September 2016

WEBROOT®
Smarter Cybersecurity™

Webroot Quarterly Threat Update

by Grayson Milbourne | Webroot Security Intelligence Director

Introduction

Webroot solutions and services continually correlate intelligence from millions of real-world endpoints and internet sensors to identify key threat topics and trends, but what do the numbers really mean? In this report, we'll examine trends in malware ranging from 2014 through the first half of 2016, as well as their causes.

Notable Findings

Drop in overall malware encounters

Users are over 20 percent less likely to encounter malware and other undesirable executable files than they were in 2015. However, attacks from malware are more sophisticated and short-lived.

Google and Wells Fargo are heavily targeted

When it comes to new phishing attacks, Google and Wells Fargo are the most targeted technology and financial companies, respectively. Wells Fargo was targeted over 10 times as often in June as it was in January.

Mobile app epidemic

The number of new malicious Android® apps is expected to quintuple in 2016 compared to 2015.

Geoblocking outwitted

The United States now hosts over 40 percent of malicious URLs, while Germany's share of malicious URLs is increasing rapidly and China's share plummets.

Shifts in malicious IP origins

Nearly half of all malicious IP addresses are associated with China, India, or Vietnam.

The facts and figures presented in this report are all based on data collected by Webroot SecureAnywhere® endpoint solutions and Webroot BrightCloud® threat intelligence services. For previous threat data, see The Webroot 2016 Threat Brief: Next-Generation Threats Exposed.

Polymorphic Malware and Potentially Unwanted Applications (PUAs)

Each year, Webroot encounters hundreds of millions of unique executable files for the first time, and a sizable percentage of these were identified as malware or potentially unwanted applications (PUAs). Figure 1 shows these percentages over the past two and a half years. Malware's percentage has dropped from 3.4% to 2.8% since 2014. The change in PUAs is much more dramatic, plummeting from 12% in 2014 to only 4.5% for the first half of 2016. The most likely reasons for these changes continue to be the consolidation of PUA vendors and improved user awareness of getting software from trusted sites.

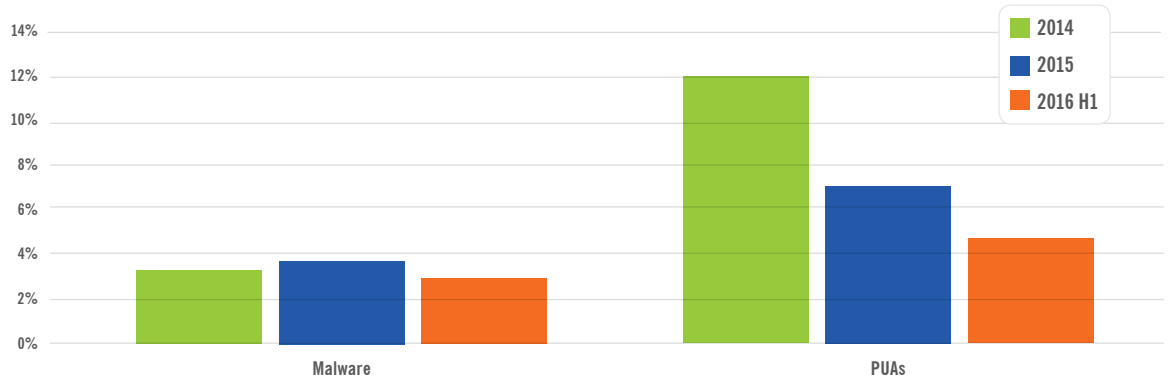

Figure 1: Malware and PUAs as a percentage of all newly observed unique executable files.

The drop in malware and PUAs as a percentage of new executables is not as important as the raw volume of malware and PUAs. Fortunately, that has also been declining. Figure 2 shows how the volume has changed since the beginning of 2014. With the 2014 monthly average depicted as 100 percent, the rest of the graph shows the 2015 monthly average, and then the actual monthly volumes for the first half of 2016. The graph makes it clear that there has been a significant decrease in the volume of malware and PUAs, with the most striking drop happening in April through June 2016. June's volume was only 38 percent of the average 2014 volume.

