Report

McAfee Labs
Threats Report

May 2015

intel Security

McAfee Labs saw almost twice the number of ransomware samples in Q1 than in any other quarter.

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.

McAfee is now part of Intel Security.

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

Follow McAfee Labs

Introduction

This Threats Report marks the first time that we explore firmware-based attacks. In our lead Key Topic, we provide new details about malware from a secretive outfit called **the Equation Group.** This threat is capable of reprogramming hard disk drive firmware. Our analysis shows the reprogrammed firmware can reload associated malware each time the infected system boots and that it persists even if the hard drive is reformatted or the operating system is reinstalled. We suspect this type of threat will be a hot topic at Black Hat and DefCon this year.

We also focus on two familiar faces—ransomware and Adobe Flash exploits—because McAfee Labs saw massive increases in new samples this quarter from both types of threat. For ransomware, we attribute much of its growth to a new, hard-to-detect ransomware family—CTB-Locker—and its use of an "affiliate" program to quickly flood the market with phishing campaigns, leading to CTB-Locker infections. And for the rise in Flash exploits, we attribute those to the growing number of Flash instances across many platforms (most notably mobile devices), the number of known, unpatched vulnerabilities, and the difficulty in detecting some Flash-based exploits.

Other items of note:

- By the time this report is published, **RSA Conference 2015** will be history. For those who attended, we hope you had a chance to listen to **Intel Security's keynote,** presented by **Chris Young, General Manager of Intel Security Group.** If you could not attend, a replay is available **here.** Young articulated Intel Security's vision for changing the way the IT security industry and its customers think about threat intelligence and real-time security incident and attack data. He emphasized that we need to go beyond just gathering and processing more data. We must find more value in our data by analyzing it in new and creative ways. It is well worth a listen.
- In addition to providing world-class threat research, threat intelligence, and cybersecurity thought leadership, McAfee Labs develops core technologies that are incorporated into Intel Security products. Recently, several notable advancements have been made to some of these core technologies:
  - The **McAfee Global Threat Intelligence service** provides file, web, IP, certificate, and email reputation information to Intel Security products. It handles tens of billions of queries per day and protects millions of systems every hour.
  - Recently, McAfee GTI's underlying cloud infrastructure was replaced—rather like replacing an engine in a car while it's moving at 100 miles an hour—to handle far more queries, more threat data, and more reputation types. It was also rearchitected to be faster, safer, more secure, more resilient, and easier to manage.
  - Late last year, Intel Security began shipping endpoint products containing "DAT reputation" technology. McAfee Labs tests our signature files extensively before publication, but there can be rare circumstances in which a DAT impacts customers. Many of our endpoint products now detect, contain, and mitigate DAT-based incidents very quickly. This enhances the safety of those products. More information about our DAT reputation technology can be found **here.**
- We continue to receive valuable feedback from our readers through our Threats Report user surveys. If you would like to share your views about this Threats Report, please **click here** to complete a quick, five-minute survey.

—Vincent Weafer, Senior Vice President, McAfee Labs

Contents

McAfee Labs Threats Report
May 2015

This report was researched and written by:

Christiaan Beek
Alexander Matrosov
François Paget
Eric Peterson
Arun Pradeep
Craig Schmugar
Rick Simon
Dan Sommer
Bing Sun
Santosh Surgihalli
James Walter
Adam Wosotowsky

Executive Summary

The Equation Group: exploiting hard disk and solid state drive firmware

Systems compromised by the Equation Group remain infected even if the hard drive is reformatted or the operating system is reinstalled. This is among the most sophisticated malware ever seen.

In February, news broke about a rare but extremely sophisticated attack campaign. The "Equation Group," named for their affinity for complex encryption schemes, is thought to be behind the attacks. The most alarming discovery is that the Equation Group's malware includes hard disk drive and solid state drive reprogramming modules. Once reprogrammed, a compromised system remains infected even if the hard drive is reformatted or the operating system is reinstalled. Further, the reprogrammed firmware and associated malware is undetectable by security software. This marks the first time in a Threats Report that McAfee Labs examines a firmware-based attack.

Ransomware returns: new families emerge with a vengeance

McAfee Labs has seen a huge rise in ransomware in Q1, mostly from a new ransomware family—CTB-Locker—and its "affiliate" program that quickly flooded the market with phishing campaigns.

In the ***McAfee Labs Threats Report: November 2014,*** we offered this prediction for 2015: "Ransomware will evolve its methods of propagation, encryption, and the targets it seeks." Sure enough, a new ransomware family has emerged—CTB-Locker. It is distributed in many ways, including Internet relay chat, peer-to-peer networks, newsgroup postings, email spam, and more. It has been extensively localized to minimize suspicion from email recipients. And to circumvent security products, the downloader is hidden in a .zip file that contains another .zip file and eventually unpacks to a screensaver file. Moreover, the authors established an underground "affiliate" program to quickly flood the market with phishing campaigns, leading to CTB-Locker infections. As a result, Q1 saw a massive increase in the number of ransomware samples, mostly due to this new family.

Adobe Flash: a favorite of designers and cybercriminals

Adobe Flash exploits grew 317% in Q1. Flash is an attractive attack vector because it is widely installed on many platforms, there are many known, unpatched vulnerabilities, and exploits are often hard to detect.

Adobe Flash has long been an attractive attack surface for cybercriminals. It is widely installed on many platforms; there are many known, unpatched vulnerabilities; and exploits are often hard to detect. Couple those elements with the rise of the Angler exploit kit—detailed in the ***McAfee Labs Threat Report: February 2015***—and you have a recipe for successful cyberattacks. In fact, the number of new Adobe Flash malware samples detected by McAfee Labs skyrocketed to almost 200,000 in Q1, an increase of 317% from the 47,000 samples detected in the last quarter of 2014. In this Key Topic, we examine Adobe Flash: how it works, the growing number of vulnerabilities and exploits, how cybercriminals are exploiting them, and what businesses can do protect against these exploits.

Key Topics

The Equation Group: exploiting hard disk and solid state drive firmware

Ransomware returns: new families emerge with a vengeance

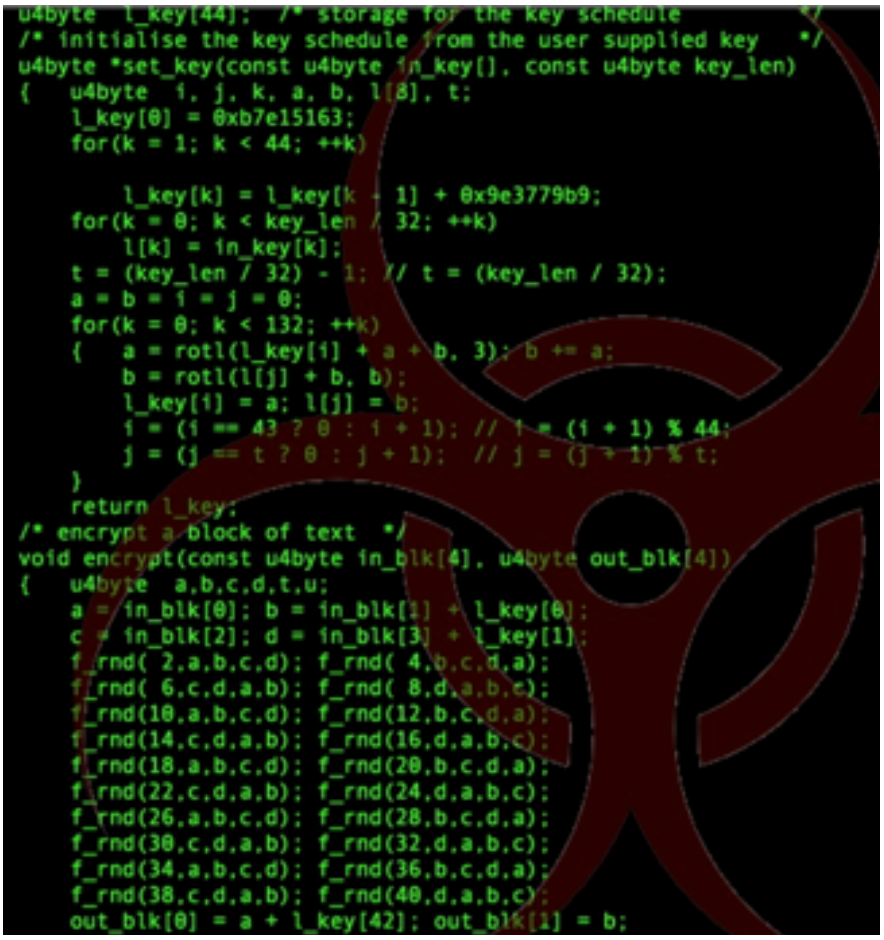
Adobe Flash: a favorite of designers and cybercriminals

Share feedback

The Equation Group: exploiting hard disk and solid state drive firmware

—James Walter and Alexander Matrosov

In February, **news** of a freshly discovered (yet very long-running) attack campaign spread wildly. The "Equation Group," named for its affinity for ultrasophisticated encryption schemes and associated malware, is now among the most sophisticated threats ever observed.



Code from the RC6 encryption algorithm used by the Equation Group.

One of the most significant finds by the Intel Security Advanced Threat Research team concerns hard disk drive (HDD) and solid state drive (SSD) firmware reprogramming modules. HDDs/SSDs whose firmware has been reprogrammed can reload associated malware each time infected systems boot and the threat remains persistent even if the drives are reformatted or the operating system is reinstalled. Further, the reprogrammed firmware and associated malware is undetectable by security software once they have infected the drive.

With the discovery of "Equation Group–specific" samples, we now consider these one of the most visible and advanced examples of firmware attack ever seen.

During the last several years, Intel Security has observed many examples of malware with firmware or BIOS manipulation capabilities. We have seen both academic proofs of concept and in-the-wild scenarios, including **CIH/Chernobyl,** Mebromi, and **BIOSkit.** We also predicted this specific attack type in the ***McAfee Labs 2012 Threats Predictions report.*** With the discovery of "Equation Group–specific" samples, we now consider these one of the most visible and advanced examples of firmware attack ever seen.

Equation Group HDD/SSD firmware reprogramming modules

The Equation Group's malware is composed of multiple modules or "platforms," each with specific functionality.

Equation Group Module	Module Function
DoubleFantasy	Target confirmation, validating recon, responsible for module and platform upgrades
EquationDrug	Full module and robust attack platform. One of the primary and persistent pieces. Holds HDD firmware reprogramming module(s).
EquationLaser	Legacy OS-compatible module (Windows 95/98)
Equestre	Interchangeable name associated with EquationDrug
Fanny	Worm component. Primarily targets specific regions.
GrayFish	Registry-resident attack platform. Includes bootkit. Holds HDD firmware reprogramming module(s).
TripleFantasy	Backdoor, target-validation Trojan

Some Equation Group modules date to 2001, which is quite old in malware terms. Despite that, these modules are one of the most sophisticated attack platforms we have seen. Threat researchers continue to uncover new behaviors every year.

The most recently discovered HDD/SSD firmware reprogramming modules were compiled starting in 2010. Both 32-bit and 64-bit versions of the plug-ins have been found. Although the analyzed samples target only Microsoft Windows systems, there are indications that versions also exist for Apple iOS and OS X systems. These new Windows-targeted modules leverage older, but still very powerful, Equation Group modules.

The modules do two things. One module reprograms the HDD/SSD firmware with code that is custom built for the HDD/SSD brand and model. The second module provides an API into a hidden area of the HDD or SSD. Through the API, the reprogrammed firmware can store and load custom payload code that can perform a variety of functions while remaining invisible to the operating system. If these new modules are similar in sophistication to other Equation Group modules, threat researchers will likely discover new behaviors for many years.

These functions deliver several powerful and important benefits to the Equation Group.

- Persistency: The reprogrammed firmware can survive disk reformatting and operating system reinstallation or reimaging.
- Invisibility: The hidden storage area is known only to the firmware and it remains intact even if the HDD/SSD is reformatted.
- Persistent firmware: In some cases, the key elements of the reprogrammed firmware will even survive reflashing (replacing) the HDD's or SSD's firmware.
- Undetectability: The reprogrammed firmware and associated malware is undetectable by security software once the drive has been infected.

Once a drive has been infected, the Equation Group HDD/SSD firmware reprogramming modules are persistent through disk reformatting or operating system reinstallation, hide drive space from OSs, and cannot be detected by security software.

File Name: nls_933w.dll_11FB08B9126CDB4668B3F5135CF7A6C5
MD5 Hash Identifier: 11FB08B9126CDB4668B3F5135CF7A6C5
SHA-1 Hash Identifier: FF2B50F371EB26F22EB8A2118E9AB0E015081500
File Size: 212480
File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

This DLL contains code that can communicate directly with hard drives through the ATA command interface.

As noted earlier, the firmware reprogramming code is specific to particular HDD/SSD manufacturers, including Western Digital, Samsung, Maxtor, Toshiba, IBM, and Seagate. The resource section of the module (nls_933w.dll) we analyzed contains a small x86 kernel-mode driver (about 20KB) that can communicate with infected hard drives via the ATA command interface.[1] The firmware update process requires that the target drive has undocumented ATA commands. Such command sets are readily available[2] and are frequently used for both good (for example, law enforcement, forensics) and malicious reasons.

