux is the underlying operating system running a large percentage of the Internet's web servers—including many of the world's most important, highest-volume, always-connected websites. Second, Linux servers are widely assumed to be safer than other operating systems, so they are sometimes overlooked as targets for infection. This means an infected Linux server may remain infected for months or years, offering exceptional return on investment to criminal organizations.

As a result, our research shows that the substantial majority of infected servers redirecting traffic to crime kit landing pages are in fact Linux servers. Therefore, even though the volume of malware running on Linux is smaller, malware infection should be a serious concern for all Linux admins.

We currently identify tens of thousands of suspicious samples of PHP code (a server-side scripting language commonly used on websites) running on Linux servers every month— even though malware authors are going to great lengths to obfuscate their PHP scripts to avoid detection, sometimes even obfuscating the same sample to a depth of more than 50 levels.

We see large numbers of malicious PHP scripts designed to make Linux servers operate as nodes in a larger traffic distribution system with many of the features of a traditional botnet. This makes it possible for the system to execute other nefarious payloads, such as DDoS attacks. (We focus directly on web server attacks such as Darkleech and Redkit on page 16.)

Compromised PHP scripts often run on vulnerable platforms such as poorly-patched versions of WordPress.[21] For example, in 2013, an exploit was found in the PHP engine running the Plesk content management system. Through a specific post command, malicious actors could potentially gain access to that engine, and run any PHP script they chose.[22]

Of course, as admins add more third-party scripts and services, they widen the attack surface of their Linux systems, making it even more important to apply patches rapidly, and to take an in-depth, layered approach to hardening both the Linux OS and the services running on it.

Often, traditional Linux file servers host malware targeting Windows and other operating systems. Therefore, even if a Linux server is not itself directly infected, it can still infect other devices which receive files from it.

In 2013, for the first time, we also began to detect significant amounts of Android malware on Linux systems. Of course, if a Linux server, scripting host, or web server *is* infected with malware, it is technically straightforward for that malware to detect HTTP requests coming from Android devices, and serve up Android malware accordingly. Wherever Linux systems provide services to Windows or other clients, they should run anti-malware software.
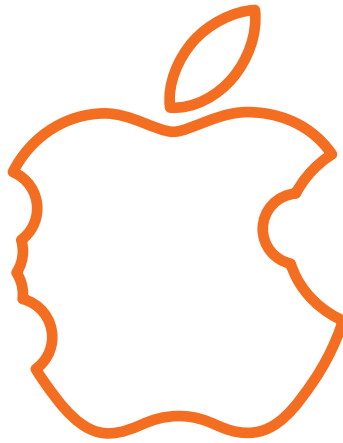
Mac OS X: A Year of Many Small Attacks

While we saw no high-profile attacks against Mac OS X this year, we did detect a steady stream of modest, creative and diverse attacks that make it wise for Mac users to keep their guard up.

Attacks against the Mac OS X platform continued to evolve in 2013, although we saw no huge global attacks comparable to 2012's Flashback. The types of Mac attacks we saw included Trojans, attacks against flaws in the Java platform and Microsoft Word document formats, aggressive browser plugins, malicious JavaScript and Python scripts, and malware signed with an Apple Developer ID to pass through Apple's Gatekeeper protection and trick users into believing it is legitimate.

In February 2013, for example, Reuters reported that Apple employees' Macs were compromised by hackers via yet another zero-day Java vulnerability—the same one that victimized Facebook a week earlier[23] and attacked Microsoft's Mac business unit soon afterwards.[24] Distributed through

a site for software developers, this "watering hole" attack may reflect hackers' recognition that it's sometimes easier to attack companies through smaller sites their employees visit, rather than to attack the companies' well-defended infrastructure directly.

Mac Trojans

Last year, AlienVault and Sophos identified backdoor Trojans that compromised Macs in Asia through boobytrapped Word documents. These Trojans were embedded in documents claiming to discuss human rights abuses in Tibet, triggering speculation that the attack might have come from sources related to the Chinese government.[25]

This February, similar attacks lay waiting in documents about alleged abuses against the Uyghur people in East Turkestan.

Free tool
Sophos Antivirus for Mac Home Edition

All these attacks rely on a Word 2004/2008 vulnerability that Microsoft has long since provided patches for (MS09-027).[26] Whether you're in this part of the world or not, if you're running those versions of Word unpatched, now would be a great time to finally patch them.

If these are in fact targeted attacks, they don't seem to be the only ones. September 2013 saw OSX/Bckdr-RQV, a new backdoor attack that, once installed, transmits a variety of information about the infected machine. According to Intego, some versions attempt to download an image from the Syrian Electronic Army, a group of hackers claimed to be waging cyberwarfare in support of Bashar al-Assad's Syrian government.[27]

Apple Developer ID attacks
By default on most recent versions of OS X, Apple's Gatekeeper tool permits the installation of OS X software retrieved from Apple's own store, or signed with an active Apple Developer ID. But what if malicious software is signed with a working Developer ID? That happened between December 2012 and February 2013, when malicious emails delivered Christmas Card apps signed by Apple Developer "Rajinder Kumar." Before Apple revoked Kumar's ID, some users had launched the OSX/HackBack-A spear phishing payload: malware that uploaded compressed versions of their document files to a remote server.[28]

Christmas Card wasn't this year's only signed piece of Mac malware: this summer, the Python-based Janicab Trojan used the same trick.[29] It is possible that additional unreported attacks based on working Apple Developer IDs exist; even if not, it seems likely that more such attacks will appear.

Adware and ransomware
As with Android, we've also detected more aggressive browser adware plugins this year—software that straddles the line between a PUA and outright malware. Often, these adware plugins either use an aggressive installer (which may even ignore user preferences); camouflage themselves as video codecs the user might need (OSX/FkCodec-A),[30] or otherwise trick the user into accepting installation.