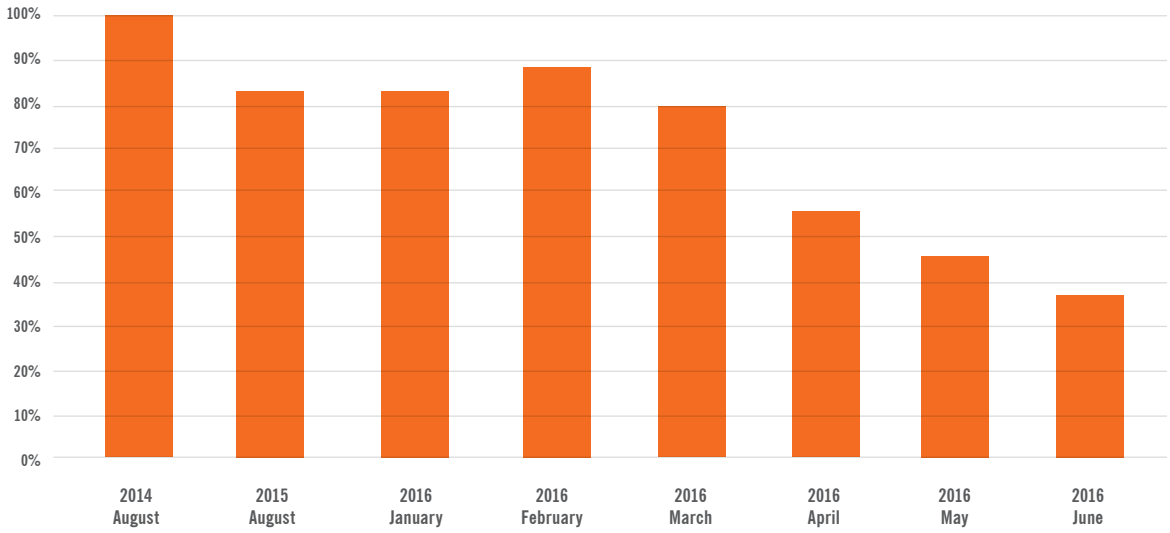

Figure 2: Monthly volume of malware and PUAs.

In accordance with the drop in malware and PUA volumes, the rates at which users encounter new, unique instances of malware and PUAs have also dropped:

» Malware from 1.6 instances per user in 2015 to an estimated rate of 1.35 instances per user in 2016, a drop of 16 percent

» PUAs from 3.0 instances per user in 2015 to an estimated rate of 2.2 instances per user in 2016, a drop of 27 percent

These lower rates mean that in general, Internet users are seeing fewer malware and PUA threats today than they did in 2014 or 2015.

A related statistic indicates that the number of variants within each malware or PUA family is also continuing to drop sharply. Figure 3 depicts the number of variants using lines. For malware, the average number of variants has fallen from 97 per family in 2015 to only 45 per family in the first half of 2016. The average number of variants within a PUA family has also gone from 263 in 2015 to only 176 in the first half of 2016. As variants per family have decreased, the number of malware and PUA families has sharply increased, shown by the columns in Figure 3. Note that the 2016 columns are estimates for the year based on the counts from the first half of 2016. The data shown in this graph indicates that attackers are being forced to create new families as the life span of each family and its polymorphic variants continues to get shorter.

