McAfee Labs
Threats Report

August 2014

Heartbleed was the most significant security event since the Target data breach in 2013.

About McAfee Labs

McAfee Labs is one of the world's leading sources 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

Follow McAfee Labs

Introduction

For many of us, summertime is a chance to relax and enjoy the world's bounties. But to the bad guys, summer is merely another season, presenting new opportunities to steal. Early this summer with an eye on the FIFA World Cup, McAfee's consumer division highlighted risky websites associated with the world's top fútbol players in the **McAfee Red Card Club**. These sites draw excited and unsuspecting fans, and either automatically infect systems or trick visitors into revealing personal information. The story clearly illustrates how summertime fun can turn into a summertime nightmare with a single click of the mouse.

This quarter, our lead topic concerns the Heartbleed vulnerability. As most security professionals know, Heartbleed was the most significant security event since the Target data breach in 2013. McAfee Labs worked around the clock to understand this vulnerability and ensure that relevant McAfee technologies could detect and prevent Heartbleed-based theft from occurring. Unfortunately, the bad guys continue to reap rewards from this vulnerability because many websites remain unpatched.

We also detail what we learned from our **McAfee Phishing Quiz**, which tested business users' ability to correctly detect phishing emails. Finally, we document what has happened since international law enforcement agencies, jointly with IT security industry participants including McAfee, **took down the Gameover Zeus and CryptoLocker infrastructure**. It was a resounding success, but as we all expected, the relief was only temporary.

Reporting on threats is an ever-changing art. For longtime readers of the *McAfee Labs Threats Reports,* you will have seen many changes in what we report and how we present the information. To help guide our future work, we're interested in your feedback. If you would like to share your views, please **click here** to complete a quick, five-minute threats report survey.

Vincent Weafer, Senior Vice President, McAfee Labs

Share feedback

Contents

McAfee Labs Threats Report
August 2014

This report was prepared and written by:

Christiaan Beek
Benjamin Cruz
Daniel Flaherty
Charles McFarland
Francisca Moreno
Daisuke Nakajima
François Paget
Eric Peterson
Craig Schmugar
Rick Simon
Dan Sommer
Bing Sun
James Walter
Adam Wosotowsky
Chong Xu

Executive Summary

Heartbleed's aftermath: another cybercrime opportunity

By far the most important security event in the second quarter was the public disclosure of the "Heartbleed" vulnerability contained in several versions of the OpenSSL implementation of the SSL and TLS security protocols. This vulnerability, which affected every IT organization—knowingly or unknowingly—is likely to cost **hundreds of millions of dollars** to repair. Estimates suggest that Heartbleed affected globally about 17% of all TLS-enabled websites, which are typically those that request user authentication through username and password. That comes to more than 600,000 sites.

In this *Threats Report,* McAfee Labs explores how attackers use lists of unpatched websites to mine for sensitive information. The Heartbleed-vulnerable site lists were initially created to assist users who wanted to ensure they were authenticating safely to a site, but they quickly became hit lists for cybercriminals. One enterprising cyber thief has even done the heavy lifting for other cybercriminals by extracting data from still-vulnerable sites and selling the stolen data on the black market. As of this writing, more than 300,000 websites remain unpatched and vulnerable to this type of criminal activity, according to one source.

Cybercriminals are using publicly available lists of unpatched Heartbleed-vulnerable websites to target their attacks.

Phishing lures the unsuspecting: business users easily hooked

In this report, we also examine the exceedingly effective tactic of phishing. Phishing attacks exploit the often times weakest link in a business' cyber defense—human behavior—and they continue to be quite successful. McAfee has been testing business users' ability to detect phishing though our **McAfee Phishing Quiz**. We have found that 80% of all test takers have fallen for at least one in seven phishing emails. Further, we see that accounting and finance, and HR—which arguably hold some of the most sensitive corporate data—perform the worst.

The McAfee Phishing Quiz reveals that 80% of test takers have fallen for at least one in seven phishing emails.

Operation Tovar: a big hit with a short life

Finally, we reveal new information about Operation Tovar, a very successful takedown campaign conducted jointly among international law enforcement agencies and key IT security industry participants including McAfee. Operation Tovar crippled the Gameover Zeus and CryptoLocker infrastructure by taking control of the domains that form part of the communications network. Prior to the takedown, McAfee Labs discovered a criminal ring that collected US$255,000 in ransom payments in a single month. Since the takedown in early June, copycats have already begun to spring up. In one example detailed in this report, a CryptoLocker-like service has been offered for $3,000.

Prior to the Operation Tovar takedown, McAfee Labs tracked one criminal ring that collected US$255,000 in a single month.

Key Topics

Heartbleed's aftermath: another cybercrime opportunity

Phishing lures the unsuspecting: business users easily hooked

Operation Tovar: a big hit with a short life

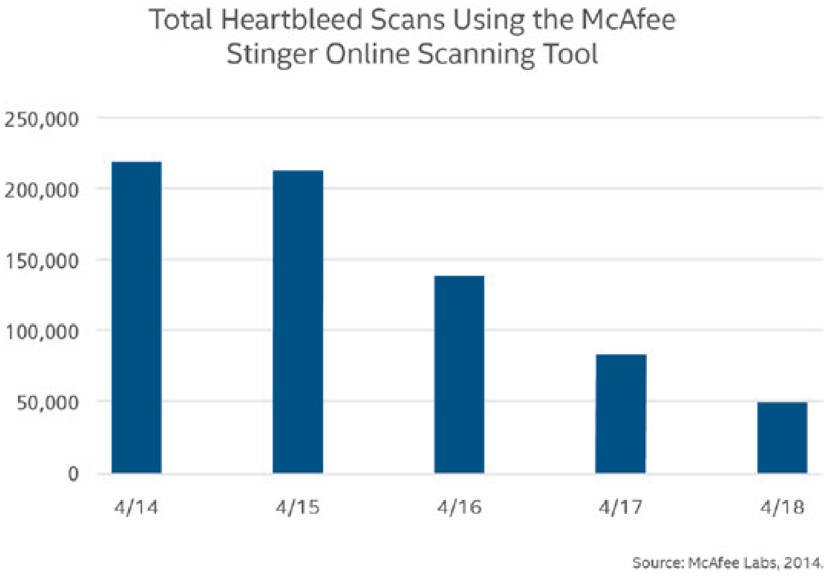
Share feedback

Heartbleed's aftermath: another cybercrime opportunity

On April 7, the vulnerability CVE-2014-0160, which affects the OpenSSL open source library, was publicly announced. The vulnerability allowed a hacker to access data in memory by using a malformed "heartbeat" in the transport layer security (TLS) cryptographic protocol. Due to its prevalence, many consider this the worst vulnerability ever discovered. The flaw was soon called Heartbleed. Because of the popularity of OpenSSL on commercial servers, Heartbleed affected a significant portion of the Internet, estimated to be around 17% of websites using TLS. That estimate includes some of the most often visited websites on the net as well as many smaller, less well-known sites. In response to the disclosure, McAfee Labs saw a surge of data and resource sharing among security experts. Within days, an abundance of free tools and resources were available from security venders, security professionals, academia, and hobbyists. As an industry, we witnessed the first-hand impact of mutually beneficial collaboration and its ability to quickly secure affected systems. But despite the plethora of available tools, many applications, websites, and devices that remain unpatched are almost certain to be victims of an attack.

The OpenSSL library is an open source project that implements multiple versions of SSL (secure sockets layer) and TLS (transport layer security). These protocols enable encrypted communications between a client and server and enable much web content—including encrypted email, online banking, and other services requiring end-to-end encryption. It is widely used by many websites.

The TLS heartbeat ensures that both server and client can communicate with one another. The client sends data such as "hello" to the server. The expected behavior is that the server will respond with the same data. An attacker can arbitrarily define the data to be much larger than the data sent. This will result in memory disclosure that could contain sensitive data such as private encryption keys.



Source: McAfee Labs, 2014.

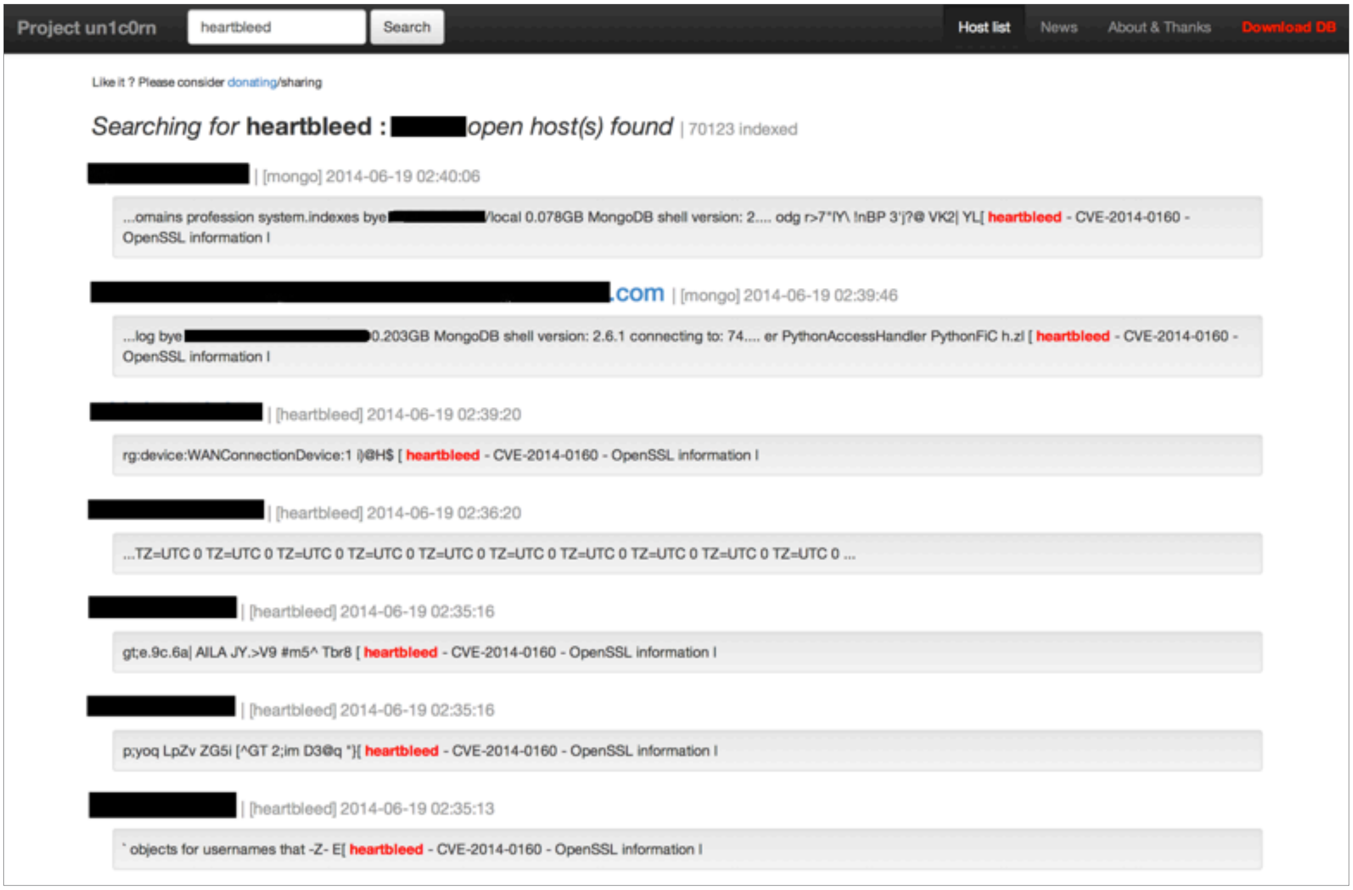
Use of the free scanning tool McAfee Stinger shows a rapid decline in interest in Heartbleed.