Speaking of web browsers, some unfortunate Mac Safari users encountered a low-rent form of ransomware this year. Like most ransomware, it presents frightening messages falsely portraying themselves as coming from law enforcement, declaring that the user has been caught viewing or retrieving illicit content, and demanding immediate payment of a fine. Unlike this year's worst ransomware (Cryptolocker, which only affects Windows), this Mac malware doesn't encrypt your files: it simply runs JavaScript code that captures your browser, and reappears after a Force Quit. Fortunately, as Malwarebytes has pointed out, this JavaScript can be removed by choosing Reset Safari from the Safari menu—thankfully, with no cost or damage.[31]

Finally, as with Linux servers, Mac OS X servers (and in some cases clients) often host Windows malware that is inactive until it is transferred to a Windows system. Moreover, many users run Windows virtual machines inside OS X using software such as Parallels Desktop. These Windows virtual machines are as susceptible to malware as any other Windows system. Some Mac owners who only work with Windows occasionally may leave them unprotected—they shouldn't.

---

4 Easy Ways to Protect Your Mac
Yes, malware is less prevalent on Macs than on Windows or Android. But some people do get infected, and if you're one of them, the Mac's relative safety will be cold comfort indeed. Fortunately, a few easy steps can help you reduce your risk.

Remove Java from your Mac unless you absolutely need it.
If you can't eliminate Java completely, at least turn it off in your browser, where most of the worst Java threats are. Lately, Apple is making it easier to avoid Java. OS X Lion and later versions don't install it by default; and if you install it anyway, they automatically disable it if you've left it unused for five weeks.[32]

Keep your software patched with up-to-date security fixes.
Hackers are still finding plenty of victims by using attacks that could have been halted years ago. Not to say there aren't newly discovered vulnerabilities to fix, too: Apple's September 2013

OS X 10.8.5 update found and fixed remote execution holes in multiple areas of the system, from CoreGraphics and ImageIO to PHP and QuickTime.[33]

If your version of OS X permits it, limit your Mac to installing apps downloaded from the Mac App Store. Then, you can temporarily relax the restriction when you know you're downloading a legitimate app from a safe location, but the rest of the time, you'll have a valuable added layer of protection.

Run antivirus software on your Macs, if you aren't already.
If you're a consumer running a Mac without antivirus, consider downloading the free Sophos Antivirus for Mac Home Edition, which halts malware threats using the same business-class technology that protects our corporate customers—including threats from a new generation of web-based malware.

Web-Based Malware: More Sophisticated, Diverse and Hidden

Dangerous, difficult-to-detect web server attacks and exploit kits broadened in 2013, leading to more drive-by attacks against vulnerable web clients.

As briefly mentioned above in our discussion of Linux malware, we have seen significant increases in attacks that take the form of malicious Apache modules; these modules, once installed on compromised legitimate sites, dynamically launch drive-by attacks through web browsers with well-known vulnerabilities.

Darkleech attacks web servers

The highest profile example this year was Darkleech, which (by one report) had successfully compromised over 40,000 domains and site IPs by May 2013, including 15,000 that month alone. Prominent websites including the Los Angeles Times and Seagate were reportedly victimized. Darkleech-compromised web servers were responsible for delivering some exceptionally serious malware, including Nymaim ransomware, which encrypted users' files and demanded a $300 payment to provide the key.[34] In our research, 93% of Darkleech infected sites were running Apache.[35]

In March 2013, Darkleech and related attacks were the most prevalent web threat detected on customer endpoints and web appliances, accounting for almost 30% of all detected web threats.

Some of these attacks have also been carefully designed to make them exceptionally difficult to reproduce. For example, they might only be triggered one time out of ten, leading suspicious administrators to believe that the problem—if it even exists—is not coming from the local system. Darkleech maintained blacklists to ensure that any specific IP was only sent a malicious redirect once. Many attackers also choose not to inject the redirect when they encounter an IP believed to originate from the security community or a search engine.

Learn more

Choosing a Hosting Provider

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

Five Stages of a Web
Malware Attack

Malware 101

Web server attacks highlight the need for closer relationships between security and hosting firms to gain greater visibility into complex and subtle attacks like Darkleech. From a technical standpoint, these attacks are already exceptionally difficult to detect. We've worked closely with several affected hosting providers to help them clean their servers. But, due to the low-margin nature of the hosting business, when some hosting providers discover an infected server, they often simply rebuild a new virtual server instance, rather than diagnosing what took place. Since neither they nor their security partners understand what happened, the new instances often become rapidly infected as well.

Customers should ask what procedures their host providers follow in the case of infection, and specifically, what providers do to avoid reinfection.

More malvertising

Malvertising is malicious advertising delivered through legitimate online ad networks and websites. It's been around for years, but in 2013, we saw more of it—some arriving through extremely prominent sites such as YouTube.

These days, malvertising often takes the form of malicious Flash content. If a user clicks on a Flash advertisement, he or she may be redirected to a malicious site via ActionScript code. An excellent example is the recent Troj/SWFRed-D Trojan. Widely encountered in YouTube ads during 2013, this Trojan redirects users to the Styx exploit kit—helping to account for Styx's high prevalence of late (see chart below).

In certain cases, Flash users can be infected without even being redirected, because the Flash ad contains exploit code targeted at flaws in the client's own Flash Player.

Beyond Blackhole: A world of exploit kits

Last year's Threat Report included extensive coverage of Blackhole, a pioneering pre-packaged exploit kit that made it far easier for malware authors to deliver virtually any payload they desired. Blackhole is still around: in fact, it's utilized in the Darkleech attacks discussed above. But Blackhole is no longer unique.

Even without reverse engineering Blackhole, several groups have created powerful new exploit kits that build on its innovations. In our most recent research, Blackhole was only eighth in prevalence—and, with the October 2013 arrest of Blackhole's alleged lead author, Paunch,[36] it may fade even further. In an example of raw market forces at work, Paunch's arrest reportedly led one of his competitors, Neutrino, to immediately increase prices.[37]

Exploit Kits: Blackhole falls behind improved models

In 2012, Blackhole was the dominant exploit kit worldwide, but in 2013, newer kits such as Neutrino and Redkit became far more prevalent.

