McAfee Labs
Threats Report

November 2014

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

The holiday season is upon us and the bad guys are up to their usual tricks. McAfee recently published our ***12 Scams of the Holidays***, a list that highlights some of those antics. It's a fun read and I encourage you to check it out. We've also begun to see predictions for everything in 2015 from the direction of the global economy to which Hollywood stars will shine the brightest.

For the past several years, McAfee Labs has also provided predictions in our area of expertise. In **last year's predictions report**, we were on the button with many of those predictions. For example, we correctly predicted that ransomware would proliferate (including ransomware on mobile platforms!), politically motivated attacks would increase, and enterprises would aggressively embrace threat intelligence services and analytic tools to identify increasingly stealthy threats. But, of course, we weren't perfect so we missed a few too. Such is the nature of predictions.

This year, we decided to move forward the publication of our 2015 threats predictions and include them in this report. By doing so, our customers will have more time to think through what to expect in 2015 and prepare for the most significant threats. Of course, we continue to deliver Key Topics and Threats Statistics as we do in every quarterly report.

Our lead Key Topic this quarter discusses BERserk, a vulnerability inside RSA signature verification software that could be exploited by cybercriminals in a number of far-reaching ways. McAfee's disclosure of BERserk was overshadowed by the **Shellshock** announcement but the former's potential for harm is also significant. More details about BERserk can be found **here**. In a related story, we discuss the various ways in which user trust is abused by cybercriminals. It reminds us that awareness and training are paramount in the battle against this type of threat.

You will notice in this report that we have added new charts and changed some on-going charts in the Threats Statistics section. Reader feedback prompted us to add statistics that are valuable to you. Further, we are starting to leverage better reporting from our own systems to improve the accuracy of some of our charts. We hope you like these changes and additions.

To those who responded to our reader survey in the ***August Threats Report***, we thank you. We are listening, as evidenced by the threat statistics improvements noted above. If you would like to share your views about this report, please click **here** to complete a quick, five-minute survey about the current *Threats Report.*

Happy holidays to you and your loved ones.

—Vincent Weafer, Senior Vice President, McAfee Labs

Share feedback

Contents

McAfee Labs Threats Report
November 2014

This report was researched and written by:

Cedric Cochin
Benjamin Cruz
Michelle Dennedy
Aditya Kapoor
Dan Larson
Haifei Li
Chris Miller
Igor Muttik
François Paget
Eric Peterson
Mary Salvaggio
Craig Schmugar
Ryan Sherstobitoff
Rick Simon
Dan Sommer
Bing Sun
Vinoo Thomas
Ramnath Venugopalan
James Walter
Adam Wosotowsky
Stanley Zhu

Executive Summary

McAfee Labs 2015 threats predictions

This *Threats Report* kicks off with threat activity we expect to see in 2015. Our predictions run the gamut, including opinions around the Internet of Things, cyber espionage, mobile devices, privacy, ransomware, and more.

Going BERserk: trusted connectivity takes a big hit

In September, **Intel Security released details** of a far-reaching vulnerability dubbed BERserk, in a nod to the underlying code that forms the source of the vulnerability. At the time of this writing, BERserk's full impact is not known, but it is very significant. BERserk takes advantage of a flaw in RSA's signature verification software, opening the door to cybercriminals to establish man-in-the-middle attacks without users knowledge. Establishing trust when accessing a website usually starts with "https" at the beginning of a URL coupled with a friendly padlock to seal the deal. BERserk compromises that link, allowing bad guys to watch and do anything they want with the flow of information between the user and the website.

BERserk takes advantage of a flaw in RSA's signature verification software, opening the door to cybercriminals to establish man-in-the-middle attacks without users knowledge.

Abuse of trust: exploiting online security's weak link

The weakest links in most security setups are users. We rely on devices for most of our information and trust that they provide accurate information in a secure manner. Attackers often zero in on the trust we place in our devices, using it against us to steal information. This Key Topic explores trust abuse, highlighting through recent examples the many ways in which cybercriminals take advantage of our trust relationships. McAfee Labs believes that trust in many forms of online interaction will go the way of email, which inspires limited confidence in its authenticity.

McAfee Labs believes that trust in many forms of online interaction will go the way of email, which inspires limited confidence in its authenticity.

McAfee Labs 2015 Threats Predictions

Cyber espionage

Internet of Things

Privacy

Ransomware

Mobile

Point of sale

Malware beyond Windows

Vulnerabilities

Escaping the sandbox

Share feedback

Cyber espionage

Cyber espionage attacks will continue to increase in frequency. Long-term players will become stealthier information gatherers while newcomers will look for ways to steal money and disrupt their adversaries.

Small nation states and foreign terror groups will take to cyberspace to conduct warfare against their enemies. They will attack by launching crippling distributed denial of service attacks or using malware that wipes the master boot record to destroy their enemies' networks. At the same time, long-term cyber espionage players will implement better methods to remain hidden on a victim's network, using better and more sophisticated stealth technologies and other means to remain below the operating system and out of sight.

Of particular note, McAfee Labs now sees sophisticated Eastern European cybercriminals shifting from quick, direct attacks on financial-institution customer credentials (leading to financial theft) to a more sophisticated advanced persistent threat (APT) approach in which they collect intelligence that they can either sell or use at a later date. In this way, criminals are beginning to look and act more like sophisticated nation-state cyber espionage actors, who watch and wait to gather intelligence.

A similar approach has begun to emerge in the retail sector. Many retailers now build rich profiles about their customers—including buying habits and product interests, credit history, location history, contact details, and more. Further, successful retailers' strategic, operational, and financial plans can be quite valuable to the right buyer. Some cybercriminals appear to be using an APT-based cyber espionage approach to infiltrate retailers' systems, from which they surreptitiously gather intelligence beyond credit card information to sell to the highest bidder.

—Ryan Sherstobitoff

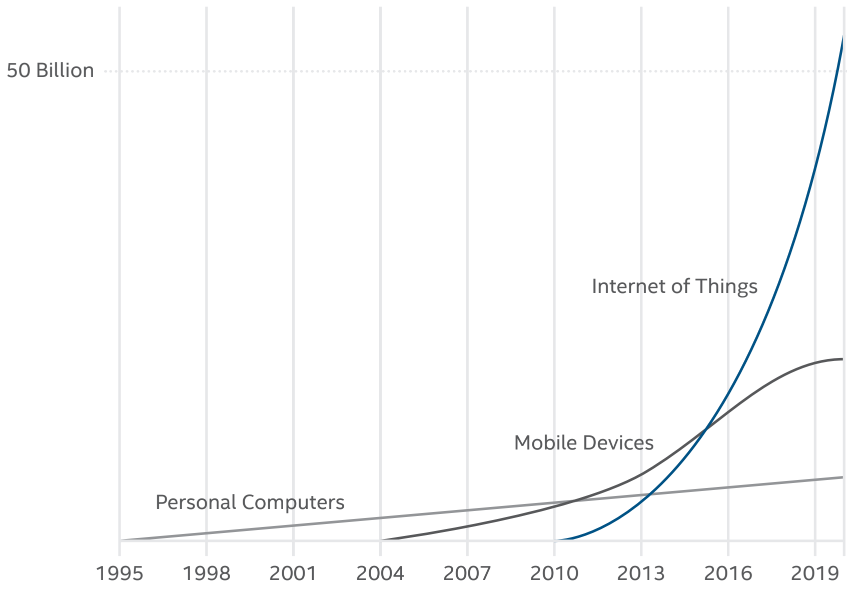
Internet of Things

Attacks on the Internet of Things devices will increase rapidly due to hypergrowth in the number of connected objects, poor security hygiene, and the high value of data on those devices.

The number and variety of devices in the Internet of Things (IoT) family is growing exponentially. In the consumer space, they are now seen in appliances, automobiles, home automation, and even light bulbs. On the business side, there are many applications, including uses in farming, manufacturing, and health care. IoT devices are made from an ever-widening array of software and hardware building blocks, leading to significant complexity, which is the enemy of security.

These components and thus the devices themselves are not typically built with security as a basic design principle. The increasingly vast deployment of IoT devices combined with the lack of robust security represents a burgeoning threat to the privacy and security of both individuals and companies.

Global Internet-Connected Devices



Sources: McAfee, based on research by BI Intelligence, IDC, and Intel.

Attacks against IoT devices are already common place—from IP cameras with weak security controls to smart meters with basic encryption flaws to the SCADA devices that power critical infrastructure throughout the world. In Spain, for example, network-connected electric meters installed in millions of homes contain vulnerabilities that attackers could use to carry out billing fraud or even cause blackouts. At a white-hat hackers conference last year, researchers illustrated how some Internet-connected security cameras could be easily breached, allowing them to both steal the video from the cameras and gain entry to the cameras' network.

One type of threat is particularly alarming: With the increasing proliferation of healthcare IoT devices and their use in hospitals, the threat of the loss of information contained on those devices becomes increasingly likely. Healthcare data is even more valuable than credit card data because stolen health credentials can go for US$10 each, which is about 10 to 20 times the value of a U.S. credit card number, **according to Reuters.**

What was once the realm of nation states and enterprising cybercrime organizations can now become the playground of any motivated attacker. We predict that there will be a major attack in 2015 directly related to vulnerabilities in IoT devices.

—*Chris Miller and Ramnath Venugopalan*

Privacy

Data privacy will remain under attack as governments and businesses continue to grapple with what is fair and authorized access to imperfectly defined "personal information."

We define data privacy as the fair and authorized processing of personally identifiable information. Although the practice and problem of privacy may be stated in this simple sentence, the complexity and risk associated with privacy mishaps are growing and will continue to grow at an exponential rate in 2015.

Unpacking the definition, "fair" is a concept that is subjective to system users, customers or employees of businesses, or citizens of a nation state. Fairness can be further defined by a group of fair information practice principles that have been internationally recognized as far back as the 1960s. Transparency, notice, choice, proportionate collection, cross-border data sharing and handing, security, limited access, and disposal are some of these principles.

"Authorized" is another element of data privacy. Who am I and what do I get to do when managing data assets? Who are you as a customer, employee, or citizen in an increasingly digital and at-arm's-length global economy? In 2015, we will continue to see antiquated role-based systems and password schemas fail and be owned by those with malicious intent or at least sloppy practices. Biometrics and IDs in context are probably the best indicators of presence and intent; they will be a huge area for innovation. We predict that who, when, and where you are will continue to push innovation and exploitation risks skyward.

The last element of privacy's definition is "personally identifiable information." In 2015 we will see yet more discussion and lack of clarity about what exactly is our "personal" information and what is reasonably available for observation by state or private actors. The legal definition in many places is that personal information is either data that directly identifies a specific individual or data that, in combination with other data, is likely to identify a specific person. Although statisticians and economists have always taken large sets of anecdotes to create "data," the technically trendy like to call the phenomenon of using large sets of information "Big Data." The bigger the Big Data, the less likely we are able to truly remain anonymous. Thus, the trend for 2015 and beyond will be the ever-increasing scope of data privacy rules and regulations, with all their breach requirement and security specifications, into the realm of the previously anonymous data sets.

By the close of 2015, we expect to see the European Union update its **1995 Data Protection Directive** with a 2016 Data Protection Regulation that will take effect in all EU member states and will reach all international organizations. This move on the part of the EU is perhaps the loudest of the public policy machinations, but countries in Latin America, Australia, Japan, South Korea, Canada, and many others will become more aggressive and more specifically territorial with data privacy laws and regulations.

—Michelle Dennedy

Ransomware

Ransomware will evolve its methods of propagation, encryption, and the targets it seeks. More mobile devices will suffer attacks.

We predict ransomware variants that manage to evade security software installed on systems will specifically target endpoints that subscribe to cloud-based storage solutions such as Dropbox, Google Drive, and OneDrive. Once those endpoints have been infected, the ransomware will attempt to exploit the logged-on users' cloud access credentials to also infect data backed up to the cloud.