When a vulnerability such as Heartbleed is discovered, it is imperative that IT professionals and security researchers have the tools not only to test their own systems but also to understand the vulnerability at its deepest level. Heartbleed testing examples include the dozens of online scanning tools that became available shortly after the disclosure, a handful of Python and Ruby scripts code samples, NMAP (network mapper) scripts, penetration testing plug-ins, and many more. However, not everyone is an upstanding security professional. There are many who would use these tools for malicious purposes or to build other tools with less noble intentions.

Share this Report

Among the many useful Heartbleed tools, including **one from McAfee**, available to security professionals is a full-featured tool called heartleech, which is available free on GitHub. Not only does heartleech test for the Heartbleed vulnerability but it also stores the leaked data and analyses it for private keys. Furthermore, heartleech was written to sidestep some forms of intrusion detection so network administrators can both detect whether their systems are vulnerable and extract any sensitive keys that may have been leaked. This information is invaluable to both white hat and black hat security professionals.

A less noble tool is Project Un1c0rn, which appears to have been released May 12 on the Deep Web network TOR and on May 15 for other Internet users. This tool is unique in that it attempts to make vulnerable public IPs searchable. Although it is likely that nearly all of the world's most important websites have been patched for Heartbleed, a large number of small-site owners do not have the expertise or are still unaware that they are vulnerable. Project Un1c0rn collects these targets in the same way a thief might assemble a to-do list of unlocked houses. McAfee Labs ran this particular search and found 2,440 unique and potentially vulnerable targets, but at least one industry analyst suggests perhaps 300,000 sites remain vulnerable.[1] This figure does not take into account nonstandard ports or IP-enabled devices.



Like it ? Please consider donating/sharing

Searching for **heartbleed :** [redacted] *open host(s) found* | 70123 indexed

[redacted] | [mongo] 2014-06-19 02:40:06

...omains profession system.indexes bye[redacted]/local 0.078GB MongoDB shell version: 2.... odg r>7"IY\ !nBP 3'j?@ VK2| YL[**heartbleed** - CVE-2014-0160 - OpenSSL information I

[redacted].com | [mongo] 2014-06-19 02:39:46

...log bye[redacted]0.203GB MongoDB shell version: 2.6.1 connecting to: 74.... er PythonAccessHandler PythonFiC h.zl [**heartbleed** - CVE-2014-0160 - OpenSSL information I

[redacted] | [heartbleed] 2014-06-19 02:39:20

rg:device:WANConnectionDevice:1 i)@H$ [**heartbleed** - CVE-2014-0160 - OpenSSL information I

[redacted] | [heartbleed] 2014-06-19 02:36:20

...TZ=UTC 0 TZ=UTC 0 TZ=UTC 0 TZ=UTC 0 TZ=UTC 0 TZ=UTC 0 TZ=UTC 0 TZ=UTC 0 TZ=UTC 0 TZ=UTC 0 ...

[redacted] | [heartbleed] 2014-06-19 02:35:16

gt;e.9c.6a| AILA JY.>V9 #m5^ Tbr8 [**heartbleed** - CVE-2014-0160 - OpenSSL information I

[redacted] | [heartbleed] 2014-06-19 02:35:16

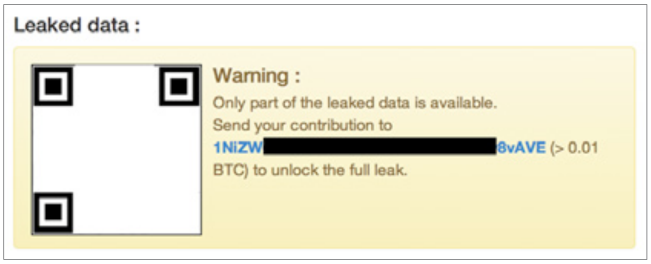
p;yoq LpZv ZG5i [^GT 2;im D3@q ")[**heartbleed** - CVE-2014-0160 - OpenSSL information I

[redacted] | [heartbleed] 2014-06-19 02:35:13

` objects for usernames that -Z- E[**heartbleed** - CVE-2014-0160 - OpenSSL information I

The Project Un1c0rn tool allows anyone to search for servers vulnerable to Heartbleed.

Unsophisticated cybercriminals may use tools such as Project Un1c0rn to pay for leaked data instead of extracting it themselves. For as little as 0.01 Bitcoin, roughly $6 at the time of this writing, cyberthieves can purchase leaked Heartbleed data. A slightly more sophisticated cybercriminal could use the tool as a personal hit list, targeting only websites most likely to be vulnerable. Although the latter adversary is more dangerous due to his or her ability to tailor an attack, with only slightly more skill someone could set up an automated script to attack all known vulnerable IP addresses. Essentially if a website is not patched, it's nearly guaranteed to become a victim if it is indexed by tools such as Project Un1c0rn. The tool is available on the Deep Web, so it stands a good chance of staying online for some time.



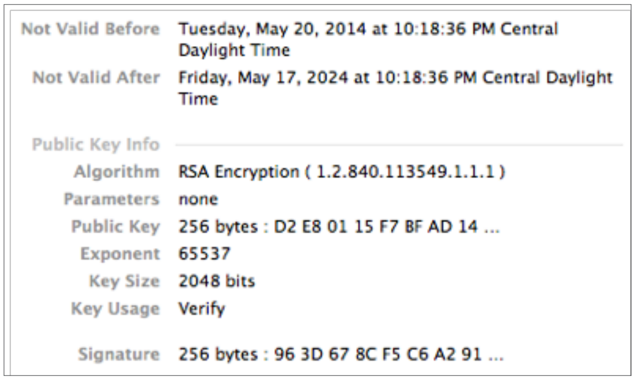
Leaked data :

Warning :

Only part of the leaked data is available.
Send your contribution to
1NiZW[redacted]8vAVE (> 0.01 BTC) to unlock the full leak.

A buyer can pay for leaked Heartbleed data by sending Bitcoin to Project Un1c0rn's Bitcoin wallet.

Although most high-traffic websites have been patched for Heartbleed, there are many IP-enabled devices that have not received the same quality of security management as those high-profile websites. Security cameras, for example, were found vulnerable to Heartbleed and patches were made available. However, not everyone applied those patches. In another example, an IP-enabled network attached storage (NAS) device was found to be vulnerable to Heartbleed. A security patch was posted for this device shortly after Heartbleed's disclosure, yet 10 weeks later McAfee Labs found an unpatched NAS system. The owner even had a new certificate issued on May 20, 43 days after Heartbleed's disclosure, but the NAS device was still using a vulnerable version of OpenSSL.



```
Not Valid Before  Tuesday, May 20, 2014 at 10:18:36 PM Central
                  Daylight Time
 Not Valid After  Friday, May 17, 2024 at 10:18:36 PM Central Daylight
                  Time

 Public Key Info
       Algorithm  RSA Encryption ( 1.2.840.113549.1.1.1 )
      Parameters  none
      Public Key  256 bytes : D2 E8 01 15 F7 BF AD 14 ...
        Exponent  65537
        Key Size  2048 bits
       Key Usage  Verify

       Signature  256 bytes : 96 3D 67 8C F5 C6 A2 91 ...
```

One site updated its certificate well after the discovery of Heartbleed, yet it remains vulnerable.

How hard would it be for hackers to escalate from attacking Heartbleed-vulnerable targets manually to attacking them in a fully automated way? Unfortunately, this is so trivial that it is likely already being done. In fact, an intermediate programmer could build such a system in less than day. In the same way security professionals can use an abundance of commercial tools, so can cybercriminals. With simple tools, a few lines of code, and some coffee, it's possible to tie together an automated system that targets only known vulnerable machines and extracts sensitive private keys.

Does this event mean that the security industry should become more secretive? Should McAfee and others safeguard information about vulnerabilities, hacks, and other intelligence? Certainly not! Heartbleed has proven that the security industry can protect internal networks and the Internet itself by sharing information and resources. By doing so, the security industry can prepare for the next Heartbleed. Until such time, users must be diligent in maintaining the best security practices for any services they use.

Common brands are often imitated to deceive email recipients into taking action. Learn more about detecting phishing emails by clicking these links:

PayPal

Amazon

eBay

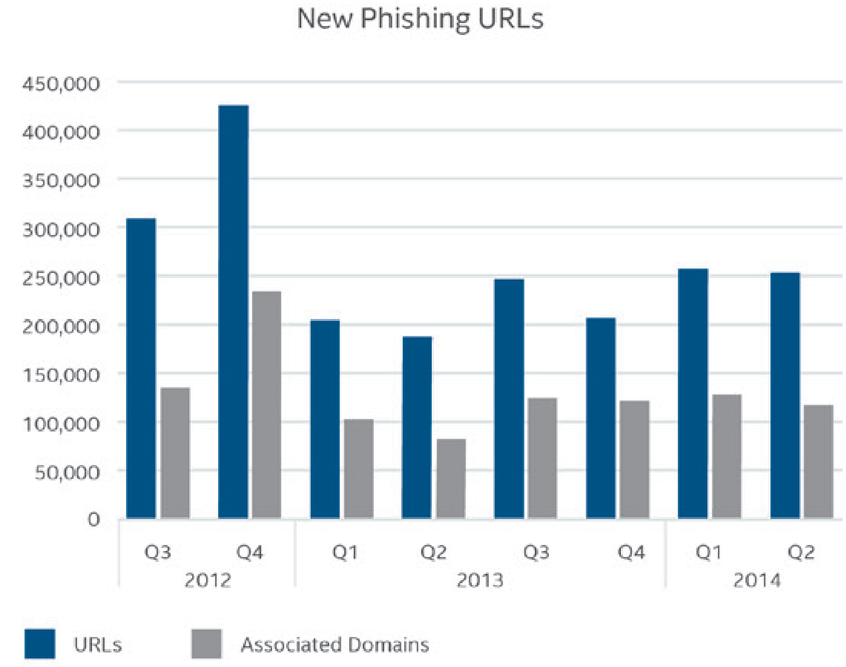
Bank of America

HSBC

Phishing lures the unsuspecting: business users easily hooked

Since our last Threats Report, McAfee Labs has collected more than 250,000 new phishing URLs—bringing us to a total of almost one million new sites in the last year. What we see from the data, however, is not only an increase in total volume, but also an increase in the sophistication of phishing attacks occurring in the wild. Effectively, it has become easier for the bad guys to know their targets, where they work, what they are interested in, and more. All forms of digital media have accelerated this capability, especially social media. We base our decisions on trust: Did the email come from a party or organization you know and currently do business with? Does it contain an element of personalization that makes it appear legitimate? That is often enough to ensure a click. Take a look at the top brands used in phishing attacks these days. Would you click a link in one of those emails?

- PayPal
- Amazon
- eBay
- Bank of America
- HSBC



Source: McAfee Labs, 2014.

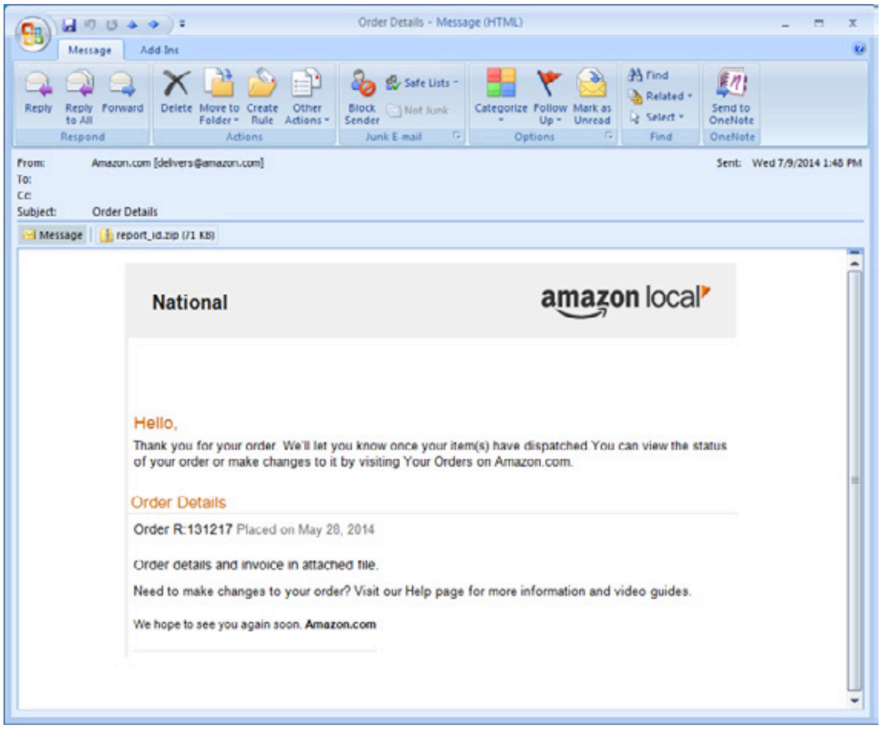
Share this Report

Phishing is an attempt to acquire sensitive information through emails or instant messages that appear to be coming from a trustworthy source. The messages typically contain malware-laden attachments or links to websites that are infected with malware.