○ Neutrino	24%	◉ SweetOrange	11%	○ Nuclear	4%
○ Unknown kit	21%	○ Styx	10%	○ Blackhole/Cool	3%
○ Redkit	19%	○ Glazunov/Sibhost	5%	● Other	3%

Note: Percentages rounded to nearest whole percent
Source: SophosLabs
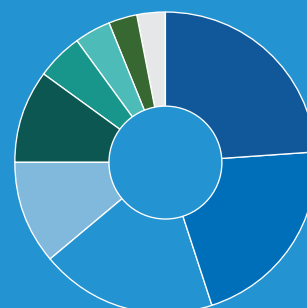
Learn more

Preventing website compromises

Rise of Redkit

Blackhole targets flaws in Java, Adobe PDF and Flash, but many new kits find plenty of fertile ground by simply focusing on Java. One leading example is Redkit, which targets legitimate websites, was used in the February 2013 NBC website hack,[38] and was implicated in spam campaigns that followed the Boston Marathon bombings. By July 2013, it had become the most prevalent exploit kit reported, accounting for 42% of exploit kit detections that month.

Like conventional drive-by downloads, Redkit redirects users from a legitimate site to a malicious exploit site. However, Redkit first redirects to another legitimate, but compromised server. Then, in a second-stage redirect, it bounces the victim to a compromised .htm or .html landing page, from where it delivers malicious content in the form of a Java JAR file (a file format often used to distribute Java applets).

From the victim's standpoint, the malicious content is delivered from the compromised web server used in the second-stage redirect. But, to make Redkit even harder to detect, the content is never stored there. Instead, Redkit's compromised web servers run a PHP shell, which connects to a remote Redkit command and control server. This shell updates its list of compromised sites every hour, handles bouncing victims to the right locations, and ensures that the most current malicious content is delivered from its real source.[39]

Exploit Pack Payloads, June 2013: Exploit kits can carry just about anything—here's what they do carry

Exploit kits are designed to carry a wide range of payloads: as of June 2013, ransomware and the ZeroAccess botnet are the most prevalent.

○ Ransomware	29%	○ Karagany	4%	● Tobfy	1%
○ ZeroAccess	24%	○ FakeAV	4%	○ Tranwos	1%
○ Fareit	7%	○ Simda	2%	● Andromeda	1%
● Moure	7%	○ Dofoil	2%	● Other	5%
○ Shylock	5%	● Medfos	2%		
○ Zbot	4%	● Redyms	2%		

Note: Percentages rounded to nearest whole percent
Source: SophosLabs
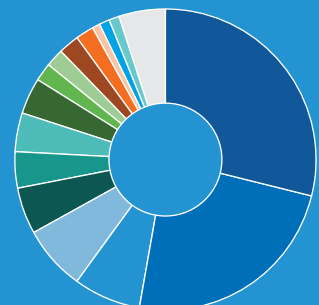
Redkit adopts certain attributes of botnets to control web servers that may each interact with thousands (or even millions) of users. Since these web servers run 24/7 and reach so many users, they are extremely valuable to those who wish to operate DDoS attacks or deliver malware in especially large volumes.

But Redkit isn't the only new exploit kit targeting web servers. We've identified Glazunov at hosting providers all over the world. As the chart on page 15 shows, Glazunov was responsible for 5.47% of all exploit kit detections during the third quarter of 2013. This exploit kit has become notorious for delivering dangerous ransomware. Two other emerging exploit kits, Sibhost and Flimkit, are similar enough that it is possible they come from the same source.

Zbot Spreading Across the Globe

The widespread Zbot exploit kit payload spread throughout the U.S., Europe and Australia in 2013, with 31% of detections in the U.S., another 23% in the UK, and 12% of detections in Italy.

Unique Endpoints

○ United States	2,322
○ United Kingdom	1,749
○ Italy	884
● Germany	693
○ Australia	365
○ France	188
○ Thailand	156
○ Canada	144
○ Netherlands	135
● Singapore	84
● Other	795
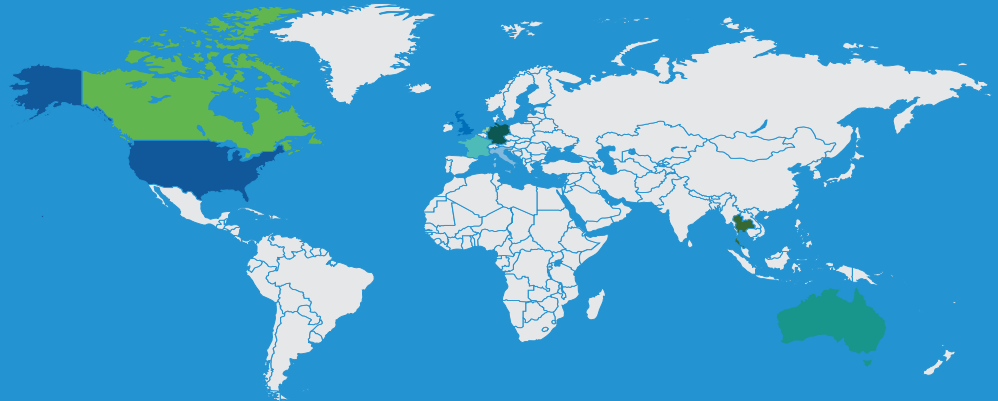
Source: SophosLabs

Tips for Protecting Your Web Server and Clients

Rely on layered protection. Combine up-to-date malware detection with web filtering and runtime detection/host intrusion prevention.

Patch everything, and do it fast. While zero-day attacks get much of the publicity, the vast majority of attacks rely on older vulnerabilities you really should have patched by now.

Limit or eliminate Java on the client. In 2013, many botnet and exploit kit authors refocused their efforts away from Flash and PDF, to specialize in Java. That's where they see the greatest vulnerabilities—which means you should again consider whether you really still need Java on your clients.

Reduce attack surfaces by avoiding or removing unnecessary site plugins, for example, WordPress plugins you aren't using.

Protect your website credentials. Use unique passwords, and be absolutely sure you've changed any default admin passwords.

Targeted Threats to Your Financial Accounts

We are seeing more persistent, targeted attacks—and many seem to be aimed at compromising financial accounts.