Once they discover that their endpoint data has been encrypted, ransomware victims will be in for a rude shock when they attempt to access their cloud storage to restore data—only to find their backups have also been encrypted by the ransomware.

Although files encrypted by ransomware cannot spread and infect other devices on their own, we can imagine an evolution in tactics in which each encrypted file becomes a carrier of the ransomware itself by converting the target file into an executable with the original data file stored within the body of the malware. This technique has been used by file-infecting viruses to take over legitimate executables and make them carriers. Ransomware authors could replicate the same model for file encryption.

As we predicted last year, we again expect a rise in ransomware targeting mobile devices. With phones and tablets hosting cherished pictures and personal data, they make an attractive target for malware authors. And we expect the technique of ransomware targeting cloud-backed-up data to be repeated in the mobile space. With mobile platforms supporting a myriad of unregulated payment methods, attackers will find multiple avenues to extract ransom payments from victims to release their encrypted data.

—*Vinoo Thomas*

Mobile

Mobile attacks will continue to grow rapidly as new mobile technologies expand the attack surface and little is done to stop app store abuse.

PC malware historically grew in volume on the heels of notable events, such as the emergence of malware-generation kits (allowing those with no programming knowledge to create threats), the release of malware source code (allowing those with minimal programming experience to modify threats), and abuse of popular features, applications, or script engines. We will see a similar impact on the mobile malware landscape in 2015. Open and commercial mobile malware source code is on the rise, the fruits of which are likely to be harvested in the near future. And it's only a matter of time before mobile malware–generation kits take off, lowering the barrier of entry for would-be thieves.

The Apple iPhone 6, with its near field communication (NFC) chip and integrated digital wallet, will legitimize the use of NFC to make digital payments. Other mobile device vendors will quickly adopt these technologies in 2015 and users will begin transacting business in a meaningful way using these technologies. Because these are point-of-sale (POS) transactions and cyberthieves love POS theft, this will be a big target for the bad guys. In 2015, researchers will likely discover vulnerabilities in NFC hardware and digital wallet software and cyberthieves will attempt to exploit them.

The method of mobile malware installation will largely remain the same. Trusted app stores like Apple's App Store and the Google Play store do a fairly good job keeping malware-laden apps off their shelves, but it still occurs. Further, there are many untrusted app stores and direct app download websites whose apps frequently contain malware. Traffic to these malevolent app stores and sites is often driven by "malvertising," which has grown quickly on mobile platforms. In 2015, we will continue to see rapid growth in malvertising that targets mobile users, perpetuating the growth in mobile malware.

We also expect growth in mobile ransomware as attackers seek to port effective extortion methods from the PC world. Once perfected on mobile platforms, ransomware will be even more lucrative to cyberthieves than it is on PCs because mobile users depend a great deal on their devices for immediate access to critical information such as contacts, schedules, and directions. With so many eggs in the mobile device basket, users will do what it takes—including the payment of ransom—to regain access.

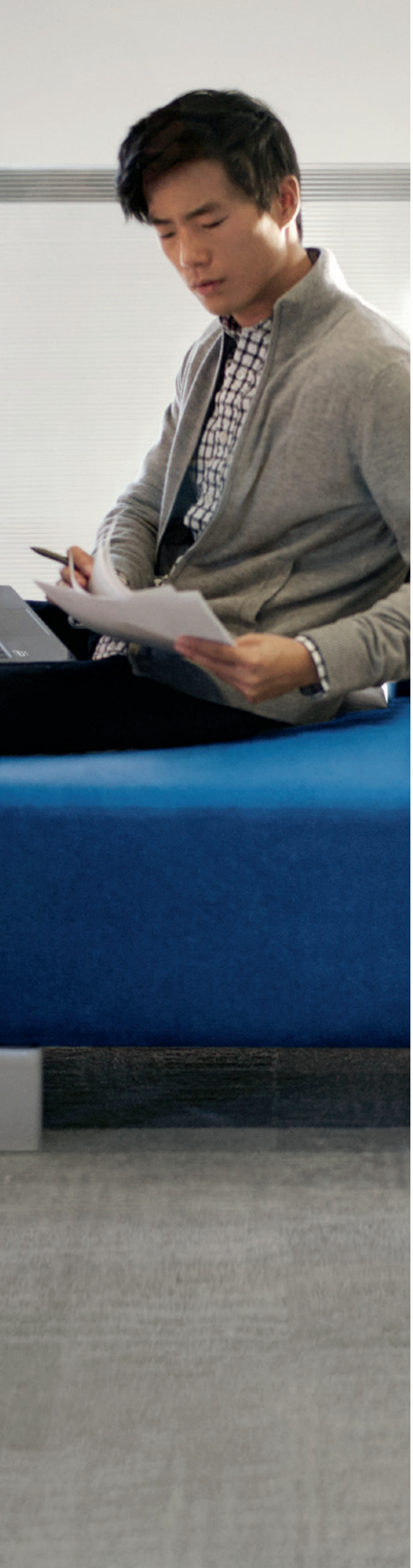
—Craig Schmugar and Bing Sun

Point of sale

Point of sale (POS) attacks will remain lucrative, and a significant upturn in consumer adoption of digital payment systems on mobile devices will provide new attack surfaces that cybercriminals will exploit.

In 2013, $15 trillion exchanged hands in retail transactions, according to one **Forbes article**. This makes payment systems for those transactions an enticing target for cybercriminals. In 2014 we saw a significant uptick in attacks on these systems, including a massive breach at Home Depot. All the while, credit card skimmers continued to plague consumers. They too became more pervasive this year, seen in everything from restaurant card swipers to ATMs to gas pumps. POS attacks are so common that they have become a part of the daily routine for those working in the industry. Yet little has been done to improve POS security, so we expect to see continued growth in POS system breaches in 2015. However, in the United States we may see relief late in 2015 as retailers begin to deploy chip-and-pin cards and card readers.

Next year we expect to see a significant increase in the use of digital payment systems. Apple updated its iPhone to include NFC technology. This enables its new iWallet feature, which will beam credit card info into payment systems rather than requiring consumers to swipe their cards. Several Android devices also support NFC, and they use the process called Host Card Emulation to facilitate mobile payments. Both Visa and MasterCard have adopted this technology and now offer mobile payment apps that work with NFC-enabled devices. With the infrastructure now in place, we expect to see broad consumer adoption. And, in turn, we also expect to see successful attacks on these systems.



Digital payment systems can eliminate the risk of credit-card skimmers, but they come with risks of their own. Paramount among those risks are vulnerabilities in the underlying NFC technology. Some of these vulnerabilities were highlighted at DEF CON 2013 and continue to be tracked by the **NFC Awareness Project**. The fundamental problem is that sensitive information is now sent wirelessly, and there is potential for attackers to exploit this connection. There is an established history for attacks of this nature including the "Bluetooth Sniper Rifle" attack in 2005 and the remote cloning of radio frequency identification (RFID) passports in 2009. Similar attacks targeting NFC devices are likely because there are already **documented vulnerabilities**. With consumers now sending payment information over a protocol with known vulnerabilities, it is highly likely that attacks on this infrastructure will emerge in 2015.

—Dan Larson

Malware beyond Windows

Non-Windows malware attacks will explode, fueled by the Shellshock vulnerability.

During the second half of 2014, we learned of the **Shellshock vulnerability**: a weakness in Bash, a command shell found on Unix, Linux, and OS X machines. It lets an attacker perform arbitrary commands on the victim's machine, which makes it the most dangerous type of vulnerability—rated 10 out of 10 for severity by the **U.S. National Vulnerability Database**.

The aftershocks of this newly discovered vulnerability will be felt for years to come. Many, many devices run some form of Unix or Linux, from routers to TVs, industrial controllers, flight systems, and critical infrastructure. We are just beginning to understand the scope of this vulnerability.

This vector of attack will be the entry point into infrastructures from consumer appliances to enterprises that are heavily dependent on non-Windows systems. As a result, we expect to see a significant increase in non-Windows malware during 2015 as attackers look to capitalize by exfiltrating data, holding systems ransom, assimilating spam bots, and carrying out other nefarious escapades. Shellshock will grip the headlines as attackers exploit new, and old, vulnerable devices to carry out their attacks.

—Craig Schmugar

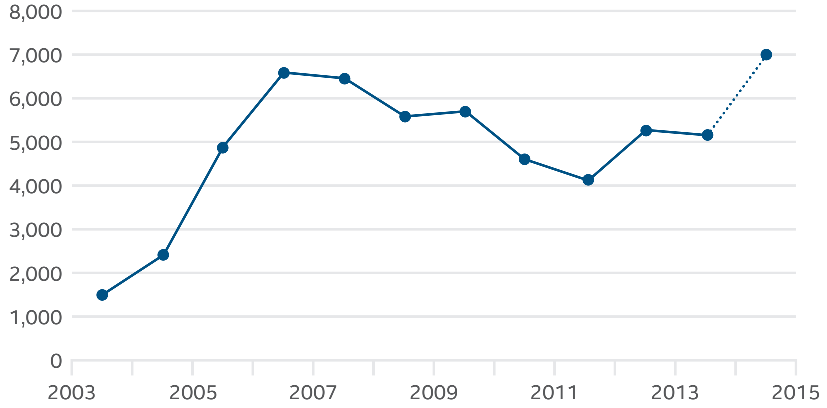
Vulnerabilities

Vulnerabilities will increase as the number of flaws in popular software continues to grow.

Data from the U.S. government's National Vulnerability Database show that for the last three years the number of vulnerabilities has increased. Based on about 5,200 entries recorded as of September 30, the total number for 2014 might exceed the record set in 2006.

Counting vulnerabilities is not a direct indication of risk because many interrelated factors are in play—the speed and coverage of patches, the severity of each vulnerability, the window of exposure, and many others. These counts, however, give us a view of the general health of the ecosystem.

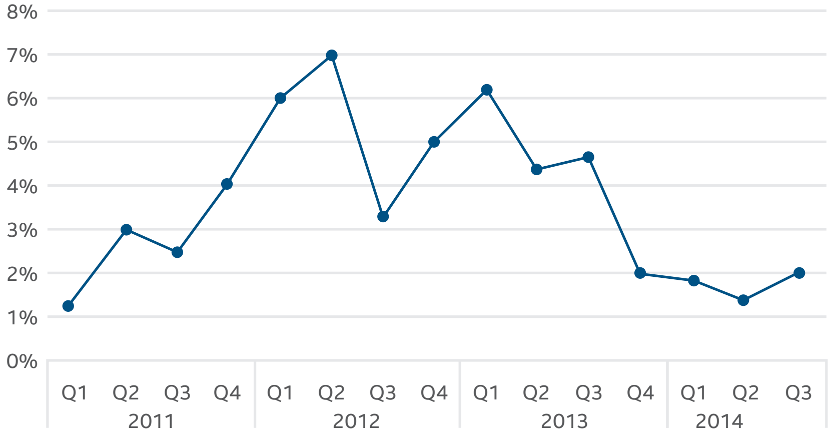
Application Vulnerabilities Reported



Source: National Institute of Standards and Technology—National Vulnerability Database.

We saw a decline in the number of vulnerabilities from 2006–2011, but that's no longer the case. The downturn might be attributable to stack checking in compilers, data execution prevention, and address space layout randomization in 64-bit software. The recent upward trend likely reflects new exploitation techniques such as stack pivoting as well as return- and jump-oriented programming in combination with a deeper understanding of 64-bit software by black-hat and white-hat vulnerability hunters.

Percentage of New Malware Samples That Exploit Known Vulnerabilities



Source: McAfee Labs.