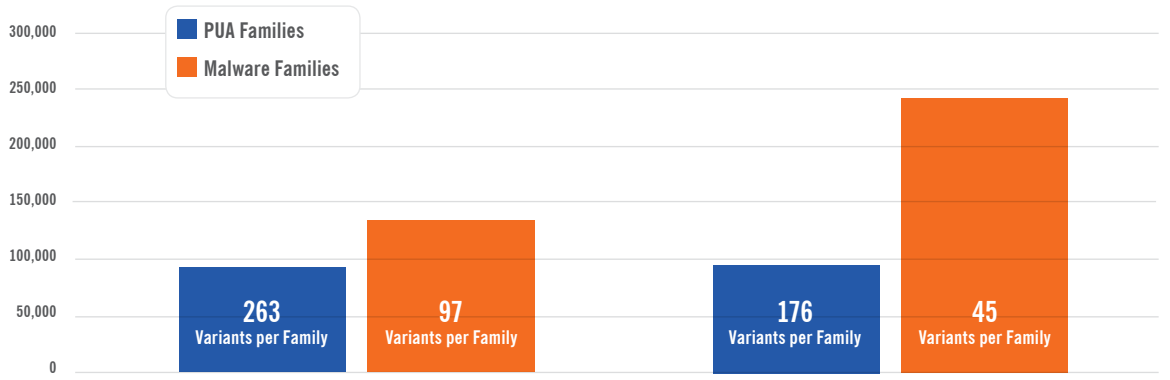

Figure 3: Malware and PUA families and variants per family.

IP Addresses

Webroot constantly updates a blacklist containing millions of known malicious IP addresses. On average Webroot adds over 85,000 addresses and removes around 89,000 addresses every day. These rates have stayed roughly the same over the past few years. The rapid rate of change in the IP address blacklist indicates how important it is to use a continuously updated blacklist to stop activity from malicious IP addresses and to reduce false positives by recognizing when malicious IP addresses have become benign.

Figure 4 shows the percentages of non-spam, malicious IP addresses by country of origin for the top 10 countries, with all other countries together (more than 200) represented by the "other" category in the upper left corner. As this shows, the top 10 countries comprise nearly three-fourths of all malicious IP addresses, with the top three, China, India, and Vietnam, being the source of nearly half of all malicious IP addresses.

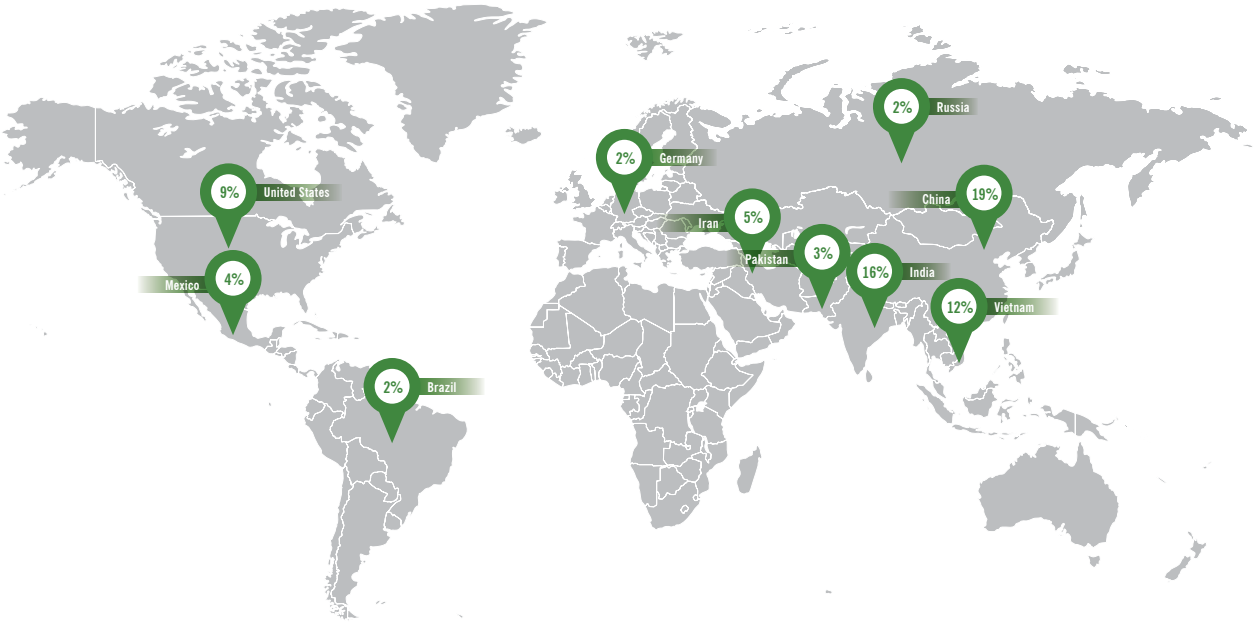

Figure 4: Top 10 threat IP origin countries.