ATA commands are commonly used to control and manipulate the mechanical and electrical behavior of drives. They can also control or toggle specific features.

Examples of Maxtor commands:

- Check power mode
- Download microcode
- Flush cache
- Device configuration identify
- Security erase unit
- Security unlock
- Smart write log

Many ATA commands are shared across drive manufactures; the firmware reprogramming module takes advantage of those wherever possible.

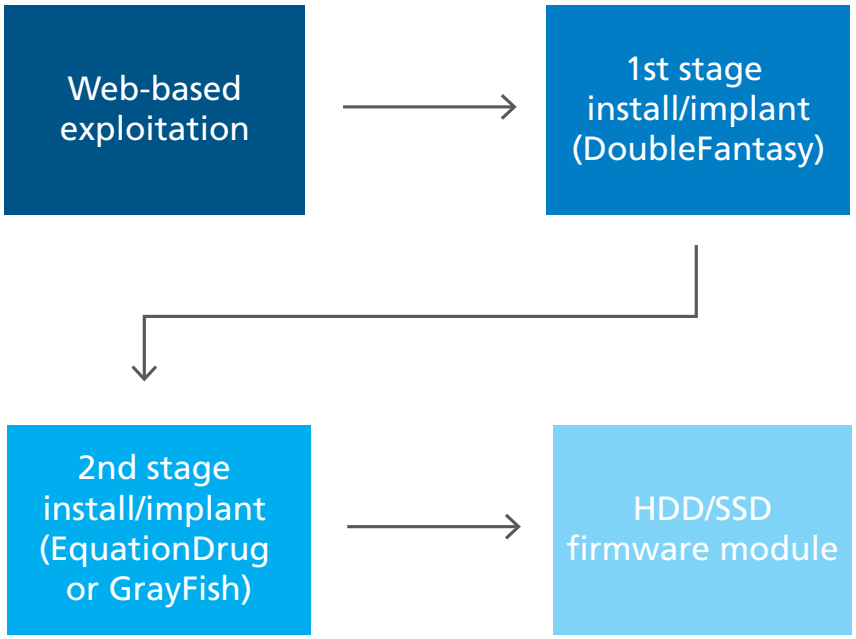
The file nls_933w.dll was compiled in 2010. However, it drops an additional driver (win32m.sys—MD5: 2b444ac5209a8b4140dd6b747a996653) onto the system that was compiled in 2001. The infectious driver is dropped into the %WINDIR%\System32\drivers\win32m.sys directory on victims' machines. Although there are more recent examples of the HDD modules, this one appears to be Version 3.0.1.

Infection mechanism for HDD/SSD firmware modules

The infection footprint and methodologies differ across Equation Group platforms. However, there are some specific and consistent behaviors in the delivery of the HDD/SSD firmware modules.

The initial infection vector is a web-based exploit. The Equation Group employs a "watering hole" attack, in which they infect websites frequented by their targets. When the victim visits one of those sites, the target's system is infected by the DoubleFantasy first-stage malware. DoubleFantasy confirms the target, runs various recon activities, and (once confirmed) delivers the second-stage malware—either EquationDrug or the newer GrayFish. The second-stage platform then manages the installation and maintenance of the HDD/SSD firmware reprogramming modules.

Equation Group HDD/SSD Attack Steps



Attribution

Who is behind the Equation Group and what other attacks have they supported? The Equation Group has been linked to **Flame, Duqu, Stuxnet,** and Gauss. Our analysis shows similarities in the writing style and use of specific structures and methodologies in the code and infection patterns of these attacks. There are also strong similarities in the use of RC5 or RC6 encryption. In some cases, the encryption is identical to other attacks.

In addition, the string-encoding algorithms appear to be based on the same basic idea or source. Comparing code attributed to the Equation Group with code from Flame and TripleFantasy reveals the use of symmetric primitives for encoding/decoding:

```
char *__cdecl string_decrypt(char *str, int len)
{
  unsigned int str_size; // edi@1
  char v3; // dl@1
  signed int counter; // ecx@1
  char *result; // eax@3

  str_size = *(len + 1);
  v3 = *(len + 3);
  counter = 1;
  if ( str_size < 1u )
  {
    result = str;
  }
  else
  {
    do
    {
      str[counter - 1] = v3 ^ counter ^ *(len + counter + 3) ^ 0x47;
      v3 += *(len + counter++ + 3);
    }
    while ( counter <= str_size );
    result = str;
  }
  return result;
}
```

Equation Group malware string decryption.

```
char *__usercall string_decrypt@<eax>(char *str@<eax>, int Length@<edx>)
{
  char *v2; // esi@1
  char *key; // edi@2

  v2 = str;
  if ( Length )
  {
    key = (11 - str);
    do
    {
      str = (IV + &v2[key] * &v2[key + 12]);
      *v2 -= str ^ ((IV + (key + v2) * (key + v2 + 12)) >> 8) ^ ((IV + &v2[key] * &v2[key + 12]) >> 16) ^ ((IV + &v2[key] * &v2[key + 12]) >> 24);
      ++v2;
      --Length;
    }
    while ( Length );
  }
  return str;
}
```

Flame string decryption.

```
BYTE *__cdecl string_decrypt(int a1, _BYTE *a2, int a3, char a4)

{
  _BYTE *result; // eax@2
  int v5; // edi@3
  char v6; // dl@3
  _BYTE *v7; // ecx@4

  if ( a1 )
  {
    v5 = a3;
    v6 = a4 - 57;
    if ( a3 > 0 )
    {
      v7 = a2;
      while ( 1 )
      {
        *v7 = ((v6 - 33 * v7[a1 - a2]) << 6) | ((v6 - 33 * v7[a1 - a2]) >> 6) | (v6 - 33 * v7[a1 - a2]) & 0x3C
        ++v7;
        if ( !--v5 )
          break;
        v6 += a4;
      }
    }
    result = a2;
  }
  else
  {
    result = 0;
  }
  return result;
```

TripleFantasy string decryption.

The similarities shown in these screen captures strengthen the possibility of a relationship to other contemporary, state-sponsored attacks.

Learn how Intel Security can help protect against this threat.

Protecting against firmware and BIOS manipulation

As noted earlier, a HDD or SSD whose firmware has been reprogrammed by an Equation Group module can reload associated malware each time the infected system boots, and the malware persists even if the hard drive is reformatted or the operating system is reinstalled. Further, the reprogrammed firmware and associated malware is undetectable by security software once it is installed.

Intel Security and others in the threat research community believe this firmware reprogramming module is very rare and that it is deployed only in very high-value, targeted attacks. Consequently, most enterprises are unlikely to suffer from this threat.

Nonetheless, protecting against firmware and BIOS manipulation attacks should be part of every enterprise's security approach. The focus should be concentrated in two areas:

- Establish ways to detect the initial delivery of the Equation Group's malware. The known attack vectors are phishing, CDs, and USB drives; so special attention should be placed in those areas.
- Secure systems from data exfiltration. Although the firmware reprogramming module cannot be detected today, the overall attack objective is very likely to be reconnaissance. Because reconnaissance depends on systematic communication and data exfiltration with a control server, stopping that step is critically important.

Recommended Policies and Procedures	
General	▪ Defense-in-depth: integrated, layered security ▪ Endpoint security software on all endpoints ▪ Enable automatic OS updates, or download OS updates regularly, to keep operating systems patched against known vulnerabilities ▪ Install patches from other software manufacturers as soon as they are distributed ▪ Encrypt important data and hard drives
Phishing	▪ Eliminate mass phishing campaigns with secure gateway email filtering ▪ Implement sender-identity verification to reduce risk of cybercriminals being mistaken for trusted parties ▪ Detect and eliminate malicious attachments with advanced antimalware ▪ Scan URLs in email when received, and again when clicked ▪ Scan web traffic for malware when phishing leads the user on a multiclick journey to infection ▪ Educate users on best practices in detecting and acting upon suspicious emails
Exfiltration	▪ Implement data-loss prevention to stop exfiltration in the event of a breach

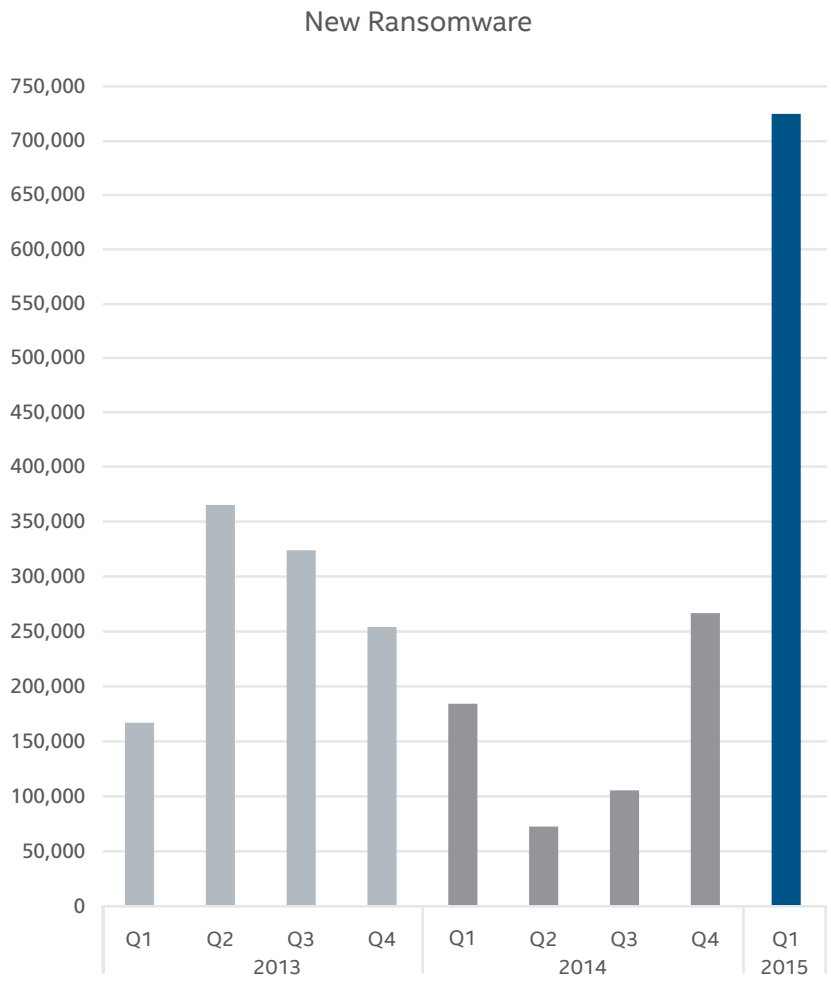
Ransomware returns: new families emerge with a vengeance

—*Christiaan Beek*

In the ***McAfee Labs Threats Report: November 2014*** we predicted nine major threats that would occur in 2015. Regarding ransomware, we said this: "Ransomware will evolve its methods of propagation, encryption, and the targets it seeks."

Almost immediately, we began to see a huge rise in ransomware, especially with the family CTB-Locker, followed by new versions of CryptoWall, TorrentLocker, and spikes of BandarChor. We also saw the new family **Teslacrypt** surface in the first quarter.

McAfee Labs has seen a 165% rise in ransomware in Q1, especially with the family CTB-Locker, along with new versions of CryptoWall, TorrentLocker, and spikes of BandarChor. We also saw the new family Teslacrypt surface in the first quarter.



Source: McAfee Labs, 2015.

These ransomware campaigns mainly target victims in relatively rich countries, because users in those countries are the most willing to pay the ransoms, according to statements made on underground forums that host discussions on the effectiveness of ransomware campaigns.

The phishing email topics that lead to infestation by ransomware are very specific. The email template and attachment names appear not only in the local language but also pretend to be coming from real companies in the targeted countries. As an example, in March we saw a ransomware campaign in Turkey that sent fake emails that appeared to come from postal and telephone companies and asked people to change or verify their addresses, fill in a form for redelivery of goods, or check their bills:

Ptt posta hizmetleri

EA273182901BE takip numaralı kargonuz **09 Mart 2015** adresinize teslim edilememiştir. Lütfen adres bilgilerinizi güncelleyerek kargonuzu teslim alınız.

Teslimat adresi değiştirmek için PTT Adres Degişikliği Formu indirip dikkatlice ve eksiksiz olarak doldurmanız gerekmektedir.

Adres Değişikliği Formu İndir

Dikkat

Kargonuz 15 iş günü içinde almanız gerekmektedır. Fazladan her gün için PTT sizden 25TL/günlük tazminat talep etme hakkına sahip olacaktır.