McAfee Labs analyzed our malware zoo to determine how often malware exploits known vulnerabilities. Depending on the quarter, between 1% and 6% of all new malware samples take advantage of a known vulnerability. In this period, the figure was about 2%, which translates to 821,000 new malware samples that exploited a known vulnerability. As the absolute number of samples that make use of exploit techniques grows, the volume of malware grows as well; thus the proportion of "exploit-related" samples remains relatively stable.

In 2015 we expect no significant changes to the vulnerability mitigations available to applications or operating system developers. Further, the rate of adoption for current and emerging best practices is unlikely to increase. Thus we predict that the number of newly discovered vulnerabilities will keep climbing and in turn so will the volume of malware that exploits those newly discovered vulnerabilities.

—Igor Muttik and François Paget

Escaping the sandbox

Escaping the sandbox will become a significant IT security battlefield.

Many critical and popular applications, including Microsoft Internet Explorer, Adobe Reader, and Google Chrome, have implemented their own sandboxing technology to confine malicious behaviors. Because application sandboxing is effective in stopping many types of attacks, malware authors have been looking for ways to get around this type of security mechanism.

Let's take Internet Explorer as an example. Malware that can't bypass its sandbox won't pose a threat to users, because the exploit can make no persistent change to the system. However, there are two versions of Internet Explorer's sandboxing technology—Protected Mode (PM) and Enhanced Protected Mode (EPM). Currently, the default for Internet Explorer 10 and 11 is PM, and our research has shown that PM is relatively easy to bypass. Although we have not seen an in-the-wild exploit that bypasses either PM or EPM, the building blocks are there, so we will probably see some cases of Internet Explorer sandbox escape and subsequent zero-day attacks in 2015.

Vulnerabilities that can lead to an application sandbox escape have been found and disclosed in many major client applications. Documented vulnerabilities have been found in Adobe Reader and Flash, Chrome, Apple Safari, Oracle Java, and Internet Explorer. Those vulnerabilities have led both researchers and attackers to investigate further. At BlackHat 2014, for example, researchers outlined four application sandbox bypass techniques successfully used in winning entries at this year's Pwn2Own hacking contest. In fact, almost all successful "pwns" in this year's contest included successful sandbox escapes in the final stage of exploitation.

We have already seen techniques that exploit vulnerabilities and escape application sandboxes. It's only a matter of time before those techniques are offered to cybercriminals on the black market. We believe that will happen in 2015.

One additional prediction: To date, cybercriminals have mainly focused on escaping application sandboxes. However, increasingly popular standalone sandbox systems offered by security software vendors pose a new hurdle for cyberthieves. In response, cybercriminals have begun to explore ways for their malware to escape from those sandbox systems. Today a significant number of malware families identify and evade sandbox-based detection. However, to date we know of no malware in the wild that has successfully exploited hypervisor vulnerabilities to break out of a standalone sandbox system. We expect that to change in 2015.

—Haifei Li, Rick Simon, Bing Sun, and Stanley Zhu

Key Topics

Going BERserk: trusted connectivity takes a big hit

Abuse of trust: exploiting online security's weak link

Share feedback

Going BERserk: trusted connectivity takes a big hit

—James Walter

In the Key Topic **"Abuse of trust: exploiting online security's weak link,"** we offer an overview of the challenges we now face regarding the trustworthiness of online websites. In this Key Topic we take a look at a specific vulnerability that profoundly affects trust.

The Intel Security Advanced Threat Research team focuses on several key areas that affect the safety of online transactions and information flow. One of these key areas is the Security Communications Baseline. This area includes deep threat and exposure analysis within SSL/TLS, TPM 2.0, cryptographic side channels, and other areas that we often take for granted when assuming that the existing trust model is "solid."

In September, the Intel Security Advanced Threat Research team released details of the vulnerability dubbed BERserk. The name is derived from the vulnerable condition enabled by the parsing of specific encoded sequences that follow basic encoding rules (BER) within the implementation of RSA signature verification. Both Intel Security and security researcher Antoine Delignat-Lavaud disclosed the vulnerability to Mozilla, prompting the company to release updates to multiple products, including Firefox, Thunderbird, SeaMonkey, and NSS. Google also updated its Chrome browser and OS because the NSS cryptographic library is used in those products.

The flaw lies within RSA signature verification, specifically, within the incorrect parsing of ASN.1-encoded sequences during sequence verification. This vulnerability is a variation of the Bleichenbacher PKCS#1 v1.5 RSA Signature Forgery vulnerability defined in **CVE-2006-4339**. Vulnerable implementations scan the encoded message for padding bytes 0xFF until separator byte 0x00 is found. The process continues validating DigestInfo and the message digest against expected values without making sure that the DigestInfo and the message digest are right-justified in the encoded message (EM), which would ensure that there are no extra bytes left after the message digest. Without that check, an EM' could be constructed to include extra garbage right after the message digest such that this EM' would satisfy the following signature verification:

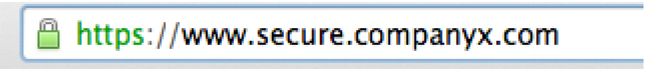
EM' = 00 01 FF FF FF FF FF FF FF FF 00 DigestInfo MessageDigest Garbage

The additional garbage in EM' allows an adversary to generate RSA signatures that, after cubing performed over RSA modulus, gives this EM':

EM' = (s')^3 mod N

An adversary can create an RSA signatures' without knowing the RSA private key {p,q,d} and thus can forge RSA signatures.

The result allows an attacker to forge RSA certificates with no knowledge of the corresponding RSA private key. But what does this mean? How are we impacted?



https://www.secure.companyx.com

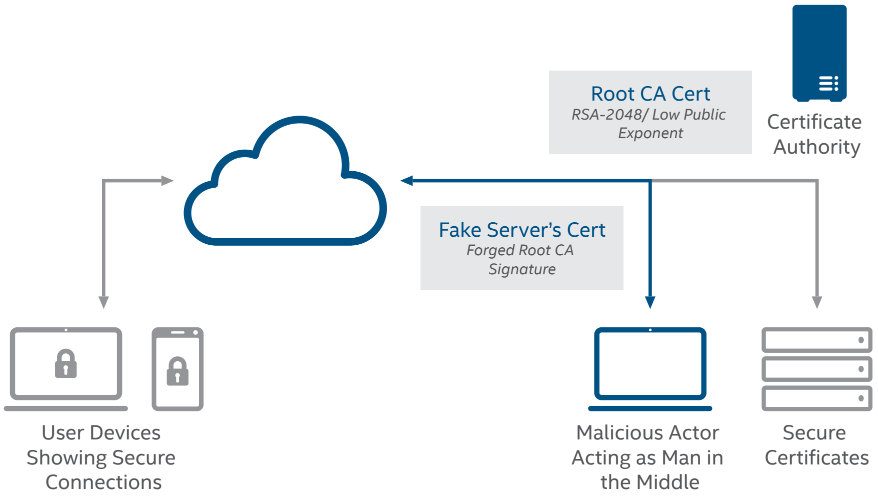
Share this Report

BERserk opens the door to cybercriminals to establish Internet session man-in-the-middle attacks without users knowledge. Its potential for harm rivals that of Shellshock.

The answer is simple. We good citizens and users of the Internet have grown accustomed to a certain trust model. When we are working on an online transaction (banking, medical, or other transactions requiring personal data), we know how to check whether the session is secure. We have been taught to look for "https" in URLs, along with helpful pictures of padlocks. These things help us decide whether a site or application is secure and not exposing any data to nefarious parties.

BERserk and related vulnerabilities change this and challenge our perception of trust and the security of sessions communicated over SSL/TLS. With the ability to accurately forge RSA signatures, an attacker can establish man-in-the-middle sessions in any number of scenarios.

BERserk Vulnerability Could Lead to Man-in-the-Middle Attacks


Root CA Cert
RSA-2048/ Low Public Exponent
Certificate Authority
Fake Server's Cert
Forged Root CA Signature
User Devices Showing Secure Connections
Malicious Actor Acting as Man in the Middle
Secure Certificates

The confidentiality and integrity of sessions between customers and their banking websites, for example, can be compromised. With fake certificates in place, users can visit sites, and even view certificates to confirm their authenticity. All will appear valid when the opposite is true. In similar fashion, users logging into doctors' websites for results could fall victim to this flaw. The same applies to doing online taxes and many more scenarios.

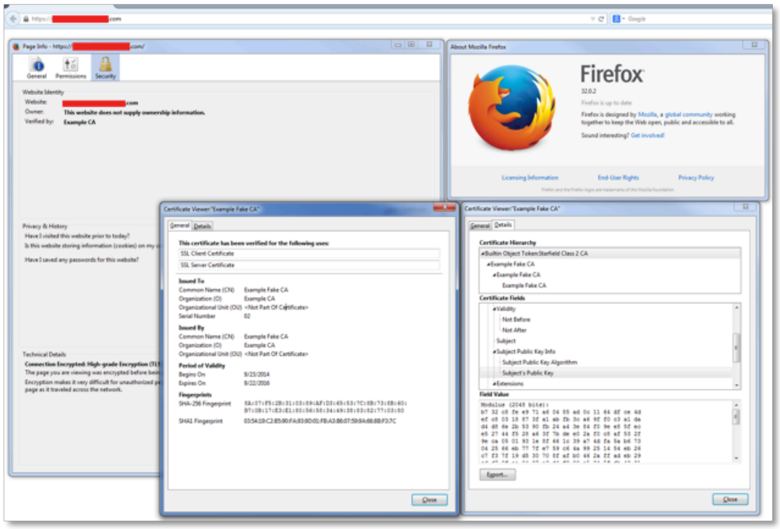
Looking beyond web and software threats, cryptographic libraries used within hardware devices such as phones store sensitive data that is accessed by applications on demand. Imagine that a mobile phone or tablet contains secure memory and execution for providing cryptographic functions to the device's software. There will be firmware on the device that is digitally signed to prevent unauthorized modification by malware or manual user intervention. With the BERserk flaw, however, it is possible to compromise the firmware, thereby impacting the integrity and confidentiality of data subject to the secure hardware element.

Share this Report

Learn how McAfee can help protect against this threat.

A common use of this model is the storage of financial account data used for payments at specialized vendors or terminals such as NFC payment systems in which all card data is stored on the device. In this scenario, attackers could manipulate sessions in multiple ways, including hijacking and manipulating input and output, or simply collecting and stealing sensitive data.

In our research, we have been able to forge up to 1,024- and 2,048-bit RSA certificates. Doing so can benefit an attacker. Specifically with Mozilla NSS, attackers can forge their certificates, and the certificate chain will be trusted by Mozilla NSS.



Website Identity
Website: [redacted].com
Owner: **This website does not supply ownership information.**
Verified by: **Example CA**

Privacy & History
Have I visited this website prior to today?
Is this website storing information (cookies) on my c

Have I saved any passwords for this website?

Technical Details
Connection Encrypted: High-grade Encryption (TLS
The page you are viewing was encrypted before bein
Encryption makes it very difficult for unauthorized p
page as it traveled across the network.

32.0.2
Firefox is up to date
Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.
Sound interesting? Get involved!

Firefox and the Firefox logos are trademarks of the Mozilla Foundation.

This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate

Issued To
Common Name (CN) Example Fake CA
Organization (O) Example CA
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 02

Issued By
Common Name (CN) Example Fake CA
Organization (O) Example CA
Organizational Unit (OU) <Not Part Of Certificate>

Period of Validity
Begins On 9/23/2014
Expires On 9/22/2016

Fingerprints
SHA-256 Fingerprint [illegible]
SHA1 Fingerprint 03:54:19:C2:85:90:FA:93:9D:01:FB:A3:B6:07:59:8A:66:8B:F3:7C

Certificate Hierarchy
Builtin Object Token:Starfield Class 2 CA
Example Fake CA
Example Fake CA
Example Fake CA

Certificate Fields
Validity
Not Before
Not After
Subject
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions

Field Value

```
Modulus (2048 bits):
b7 32 c8 fe e9 71 a6 04 85 ad 0c 11 64 df ce 68
ef c8 03 18 87 3f a1 ab fb 3c a6 9f f0 c3 a1 da
d4 d8 6e 2b 53 90 fb 24 a4 3e 84 f0 9e e8 5f ec
e5 27 44 f5 28 a6 3f 7b de e0 2a f0 c8 af 53 2f
9e ca 05 01 93 1e 8f 66 1c 39 a7 48 fa 5a b6 73
04 25 66 eb 77 7f e7 59 c6 4a 99 25 14 54 eb 26
c7 f3 7f 19 d5 30 70 8f af b0 46 2a ff ad eb 29
```

A forged certificate, seen in Firefox.