Analyzing the nature of these malicious IP addresses shows that approximately 92 percent of them are associated primarily with spam generation. When spam generation is omitted, the most prevalent threat types are scanners (55 percent) and proxies (42 percent), with phishing, web attacks, and other types of threats only comprising a total of 3 percent. These percentages are all nearly identical to those from 2015, showing a great deal of stability in what these malicious IP addresses are being used for.

Malicious URLs

Webroot continuously monitors URLs and assesses their reputations. Webroot has identified over 9 million new malicious URLs in the first six months of 2016. Approximately one third of those malicious URLs were associated with a particular host country. Figure 5 shows the countries known to have hosted the most malicious URLs in 2015 and the first half of 2016. The United States had the largest net change in malicious URL hosting, increasing from 30 to 42 percent. However, other countries had more dramatic changes during this short time period. For example, Germany increased from 4 percent in 2015 to 13 percent in the first half of 2016. China, meanwhile, dropped from 11 percent in 2015 and only 3 percent in the first half of 2016. Most other countries shown in Figure 5 had larger percentages in 2016, leading to a large drop in the Other category, from 42 percent all the way down to 24 percent.

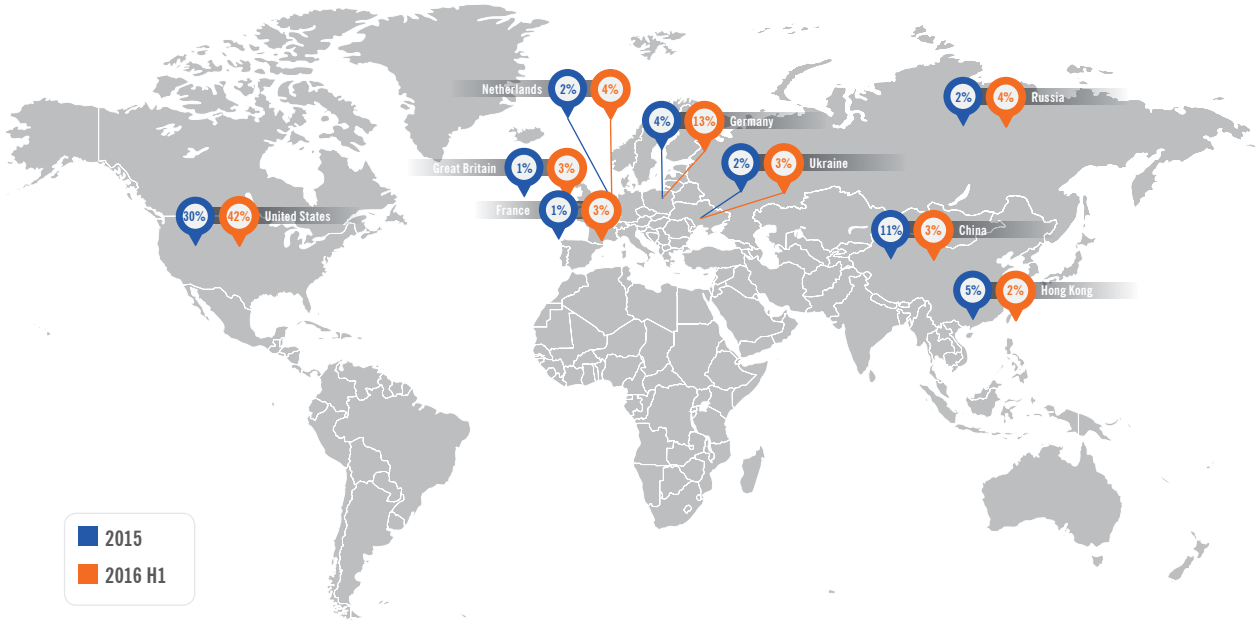

Figure 5: Countries hosting the greatest number of malicious URLs

The most likely explanation for the United States continuing to dominate malicious URL hosting is that the U.S. is unlikely to be targeted by geofiltering services. Such services are configured to block network traffic involving certain geographic regions. The United States hosts so many legitimate websites that it is counterproductive to attempt to block all traffic to and from the United States. This underscores the importance of leveraging both URL reputation filtering and IP address filtering in conjunction.