Spear phishing is an attempt directed at a specific individual or organization. Typically, a spear phishing message contains personalized information that might lead the recipient to believe that it has come from a legitimate source.

A modern phishing attack

Both mass campaign phishing and its devilish child, spear phishing, are still rampant in the attack strategies used by cybercriminals around the world. To demonstrate the sophistication and potential impact of modern phishing attacks, let's walk through a sample currently making the rounds.



From: Amazon.com [delivers@amazon.com]
To:
Cc:
Subject: Order Details
Sent: Wed 7/9/2014 1:48 PM

Hello,

Thank you for your order. We'll let you know once your item(s) have dispatched You can view the status of your order or make changes to it by visiting Your Orders on Amazon.com.

Order Details

Order R:131217 Placed on May 28, 2014

Order details and invoice in attached file.

Need to make changes to your order? Visit our Help page for more information and video guides.

We hope to see you again soon. **Amazon.com**

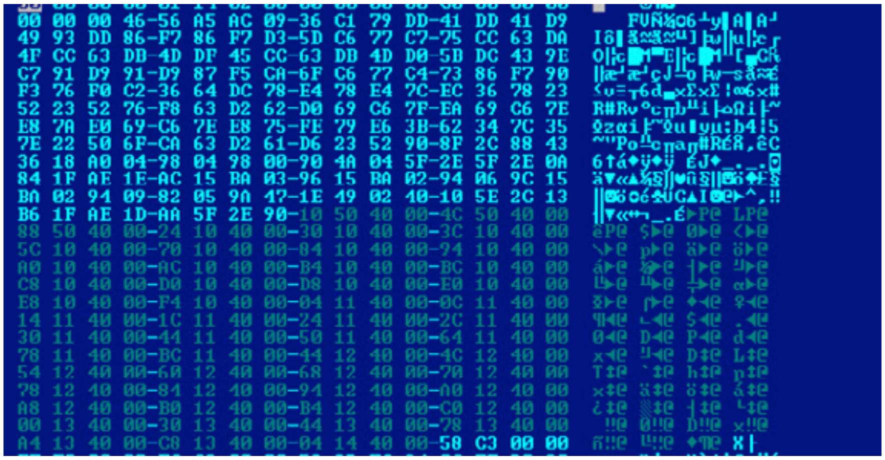
This phishing email appears to come from amazon.com.

This phishing message uses a classic tactic: Spoof a trusted brand and wait for a click. Posing as an order confirmation email, the message keeps its content short and simple, like many order confirmations from legitimate companies. Key to the deception here are two elements—the spoofed email address with an @amazon.com domain, and dynamically loaded images from a spoofed amazon.com domain. Over the course of one week, we observed 21,000 unique-sender IP addresses distributing this message worldwide.

However, we chose this sample not for its social engineering tactics—those are common today, and even less convincing than a well-developed spear phish—but instead for its malware payload. Clicking on the attached "invoice" starts a chain of events that many defenses would find difficult to block.

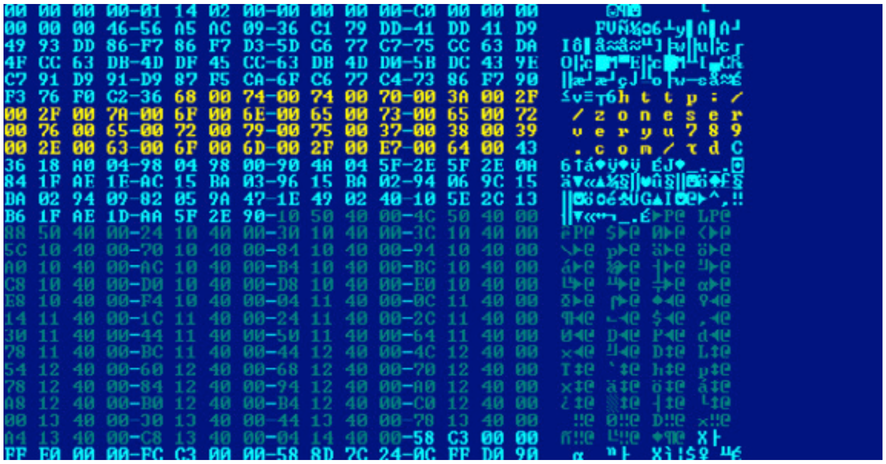
From that click, the malware performs a series of checks before it allows itself to execute. With the malware starting in a status of "infinite sleep," a check determines if the local disk is a virtual machine, potentially indicating that it is in a sandbox environment. If this is true, the malware will remain inactive. Further illustrating its sophistication, the code itself is self-modifying. McAfee Labs reverse-engineered this malware and found that it decrypts its own code in real time and overlaps instructions to deter static analysis by security products. We also saw jump instructions, indicating an attempt to avoid AV signatures.

If these checks (as well as others not mentioned here) are passed, then the malware will wake up and unpack itself through several layers of encryption and compression, allowing the real malicious code to run. Injecting itself into an instance of the Windows process svchost.exe, it then checks for an active Internet connection by attempting to visit msn.com. If this fails, the malware remains inactive. If a successful connection is made, it will decrypt several control server domain names from its own code.



```
00 00 00 46-56 A5 AC 09-36 C1 79 DD-41 DD 41 D9
49 93 DD 86-F7 86 F7 D3-5D C6 77 C7-75 CC 63 DA
4F CC 63 DB-4D DF 45 CC-63 DB 4D D0-5B DC 43 9E
C7 91 D9 91-D9 87 F5 CA-6F C6 77 C4-73 86 F7 90
F3 76 F0 C2-36 64 DC 78-E4 78 E4 7C-EC 36 78 23
52 23 52 76-F8 63 D2 62-D0 69 C6 7F-EA 69 C6 7E
E8 7A E0 69-C6 7E E8 75-FE 79 E6 3B-62 34 7C 35
7E 22 50 6F-CA 63 D2 61-D6 23 52 90-8F 2C 88 43
36 18 A0 04-98 04 98 00-90 4A 04 5F-2E 5F 2E 0A
84 1F AE 1E-AC 15 BA 03-96 15 BA 02-94 06 9C 15
BA 02 94 09-82 05 9A 47-1E 49 02 40-10 5E 2C 13
B6 1F AE 1D-AA 5F 2E 90-10 50 40 00-4C 50 40 00
88 50 40 00-24 10 40 00-30 10 40 00-3C 10 40 00
5C 10 40 00-70 10 40 00-84 10 40 00-94 10 40 00
A0 10 40 00-AC 10 40 00-B4 10 40 00-BC 10 40 00
C8 10 40 00-D0 10 40 00-D8 10 40 00-E0 10 40 00
E8 10 40 00-F4 10 40 00-04 11 40 00-0C 11 40 00
14 11 40 00-1C 11 40 00-24 11 40 00-2C 11 40 00
30 11 40 00-44 11 40 00-50 11 40 00-64 11 40 00
78 11 40 00-BC 11 40 00-44 12 40 00-4C 12 40 00
54 12 40 00-60 12 40 00-68 12 40 00-70 12 40 00
78 12 40 00-84 12 40 00-94 12 40 00-A0 12 40 00
A8 12 40 00-B0 12 40 00-B4 12 40 00-C0 12 40 00
00 13 40 00-30 13 40 00-44 13 40 00-78 13 40 00
A4 13 40 00-C8 13 40 00-04 14 40 00-58 C3 00 00
```

Encrypted binary code.



```
00 00 00 00-01 14 02 00-00 00 00 00-CA 00 00 00
00 00 00 46-56 A5 AC 09-36 C1 79 DD-41 DD 41 D9
49 93 DD 86-F7 86 F7 D3-5D C6 77 C7-75 CC 63 DA
4F CC 63 DB-4D DF 45 CC-63 DB 4D D0-5B DC 43 9E
C7 91 D9 91-D9 87 F5 CA-6F C6 77 C4-73 86 F7 90
F3 76 F0 C2-36 68 00 74-00 74 00 70-00 3A 00 2F     h t t p : /
00 2F 00 7A-00 6F 00 6E-00 65 00 73-00 65 00 72    / z o n e s e r
00 76 00 65-00 72 00 79-00 75 00 37-00 38 00 39    v e r y u 7 8 9
00 2E 00 63-00 6F 00 6D-00 2F 00 E7-00 64 00 43    . c o m / τ d C
36 18 A0 04-98 04 98 00-90 4A 04 5F-2E 5F 2E 0A
84 1F AE 1E-AC 15 BA 03-96 15 BA 02-94 06 9C 15
DA 02 94 09-82 05 9A 47-1E 49 02 40-10 5E 2C 13
B6 1F AE 1D-AA 5F 2E 90-10 50 40 00-4C 50 40 00
88 50 40 00-24 10 40 00-30 10 40 00-3C 10 40 00
5C 10 40 00-70 10 40 00-84 10 40 00-94 10 40 00
A0 10 40 00-AC 10 40 00-B4 10 40 00-BC 10 40 00
C8 10 40 00-D0 10 40 00-D8 10 40 00-E0 10 40 00
E8 10 40 00-F4 10 40 00-04 11 40 00-0C 11 40 00
14 11 40 00-1C 11 40 00-24 11 40 00-2C 11 40 00
30 11 40 00-44 11 40 00-50 11 40 00-64 11 40 00
78 11 40 00-BC 11 40 00-44 12 40 00-4C 12 40 00
54 12 40 00-60 12 40 00-68 12 40 00-70 12 40 00
78 12 40 00-84 12 40 00-94 12 40 00-A0 12 40 00
A8 12 40 00-B0 12 40 00-B4 12 40 00-C0 12 40 00
00 13 40 00-30 13 40 00-44 13 40 00-78 13 40 00
A4 13 40 00-C8 13 40 00-04 14 40 00-58 C3 00 00
FF F0 00 00-FC C3 00 00-58 8D 7C 24-0C FF D0 90
```

Decrypted binary code, revealing one of three control servers.