The Intel Security Advanced Threat Research team continues to examine these issues and how other scenarios outside of browser behavior are affected. Our team is also cooperating with CERTs and affected vendors to address these issues.

Vendors of affected cryptographic libraries continue to release updates and guidance. Mozilla and Google have updated products. Affected users should follow the guidance of their vendors and keep systems up to date.

For additional information on BERserk:

- BERserk vulnerability: **Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5**
- BERserk vulnerability: **Part 2: Certificate forgery in Mozilla NSS**
- Intelsecurity.com: **BERserk**
- Computer Emergency Response Team: **VU#772676**
- National Vulnerability Database: **CVE-2014-1568**

Share this Report

Abuse of trust: exploiting online security's weak link

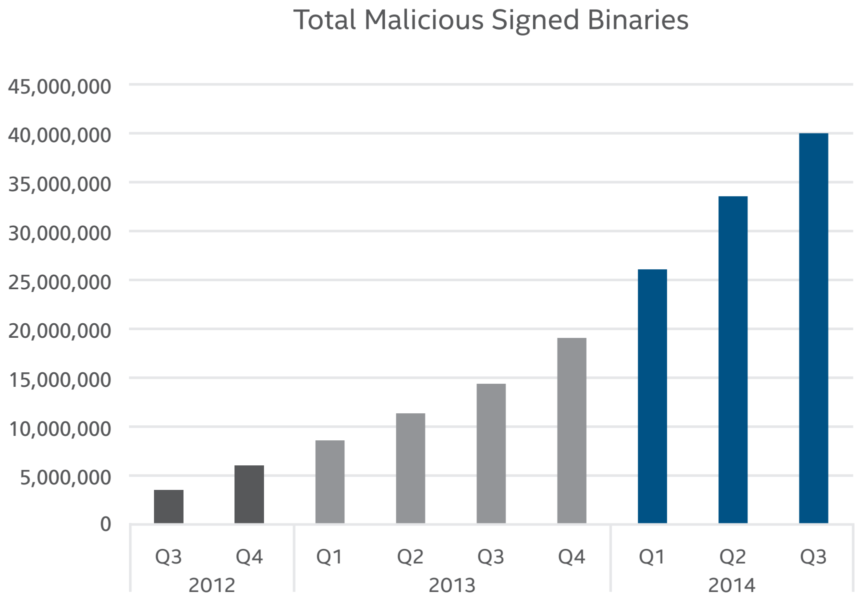
—Cedric Cochin and Craig Schmugar

Every day, much of the world's population relies on an electronic device, whether it's a personal computer, a mobile phone, a television, or even an automobile. We've come to rely on these items and in most cases trust that they provide accurate information.

But trust must be earned and established, a process that often takes time and money. Corporations spend millions of dollars each year to strengthen their brands, knowing a good investment in this area will yield returns many times over. They understand that consumers are more likely to take action when a good name is associated with an item.

Attackers are well aware of this, but often lack the time, resources, and patience required to establish a trust relationship with their victims. They're left to find ways to exploit trust investments and the relationships of others.

Forms of trust abuse occur many times a day, and the trend is getting worse. For example, McAfee Labs tracks malicious signed binaries, which are a form of trust abuse because attackers camouflage malware by making it appear to be a legitimate, certified file. The growth of malicious signed binaries has risen unabated since we began tracking it in 2007.

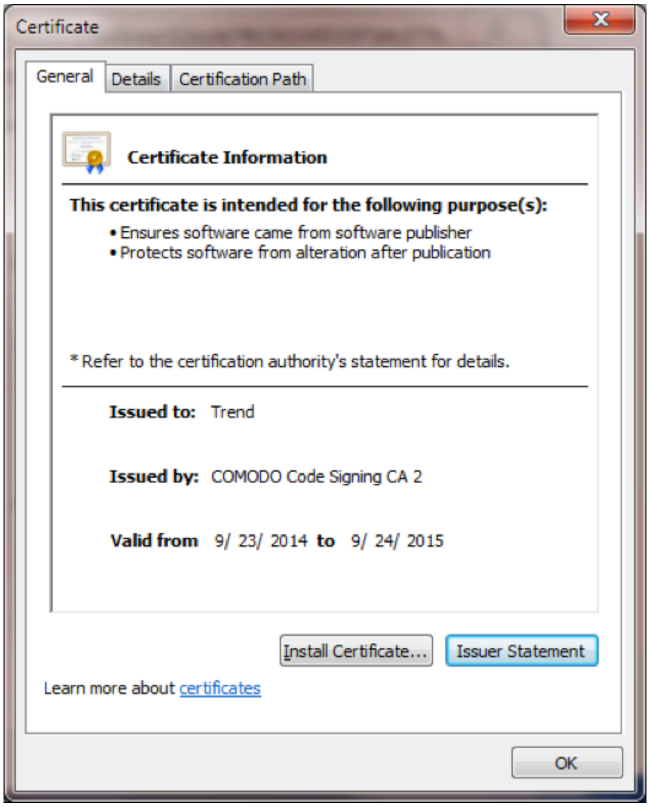


Malware authors digitally sign their threats to abuse user, product, and operating system trust. Source: McAfee Labs.

Inherited trust exploits the value users place in a brand name. Websites often blur the relationship between trusted brands and other brands also appearing on their sites.

Inherited trust

For many years, establishing trust with a commercial brand during a transaction was as simple as confirming the brand. Today, consumers must also determine whether the trusted brand in turn trusts other brands represented through the trusted brand's online presence. In September the **"Kyle and Stan" malicious advertising network** was exposed distributing "malvertisements" through popular websites such as Amazon.com, ads.yahoo.com, and youtube.com, as well as **major advertising networks such as Double-Click and Zedo**. One malicious campaign delivered through the Zedo ad network **reportedly impacted users** of Alexa top-ranked websites to deliver signed CryptoWall Trojan variants. The digital signature used was issued to "Trend," likely intended to mimic the security vendor Trend Micro. Initial telemetry shows North American users were among the most affected. Unfortunately many consumers infer an "innocence by association" trust that is often misplaced.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Trend

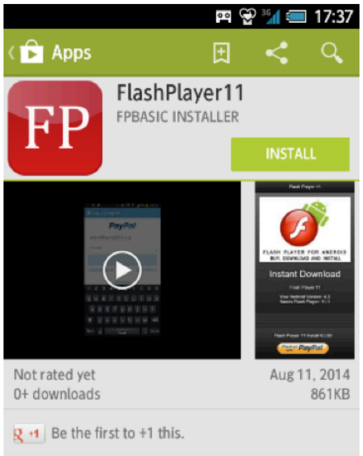
Issued by: COMODO Code Signing CA 2

Valid from 9/ 23/ 2014 **to** 9/ 24/ 2015

Learn more about certificates

Certificate used to sign CryptoWall.

This trust relationship between a consumer and a commercial brand is commonly abused. One example is a copycat application in which a virus or Trojan is said to be a legitimate, usually popular program. During the past quarter, scammers attempted to pawn off an Adobe knockoff "FlashPlayer11" as the real deal. According to both the Google Play download count and McAfee Mobile Security detection telemetry, the scammers achieved some success in tricking users.



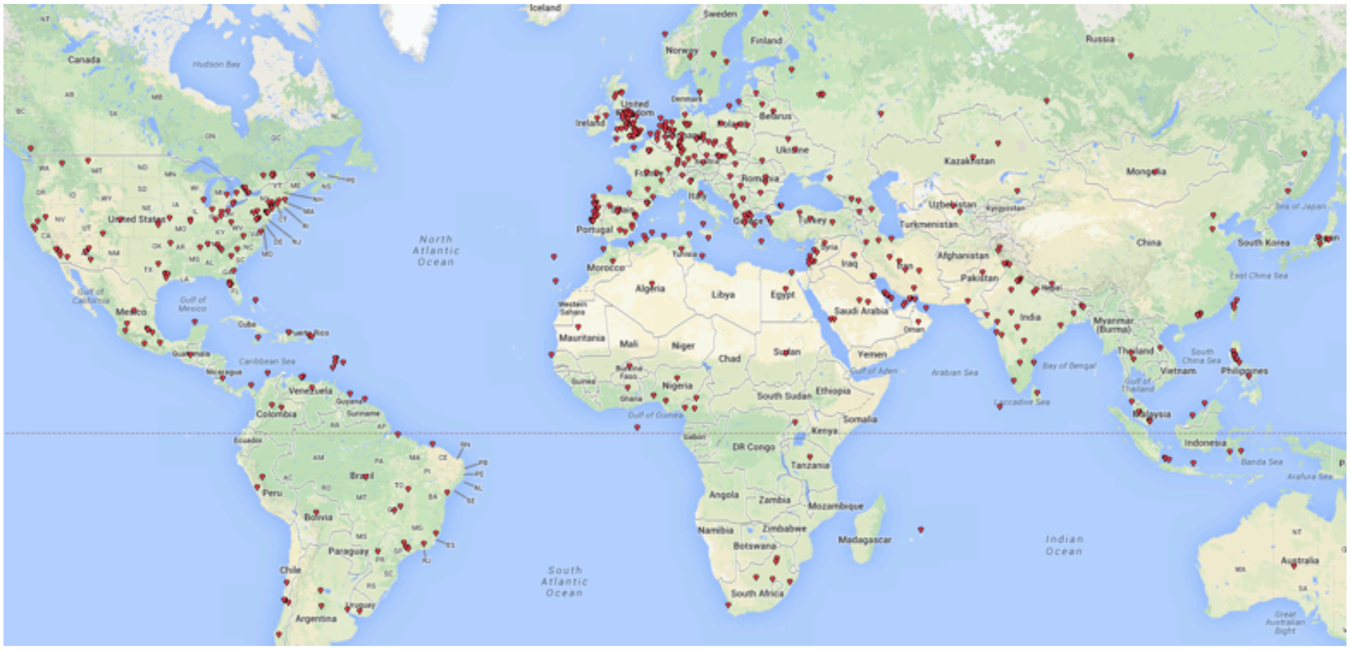
FlashPlayer11
FPBASIC INSTALLER

Not rated yet
0+ downloads

Aug 11, 2014
861KB

Be the first to +1 this.

One of several copycat "FlashPlayer11" apps on Google Play.

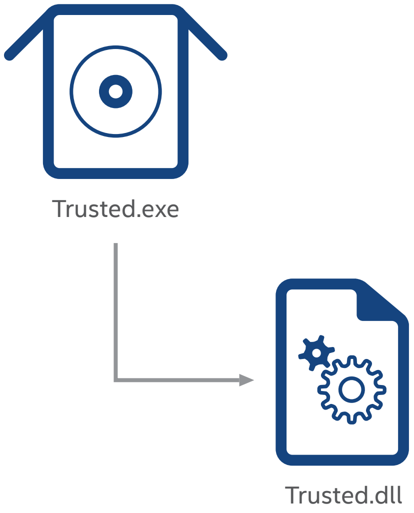


McAfee Mobile Detections of "FlasherPlayer11" malware (Android/Fladstep.B).

