Avast
Threat Report
2015

QUARTER 1

Contents

Executive summary

The Avast Virus Lab analyzes, researches, and provides real-time threat intelligence based on data received daily from nearly 230 million sensors worldwide. We stream more than 250 micro-updates to active devices every day to prevent attacks. By protecting more devices than any other security provider, we have the best insight into the threat landscape. This also means we not only keep up with the latest security threats, but stay ahead of them. This translates into better protection for our customers.

In Q1 2015, Avast researchers ventured out of the office and traveled to nine cities on three continents to research the security of public Wi-Fi networks. The project's results found that users around the world are prone to Wi-Fi attacks; in Asia even more than in Europe and the U.S.

In terms of threats, Romania was the most targeted country, with a 54 percent chance of users encountering PC threats. Nearly one out of every three PC users in the United States and Great Britain were targeted with PC threats.

Within the mobile sphere, China was targeted the most, which is most likely due to the fact that the Google Play Store is blocked in the region. Potentially unwanted programs (PUPs) including adware dominated the top 10 Android detections.

Additionally in Q1, the steady evolution of ransomware targeting mobile devices and PCs has shown that this fairly simple way for malware authors to profit remains as an invaluable and feasible option.

Stories

- It's called PUBLIC Wi-Fi for a reason
- Ransomware on steroids

It's called PUBLIC Wi-Fi for a reason

Global Wi-Fi experiment

Avast mobile security experts traveled to nine cities in the United States (San Francisco, Chicago, New York), Europe (Barcelona, London, Berlin), and Asia (Seoul, Hong Kong, Taipei) to observe public Wi-Fi activity. Each expert was equipped with a laptop and a Wi-Fi adapter with the ability to monitor Wi-Fi traffic in the area. For this purpose, we developed a proprietary app, monitoring the wireless traffic at 2.4 GHz frequency. It's important to mention that there are commercial Wi-Fi monitoring apps like this available in the market that are easy-to-use and free of charge.

Our observations revealed major security flaws in Wi-Fi hotspots and showed how easy it is for hackers to see browsing activity, searches, passwords, videos, emails, and other personal information. While security issues were found in all cities, the experiment showed that users in Asia are more prone to attacks than users in Europe and the U.S. Users in Berlin and San Francisco were most likely to take steps to protect their browsing.

Open Wi-Fi

Asian cities proved to have the most open Wi-Fi networks with an average of 42.3% of Wi-Fi networks being public, followed by the U.S. (31.7%) and Europe (28.5%).

Percentage of open Wi-Fi networks

1) Taipei: 43.6 percent
2) Hong Kong: 42.9 percent
3) Seoul: 40.4 percent
4) Chicago: 39.0 percent
5) London: 33.3 percent
6) New York: 33.1 percent
7) Berlin: 26.3 percent
8) San Francisco: 24.9 percent
9) Barcelona: 24.3 percent

HTTP Browsing

Our experiment also shed light on the fact that a significant portion of users browse primarily on unsecured HTTP sites while connected to open Wi-Fi networks. HTTP traffic is not encrypted and therefore unprotected, meaning that our team was able to view browsing activity, including domain name and page history, searches, personal log information, videos, emails, and comments. For example, it was possible for the Avast researchers to see products that a user browsed on eBay while not being logged in to the site as well as articles that people read on Wikipedia.

Nearly half of the web traffic in Asia takes place on unprotected HTTP sites, compared with one third of U.S. traffic and roughly one quarter of European traffic. This is most likely attributed to the fact that there are more websites in Europe and the U.S. that use the HTTPS protocol. In order to improve protection, HTTPS browsing is strongly recommended to users, as it is encrypted and thus more secure.

Weak encryption

The majority of the Wi-Fi hotspots observed in this experiment were protected, but Avast found that often their encryption methods were weak and could be easily hacked. Using WEP encryption can be nearly as risky as forgoing password protection altogether, as users tend to feel safer entering their personal information, but their data can still be accessed. San Francisco and Berlin had the lowest percentage of weakly encrypted hotspots, while more than half of password-protected hotspots in London and New York and nearly 70 percent of Asian hotspots were vulnerable to attack.