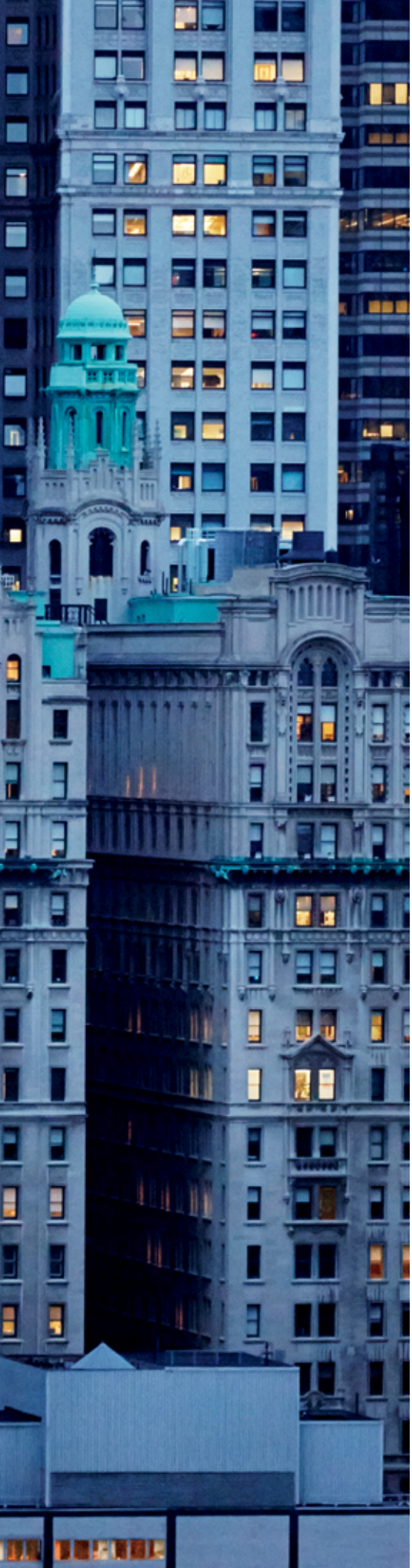
Gizlilik Politikası

PTT olarak ilgili kuralların tarafımızca tümü ile eksiksiz bir şekilde yerine getirileceğini teyit etmekteyiz. Böylelikle, aşağıda belirtilen kişisel bilgi toplama ilkelerine bağlı olarak, tüm gayretimizi tarafımızca toplanmış olan her türlü bilgiyi ekibimizce alınan sıkı güvenlik ve gizlilik önlemleri ile saklama hususunda özen göstermekteyiz. Kişisel bilgi toplama ve kullanımını en aza indirgeyerek, toplanan kişisel bilgileri sadece işlemlerin gerçekleşebilmesi için gerekli olan süre kadar tutmakta, öte yandan size en kaliteli hizmeti ve birbirinden güzel fırsatları sunmaktayız. Web sitemiz, gizlilik konusunda yeterince duyarlı olduğunu gösterebilen ve standartlarımıza uygun olan sitelere bağlantılar içermektedir. Ancak ilgili sitelerin içeriği ya da gizlilik uygulamalarından PTT sorumlu tutulamaz.

Bu e-posta [redacted] için gönderilmistir. Eğer artık ilgilenmiyorsanız haber grubu üyeliğinizi iptal edebilirsiniz

PTT Posta Hizmetleri
Posta ve Telgraf Teşilatı A.Ş. 2015

This purported legitimate email contained a link that redirected victims to a website hosting ransomware.



Ransomware history

In May 1996, Adam Young of Columbia University presented the paper ***Cryptovirology—extortion-based security threats and countermeasures*** at the IEEE's Security and Privacy symposium. He described the development of the first ransomware prototypes, which used the process of asymmetric encryption.

Asymmetric encryption is cryptography in which a pair of keys is used to encrypt and decrypt a file. Applied to ransomware, the public-private pair of keys is uniquely generated by the attacker for the victim. The private key to decrypt the files is stored on the attacker's server and is available to the victim only after the payment of the ransom. Adding insult to injury, some attackers fail to provide the private keys even after ransoms have been paid, leaving victims without their money or their files. With an asymmetric key, the ransomware author has a (private) key in his or her possession that is not accessible to malware analysts. Without access to the private key, it is nearly impossible to decrypt the files that are held ransom.

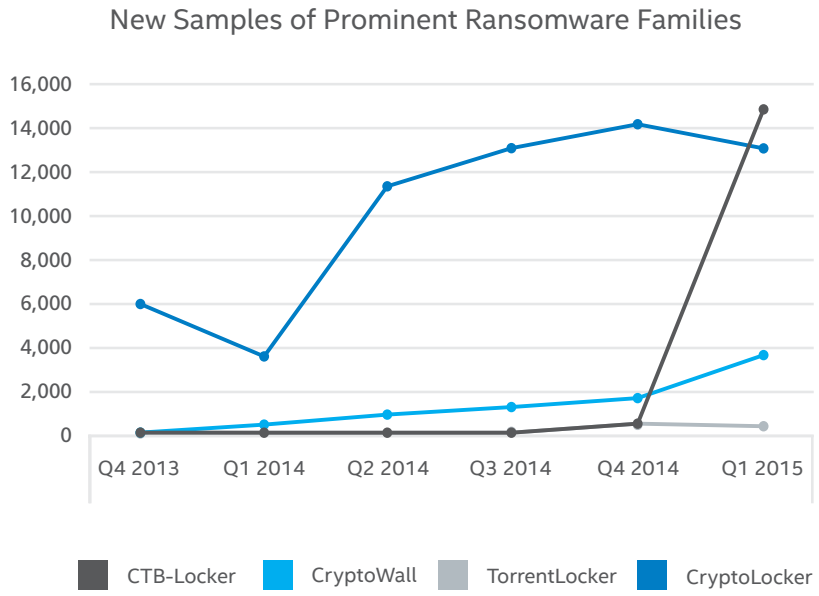
Since that seminal paper in 1996, researchers have described many scenarios in talks and papers. One of the first known ransomware families in the wild—Gpcode.ak—appeared in 2008. The malware encrypted a huge list of files on a victim's computer. The most famous ransomware family—CryptoLocker—appeared in September 2013. The then-current form of CryptoLocker was stopped in May 2014 by the takedown of one of its major distribution vehicles, the GameOver Zeus network. Currently the top ransomware families are CryptoWall (Versions 2 and 3), TorrentLocker Version 2, and CTB-Locker. (McAfee Labs dissected CryptoLocker, GameOver Zeus, and its takedown in the ***McAfee Labs Threats Report: August 2014.)***

New technologies have been adapted over the years to make ransomware more powerful:

- Virtual currency: By using **virtual currency** as the method to pay ransoms, attackers are not exposed to traditional banking and the possibility that money transfers can be traced.
- Tor network: By using the **Tor network,** attackers can more easily hide the location of their control servers, which store the victims' private keys. Tor makes it possible to maintain the criminal infrastructure for a long time and to even rent the infrastructure to other attackers so they can run affiliate campaigns.
- Moving to mobile: In June 2014, researchers discovered the first ransomware family to encrypt data on Android devices. Pletor uses AES encryption, encrypts the data on the phone's memory card, and uses Tor, SMS, or HTTP to connect to the attackers.
- Targeting mass-storage devices: In August 2014 Synolocker began targeting network attached storage (NAS) disk and rack stations from Synology. The malware exploits a vulnerability in unpatched versions of the NAS servers to remotely encrypt all data on the servers using both RSA 2,048-bit keys or 256-bit keys.

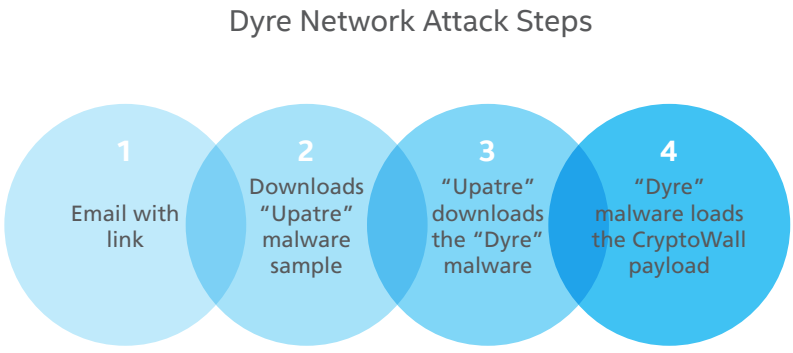
Statistics

In the following chart, we can see the proliferation of unique new samples for several prominent ransomware families:



Source: McAfee Labs, 2015.

CTB-Locker began to appear December 2014. As we write this report, it is still very active. Although the number of CryptoWall Version 1 and 2 samples has been relatively steady, Version 3 began its spread through the Dyre network in September 2014.



The Dyre network follows these steps to infect systems.

Curve-Tor-Bitcoin-Locker, also known as CTB-Locker

CTB-Locker was very active this quarter. Here's what the name means:

- Curve comes from the malware's use of **persistent cryptography based on elliptical curves,** which encrypts the files with a unique RSA key.
- Tor comes from the attackers' placement of their control servers on the Tor network, making them hard to trace and take down.
- Bitcoin refers to a virtual currency payment method that avoids most payment traces that can lead to the attackers.
- Locker refers to keeping the files locked or encrypted until the ransom is paid and the files are released.

CTB-Locker is successful because it uses clever, evasive techniques to get around security software, its phishing emails are more "believable" than others, and an affiliate program has allowed CTB-Locker to very quickly flood the market.

Why is CTB-Locker so successful? First, it uses clever, evasive techniques to get around security software. Second, the phishing emails used in CTB-Locker campaigns are more "believable" than in other ransomware campaigns. For example, the malware uses local businesses and location-relevant filenames. Finally, the presence of an affiliate program has allowed CTB-Locker to very quickly flood the market with phishing campaigns before systems have been updated with security software that can detect and contain the attacks.

CTB-Locker is distributed in many ways, including Internet Relay Chat, peer-to-peer networks, newsgroup postings, email spam, and more. We saw an interesting new approach this quarter: the use of the well-known downloader Dalexis. To circumvent antispam tools, the downloader is hidden in a .zip file that contains a .zip and eventually unpacks to a .scr (screensaver) file.

Once CTB-Locker has been executed, it displays this ominous image:

Many CTB-Locker victims first see this image.

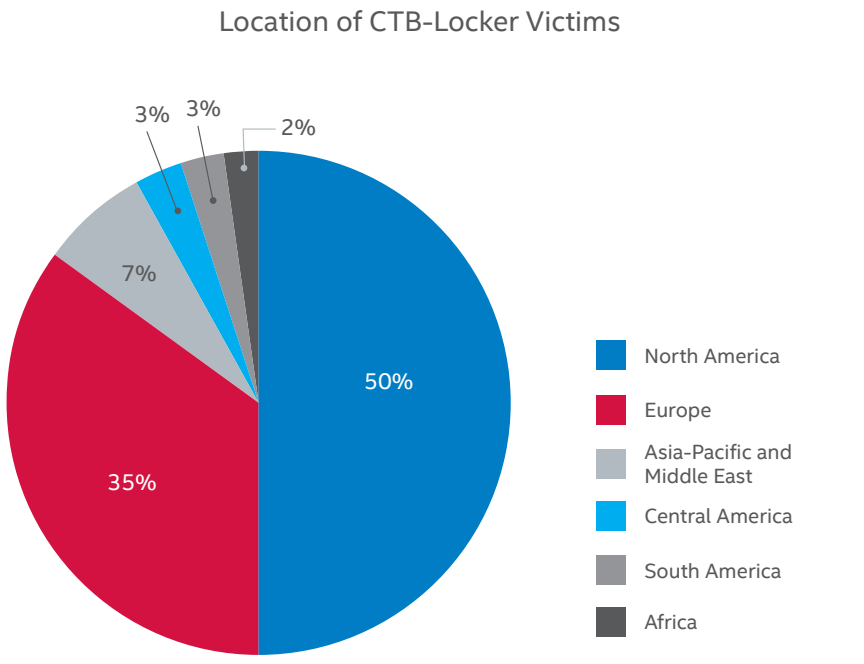
In one of the next screens, CTB-Locker offers the free decryption of five files. Unfortunately it does not connect to its control server to get the private keys to decrypt these files. If it did, malware researchers would be able to grab those private keys and attempt to learn their patterns. Instead, CTB-Locker stores five private keys in a randomly named file with an average size of 600 bytes on the disk of the victim's computer. This technique eliminates the need to connect with the server hosting the victim's private key.

CTB-Locker campaigns escalate

Campaigns using CTB-Locker started early in December 2014, but mass campaigns took off in January 2015. CTB-Locker has been found in English, Dutch, German, French, and Italian. Language options extend to the attachments, making the phishing emails more authentic. Even the filenames have been localized:

- a_la_clinique_vtrinaire_lavalle.scr
- aliments_universelles_lolivier.scr
- alte_poststr_25_72250_freudenstadt.scr
- an_der_wassermhle_3_28816_stuhr.scr
- andros_consultants_limited.scr
- b_n_r_roofing_2000_ltd.scr
- b_van_brouwershaven_and_zn_bv.scr
- bill39C6113.scr
- fairview_rehab_and_sports_injury_clinic.scr
- fashioncrest_ltd.scr
- feedback_instruments_ltd914.scr

In spite of the malware's multilingualism, most CTB-Locker victims detected by McAfee Labs are located in North America:



Source: McAfee Labs, 2015.