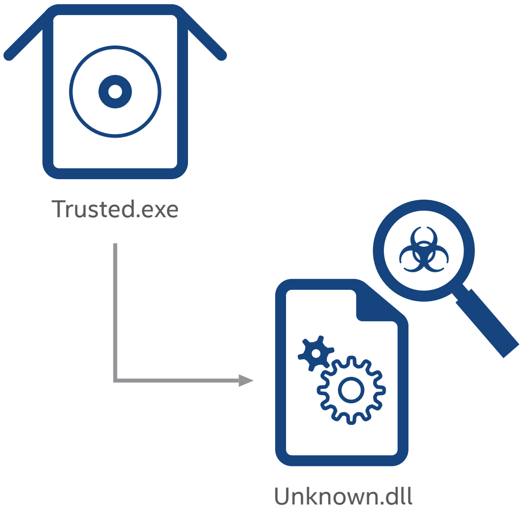
Attackers abuse product or operating system trust through DLL side loading, a common technique used to insert malicious code.

Product and operating system trust

Today's security products are often rooted in trust. To increase performance and decrease false positives, a system inventory determines innocent applications, whose behavior goes unscrutinized. Attackers know that if their malicious code can ride the coattails of a trusted application, then it has a greater chance of success. Malware has taken advantage of this factor for a number of years, using an approach known as DLL side loading. This technique involves executing a legitimate application that executes code from an external library. The attackers craft their payload to assume the role of the intended DLL, thus causing the clean application to execute malicious code.



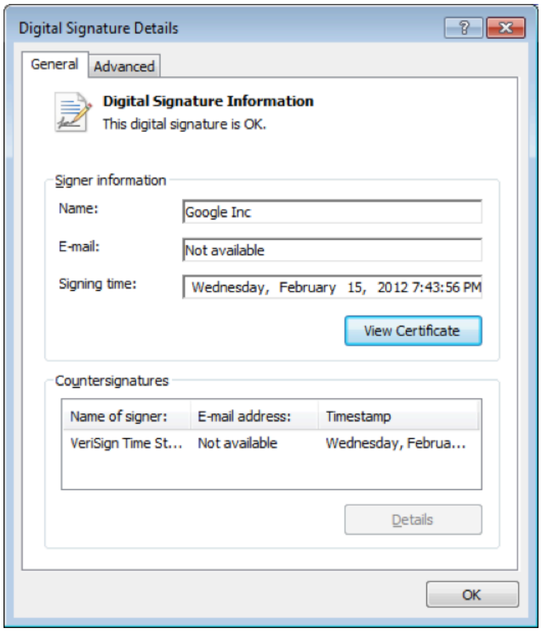
Typical scenario: trusted executable loads trusted library.



Malicious scenario: trusted executable loads unknown malware library.

Share this Report

During the third quarter, McAfee Labs observed DLL side loading attacks abusing a relatively new target—a signed Google Updater application. New PlugX malware variants assume the role of the imported goopdate.dll, but PlugX goes a step further to conceal its actions. The goopdate.dll module is nothing more than a middle man that reads the content of an encrypted data file, goopdate.dll.map, decrypts it into memory, and passes execution control to that code. This approach provides the advantage of masking the functionality of the intermediate DLL file. Each of the three components involved in the attack are benign on their own, and analyzing the files separately could easily lead to the wrong conclusion. But combined, the malicious intent is quite apparent. Products that trust files signed by a legitimate Google Inc. certificate are being abused by attackers using this technique.



Digital Signature Details

Digital Signature Information

This digital signature is OK.

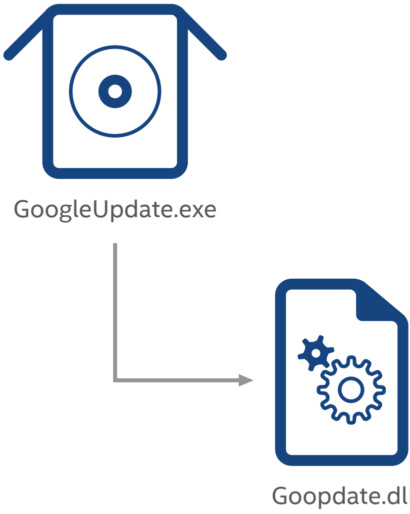
Signer information

Name:	Google Inc
E-mail:	Not available
Signing time:	Wednesday, February 15, 2012 7:43:56 PM

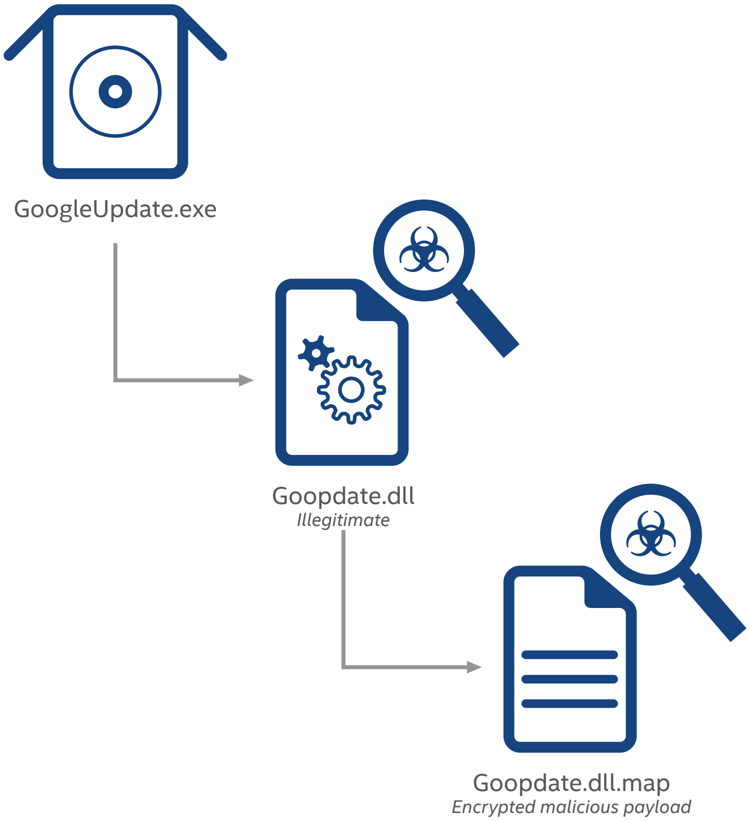
Countersignatures

Name of signer:	E-mail address:	Timestamp
VeriSign Time St...	Not available	Wednesday, Februa...

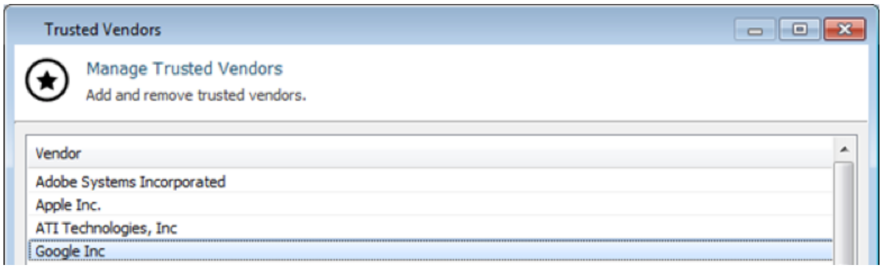
Legitimate signed Google updater application.



Legitimate Google updater loads Google library.



Legitimate Google executable loads malicious module, which loads payload. Google updater loads Google library.

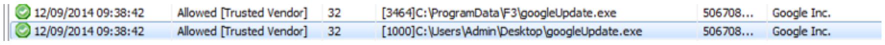


Trusted Vendors

Manage Trusted Vendors
Add and remove trusted vendors.

Vendor
Adobe Systems Incorporated
Apple Inc.
ATI Technologies, Inc
Google Inc

This whitelisting application implicitly trusts valid Google applications by default.



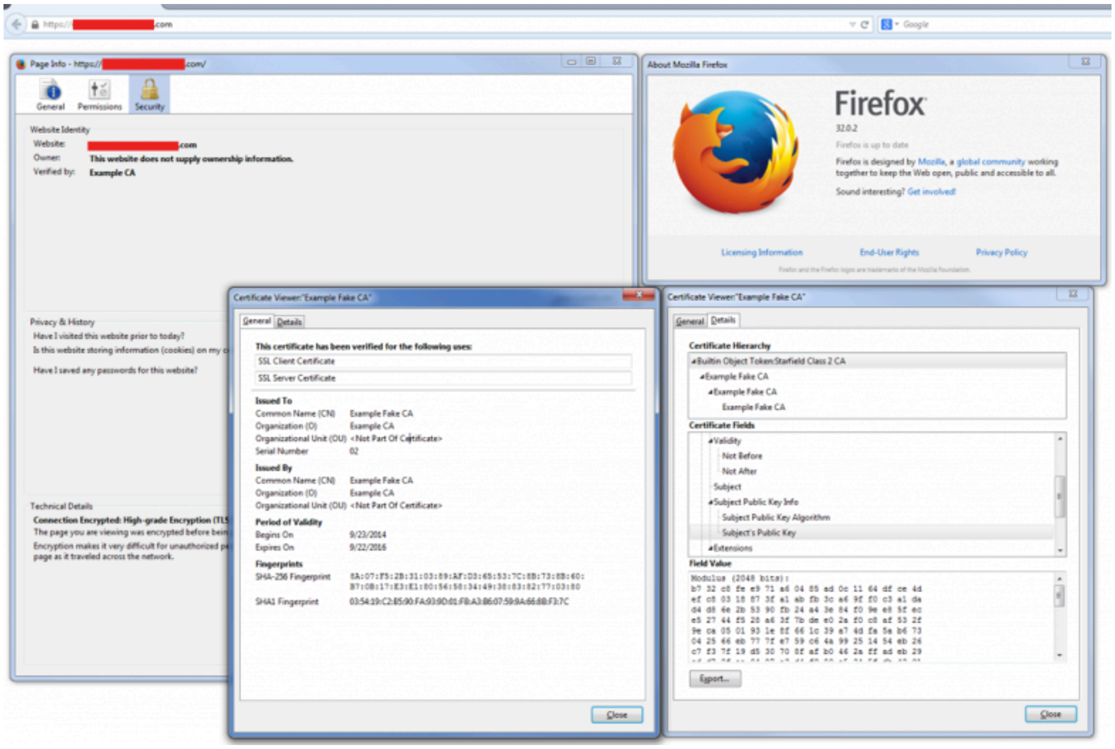
```
12/09/2014 09:38:42   Allowed [Trusted Vendor]   32   [3464]C:\ProgramData\F3\googleUpdate.exe        506708...   Google Inc.
12/09/2014 09:38:42   Allowed [Trusted Vendor]   32   [1000]C:\Users\Admin\Desktop\googleUpdate.exe   506708...   Google Inc.
```

[Trusted Vendor] application allowed by default.

We have seen a more significant advancement in product trust abuse in a recent **Angler exploit kit variant**. This attack allows for the direct execution of a payload without its first being written to disk, which removes the opportunity for whitelisting applications to allow or to deny the newly delivered, and subsequently executed, code. This step also bypasses file antivirus checks because there is no file to scan at this point of the attack.

Another form of trust abuse involves the interaction between the operating system and network routing controls. Applications rely on the operating system to provide a safe and trusted means of communication. As an example, applications assume that their traffic will be routed safely and correctly to the intended recipient. One very well-known family of malware is DNS changers. The sole purpose of this malware is to alter the DNS configuration of the operating system, forcing all DNS queries to a DNS server controlled by attackers. Although the browser acts as if it is talking with a trusted bank website, it is actually exchanging data with a fake site or a malicious transparent proxy that is capturing user data.