Percent of weakly encrypted routers

1) Seoul: 70.1 percent
2) Taipei: 70.0 percent
3) Hong Kong: 68.5 percent
4) London: 54.5 percent
5) New York: 54.4 percent
6) Chicago: 45.9 percent
7) Barcelona: 39.5 percent
8) Berlin: 35.1 percent
9) San Francisco: 30.1 percent

Ransomware on steroids

During Q1, we saw both PC and mobile ransomware evolve. Ransomware is a term for applications that lock your device or files and then demand a ransom payment for the unlock key.

PC Ransomware

CryptoWall, which originally appeared in November 2013, made its second comeback in January as CryptoWall 3.0. CryptoWall is typically distributed through drive-by download attacks by exploiting outdated vulnerabilities, via spam campaigns, or through malware that has already been installed on a compromised system. When executed, the ransomware searches for files with specific extensions, such as images, documents, and source code-files that are important to most users. The ransomware encrypts the files with a strong cipher (RSA 2048) and demands a ransom payment from the victim to decrypt the files. The ransom is typically around five hundred U.S. dollars and is paid in BitCoin to ensure anonymity. Once the payment is made, instructions to decrypt the files are sent to the victim.

The latest version of CrytpoWall differed from the second version in that it switched from using TOR to using I2P (Invisible Internet Project) to communicate with the command and control (C&C) server. This switch was most likely caused by the fact that TOR is now well known and can be blocked by network admins, whereas I2P is a lesser-known anonymization network. The original version of CryptoWall did not feature anonymization networks.

Additionally, a variant of ransomware called TeslaCrypt targeted gamers of more than 20 different games, including World of Warcraft, League of Legends and Call of Duty.

Mobile Ransomware

Simplocker is mobile ransomware that first appeared in June 2014, infecting more than 20,000 unique users. Simplocker reappeared in February 2015, emerging in a form more sophisticated than its first. The new variant of Simplocker uses asymmetrical cryptography, making it impossible to recover encrypted data without accessing the C&C server.

Statistics

- Threat levels by country
- Detections
- Exploits
- Operating Systems

Threat levels by country

The threat levels by country vary greatly between PC and mobile. Romanians have the greatest chance of encountering a PC infection. However on the mobile side, Chinese are the most targeted. We are not very surprised to see that China is highly targeted with mobile threats – according to the official China Internet Network Information Center, 83 percent (527 million) of China's Internet users access the Internet via a mobile device.

PC

Hackers targeted Romania, Turkey and Vietnam more than any other countries with PC malware in Q1.

Romania was targeted the most, with a 54 percent chance of encountering an infection. The threat levels for Avast's biggest markets were much lower than this, yet still significant:

- 41 percent Russia
- 37 percent Spain
- 34 percent Brazil and France
- 29 percent Germany
- 28 percent United States and United Kingdom

Figure 1 depicts the PC threat levels of each country. The threat level indicates the percentage of devices that have encountered an infection in Q1.