CTB-Locker affiliate programs

In August 2014, the author(s) of CTB-Locker announced the product on several Russian forums. An affiliate program is part of the business strategy.

The author has offered the use of the CTB-Locker infrastructure, which includes affiliates using their botnets to send spam to potential victims. For every successful infection in which the victim pays the ransom, the affiliate gets a percentage of the money.

On one underground forum, an affiliate explained his thinking. He stepped into the world of ransomware simply because it's an easy way to earn money with a low risk of being arrested. "The nature of the CTB-Locker infrastructure being hosted by someone else, the usage of Tor, and Bitcoin payments only, makes it a pretty safe program to be part of." The affiliate claims to make US$15,000–$18,000 per month with a net profit around $8,000–$10,000. His profit depends on the number of victims who pay, but it also depends on the cost of an exploit kit, custom cryptors, and traffic reroutes. The most profitable countries are the United States, United Kingdom, Australia, and several other European countries. According to this affiliate, around 7 percent of all victims pay the ransom.

CryptoWall Version 3 functionality

From the original CryptoWall to the latest release, Version 3, many functions have changed. The malware now exclusively uses Tor for payment, and it communicates in different ways: via hardcoded and obfuscated control server URLs or a peer-to-peer network based on the I2P protocol. Many other ransomware families have used the name CryptoLocker to mislead victims and the security industry. CryptoWall did so as well, but after a time began to use its own name.

Like CTB-Locker, the latest CryptoWall campaigns are also trying to bypass security mechanisms by using an obfuscated JavaScript attachment in an email, although CryptoWall downloads .jpeg files instead of .zip files. However, there are no actual pictures to fool victims, just ransomware executables.

A new ransomware family: Teslacrypt

Teslacrypt emerged in Q1, adding saved-game content as a target.

In February 2015, the new family Teslacrypt appeared. Although it is based on CryptoLocker code and has all the typical functions, including using Tor to hide and Bitcoin for payment, Teslacrypt also adds some new functionality. One Teslacrypt family member targets saved-game content and extra downloadable content files. More than fifty files related to games are encrypted, including these:

Some of the games targeted by Teslacrypt.

Teslacrypt also adds the option to pay with PayPal My CashCards. For a more detailed analysis of Teslacrypt, read **this recent McAfee Labs blog.**

Data recovery

The most frequently asked question about ransomware is "Can we recover the encrypted data?" The answer is generally "No"—unless you pay the ransom and the thieves provide the private key. Ransomware private keys are stored on the criminals' servers and unless you have access to that server or a copy of it, there is no other way to obtain the private key.

Occasionally, a law enforcement agency executing a takedown is able to seize the ransomware campaign's control server. If they can gain access to the database containing the private decryption keys, an encrypted-file recovery tool can be built. Recently, the Dutch National High Tech Crime Centre seized the control server of the CoinVault ransomware family. Working together with Kaspersky, they created **a recovery tool.**

In the case of CTB-Locker, there are some instances in which files can be recovered. If the Windows System Restore option has been turned on (the default for most systems), then files can be recovered from the shadow volume copies. The shadow volume copy service, also known as VSS, is a technology that performs manual or automatic file backups, even when files are in use. From Windows XP through Windows 7 and Windows Server 2008, it is implemented in the Volume Shadow Copy service. Beginning with Windows 8, it is no longer possible to browse, search, or recover older versions of files via the Previous Versions tab of the Properties dialog.

For Windows 8, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, the built-in command "Vssadmin list shadows" will list the available copies for the given volume. There are various ways of mounting a VSS copy through the command line and browsing for the files. There are a variety of open-source tools that can be used to browse volume shadow copies. It may be possible to restore ransomware-encrypted files using one of these tools.

Does this method work for all ransomware families? Unfortunately not. With CryptoWall Version 3, Crypto-Fortress, and Teslacrypt, the ransomware authors added the following command while the malware executes:

- vssadmin delete shadows /all /quiet

This means that all volume shadow copies are silently deleted. Still, with recovery software and the knowledge of the offset-values used, it might be possible to recover those deleted volumes.

What can we expect in the future?

New variants and new families will appear, along with new techniques and functionality. Early this year, for example, Swiss researchers discovered a new technique using ransom and encryption that they dubbed Ransomweb. The attackers infect web server scripts and database fields. They wait until these values are stored for a few weeks or months in backups and then remove the key from the server or remote location. The web application and database begin to malfunction, but the backups are also infected. Then the attackers send the demand for ransom.

Safe practices to protect against ransomware

By tightly monitoring intelligence feeds, McAfee Labs stays ahead of most ransomware campaigns. Staying ahead allows us to detect and stop most ransomware before it can execute. It also means that no Bitcoins will flow into criminals' pockets.

Good policies and procedures include the following:

- Back up data. Although this seems obvious, far too often there is no backup available or the backup process was never tested and didn't work. Removable storage is widely available, inexpensive, and simple to use. Home users should create a backup, disconnect the device, and store it in a safe place. For cloud-based backup services, be aware of the chance that the victim's endpoint could have copied encrypted files to the cloud, too. Some cloud-based backup services offer to restore the most recent versions of files.
- Perform ongoing user-awareness education. Because most ransomware attacks begin with phishing emails, user awareness is critically important and necessary. For every ten emails sent by attackers, statistics have shown that at least one will be successful. Don't open emails or attachments from unverified or unknown senders.

Learn how Intel Security can help protect against this threat.

- Block unwanted or unneeded programs and traffic. If there is no need for Tor, block the application and its traffic on your network. Blocking Tor will often block the ransomware from getting the public RSA key from the control server, thereby blocking the ransomware encryption process.
- Keep system patches up to date. Many vulnerabilities commonly abused by ransomware can be patched. Keep up to date with patches to operating systems, Java, Adobe Reader, Flash, and applications. Have a patching procedure in place and verify if the patches were applied successfully.
- Employ antispam. Most ransomware campaigns start with a phishing email that contains a link or a certain type of attachment. In phishing campaigns that pack the ransomware in a .scr file or some other uncommon file format, it is easy to set up a spam rule to block these attachments. If .zip files are allowed to pass, scan at least two levels into the .zip file for possible malicious content.
- Protect endpoints. Use endpoint protection and its advanced features. In many cases, the client is installed with just default features enabled. By implementing some advanced features—for example, "block executable from being run from Temp folder"—more malware can be detected and blocked.

Adobe Flash: a favorite of designers and cybercriminals

—Arun Pradeep and Santosh Surgihalli

One definition of the popular Adobe Flash calls it "a multimedia and software platform used for creating vector graphics, animation, games and rich Internet applications ... that can be viewed, played, and executed in Adobe Flash Player."[3]

Another equally accurate definition could describe Adobe Flash as "a multimedia and software platform very successfully used by cybercriminals to attack victims by exploiting the growing number of devices running old versions of Flash."

In this Key Topic, we examine Adobe Flash (formerly called Macromedia Flash and Shockwave Flash): how it works, the growing number of vulnerabilities and exploits, how cybercriminals are exploiting them, and what organizations can do to protect against Flash exploits.

The Adobe Flash platform

At its core, the Adobe Flash platform comprises three things:

- The open-source, platform-independent, object-oriented programming language ActionScript, which can be used to describe multimedia actions including animation, interactive event handling (primarily for game developers), video streaming, and audio streaming.
- The authoring tool Adobe Flash Professional, used to create multimedia applications in the ActionScript language. Source code files carry the .fla extension. Compiled multimedia applications, also known as Flash movie files, carry the .swf extension.
- The runtime engine Adobe Flash Player, which plays .swf files. Different versions run standalone or inside web browsers as plug-ins on a variety of endpoints—including desktops, laptops, tablets, and smartphones.

Third-party tools help author, run, or manage .swf files.

The use of vector graphics combined with program code allows Flash movie files to be smaller—and thus allows streams to use less bandwidth—than the corresponding bitmaps or video clips. As a result, Flash Player has become one of the most widely installed applications for viewing multimedia content.

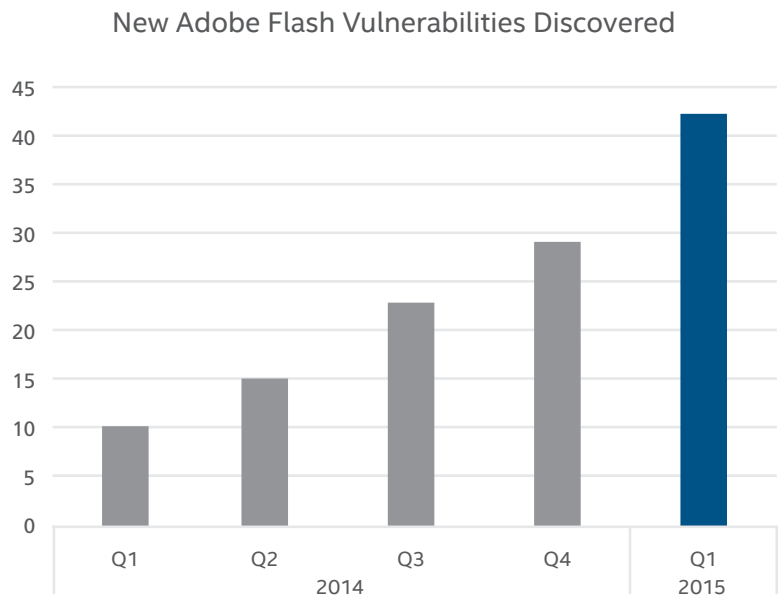
Of course, its popularity is what has attracted malware authors.

Exploits in Flash

Software vulnerabilities are usually submitted to and tracked in the National Vulnerability Database, a repository maintained by the National Institute of Standards and Technology. A recognized vulnerability is tracked by its **Common Vulnerabilities and Exposures (CVE)** number.

In the first quarter, 42 new Flash CVEs were added to the database, an increase of 50% from the 28 Flash vulnerabilities found in the fourth quarter of 2014. In fact, there has been a steady increase in the number of Flash vulnerabilities since the beginning of 2014. The most recent period has seen the highest number of vulnerabilities ever reported in a quarter.

In the first quarter, 42 new Flash vulnerabilities were found, an increase of 50% from the 28 Flash vulnerabilities found in the fourth quarter of 2014. It is the highest-ever number of Flash vulnerabilities reported in a quarter.



Source: National Vulnerability Database.

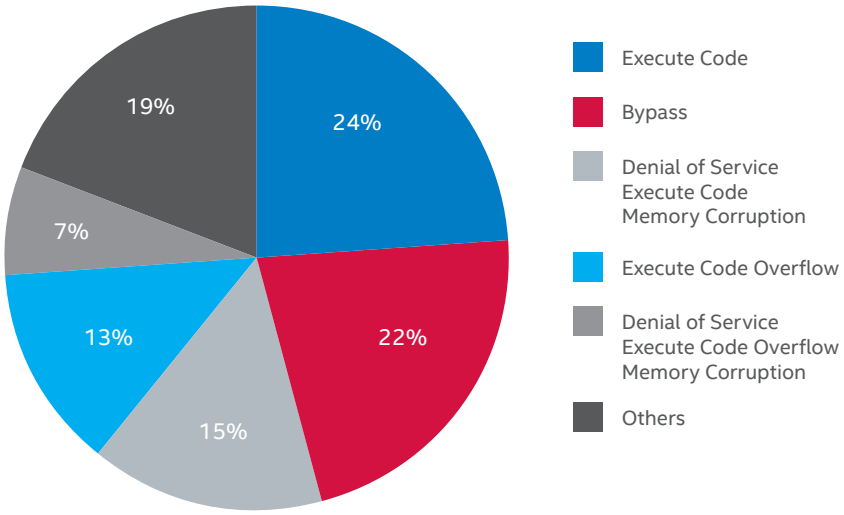
Some of the most recent Flash vulnerabilities are likely the result of Adobe's **vulnerability disclosure program** set up in late 2014 to coordinate the disclosure and patching of Adobe web application vulnerabilities. In fact, Adobe made initial fixes available to all 42 new Flash vulnerabilities discovered in Q1 on the same day that the CVEs were submitted.

Information about current fixes to Flash vulnerabilities can be found **here**. In addition, Adobe provides guidance about how quickly customers should update their Adobe products based on the severity of vulnerabilities. That guidance can be found **here**.

There are several types of Flash .swf vulnerabilities:

- Bypass: Flash Player does not properly restrict the discovery of memory addresses, which allows attackers to bypass the address space layout randomization protection mechanism on Windows.
- Denial of service executable code memory corruption: These vulnerabilities allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
- Denial of service: These vulnerabilities allow attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impacts via unknown vectors.
- Execute code overflow: Buffer overflow vulnerabilities allow attackers to execute arbitrary code via unspecified vectors.
- Execute code: Use-after-free vulnerabilities allow attackers to execute arbitrary code via unspecified vectors.

