Google Report

Android Security 2014 Year in Review

Table of Contents

Overview

New Android Security Features / Capabilities

Response to vulnerabilities found in 2014
- SSL Vulnerabilities
- Android (and Linux kernel) vulnerabilities
- OEM / SOC specific vulnerabilities
- Application Vulnerabilities

Measures of Ecosystem Security
- Scope of User Protection and Ecosystem Measurement
- Classification of Potentially Harmful Applications
- Occurrence of Potentially Harmful Applications
- New and Noteworthy PHAs
  - Spyware
  - Ransomware
  - WAP and SMS Fraud
- Safety Net Statistics
  - Platform API Abuse
    - SMS Confirmation
    - Other APIs of Interest
    - Security Model Integrity
  - Network Level Abuse
    - SSLv3 downgrade
    - CCS Injection
    - CA Man In The Middle
- Safe Browsing Statistics

Overview

Google is committed to ensuring that Android is a safe ecosystem for users and developers.

We do that by investing in security technology within the core Android platform, developer support, and in the applications and services Google provides for Android. We want to share information about what we are doing and how the ecosystem is responding, so this is the first of what we expect will be many reports that will provide in-depth insight into the security of the Android ecosystem.

In 2014, the Android platform made numerous significant improvements in platform security technology, including enabling deployment of full disk encryption, expanding the use of hardware-protected cryptography, and improving the Android application sandbox with an SELinux-based Mandatory Access Control system (MAC). Developers were also provided with improved tools to detect and react to security vulnerabilities, including the nogotofail project and the SecurityProvider. We provided device manufacturers with ongoing support for fixing security vulnerabilities in devices, including development of 79 security patches, and improved the ability to respond to potential vulnerabilities in key areas, such as the updateable WebView in Android 5.0.

Google's security services for Android increased protection for users and improved visibility into attempts to exploit Android. Ongoing monitoring by Verify Apps found that efforts to deliver Potentially Harmful Applications (PHAs) continued at low levels throughout 2014, less than 1% of all devices had a PHA installed. Fewer than 0.15% of devices that download only from Google Play had a PHA installed. Expanded protection in Verify Apps and Safebrowsing also now provides insight into platform, network, and browser vulnerabilities affecting Android devices. Exploitation attempts were tracked for multiple vulnerabilities, and the data does not show any evidence of widespread exploitation of Android devices.

Google's security services for Android increased protection for users and improved visibility into attempts to exploit Android.

1. The security industry often uses the term "malware" with little or no definition. To avoid potential confusion, the Android security team instead uses the term Potentially Harmful Application (PHA) to refer to applications which pose a security risk to users or their data. More detail on the types of PHAs that have been observed is included in the section titled "Classification of Potentially Harmful Applications".

New Android Security Features / Capabilities

There were two major updates to Android in the 12 months ending Nov 1, 2014[2]: Android 4.4 and the preview of Android 5.0. Both of these platform releases included security improvements as well as patches for newly discovered vulnerabilities. By February 2, 2015, Android 4.4 has become the most widely distributed version of Android with over 41% of Android devices that check in to Google services running Android 4.4 or greater[3]. Here are a few of the security highlights from those releases:

Android sandbox reinforced with SELinux.

Android 4.4 required that SELinux be in enforcing mode for select system domains, and Android 5.0 now requires SELinux in enforcing mode for all domains. SELinux is a mandatory access control (MAC) system in the Linux kernel used to augment the existing discretionary access control (DAC) security model. This new layer provides additional protection against potential security vulnerabilities by reducing exposure of system functionality to applications.

Improved Full Disk Encryption.

Full Device Encryption was introduced with Android 3.0, using the Android screen lock secret to wrap a device encryption key that is not sent off the device or exposed to any application. Starting with Android 5.0, the user password is protected against brute-force attacks using scrypt and, where available, the key is bound to the hardware keystore to prevent off-device password brute-forcing attacks. On devices that ship with Android 5.0 out-of-the-box, full disk encryption can be enabled by default to improve protection of data on lost or stolen devices.

Multi user, restricted profile, and guest modes for phones & tablets.

Android 4.2 introduced multiple users on tablet devices. Android 5.0 provides for multiple users on phones and includes a guest mode that can be used to provide easy temporary access to your device without granting access to your data and apps.

Improved authentication for phones and tablets.

Android 5.0 introduced Smart Lock trustlets that provide more flexibility for unlocking devices. For example, trustlets can allow devices to be unlocked automatically when close to another trusted device (via NFC, Bluetooth) or being used by someone with a trusted face.

[2] Unless otherwise specified, data within this paper is from the 12 month period between Nov 1, 2013 and Nov 1, 2014. For the rest of this paper we'll used simplified phrase "in 2014" to describe that time period, even though it means some of the data came from the last 2 months of 2013. Where a more precise time period is noteworthy, it will be explicitly described.

[3] https://developer.android.com/about/dashboards/index.html: provides the current data

Enhanced Google security services for Android

Google also enhanced the security of the Android ecosystem by expanding the set of security services that are included in the Google applications that run on the Android Platform. Enhanced Google security services for Android. Google Play provides security scanning of all applications prior to availability for download and continues to provide ongoing security checks for as long as the application is available in Google Play. Since 2012, Google Play has also offered a service called Verify Apps that provides protection from apps outside of Google Play. This check for potentially harmful behavior at the time of application install was initially available for Android 4.2 and later, and was expanded in 2013 to protect all devices with Android 2.3 and greater. In April, we announced that Verify Apps was providing enhanced protections with ongoing security scans for applications and other threats. There are currently two types of security services provided by Google Play for all Android users:

Protection within Google Play:

Review of all applications in Google Play for potentially harmful behavior and ongoing protection for apps downloaded from Google Play. Review is described in more detail on page 15 of this report.

Verify Apps Protection with Safety Net outside of Google Play:

Protection for all apps regardless of source of install. This includes a technology code-named “Safety Net” that detects and protects against non app-based security threats such as network attacks. Users who use Verify Apps may also upload applications to Google to improve detection of Potentially Harmful Applications from sources outside of Google Play.

There are over 1 billion devices protected by Google Play.

Improve ability to enhance security without full system OTAs.

In May, Google Play Services introduced an updateable Security Provider that allows application developers to use a version of SSL provided and maintained by Google Play Services. Applications that use this Security Provider will have updated cryptography without any need for a system OTA. With Android 5.0, WebView can now be updated by Google independent of the Android framework and without a system OTA.

Developer Security Warnings.

In July 2014, Google Play began to use automated systems to find potential vulnerabilities in applications published in Google Play. Google Play can now provide developers with proactive warnings within the Developer Console and via email about security issues affecting their apps. These include warnings about potentially dangerous storage of credentials, use of out-of-date open source libraries, and other best practices. These warnings help improve the overall state of software security in the mobile ecosystem. To date, over 25,000 applications have been updated and no longer contain the potential security issue.

Response to Vulnerabilities Found in 2014

In 2014, the Android Security Team rated severity of all vulnerabilities using a 4-tier rating system that combines potential for privilege escalation and risk of exploitation, as follows:

Severity	Representative issues with this level of severity
Critical	Active exploitation gaining remote execution with Android permissions of Protection Level Dangerous or System through normal use of device.
High	Remote execution with ability to run with Android permissions of Protection Level Dangerous. Local privilege escalation to root or system by nonprivileged programs. (potential rooting PHA) Remote access to data protected with Android permissions of Protection Level Dangerous. Moderate or higher severity issue with significant press coverage. (User fear is a real harm.)
Moderate	Local privilege escalation to Android permissions of Protection Level Dangerous. Local access to sensitive data without appropriate privilege. Shell user (ADB) escalation to root (potential unauthorized user device rooting). Denial of Service that renders a device unusable. High severity issue, mitigated by device specificity, or user interaction. Remote execution with ability to run with Android permissions of Protection Level Normal.
Low	Unauthorized local access to data that is not considered sensitive. Denial of Service that can be stopped by normal user action such as system restart or application removal. Other, limited violation of the Android security model.

In 2014, the Android security team provided patches for 41 Moderate, 30 High, and 8 Low Severity vulnerabilities. There were no critical vulnerabilities found in 2014. To provide OEMs with opportunity to patch prior to disclosure, patches are provided to partners but not publicly disclosed until the next API update to AOSP. At that time, patches are released to open source.

Currently, 73 of the issues patched in 2014 have been released to AOSP, and 6 will be released with the next update to AOSP.

In addition to providing fixes in the platform level, the Android Security Team monitors vulnerabilities for attempted abuse using Verify Apps, Safety Net, and other systems. Significant exploitation has only been seen for one vulnerability identified in 2014, CVE-2014-3153: Local privilege escalation in futex syscall. An exploit of this vulnerability was included in a number of rooting tools. We also continued to monitor levels of exploitation of over 25 other publicly known local privilege escalation vulnerabilities. Many of these vulnerabilities had patches available prior to 2014, but there are devices that have not been patched for all publicly known vulnerabilities.

In addition to providing fixes in the platform level, the Android Security Team monitors vulnerabilities for attempted abuse using Verify Apps, Safety Net, and other systems.

Rooting tools are prohibited within Google Play. Verify Apps has seen Rooting applications installed on approximately 0.25% of devices, with those installs from sources outside of Google Play. With respect to "malicious" applications, less than 1 out of every million installs of an application observed by Verify Apps abused a platform vulnerability in a manner that we think it would be appropriate to characterize as "malicious[4]".

We introduced an acknowledgement page for third parties that responsibly disclose security issues or otherwise contribute to Android security. The Android Security Team would again like to publicly acknowledge the contributions that more than 40 security researchers and developers have made to improve Android Security. Thank you.

[4] Although widespread, the use of the phrase "malicious" to describe application behavior is problematic. Although Rooting applications, for example, do reduce the security of a device and may cause irreparable harm to a device we do not believe they should be considered malicious as long as the behavior is adequately disclosed to the user. This is clearly distinct from an application which attempts to use a vulnerability to gain privileges without the users' awareness. Google does classify Rooting applications as "Potentially Harmful Applications" so they are prohibited in Google Play and users of Verify Apps will receive a warning prior to installation of such an application. We separately classify applications that exercise a vulnerability and appear to be attempting to mislead or harm the user intentionally as "Rooting - Malicious" -- such applications are both prohibited from Google Play and blocked by Verify Apps.

SSL Vulnerabilities

In 2014, there were a number of high-profile vulnerabilities affecting implementations of SSL. The most significant vulnerability affecting most platforms, Heartbleed, had limited impact on Android as it affected only Android 4.1.1 devices. We have expanded monitoring capability in Safety Net to look for SSLv3 and other ciphersuite downgrade attacks. We have seen limited exploitation that appears to be research related[4]. To date, we have not seen evidence of widespread exploitation of these vulnerabilities affecting Android. More details on data related to network based exploits is included in the Safety Net Data section.

The most significant vulnerability affecting most platforms, Heartbleed, had limited impact on Android as it affected only Android 4.1.1 devices.

Android Vulnerabilities

A vulnerability affecting Android 4.4 and earlier received broad attention following disclosure at Black Hat. This vulnerability was named FakeID and was formally identified as Android-13678484. In addition to providing a patch for this issue, Google has monitored potential exploitation via Verify Apps and Google Play. In 2014, we blocked one instance of an app uploaded to Google Play that exploited this vulnerability. Outside of Google Play, Verify Apps also warns users about applications that exercise this vulnerability. Verify Apps identified 258 unique applications that exercise this vulnerability, and they were installed less than once for every 1 million installs checked by Verify Apps.

Many of the FakeID installs have characteristics that associate them with security research, and we have not identified any attempted exploitation that we would consider “malicious”[5].

OEM/ SOC Specific Vulnerabilites

Android devices are generally implemented by an Original Equipment Manufacture (OEM) in partnership with a System On a Chip (SOC) to implement a kernel and device drivers that enable the Android Platform. Although not strictly part of the open-source Android Platform, these components are critical to the security of specific Android devices.

[5] A note on observation of exploitation: As with any data collected in large volume from in-the-field observation, there is non-zero chance of both false positives and false negatives. We are presenting the data to the best of our understanding. Due to the methods that we use to collect exploitation data, it is not possible to have certainty that a lack of observation means no exploitation has occurred. Conversely, it is also possible that some of the data that suggests possible exploitation is in fact innocuous. While we extensively test our detection mechanisms to ensure accuracy, privacy controls prevent detailed investigation into specific instances of exploitation observed in aggregated data.

There have been multiple OEM- or SOC-specific kernel vulnerabilities in 2014. We review these vulnerabilities to identify potential platform level hardening that can reduce potential exposure.The inclusion of SELinux in full enforcing mode on Android 5.0, for example, is expected to reduce the chance of exploitation of these vulnerabilities. Similar research into methods to reduce the possibility of vulnerabilities in OEM/SOC specific code is being conducted by major OEMs and SOC vendors.

The inclusion of SELinux in full enforcing mode on Android 5.0, for example, is expected to reduce the chance of exploitation of these vulnerabilities.

Additionally, we also monitor these vulnerabilities for attempted abuse using Google Play, Verify Apps, Safety Net, and other systems. A number of exploits for these vulnerabilities were incorporated into rooting tools that collect multiple device-specific vulnerabilities into a single tool.

We observed use of exploits for SOC/OEM-specific vulnerabilities in a manner that we would think it would be appropriate to characterize as "malicious" in fewer than 1 out of every million installs in 2014.

Application Vulnerabilites

In 2014, the Android Security Team provided updated security tips for developers and issued new guidance on best practices for secure use of SSL in Android applications. We also launched a developer notification service in Google Play and thousands of developers have been notified of potential vulnerabilities affecting their applications. If you are a security researcher who needs assistance in contacting a large number of developers about a potential security vulnerability in their application(s), please contact the Android security team at security@android.com.

