McAFEE LABS THREATS REPORT

June 2014

Report

ABOUT McAFEE LABS

McAfee Labs is the world's leading source for threat research, threat intelligence, and cybersecurity thought leadership. With data from millions of sensors across key threats vectors—file, web, message, and network—McAfee Labs delivers real-time threat intelligence, critical analysis, and expert thinking to improve protection and reduce risks.

www.mcafee.com/us/mcafee-labs.aspx

INTRODUCTION

McAfee reports show our commitment to investigating and explaining cyberespionage events.

The Scottish writer Robert Burns wrote "The best laid plans of mice and men go often awry" in his 1785 poem *To A Mouse, On Turning Her Up In Her Nest With The Plough*. More than 200 years later, his observation still holds.

It is our objective to publish the *McAfee Labs Threats Report* as quickly as possible after the end of each quarter. But this quarter was different. As almost every security practitioner knows, the Heartbleed vulnerability was disclosed publically in April, just when we were beginning to write this report. Much of our threat researchers' attention was immediately focused on Heartbleed, both to understand it and to ensure that McAfee technologies were protecting our customers against it. As a result, this report has been delayed. So much for the best laid plans.

We aren't addressing Heartbleed in this report, as it's still too early to fully understand its impact, but watch for our perspective in our next *Threats Report*. Instead, we discuss several topics of interest to many of our customers. Our two mobile malware stories touch on different aspects of this ever-evolving challenge. We also touch on a curious virtual currency mining phenomenon in which the only winners are those selling the pickaxes. And finally, we discuss the decline in new rootkits and why we think that trend is reversing.

We also call your attention to several other significant McAfee reports, all of which focus on cyberespionage. In April, Verizon released the *Verizon 2014 Data Breach Investigations Report*. McAfee partnered with Verizon by contributing information from our *Dissecting Operation Troy* cyberespionage report. Then in early June, we released a commissioned report from the Center for Strategic and International Studies entitled *Net Losses—Estimating the Global Cost of Cybercrime*. All of these reports illustrate the significant investment McAfee has made in becoming the most trusted industry source of cyberespionage knowledge and perspective.

Vincent Weafer, Senior Vice President, McAfee Labs

Follow McAfee Labs

CONTENTS

McAFEE LABS THREATS REPORT
June 2014

This report was prepared and written by:

Benjamin Cruz
Deepak Gupta
Aditya Kapoor
Haifei Li
Charles McFarland
Francisca Moreno
Daisuke Nakajima
François Paget
Craig Schmugar
Rick Simon
Dan Sommer
Bing Sun
James Walter
Adam Wosotowsky
Chong Xu

EXECUTIVE SUMMARY

Cybercriminals have created hundreds of Flappy Bird clones containing malware. Our 300 clone sample uncovered 238 Flappy Bird clones containing malware.

McAfee Labs believes that bot sellers are selling snake oil when they say that botnet operators can profitably mine virtual currencies.

Following a decline in new rootkits since 2011, McAfee Labs believes that the trend will soon reverse.

Through several examples, McAfee Labs makes the point that mobile platform protection is not enough. Mobile app developers need to do a better job to protect their apps and users should be more vigilant when granting app permission requests.

Follow McAfee Labs

Attack of the Flappy Bird clones

This may sound like a fun topic, but it has some serious consequences. The Flappy Bird mobile game enjoyed a meteoric rise in popularity late last year and early this year but was closed down by its author in February. Based on its popularity, enterprising cybercriminals developed hundreds of Flappy Bird clones containing malware. McAfee Labs sampled 300 of those clones and found that almost 80% of them contained malware. Some of the behavior we found includes making calls without the user's permission; sending, recording, and receiving SMS messages; extracting contact data; and tracking geolocation. In the worst cases, the malware gained root access, which allows uninhibited control of anything on the mobile device including confidential business information.

Not a "miner" issue

McAfee Labs has written several reports on virtual currency, including *Digital Laundry*, *Jackpot! Money Laundering Through Online Gambling*, and the *McAfee Labs Threats Report: Third Quarter 2013*. This quarter, we explore a virtual currency topic that has us scratching our heads. We now see malware botnets that include virtual currency–mining capabilities. However, doing the math on virtual currency mining through botnets suggests it's quite unlikely that botnet operators can make more money from botnets by turning on the virtual currency–mining feature. In our view, the only people actually making money from this capability are those who are selling the bot tools.

Rootkits look to rebound

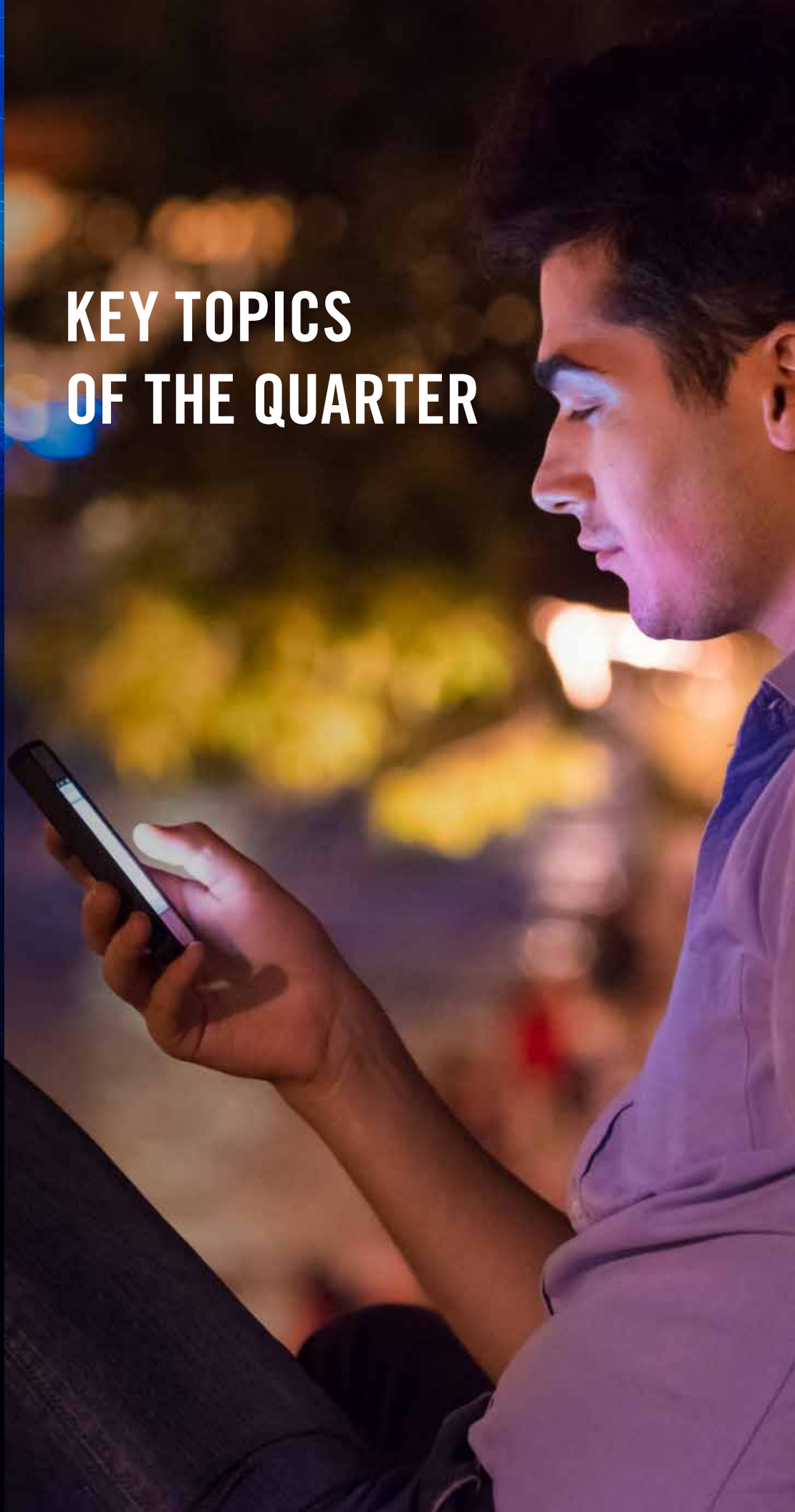
Good news—or so we thought. Since mid-2011, McAfee Labs had seen a decline in the number of new rootkits. In fact, last quarter we saw the lowest number of new rootkits since 2008. It's likely that this decline came from the added protection found in 64-bit microprocessors and their corresponding 64-bit operating systems. However, cybercriminals are ever resourceful, and this quarter we saw a reversal of the downward trend, though it was prompted by a single 32-bit malware family. Attackers have learned how to hijack root-level digital certificates, exploit existing kernel vulnerabilities, and find ways around 64-bit security safeguards. We believe new 64-bit bypass techniques will soon lead to an increase in rootkit-based attacks.

Mobile malware abuses platform vulnerabilities, apps, and services

For this topic, we assembled several vignettes that highlight ways in which malware can abuse mobile device platforms. The first example details how an app offered through the Google Play app store automatically downloads, installs, and launches other apps without a user's permission. In this example, the abusing app did not download malware but profited through a pay-to-download scheme. However, it's an easy leap from there to automatic downloads of malware-laden apps. In a second example, a Trojan exploits a security flaw in a legitimate digital wallet service to steal money. And finally, a third example illustrates how an encryption weakness in the popular messaging app WhatsApp was used to steal conversations and photos. Although that vulnerability has been fixed, it illustrates how attacks will continue to look for weaknesses in mobile platforms.