Determining whether a user is interacting with a fake site is not as easy as one would think. The "BERserk" ASN.1 vulnerability **reported by Intel on September 24** and discussed in this report's Key Topic **"Going BERserk: trusted connectivity takes a big hit"** is an excellent illustration of how browsers can be subverted to believe that they are communicating with trusted sites. This vulnerability allows attackers to forge RSA signatures, thereby bypassing authentication to websites using SSL/TLS. Given that certificates can be forged for any domain, this issue raises serious concerns around integrity and confidentiality as we visit what we perceive to be secure websites.



https://[redacted].com

Page Info - https://[redacted].com/

Website Identity
Website: [redacted].com
Owner: **This website does not supply ownership information.**
Verified by: **Example CA**

Privacy & History
Have I visited this website prior to today?
Is this website storing information (cookies) on my c
Have I saved any passwords for this website?

Technical Details
Connection Encrypted: High-grade Encryption (TLS
The page you are viewing was encrypted before bein
Encryption makes it very difficult for unauthorized pe
page as it traveled across the network.

About Mozilla Firefox

Firefox
32.0.2
Firefox is up to date
Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.
Sound interesting? Get involved!

Certificate Viewer:"Example Fake CA"

This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate

Issued To
Common Name (CN) Example Fake CA
Organization (O) Example CA
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 02

Issued By
Common Name (CN) Example Fake CA
Organization (O) Example CA
Organizational Unit (OU) <Not Part Of Certificate>

Period of Validity
Begins On 9/23/2014
Expires On 9/22/2016

Fingerprints
SHA-256 Fingerprint 8A:07:F5:2B:31:03:89:AF:D3:45:53:7C:8B:73:8B:60:
B7:0B:17:E3:E1:80:56:58:34:49:38:83:82:77:03:80
SHA1 Fingerprint 03:54:19:C2:85:90:FA:93:9D:01:FB:A3:B6:07:59:9A:66:8B:F3:7C

Certificate Viewer:"Example Fake CA"

Certificate Hierarchy
Builtin Object Token:Starfield Class 2 CA
Example Fake CA
Example Fake CA
Example Fake CA

Certificate Fields
Validity
Not Before
Not After
Subject
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions

Field Value

```
Modulus (2048 bits):
b7 32 c8 fe e9 71 a6 04 85 ad 0c 11 64 df ce 4d
ef c8 03 18 87 3f a1 ab fb 3c a6 9f f0 c3 a1 da
d4 d8 6e 2b 53 90 fb 24 a4 3e 84 f0 9e e8 5f ec
e5 27 44 f5 28 a6 3f 7b de e0 2a f0 c8 af 53 2f
9e ca 05 01 93 1e 8f 66 1c 39 a7 4d fa 5a b6 73
04 25 66 eb 77 7f e7 59 c6 4a 99 25 14 54 eb 26
c7 f3 7f 19 d5 30 70 8f af b0 46 2a ff ad eb 29
```

The "BERserk" ASN.1 exploit.

Share this Report

Learn how McAfee can help protect against this threat.

Name-resolution abuses also compromise operating systems. By pointing the system to a malicious upgrade server and using a trusted certificate outside of its intended scope, attackers have been able to deploy malware. One famous example is the **Flame espionage malware**, discovered in 2012. Flame contained code to infect targeted computers by hijacking Microsoft's Windows update mechanism for distributing security patches.

Similar attacks can compromise network elements such as consumer routers, allowing attackers to capture traffic from desktops and laptops as well as TV, console, and other connected devices. In August, such an attack occurred when users of Synology network attached storage reported infections of SynoLocker, a ransomware Trojan holding their data hostage.

Trust is an opportunity for attackers, and abuse is rampant. Users need to keep a watchful eye out. Security products need to allow customers to define what should and should not be trusted, and provide flexible controls that give trusted actors greater permissions while limiting those of others. Failure to address this challenge could result in an increasing distrust of many technologies used to access the Internet, and perhaps even to overall reduced usage of the Web.

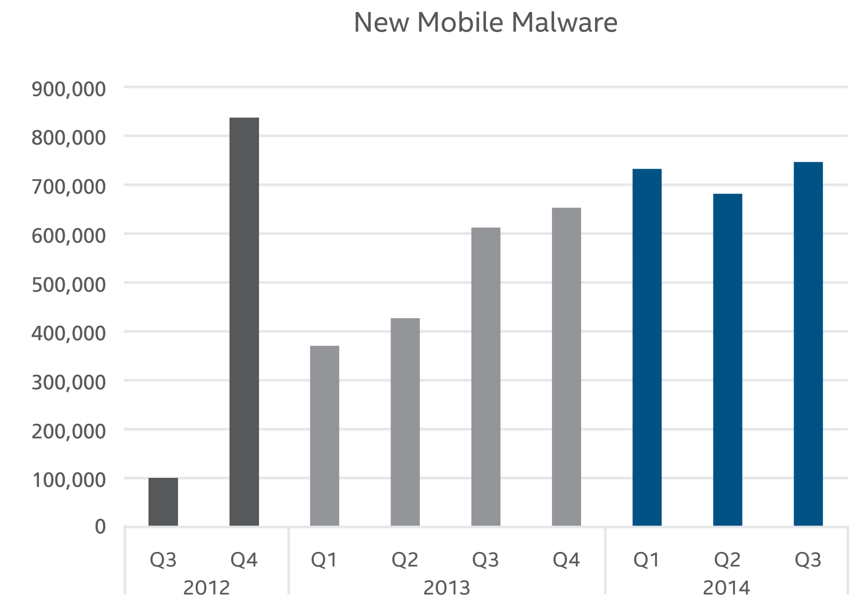
Protecting Against Trust Abuse

Abuse	Countermeasure
Inherited trust (malvertising), Product and operating system trust	Keep operating systems, applications, and security software up to date.
Malicious exploits (drive-by downloads)	Keep systems up to date. Visit reputable websites. Mouse over hyperlinks to preview destinations. Don't follow suspicious links arriving in email or through social networks.
Brand abuse (forged email, copycat apps, fake domains)	Suspect and verify, manually enter web addresses, search for apps on trusted sites, choose those that have an established reputation (many downloads, good reviews), and inspect app permission requests.
Device abuse	Keep devices up to date with the latest firmware.

Threats Statistics

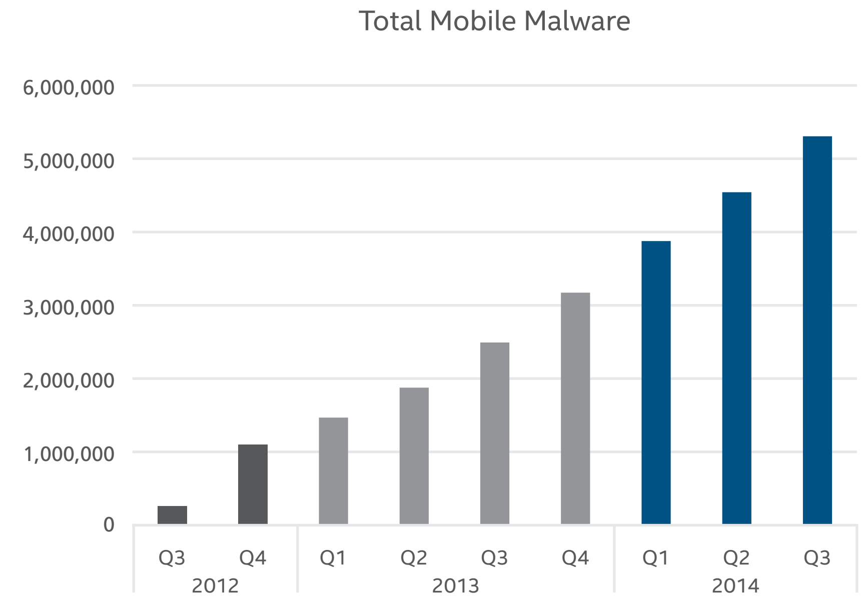
Share feedback

Mobile malware



Source: McAfee Labs.

The total number of mobile malware samples exceeded 5 million in Q3 2014, growing by 16% in this quarter and 112% in the past year.



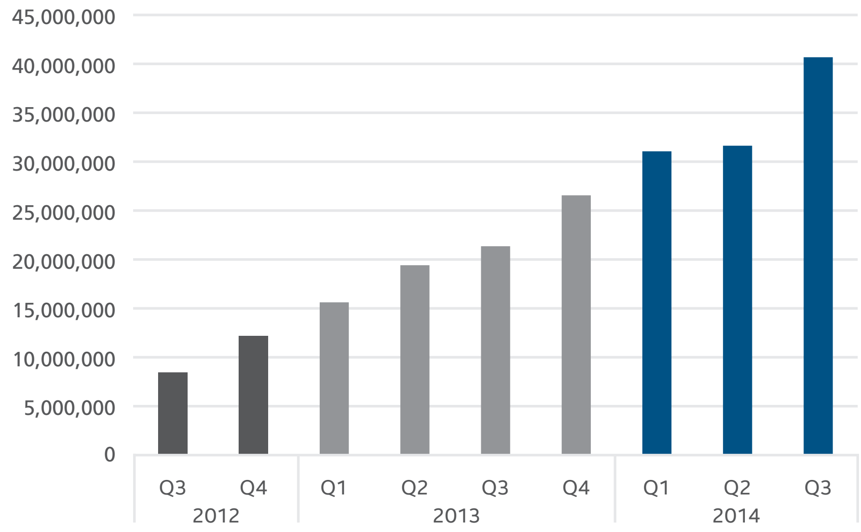
Source: McAfee Labs.

Share this Report

Malware

There are over 307 new threats every minutes, or more than 5 every second.

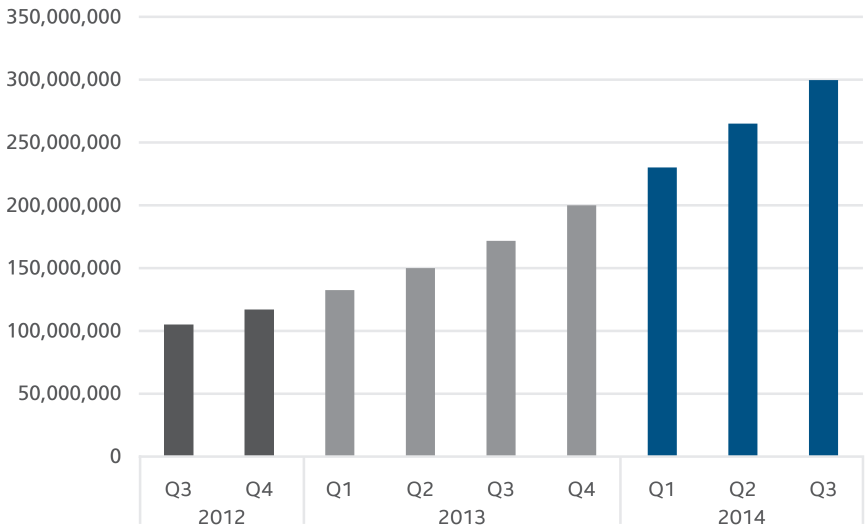
New Malware



Source: McAfee Labs.

The McAfee Labs malware zoo broke the 300 million–sample barrier in Q3 2014, growing by 76% over the past year.