In addition to providing developers with assistance in updating their applications, in some instances Google Play and Verify Apps are able to monitor and/or block potential exploitation of application vulnerabilities.

For example, Google Play policy prohibits applications that attempt to send data from the SDCard or External Storage off the device without user consent, which provides limited protection for application data that may be inadvertently stored in that world-readable location.

In 2014, we observed applications attempting to take messages that were stored on the SDCard by a popular messaging platform. Those applications are categorized as Potentially Harmful Applications. They are prohibited in Google Play and Verify Apps and Safebrowsing warns users about them outside of Google Play. We also worked with the messaging platform developer to change the format of their data to reduce risk to users. That was the only example we observed of local exploitation of an application level vulnerability in 2014.

Measures of Ecosystem Security

There are over one billion devices that are protected by Google's security services for Android. Through aggregated security data sent from these devices, we can gain a broad understanding of the security environment for mobile devices. This includes information about Potentially Harmful Applications as well as attempted abuse of sensitive APIs and vulnerabilities at the device and network level.

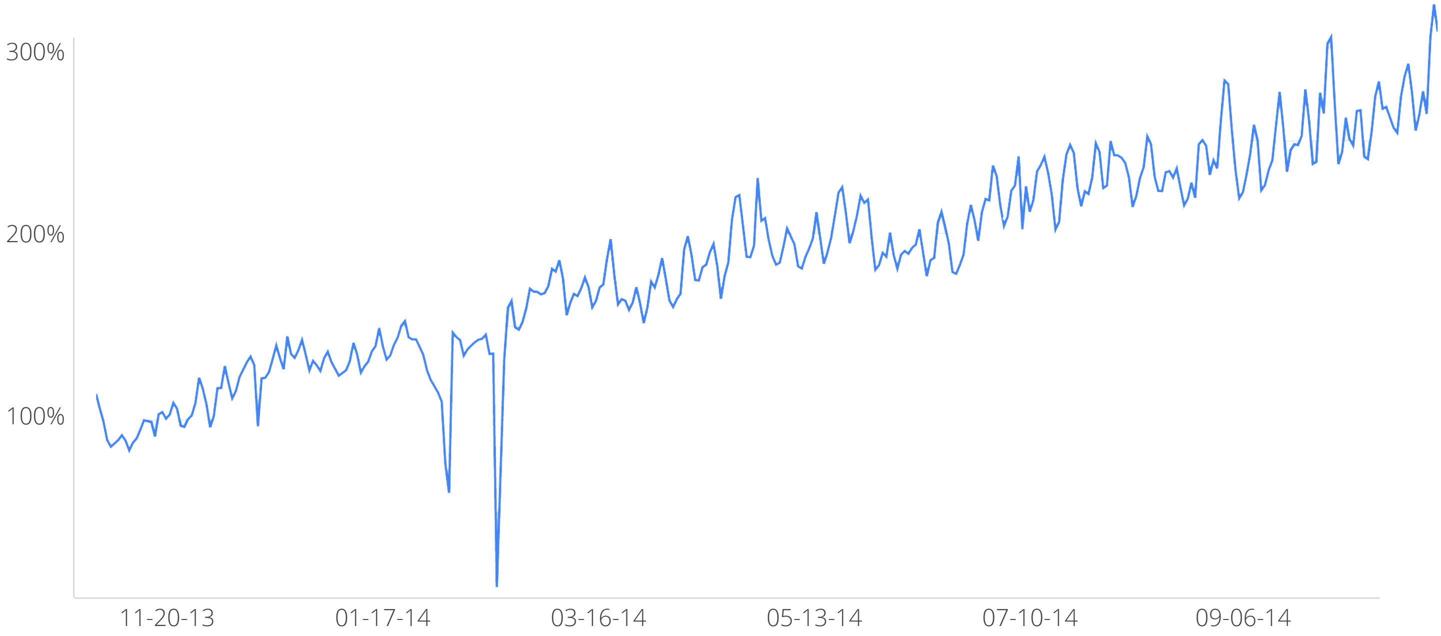
There are over one billion devices that are protected by Google's security services for Android.

Scope of User Protection & Ecosystem Measurement

Verify Apps was launched in November 2012. In the first 12 months of availability, the service grew rapidly to checking for Potentially Harmful Applications (PHAs) for millions of install attempts per day. In the next 12 months, which are the focus of this report, installs checked by Verify Apps have grown by nearly 300%. This compounding growth rate is one of the reasons that Google recommends against use of any absolute counts when evaluating potential risk to users within the Android ecosystem. As Android's ecosystem continues to grow, absolute counts will continue to grow regardless of actual risk associated with an action or device. To provide an accurate understanding of risk, the Android Security Team "normalizes" statistics relative to an action or device.

During 2014, Google Play provided security checks prior to publication for all applications published to Google Play and millions of installs per day from outside of Google Play.

Growth in Installs Checked by Verify Apps in 2014



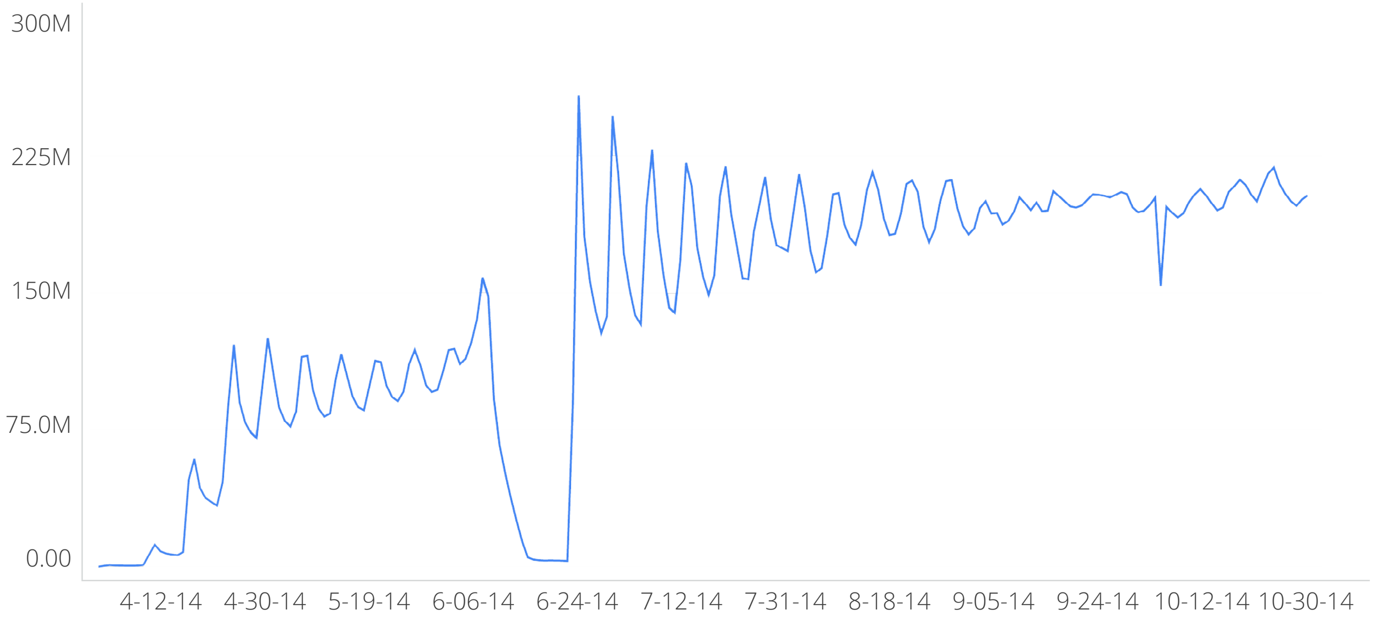
In March 2014, Verify Apps was enhanced to provide background scanning for potential security issues and Potentially Harmful Applications.

The graph below shows the growth in the number of devices using this service, which has grown to cover nearly all Android devices that check-in with any Google service.

By default, device scans are run approximately once per week which initially introduced periodic usage spikes that have been gradually removed by introducing randomness into the schedule for each device. Also note that for testing purposes, the background service was disabled briefly in June, hence the temporary drop in volume. (Devices were still protected with install time Verify Apps during this period). Volume for the week prior to 11/1/2014 was just over 200 million devices scanned per day.

Volume for the week prior to 11/1/2014 was just over 200 million devices scanned per day.

Number of Device Scans

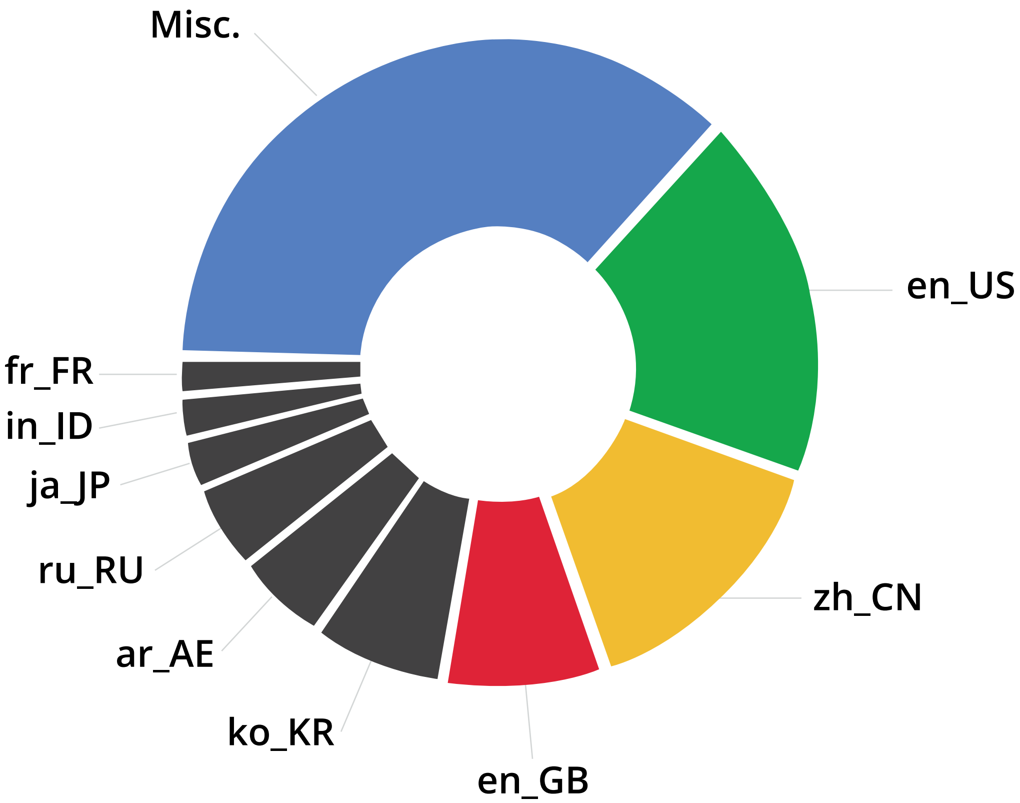


The following two graphs shows basic language information associated with these install events outside of Google Play.

For privacy reasons, Verify Apps only collects data needed to provide and improve device security. It does not access any personal information, nor does it check the physical location of the device.

Android devices have a device locale that can be configured by the user to provide localized user experience. Locale provides both the language of device and a region that can be associated with the language (for example Spanish has unique locales for Mexico, Spain, The United States, etc.). Within Verify Apps data, the device locale allows us to provide warnings in an appropriate language using region-specific characteristics of the language. The locale does not provide location of the device, per se, as a device of any locale can be in any physical location (devices may also change location without changing locale, and vice versa) but it allows us to roughly segment data by country, allowing Google's analysts to identify regional biases in the product (e.g., effects of localized warning strings) and the ecosystem (e.g., prevalence of certain types of potentially harmful apps).

Scans at Install by Locale



The Verify Apps user base is generally reflective of the worldwide mobile user population.

China is a unique market for Android in that Google services are not widely available. We believe based on numerous industry reports that there may be several hundred million Android devices in China.

In the 7 days prior to 11/1/2014, 14 million Chinese language devices used Verify Apps, and, in that 7-day period, Chinese language devices had installed 39 million apps.

So, although Google is not able to provide the same broad ecosystem-wide protection for Chinese devices, over 10 million active devices do provide significant visibility into regional variations that are unique to Chinese devices.

Classification of Potentially Harmful Applications

Google's systems use machine learning to see patterns and make connections that humans would not.

All Potentially Harmful Applications (PHAs) are prohibited from Google Play by policy -- this includes any application that can potentially harm the user, their device, or their data. Before applications become available in Google Play, they undergo an application security review process to confirm that they comply with Google Play policies, prohibiting potentially harmful applications. Google's systems use machine learning to see patterns and make connections that humans would not. Google Play analyzes millions of data points, asset nodes, and relationship graphs to build a high-precision security-detection system.

The signals and results are continuously monitored and refined to reduce error rate and improve precision.

Here are some of the ways that our machines learn what is benign and what is potentially harmful:

Signatures

Signatures are used to compare apps against a database of known apps and vulnerabilities.

Static analysis

All application features are extracted and analyzed against expected benign behavior and potentially harmful behavior. This includes static analysis of all code within the application.

Dynamic analysis

Applications are run to identify dynamic behavior that cannot be extracted with static analysis. Dynamic analysis allows reviewers to identify data-driven attacks that require connection to a server and dynamic downloading of code.

Heuristic and similarity analysis

We compare applications with each other to find trends that lead to harmful apps. For example, if 80% of recent harmful applications have <quality XX> then we may double check any application that also declares <quality XX>.