PC Threat Levels by Country

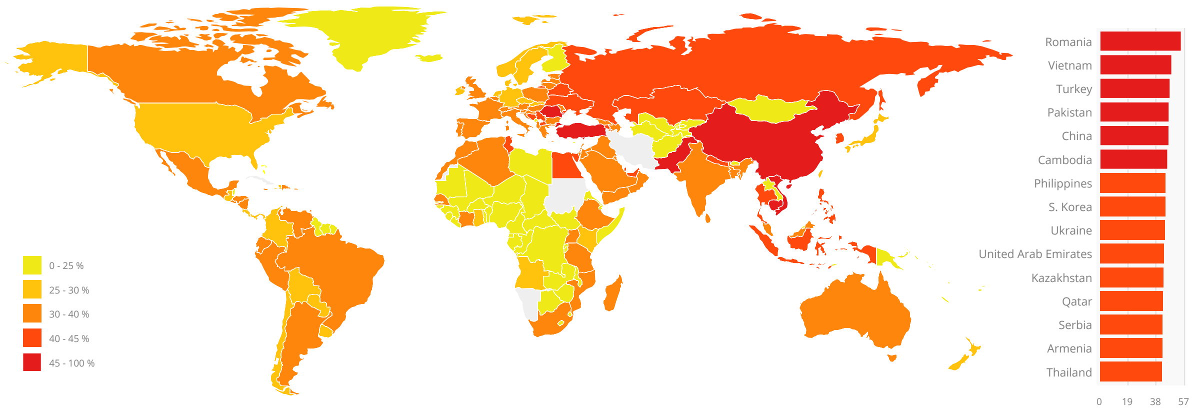

FIGURE 1 - PC Threat Levels by Country

Mobile

China, Romania, and Malaysia reported the most encountered mobile infections. This is likely due to the popularity of third-party app stores in these countries, especially in China, where the Google Play Store is blocked.

The threat levels for Avast’s biggest markets were much lower:

- 21 percent Russia
- 16 percent Spain
- 12 percent United States
- 10 percent Brazil
- 8 percent France and United Kingdom
- 6 percent Germany

Figure 2 depicts the mobile threat levels of each country. The threat level indicates the percentage of devices that have encountered an infection in Q1.

Mobile Threat Levels by Country

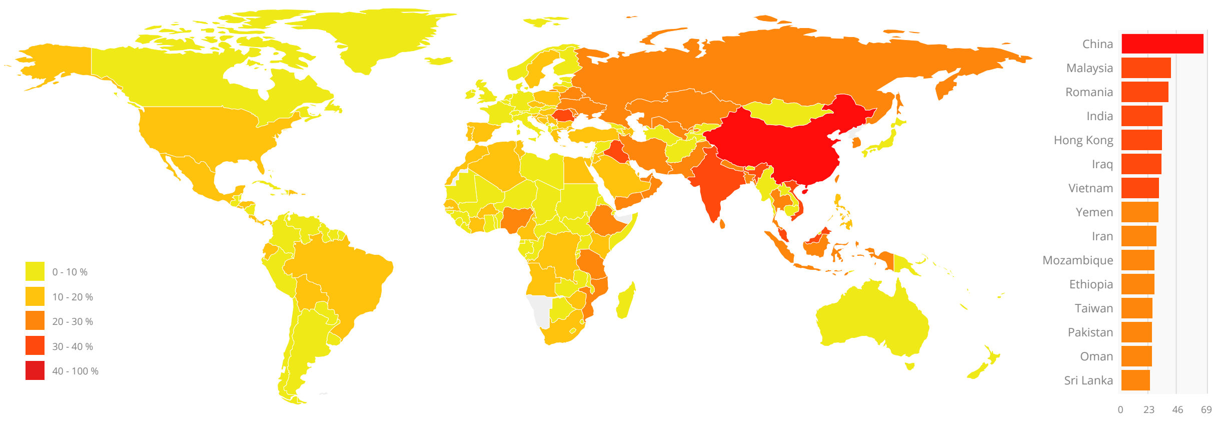

FIGURE 2 - Mobile Threat Levels by Country

Detections

Nearly 230 million people worldwide use Avast products, allowing us to stay ahead of the curve, as users act as sensors that automatically send malware and suspicious file activity to our virus lab for detailed analysis. As a result of our feedback loop, the Avast Cloud engine is constantly updated with the latest threats, providing users with real-time protection. We call this global sensor network our Community IQ.

Domains

Figure 3 shows the number of infected subdomains belonging to top-level domain names that were reported in Q1. Most reports came from .com domains, which is due to the number of infected subdomains.