Targeted Adobe Flash Vulnerabilities

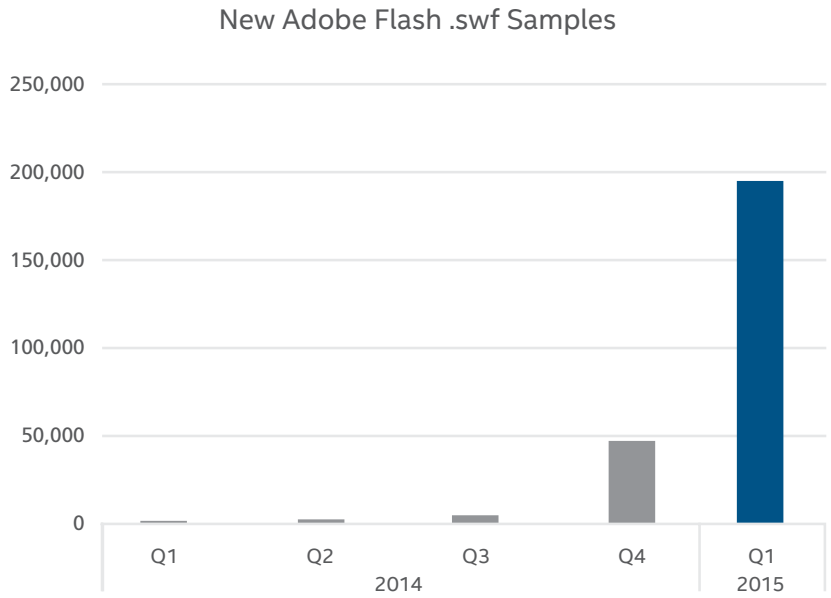


Source: McAfee Labs, 2015.

Prevalence of Flash exploits

Flash exploits began to increase dramatically beginning in the last quarter of 2014. Flash vulnerabilities are now among the main targets of exploit authors. McAfee Labs believes this is due to several factors: the steady increase in the number of Flash vulnerabilities; user delay in applying available software patches that eliminate Flash vulnerabilities; new, creative methods to exploit those vulnerabilities; a steep increase in the number of mobile devices that can play .swf files; and the difficulty of detecting Flash exploits.

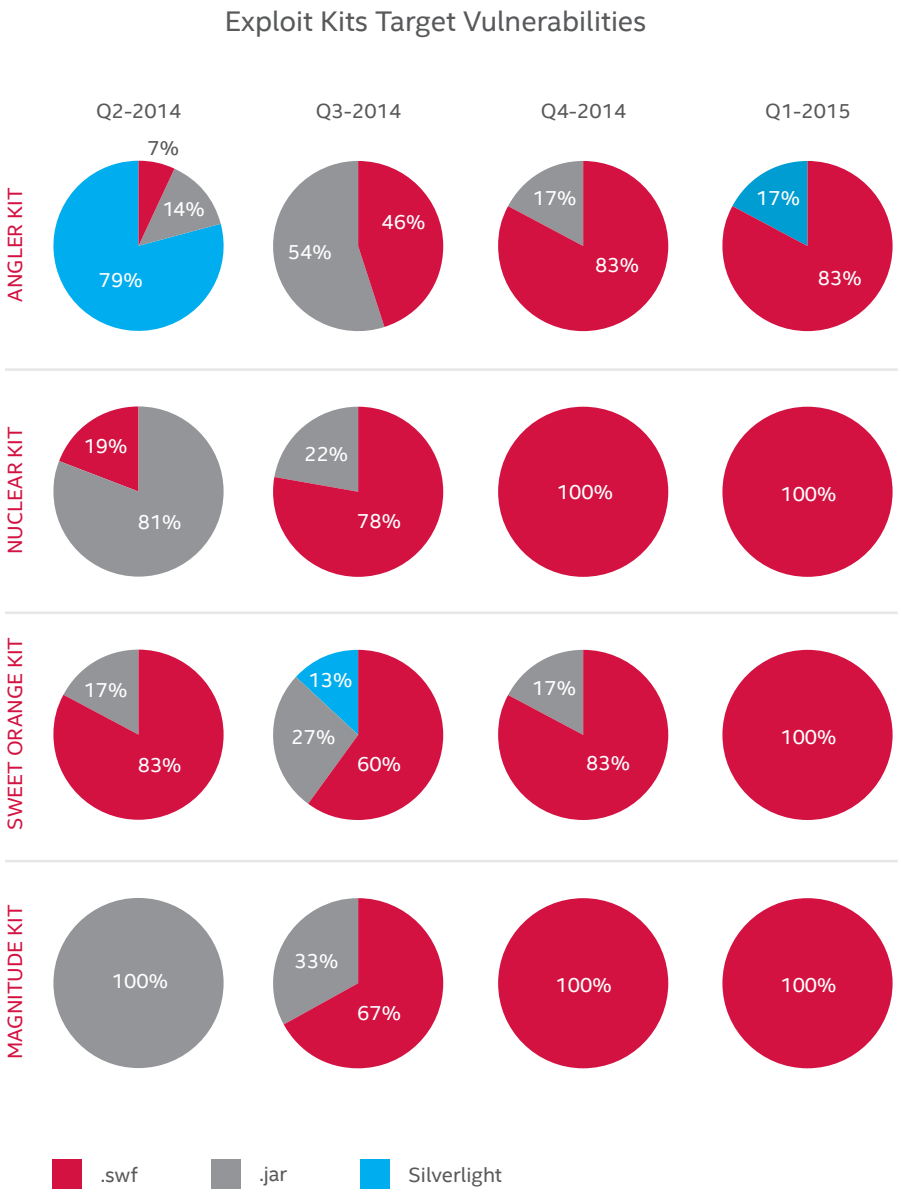
The number of new Adobe Flash .swf samples increased by 317% in Q1. These samples include clean, infected/malware, and unknown files.



Source: McAfee Labs, 2015.

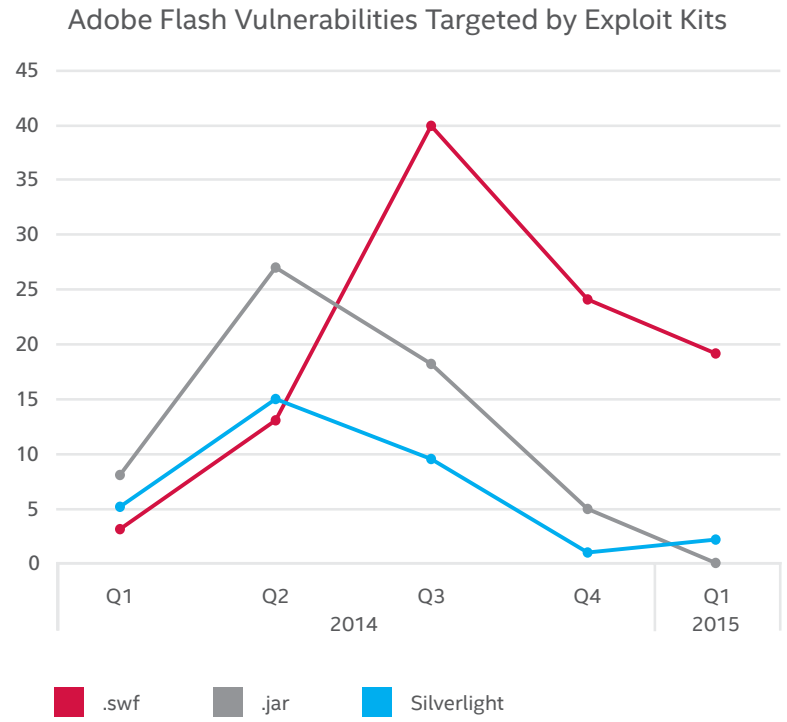
Among the exploit kits delivering Flash exploits, Angler has become the most popular. This powerful kit, discussed in depth in the ***McAfee Labs Threat Report: February 2015,*** is an off-the-shelf, easy-to-use toolkit that can deliver a wide variety of payloads through the exploitation of vulnerabilities. As shown in the following charts, Angler and other prominent exploit kits have shifted their focus from .jar (Java archive) and Microsoft Silverlight vulnerabilities to Flash vulnerabilities.

Exploit kits have shifted their focus from Java archive and Microsoft Silverlight vulnerabilities to Adobe Flash vulnerabilities.



Four leading exploit kits have shifted their focus almost exclusively to taking advantage of Flash vulnerabilities.

The following graph shows the trend of vulnerabilities targeted by various exploit kits:



Source: McAfee Labs, 2015.

Why do malware authors target Flash?

One reason malware authors attack Flash is the steady increase in the number of vulnerabilities coupled with user delay in the application of software patches for those vulnerabilities. More opportunities make it easier to exploit.

Another reason is the steep increase in the number of mobile devices. Most of these devices include player technology to execute .swf files, which adds considerably to the popularity of Flash as an attack vector.

Let's look at two more reasons for the popularity of this form of attack.

Newly discovered Flash vulnerabilities

In the following example, from CVE-2014-0497, a maliciously crafted .swf offers an easily readable ActionScript that contains functions and operations to execute the shellcode.

We can see that the malware author uses an algorithm to check the Flash Player version and assemble an ROP chain related to it. The malware then generates shell code to exploit the vulnerability.

```
if("win 11,7,700,202" !== _loc7_)
{
   if("win 11,7,700,224" !== _loc7_)
   {
      return null;
   }
   _loc5_ = _loc5_ - 10450228;
   _loc6_ = _loc5_ + 13082624;
   _loc4_.writeUnsignedInt(_loc5_ + 4646881);
   _loc4_.position = 64;
   _loc4_.writeUnsignedInt(_loc5_ + 52090);
   _loc4_.position = 76;
   _loc4_.writeUnsignedInt(_loc5_ + 4293);
   _loc4_.writeUnsignedInt(_loc5_ + 9376924);
   _loc4_.writeUnsignedInt(_loc5_ + 93510);
   _loc4_.writeUnsignedInt(_loc5_ + 1145378);
   _loc4_.writeUnsignedInt(_loc5_ + 1909483);
   _loc4_.writeUnsignedInt(param2);
   _loc4_.writeUnsignedInt(4096);
   _loc4_.writeUnsignedInt(64);
   _loc4_.writeUnsignedInt(param2 - 4);
```

Code to create return-oriented programming (ROP).

Next we see a code snippet from the famous Pixel Bender exploit from 2014:

```
public function sadad(param1:int) : *
{
   if(param1 == 1)
   {
      return "A501-0-000-00A-4-0B-003-17279-7-37-4616C6C6-9-7-A32A0-0-C6-E-6-16D-657-3706163-65-0-0317-2797374-6-16-C6C697A-3-22-0627-9-205065-747-2
   }
   if(param1 == 2)
   {
      return "EB4-89-090-9-09090-90-9-090909-090-90-90-90-9090-909-0-9-0909090-9-09-09090-90-909090-90909090-909-090-90909-0-9-09090909-0-909090-90-9
   }
}

function read_memory(param1:Vector.<int>, param2:uint, param3:uint) : uint
{
   if(param3 >= param2)
   {
      return param1[(param3 - param2) / 4];
   }
   return param1[1073741824 - (param2 - param3) / 4];
}
```

Hardcoded shellcode in the Pixel Bender exploit.

The decompiled ActionScript code has two raw shellcode commands (marked in red) that are hardcoded. After de-obfuscation, we can see the exploitation code.

New methods of Flash exploitation

Exploits from malicious advertisements on legitimate websites use an RC4 algorithm to obfuscate the malicious code. Recent exploits CVE-2015-0311, CVE-2015-0312, and CVE-2015-0313 use this technique to obfuscate the exploit and shell code.

```
private function InitEx() : void
{
   ggew = jtyk.xxfrh();
   var _loc1_:* = kryuje.wecy();
   var _loc2_:* = new RegExp("[3892754016]+","g");
   var _loc3_:* = "158l467o395a839d024B304y549t110e672s730".replace(_loc2_,"");
   _loc1_[_loc3_](ggew);
   stage.addChild(_loc1_);
}
```

Encrypting the function loadBytes.

In the preceding main function, variable _loc3_ contains the junk data 158l467o395a839d024B304y549t110e672s730. When we replace the numbers with null we get “loadBytes,” which loads a byte array (possibly containing file types .swf, .gif, .jpeg, or .png) into the Flash Player.

Variable _loc1_ will call another private function that returns a string new Loader(), as follows:

```
public function kryuje()
{
   super();
}

public static function wecy() : Loader
{
   var _loc1_:* = new Loader();
   return _loc1_;
}
```

Assigning the function new Loader to a variable.