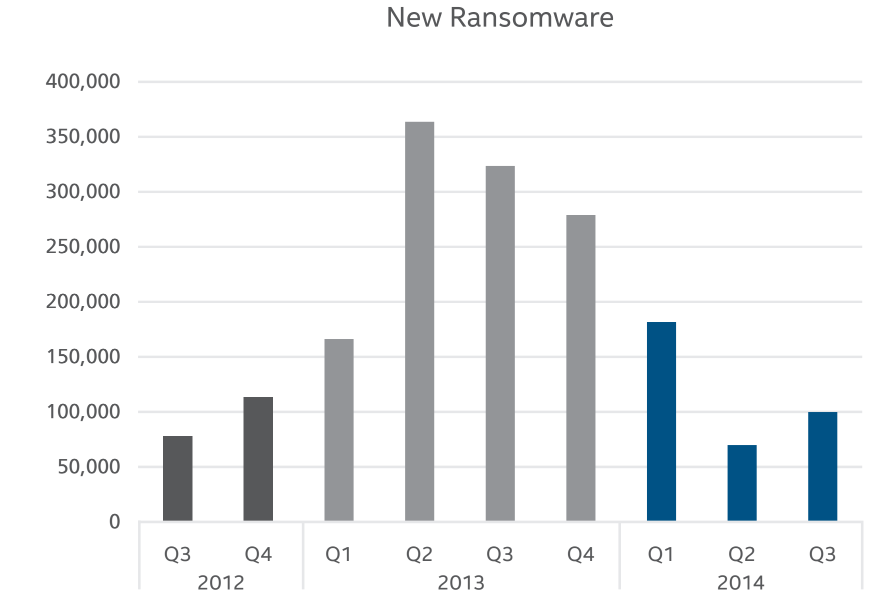
Total Malware



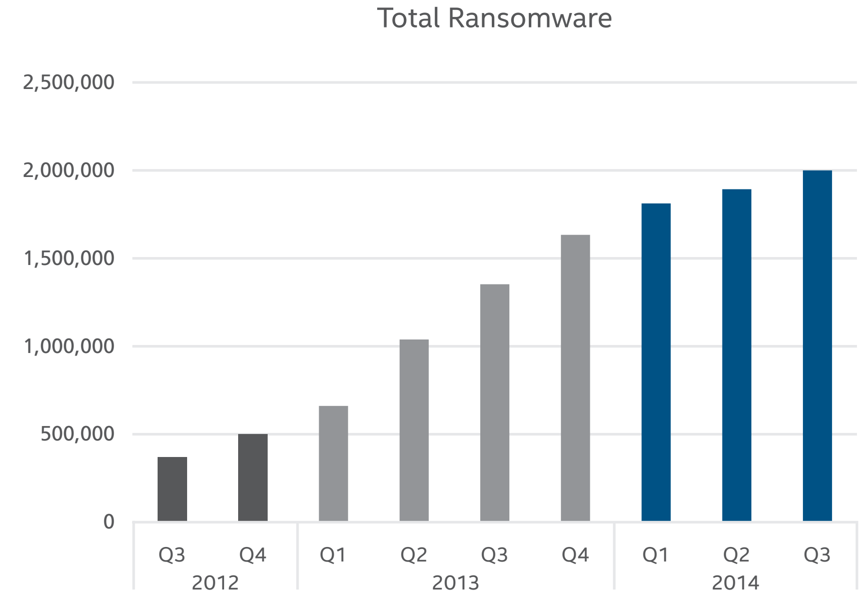
Source: McAfee Labs.

Share this Report

After four quarters, the number of new ransomware samples has stopped dropping. We're perplexed by the drop but not surprised that the number is now growing again.



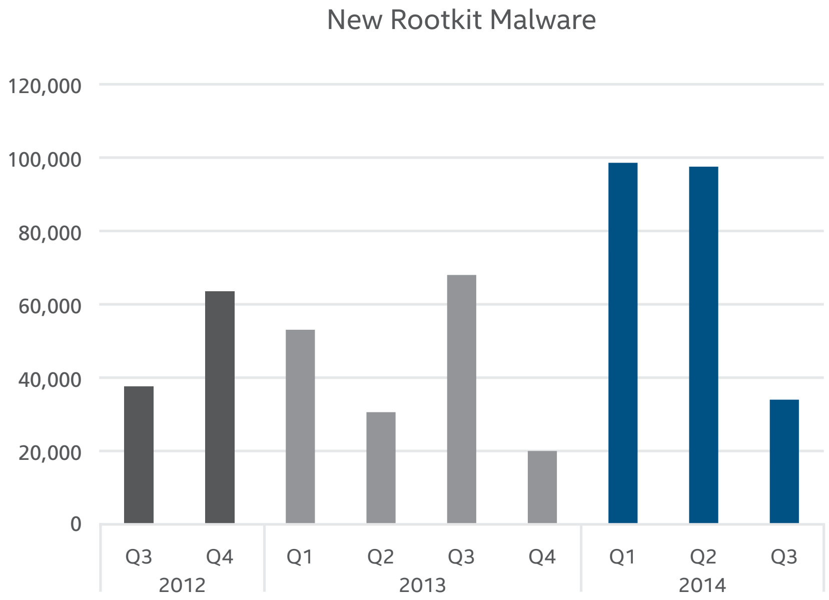
Source: McAfee Labs.



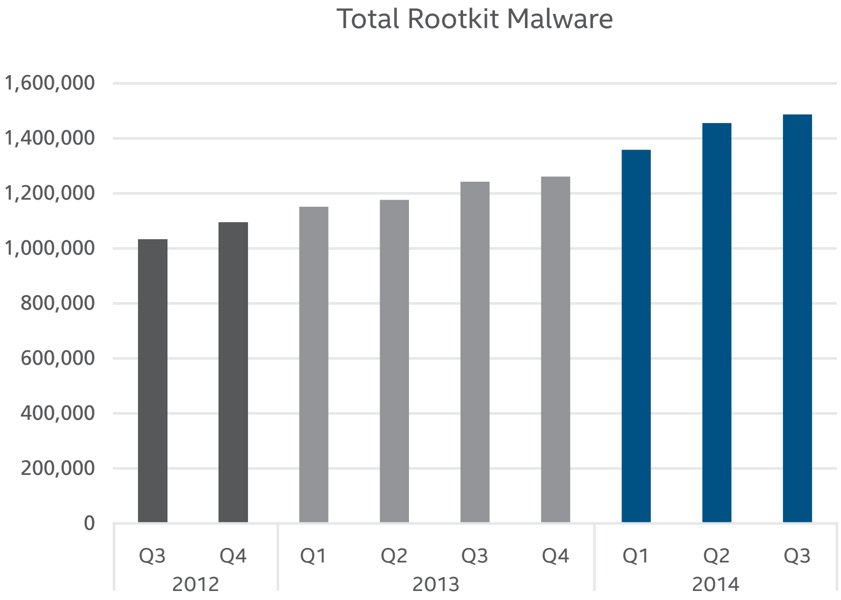
Source: McAfee Labs.

Share this Report

New rootkits dropped by 65% in Q3, reflecting this form of malware's volatility.



Source: McAfee Labs.



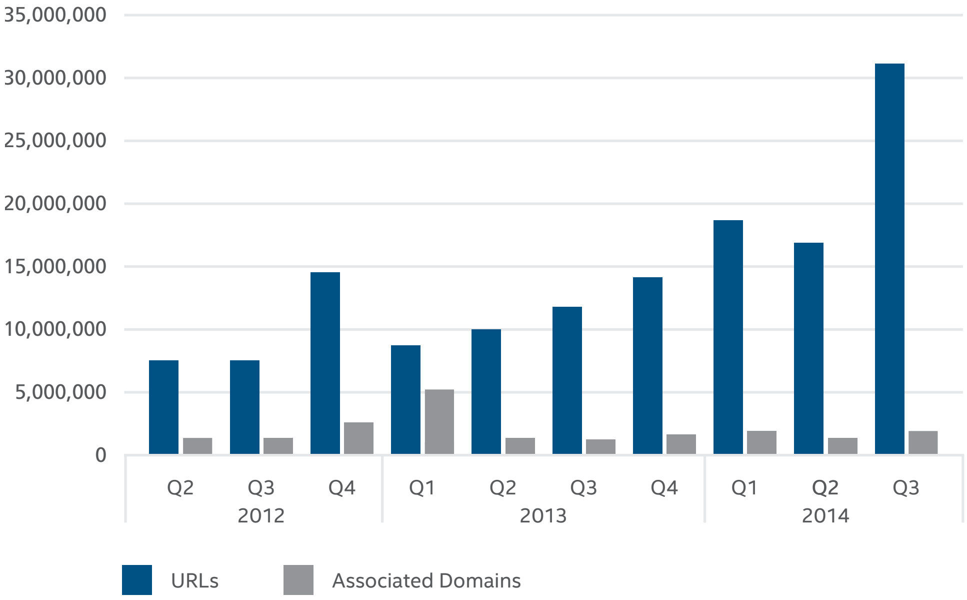
Source: McAfee Labs.

Share this Report

Web threats

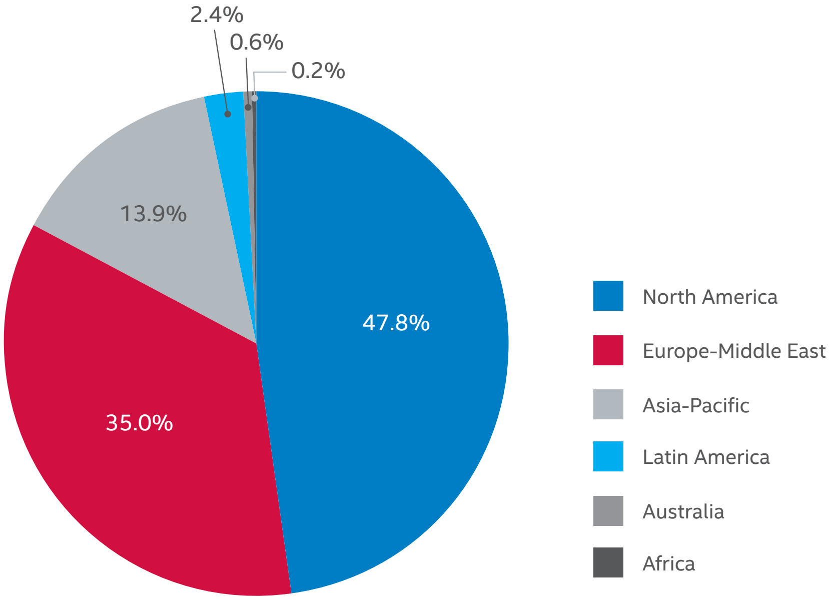
The number of new suspect URLs skyrocketed this quarter. Some of that growth can be attributed to a doubling in the number of new short URLs, which often hide malicious websites, and a sharp increase in phishing URLs.

New Suspect URLs



Source: McAfee Labs.

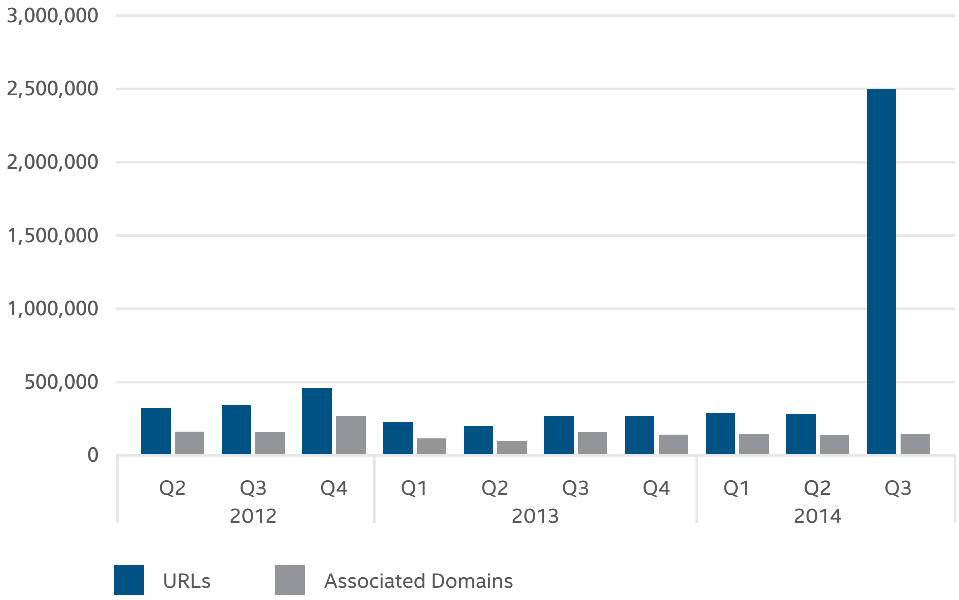
Location of Servers Hosting Suspect Content



Source: McAfee Labs.