In Q1 2014 the total malware sample count in the McAfee Labs "zoo" broke the 200 million sample barrier.

KEY TOPICS OF THE QUARTER



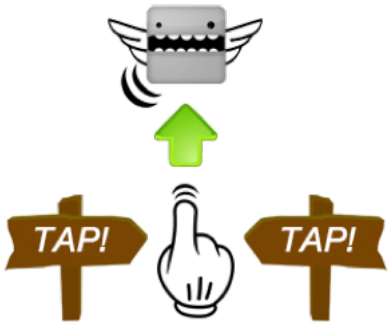
Attack of the Flappy Bird clones

Once again we see that social engineering, combined with the latest "hot game," leads to plentiful malware. The current infestation is a flock of malevolent "Flappy Bird" clones.

The original "Flappy Bird" game was released in mid-2013 on Apple iOS and early this year on Android. The game was a huge success, with more than 50 million downloads, and brought a great deal of notoriety to developer Dong Nguyen before he pulled the app from the marketplace in February.

During the last several *McAfee Labs Threats Reports,* we have reported on the steep rise in mobile malware. The Flappy Bird craze and subsequent malware sweep is a prime example of malware authors taking full advantage of over-the-top user enthusiasm for legitimate apps or games. Malicious Flappy Bird clones existed prior its removal from online marketplaces, but the demand for Flappy Bird–like games only rose after the app was pulled. During the first quarter of 2014, we saw hundreds of Flappy Bird clones emerge, the majority of which were malicious.

The original Flappy Bird game.



A malicious Flappy Bird clone.

Another malicious Flappy Bird clone.

Follow McAfee Labs

Late in the first quarter, McAfee Labs took a sampling of 300 Flappy Bird clones from our mobile malware "zoo." Of those 300 samples, we rated 238 samples as malicious. Considering how quickly these malicious apps popped up, and the number of times they have been downloaded, the situation is startling.

What are these malicious apps doing? Apart from taking advantage of Flappy Bird as a social engineering lure, they pack a lot more functionality than the original game. In fact, they are capable of many questionable, damaging, and invasive behaviors.

When looking at the maliciousness of a mobile application or package, certain behaviors raise more red flags than others. The following example illustrates this: com.touch18.flappybird.app (3113ad96fa1b37acb50922ac34f04352) is one of the many malicious Flappy Bird clones.

The malicious Flappy Bird clone com.touch18.flappybird.app.

Among its malicious behaviors, this clone does the following:

- Makes calls without the user's permission
- Installs additional applications without the user's permission
- Allows an app to monitor incoming SMS messages, and to record or process them (undeclared permission)
- Sends SMS messages without the user's permission
- Extracts SMS messages
- Sends data to a cell number via SMS
- Allows an app to read the user's contacts data (undeclared permission)
- Extracts GPS location (latitude and longitude)
- Reads IMEI number and MAC address and transmits them to third parties (JSON) without user's permission
- Sends user activity data to third-party sites
- Allows an app to call the killBackgroundProcesses(String) (undeclared permission)

A malicious Flappy Bird clone seeking root access.

As we illustrate elsewhere in this report, mobile malware continues its rapid rise in numbers and effectiveness. These devices are easy targets for attackers. We must be diligent and persistently aware of our own behaviors to prevent the installation of malicious code. Mitigation via software controls (antimalware, secure containers, and the like) are just a step in this process. Be aware and in control of where you encounter, acquire, or install apps and games. Strong and safe device "hygiene" and common sense go a long way.

Follow McAfee Labs

Not a 'miner' issue

From the perspective of security and malware research, the business of virtual currencies has taken another interesting step. We now see botnets with various levels of virtual currency–mining functionality. But even if we allow a zero cost for hardware and power (the costs of the bots and their power are borne by the victims), the difficulty level of common mining algorithms and the nonspecialized hardware that the malware infects make this a futile effort. In essence, botnet sellers are selling snake oil when they say that buyers can profitably mine virtual currencies. Further, botnet operators are risking exposure because bot hardware victims are more likely to detect the resource-consuming mining activity.

Financial gain has been the primary motive behind the botnet malware industry for many years. There is money to be made for the authors of malware, kits, and exploits, as well as for those who buy them and create their own botnets.

Recently, an additional factor has come into the picture: the commoditization of virtual currency mining as a core botnet function. We see this functionality being adopted across popular platforms, including mobile. This emergence is very similar to past innovations in bots and malware, such as the rise of distributed denial of service (DDoS) attacks, the persistence of installations, private update mechanisms, and active detection evasion.

Spend some time digging around any underground security forum or marketplace and you will find a myriad of SHA-256 and SCRYPT miner botnets, builders, and cracked versions of commercial builders and kits, along with the usual assortment of DDoS bots, cryptors, and other nefarious services and tools. Some recent examples include EnvyMiner, DeadCow, SovietMiner, JHTTP, Black Puppet, and Aura. These are just a tiny fraction of what exists.

Some examples of builders or services and prices:

- Aura (SHA-256, SCRYPT, SCRYPT-Jane miner). US$50 for a lifetime license
- Black Puppet (Bitcoin). US$10 per month or US$20 lifetime
- HTTP (SHA-256, SCRYPT). US$50 per month or US$200 lifetime
- SovietMiner (SHA-256, SCRYPT). US$15 per month
- DeadCow (SHA-256, SCRYPT). US$15 per month or US$45 lifetime

Many of the most popular miner bots and toolkits have been leaked or cracked, allowing others to use these tools free of license restrictions.

The leaked Chrome Miner app.

Cryptocurrency Hashing Algorithms

SHA-256: The cryptographic hash function for mining is the NIST-standard SHA-256. This is the most complex method. Successful "mining" requires specialized or separate hardware or computing resources (ASICs). Examples: Bitcoin, Namecoin

SCRYPT: A simplified key derivation function used for mining. This method benefits from high-powered GPU-based processing. Examples: Litecoin, Dogecoin, Vertcoin

Follow McAfee Labs

The leaked Aura Miner app.

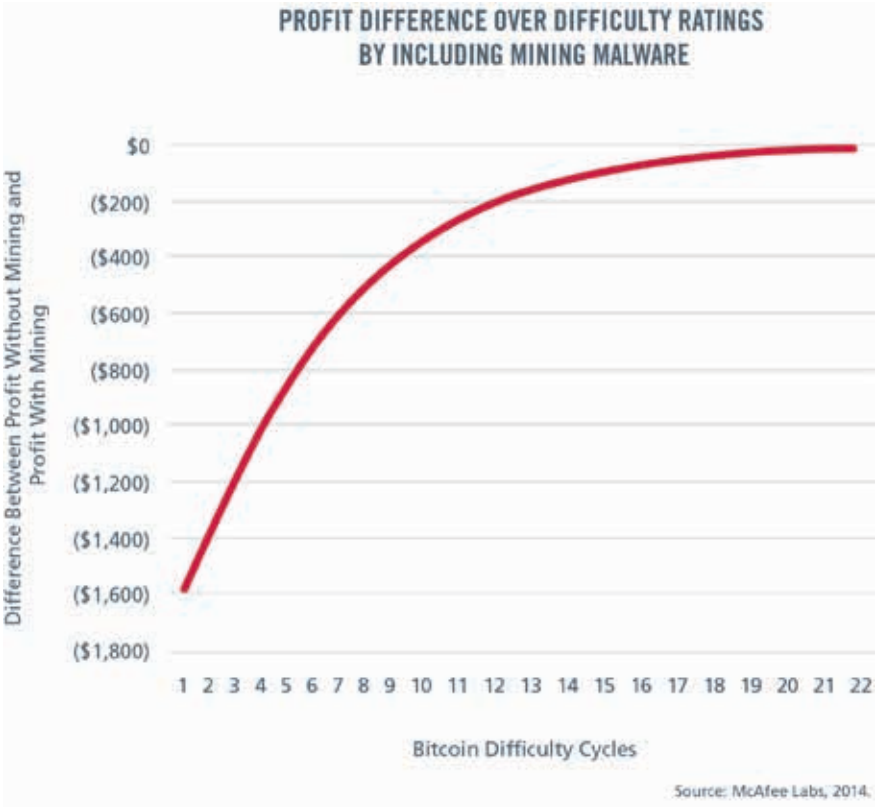
As with most kits and builders, much of the virtual currency–mining functionality is customizable and configurable. This can get as granular as controlling the maximum CPU temperature allowed while mining. GPU/CPU mining is very resource intensive, so to remain somewhat stealthy, the functionality must be throttled. This restriction works against the overall return on investment for these bots, and also adds a much greater and more noticeable presence or footprint of the bot on the infected machines.

This development is interesting in that virtual currency–mining functionality does not increase a botnet operator's profit. That's because virtual currency mining becomes more difficult and resource intensive as more miners are added to the ecosystem. At the current levels of difficulty, it is unlikely that a botnet operator could gain more profit by adding a virtual currency–mining feature to existing attacks.

A number of variables affect the profitability of virtual currency mining, including the rate of increasing difficulty,[1] hash rate,[2] market value of the virtual currency, and miner attrition. Attrition in the botnet ecosystem occurs when the bot malware is detected, or the malware is removed due to its observable presence on the machine.

Botnet operator profit can be calculated by factoring in the average hash rate (across consumer- and business-class GPUs and CPUs), attrition, estimated increase in difficulty, and number of infections, among other variables.