One of the reasons why this number is so large is that malware authors use a technique called domain rotation to avoid domain blacklisting. Domain rotation regularly creates new domains and subdomains and redirects malicious traffic to them, exploiting the fact that it takes time for antivirus software to find these new domains, check them and release new detections, if necessary. Avast uses advanced algorithms to recognize domain rotations and immediately blocks infected subdomains before they can cause any harm.

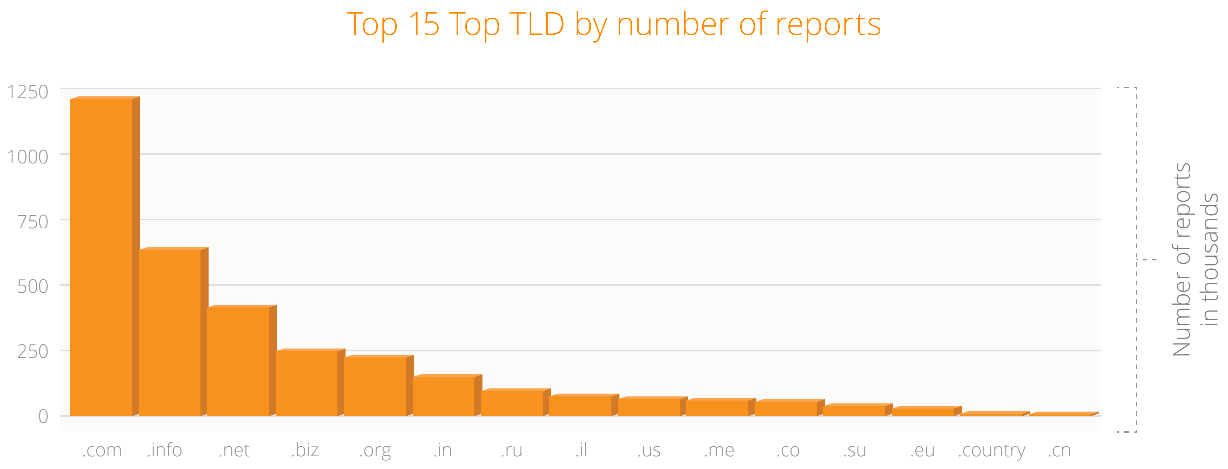

FIGURE 3 - Top 15 TLD by Number of Reports

URL Detections

The Avast Web Shield protects Internet-connected devices from malicious software while browsing the web and downloading files. While the user surfs online, Avast detects and blocks known and potential threats, such as hacked web pages and pages containing malicious scripts.

Figure 4 shows the number of unique users Avast protected from web-based malware in Q1.

The Avast Virus Lab receives more than 300,000 samples of new potential viruses every day. We verify these potential viruses and when confirmed as malicious, we add them to our virus database.

Due to the high number of samples we receive, false positives can occasionally occur. There is no way to avoid false positives completely, but we do our best to avoid them at all costs and to limit their impact. The peak on January 25 that can be seen in Figure 4 was caused when an e-shop was wrongly detected as malicious. The detection was disabled after a few hours.