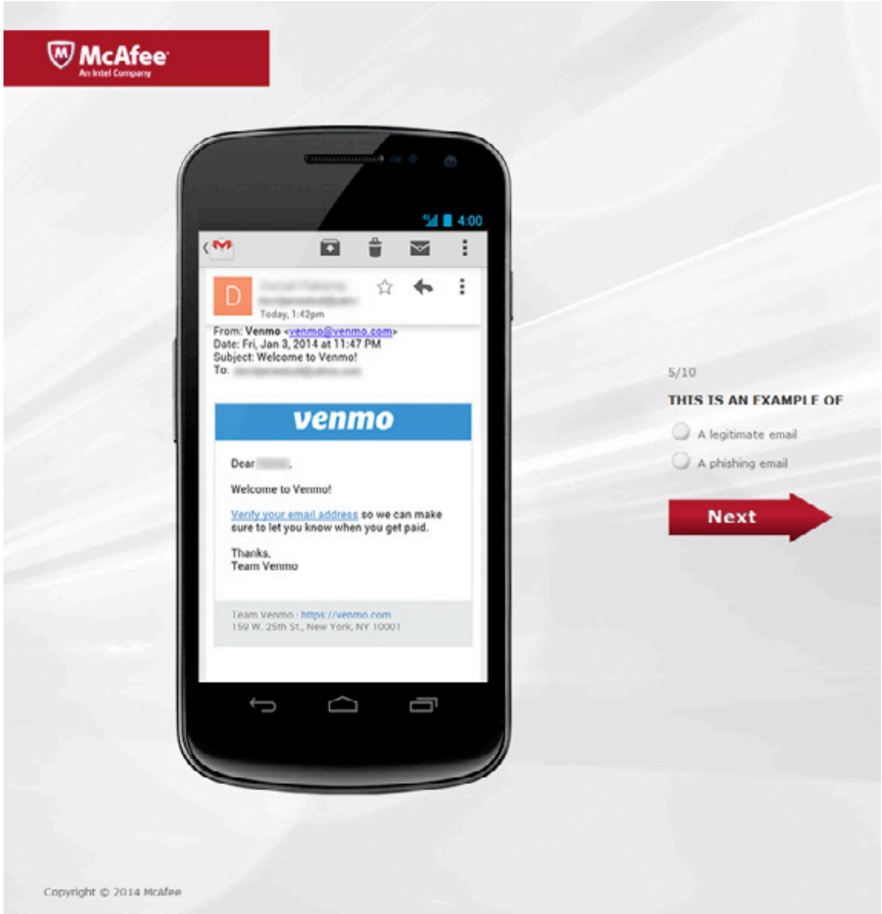
For more information on detecting spoofed emails claiming origin from amazon.com, **click here.**

Want to test your ability to detect phishing emails? Take the **McAfee Phishing Quiz.**

Next in the chain of events, additional malware is downloaded from the decrypted control domains. The success of these downloads is verified by the control servers, and the original sample takes the reins by installing autostart mechanisms such as .lnk files and registry entries for the new malware. In our observations, these have taken the form of a password stealer and a spam bot. You can imagine what type of data could be stolen once login credentials have been compromised. The newly infected host machine then continues the campaign, sending identical amazon.com order confirmation messages to fool the next unsuspecting recipients.

Phishing has proven to be effective again and again. Although technology can assist in detecting malware and bad senders, much of the onus for detecting fraud lies with the email recipient.

McAfee has been testing the ability of business users to detect phishing though our **McAfee Phishing Quiz,** which consists of 10 email messages presented in emulated email clients. The test asks respondents, as if they were looking at their own inboxes, to identify each sample as a real message or a phishing attempt. Each email sample contains active functionality, with the obfuscation of personally identifiable information and malicious content where necessary.



[redacted]
Today, 1:42pm

From: Venmo <venmo@venmo.com>
Date: Fri, Jan 3, 2014 at 11:47 PM
Subject: Welcome to Venmo!
To: [redacted]

venmo

Dear [redacted],

Welcome to Venmo!

Verify your email address so we can make sure to let you know when you get paid.

Thanks,
Team Venmo

Team Venmo · https://venmo.com
159 W. 25th St., New York, NY 10001

5/10

THIS IS AN EXAMPLE OF

○ A legitimate email
○ A phishing email

Copyright © 2014 McAfee

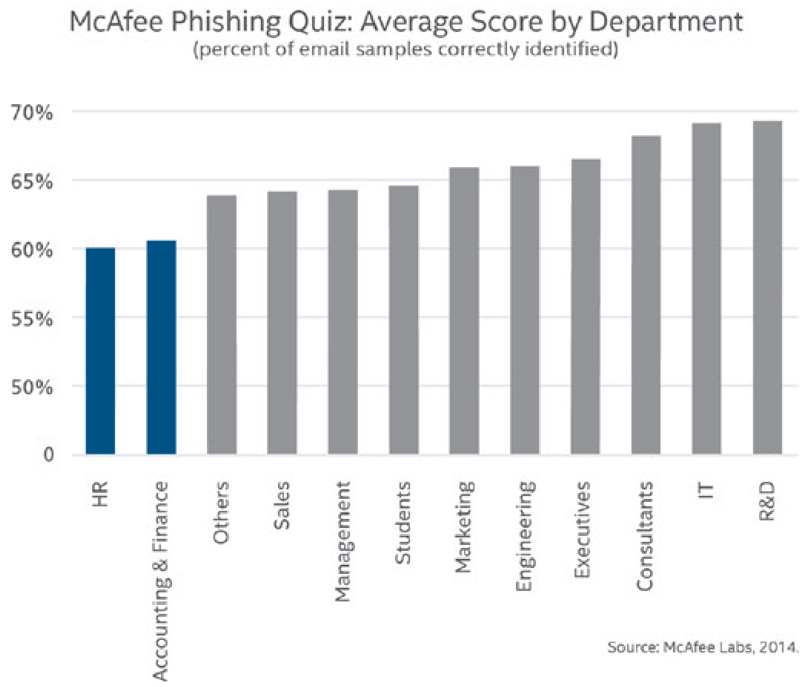
Sample question from the McAfee Phishing Quiz, presented in an Android mobile client.

Share this Report

Of the 16,000 business users who have taken the test, 80% fell for at least one phishing email. Although the respondents were not really in their own inboxes, we find this figure shockingly high. It takes only one successful delivery of malware to a vulnerable system to establish a foothold in almost any business.

> *80% of all test takers missed at least one of seven phishing emails. Accounting and Finance, and HR performed the worst.*

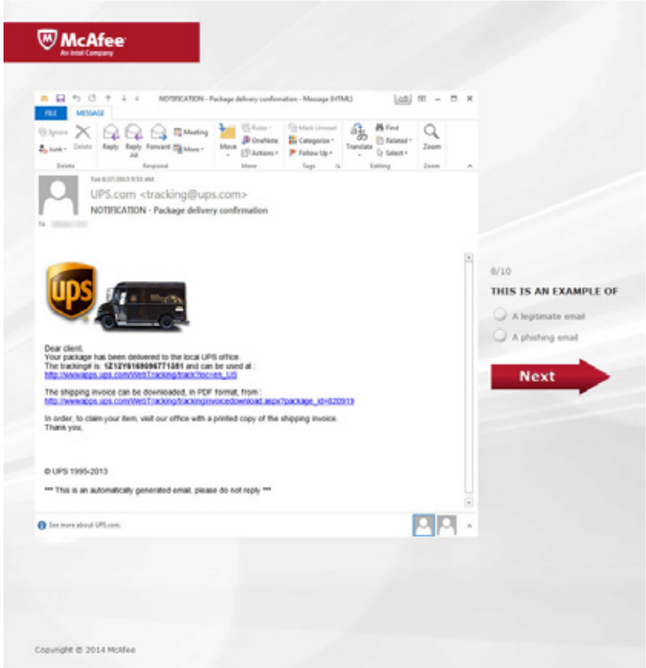
Further, averaging the accuracy rate at which respondents detect the legitimacy or illegitimacy of these messages, we discovered that the departments holding the most sensitive data performed the worst by a significant margin. As shown in the following chart, both accounting and finance and HR are the worst at detecting fraud, falling behind other departments by a margin of 4% to 9%. Access to systems in these departments can open the doors to a host of sensitive information. Clearly there is a need for additional security education in these areas.



Source: McAfee Labs, 2014.

Performance on the McAfee Phishing Quiz based on self-selected department.

We also identified the tactic that was most effective in fooling respondents—the use of spoofed email addresses. Two of our email samples used this tactic, and test takers missed them 63% and 47% of the time, respectively.



Tue 8/27/2013 9:53 AM
UPS.com <tracking@ups.com>
NOTIFICATION - Package delivery confirmation

Dear client,
Your package has been delivered to the local UPS office.
The tracking# is: 1Z12Y6169096771381 and can be used at :
http://wwwapps.ups.com/WebTracking/track?loc=en_US

The shipping invoice can be downloaded, in PDF format, from :
http://wwwapps.ups.com/WebTracking/trackinginvoicedownload.aspx?package_id=820919

In order, to claim your item, visit our office with a printed copy of the shipping invoice.
Thank you,

© UPS 1995-2013

*** This is an automatically generated email, please do not reply ***

THIS IS AN EXAMPLE OF

○ A legitimate email
○ A phishing email

Copyright © 2014 McAfee

UPS phishing email sample from the McAfee Phishing Quiz, presented in an Outlook email client.

The most successful phishing email sample appeared to be sent from UPS. The methods of disguise were common but effective. First, the sender address was spoofed to appear as if it originated from the UPS.com domain. Several UPS branding elements were part of the message, including the official logo. However, what we found most interesting was the use of only one malicious URL in the entire email. The first URL directed the recipient to track the shipment—and actually sent victims to the UPS package-tracking website. The second URL prompted a download of the "invoice," and it indeed opened a file—but not one in the UPS domain. That link delivered the payload: malware wrapped in a .zip archive.

Phishing is still heavily in use, and carries a high level of efficacy. It is not an easy problem to address, requiring both technology and behavioral filters. To give readers a sense of our best practices, we offer a short checklist to help guide security professionals. We're going to need all hands on deck for this one.

Reeling in Phishing Attempts: A Guide for Security Professionals

Activity	Key Technologies
Eliminate mass phishing campaigns with secure gateway email filtering	Sender IP, URL, file, and network reputations, antivirus (AV), and real-time block lists
Implement sender identity verification to reduce risk of cybercriminals being mistaken for trusted parties	Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC)
Detect and eliminate malicious attachments with advanced antimalware	File reputation, AV, content emulation, sandboxing, and static code analysis
Scan URLs in email when received, and again when clicked	URL reputation, AV, content emulation, sandboxing, and static code analysis
Scan web traffic for malware when phishing leads the user on a multiclick journey to infection	URL reputation, AV, content emulation, sandboxing, and static code analysis
Implement data loss prevention to stop exfiltration in the event of a breach or user input	Data loss prevention for endpoints, email traffic, and web traffic
Educate users on best practices in detecting and acting upon suspicious emails	**Follow this link for a list of recommended tips**

Source: McAfee Labs, 2014.

Share this Report

Operation Tovar: a big hit with a short life

Under Operation Tovar, global law enforcement—in conjunction with the private sector and McAfee Labs—launched an action to dismantle the infrastructure of Gameover Zeus and CryptoLocker. Taking control of domains that form part of the communications network provided a rare opportunity for owners of infected systems to remove the malware and take back control of their digital lives.

Distinct threats

The two threats are very different. Gameover Zeus is a peer-to-peer botnet based on the Zeus banking Trojan. Once Gameover Zeus finds its way onto a victim's computer, it attempts to steal various types of information. Cybercriminals have successfully used the malware in all manner of attacks. From the theft of online banking credentials, credit card numbers, and even login credentials for online job boards, the trail of destruction behind Gameover Zeus is substantial, netting criminals millions of dollars. For example, in August 2012 alone, estimates place the number of infections at more than 600,000 systems, many of these in Fortune 500 firms.

Estimates claim that Gameover Zeus has infected more than 600,000 systems, including many in Fortune 500 companies.

Gameover Zeus is based on the original Zeus, which steals banking credentials, but works differently in that it decentralizes the control system and creates a peer-based network. Victims are typically infected via spear phishing campaigns that use various browser- and web-based exploits to deliver the malware onto the targeted system. The malware injects itself into legitimate Windows processes to maintain persistence, and also hooks system and browser functions to inject "fake" content into a user's browser to conceal fraudulent activity.