For example, a virtual currency–mining botnet with 10,000 persistent bots, mining at an aggregate average hash rate of 100 megahashes per second, with 5% removed due to detection or mitigation during each difficulty cycle, and the value of Bitcoin at US$500 would result in the following graph:



Follow McAfee Labs

The preceding graph shows the potential difference in profitability between operating a botnet with Bitcoin mining as added functionality and operating the botnet without Bitcoin mining functionality. The profit difference is shown over Bitcoin difficulty cycles, which average about one every two weeks.

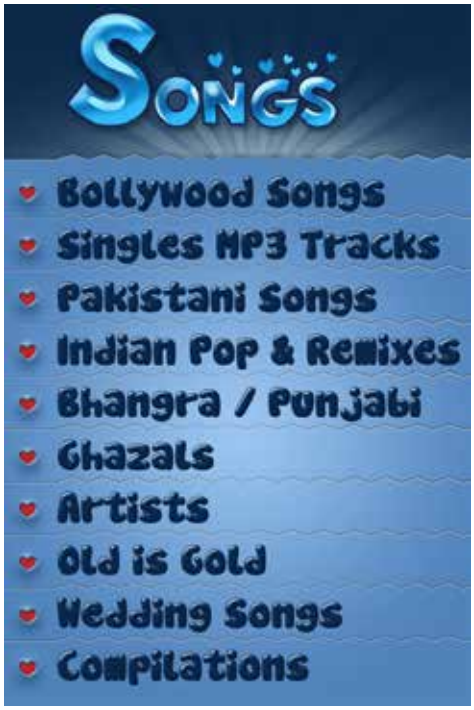
In this example, the addition of virtual currency mining diminishes potential profit through greater bot attrition and time lost by not performing other, more profitable tasks such as stealing passwords or credit card numbers. Further, the graph assumes only a 5% loss of these bots, which is unrealistically low. SCRYPT-based virtual currency mining, such as Litecoin and Dogecoin, suffers from similar problems.

The inability to profit becomes even more perplexing with virtual currency–mining bots running on mobile platforms. Recent examples of mining on Android include Zorenium, BadLepricon, and Songs.

Mobile platforms suffer in two ways. First, their processors are slower than consumer desktop or laptop processors. Second, the attrition rate of mobile platforms is likely to be disproportionately higher. This is due to the limited battery life of mobile platforms and the added risk of hardware failure due to the intense nature of virtual currency mining. Any meaningful return using an average mobile platform is nonexistent unless the botnet has unrealistically low attrition rates.

In a hypothetical example of a 10,000-device botnet, profit without mining is US$11,000.00 while profit with mining is US$11,007.61—just a US$7.61 gain. This assumes an unrealistic attrition rate of 0.25%. A realistic attrition rate of 30% would result in a loss of US$3,265 in potential profit.

Virtual currency mining via botnets has moved into the mainstream. It's a bundled feature in many toolkits and builders across multiple platforms. However, there is a great deal of doubt around the profitability of this practice given the resource requirements of the mining algorithms. Nonetheless, the nefarious malware sellers seem to have plenty of motivation to squeeze every possible ounce of profit out of their efforts.



The Android miner app Songs.

Bitcoin difficulty cycle

Difficulty is the measurement of how much work (processing) is required to generate block chains. By design, Bitcoin difficulty adjusts every 2,016 blocks (around two weeks).

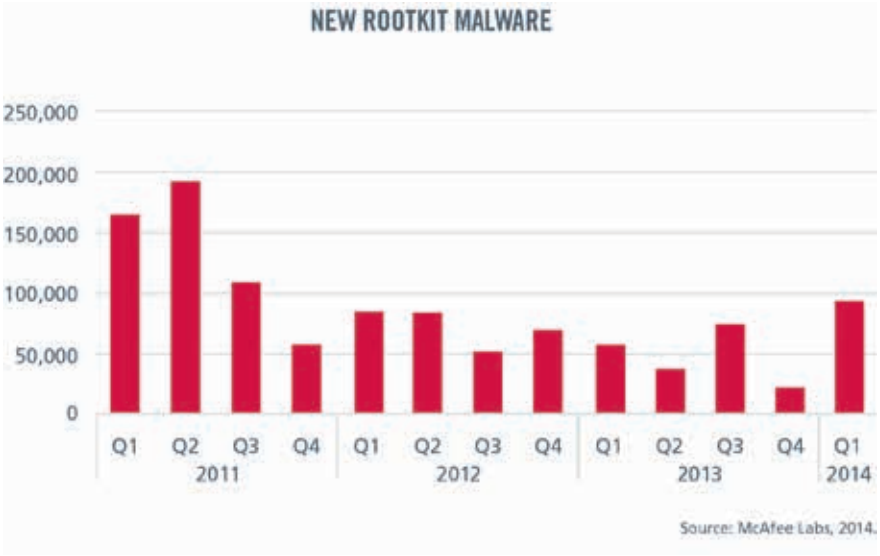
Follow McAfee Labs

Rootkits look to rebound

In early 2011 rootkit malware reached record highs. Since then McAfee Labs has seen a drop to more modest levels, with last quarter's figure the lowest we've tallied since 2008. We attribute the decline to the adoption of 64-bit microprocessors, which make it more difficult to attack the operating system kernel. However, attackers have begun to find ways around 64-bit defenses. This quarter new rootkit infections rose again, though the chief culprit was a single 32-bit family, which may represent an anomaly. Hijacking digital certificates, exploiting kernel vulnerabilities, creating shell companies to digitally sign rootkit malware, and attacking the built-in security safeguards of operating systems are all tactics to get around 64-bit safeguards. We believe that these techniques and others will result in an increase in rootkit-based attacks.

Platform security: a perceived roadblock for rootkits

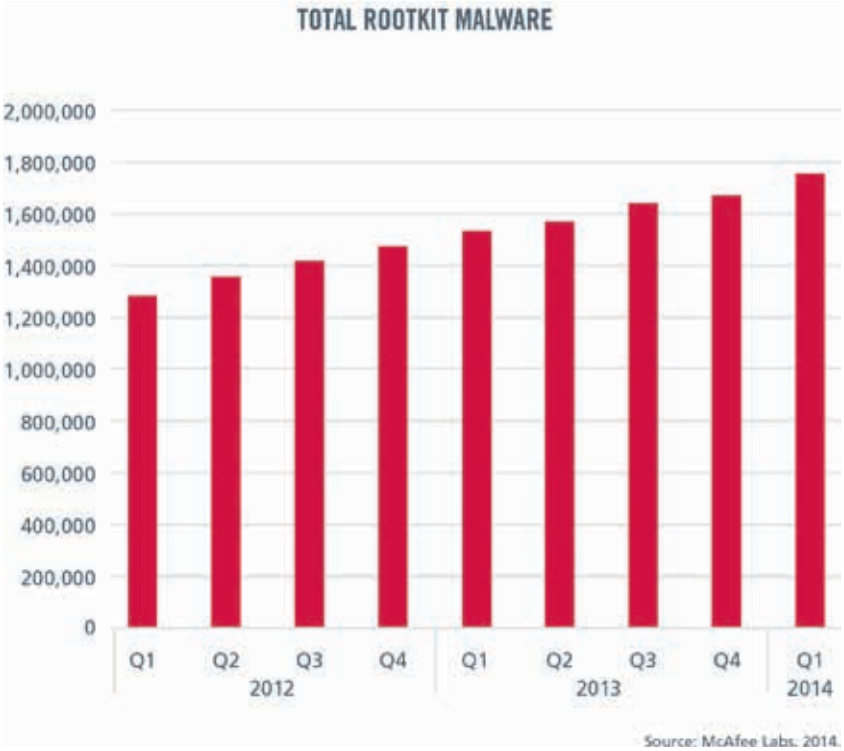
The sharp drop in the number of new rootkit samples (see chart) attacking Windows a couple of years ago is generally attributed to higher adoption of the 64-bit platform. The 64-bit microprocessor and OS designs increase system security due to enforcements such as digital signature checking and kernel patch protection for software that seeks to run at the highest privilege level inside the kernel.



The number of new rootkit samples collected by McAfee Labs declined from 2011 to 2012 and has remained relatively constant since then. We believe that new rootkit samples will grow as attackers learn how to circumvent security protection in 64-bit systems.

Intel 64-bit microprocessors started to appear in volume in the mid-2000s and are now found on most systems. Intel's Core i3, i5, and i7 microprocessors implement the 64-bit instruction set.

Follow McAfee Labs



In addition to the slowing of the sample count, we have also seen a significant drop in the techniques that rootkits can employ to gain kernel privileges. No longer are attackers able to hook the kernel as freely as they once did or even install malicious device drivers. These protections have certainly increased the cost to build and deploy rootkits on 64-bit platforms.

Why are rootkits so dangerous? Their use of stealth to infect a system allows them to remain hidden and potentially steal information for an extended period. The longer the period of infection, the greater are the chances of attackers stealing or destroying corporate and individual data.