Phishing

In addition to analyzing URLs to determine if they are associated with general malicious behavior, Webroot looks for new phishing URLs, also known as zero-day phishing URLs. Figure 6 shows the unique zero-day phishing URLs by month since the beginning of 2016. There was a 74 percent increase in the average monthly count from the first quarter to the second quarter of 2016. Webroot's careful analysis of the data showed that this increase is mostly attributable to a phenomenon known as polymorphic URLs. This method is employed by "phishers" who generate thousands of slightly different phishing URLs at once as part of a single phishing campaign. The idea behind this method is to make it harder for traditional defensive technologies to stop all the phishing attacks because of their varying characteristics.

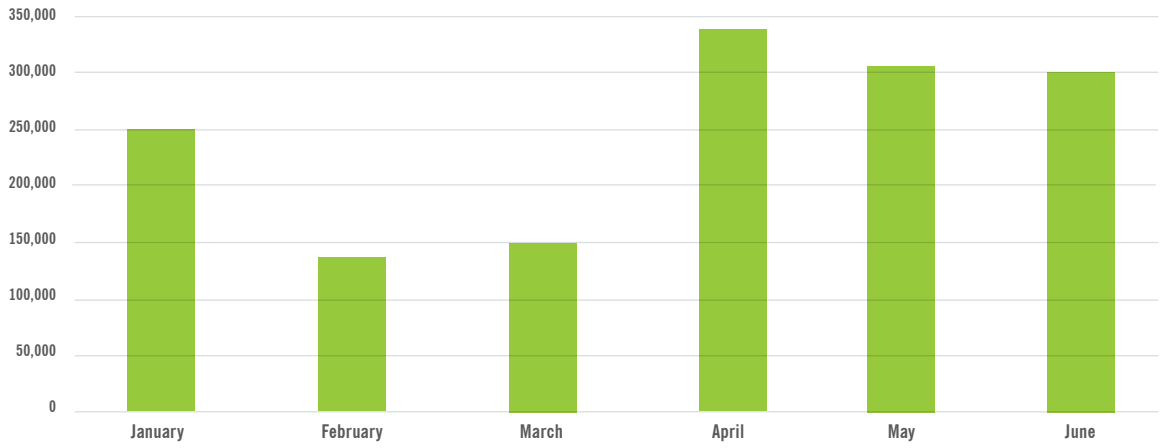

Figure 6: Unique zero-day URLs by month

Webroot identified the ten companies most often targeted by unique zero-day phishing URLs during the first half of 2016. Six of these companies are technology firms and four are related to finance. Figure 7 shows the monthly unique new phishing URL counts for the technology firms. In January, Google had around 9,000 new URLs, and Facebook was a close second with over 6,500. Their February numbers were almost equal, but starting in March, they trended in opposite directions. By June, Google had over 25,000 new URLs in that month alone, a higher count than the other five technology companies combined, while Facebook had fallen to fifth among the technology companies with only around 1,600 new URLs. The sharply increased counts for Google are primarily due to the use of polymorphic URLs, thousands of sites with small variants from a single IP address, for phishing campaigns.