Developer relationships

Non-code features are analyzed to determine possible relationships between applications and to evaluate whether the developer that created the application may have previously been associated with creation of Potentially Harmful Applications.

Third-party reports

Google Play has active relationships with industry and academic security researchers that feed into our analysis engine.

This same analysis is conducted for applications that Google has found outside of Google Play to deliver the Verify Apps feature. For users who have enabled protection for applications that are downloaded from outside Google Play, Verify Apps provides users with a warning based on classifying the application into 14 different categories.

As of 11/1/2014, the following classifications were in use: Generic PHA, Phishing, Rooting Malicious, Ransomware, Rooting, SMS Fraud, Backdoor, Spyware, Trojan, Harmful Site, Windows Threat, Non-Android Threat, WAP Fraud, Call Fraud. Each of these categories is associated with a warning string that is provided to the user if they attempt to install a PHA or if one is detected already installed on their device. These categories are based on PHAs that have been found in the wild on Android devices or that have been demonstrated by researchers. We expect that more categories will be added in the future. The most recently added categories are WAP Fraud and Ransomware, both of which were first detected affecting Android users during 2014. We have observed code associated with malicious activity on other operating systems embedded within Android applications; to prevent unintentional transmission of this code, two categories (Windows Threat and Non-Android Threat) warn users if the application shows evidence of a threat that exists for other operating systems. More details on the prevalence of each of the categories of PHA will be provided later in this document.

The vast majority of application installs are not classified as potentially harmful, so for most installations, the users of Verify Apps will see nothing displayed at the time of install.

If an application is classified as potentially harmful, then in addition to displaying the warning, Verify Apps may either block the installation or allow the user to decide whether to allow installation to continue. An early design considered blocking all installations that were classified as potentially harmful, but user studies found that users might disable the feature if they disagreed with certain classifications. For example, many users will proceed to install Rooting apps after a warning is provided as they likely already knew that it would bypass Android security protections.

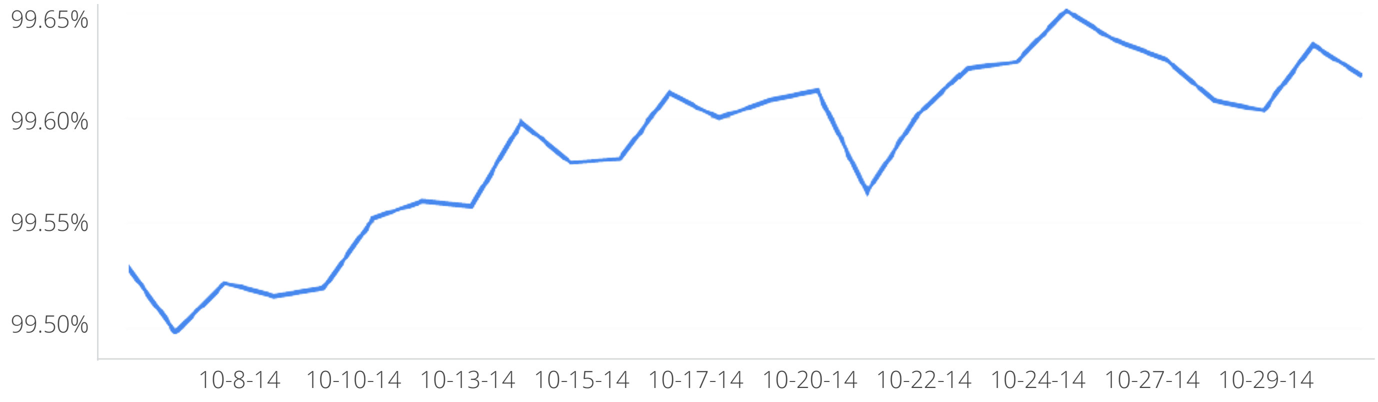
Occurrence of Potentially Harmful Applications[6]

This section will provide a detailed breakdown of information gathered from Verify Apps on the frequency of occurrence of Potentially Harmful Applications (PHAs). It provides the most complete picture available of the overall state of the Android ecosystem with respect to PHAs. As noted in the introductory pages of this report, in 2014 less than 1% of all devices had a PHA installed. Fewer than 0.15% of devices that download only from Google Play had a PHA installed. The rate of installation of PHAs from outside Google Play also decreased by nearly 60% between Q1 and Q4 of 2014. Those findings will be explained in detail in the following pages. They will also be broken down by the categories of behavior and using device locale information to better identify relevant trends and variations within the worldwide Android ecosystem.

During October 2014, the lowest level of device hygiene was 99.5% and the highest level was 99.65%, so less than 0.5% of devices had a PHA installed (excluding non-malicious Rooting apps).

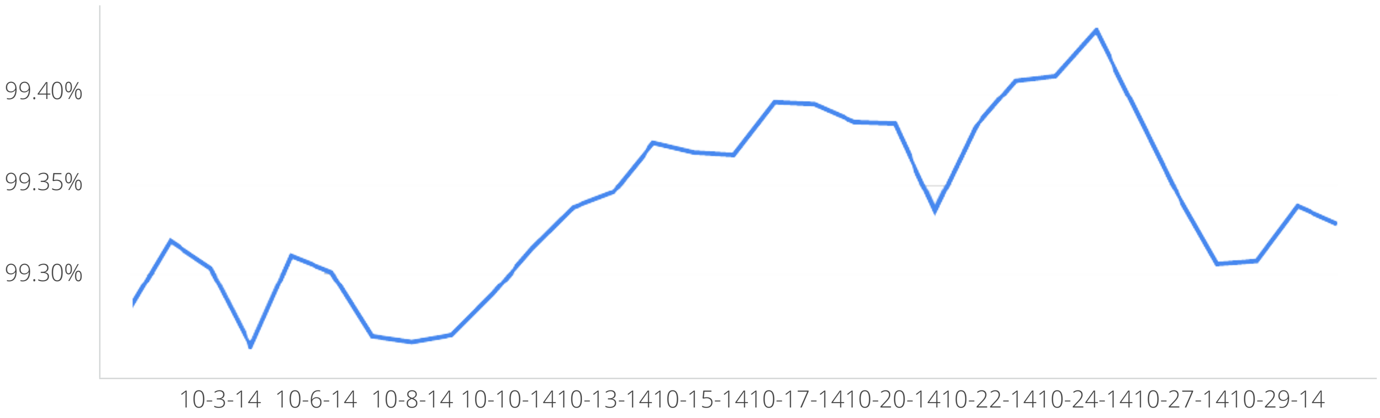
The broadest statistic that Verify Apps is currently tracking is the frequency with which Verify Apps detects an installed Potentially Harmful Application at the time that it does a full-device scan. We refer to this statistic as “device hygiene” and began to collect this statistic in early October 2014. Previously, data collection was associated with an install at the time of install and could not be tracked at the device level. During October 2014, the lowest level of device hygiene was 99.5% and the highest level was 99.65%, so less than 0.5% of devices had a PHA installed (excluding non-malicious Rooting apps). During that same time period, approximately 0.25% of devices had a non-malicious Rooting application installed. The device hygiene when incorporating all PHA applications is depicted in the following graph.

Devices without PHA (Excluding Rooting)



[6] A note on counting Potentially Harmful Apps (PHAs): Applications may not be classified as PHAs when first identified because later investigation reveals behavior that was hidden or believed to be innocuous which is actually potentially harmful. This means that the discovery of a new PHAs can lead to a restating of previous install statistics. To balance the need for timeliness and accuracy, the final version of this paper paper is being produced on February X, 2015 more than 60 days after 11/1/2014. Since we began collecting data in 2012, our data has shown that most PHAs are identified within 60 days of installation. For “time of install” statistics, this report includes installs of PHAs that were identified as PHA after 11/1/2014 if the install occurred prior to 11/1/2014. It is possible that some installations that occurred later in 2014 will be identified as PHAs in the future, but we don’t expect that will have a significant effect on the overall statistics. Also, as Google does not retain a historical record of apps per device the “device hygiene” statistics do not include applications classified as potentially harmful at a future date. They are the the best information available on the day of the scan.

Devices without Known PHA

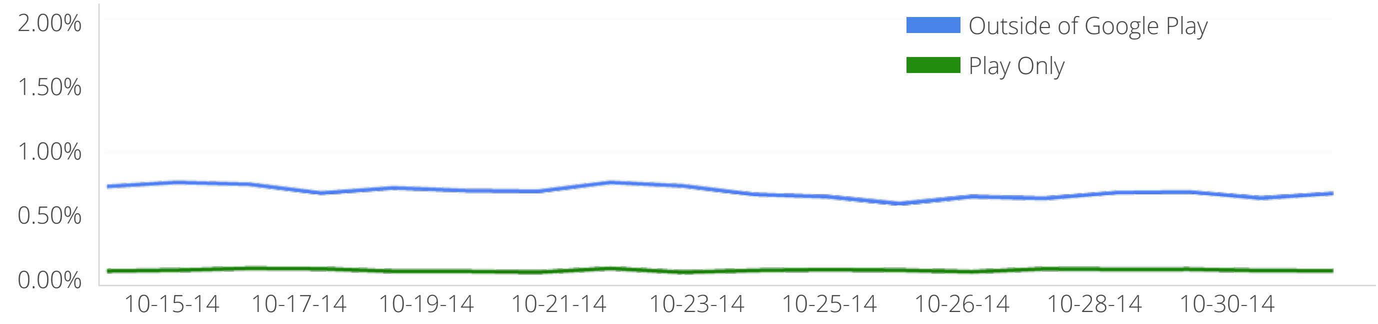


Google Play reviews all applications for potential security issues prior to making them available to users. No review process is perfect, and with over 1 million applications in Google Play, there are a small number of Potentially Harmful Applications that do still manage to be published in Google Play. To monitor all possible use scenarios, we are now tracking relative occurrence of PHAs for (1) devices that install only from Google Play, (2) devices that have installed from from outside of Google Play previously, and (3) devices that are currently configured to allow installation of apps from outside of Google Play.

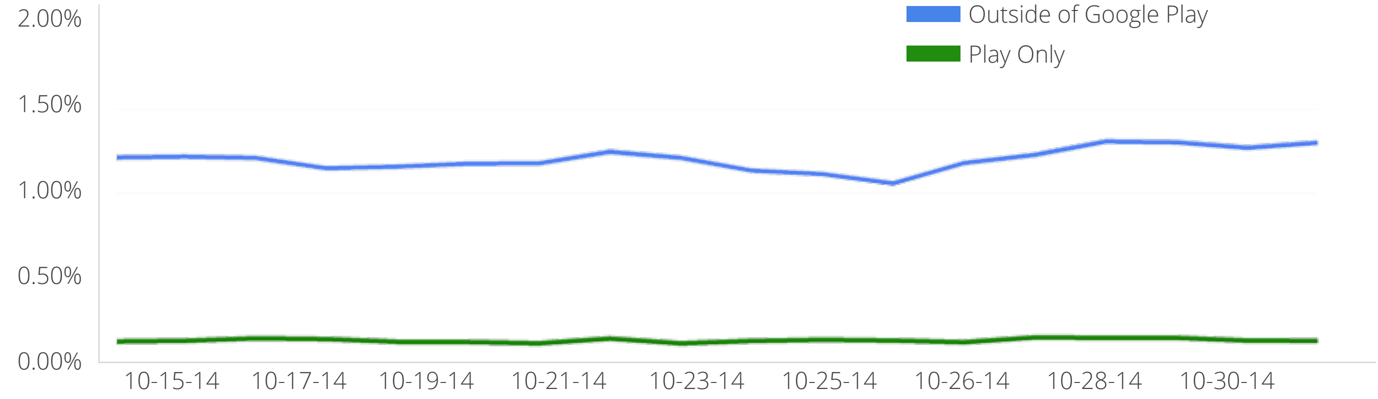
This was launched in mid-October 2014, so we currently have only 2 weeks of data prior to 11/1/2014. The blue line indicates devices which have unknown sources enabled and have installed applications from outside of Google Play. The green line represents devices that have only installed applications from Google Play. Worldwide, excluding non-malicious Rooting applications, PHAs are installed on less than 0.1% of devices that install applications only from Google Play. Non-rooting PHAs are installed on approximately 0.7% of devices that are configured to permit installation from outside of Google Play. Additionally, the second graph shows devices with any PHA (including Rooting applications). Rooting applications are installed on about 0.5% of devices that allow sideloading of applications from outside of Google Play.

Worldwide, excluding non-malicious Rooting applications, PHAs are installed on less than 0.1% of devices that install applications only from Google Play.

