The Webroot 2016 Threat Brief

Next-Generation Threats Exposed

WEBROOT®
Smarter Cybersecurity™

Foreword

2015 was yet another record year for cybercrime, during which more malware, malicious IPs, websites, and mobile apps were discovered than in any previous year. It comes as no surprise that the cybercrime ecosystem continues to thrive, given new innovations and little in the way of risk for those who choose to participate. The continued onslaught of hacks, breaches, and social engineering scams targeting individuals, businesses, and government agencies alike has caused many in the security field to ask if it's truly possible to defend against a persistent attacker.

At Webroot, we believe it is possible to effectively protect enterprises and users, but only by understanding your adversary and the techniques they employ for their attacks. This insight enables Webroot research teams to finely tune defenses to identify attacks as they occur, while also neutralizing new threats by restricting access to the systems and networks they are trying to infect.

To defend against today's threats, intelligence must flow in real time from the systems that collect, analyze, and classify data to the endpoints and network appliances under protection. That's why Webroot provides up-to-the-second, highly accurate intelligence that outpaces the speed of cybercrime; that offers automatic, real-time protection to millions of users around the world; and continues to grow in breadth and efficacy with each new endpoint added.

Our approach and security solutions reflect our in-depth understanding of the threat landscape and how attackers think, to provide cutting-edge, proven next-generation protection and real-time detection of threats as they emerge. The Webroot 2016 Threat Brief shares a glimpse into the analysis and discoveries made by the Webroot® Threat Intelligence Platform to provide insights on key trends and risks seen by our users over the past year.

Hal Lonas
Chief Technology Officer

The Webroot Perspective

The Webroot® 2016 Threat Brief provides an overview of the internet threat landscape during 2015, spanning threats from websites, malicious IPs, malware, and mobile applications. This report focuses on identifying threat trends, including a comparison to those identified in the Webroot 2015 Threat Brief. The statistics presented in these reports are based on analysis of threat intelligence metrics automatically captured, analyzed and correlated across threat vectors by the Webroot® Threat Intelligence Platform, a big data security platform that acts as the backbone for all Webroot endpoint solutions and threat intelligence services.

Webroot endpoint solutions and threat intelligence services are powered by the Webroot Threat Intelligence Platform, which was purpose-built as a revolutionary approach to next-generation threat protection. This platform integrates billions of pieces of information from millions of real-world endpoints, globally distributed active and passive sensors, validated third-party databases, and leading security partners to create the world's largest cyber threat detection net (Figure 1). The intelligence produced by this platform is a critical component of Webroot SecureAnywhere® endpoint security products, and is also made available to Webroot partners through Webroot BrightCloud® Threat Intelligence Services.

This system provides proactive protection for users and networks against both known and never-before-seen attacks. Because Webroot maps this data across vectors, analyzing relationships between URLs, IPs, files, and mobile applications for greater insight and accuracy, Webroot is able to provide predictive risk scoring based on a guilt-by-association model. For example, an IP may seem benign when examined independently, but it may be connected to malicious IPs, URLs, files, or mobile apps, which would affect its reputation score within the Webroot platform. That IP's reputation score can indicate its likelihood that it will be involved in an attack, so it can be blocked preemptively through automated systems.

Figure 1. Webroot Threat Intelligence Platform

A key differentiator for Webroot is its unique approach to machine learning. Many security vendors use either Bayesian Networks or Support Vector Machine (SVM) models to populate work queues for human analysis, which aren't scalable or even particularly accurate. Webroot uses Maximum Entropy Discrimination (MED) for automated, highly accurate and scalable threat analysis, enabling classification of over 2,500 URLs per second.

The massive data processing capacity used in this platform, coupled with Webroot's proprietary implementation of the most advanced machine learning technology available and a powerful contextual analysis engine, has enabled the Webroot® Threat Intelligence Platform to:

» **Accurately monitor** the entire IPv4 space and in-use IPv6 addresses, to continuously update a dynamic list of approximately 12 million malicious IP addresses at any given time

» **Classify** and score billions of URLs and detect phishing sites in real time

» **Analyze** behaviors to classify over one million new files a day as seen across millions of Webroot customer endpoints

» **Assess** the risk of millions of mobile apps, including over 12 million new and updated apps in 2015

This intelligence helps to protect millions of consumers and businesses around the world, both directly and through a multitude of industry-leading security products from Webroot partners. Its powerful, real-time threat analysis platform also provides Webroot with an exceptional perspective on the threats facing customers. Thus, while it is primarily used to keep ahead of the exponential proliferation of threats facing companies and end users today, the Webroot team has also analyzed data from this platform to develop the overarching view of the threat landscape presented in this brief.