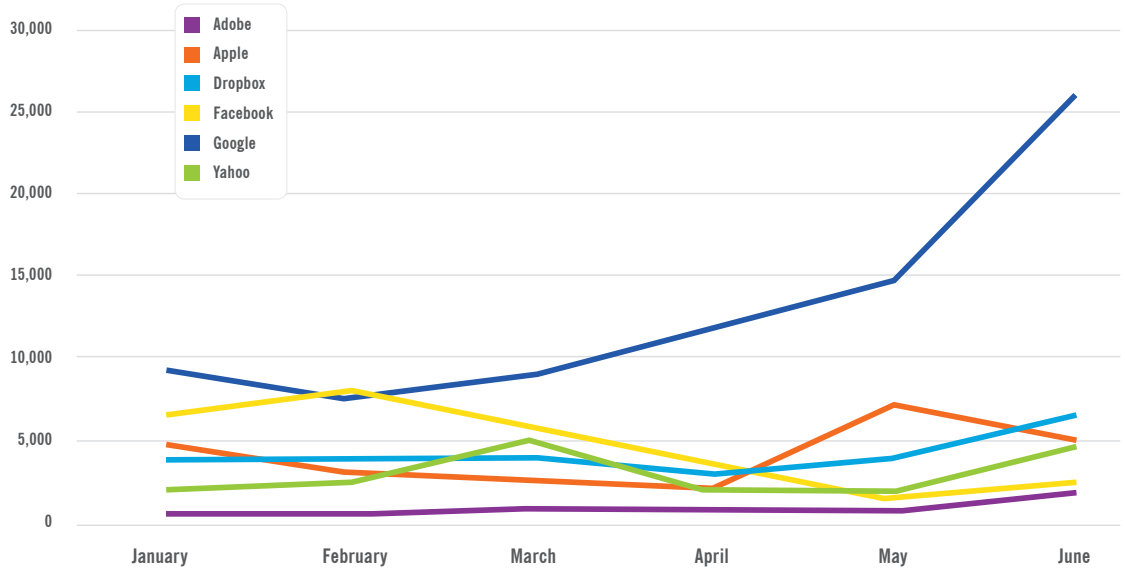

Figure 7: Technology companies with the most unique zero-day phishing URLs.

Figure 8 shows the monthly counts for the four financial companies in the top ten. From January through May, Paypal and Wells Fargo switched positions every month. However, in June there was a dramatic increase in Wells Fargo's counts, from under 2000 in May to nearly 24,000 in June. Note that the June count for Wells Fargo is almost as high as the June count for Google. The explanation for the Wells Fargo increase is the same as the reason for the Google increase: phishers are shifting to polymorphic URLs to target numerous users at once while avoiding detection by traditional methodologies.

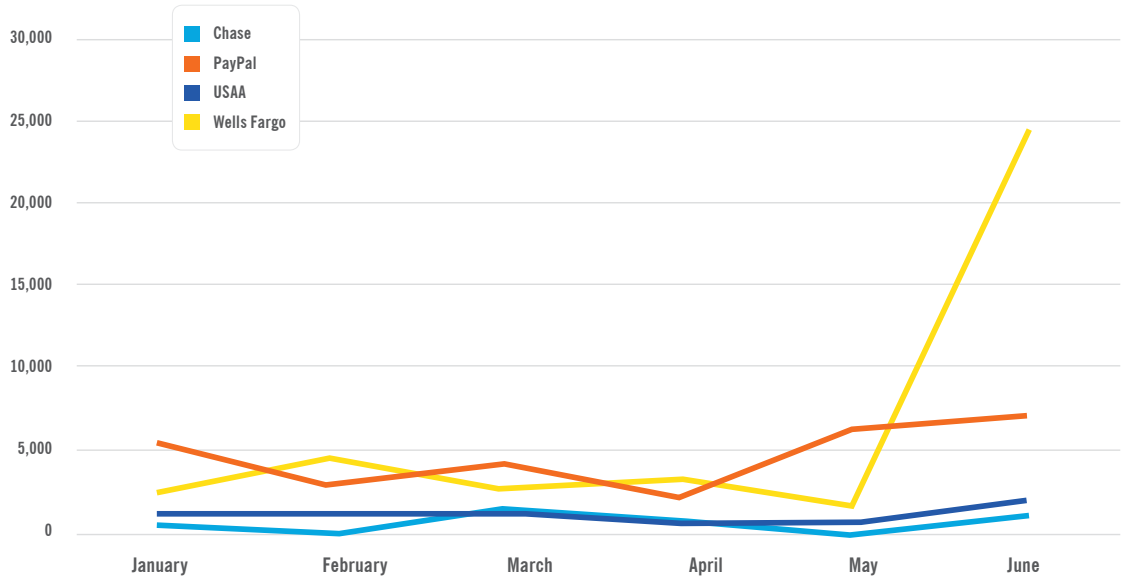

Figure 8: Financial companies with the most unique zero-day phishing URLs.

Malicious Apps for Android® Devices

In 2015, Webroot identified over 5 million new Android apps. In just the first half of 2016, Webroot identified over 7 million new Android apps; at that rate, there will be 300 percent as many new Android apps in 2016 than 2015.