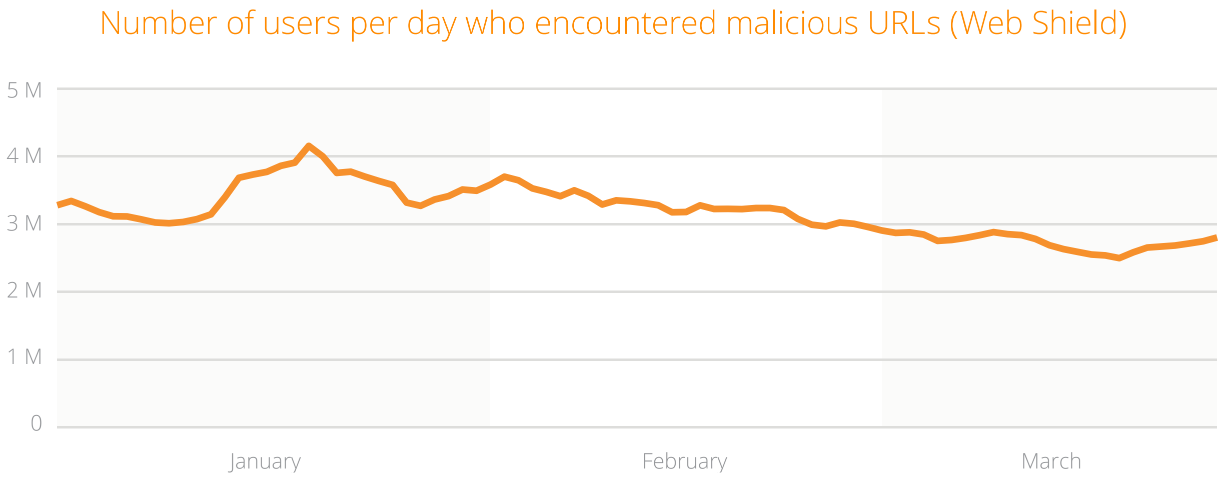

FIGURE 4 - Number of users per day who encountered malicious URLs (Web Shield)

File Detections

The Avast File Shield checks all programs the moment they are started and checks other files as soon as they are opened, as well as files downloaded using file sharing programs and files received over chat and instant messaging programs.

Figure 5 shows the number of unique users we protected in Q1 using File Shield. Apart from the seasonal and weekly fluctuations, there is just one major peak in February that was caused by a new version of a PUP.

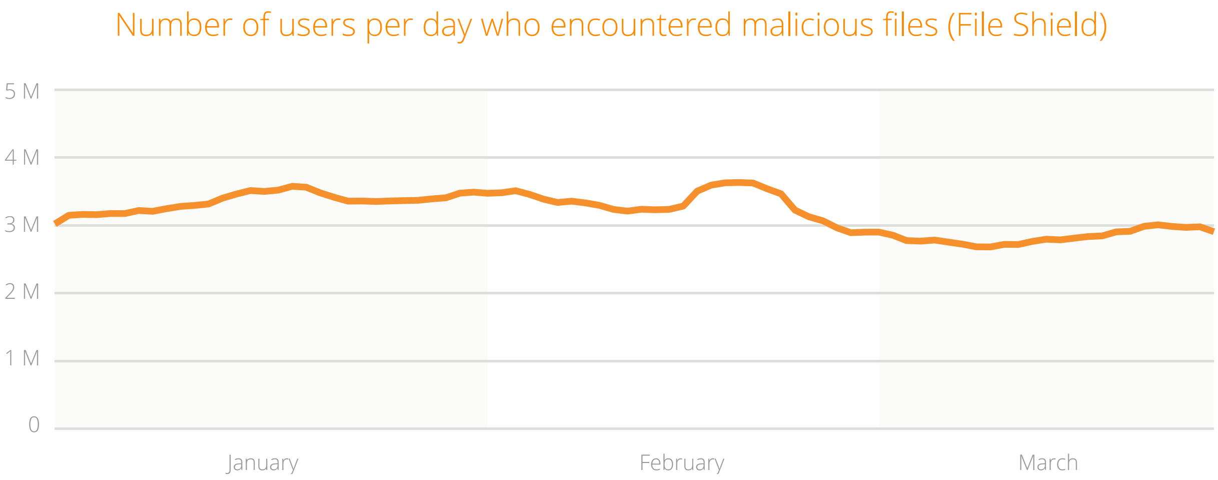

FIGURE 5 - Number of users per day who encountered malicious files (File Shield)

Top PC detections

The top 10 Windows PC detections reported were dominated by LNK detections. LNK files are used to create shortcuts that typically point to an executable file or script. The LNK files appear on your computer desktop as an icon, which is convenient for programs you frequently use. However, malware authors abuse LNK files to trick people into using malicious shortcuts.