While we can't quantify the increase, SophosLabs has been observing more persistent attacks that seem to be targeted at specific companies or institutions, including organizations not previously seen as prime targets. Increasingly, these attacks appear to be aimed at compromising financial accounts, indicating the interest of traditional money-stealing cybercriminals in delivery methods previously used in advanced persistent threat (APT) attacks.

A wolf in sheep's clothing: Plugx, Blame and Simbot

Some targeted attacks try to camouflage themselves as legitimate applications. In particular, we are seeing dangerous certificate-stealing attacks, which use clean, signed components from the Windows OS or third-party vendors in order to load malicious components. The malicious code is then executed by a trusted process, so if a firewall sees data traffic headed outbound, it may conclude that the traffic is legitimate.

Sophos Principal Researcher Gabor Szappanos recently presented new insights on these targeted attacks, describing how they persist undetected for months or years by minimizing system impact, keeping nearly everything in encrypted form, and closely aligning with clean applications. These techniques point the way toward an era when attacks will be even harder to uncover.[40]

Plugx, for example, relies extensively on abusing digitally-signed clean applications. It makes use of Windows' well-known DLL load order vulnerability, dropping the malicious library next to the application. When the application is executed, it loads the malware DLL from the current folder, instead of the clean DLL located in the system folder.[41] This vulnerability reflects a design decision made many years ago; if Microsoft were to change it, many legitimate applications would likely break.[42] Therefore, it seems likely that we will be coping with this vulnerability for a long time to come.

Another specimen, Blame, hides its malicious content deep within a DLL compiled from various open source projects. One of these is the widely-used LAME MP3 encoder, which serves as a decoy, adding enough clean code to hide the malicious code.

A third specimen, Simbot, defines the new BYOT (bring your own target) attack model. It conveniently carries a clean but vulnerable application, which is started with an extremely long command line. This leads to execution of a malicious shellcode, which decrypts and loads the main payload.

While exploiting vulnerable applications is not a new tactic, Simbot is unusual in using it during each startup on already infected systems to ensure that only a clean application is executed, and that malicious code is only executed via the exploit. By bringing the application along with it, Simbot need not depend on the application already being installed on the system, and need not care if the vulnerability was fixed in a later version of the application. Simbot's approach leaves almost no trace behind.
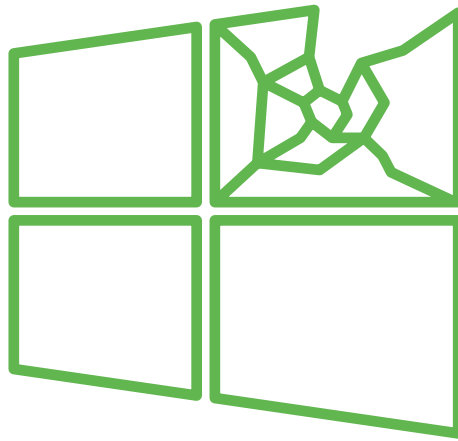
Windows: The Growing Risk of Unpatched Systems

Starting in April 2014, no new patches will be available for Windows XP and Office 2003. Meanwhile, Windows patching has emerged as a significant issue in specialized markets such as point-of-sale and medical equipment.

Android and the web get well-deserved attention these days. It's easy to forget that well over a billion computers still run Windows. While the automated Microsoft Update tool keeps many of these systems patched and up to date, significant and worrisome gaps exist. In this section, we'll focus on three: Microsoft's impending abandonment of support for Windows XP and Office 2003; unpatched or unpatchable point-of-sale (POS) systems; and the widespread presence of malware on unpatched medical equipment running diverse versions of Windows.

According to NetMarketShare, as of September 2013, more than 31% of all PCs were still running Windows XP,[43] the hugely popular version first introduced in 2001. Microsoft has repeatedly reiterated that it will stop providing support and security updates for Windows XP on April 8, 2014.[44]

If you're running a Windows XP system, or if you're responsible for others who are, that's a serious concern. As Microsoft's own Trustworthy Computing Director notes, some vulnerabilities in newer versions of Windows will be backward-compatible with Windows XP. When Microsoft fixes these vulnerabilities in Windows Vista, Windows 7 or Windows 8, it will inevitably be calling attention to the fact that they are still unpatched in Windows XP.[45]

Windows End of Life affects POS and medical devices

With increased worry about unpatched systems, attention has turned to other categories of devices running Windows, many of which are not reliably or consistently patched. In some cases, these run Windows XP (or even older versions of Windows, such as Windows 2000); for these systems, even organizations that have established appropriate patching procedures will not have patches to apply. In other cases, these devices run newer versions of Windows that are still patchable, but their owners or manufacturers do not adequately provide for patching.

POS systems frequently run Windows to handle credit card and other transactions. Despite industry standards that require rapid application of security patches, some of these systems are updated inconsistently, especially in smaller retail environments without sophisticated IT organizations.[46] Due to Windows XP's popularity and length of life, many POS systems use it. Some of these systems can be updated to newer versions of Windows, but according to leading industry payment consultant Walter Conway, others have only been tested and validated for Windows XP.[47]

The risks are by no means purely theoretical. In December 2012, Visa notified merchants of recent reports of Dexter, malicious Windows malware designed specifically to compromise POS systems, steal magnetic stripe data, and send it to a central command-and-control server.[48]

Distressing Windows security risks have also emerged in medical devices. In June 2013, after extensive publicity, the U.S. Food and Drug Administration identified widespread vulnerabilities in medical devices that are either "infected or disabled by malware," including malware capable of "access[ing] patient data, monitoring systems, and implanted patient devices."[49]

One reason: many manufacturers, whose devices run on Windows and other PC platforms, have failed "to provide timely security software updates and patches." As with POS systems, the failure to apply timely patches on medical devices isn't Microsoft's responsibility. In this case, it is equipment manufacturers who must certify that their systems will work reliably with Microsoft's latest fixes. However, when Microsoft halts Windows XP security updates, even manufacturers who improve their certification processes will no longer have new Windows XP patches to test.