Driving around the roadblocks

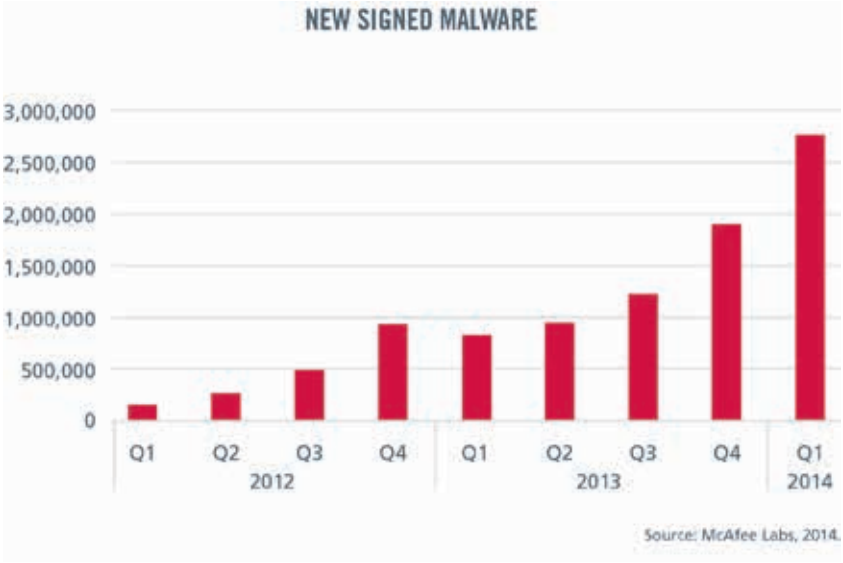
The roadblocks set in place by 64-bit systems now appear to be mere speed bumps for well-organized attackers, who have already found ways to gain entry at the kernel level.

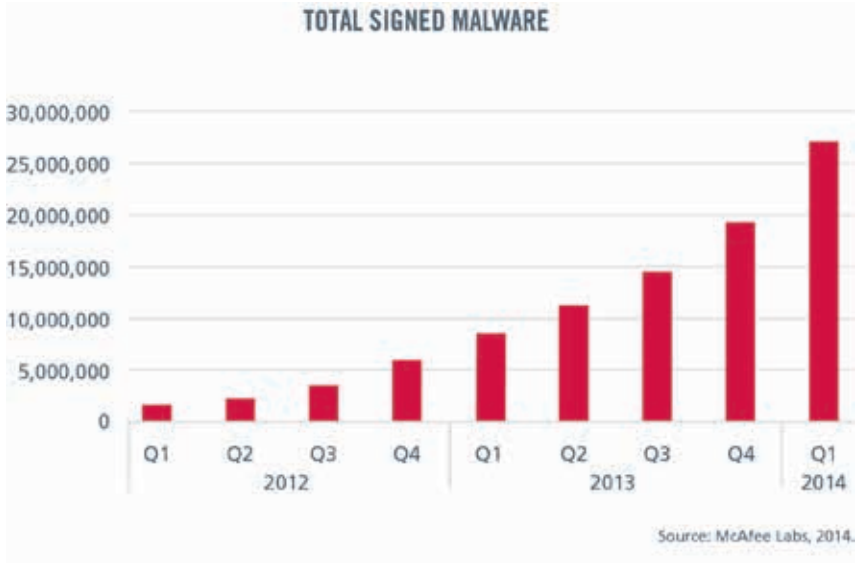
The most recent example of a malicious detour was demonstrated by the Uroburos[3] rootkit, which went undetected for three years. Uroburos took advantage of an old VirtualBox kernel driver that had a valid digital signature and a known vulnerability. (VirtualBox is a virtual machine provided by Oracle.) Uroburos exploited the kernel driver's vulnerability to disable the digital certificate check by the operating system and load its unsigned malware. Once loaded in the kernel, the malware disabled kernel patch protection—also known as PatchGuard—introduced with 64-bit Windows. PatchGuard prevents kernel patching, a technique often used by attackers.

Abusing trust

In addition to exploiting vulnerabilities in third-party drivers to gain kernel access, the outright theft of private keys offers attackers a path to get malicious code onto 64-bit systems. A valid digital signature also helps in bypassing security. We have seen a strong upward trend in all kinds of malicious binaries using digital signatures. (See charts.)

New malicious signed binaries remain a popular form of attack, increasing by 46% this quarter.





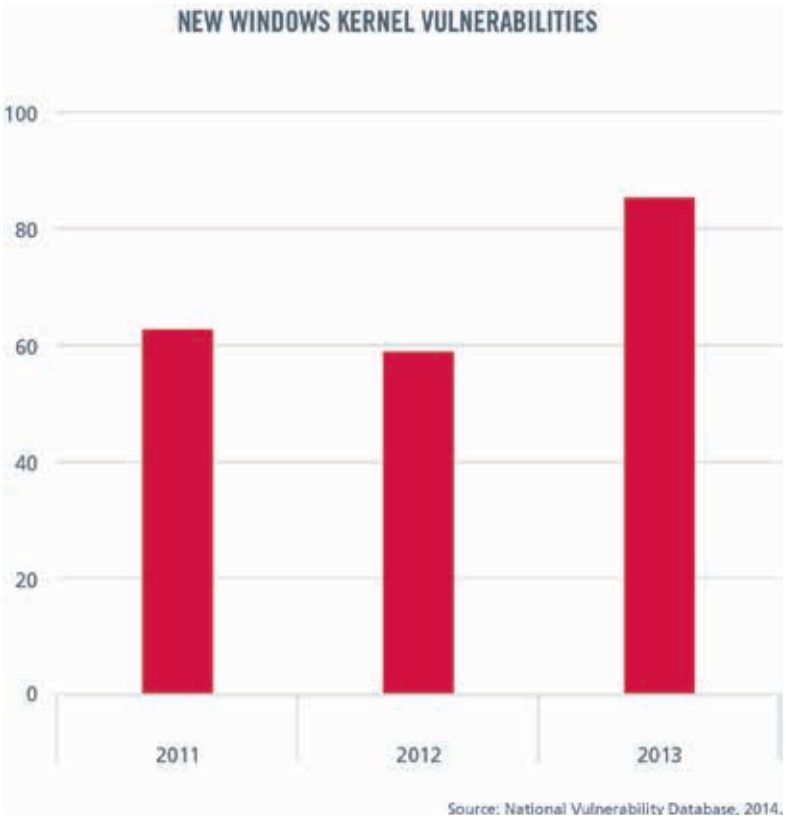
Follow McAfee Labs

We analyzed the last two years of data to see how many 64-bit rootkits have used known stolen digital certificates. We found the following:

- Since January 2012 at least 21 unique 64-bit rootkit samples have used stolen certificates.
- The malware W64/Winnti stole at least five private keys of legitimate vendors to install its rootkit on 64-bit systems since 2012. Of these five, at least two have not been revoked and may still be in use for both legitimate and malicious purposes.
- At least one rootkit, W64/Korablin, was used in the zero-day exploit CVE-2013-0633, possibly by state-sponsored actors.

Privilege escalations: kernel zero days

In recent years, the number of privilege-escalation bugs has been on the rise, even in the more secure 64-bit kernel (see chart). So, too, is the sophistication in methodology used by researchers for finding zero-day vulnerabilities in kernel code. Researchers are developing targeted tools such as "double fetch" race conditions to find flaws in kernel code. History tells us that once such work happens in the research community, we will soon see its impact in the threat landscape as well.



The number of new kernel vulnerabilities in all versions of Windows increased by more than 33% in 2013, according to the National Vulnerability Database.

Follow McAfee Labs

The preceding data is just for kernel and related components from Microsoft. Third-party kernel components with valid digital signatures also have a large number of vulnerabilities. We believe the new wave of rootkit attacks will rely on exploiting this growing number of vulnerabilities to sneak into the kernel and take control.

Although 64-bit microprocessors and 64-bit Windows introduced many new security measures, no security system is bulletproof; with enough money and motivation, any can be broken. We believe that 64-bit systems are about to see an increase in attacks from valid digitally signed malware—because that seems to be the easiest way to take advantage of stolen digital certificates.

We can't rely solely on any microprocessor or OS to build roadblocks because they will eventually be bypassed. The best way to stop kernel attacks is to employ holistic defenses that combine hardware and software, in addition to multiple network and endpoint safeguards.

Mobile malware abuses platform vulnerabilities, apps, and services

Most mobile malware attempts to steal sensitive information or send premium SMS messages by taking advantage of standard platform APIs. In effect, the malware abuses the official features provided with the platform. Recently malware developers have started abusing features or exploiting vulnerabilities of not only the platform, but also of legitimate apps and services.

App abuses Google account authentication and authorization

McAfee has discovered a suspicious Android app, Android/BadInst.A, on the Google Play app store that automatically downloads, installs, and launches other apps without user permission, which is usually required when manually installing apps from Google Play.[4] Because this confirmation procedure at installation plays a critical role in securing a mobile platform, allowing apps to skip this process poses a significant risk to device users, including the silent installation of more dangerous malware.

Android/BadInst.A retrieves a device user's Google account name and then asks the user to authorize its access to various Google services. This is done with a standard Android framework API, AccountManager, with the corresponding permissions granted. The app then communicates with the Google Play server using the granted authorization tokens in an unofficial way. Finally the app downloads, installs, and launches other apps published on Google Play without any interaction from the user.

The communication protocol used between the Google Play server and its counterpart service app on mobile devices to automatically download and install apps is not documented; this unofficial method is not intended for use by third-party apps. We suspect the developer of Android/BadInst.A reverse-engineered the protocol and implemented the same procedures in the suspicious app. We also know that the obtained authorization tokens can be used for Google services other than Google Play, so malware abusing this Google account authorization mechanism could easily lead to user information leaks and impersonated user actions on various Google services.

The Japanese-language malware Android/BadInst.A requests that users authorize access to various Google services.