Top 10 PC detections

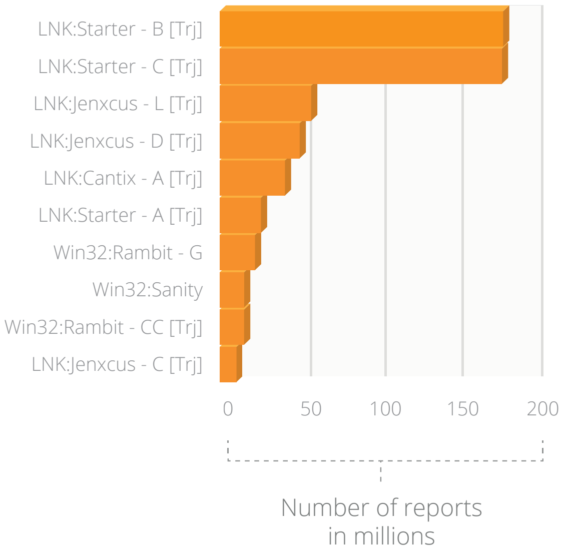

FIGURE 6 - Top 10 PC detections

Top Mobile detections

Mobile malware continued to grow dramatically, but Android is still fairly secure due to Google Play app restrictions and security.

The top 10 Android detections for Q1 consist mainly of PUPs, which include aggressive in-app advertising. App developers monetize their apps by displaying ads, but ad libraries can be abused and some leak personal data or bombard users with ads outside of the app.

The top two Trojans in the top 10 detections were capable of sending premium SMS, which was mainly targeted at Western European and Asian mobile users as carriers in these areas allow premium-rate SMS billing.

Top 10 Android detections

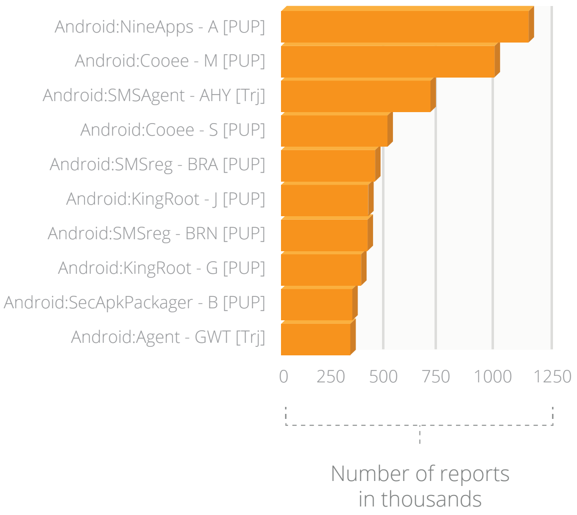

FIGURE 7 - Top 10 Android detections

Exploits

Exploits are an ever-present problem in computer security. Faults in application design or code can be exploited and are therefore security threats. Hackers target vulnerabilities in frequently used software and devices because it gives them a good chance of infecting a large numbers of users at once. Applications that hackers often target are browsers, Java, Adobe's Acrobat Reader, and office suites such as Microsoft office.

In January and February, we saw a large amount of JavaScript exploits. Two of the biggest security vulnerabilities that were exploited in Q1 were CVE-2013-2551 and CVE-2013-3882. CVE-2013-2551 targets JavaScript and can lead to remote code execution in Internet Explorer versions 6 to 10. CVE-2013-3882, on the other hand, targets an HTML parser in Internet Explorer 10 and if successful, the attack can lead to remote code execution. If the attack doesn't succeed, it can cause a denial of service.

The malware families from March in the "Other" chart in Figure 8 are mainly document macro exploits of vulnerability CVE-2006-2492 that use a buffer overflow attack and MIDI vulnerability CVE-2012-0003, which allows remote code execution via a crafted MIDI audio file.