How real is the problem? As MIT Technology Review reported in late 2012, medical equipment is "becoming riddled with malware."[50] At Beth Israel Deaconess Medical Center in Boston, "664 pieces of medical equipment are running on older Windows operating systems that manufacturers will not modify or allow the hospital to change—even to add antivirus software … As a result, [they] are frequently infected with malware, and one or two have to be taken offline each week for cleaning."

Last but not least, it's worth mentioning that Windows XP isn't the only ubiquitous Microsoft product set to lose security updates on April 8, 2014. Microsoft Office 2003 will too. Also still in widespread use, Office 2003 was the last version of Office to rely on Microsoft's old document formats, which are now viewed as insecure even after three Service Packs. Since Office 2003 also runs on Vista and Windows 7, years from now you might be running a fully-patched version of Windows, and still find yourself at risk from a new Office vulnerability.

Spam Reinvents Itself

Yet another year of spam. It isn't glamorous, but the security risk just never goes away.

As long as people send email, the bad guys will probably keep sending spam. Some spam is merely annoying. Other types of spam are connected to financial scams most of us have hopefully learned to ignore. And some spam links to malware that's flat-out dangerous.

A few tactics used by spammers never seem to go away. For example, image-based spam (attempts to sell fake Rolex watches remain a perennial); and spam linked to current events (for example, the April 2013 terrorist attack on the Boston Marathon).

Other forms of spam seem cyclical, falling out of fashion and then re-emerging years later. For instance, in 2013 we saw the revival of classic stock pump-and-dump spam.

Pump-and-dump stock scams return
Pump-and-dump messages promise that a penny stock is about to jump in price. When a few victims buy into the hoax, the senders sell and capture all the profits. Several years ago, pump-and-dump spam accounted for over 50% of all spam on some days, but after a U.S. Securities and Exchange Commission crackdown, it nearly disappeared.

Beginning in early 2013, however, we began to see higher volumes again, appearing in bursts: pump and dump was 1-7% of all spam from January 17-31; 5-15% from February 16-20; and 5-20% through most of March. These messages quieted down until late June. Then, volume soared: through July, August and September we saw daily volumes from 10-20%, with pump and dump accounting for up to 50% of all spam on some days.

You can never be too rich or too thin, as they say. So it's not surprising that the second immense spam campaign we've seen lately is the "greencoffee" health/weight-loss scam. These messages attempt to forge legitimate newsletters, often citing prominent TV physicians such as Dr. Oz for increased credibility. But those who click go to domains registered only for spam calls-to-action that redirect to main sites advertising these products.

Distributed servers and snowshoe spam
Spammers are continually susceptible to having their spambots and servers disrupted. So, like other malware developers, they aggressively seek to hide their tracks.

In 2013, for example, we again saw many spammers utilize snowshoe techniques—which, thankfully, our spam detection filters are generally able to recognize and handle. The term snowshoe spam describes how some spammers distribute their load across a larger surface to keep from sinking, just as snowshoe wearers do.

Snowshoe spammers distribute their spamming across many IP addresses, websites and sub-networks. Some may flood large volumes over a single IP address for a short period; then move on to another IP address, often in the same neighborhood. These strategies attempt to defeat volume-based detection schemes used by large email hosts, and to sneak through loopholes in the U.S. anti-spam law, the CAN-SPAM Act of 2003.[51] In organizations with inadequate filtering, snowshoe spam often makes up the vast majority of junk mail their filters miss.

**Spam Attachments, June 2013: Loading plenty of trouble**
In June 2013, two loaders, Fareit and Andromeda, were the leading forms of malware embedded in spam attachments. Fareit (aka Pony, Ponik) often downloads P2P Zeus, but also collects passwords stored in software such as email and FTP clients. Andromeda downloads other malware such as P2P Zeus, spambots, and ZeroAccess; and sometimes downloads its own modules, in order to infect network shares and portable drives.

Fareit	52%	Donx	4%	DarkComet	1%
Andromeda	17%	Bublik	3%	Banload	1%
Zbot	12%	Ransomware	2%		
Dofoil	8%	DnetBckdr	1%		

Note: Percentages rounded to nearest whole percent
Source: SophosLabs
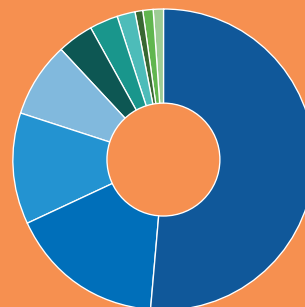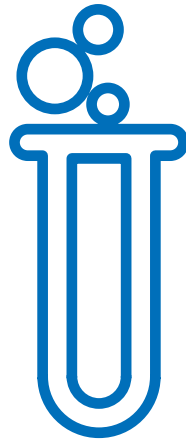
SophosLabs: Staying Ahead of Today's Most Sophisticated Attacks

As malware attacks grow increasingly complex and elusive, security companies must respond with greater intelligence, flexibility and speed. SophosLabs is doing just that.

Once upon a time, anti-malware companies focused primarily on identifying the signatures associated with malicious software. Then, attackers responded with polymorphic attacks that generate unique versions of malware for each computer they infect—thereby rendering static detection far less effective.

Some polymorphic attacks are easy to prevent. For example, email filtering can nearly always prevent attacks delivered through email attachments. But today, the most dangerous attacks are comprised of complex chains of attack components spread widely across the web. And, as this year's report describes, they've adopted powerful new techniques to resist detection.

In response, we rely on several integrated layers of protection. For instance, we invest heavily in detecting and blocking websites that host exploit kits and malicious content. We have built detection layers aimed at detecting several specific exploit kit components, including obfuscated JavaScript redirects, exploited Java JARs, and compromised documents. By itself, no individual layer can be perfect; together, however, they are extremely effective.

But we're learning how to do even better.

For instance, we're focused on context-based detection that combines information about files being downloaded and the sites they're coming from. Standing alone, a file or its source site might not be suspicious enough to flag. Considered together, they often reveal subtle patterns associated with threats—triggering our software to act, without risking false positives.