In addition to insights from the Webroot Threat Research team, this brief includes analysis and findings on the following:

» Polymorphic malware and potentially unwanted applications (PUAs)

» Patterns of IP addresses associated with malicious activity

» The value of classifying URLs and judging their reputations

» Trends in phishing target selection

» The increasing risks of mobile app security

Webroot Threat Intelligence by the Numbers

27+
Billion URLs

600+
Million Domains

4+
Billion IP Addresses

9+
Billion File Behavior Records

20+
Million Mobile Apps

10+
Million Connected Sensors

Polymorphic malware on the rise

Nearly all malware and potentially unwanted application (PUA) delivery uses polymorphism—either at the server level, where every executable generated is a unique variant, or the threat itself is polymorphic, making it unique to the recipient. This tactic poses a major problem to traditional security approaches, which struggle to discover singular variants, let alone do so in time to stop data breaches and other compromises.

The Webroot threat intelligence and discovery model was specifically designed to detect and prevent unique polymorphic executables. Webroot protects its customers from Windows malware and PUAs, such as spyware and adware, and also provides BrightCloud File Reputation intelligence to partners. In independent comparative analysis against leading competitors, Webroot SecureAnywhere® Business Endpoint Protection was the only endpoint security product in the group that protected against 100% of the malware tested within a 24 hour period.[1]

During 2015, Webroot saw hundreds of millions of new, unique executable files. Of these files, approximately 3.7% were determined to be malware, and 7.1% were identified as PUAs. Figure 2 shows the relative percentages of malware and PUAs among all observed executables for 2014 and 2015. Malware showed a small increase, but PUAs had a steep decline, down from 12% in 2014. The number of PUA vendors has dropped recently, and we believe this is driven, at least in part, by consumers being more diligent about installing applications from legitimate sources. Also, Google has changed their indexing policies so that searches for applications return the vendor site first, instead of other distribution points, helping to guide consumers to legitimate software sources.

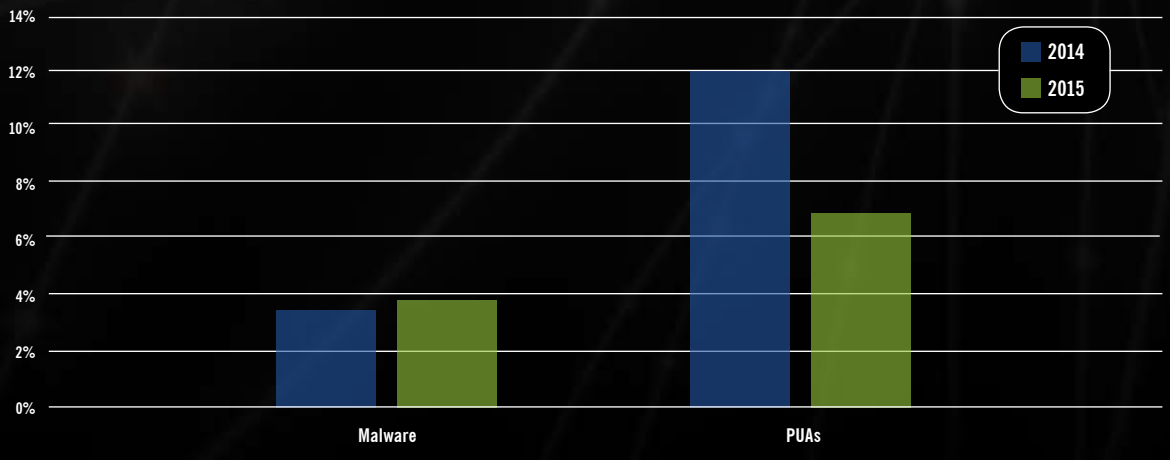

Figure 2. Malware and PUAs as a percentage of all observed unique executable files.