Exploit types

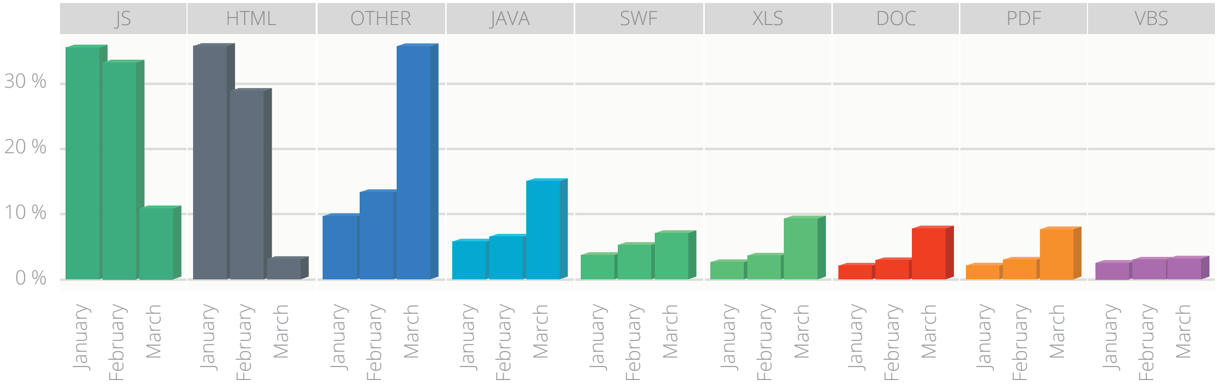

FIGURE 8 - Exploit types

Operating systems

Most used on PC

Within the Avast user base, we have seen a decline in Windows XP and Windows 8.0 in favor of Windows 8.1. Although official support of Windows XP ended almost a year ago, Avast continues to support the more than 10 percent of users using Windows XP. Windows 7 continued to be the most popular PC operating system, with 60 percent of Avast users using the OS.