Devices with Known PHA (Excluding Rooting)



Devices with Known PHA (Including Rooting)

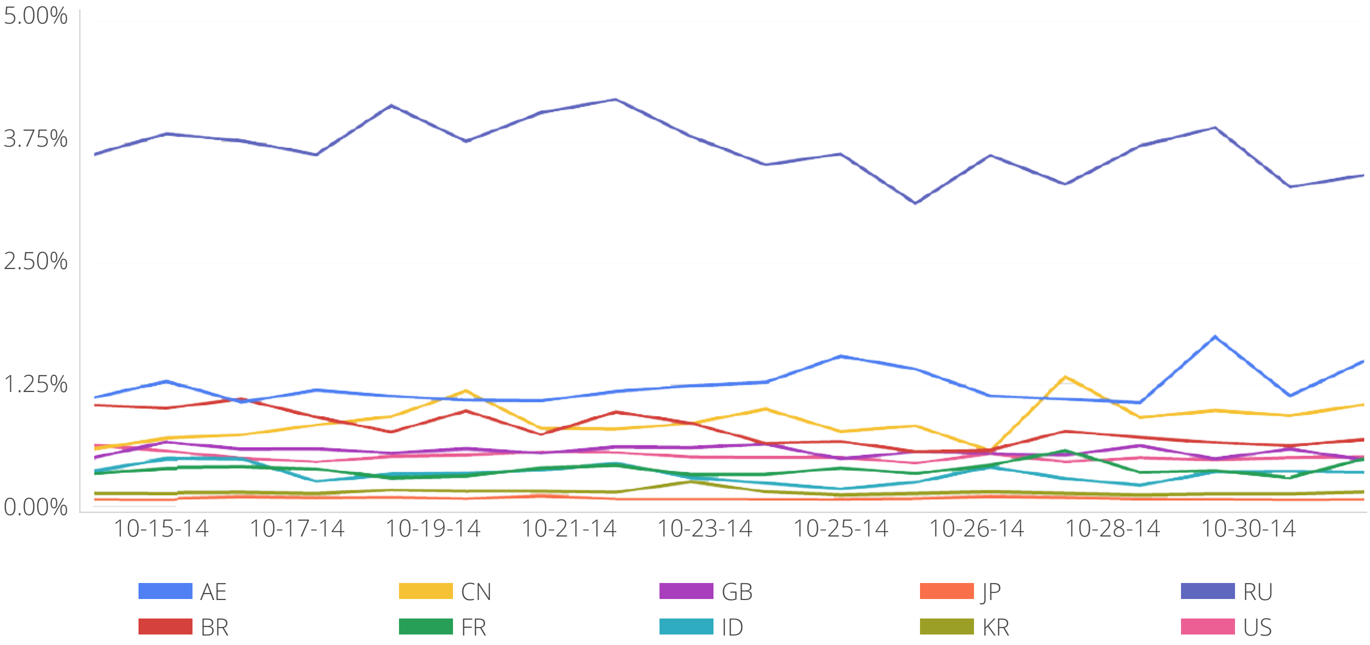


For devices that allow installation of applications from outside of Google Play, there are regional variations in the rate of installing PHAs. For comparison, below is a graph that shows prevalence of installed PHAs (excluding Rooting) by locale on devices that have been configured to install outside of Google Play for each of the locales that report the most installation events to Verify Apps.

During this period of time, US English devices have a PHA installed on about 0.4% of devices, which is about 0.2% below the worldwide average.

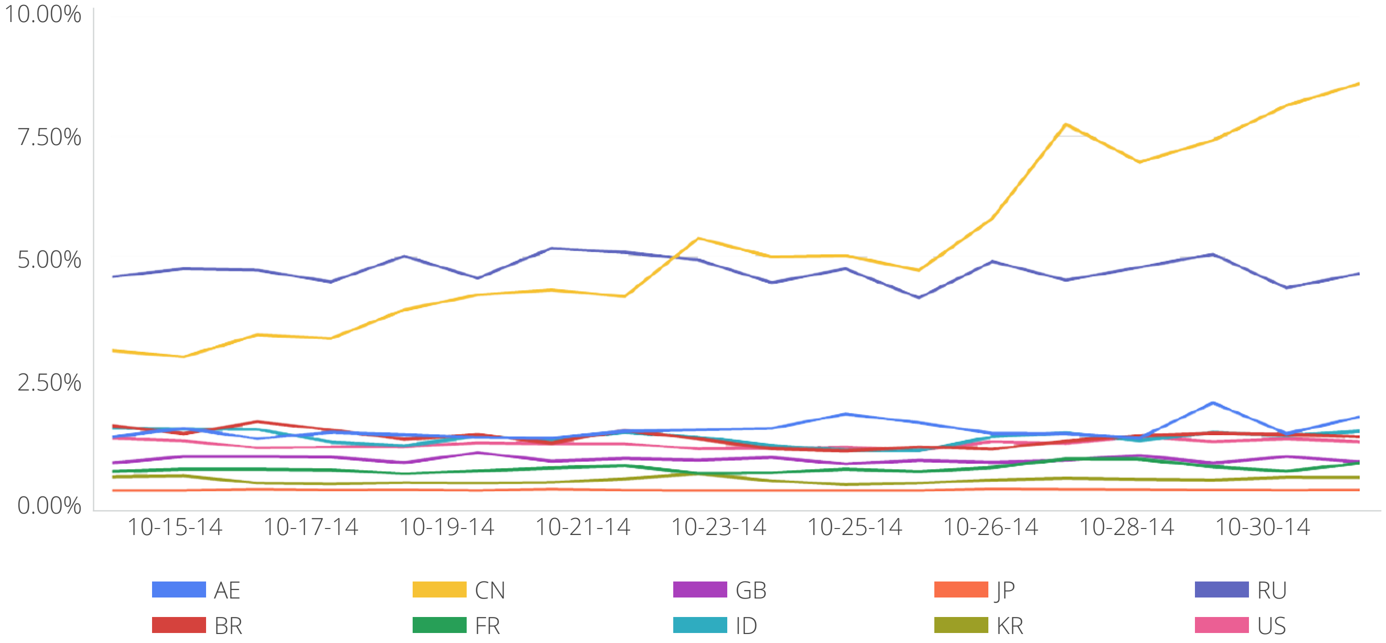
Chinese devices have a higher rate than the worldwide average, with a PHA installed on about 0.8% of devices and Russia has a much higher rate, with approximately 3-4% of devices having an installed PHA.

Fraction of Devices with Known PHA (Excluding Rooting), Safety Net users with Sideloading



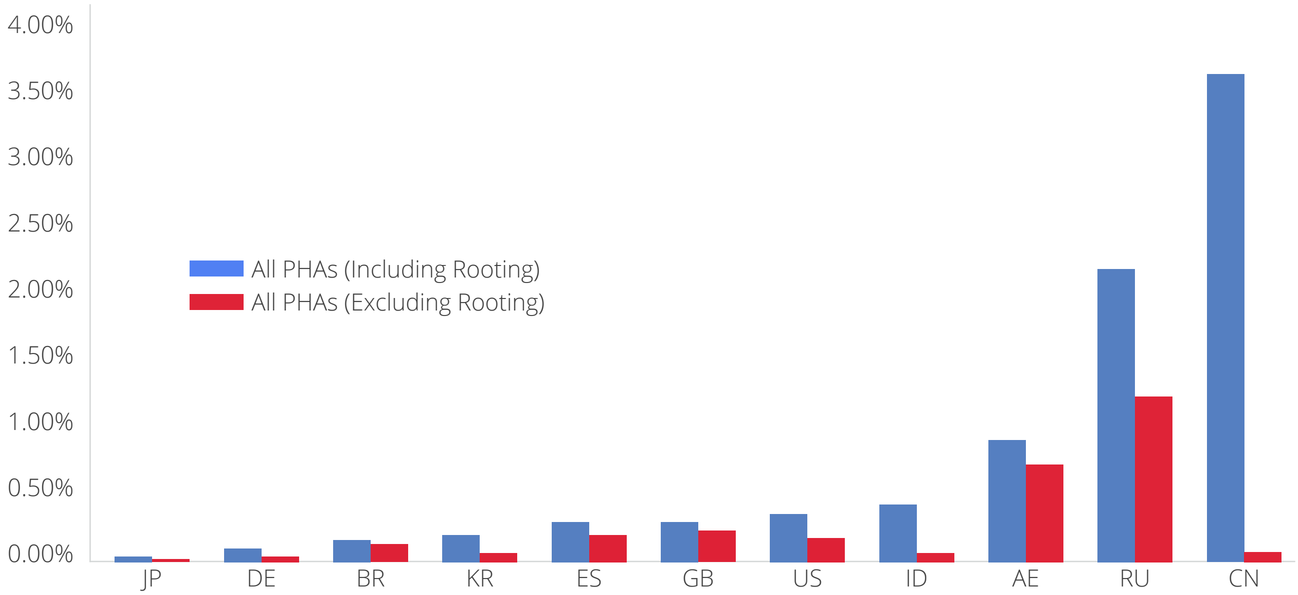
There is also regional variation in the prevalence of Rooting applications. The following graph shows the presence of all PHAs, including non-malicious Rooting applications. The basic shape of the graph is similar to the previous graph, with the exception of China. Chinese devices which install apps from outside of Google Play are more likely to have a non-malicious Rooting application than any other region or type of PHA. About 3-4% of Chinese devices have a Rooting application installed. In fact, there are numerous applications from major Chinese corporations that include rooting exploits to provide functionality that is not provided by the Android API. Some of these Rooting applications explicitly describe that they will use an exploit to root the device, but there are some applications which do not describe this functionality to users. In those cases, Verify Apps may provide the only indication that an exploit is included and that installation of the application may degrade the overall security of the device.

Fraction of Devices with Known PHA, Safety Net users with Sideloading



Below is a chart that provides the average fraction of devices with a PHA installed during the two weeks preceding 11/1/2014 for the most common locales.

Fraction of Devices with a PHA Installed, All Safetynet Users (Including Rooting)

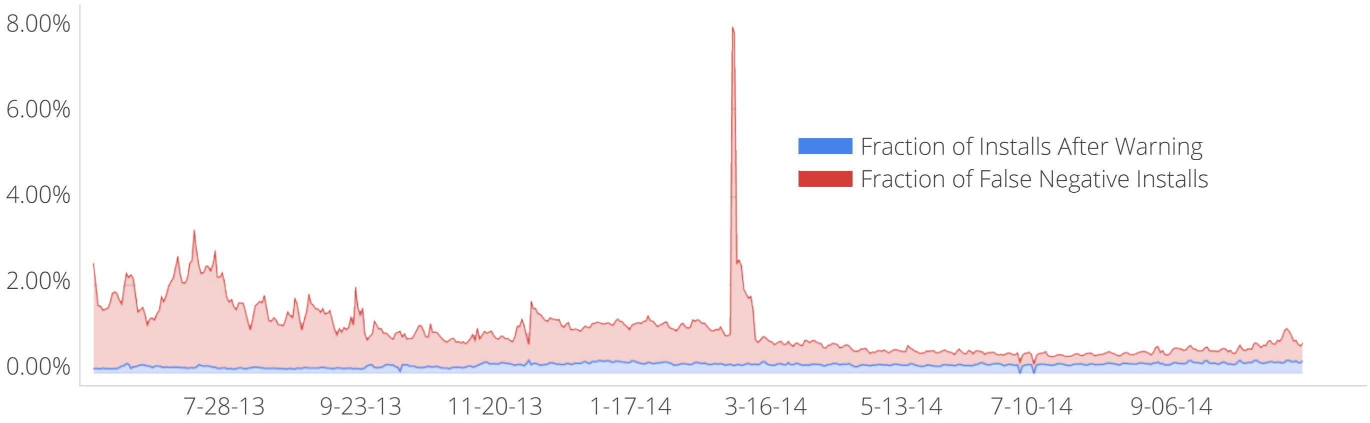


Although device-level statistics for PHAs only recently became available for applications installed from outside of Google Play, Verify Apps has been tracking per install ratios since 2012. From November 2012 until June 2013, it was available only on devices running the then current version of Android, Android 4.2. In June 2013 Verify Apps became available for previous versions of Android (specifically, Android 2.3 and above).

The graph below shows the overall tracking since June 15, 2013, when Verify Apps became widely available.

In the graph, the combined area of the red and blue curves shows the ratio of PHA installs relative to total installs. The blue curve depicts installs that may occur if a user choses to install an application despite a warning from Verify Apps (for example, they choose to install a rooting application despite a warning). The red curve depicts installation for which a warning was not provided at the time of installation and the application was subsequently determined to be potentially harmful (a false negative at the time of install).

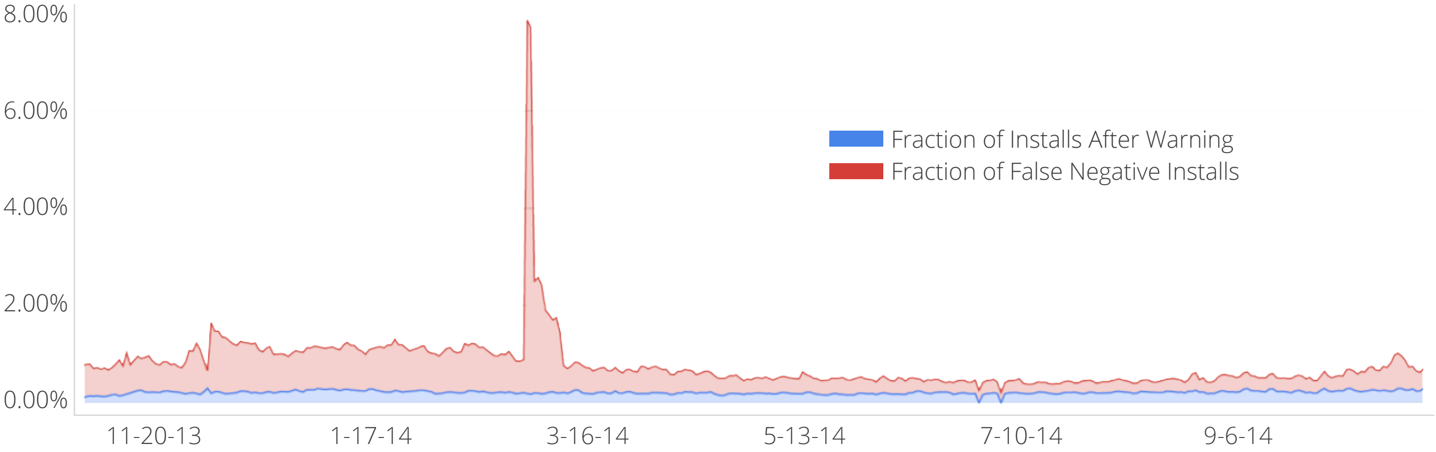
Fraction of Installs Outside of Google Play that Result in Known PHA Being Installed



There is a clear and substantial reduction in the number of PHA Installs between mid 2013 and late 2014. Although it is not broken down in this paper, our internal analysis has shown that this is related to (1) a reduction in the frequency with which Android users encounter[7] PHAs, (2) a reduction in the number of installations that actually occur, and (3) a reduction in the Verify Apps false negative rate. The graph below shows the same data, but limited to the 2014 time period that is the focus of this document.