Malware exploit digital wallet service, popular messaging app

The Android/Waller.A Trojan exploits a security flaw in a legitimate digital wallet service to steal money.[5] The malware exploits the money-transfer protocol used by the Visa QIWI Wallet. This malware is installed disguised as an update for Adobe Flash Player or another legitimate utility app, and is hidden from the home screen after installation. In the background, the malware checks whether the device user has a digital wallet account and whether there is a balance in the wallet, intercepts the confirmation response, and finally sends the money transfer to the attacker's server. In this case, the malware exploits the protocol that allows these steps via SMS messages without sufficient authentication, effectively impersonating the official app.

The Android/Waller.A malware disguised as Adobe Flash Player.

McAfee Labs also discovered the Android/Balloonpopper.A Trojan, which exploits an encryption method weakness in the popular messaging app WhatsApp.[6] This malware disguises itself as a game app, BalloonPop, but steals WhatsApp conversations and pictures stored on the device and secretly sends them to the criminal's remote server to decrypt and later disclose in public on the attacker's website.[7] Although this vulnerability has now been fixed, we can easily imagine cybercriminals continuing to look for other flaws in this well-known app.

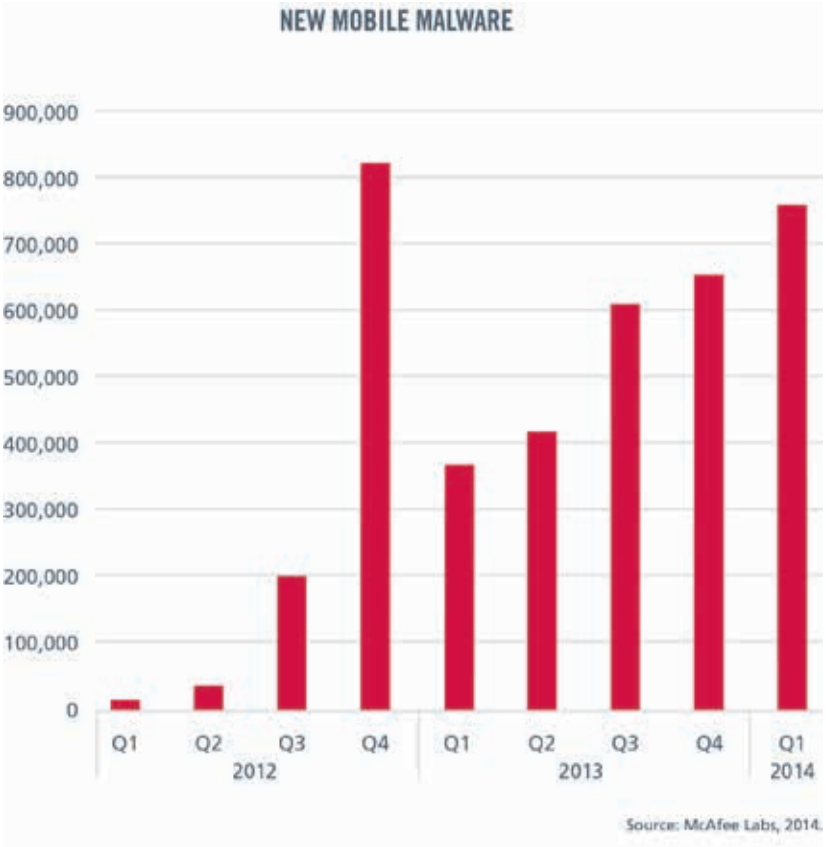
The attacker's website can disclose collected WhatsApp conversations.

Platform and apps need protection

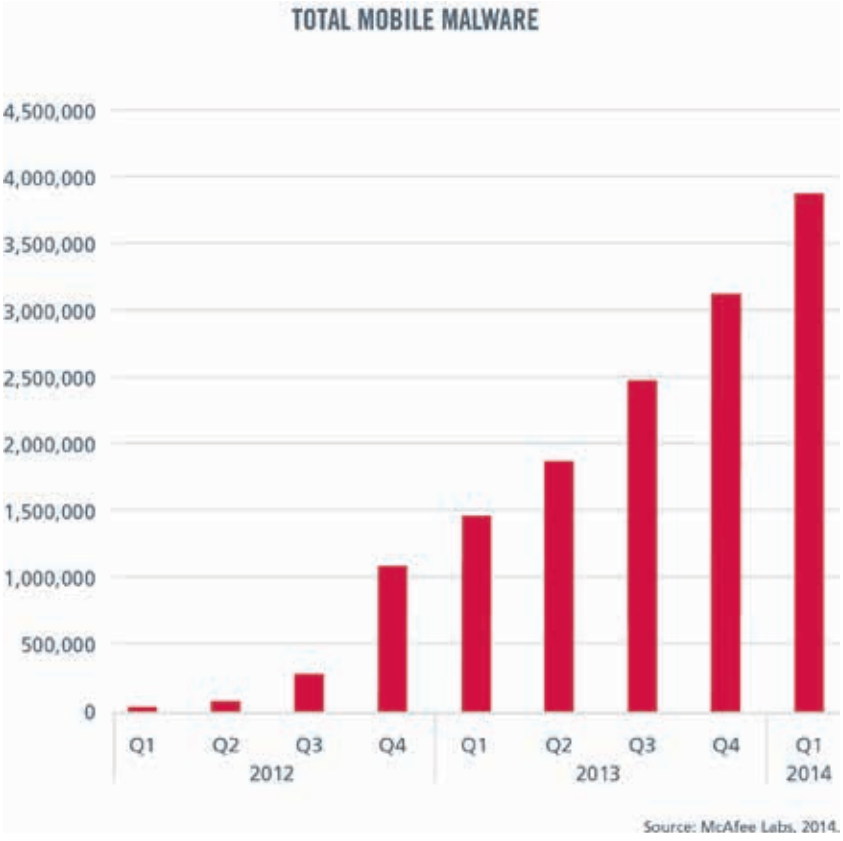
As we see from these examples, mobile malware has recently started to use legitimate apps and services, in addition to a platform's standard features, to circumvent conventional surveillance by app stores and security products. Consequently, protecting only the underlying platform is no longer sufficient. We believe that developers need to protect their apps and services from unauthorized and malicious use. Further, app stores must ensure that all data access comes from only authenticated and authorized client apps. These steps are crucial when an app has higher privileges than normal or deals with banking, payments, and other highly sensitive data. Users should not grant excessive or unfamiliar permission requests at installation and runtime. Users should also update their apps to fix security issues once vulnerabilities are found, and should certainly avoid any apps known to be unsafe.

THREATS STATISTICS

Mobile Malware



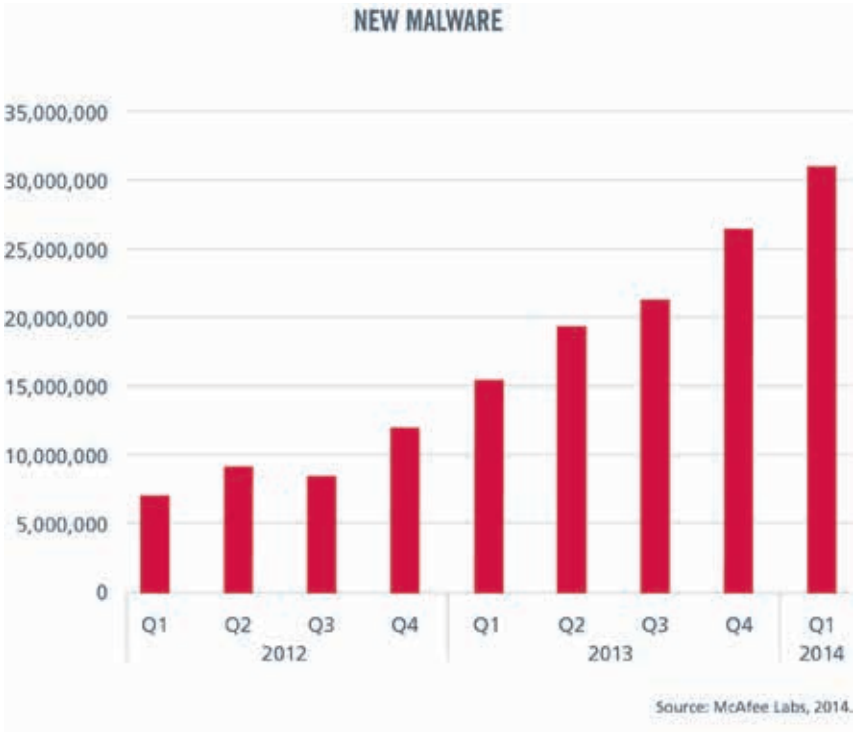
In just one year, the total number of mobile malware samples has grown by 167%.