For the rare occasions when every protection layer fails, we're adding another final layer of defense: runtime detection. We look for signals that malware may be executing. For example, is a program doing something strange that legitimate programs rarely do? We combine this with previous analysis about the executable. A file that might have been only slightly worrisome when it was downloaded might behave in ways that raise our suspicions and lead us to block it immediately.

New versions of our network security appliance use similar techniques to block devices behaving in ways indicating likely malware infection—for example, devices that seem to be under botnet control. Sophos UTM 9.2 not only inspects network packets and identifies endpoints trying to reach illicit domains; it can also recognize malicious configuration files forwarded from botnets to infected endpoints over HTTP.

Of course, since infected C&C web servers and malware change at breakneck speed, Sophos products now provide instant cloud-based updates.

SophosLabs manages a massive amount of data now required to stay ahead of today's attackers. Every day, we capture billions of data points from millions of endpoints all over the world. We've constructed a state-of-the-art big data infrastructure to help us quickly transform that data into knowledge. That involves correlating massive amounts of information coming from protected endpoints and servers to identify emerging attacks; and to collect binaries, URLs and telemetry to help us develop better protection.

For the technical among you, our big data infrastructure is built around Hadoop. This open source software is based on ideas pioneered at Google and Yahoo. It's for companies who have truly colossal amounts of data to analyze right now— folks like Facebook, Twitter, eBay, and yes, Sophos.

Trends to Watch in 2014

By SophosLabs

Major technology developments over the last year—and a series of revelations about the National Security Agency that shook the international security community—made 2013 an interesting year for trend watchers. In highlighting the past year's security events, we've considered some emerging trends we are likely to see in the coming year.

Attacks on corporate and personal data in the cloud

As businesses increasingly rely on various cloud services for managing their customer data, internal project plans and financial assets, we expect to see an emergence of attacks targeting endpoints, mobile devices and credentials as means to gaining access to corporate or personal clouds.

It's hard to predict what form future attacks will take—but we can imagine ransomware taking hostage not just your local documents, but any type of cloud-hosted data. These attacks may not require data encryption and could take the form of blackmail—threats of going public with your confidential data.

Strong password and cloud data access policies are more important than ever. Your security is only as good as your weakest point, in many cases your Windows endpoint and your users' awareness.

APTs meet financially motivated malware

We expect the success of advanced persistent threats (APTs) in carrying out attacks for the purposes of industrial espionage will inspire old-school financial malware gangs to adopt their techniques. In fact, we're already seeing exploit techniques borrowed from APT groups being used for malware distribution.

As security vendors make progress with improving layers of defense, OS security and user awareness, cybercriminals are forced to make bigger financial gains from a smaller number victims. New attacks initiated by traditional malware actors may in the future include components and delivery mechanisms purposely built or customized for a narrower target audience. The line marking the difference between APT and traditional malware will continue to blur in 2014.

Android malware, increasingly complex, seeks out new targets
In 2013 we saw exponential growth in Android malware, not only in terms of the number of unique families and samples, but also the number of devices affected globally.

While we expect that new security features in the Android platform will make a positive change in infection rates over time, their adoption will be slow, leaving most users exposed to simple social engineering attacks. Cybercriminals will continue to explore new avenues for Android malware monetization. Although their options on this platform are more limited than Windows, mobile devices are an attractive launching pad for attacks aimed at social networks and cloud platforms.

Mitigate this risk by enforcing a BYOD (bring your own device) policy that prevents side-loading of mobile apps from unknown sources and mandates anti-malware protection.

Malware diversifies and specializes
The diversity in financially-motivated malware reflects differences between various geographic and economic regions. We already see it through country-specific social engineering techniques, malware monetization options and attack purposes. Malware diversity by targeted audience will likely continue to grow in 2014, especially to differentiate between consumer and business users. We can also expect more specialized attacks in relation to the varying degrees of cyber-defense levels and target value.

Personal data danger from mobile apps and social networks
Mobile security in general will continue to be a hot topic in 2014. The continuing adoption of emerging apps for personal and business communication widens the attack surface, particularly for socially engineered scams and data exfiltration attempts. Your address book and your social connections graph is a treasure for cyber-crooks of all sorts, so be mindful of who you entrust to access it and why. Mobile and web applications control for business users will help mitigate this risk.

Penetrating defenses
In the never-ending fight between the cybercriminals and security vendors, we expect to see new weapons aimed at the latest cyber-defense mechanisms. Reputation services, cloud security databases, whitelisting and sandboxing layers will be attacked in new and sinister ways. We'll see more malware signed with stolen digital signatures, attempts to poison security data and telemetry analytics, new sandbox detection and bypass techniques, and increased use of legitimate tools for malicious purposes.

64-bit malware
With growing adoption of 64-bit operating systems on PCs, we're expecting a growth of malware that is unable to run on 32-bit PCs.

Exploit kits continue to be a primary threat for Windows
Although Microsoft has made technological advances in the Windows operating system that raise the bar for exploit developers, the company is not yet winning the war.

With Windows XP reaching end-of-life after 12 years, it will become a huge target for attackers. Will Windows 7 enjoy such widespread dominance for as many years? How long before we see the majority of endpoints migrating to more recent versions of Windows with improved security features?

Threat delivery that requires user interaction (social engineering) will also continue to be a major infection vector. But malware authors will have to refine their techniques to convince victims to execute the payload, as people become smarter about distinguishing malicious from benign. Mass malware authors will have to make their lures more targeted and more convincing.

Undermining hardware, infrastructure and software at the core
The revelations throughout 2013 of government agency spying and backdoors (not only by governments, but also commercial organizations) showed the world that broad-scale compromise of the core infrastructure we all operate on is not only possible, but happening. We'll need to re-evaluate technologies and trusted parties.

The discoveries so far likely only scratch the surface and we can expect to see many more of these stories in 2014. Most enterprises won't have the resources or skills to go digging for backdoors. But it would be wise to closely monitor the work of security researchers and media outlets for new revelations.