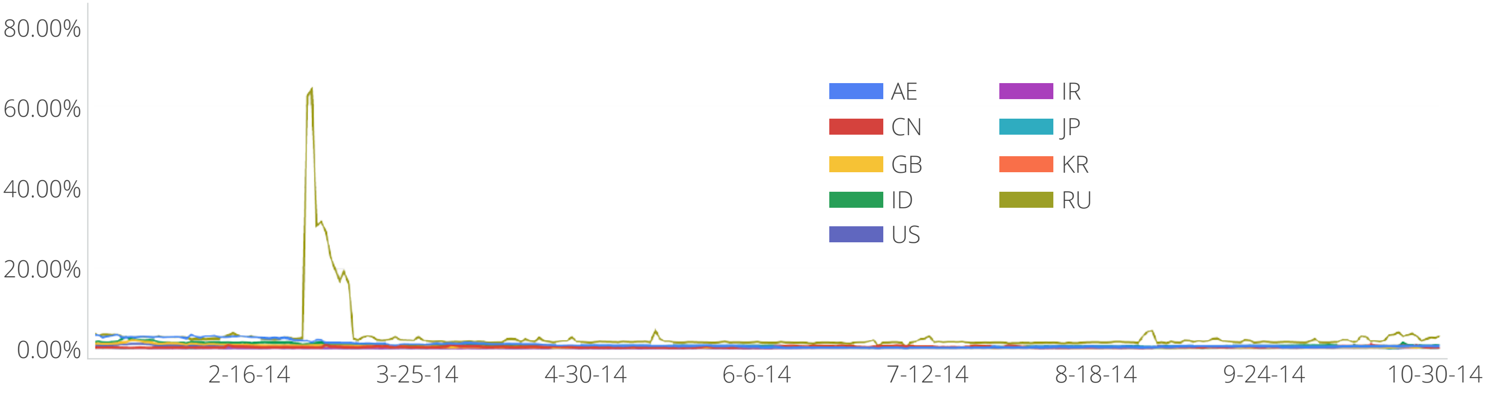
During 2014, there has been an ongoing decrease in the overall exposure of Android users to PHAs, including applications installed from outside of Google Play.

Fraction of Installs Outside of Google Play that Result in Known PHA Being Installed



The overall numbers in the previous graph mask a significant regional bias. The graph below shows the frequency of warnings across the most common locales. Note the change in the Y-axis relative to previous graphs. Also note that a single country (Russia - represented by a light green line) was the source of most of the installs that occurred in the campaign in March of 2014. Throughout 2014, Russian devices were almost 5x more likely to install a PHA than the worldwide average.

Fraction of Installs Outside of Google Play that Result in Known PHA Being Installed (Top Locales)

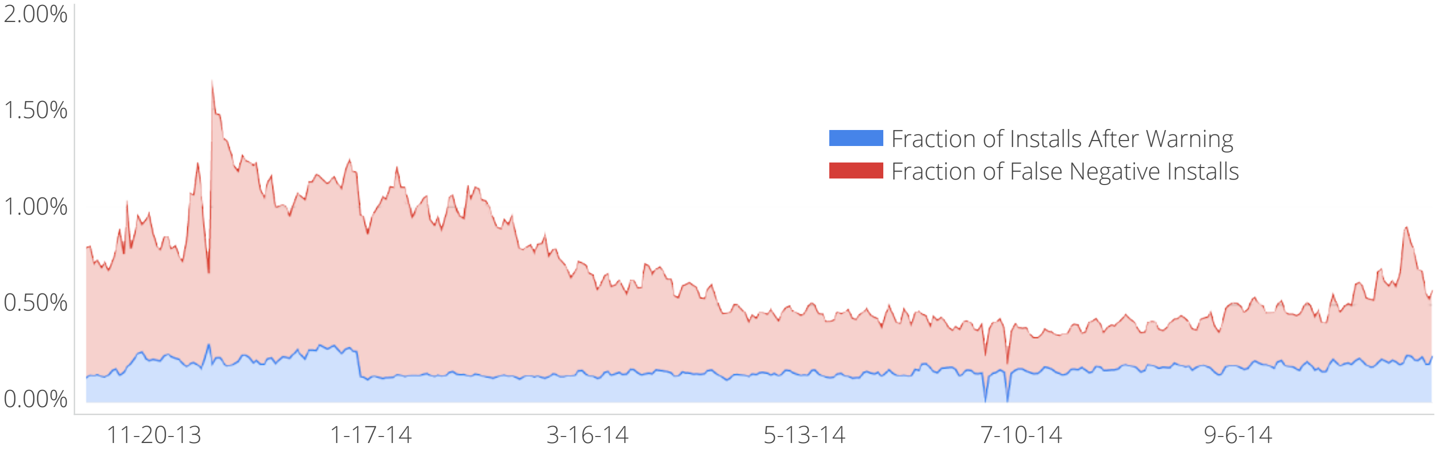


[7] For purposes of PHA analysis using Verify Apps, we define an "encounter" as any time that the user attempts to install an application. If that user receives a warning from Verify Apps and chooses not to proceed, then they have encountered the application but it has not been installed.

The following graph shows the worldwide rate of PHA installs for all locales in aggregate, excluding Russia. Excluding Russia, the worldwide average rate of PHA installs outside of Google Play has decreased by about 50% between Q1 and Q4 of 2014. That is also true when including Russia, though the large campaign affecting Russian devices in March 2014 obscures the data slightly.

The worldwide average rate of PHA installs outside of Google Play has decreased by about 50% between Q1 and Q4 of 2014.

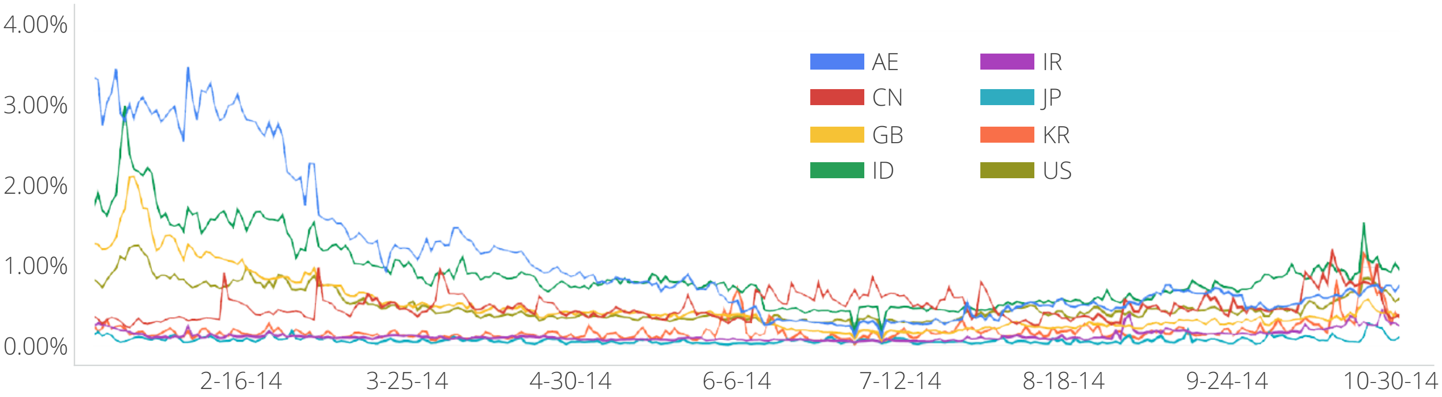
Fraction of Installs Outside of Google Play that Result in Known PHA Being Installed (Excluding Russia)



To provide more detail, here is the graph broken down by country, for the top locales, excluding Russian devices. British English, US English, Arabic, and Indonesian devices have all seen a decrease of about 75% in the rate of installation of PHAs from outside of Google Play throughout 2014. The remaining locales have all had relatively stable levels of warnings throughout the year at under 1% of installs from outside of Google Play.

Great Britain English, US English, Arabic, and Indonesian devices have all seen a decrease of about 75% in the rate of installation of PHAs from outside of Google Play throughout 2014.

Fraction of Installs Outside of Google Play that Result in Known PHA Being Installed (Top locales)



To summarize the previous series of graphs, the following table shows the rate of occurrence of any PHA per installation of an application from a source outside of Google Play during 2014. The data has been broken down by each quarter of the year and includes both a worldwide statistic and statistics for each of the top locales.

To summarize the previous series of graphs, the following table shows the rate of occurrence of any PHA per installation of an application from a source outside of Google Play during 2014. The data has been broken down by each quarter of the year and includes both a worldwide statistic and statistics for each of the top locales.

Fraction of Installs Outside of Google Play that result in Known PHA Being Installed (Including Rooting), Worldwide & for Top Locales

Locale	Q1	Q2	Q3	Q4	2014 Average
JP	0.0919%	0.0688%	0.0457%	0.0742%	**0.0702%**
IR	0.1810%	0.1157%	0.0774%	0.1802%	**0.1386%**
KR	0.1938%	0.1448%	0.1630%	0.2513%	**0.1882%**
CN	0.3097%	0.5006%	0.5137%	0.5145%	**0.4596%**
US	1.0069%	0.5678%	0.3376%	0.4889%	**0.6003%**
GB	1.5525%	0.6851%	0.2836%	0.3143%	**0.7089%**
Worldwide	1.0590%	1.0625%	0.4679%	0.5670%	**0.7891%**
BR	1.5518%	1.0639%	0.4989%	0.8836%	**0.9996%**
ID	2.0603%	1.1477%	0.5928%	0.7520%	**1.1382%**
AE	3.0692%	1.7243%	0.5016%	0.5859%	**1.4703%**
RU	3.2671%	8.2968%	1.7496%	2.1057%	**3.8548%**

The following table shows the same data as above, but excludes non-malicious Rooting applications, which are intentionally installed by some users. This includes only installs of applications from outside of Google Play. The data has been broken down by each quarter of the year and includes both a worldwide statistic and statistics for each of the top locales.

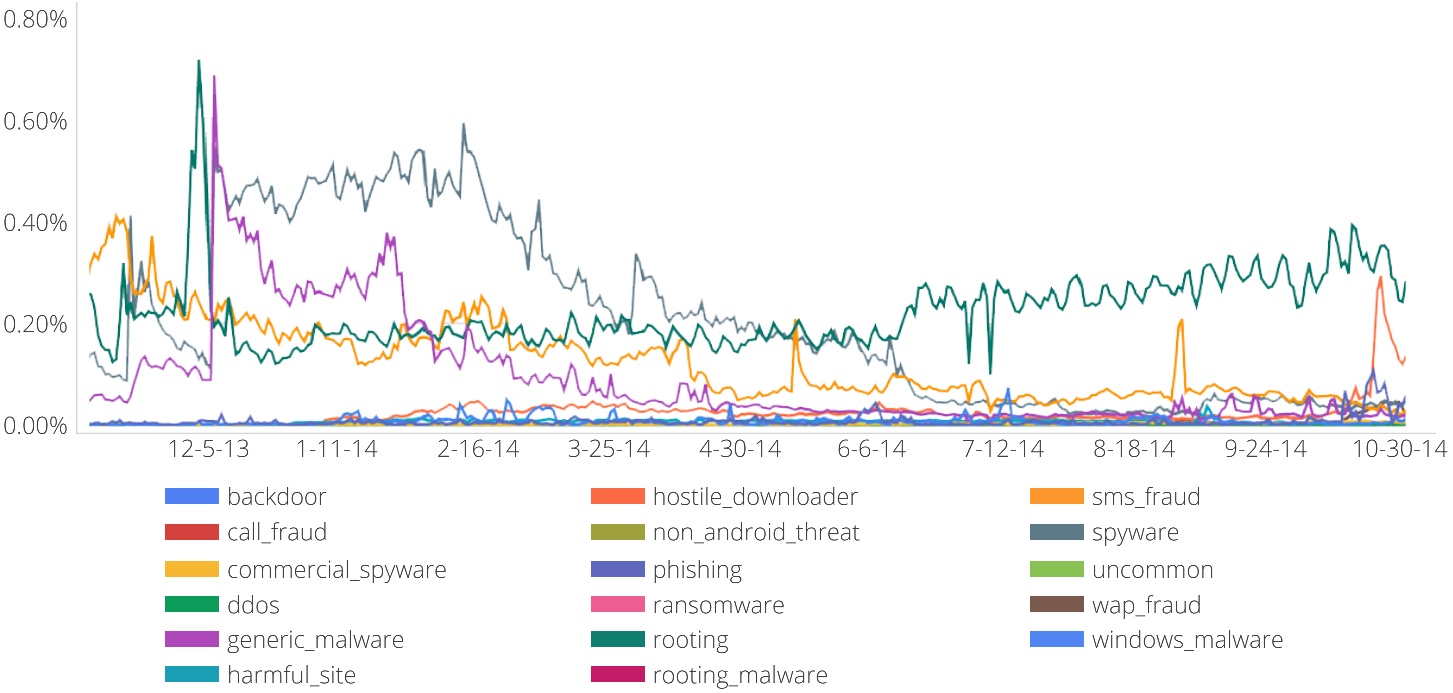
Fraction of Installs Outside of Google Play that result in Known PHA Being Installed (Excluding Rooting), Worldwide & for Top Locales

Locale	Q1	Q2	Q3	Q4	2014 Average
JP	0.0705%	0.0503%	0.0121%	0.0254%	**0.0396%**
KR	0.1001%	0.0681%	0.0833%	0.1254%	**0.0942%**
IR	0.1661%	0.0958%	0.0579%	0.1372%	**0.1142%**
CN	0.0691%	0.2132%	0.1811%	0.0434%	**0.1267%**
US	0.8733%	0.4369%	0.1673%	0.2264%	**0.4260%**
Worldwide	0.8586%	0.8839%	0.2580%	0.2791%	**0.5699%**
GB	1.4870%	0.6193%	0.2015%	0.1553%	**0.6158%**
BR	1.4220%	0.9242%	0.2752%	0.4567%	**0.7695%**
ID	1.8482%	0.8768%	0.2446%	0.2161%	**0.7964%**
AE	2.9926%	1.6289%	0.3703%	0.4337%	**1.3564%**
RU	2.9815%	7.9520%	1.2431%	1.4263%	**3.4007%**

Verify Apps classifies every application installation into distinct category based on application behavior.