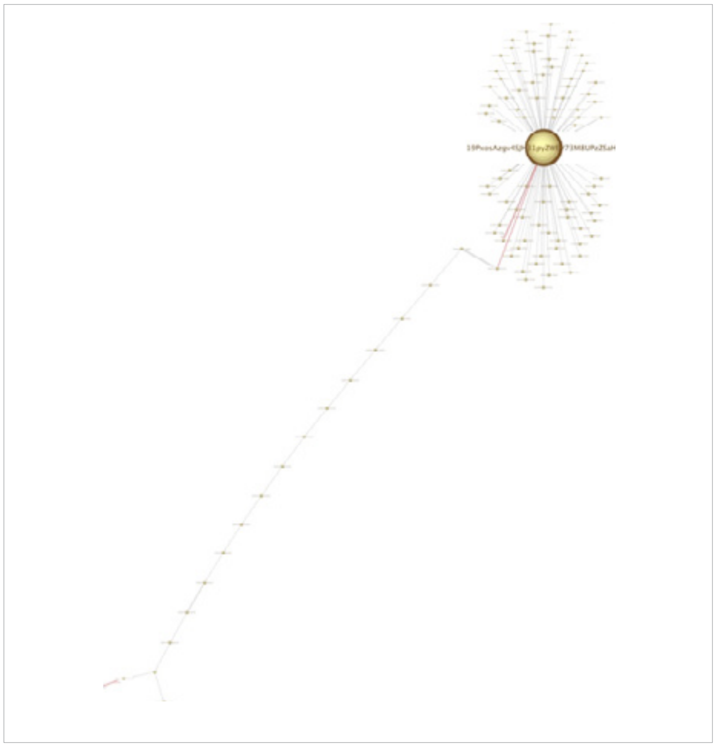
This method is highly effective when the criminal wants to steal large sums of money from a business account but needs to conceal the activity until the funds are wired to the criminal's account. Variants of Gameover Zeus get their updates and configurations from available hosts on the peer network—making it much more difficult to disrupt. Gameover Zeus also has a function to dynamically update the configuration file that contains the payload for stealing funds from a user's bank account.

CryptoLocker is a ransomware Trojan that encrypts the victim's files and holds them ransom until payment is made, generally with a virtual currency such as Bitcoin. Having encrypted a system, CryptoLocker generates a pop-up demanding that the victim pay to recover the files. The malware uses public key cryptography algorithms to encrypt the victim's files. Once the victim's machine is infected, the key is generated and the private key is sent to the criminal's server. The malware typically gives the victim 72 hours before the CryptoLocker server is supposed to destroy the private key, making the files unrecoverable. CryptoLocker victims are infected via phishing emails and botnets.

McAfee Labs has researched CryptoLocker since September 2013. During one recent investigation, we discovered a family of malware samples that pointed to a portal that charged BTC 0.7 (about $461 at the time of this writing) for decrypting files. Tracing the Bitcoin transaction stream revealed some interesting data. During a single day, 83 victims paid BTC 76 ($35,036) for decryption. We also observed that the criminals behind this campaign own multiple wallets and transferred large amounts of Bitcoin between them, ultimately landing in just two wallets.

During one observed month, Wallet A contained BTC 110.892 and Wallet B BTC 442.477. Using current Bitcoin exchange rates, those figures total about $255,000, all earned in one month. Ransomware is indeed a profitable business.

In one CryptoLocker ransomware instance, McAfee Labs observed the theft of $255,000 in a single month.



CryptoLocker Bitcoin transfer stream.

McAfee Stinger, a free tool that detects and removes malware, was downloaded more than 80,000 times in the three days following the Operation Tovar announcement.

The Gameover Zeus and CryptoLocker takedown

Both Gameover Zeus and CryptoLocker make use of domain-generating algorithms (DGAs). In the case of CryptoLocker, the malware binary first tries to connect to a hardcoded control server with an IP address. If this attempt fails, it generates a domain name using a random domain name algorithm.

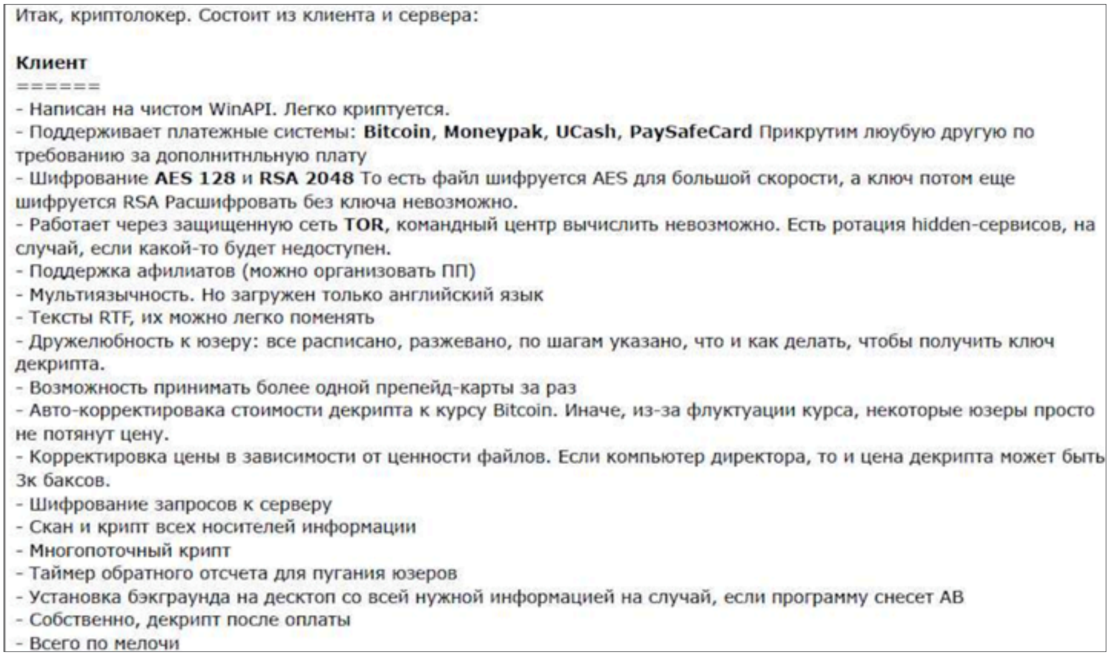
During Operation Tovar, the DGAs of both malware families were cracked, allowing law enforcement to predict the domain names that would be generated through 2014. By blocking and sinkholing these domains, customers were either prevented from communicating with the control server or from downloading further payloads. For CryptoLocker alone, more than 125,000 domains were blocked during the operation and more than 120,000 Gameover Zeus domains were sinkholed. In the three days following the announcement of Operation Tovar, McAfee Stinger, a free tool that detects and removes malware (including Gameover Zeus and CryptoLocker), was downloaded more than 80,000 times. Similar tools saw download increases in the 300% to 400% range.

A sinkhole is a DNS server that has been configured to return nonroutable addresses for all domains in the sinkhole, so that every computer requesting domain address resolution will be unable to connect with the target. Sinkholes are common and effective at detecting and blocking malicious traffic.

The future

Although Operation Tovar was a huge success, many copycats are on the rise, creating new variants of ransomware or financial-targeting malware using the leaked Zeus source code.

We already see new projects in underground forums:



Итак, криптолокер. Состоит из клиента и сервера:

Клиент

======

- Написан на чистом WinAPI. Легко криптуется.
- Поддерживает платежные системы: **Bitcoin**, **Moneypak**, **UCash**, **PaySafeCard** Прикрутим люубую другую по требованию за дополнитнльную плату
- Шифрование **AES 128** и **RSA 2048** То есть файл шифруется AES для большой скорости, а ключ потом еще шифруется RSA Расшифровать без ключа невозможно.
- Работает через защищенную сеть **TOR**, командный центр вычислить невозможно. Есть ротация hidden-сервисов, на случай, если какой-то будет недоступен.
- Поддержка афилиатов (можно организовать ПП)
- Мультиязычность. Но загружен только английский язык
- Тексты RTF, их можно легко поменять
- Дружелюбность к юзеру: все расписано, разжевано, по шагам указано, что и как делать, чтобы получить ключ декрипта.
- Возможность принимать более одной препейд-карты за раз
- Авто-корректировака стоимости декрипта к курсу Bitcoin. Иначе, из-за флуктуации курса, некоторые юзеры просто не потянут цену.
- Корректировка цены в зависимости от ценности файлов. Если компьютер директора, то и цена декрипта может быть 3к баксов.
- Шифрование запросов к серверу
- Скан и крипт всех носителей информации
- Многопоточный крипт
- Таймер обратного отсчета для пугания юзеров
- Установка бэкграунда на десктоп со всей нужной информацией на случай, если программу снесет AB
- Собственно, декрипт после оплаты
- Всего по мелочи

A malware project similar to CryptoLocker.

The preceding screenshot came from an underground forum offering a "CryptoLocker-like service" for $3,000. Features included:

- Use of AES 128 and RSA 2048 encryption.
- Use of TOR services.
- Support for affiliation platforms.
- Ransom price adjustment based on Bitcoin rate and a selection of victim's file types to encrypt.
- Creation of Bitcoin wallets for each client.
- Accepting prepaid cards, such as iTunes and others.

Gameover Zeus and CryptoLocker are nasty threats and have been very lucrative for their developers. Operation Tovar has been a great success, severely crippling this criminal infrastructure. Further, many users have been able to clean their systems. That's a rare victory for those plagued with malware. However, malware developers are persistent because there's so much money to be made. We have already seen replacement malware and infrastructures appear.

Operations such as Tovar are designed to combat cyberthreats that impact businesses, infrastructure, individuals, and other targets. Cooperation among many players—global law enforcement agencies, ISPs, and security vendors—made this operation successful. During the past six months, several criminals were arrested and sentenced to lengthy jail terms. Cybercrime can be lucrative, but Operation Tovar demonstrates that attackers will not always get away with it. McAfee Labs will assist with these operations at all times.