The byte array or the binary data used for loading is in the variable ggew, which calls the function jytk. This public function contains the binary data that is decrypted and loaded using the loader. About 60KB of binary data needs to be decrypted, using the RC4 algorithm, as shown here:

```
public static function xxfrh() : *
{
    var _loc1_:* = wigr(ejtey.ybe);
    var _loc2_:* = kyte();
    var _loc3_:* = new ejtey.vree();
    var _loc4_:* = 0;
    var _loc5_:* = 0;
    var _loc6_:* = 0;
    var _loc7_:* = 0;
    var _loc8_:* = 0;
    var _loc9_:* = 0;
    var _loc10_:* = 0;
    _loc4_ = 0;
    while(_loc4_ < 256)
    {
        _loc3_[_loc4_] = _loc4_;
        _loc4_++;
    }
    _loc3_[ejtey.fhrw] = 0;
    _loc4_ = 0;
    while(_loc4_ < 256)
    {
        _loc8_ = (_loc2_[_loc7_] & 255) + (_loc3_[_loc4_] & 255) + _loc8_ & 255;
        _loc10_ = _loc3_[_loc4_];
        _loc3_[_loc4_] = _loc3_[_loc8_];
        _loc3_[_loc8_] = _loc10_;
        _loc7_ = (_loc7_ + 1) % _loc2_[ejtey.weruji];
        _loc4_++;
    }
    _loc3_[ejtey.fhrw] = 0;
    _loc4_ = 0;
    while(_loc4_ < _loc1_[ejtey.weruji])
    {
        _loc5_ = _loc5_ + 1 & 255;
        _loc6_ = (_loc3_[_loc5_] & 255) + _loc6_ & 255;
        _loc10_ = _loc3_[_loc5_];
        _loc3_[_loc5_] = _loc3_[_loc6_];
        _loc3_[_loc6_] = _loc10_;
        _loc9_ = (_loc3_[_loc5_] & 255) + (_loc3_[_loc6_] & 255) & 255;
        _loc1_[_loc4_] = _loc1_[_loc4_] ^ _loc3_[_loc9_];
        _loc4_++;
```

A close look at the RC4 algorithm.

After deobfuscating the code, we get:

> "Loader.LoadBytes(RC4_decode(RC4_encrypted_data))"

This command loads the decrypted data, which generates the ROP chain from Flash DLLs to dynamically load the shellcode and run the exploit.

Learn how Intel Security can help protect against this threat.

Unlike prior Flash attacks, in which the exploit code or shellcode was easily detected by antimalware products, these new attacks include multiple levels of obfuscation that effectively hide their behavior from even the most sophisticated security products. The creativity of this method clearly demonstrates the increased sophistication and complexity that these exploits have developed.

Protecting against exploits of Flash vulnerabilities

McAfee Labs recommends several ways to protect systems against Flash-based attacks:

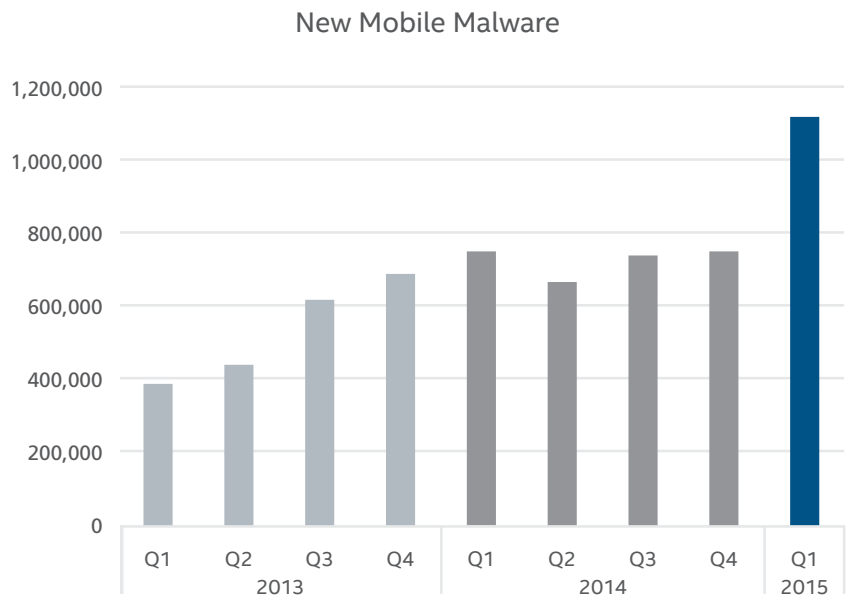
- Install Flash patches as soon as they are distributed. Patches are usually available on the same day that a Flash CVE is submitted. Information about current updates to Flash can be found **here**. A fully patched computer behind a firewall is a strong defense against cyberattacks.
- Enable automatic operating system updates, or download operating system updates regularly, to keep them patched against known vulnerabilities.
- Configure antivirus software to automatically scan all email and instant-message attachments. Make sure email programs do not automatically open attachments or automatically render graphics, and turn off the preview pane.
- Configure antivirus software to block attachments containing the .swf extension.
- Configure the browser security settings to medium level or above.
- Use a browser plug-in to block the execution of scripts and iframes.
- Do not install untrusted browser plug-ins.
- Use great caution when opening attachments, especially when those attachments carry the .swf extension.
- Never open unsolicited emails, or unexpected attachments—even from known people.
- Beware of spam-based phishing schemes. Don't click on links in emails or instant messages.
- Type the URLs or copy the URLs to the address bar of the browser and verify the address rather than clicking on web advertisements.
- Don't click on Flash movies on untrusted websites.

Threats Statistics

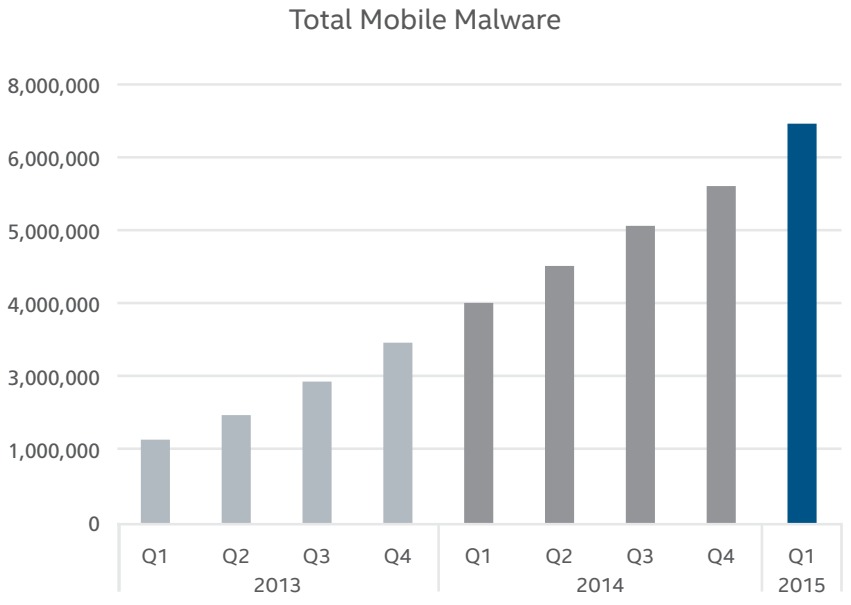
Share feedback

Mobile malware

The number of new mobile malware samples jumped by 49% from Q4 2014 to Q1 2015.



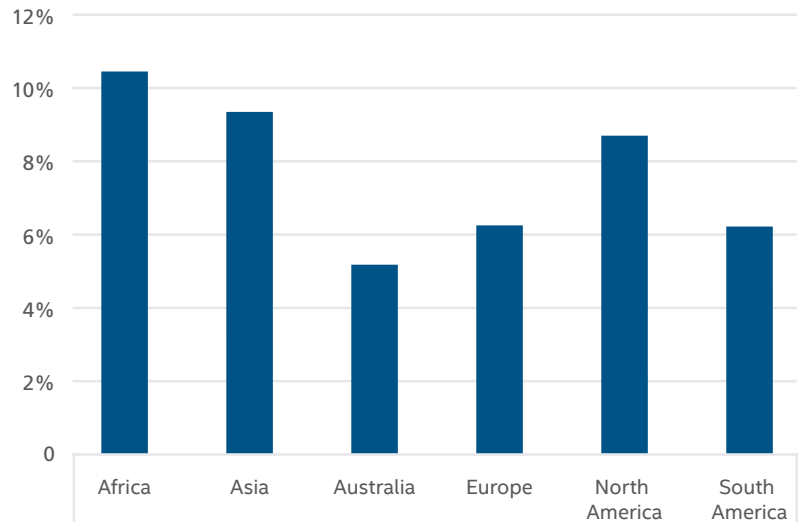
Source: McAfee Labs, 2015.



Source: McAfee Labs, 2015.

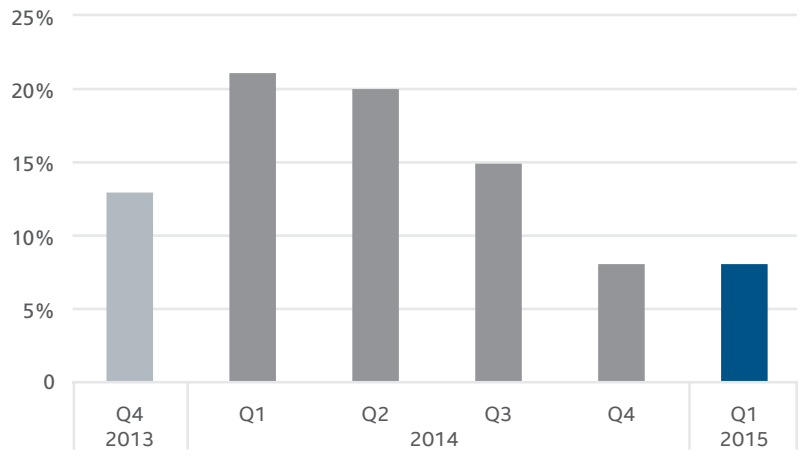
Share this Report

Regional Mobile Malware Infection Rates in Q1 2015



Source: McAfee Labs, 2015.

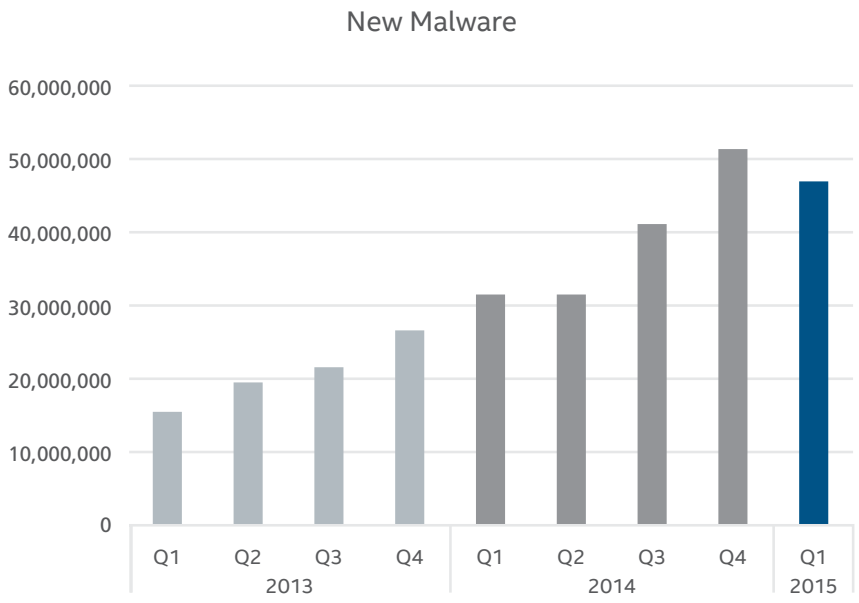
Global Mobile Malware Infection Rates



Source: McAfee Labs, 2015.

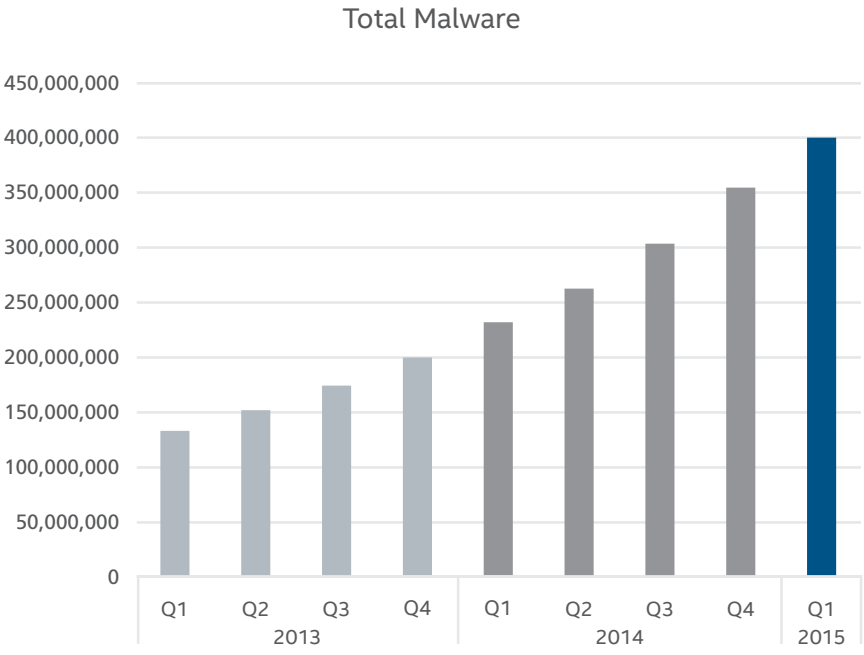
Malware

The decline in new malware this quarter is primarily due to one adware family, SoftPulse, which spiked in Q4 and returned to normal levels in Q1.