Unfortunately, the number of new malicious Android apps is increasing even faster than that. Figure 9 shows how the distribution of app reputations has changed during the past few years. In the first half of 2014, just over 10 percent of new apps were malicious. In the first half of 2016, that has risen to almost 45 percent. Similarly, the percentage of new apps considered benign has dropped from 27 percent to 14 percent during the same time period.

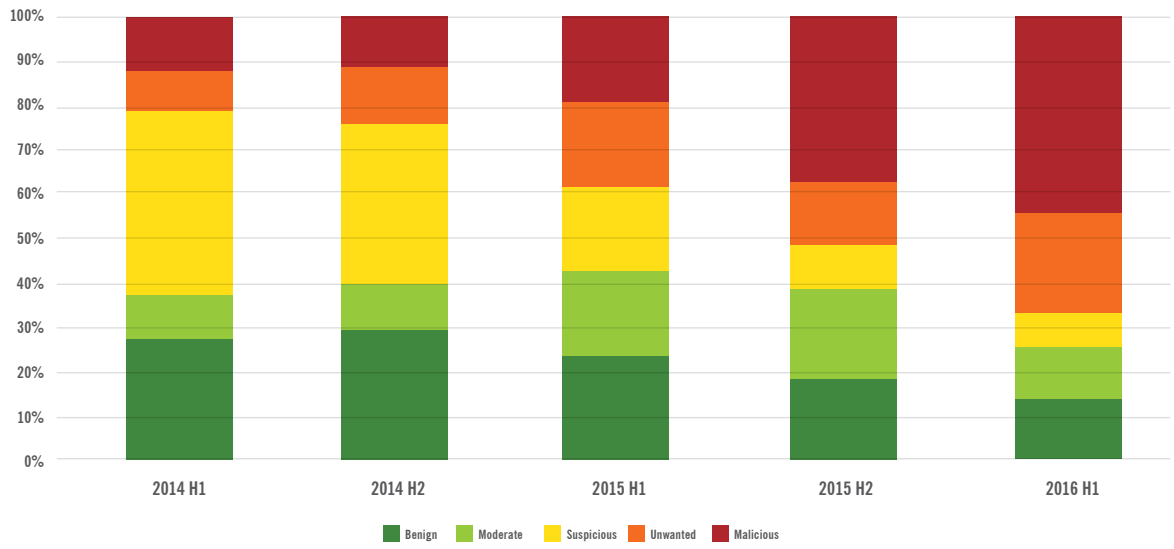

Figure 9: Distribution of Android app reputations.

The implications of the huge increase in the number of new Android apps and the continuing growth of new malicious Android apps are incredible. The raw number of new malicious Android apps is on track to increase by almost 400 percent. These malicious apps are mainly targeting Asian countries. The most likely reasons for this are threefold:

1. Android devices are more prevalent in many Asian countries than elsewhere.
2. Many people in Asian countries use their Android devices for all their online activities, rather than a desktop or laptop computer, making Android devices more valuable targets.
3. Many Android users in Asian countries download their apps from unofficial app stores instead of Google Play. Unofficial app stores' evaluation processes are rarely as robust as Google Play's, which increases the likelihood their users will download malicious apps.

Figure 10 shows the breakdown of malicious mobile apps by type since the beginning of 2014. Three trends are the most noteworthy:

» The percentage of malicious mobile apps classified as Trojans has significantly dropped. The average in 2014 was 77 percent, but this dropped to 60 percent in 2015 and is down to only 56 percent in the first half of 2016.

» The percentage of malicious mobile apps classified as adware or PUAs has skyrocketed. From comprising barely 10 percent of malicious apps in 2014, adware and PUAs shifted to 28 percent in 2015 and so far in 2016 are over 35 percent.

The percentage of rootkits has dropped so much since 2014 that it is not visible on the 2015 or 2016 bars. However, this can largely be explained by a sharp increase in adware containing rootkits instead of rootkits being used alone.