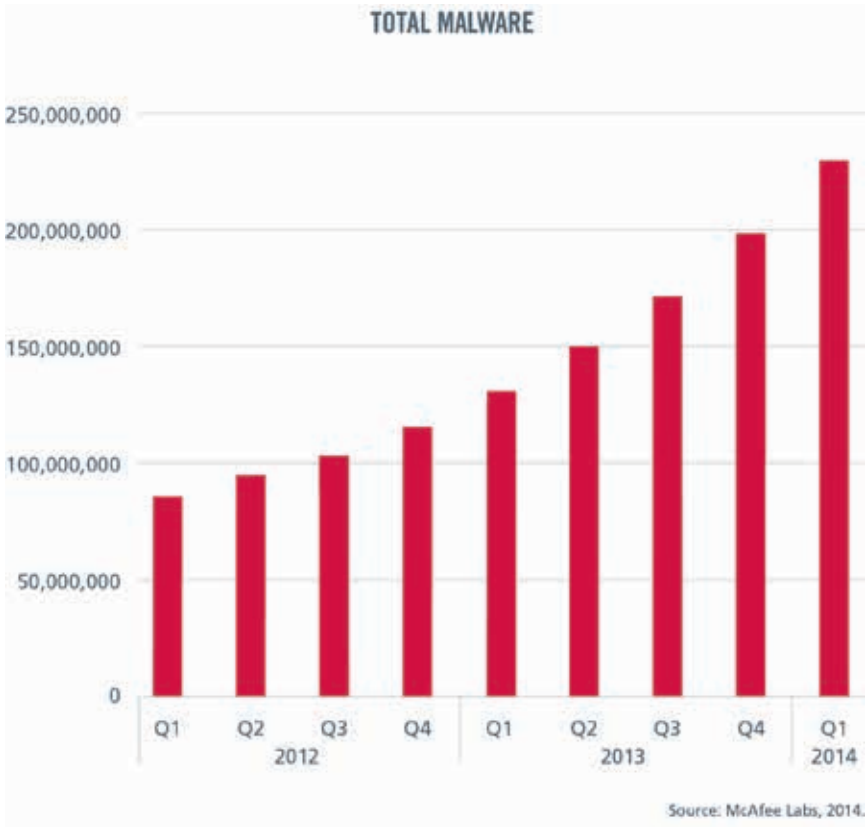


Beginning with the *McAfee Labs Threats Report: Third Quarter 2013,* we switched our reporting of mobile malware from a count of malware families to unique samples (a hash count). We did this for two reasons: First, we wanted the method we use for mobile malware to be consistent with the way we report all malware. Second, by reporting the total number of variants instead of the total number of mobile malware families, we present a better overall picture of how mobile malware affects users.

Follow McAfee Labs

Malware

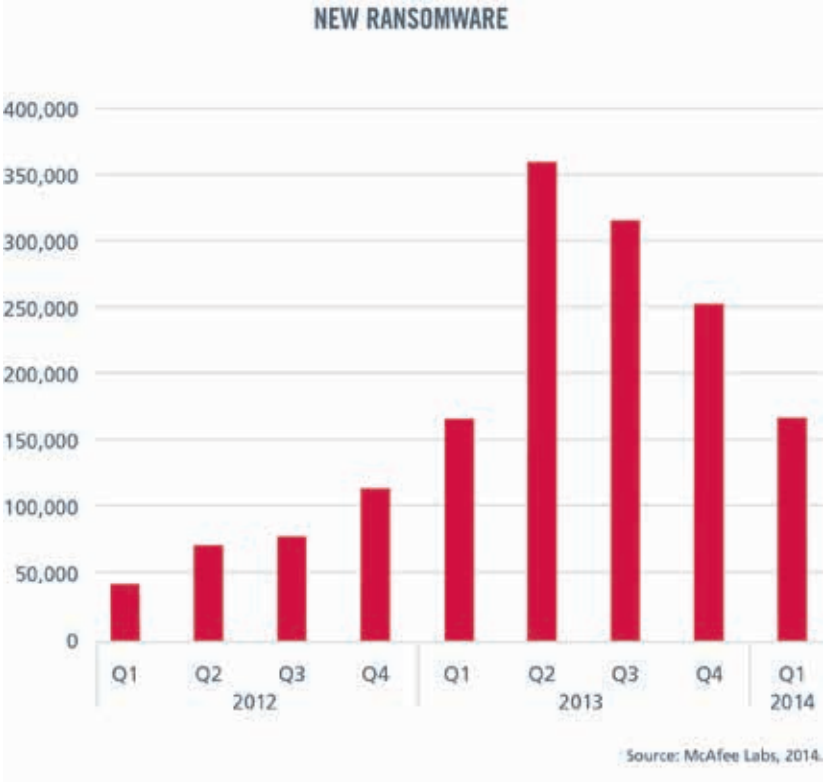


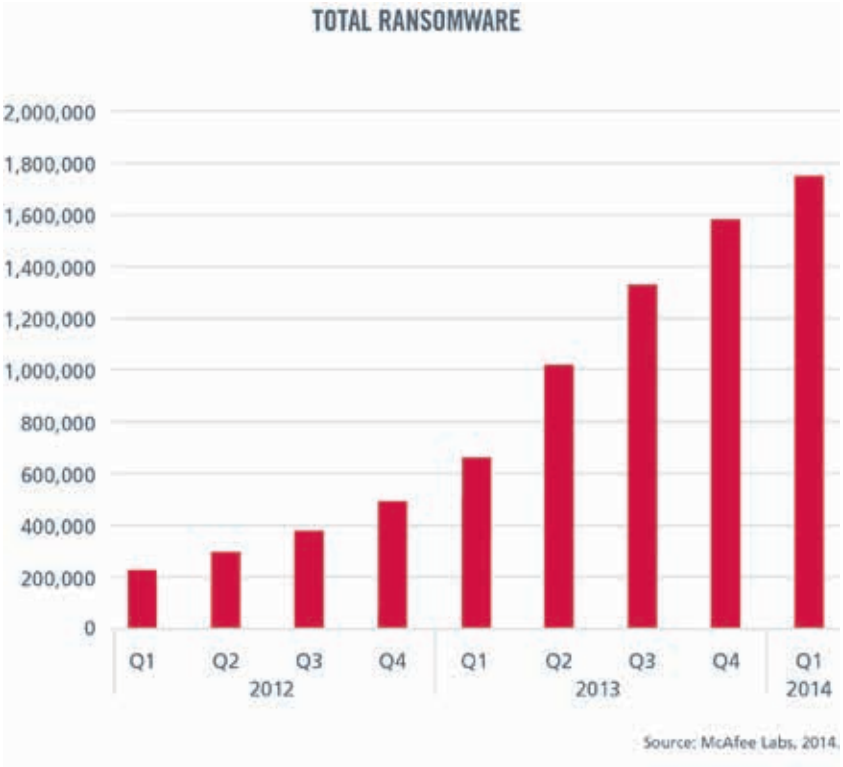


The march continues. In Q1 2014 the total malware sample count in the McAfee Labs "zoo" broke the 200 million sample barrier.

Follow McAfee Labs

The number of new ransomware samples has dropped for three straight quarters. McAfee Labs has confirmed that the trend is not the result of an anomaly. We have several theories for why this is happening, but we haven't pinpointed an exact cause. It's also possible we're seeing a trough before another increase. That has happened with many other types of malware.

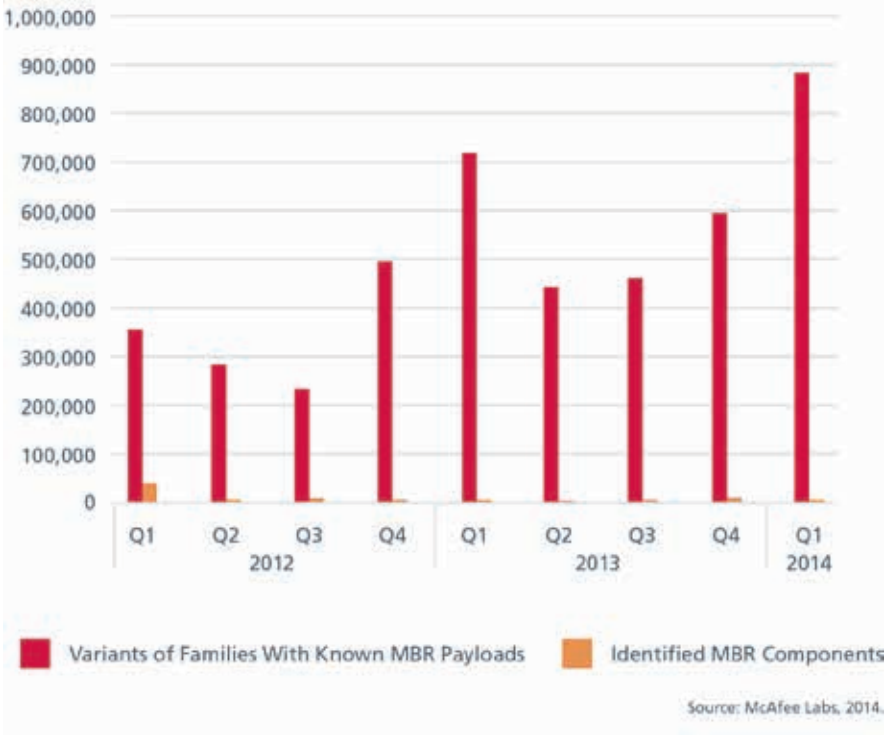




Follow McAfee Labs

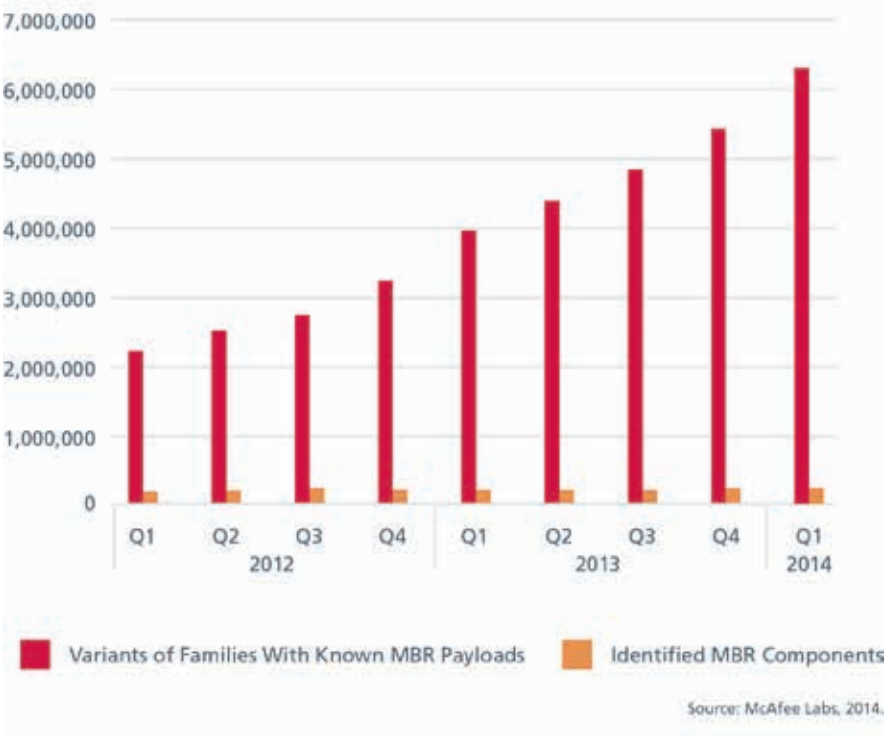
New threats attacking the master boot record increased by 49% this period, reaching an all-time high for a single quarter.