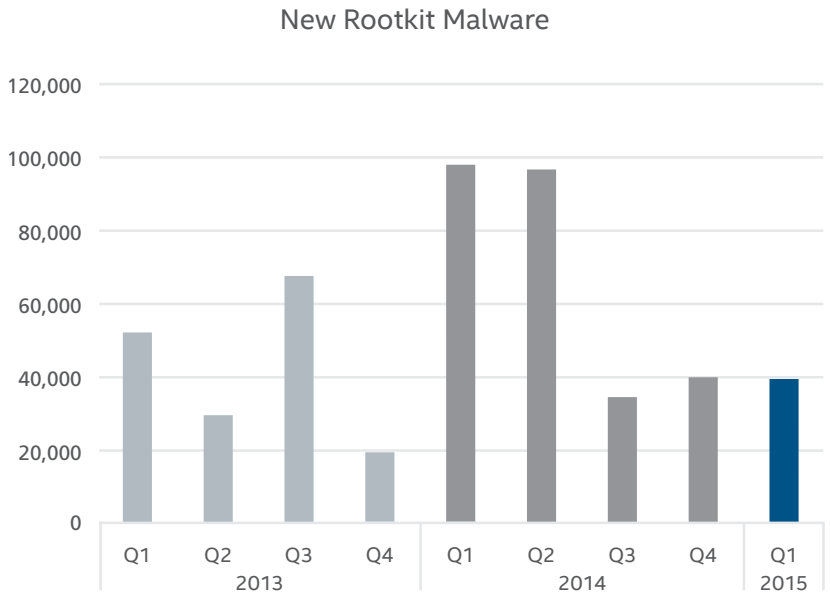
Source: McAfee Labs, 2015.

The McAfee Labs malware zoo grew 13% from Q4 2014 to Q1 2015. It now contains 400 million samples.

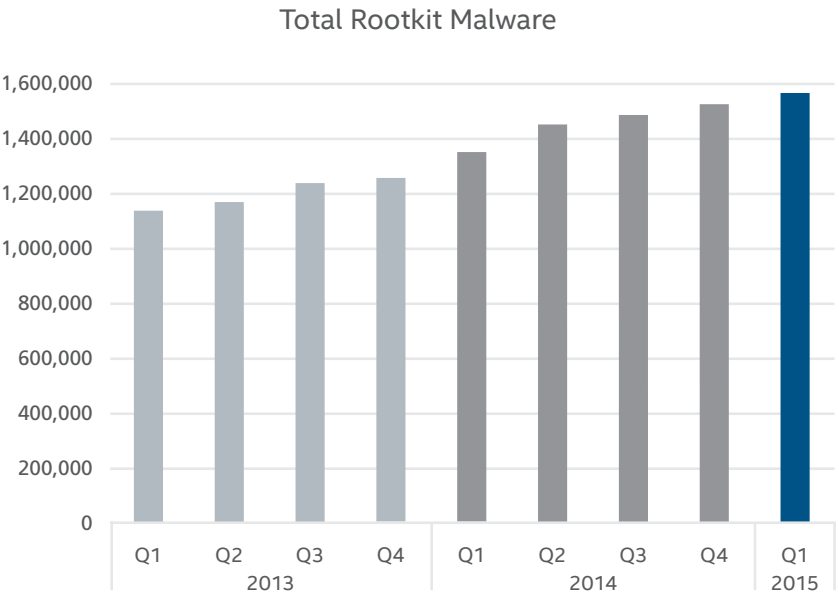


Source: McAfee Labs, 2015.

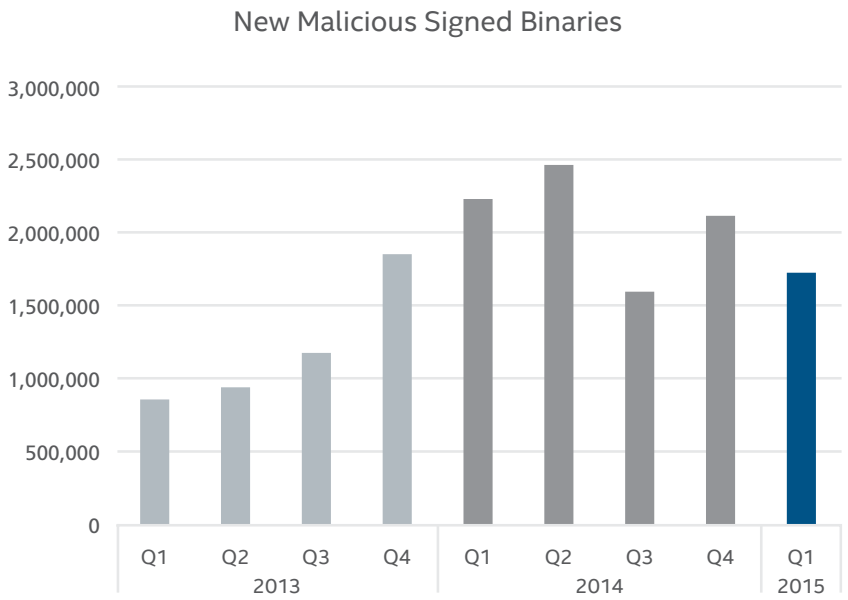
Share this Report



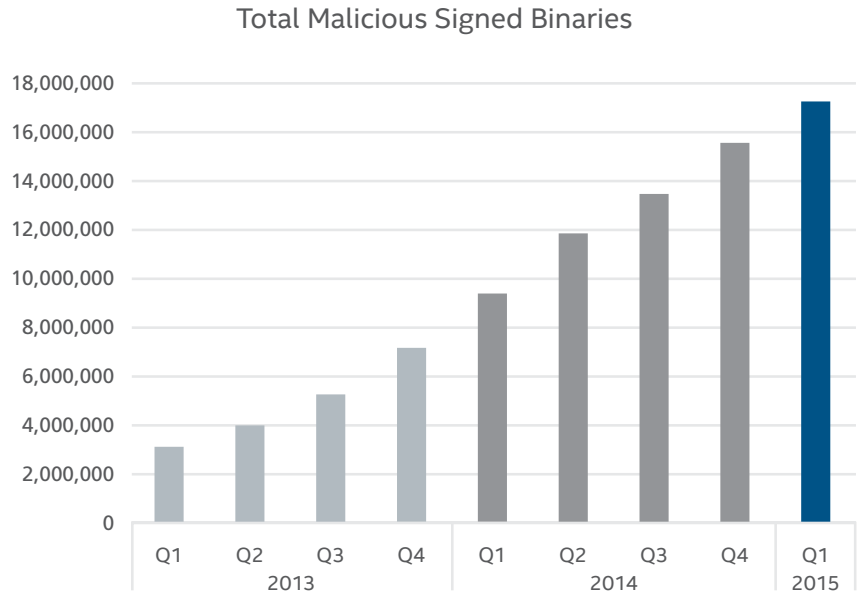
Source: McAfee Labs, 2015.



Source: McAfee Labs, 2015.



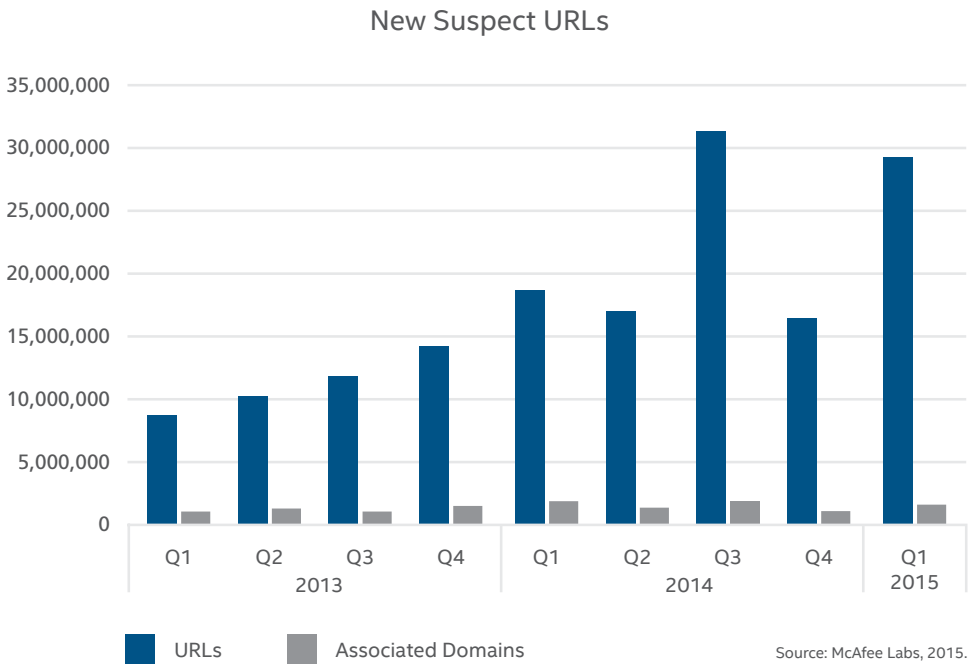
Source: McAfee Labs, 2015.



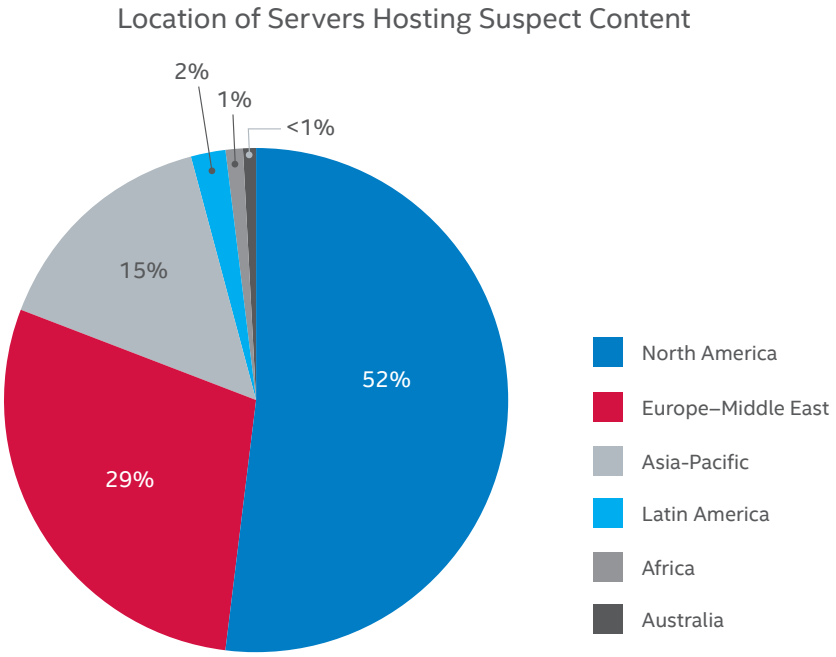
Source: McAfee Labs, 2015.

Web threats

In Q3 2014, we explained the high increase in new suspect URLs by an increase in malicious shortened URLs. In Q1 2015, we see the same increase, but it is not due to malicious shortened URLs. We do not yet know the cause.

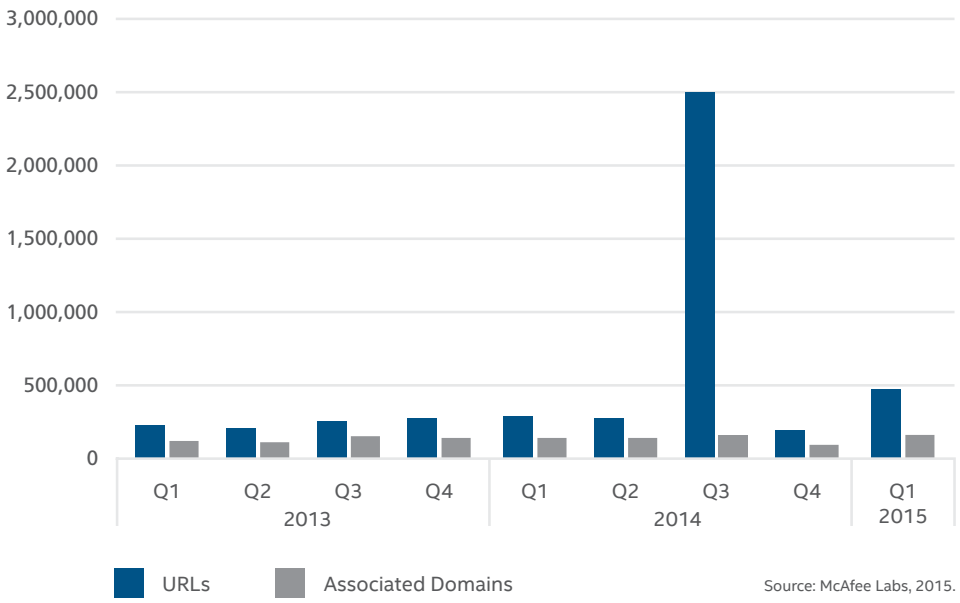


Source: McAfee Labs, 2015.