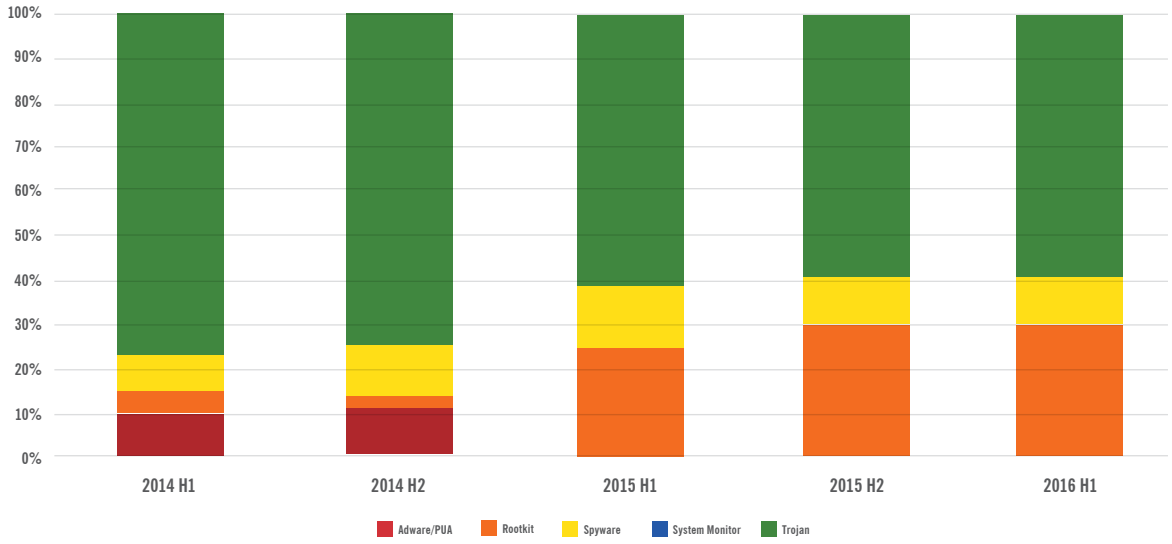

Figure 10: Malicious mobile apps by type.

Even with the percentage of some malicious mobile app types dropping significantly or being so small as to not appear in Figure 10, all five types are expected to have increases of at least 100 percent in their raw volume from 2015 to 2016, with Trojans on pace for 325 percent growth and adware/PUAs on track for astonishing growth of over 500 percent. It is worth noting that many of these new malicious mobile apps are targeting version 4 or earlier of the Android operating system, which means older Android devices are at greatest risk from new malicious mobile apps.

Another analysis of the nature of malicious mobile apps is presented in Figure 11. This chart shows the relative percentages of these apps based on six categories: Tools, Games, Entertainment, Work/Business, Communications, and Other. The Tools category encompasses a wide variety of utilities, and while it may seem surprising that more malicious apps would be Tools than another category, consider that users might be more likely to accept permission requests from tools than games or other categories of apps. This would make apps in the Tools category more attractive for attackers because they could use them to gain a greater degree of access over mobile devices.

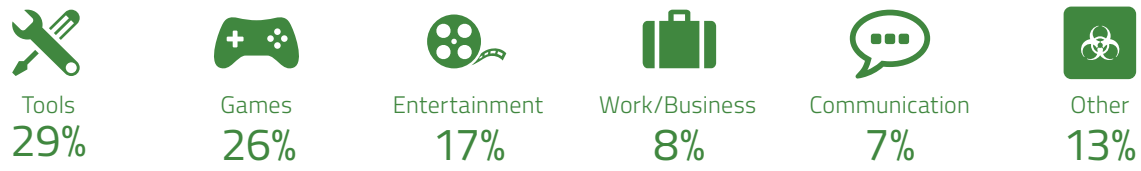

Figure 11: Malicious mobile apps by category.

Conclusion

Although the number of phishing attacks and overall malware encounters are decreasing, these statistics can be deceiving. Many attacks appear, inflict, and disappear within hours, even minutes, having stolen user credentials, corporate documents, and other sensitive information; launched a ransomware encryption, or found other means to achieve financial gain. As polymorphism continues to grow in prevalence and attack timelines speed up, it is more pressing than ever for organizations to adopt next-generation security approaches that can adapt and predict malware behaviors as they evolve.

About Webroot

Webroot delivers next-generation endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions and BrightCloud® Threat Intelligence Services protect tens of millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at www.webroot.com

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900