For installs of application outside of Google Play and checked by Verify Apps, the following graph provides the rate of occurrence for each type of warning issued during 2014. Because a campaign in early March overwhelms all the data (see page 23 for more information), the Trojan category has been excluded here. During the first half of the year the most common installs is for Spyware. This category decreased throughout the year. The second most common type is Generic Malware. This category is provided when applications are known to be potentially harmful based on association with previous potentially harmful apps, and in particular these installs were being downloaded from websites that were targeting Russian devices with SMS and WAP fraud. In the second half of the year, the most common type of PHA that is installed is Rooting.

Fraction of Installs Outside of Google Play that Result in Known PHA of the Given Category Being Installed



New & Noteworthy PHAs

The following section includes data that has been collected via Verify Apps about particular types of Potentially Harmful Applications that rose in prominence or that received significant media attention in 2014.

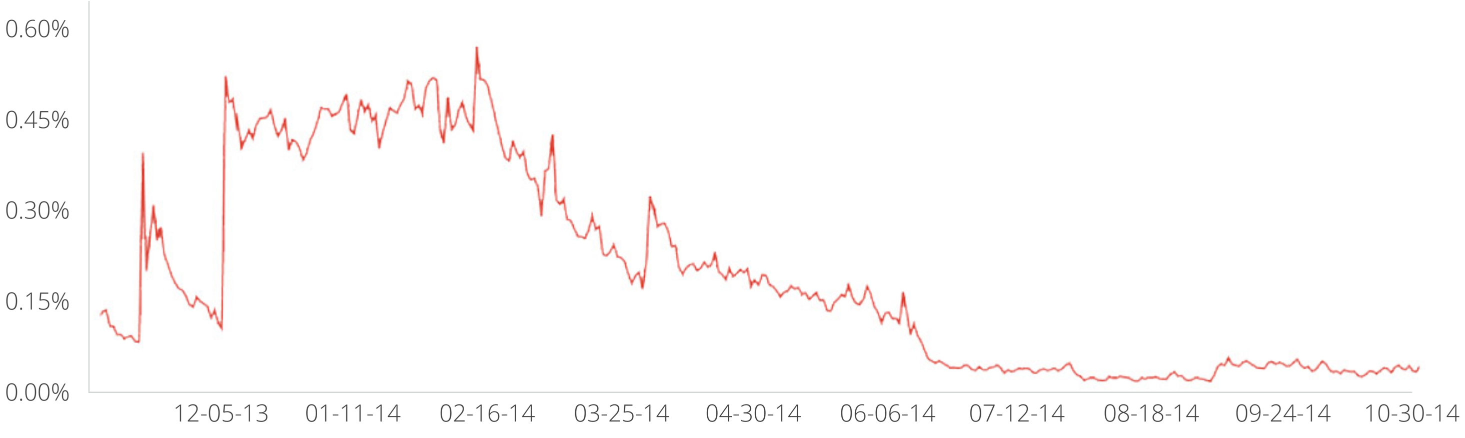
Spyware

Spyware is a category used to describe any application that attempts to take information from a device and send it to a third party without adequate consent from the user of the device.

Throughout 2014, we have regularly tightened the definition of Spyware, for example in 2014 we began to classify applications that send the list of other applications on the device as Spyware. The graph below shows the overall rate of install of applications categorized as Spyware. We believe the the decline is due to increasing strict definition of Spyware throughout 2014 -- in response to increasingly tight policies, applications developers have reduced the amount of information that is sent from devices without user consent. This leads us to conclude that many applications categorized as Spyware are not something we would consider malicious.

many applications categorized as Spyware are not something we would consider malicious.

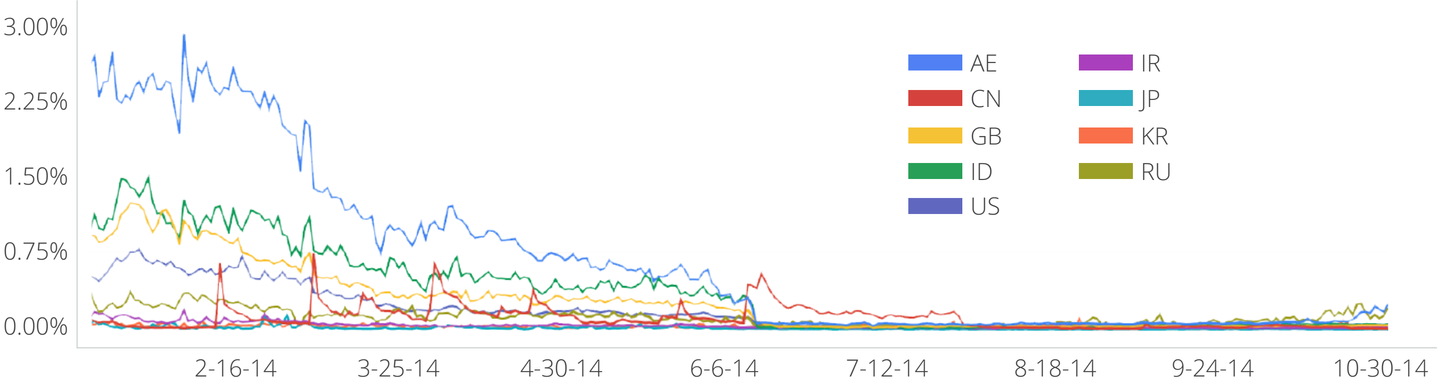
Fraction of Installs Outside of Google Play that Result in Known Spyware Being Installed



The graph below shows the prevalence of Spyware for each of the locales with the most installs.

All regions have seen a decline in installation rates of spyware throughout 2014. The decline was most significant in Arabic and Indonesian locales.

Fraction of Installs Outside of Google Play that Result in Known Spyware Being Installed



To summarize the previous two graphs, the following table shows the rate of occurrence of Spyware per installation of an application from a source outside of Google Play during 2014. The data has been broken down by each quarter of the year. It includes both a worldwide statistic and statistics for each of the top locales.

Fraction of Installs Outside of Google Play that result in Known Spyware Being Installed, Worldwide and for Top Locales

Locale	Q1	Q2	Q3	Q4	2014 Average
JP	0.0277%	0.0189%	0.0081%	0.0017%	**0.0141%**
KR	0.0481%	0.0340%	0.0180%	0.0150%	**0.0288%**
IR	0.0987%	0.0490%	0.0222%	0.0151%	**0.0463%**
CN	0.0451%	0.1812%	0.1387%	0.0204%	**0.0964%**
RU	0.2367%	0.1653%	0.0716%	0.0772%	**0.1377%**
Worldwide	0.3704%	0.3067%	0.0993%	0.0377%	**0.2035%**
US	0.5342%	0.2744%	0.0778%	0.0342%	**0.2302%**
GB	0.9834%	0.4693%	0.1221%	0.0288%	**0.4009%**
BR	0.9894%	0.3615%	0.0998%	0.2364%	**0.4218%**
ID	1.2066%	0.6957%	0.1689%	0.0353%	**0.5266%**
AE	2.2556%	1.3119%	0.2567%	0.0581%	**0.9706%**

In 2014, we also began to differentiate a new subcategory of Spyware that we refer to as Commercial Spyware. These are applications that are installed by an individual who has temporary possession of another user's device. Our research suggests that this is likely someone who has a personal relationship with the device owner, so we have also seen use of the phrase "spouseware" for this category of application. These applications have also been associated with target attacks against individuals, sometimes referred to as Advanced Persistent Threat (APT) or Spear Phishing.

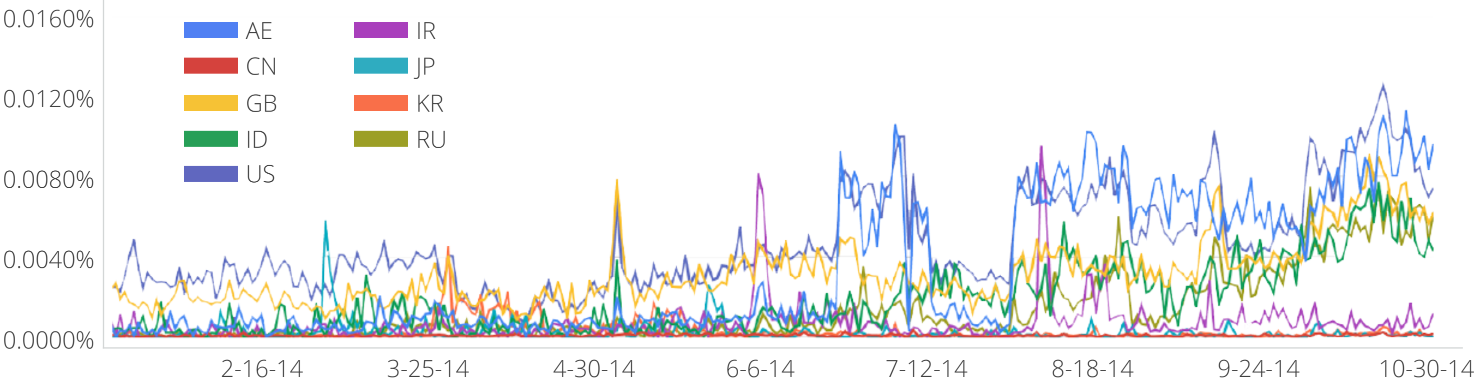
In 2014, we also began to differentiate a new subcategory of Spyware that we refer to as Commercial Spyware.

Commercial Spyware generally use legitimate system functionality on the device such as location tracking to send information to the party that installed the application and they do not have access to application specific information that is protected by Android's application sandbox such as email. In some instances, these applications do have the ability to access application data if the device has been previously rooted. We have not seen Commercial Spyware that incorporates exploits for a local privilege escalation vulnerability.

The fraction of installs classified as Commercial Spyware is below 0.01% of installs in 2014.

Although rates are below 0.01% (or below 1 in 10,000) of installs, in contrast to other categories of PHA, rate of installs of Commercial Spyware have increased in 2014. We do not know the exact reason for this increase. With respect to Commercial Spyware, there are a number of Android platform level changes that are being incorporated to reduce the risk of the threat of a local attacker with physical access to the device. In Android 5.0, these included expanded use of device encryption and simplified authentication mechanisms. The graph below shows the fraction of installs that result in Commercial Spyware being installed in each of the major locales.

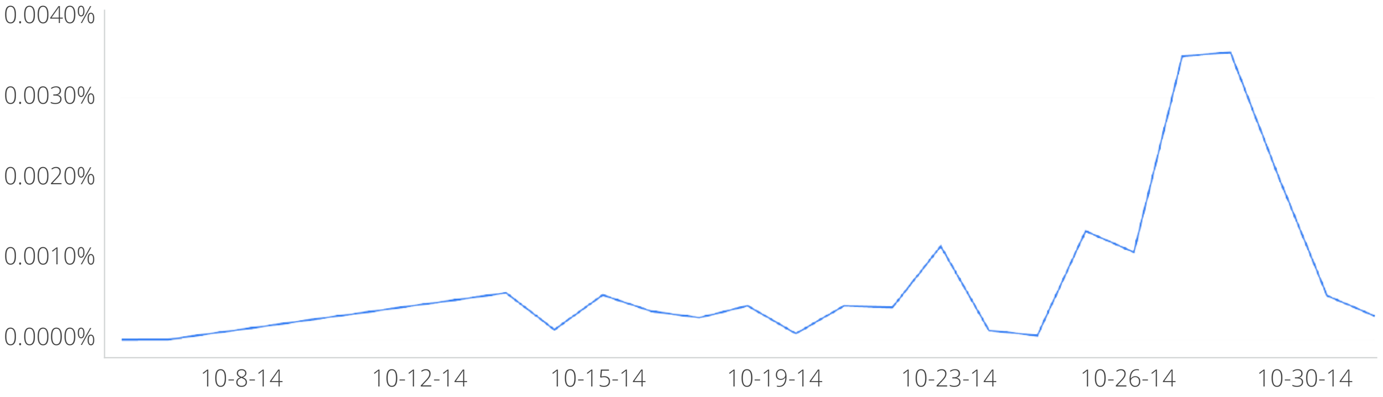
Fraction of Installs Installs Outside of Google Play that Result in Known Commercial Spyware Being Installed



Ransomware

The beginning of 2014 revealed the first instances of a new type of PHA. As these applications often masquerade as another application, prior to 10/1/2014 these were classifed as Trojans. Subsequent to 10/1/2014 they have been classified as Ransomware. These applications have taken two dominant forms: (1) applications that encrypt data on the device external storage (such as an SDCard) and then demand payment to decrypt the data, or (2) applications that prevent normal functioning of the device and then demand payment to regain access to the device. The graph below shows the frequency of installation of these Ransomware applications since 10/1/2014.