NEW MASTER BOOT RECORD–RELATED MALWARE



Source: McAfee Labs, 2014.

TOTAL MASTER BOOT RECORD–RELATED MALWARE

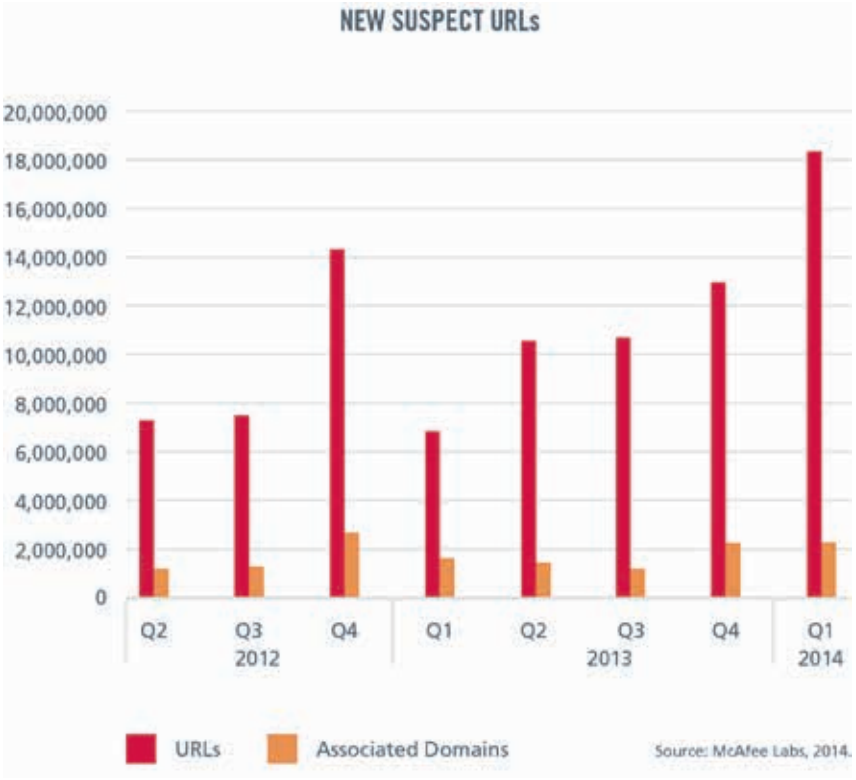


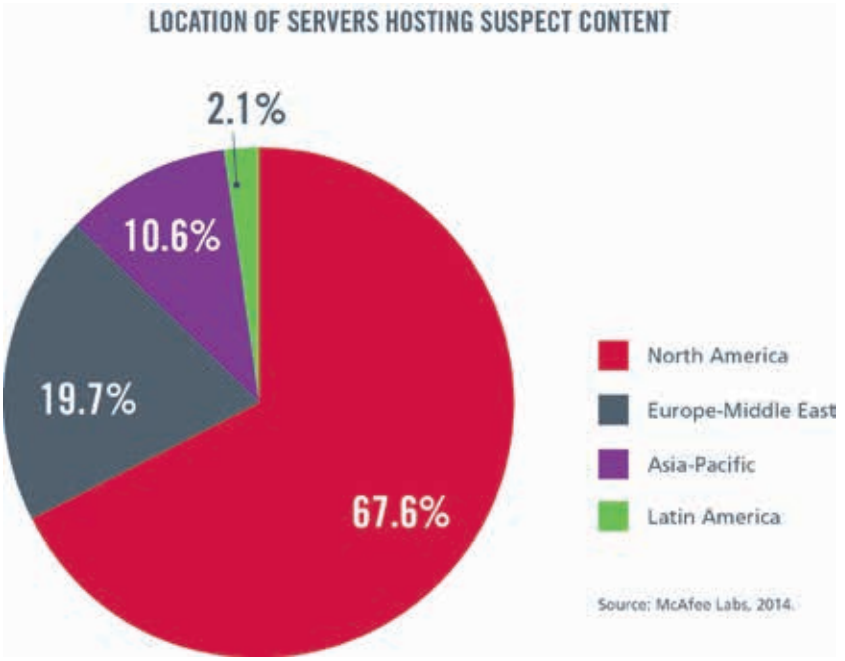
Source: McAfee Labs, 2014.

Follow McAfee Labs

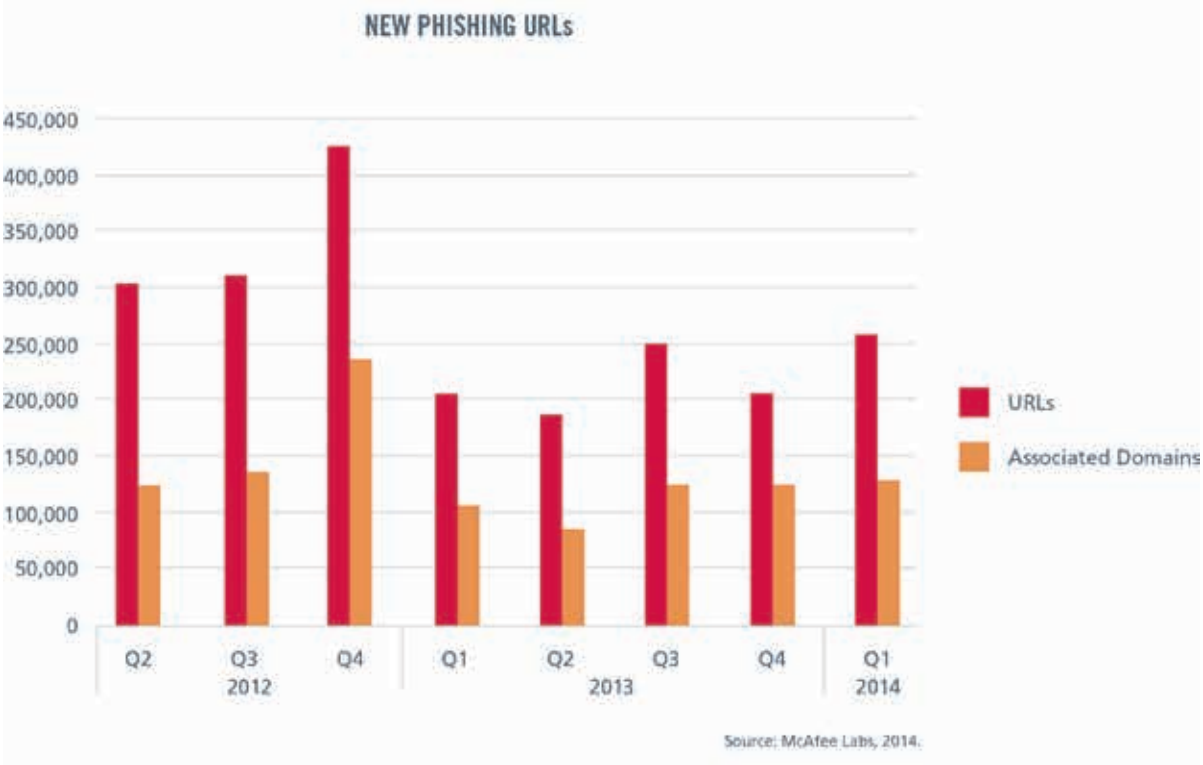
Web threats

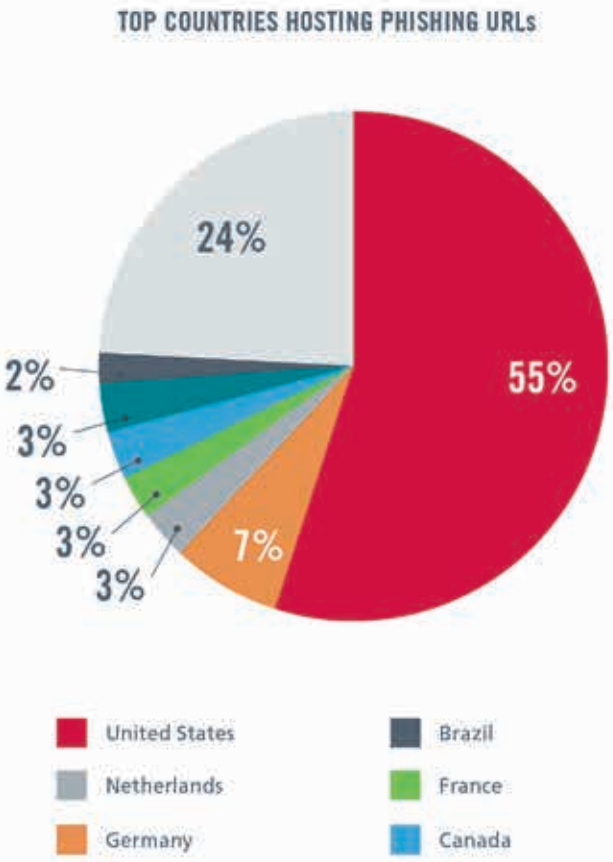
The McAfee Labs count of new suspect URLs set a three-month record with more than 18 million, a 19% increase over Q4 and the fourth straight quarterly increase.