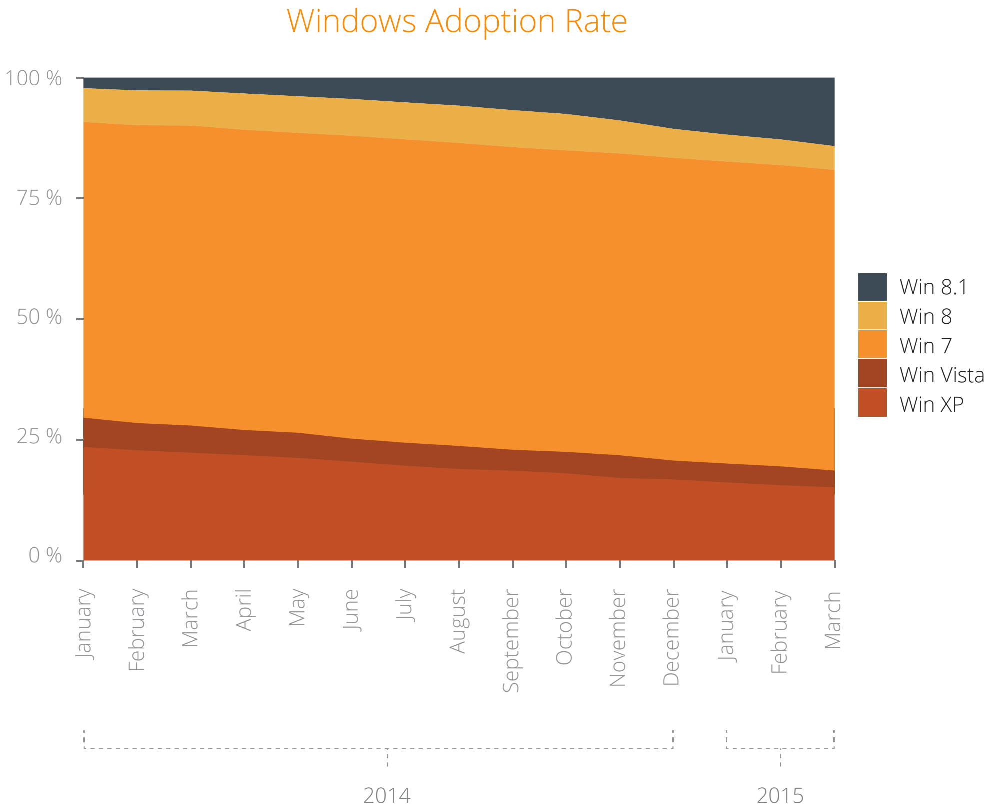

FIGURE 9 - Windows Adoption Rate

Most used on Android

Our mobile users' operating systems are much more diverse than PC operating systems. Many Android users do not use the latest version of the operating system, which can be attributed to one of two reasons. The first reason is that some vendors stick to older OS versions to ensure compatibility with their specific system tweaks, like custom user interfaces in Samsung's TouchWiz or system applications like calendars and dialers. The second reason is that not all older phones are capable of supporting newer operating systems due to lack of memory or computational power.

Within the Avast user base, six percent of users still use Gingerbread (2.3), which was followed by Ice Cream Sandwich (4.0) in October 2011. We are happy to see that versions older than KitKat (4.4) are slowly but steadily decreasing in favor of KitKat (4.4) and Lollipop (5.0). The more up-to-date the operating system, the safer it is, as security bugs are corrected with every version.

Android adoption Rate

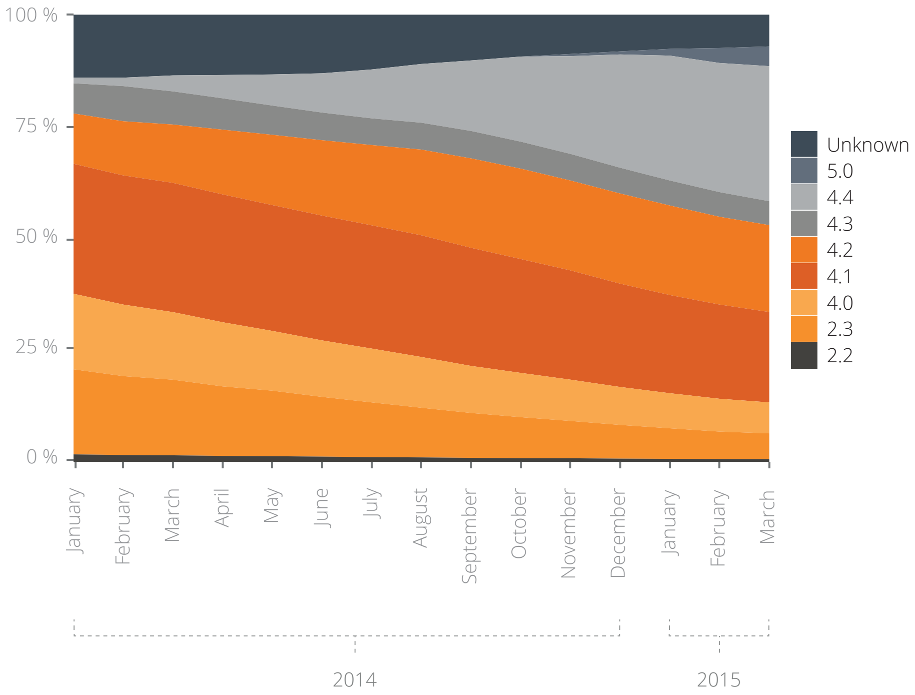

FIGURE 10 - Android adoption Rate

About Avast

Avast Software (www.avast.com), maker of the most trusted mobile and PC security in the world, protects 230 million people, mobile devices, and computers with its security applications. In business for over 25 years, Avast is one of the pioneers in the computer security business, with a portfolio that includes free antivirus for PC, Mac, and Android, to premium suites and services for both consumers and business.

In addition to being top-ranked by consumers on popular download portals worldwide, Avast is certified by, among others, VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, and West Coast Labs.