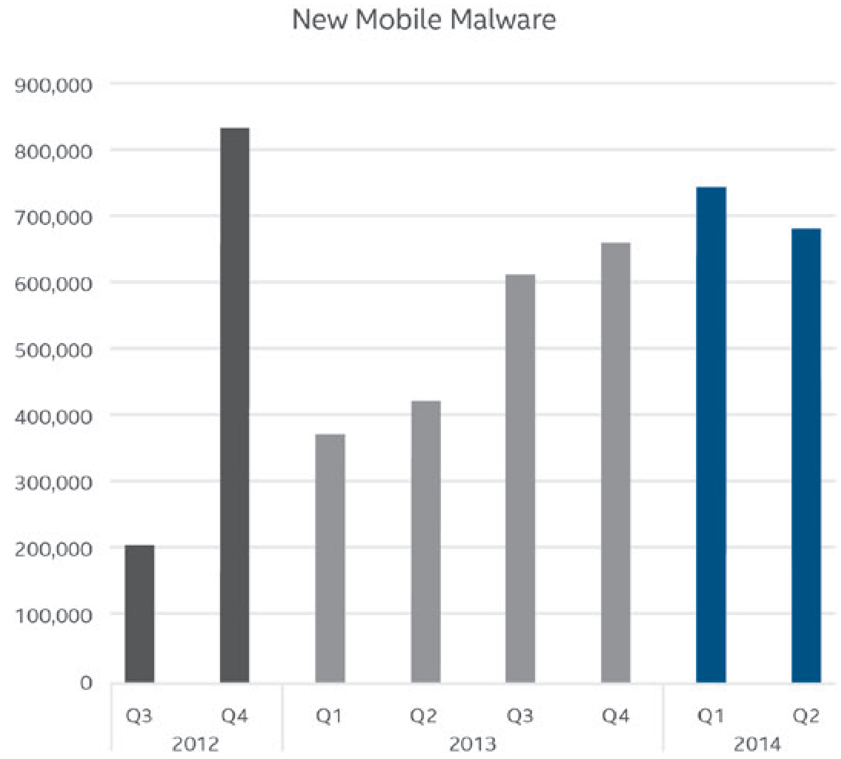
Threat Statistics

Mobile malware
Malware
Web threats
Messaging threats
Network threats

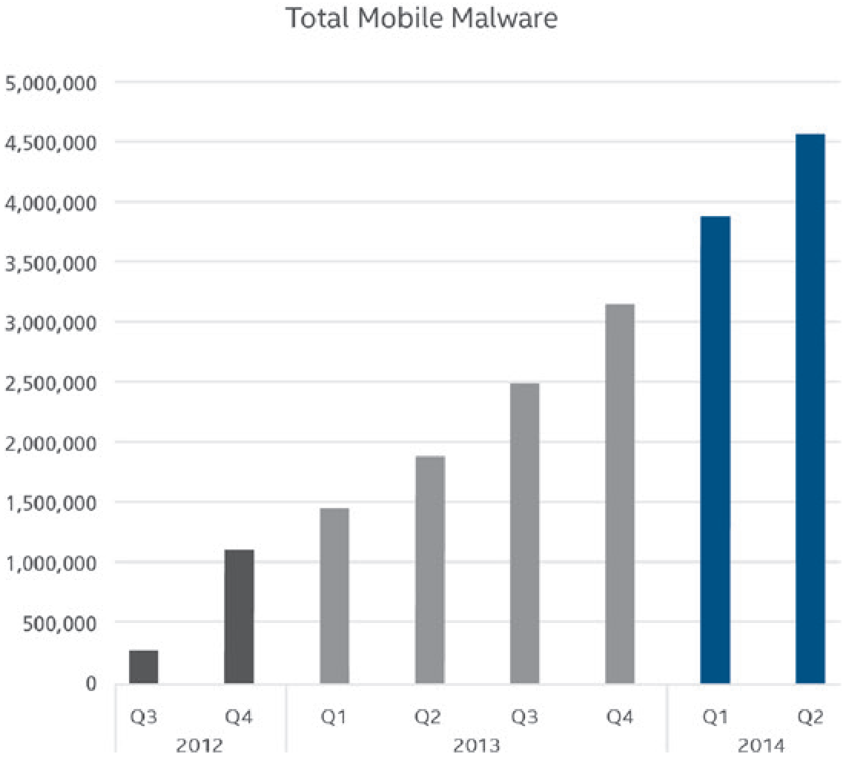
Share feedback

Mobile malware

Our total count of mobile malware increased by 17% in Q2. Meanwhile, the rate of new mobile malware appears to have leveled off at about 700,000 per quarter.



Source: McAfee Labs, 2014.

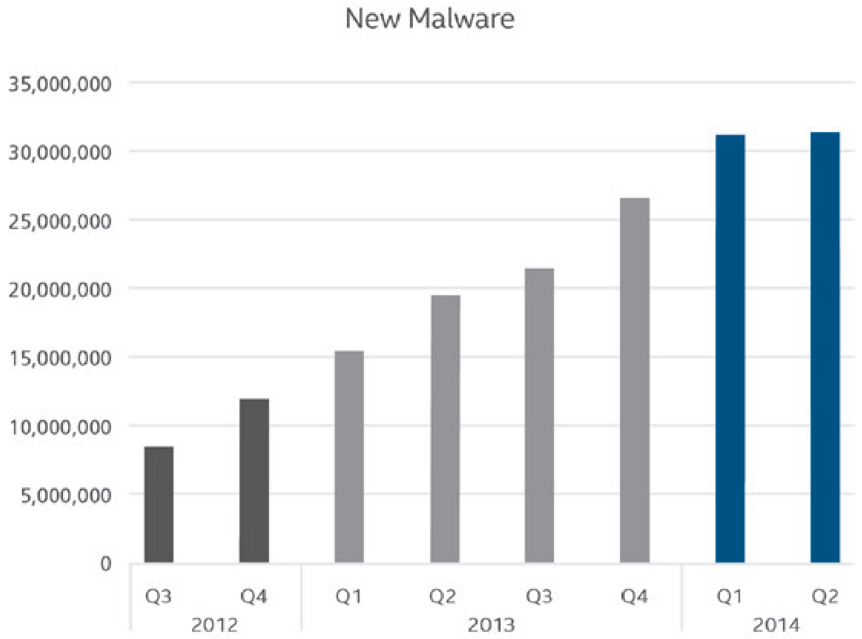


Source: McAfee Labs, 2014.

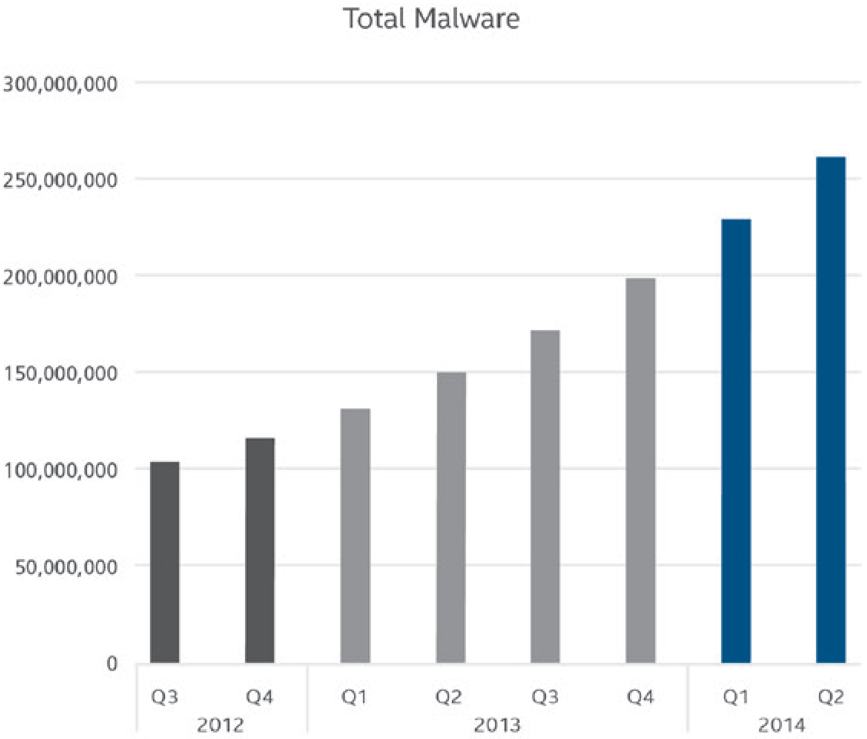
Share this Report

Malware

New malware in Q2 rose by only 1%, although at more than 31 million new samples this is still the largest amount we have recorded in a single quarter.



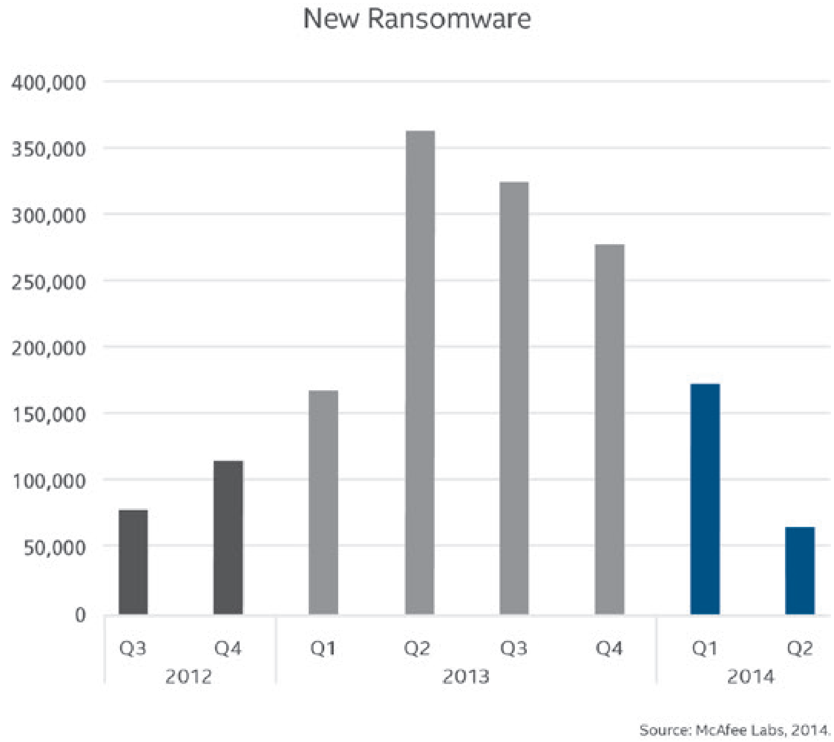
Source: McAfee Labs, 2014.



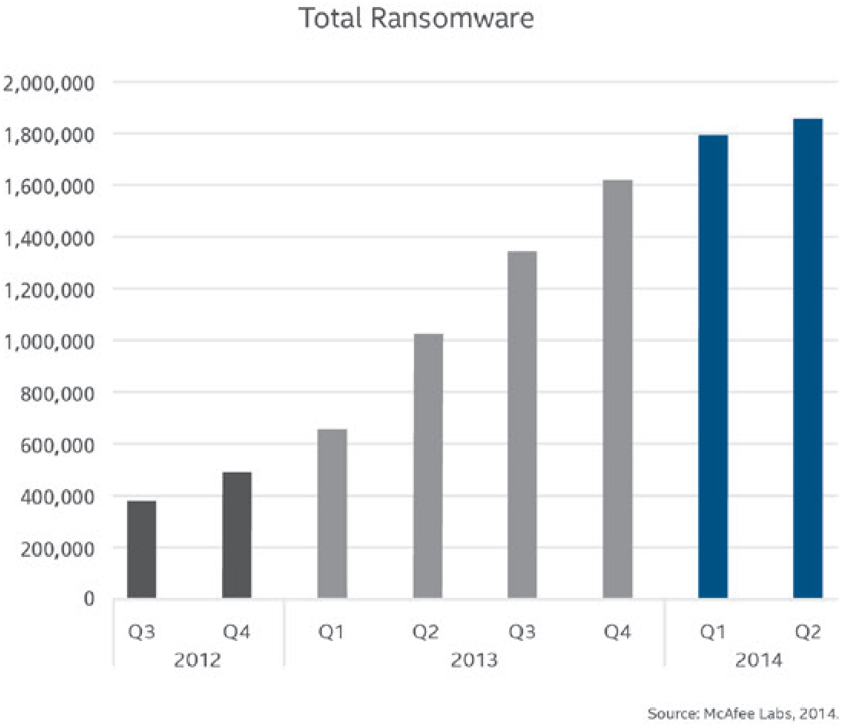
Source: McAfee Labs, 2014.

Share this Report

New ransomware continued the decline that began one year ago, falling 63% during this quarter to 63,857 new samples.



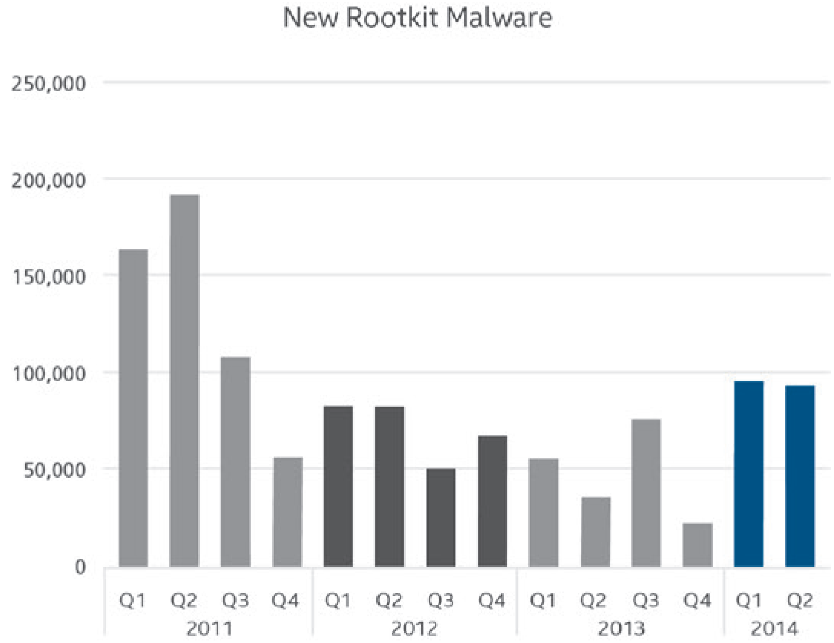
Source: McAfee Labs, 2014.