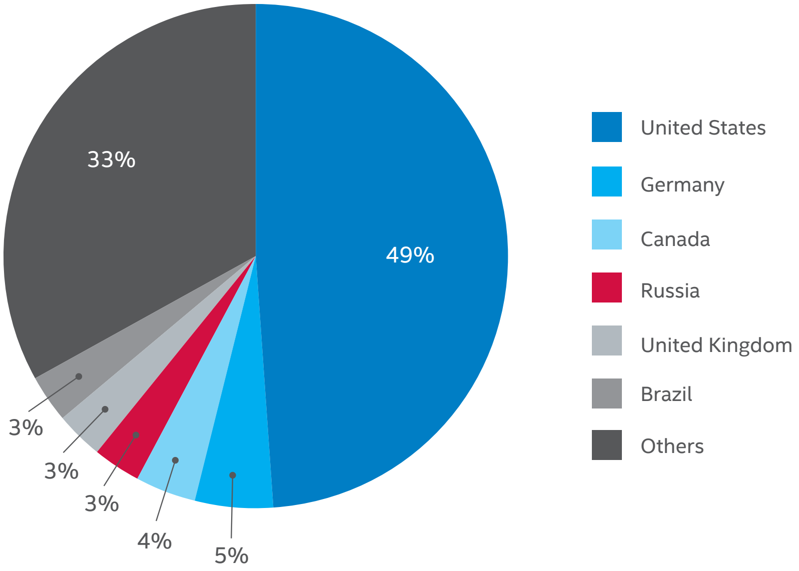
We primarily attribute the immense leap this quarter to a Russian pill-spam phishing campaign that creates a separate subdomain for every recipient. Our data gathering counts every one of those subdomains.

New Phishing URLs



Source: McAfee Labs.

Top Countries Hosting Phishing Domains

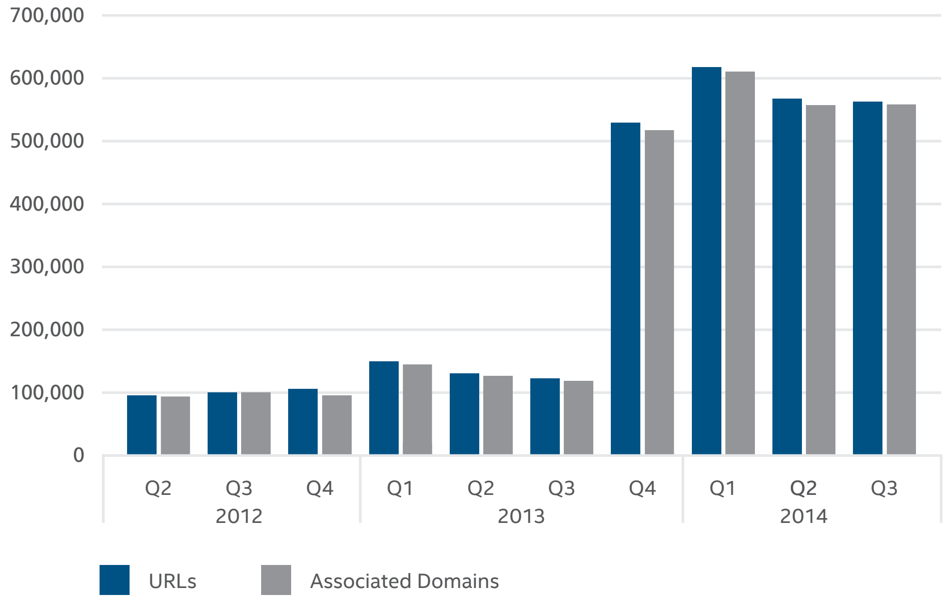


Source: McAfee Labs.

Share this Report

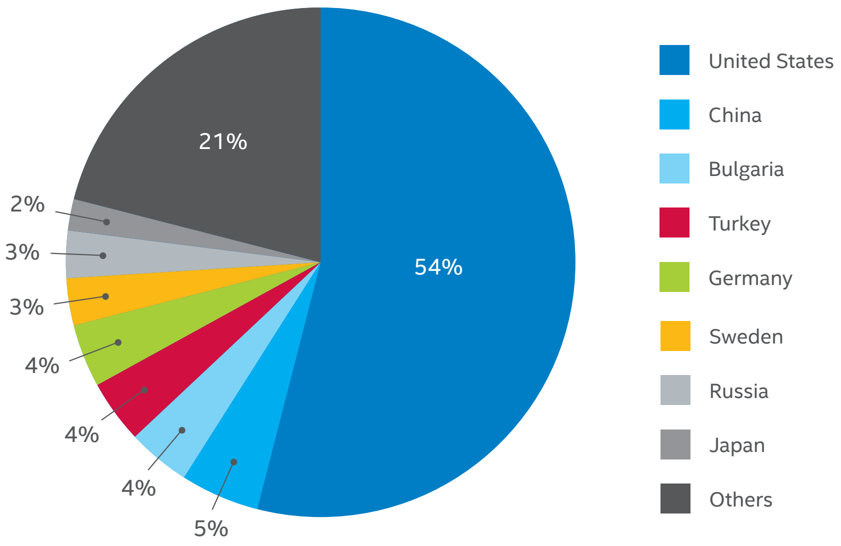
Starting this quarter we offer a count of new spam URLs around the world. The number of new URLs in Q3 declined slightly compared with Q2. The big jump occurred in Q4 last year, as we improved our data harvester.

New Spam URLs



Source: McAfee Labs.

Top Countries Hosting Spam Domains



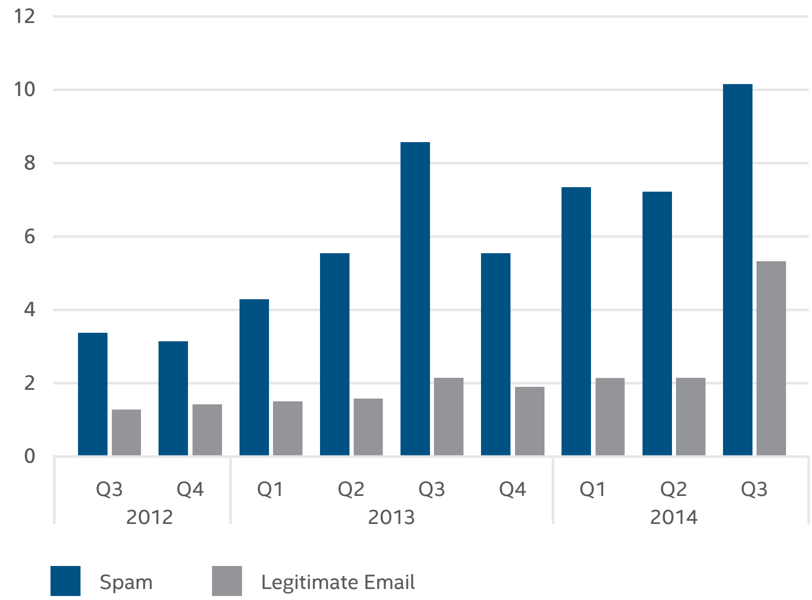
Source: McAfee Labs.

Share this Report

Messaging and network threats

The 148% increase this quarter in legitimate email is due to improvements in how we gather data. The figure is not directly comparable to past quarters, but in the future we'll have a more accurate historical measure of mail volume. Meanwhile, spam volume has increased by 40%. We attribute that in part to how we gather data but also to a growing customer base, the increase in botnet activity, and more snowshoe spam.

Global Spam and Email Volume
(trillions of messages)

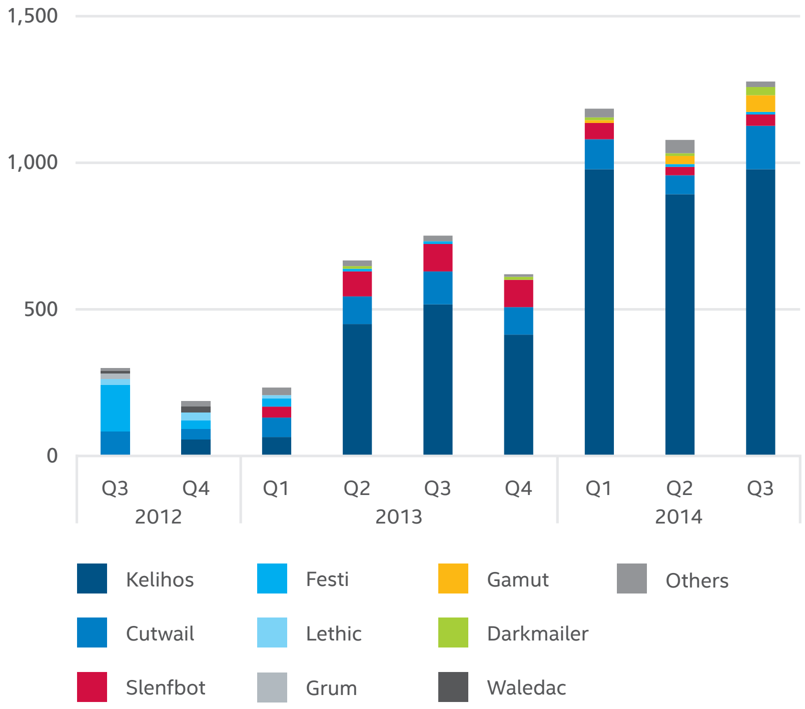


Source: McAfee Labs.

Starting this quarter we offer a new breakdown of the Top 20 spamming botnets. Kelihos has been the most prolific botnet this year. In Q3, Kelihos emails made up 76% of spam generated by the Top 20. Most recently, Kelihos has been associated with business-improvement spam, ("8 Simple Rules express the essence of B2B sales"), pill spam ("Buy Cheap Meds. Save up to 70%"), and get-rich-quick spam ("$376 in JUST A DAY? Really? Here's proof"). Kelihos is widely distributed, with spam-sending IPs originating from 226 countries this year.

Spam Emails From Top 20 Botnets

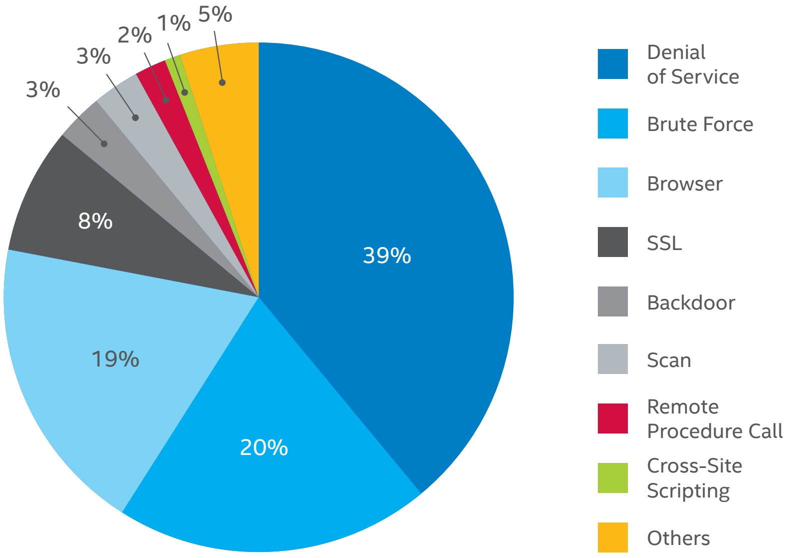
(millions of messages)



Source: McAfee Labs.

The top three threat types this quarter account for 78% of all threats. SSL attacks jumped to 8% in Q3, up 5% from Q2. This increase is likely related to the on-going massive outbreak of Heartbleed.

Top Network Attacks



Source: McAfee Labs.

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

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.