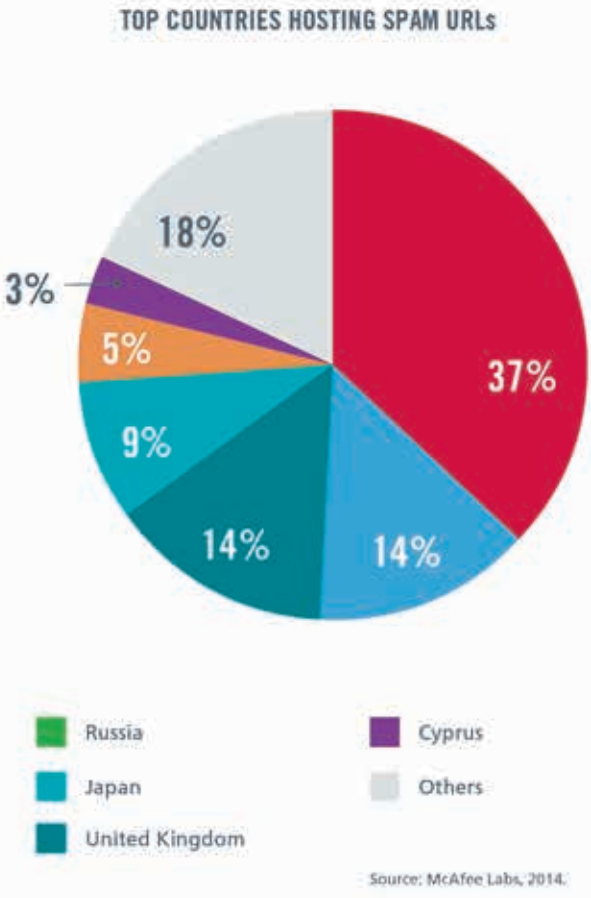




Follow McAfee Labs

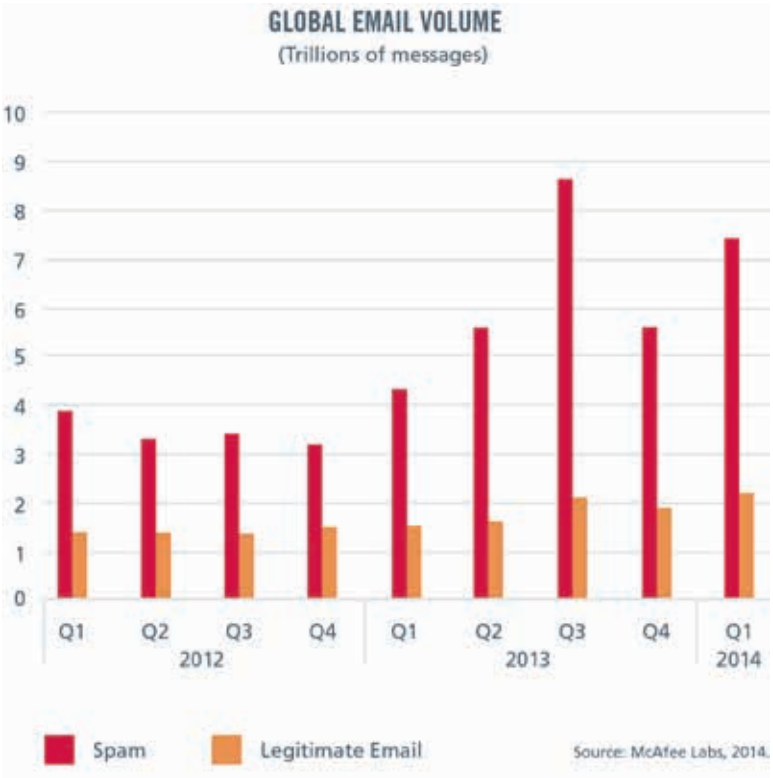


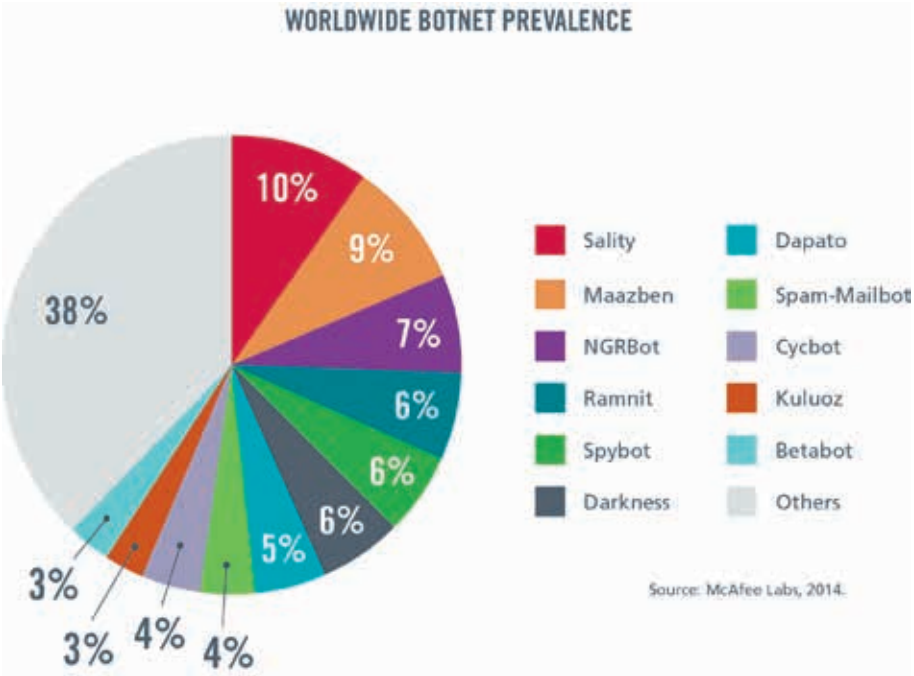




Follow McAfee Labs

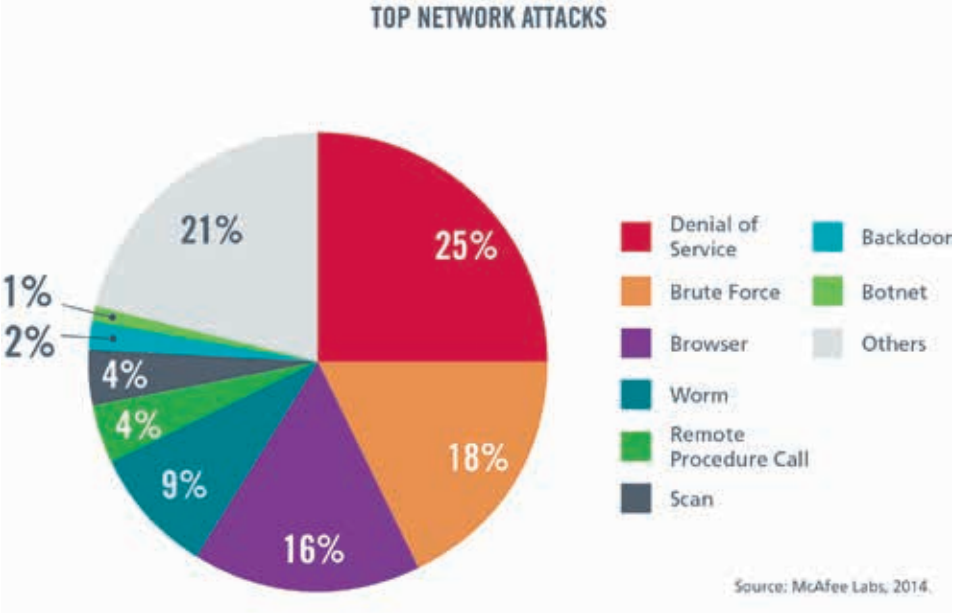
Messaging threats





Follow McAfee Labs

Network threats



Follow McAfee Labs

ABOUT McAFEE

McAfee, part of Intel Security and a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe.

http://www.mcafee.com

1 Difficulty is the measurement of how much work (processing) is required to generate block chains. By design, Bitcoin difficulty adjusts every 2,016 blocks (around two weeks).

2 Hash rate is the measure of hardware performance as it relates to operations in the mining network.

3 http://blogs.mcafee.com/mcafee-labs/analyzing-uroburos-patchguard-bypass

4 http://blogs.mcafee.com/mcafee-labs/automatic-app-installation-google-play-store-poses-big-risk

5 http://home.mcafee.com/virusinfo/virusprofile.aspx?key=7358408

6 http://blogs.mcafee.com/mcafee-labs/androidballoonpopper-sums-up-mobile-threat-landscape-in-2013

7 http://blogs.mcafee.com/consumer/whatsapp-security-flaw

61158rpt_qtr-q1_0614_fnl_PAIR