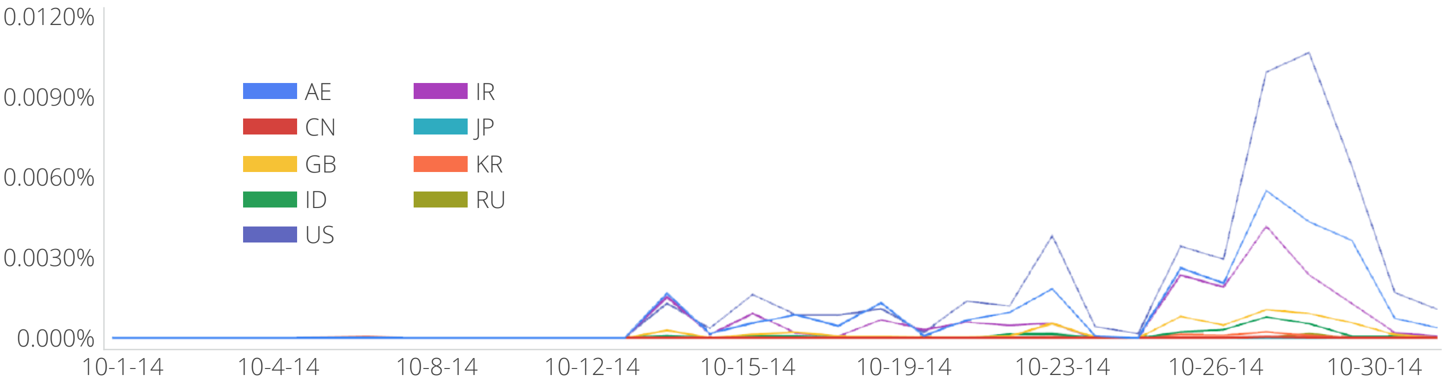
Fraction of Installs Outside of Google Play that result in Known Ransomware Being Installed



At this point, the total volume of Ransomware is sufficiently low that it is difficult to identify persistent regional patterns.

For completeness, the graph below shows the locale specific frequency of installation for the locales with the largest number of installs.

Fraction of Installs Outside of Google Play that result in Known Ransomware Being Installed (Top Locales)



In addition, Verify Apps can provide users with a warning and block installation before Ransomware affects users.

We are implementing technical changes in the Android platform that can make these techniques less effective on newer Android devices. In addition, Verify Apps can provide users with a warning and block installation before Ransomware affects users. While some early instances of Ransomware did manage to be distributed within Google Play, most distribution has occurred outside of Google Play.

WAP and SMS Fraud

Installs of SMS Fraud applications declined in frequency of occurrence by about 60% between the first and last quarter of 2014.

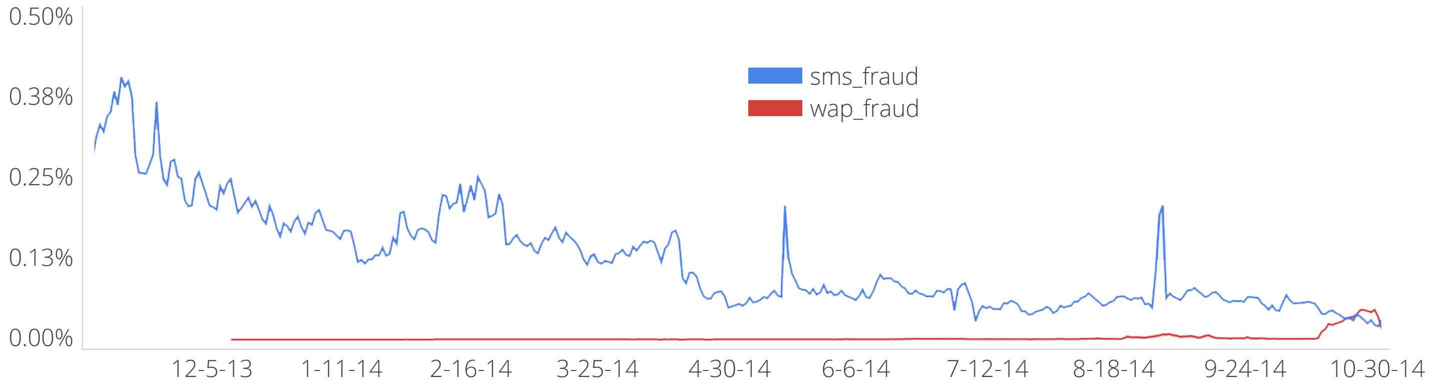
This is likely a result of two factors (1) changes in carrier billing regulations and carrier billing practices in multiple countries (2) increasing reach of security tools such as Verify Apps. Specifically, as usage of Verify Apps increased the profitability of this type of PHA was correspondingly reduced.

Although it did not receive much media attention, 2014 also showed an increase in applications attempting to abuse WAP billing by automating website interactions. The behavior of these applications is to connect to a website that can use carrier-billing based on carrier-specific network connection and then automate interaction with the website. These interactions were designed with the intention that the user would be using a website in a browser to register for a premium service, but automation can be used to improperly register the device for the service. This may appear on a customer bill as a premium services charge, similar to services that are authorized by premium SMS message.

Although it did not receive much media attention, 2014 also showed an increase in applications attempting to abuse WAP billing by automating website interactions.

The graph below shows the daily number of installs of applications categorized as SMS Fraud or WAP Fraud.

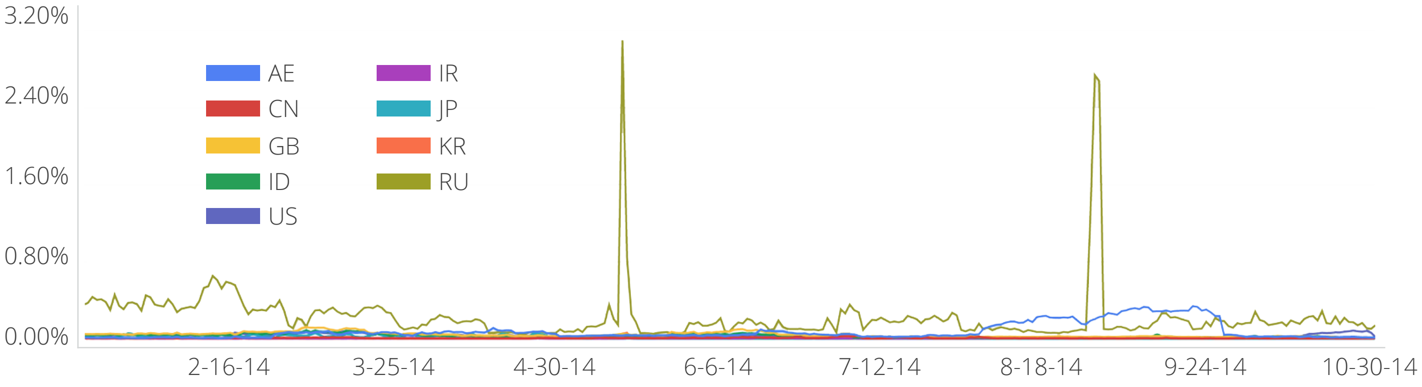
Fraction of Installs Outside of Google Play that result in Known SMS or Wap Fraud Being Installed



The graph below shows the daily number of installs of applications classified as SMS Fraud or WAP Fraud for devices with each of the most popular locales. Russian devices showed the highest level of risk throughout the year. They were also the focus of two specific campaigns in May and September which affected more than 2% of installs for two days. In early Q3 of 2014, Arabic devices exhibited a period of elevated rate of install of SMS Fraud applications, peaking at about 0.33% of installs in early September 2014.

Russian devices showed the highest level of risk throughout the year.

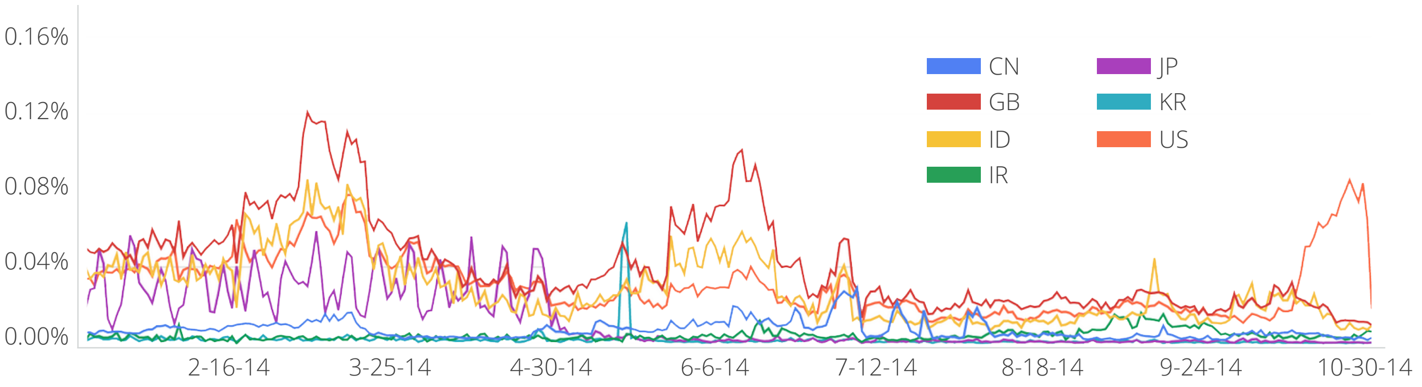
Fraction of Installs Outside of Google Play that result in Known SMS or WAP Fraud Being Installed (Top Locales)



To provide more granular information, this final graph of SMS and WAP Fraud shows the frequency installation of a PHA for devices in the other top locales.

Frequency of installation of SMS Fraud applications has decreased in most locales throughout 2014.

Fraction of Installs Outside of Google Play that Result in Known SMS or WAP Fraud Being Installed (Top Locales, excluding Russia)



To summarize the previous three graphs, the following table shows the rate of occurrence of SMS Fraud per installation of an application from a source outside of Google Play during 2014. The data has been broken down by each quarter of the year. It includes both a worldwide statistic and statistics for each of the top locales.

Fraction of Installs Outside of Google Play that result in Known SMS Fraud Being Installed, Worldwide and for Top Locales

Locale	Q1	Q2	Q3	Q4	Grand Total
KR	0.0021%	0.0021%	0.0022%	0.0006%	**0.0018%**
IR	0.0035%	0.0029%	0.0034%	0.0061%	**0.0040%**
CN	0.0061%	0.0068%	0.0096%	0.0044%	**0.0067%**
JP	0.0267%	0.0274%	0.0020%	0.0009%	**0.0142%**
US	0.0370%	0.0435%	0.0229%	0.0148%	**0.0296%**
ID	0.0397%	0.0416%	0.0260%	0.0155%	**0.0307%**
GB	0.0496%	0.0581%	0.0411%	0.0199%	**0.0422%**
AE	0.0100%	0.0508%	0.0377%	0.1411%	**0.0599%**
Worldwide	0.2105%	0.1447%	0.0679%	0.0587%	**0.1204%**
BR	0.0090%	0.4895%	0.1185%	0.0940%	**0.1778%**
RU	0.3760%	0.2398%	0.1789%	0.1934%	**0.2470%**

Safety Net Statistics

The expansion of the Verify Apps capability in 2014 has provided new ability to understand abuse of user devices through mechanisms other than installation of applications. This includes attempted exploitation of platform or application level vulnerabilities as well as network-level exploitation.

Platform API Abuse

On any open platform, there are APIs that provide valuable functionality to legitimate applications which when used inappropriately can lead to abuse. Within the Android OS, we react to this abuse by modifying or improving APIs, or by providing improved user notification so they can make decisions about which behaviors they would like to allow. Safety Net provides a third technique: detecting and responding to abuse that is attempted on user devices. There are a number of system APIs that can be checked for potential abuse by applications without having access to any user data.

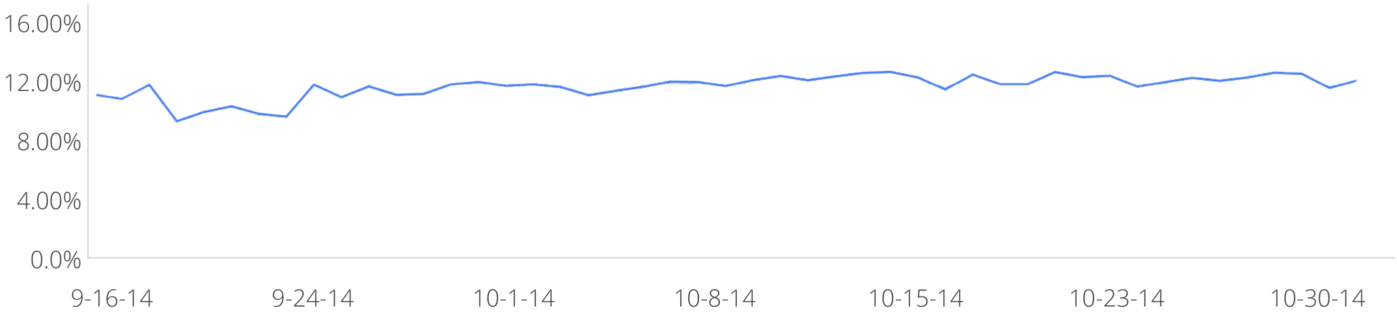
Safety Net provides a third technique: detecting and responding to abuse that is attempted on user devices.