Hacking everything
We have continued to diversify the devices in our environments, and those devices hold sensitive business data. The security ecosystem simply is not as well developed around such devices as the traditional PC environment.

For those wishing to harm us, embedded devices in our homes, offices and even cities represent interesting attack targets. And new electronic currencies and payment techniques make far more than just the credit card worth considering.

While we don't expect attacks against the "Internet of Things" to become widespread in 2014, we do predict an increase in reported vulnerabilities and proof-of-concept exploits.

The Last Word

The creators of malware, exploit kits and botnets became smarter and more aggressive in 2013. They identified new forms of attack, new ways to repurpose older approaches, new targets, and new techniques for hiding their activities.

Defending against these new attacks requires us all to get smarter. At Sophos, we're working around the clock to build more sophisticated detection, delivering real-time updates from the cloud, and helping you secure a new generation of mobile devices—whether you chose those devices, or your BYOD users have chosen them for you.

Whether you're an IT professional, entrepreneur, or individual user, chances are you're getting smarter about security too. You are (or should be) making sure all your systems are protected, whatever conventional or mobile platform they're running on. Shrink attack surfaces by eliminating platforms like Java where you don't need them. Stay up to date with patches, because most attacks are aimed at old vulnerabilities. And do the security basics right (like using strong passwords, and training your users to evade social engineering).

The battle for IT security won't end any time soon. But if you stay focused, apply best practices, judiciously use security technology, and get the right help, you can keep your organization safe. At Sophos, we have the right help to offer— and we are at your service.

Sources

1. ZeuS-P2P Monitoring and Analysis, v2013-06, NASK/CERT Polska, http://www.cert.pl/PDF/2013-06-p2p-rap_en.pdf

2. An Analysis of the Zeus Peer-to-Peer Protocol, Dennis Andriesse and Herbert Bos, VU University Amsterdam, The Netherlands, Technical Report IR-CS-74, rev. May 8, 2013, http://www.few.vu.nl/~da.andriesse/papers/zeus-tech-report-2013.pdf

3. Symantec Uses Vulnerability to Take Out Part of the ZeroAccess Botnet, CSO, http://www.csoonline.com/article/740626/symantec-uses-vulnerability-to-take-out-part-of-the-zeroaccess-botnet

4. CryptoLocker Ransomware - See How It Works, Learn about Prevention, Cleanup and Recovery, Sophos Naked Security, http://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/

5. Destructive Malware "CryptoLocker" on the Loose - Here's What to Do, Sophos Naked Security, 12 October 2013, http://nakedsecurity.sophos.com/2013/10/12/destructive-malware-cryptolocker-on-the-loose/

6. With Carberp Source Code's Release, Security Pros Expect the Worst, CSO Online, 27 June 2013, http://www.csoonline.com/article/735569/with-carberp-source-code-s-release-security-pros-expect-the-worst

7. Carberp: The Never Ending Story, We Live Security, 25 March 2013, http://www.welivesecurity.com/2013/03/25/carberp-the-never-ending-story/

8. Shylock Financial Malware Back and Targeting Two Dozen Major Banks, ThreatPost, 18 September 2013, http://threatpost.com/shylock-financial-malware-back-and-targeting-two-dozen-major-banks

9. Cyber-thieves Blamed for Leap in Tor Dark Net Use, BBC News, 6 September 2013, http://www.bbc.co.uk/news/technology-23984814

10. Bitcoincharts.com, http://bitcoincharts.com/charts/mtgoxUSD#rg60ztgSzm1g10zm2g25zv

11. Back Channels and Bitcoins: ZeroAccess' Secret C&C Communications, James Wyke, Senior Threat Researcher, SophosLabs, Virus Bulletin, October 2013, http://www.sophos.com/en-us/medialibrary/PDFs/technical papers/Wyke-VB2013.pdf

12. The Delicate War Between Bitcoin Miners and Botnet Miners, Red Orbit, 28 March 2013, http://www.redorbit.com/news/technology/1112812519/bitcoin-miners-versus-botnet-miners-032813/

13. Botcoin: Bitcoin Mining by Botnet, Krebs on Security, 18 July 2013, http://krebsonsecurity.com/2013/07/botcoin-bitcoin-mining-by-botnet/

14. GinMaster: A Case Study in Android Malware, Rowland Yu, SophosLabs Australia, Virus Bulletin, October 2013, http://www.virusbtn.com/pdf/conference_slides/2013/Yu-VB2013.pdf

15. Billion Dollar Botnets, Cathal Mullaney, Symantec, presented at Virus Bulletin, October 2013, http://www.virusbtn.com/conference/vb2013/abstracts/Mullaney.xml

16. Hey Android, Are You Frightened of FakeAV plus Ransomware? Rowland Yu, SophosLabs, October 2013

17. Revealed! The Top Five Android Malware Detected in the Wild, Graham Cluley, Sophos Naked Security, 14 June 2012, http://nakedsecurity.sophos.com/2012/06/14/top-five-android-malware/

18. Qadars: A New Banking Malware With a Fraudulent Mobile Application Component, 2 October 2013, http://www.lexsi-leblog.com/cert-en/qadars-new-banking-malware-with-fraudulent-mobile-application-component.html

19. Google Play Developer Program Policies, https://play.google.com/about/developer-content-policy.html

20. Graphic inspired by The Scrap Value of a Hacked PC, Revisited, Krebs On Security, http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

21. CVE Details: WordPress Vulnerabilities, http://www.cvedetails.com/vulnerability-list/vendor_id-2337/product_id-4096/

22. Hacker Publishes Alleged Zero-Day Exploit for Plesk, Parity News, 6 June 2013, http://www.paritynews.com/2013/06/06/1112/hacker-publishes-alleged-zero-day-exploit-for-plesk/

23. Exclusive: Apple, Macs Hit by Hackers Who Targeted Facebook, Reuters, 19 February 2013, http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I0920130219

24. Microsoft Also Victim of Recent Watering Hole Attack, Help Net Security, 25 February 2013, https://www.net-security.org/secworld.php?id=14482