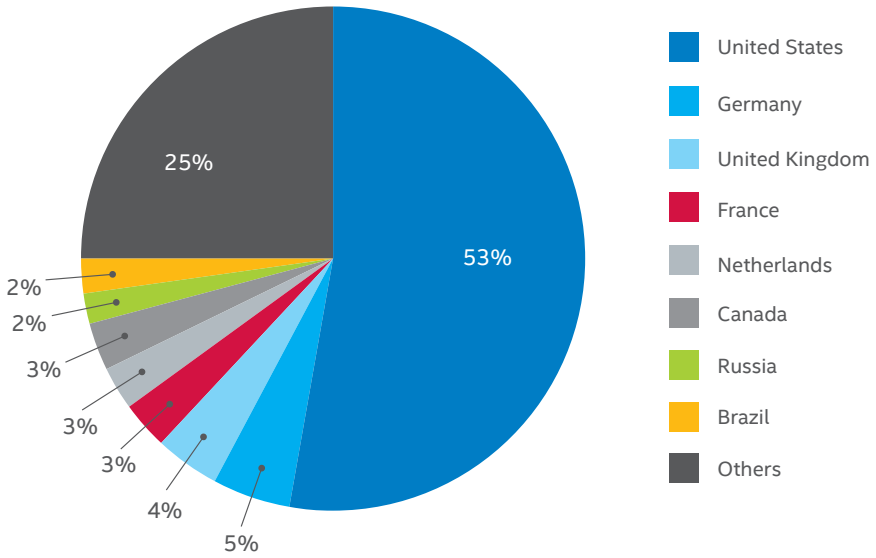
Source: McAfee Labs, 2015.

New Phishing URLs



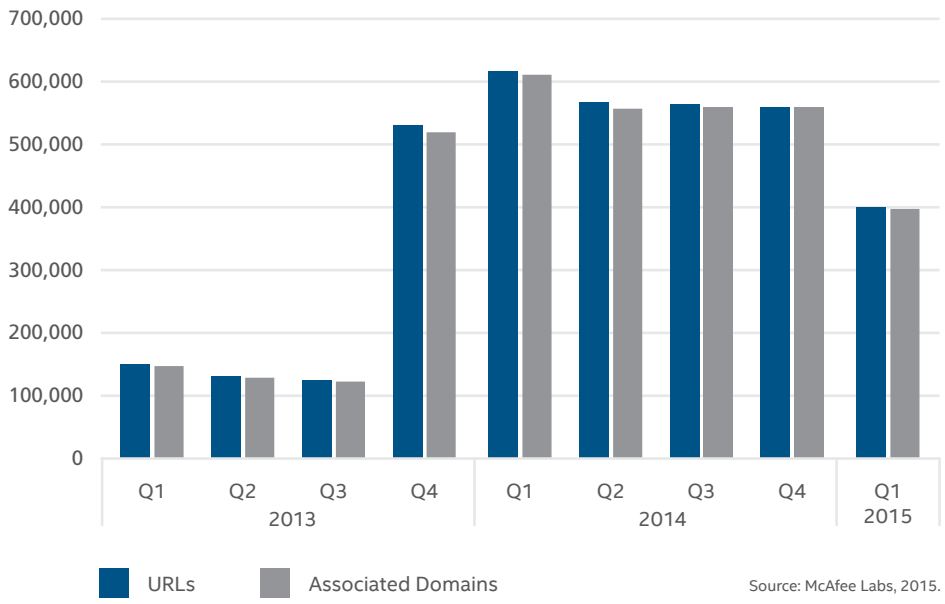
Source: McAfee Labs, 2015.

Top Countries Hosting Phishing Domains



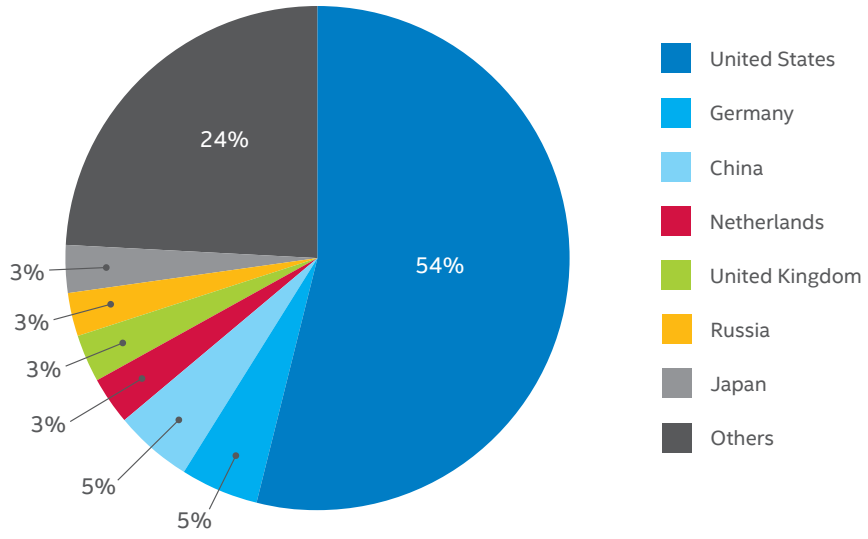
Source: McAfee Labs, 2015.

New Spam URLs



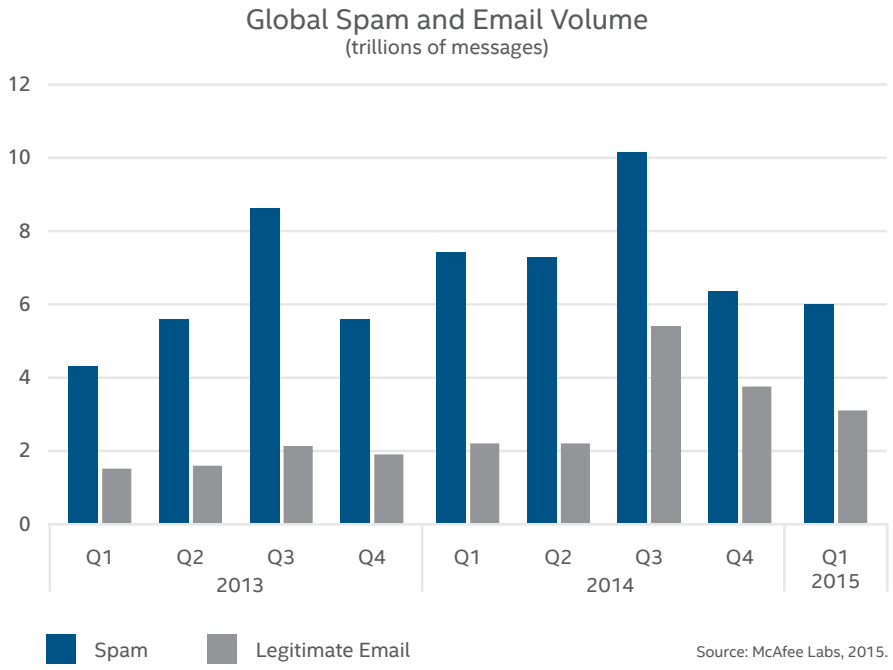
Source: McAfee Labs, 2015.

Top Countries Hosting Spam Domains

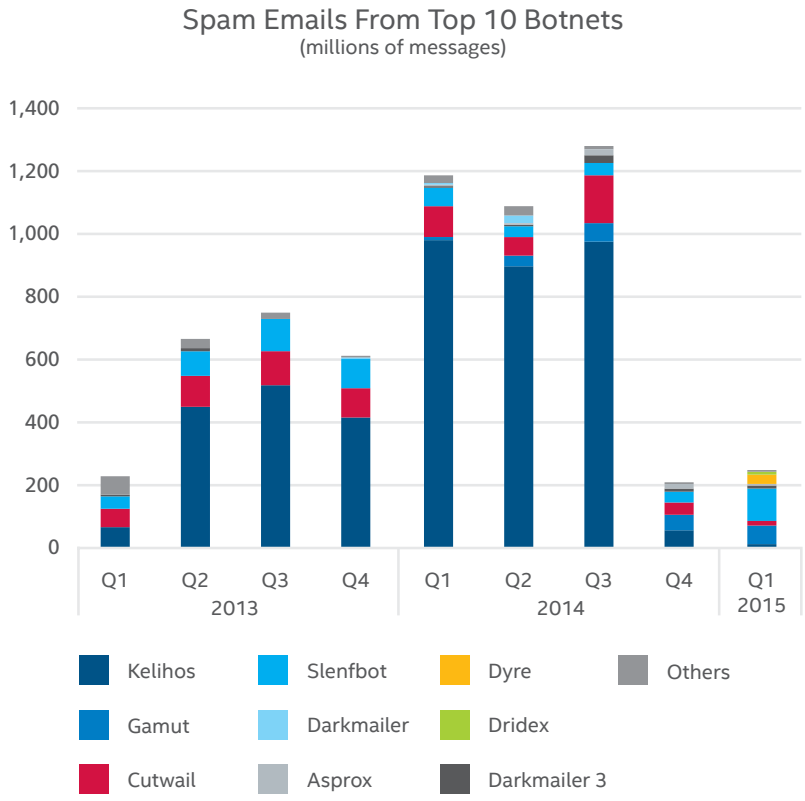


Source: McAfee Labs, 2015.

Messaging and network threats



Source: McAfee Labs, 2015.

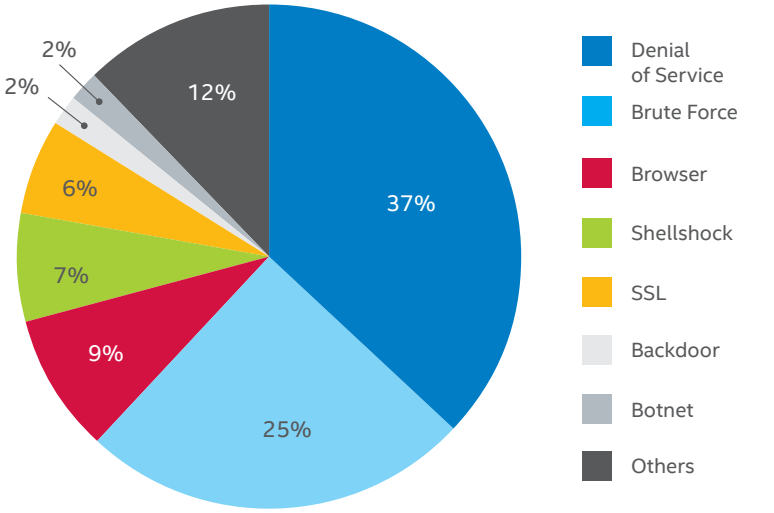


Source: McAfee Labs, 2015.

In Q1 snowshoe as well as the Festi and Darkmailer2 botnets were replaced in the top ranks by Dyre, Dridex, and Darkmailer3. Slenfbot, which has been a consistently pervasive spam sender, claimed the first position during Q1 by pushing pharmaceuticals, stolen credit cards, and shady social-media marketing tools.

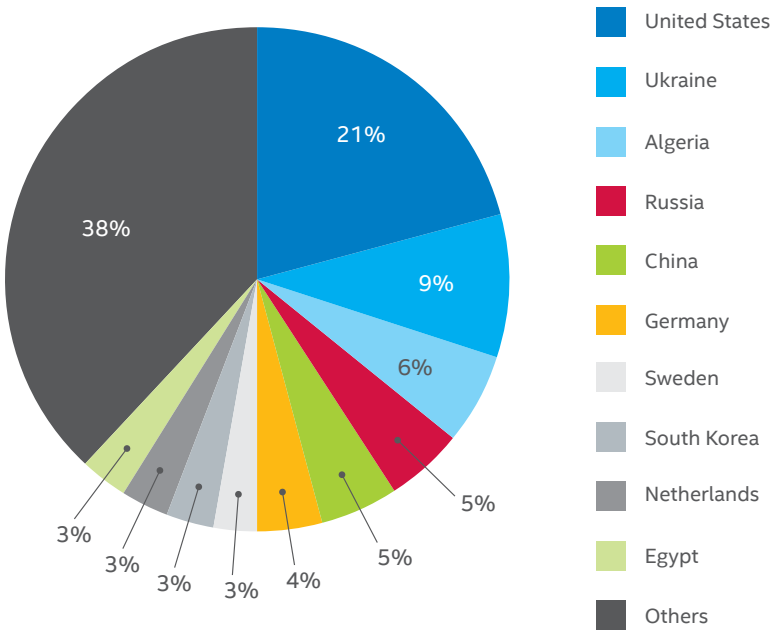
SSL-related attacks continue, although they have subsided somewhat from Q4 2014. This reduction is likely the result of SSL library updates that have eliminated many of the vulnerabilities exploited in prior quarters. Shellshock attacks are still quite prevalent since their emergence late last year.

Top Network Attacks



Source: McAfee Labs, 2015.

Top Locations of Botnet Control Servers



Source: McAfee Labs, 2015.

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 Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world.

www.intelsecurity.com

1. https://msdn.microsoft.com/en-us/library/windows/hardware/ff559309%28v=vs.85%29.aspx.
2. http://www.cse.scu.edu/~tschwarz/coen252_07/Resources/foi-computer-forensics.pdf.
3. http://en.wikipedia.org/wiki/Adobe_Flash.

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