SMS Confirmation

Starting with Android 4.2, Android provides a user confirmation prompt prior to an application sending an SMS to a shortcode that might result in a premium service. SafetyNet aggregates these events and uses them as a signal for identifying Potentially Harmful Applications that attempt to use premium services without user consent. This also provides high-level insight into how users interact with the premium SMS warning.
As shown in the graph below, worldwide during 2014, approximately 12% of attempted requests to send premium SMS were blocked.

worldwide during 2014, approximately 12% of attempted requests to send premium SMS were blocked.

Fraction of SMS Sent to Premium Shortcodes Blocked by User



Specifically, whether the user decides to allow the application to send the SMS can be used as a signal to indicate whether the application is behaving in a manner that matches user expectations.

For example, an SMS client that sends to a shortcode after the user intentionally inputs the shortcode is more likely to be approved by the user than an application that sends without first notifying the user.

SafetyNet aggregates data that is collected about which applications are more likely to have requests to send premium SMS be rejected by a user. This is used to identify Potentially Harmful Applications which are subsequently blocked by Verify Apps, or removed from Google Play.

Other APIs of Interest

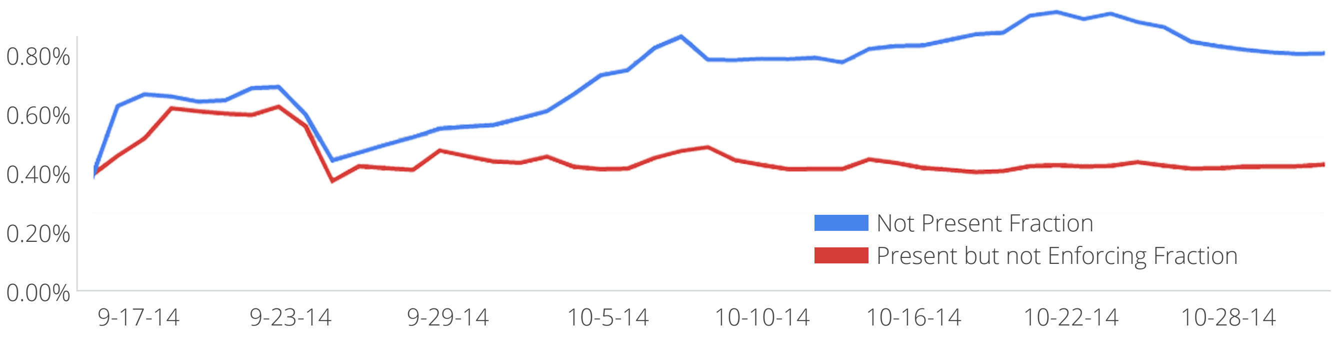
In 2014, Safety Net began to conduct small-scale experiments into methods to detect potential abuse of other APIs including Device Administrator, SD Card / External Storage, and telephony APIs. We do not currently have results from those experiments.

Security Model Integrity

Safety Net uses multiple different tests to determine whether a device is operating in a manner that is consistent with the expectations of the Android security model.

For example, starting with Android 4.4, SELinux is required to be set to Enforcing on all compatible Android devices. Safety Net began to track the status of SELinux on Android 4.4 and newer devices in September 2014. During the time measured in 2014, approximately 0.6% of devices had SELinux fully disabled and about 0.3% of devices had SELinux enabled and configured in Permissive mode. These settings indicate either that the device is running a non-certified system image (e.g. a custom ROM or one that did not pass CTS compatibility) or that the system integrity has been compromised (e.g. by a rooting application that subsequently disabled or reconfigured SELinux) -- in either case it is not a CTS-compatible Android 4.4 device.

Fraction of Android 4.4 Devices With Modified SELinux Configuration



Network Level Abuse

In 2013 and 2014, there was significant security community focus on attacks originating from off-device sources, including attacks on SSL protocol and CA infrastructure. The Android Security Team responded to these issues by developing multiple techniques to prevent exploitation including platform level changes, application level changes, including the release of the updateable SecurityProvider in Google Play Services and the release of the nogotofail testing framework. In addition to these protection mechanisms, Safety Net was updated to include the capability to measure attempted network exploitation.

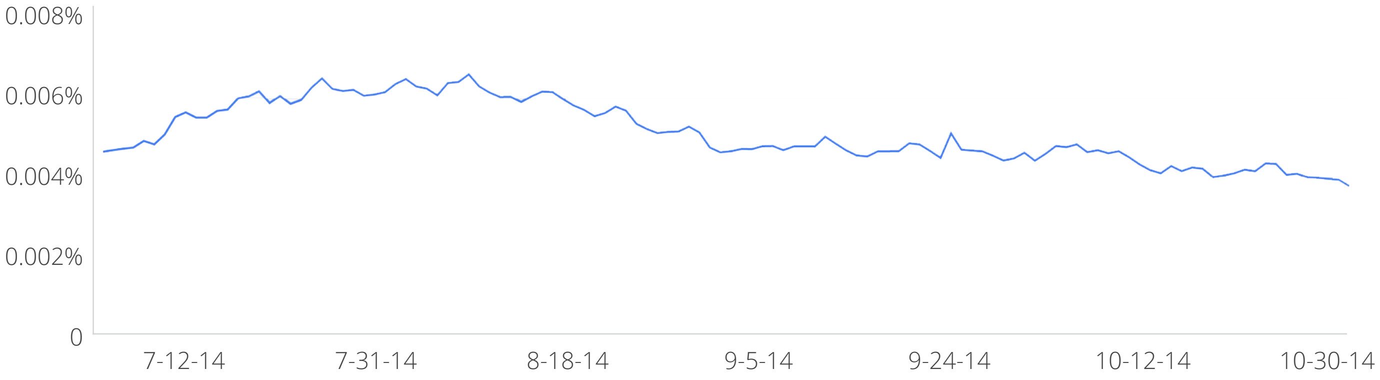
Safety Net currently analyzes about 400 million network connections per day to identify attacks that targeting network traffic.

SSLv3 downgrade

As part of the Android response to the disclosure of the POODLE attack, we began to actively monitor downgrade of SSLv3 connections. We are currently analyzing approximately 400 million connections per day to Google servers from Android devices throughout the world. Our goal is to monitor for individual instances of exploitation as well as determine if there are broad changes in the prevalence of SSLv3 downgrades that that might be indicative of large scale exploitation targeted at specific classes of devices or regions. So far, this research has not found any evidence of exploitation outside of research experiments, but we plan to continue the research. The graphs below show the frequency of a TLS connection to Google being downgraded to SSLv3. Worldwide about 50 out of every million attempts are downgraded. We do see regional variation, as reflected in the second graph below.

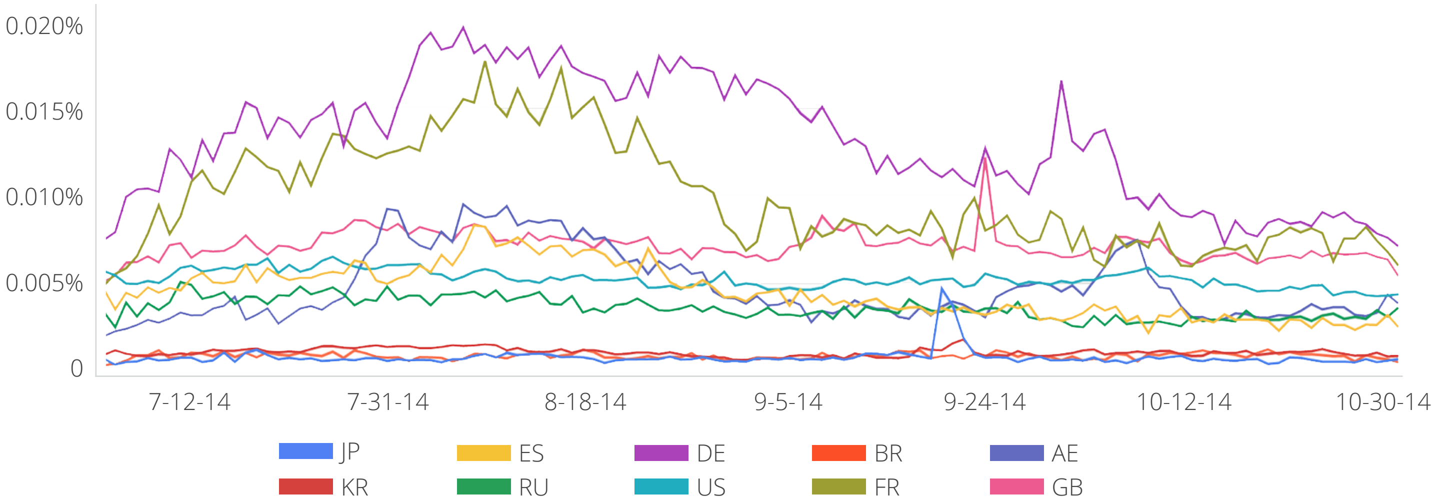
So far, this research has not found any evidence of exploitation outside of research experiments, but we plan to continue the research.

Fraction of SSL Connections Downgraded to SSLv3 (Worldwide)



The following graph shows the frequency of SSL v3 Downgrades per device locale. We do not currently have an explanation for the cause of these regional variations, but they appear to be stable per device locale. German, French, and English (GB) devices have the highest frequency of SSLv3 Downgrade among the most common device locales.

Fraction of SSL Connections Downgraded to SSLv3 (Top Locales)



CCS Injection

In July, OpenSSL released an advisory that included a fix for CVE-2014-0224. We used Safety Net to instrument the patch for this vulnerability to detect attempted exploitation against clients that had been patched. As with the SSLv3 downgrade monitoring, our goal is to use client connections to determine whether there is evidence of large scale exploitation. This data does not make for an interesting graph: to date we have seen 6 instances of "in the wild" attempts at exploitation all targeting the same private messaging application. As this application has been updated to use the Google Play Services SecurityProvider, these attempts were unsuccessful. While we don't have visibility into attempts at exploitation against all clients, this data suggests that there has not been large scale exploitation of this issue.

Our goal is to use client connections to determine whether there is evidence of large scale exploitation.

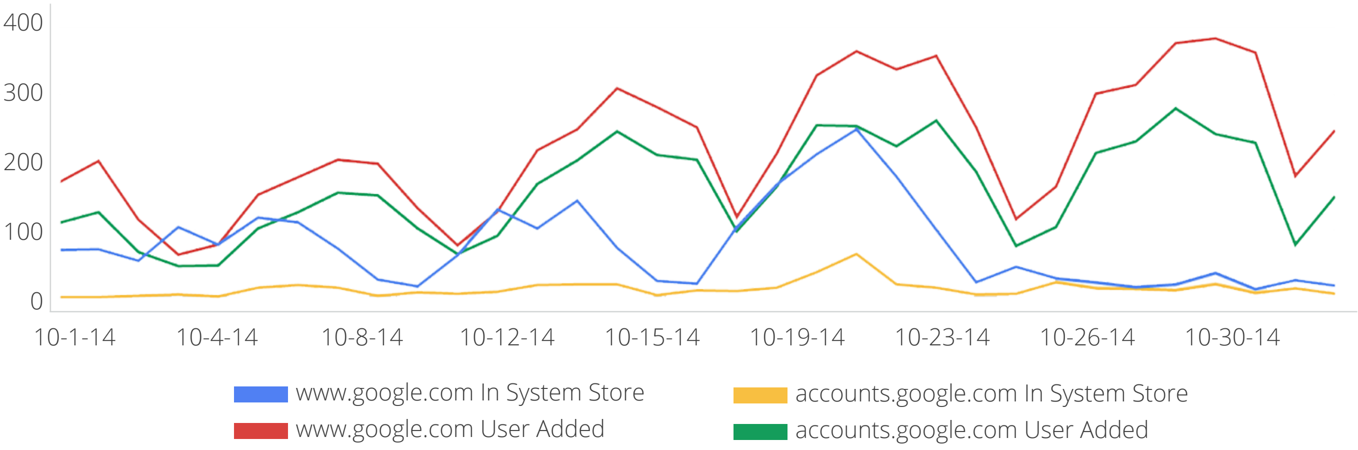
CA Man In The Middle

Certificate pinning and blacklisting were introduced in Android 4.2 to provide a mechanism for responding to potential compromises in the CAs that are installed by default on Android devices.

Starting with Android 4.4 and greater, Android began to display a warning to users if a certificate was installed locally on the device that could allow interception of SSL traffic.

Starting in October 2014, Safety Net has used active network probes to identify cases where the CA system is manipulated. Safety Net detected several hundred instances each day where users have installed a local certificate to Man-in-the-Middle network connections to Google services. We have seen a small number of instances of devices that have been compromised and had a certificate installed into the system CA (this avoids the security warning to users). All instances that we have seen appear to be part of "enterprise" security efforts. At this time, we have not detected any MiTM efforts that we would classify as "malicious".

Observed Instances of Local MiTM of Google Services



Safe Browsing Statistics

In 2014, Safe Browsing was enabled for Google Chrome on Android when using network compression. This service provides protection against a wide range of potential browser based security issues including websites that attempt to deliver PHAs and websites that attempt to exploit browser vulnerabilities. Safe Browsing checked billions of page views per day during the period and on average, users were warned about a potential security issue affecting 1250 out every 1 million user sessions. Of those, nearly all warnings are for attempted delivery of a PHA -- these users will have received a warning in Safe Browsing and chosen not to install the application. Safe Browsing checked billions of page views per day during the period and on average, users were warned about a potential security issue affecting 1250 out every 1 million user sessions. As noted previously, there are likely to be some attempted exploitations that are not detected by SafeBrowsing but so far widespread attempted exploitation of browser vulnerabilities has not been observed.

Safe Browsing checked billions of page views per day during the period and on average, users were warned about a potential security issue affecting 1250 out every 1 million user sessions.