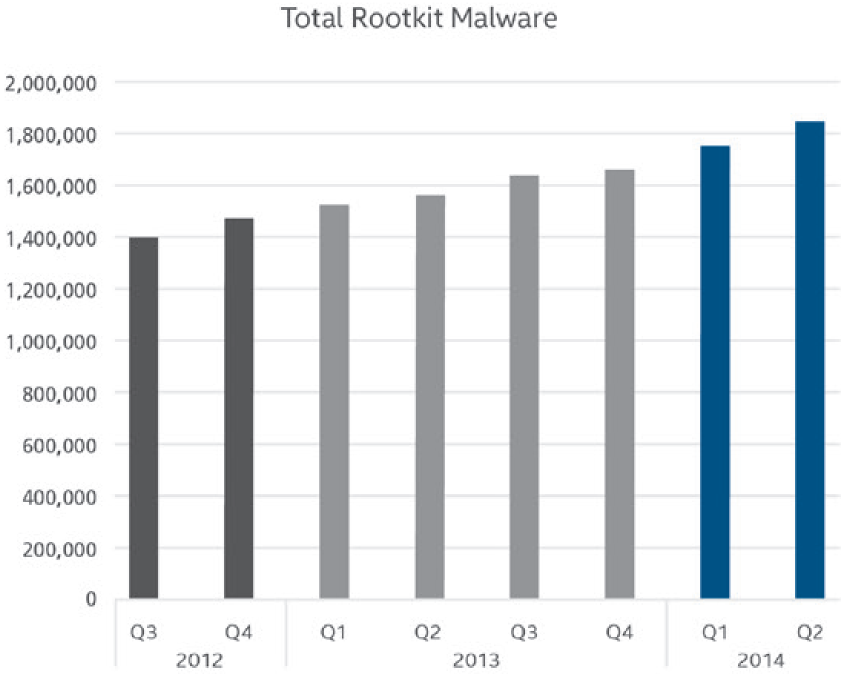
Source: McAfee Labs, 2014.

Share this Report

The trend in rootkits is generally flat, with a single bootkit family, Gupboot, responsible for the increase during the past two quarters. As noted in our ***McAfee Labs Threats Report, June 2014,*** we believe that new rootkit samples will grow as attackers learn how to circumvent security protection in 64-bit systems.



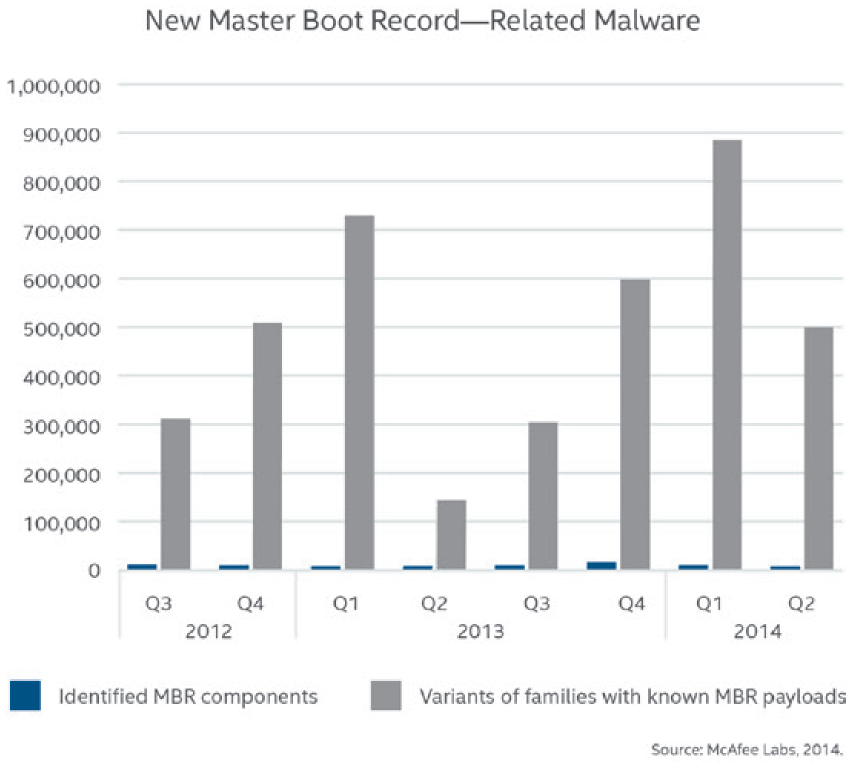
Source: McAfee Labs, 2014.



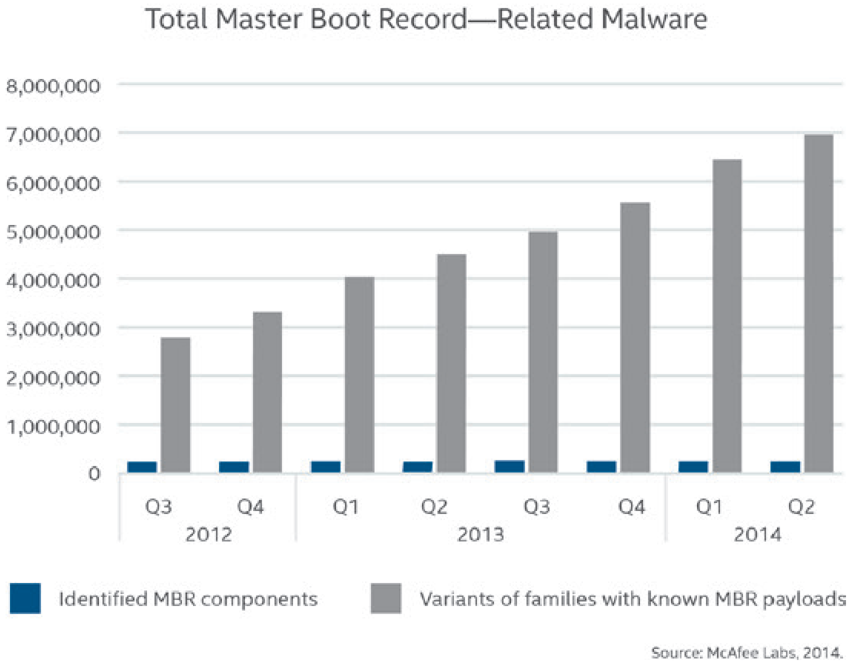
Source: McAfee Labs, 2014.

Share this Report

Threats that attack a system's master boot record dropped by 44% this quarter.



Source: McAfee Labs, 2014.

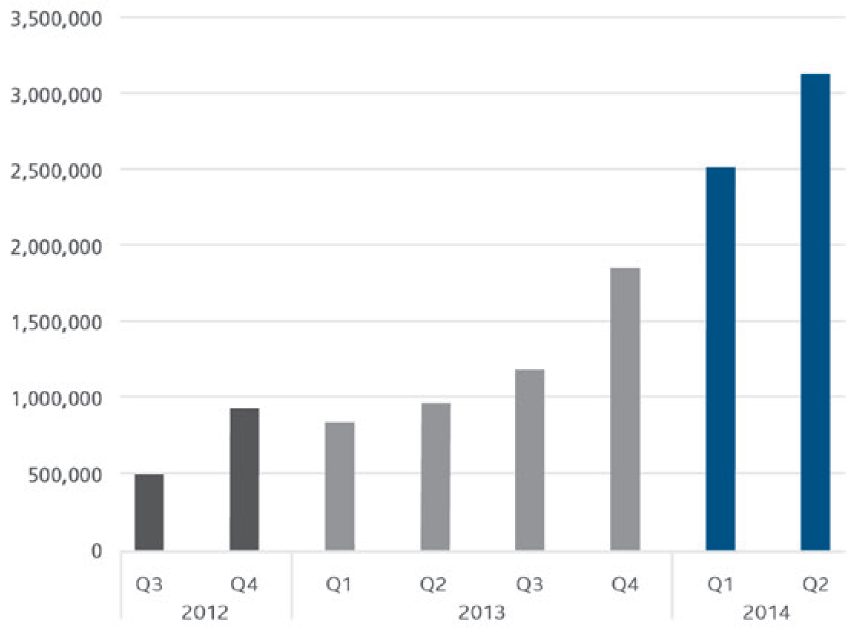


Source: McAfee Labs, 2014.

Share this Report

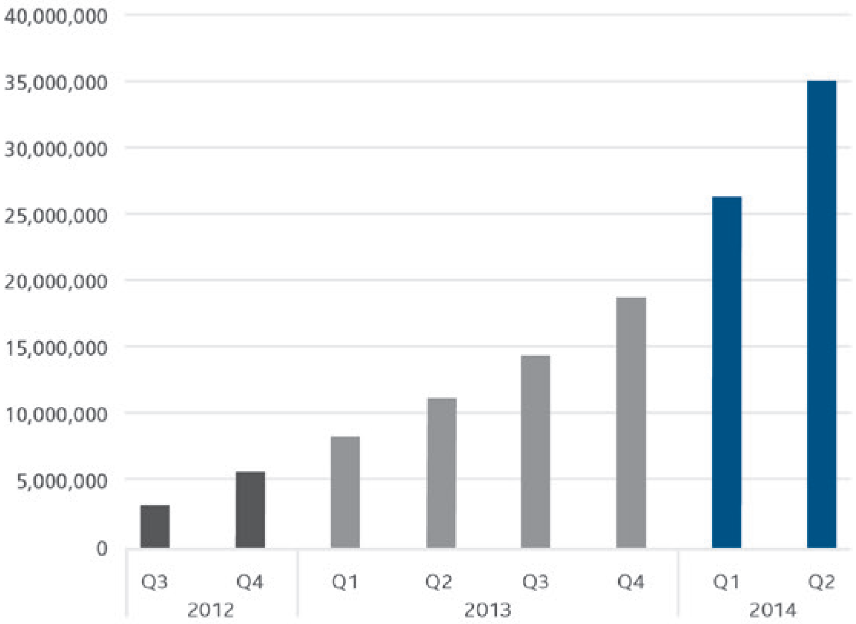
Continuing its relentless rise, new malicious signed binaries passed the 3 million per quarter barrier in Q2.

New Malicious Signed Binaries



Source: McAfee Labs, 2014.