25. Mac Backdoor Trojan Embedded Inside Boobytrapped Word Documents, Sophos Naked Security, 30 March 2012, http://nakedsecurity.sophos.com/2012/03/30/mac-malware-backdoor/

26. Chinese Uyghur Dissidents Targeted by Mac Malware, Ben Weitzenkorn, TechNewsDaily, 15 February 2013, http://www.technewsdaily.com/16937-china-uyghur-attacks.html

27. New Mac Trojan Discovered Related to Syria, Intego, 17 September 2013, http://www.intego.com/mac-security-blog/new-mac-trojan-discovered-related-to-syria/

28. Mac Spyware: OSX/KitM (Kumar in the Mac), F-Secure, 22 May 2013, http://www.f-secure.com/weblog/archives/00002558.html

29. New Signed Malware Called Janicab, http://www.thesafemac.com/new-signed-malware-called-janicab/

30. OSX/FkCodec-A, Detailed Analysis, Sophos, 11 June 2013, https://secure2.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/OSX~FkCodec-A/detailed-analysis.aspx

31. FBI Ransomware Now Targeting Apple's Mac OS X Users, Malwarebytes, 15 July 2013, http://blog.malwarebytes.org/fraud-scam/2013/07/fbi-ransomware-now-targeting-apples-mac-os-x-users/

32. Apple Gets Aggressive - Latest OS X Java Security Update Rips Out Browser Support, Paul Ducklin, Sophos Naked Security, 18 October 2012, http://nakedsecurity.sophos.com/2012/10/18/apple-gets-aggressive-latest-os-x-java-security-update-rips-out-browser-support/

33. Apple Ships OS X 10.8.5 Security Update - Fixes "sudo" Bug At Last, Paul Ducklin, Sophos Naked Security, 13 September 2013, http://nakedsecurity.sophos.com/2013/09/13/apple-ships-os-x-10-8-5-security-update-fixes-sudo-bug-at-last/

34. Rampant Apache Website Attack Hits Visitors With Highly Malicious Software, Ars Technica, 3 July 2013, http://arstechnica.com/security/2013/07/darkleech-infects-40k-apache-site-addresses/

35. Rogue Apache Modules Pushing Iframe Injections Which Drive Traffic to Blackhole Exploit Kit, Fraser Howard, Sophos Naked Security, 5 March 2013, http://nakedsecurity.sophos.com/2013/03/05/rogue-apache-modules-iframe-blackhole-exploit-kit/

36. Blackhole Malware Toolkit Creator 'Paunch' Suspect Arrested, ZDNet, 9 October 2013, http://www.zdnet.com/blackhole-malware-toolkit-creator-paunch-arrested-7000021740/

37. Blackhole Exploit Kit Author Arrested in Russia, ComputerWorld, 8 October 2013, http://www.computerworld.com/s/article/9243061/Blackhole_exploit_kit_author_arrested_in_Russia

38. Lifting the Lid on the Redkit Exploit Kit, Fraser Howard, Sophos Naked Security, 3 May 2013, http://nakedsecurity.sophos.com/2013/05/03/lifting-the-lid-on-the-redkit-exploit-kit-part-1/

39. The Four Seasons of Glazunov: Digging Further into Sibhost and Flimkit, Fraser Howard, Sophos Naked Security, 2 July 2013, http://nakedsecurity.sophos.com/2013/07/02/the-four-seasons-of-glazunov-digging-further-into-sibhost-and-flimkit/

40. Hide and Seek - How Targeted Attacks Hide Behind Clean Applications, Gabor Szappanos, SophosLabs Hungary, October 2013, Virus Bulletin, http://www.virusbtn.com/conference/vb2013/abstracts/LM1-Szappanos.xml

41. Plugx "Malware Factory" Celebrates CVE-2012-0158 Anniversary with Version 6.0, Gabor Szappanos, Principal Researcher, SophosLabs, May 2013, http://sophosnews.files.wordpress.com/2013/05/sophosszappanosplugxmalwarefactoryversion6-rev2.pdf

42. The Windows DLL Loading Security Hole, Dr Dobbs Journal, 9 September 2010, http://www.drdobbs.com/windows/the-windows-dll-loading-security-hole/227400009

43. NetMarketShare, http://www.netmarketshare.com/

44. Windows XP SP3 and Office 2003 Support Ends April 8, 2014, Microsoft, http://www.microsoft.com/en-us/windows/endofsupport.aspx

45. The Risk of Running Windows XP After Support Ends, Tim Rains, Microsoft Security Blog, April 2014, http://blogs.technet.com/b/security/archive/2013/08/15/the-risk-of-running-windows-xp-after-support-ends.aspx

46. Windows XP End of Life Affects PCI Compliance, Credit Card Processing Space, 6 March 2013, http://www.creditcardprocessingspace.com/windows-xp-end-of-life-affects-pci-compliance/

47. Windows XP End-of-Life Could Cripple PCI Compliance, Walter Conway, 6 February 2013, Storefront Backtalk, http://storefrontbacktalk.com/securityfraud/windows-xp-end-of-life-could-cripple-pci-compliance/

48. Dexter Malware Targeting Point-of-Sale (POS) Systems, Visa Data Security Alert, December 2012, http://usa.visa.com/download/merchants/alert-dexter-122012.pdf

49. FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks, U.S. Food and Drug Administration, 13 June 2013, http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm

50. Computer Viruses Are "Rampant" on Medical Devices in Hospitals, MIT Technology Review, 17 October 2012, http://m.technologyreview.com/computing/41511/

51. Following the Tracks: Understanding Snowshoe Spam, Brett Cove, SophosLabs, http://sophosnews.files.wordpress.com/2011/10/vb2011-snowshoe2.pdf

SOPHOS

United Kingdom and Worldwide Sales	North American Sales	Australia and New Zealand Sales	Asia Sales
Tel: +44 (0)8447 671131	Toll Free: 1-866-866-2802	Tel: +61 2 9409 9100	Tel: +65 62244168
Email: sales@sophos.com	Email: nasales@sophos.com	Email: sales@sophos.com.au	Email: salesasia@sophos.com

SOPHOS