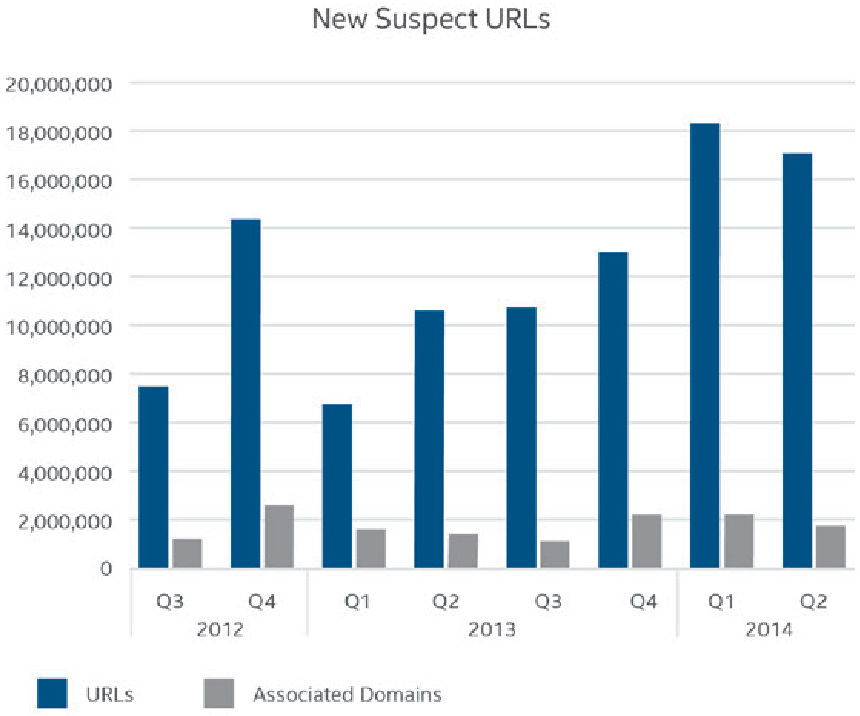
Total Malicious Signed Binaries



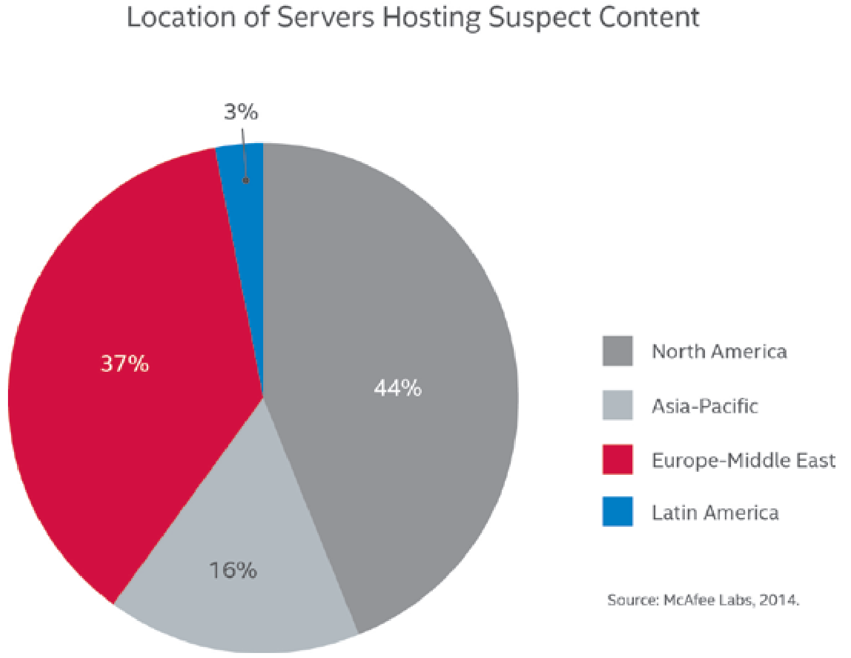
Source: McAfee Labs, 2014.

Share this Report

Web threats



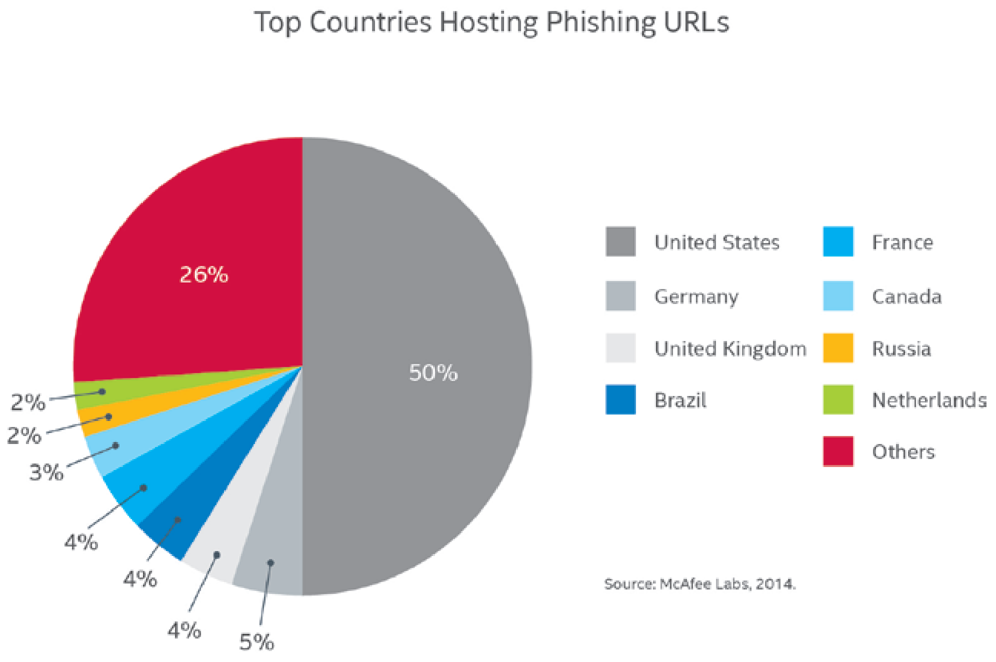
Source: McAfee Labs, 2014.



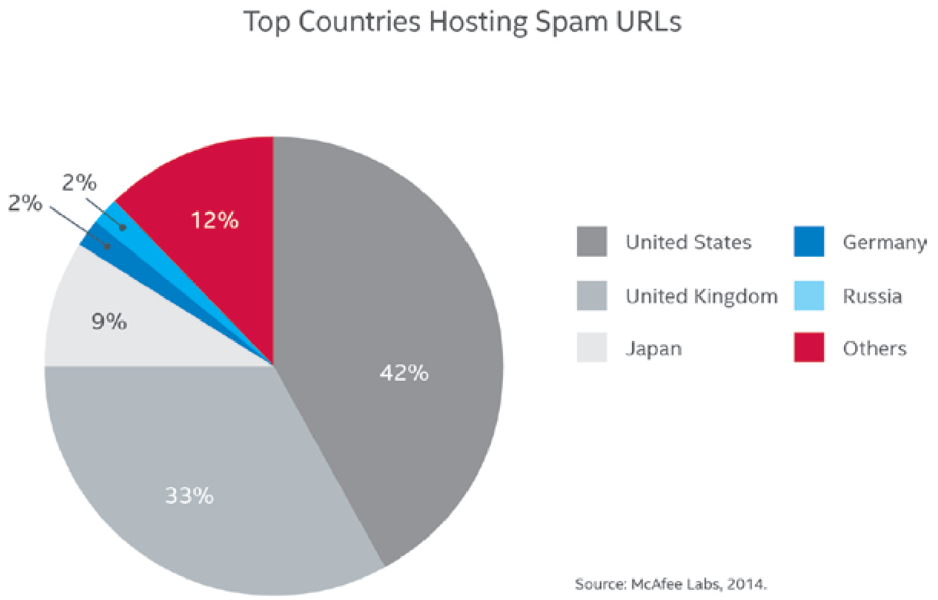
Source: McAfee Labs, 2014.

North America continues to host more suspect content than any other region.

Share this Report



Source: McAfee Labs, 2014.

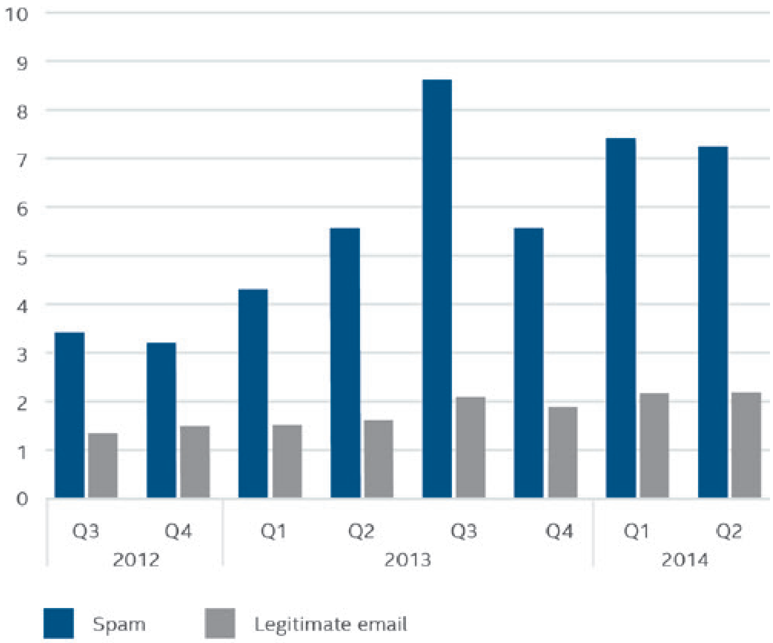


Source: McAfee Labs, 2014.

Share this Report

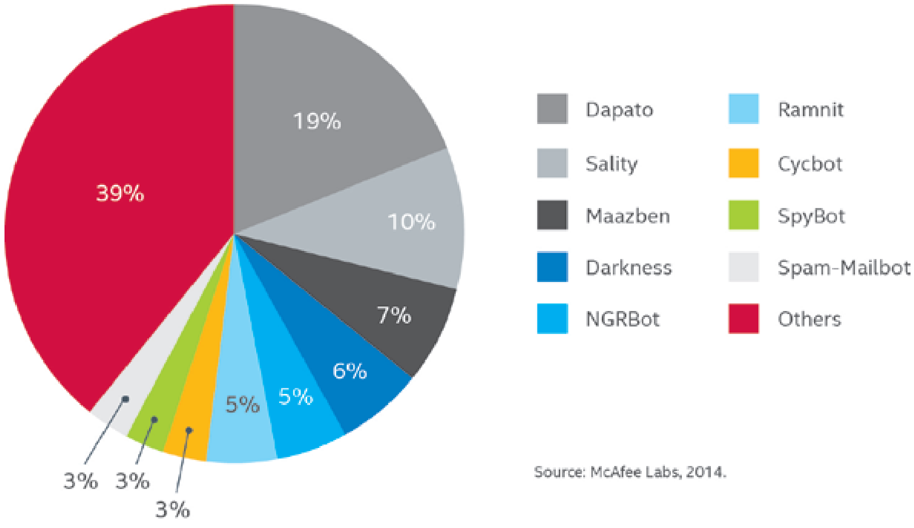
Messaging threats

Global Spam and Email
(trillions of messages)



Source: McAfee Labs, 2014.

Worldwide Botnet Prevalence



Source: McAfee Labs, 2014.

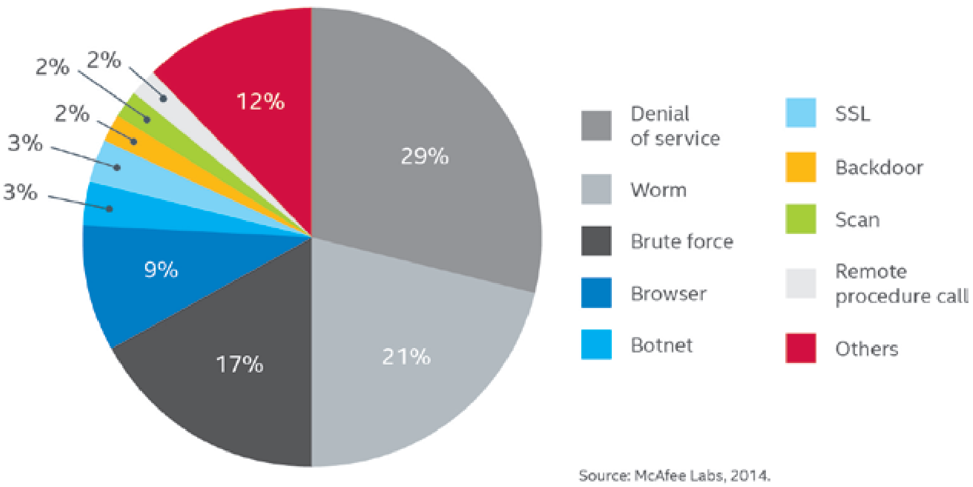
The number of infections by the Dapato botnet, also known as Carberp and by other names, rose dramatically this quarter.

Share this Report

Network threats

Denial of service attacks rose by 4% this quarter and remain the most prevalent type of network threat.

Top Network Attacks



Source: McAfee Labs, 2014.

Share this Report

Feedback. To help guide our future work, we're interested in your feedback. If you would like to share your views, please **click here** to complete a quick, five-minute Threats Report survey.

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] http://blog.erratasec.com/2014/06/300k-vulnerable-to-heartbleed-two.html#.U8P7VY1dVYO.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "as is," without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.