"Webroot SecureAnywhere Business Endpoint Protection Versus […]" MRG Effitas. January 2016. www.mrg-effitas.com/sponsored-tests

There were also major changes in terms of raw counts of malware and PUAs from 2014 to 2015. The number of new malware files increased by 29% from year to year, while the number of PUAs declined by 30% over the same time period. This indicates a significant shift in interest from PUAs to malware, although new PUAs are still roughly twice as common as new malware. It also shows a decline in malicious executables in general; the rate of growth in malware has historically been over 100% each year, so the 2015 rate of 29% marks a major decrease. The most likely explanation for this is that, in previous years, attackers were transitioning from traditional delivery models to polymorphic ones, which caused the apparent rate of change in malware to be inflated. Now that malware is almost purely polymorphic, attackers are replacing malware variants with other malware variants, instead of replacing one traditional malware instance with many polymorphic instances.

On average, each Webroot user encountered 1.6 new, unique instances of malware, and 3.0 new, unique instances of PUAs during 2015. This reflects the trends shown in Figure 2, with a slight increase in unique instances of malware from 2014 (from 1.3 to 1.6), and a sharp drop in unique instances of PUAs (from 4.6 to 3.0). Executable threats continue to emerge quickly and be highly customized and targeted. Observations from 2015 show that over 97% of malware encountered by Webroot customers was seen on only a single endpoint.

These numbers underscore the polymorphic nature of almost all malware today and how ineffective older, largely signature-based malware detection technologies have become. Organizations need to be aware of which applications are on each endpoint at all times so that malicious executables can be detected as quickly as possible.

Also worth noting is the sheer number of variations among malware and PUAs. In 2014, Webroot detected an average of almost 700 file instances per malware family, and nearly 30,000 file instances per PUA family. This suggests that, on average, an instance of malware was spread to far few users than an instance of a PUA. In 2015, the picture is dramatically different. The average file instances per malware family have dropped to less than 100, and the instances per PUA family have plummeted from nearly 30,000 to just over 260, suggesting strongly that attackers are now making their PUAs more difficult to detect, using polymorphic distribution models and rapid new variant generation to circumvent traditional detection methods.

Corresponding to this sudden increase in diversity is a similar spike in the number of malware and PUA family variants. Webroot identified over 14,000 malware family variants and over 1,000 PUA family variants in 2014; in 2015, the number of malware family variants jumped to over 130,000, and the PUA family variants increased by a factor of nearly 100, reaching well over 90,000.

One type of malware that has become particularly high-profile recently is ransomware, which typically encrypts a device and demands payment to reverse the encryption and restore access to files and device functionality.

Webroot threat researchers closely monitor the evolution of ransomware as it continues to increase, and have noted several significant trends during 2015:

» Attackers using ransomware are increasing their adoption of IP address anonymizing services, such as Tor, for ransomware delivery and cryptographic key provisioning for each affected host. Anonymizing services make it much more difficult to identify the individual or group behind a ransomware infection.

» Ransomware is becoming a commodity. Attackers can license ransomware from third parties, and there have even been attempts at selling ransomware-as-a-service to enable anyone to build and distribute their own ransomware.

» Ransomware varies widely in terms of technical sophistication. For example, some ransomware relies heavily on links to third-party libraries, making it much easier to detect. Other types, however, use thread injection, process hollowing, and other techniques to evade detection. CTB-Locker, for instance, uses a position-independent payload wrapper, making it nearly impossible to detect using traditional signature-based methods.

One of the most widely used forms of ransomware is CryptoWall. Since its initial release in early 2014, CryptoWall has been refined to make it stronger. For example, CryptoWall 3.0 performs cryptographic key management functions, generating unique encryption keys instead of using one key for all infections, and secures the master encryption key itself to prevent unauthorized access to it. CryptoWall 3.0 also uses IP address anonymization services to conceal the location of the servers containing the decryption keys and payment mechanisms. In late 2015, CryptoWall 4.0 was released, with numerous enhancements to help sidestep security software.

Around the same time, the first JavaScript-based ransomware was released. Known as Ransom32, this emergence could have a profound impact on ransomware in the coming year. Because Ransom32 uses JavaScript, it could easily be adapted for numerous platforms, including some that have not been widely targeted before, such as Linux and Mac OS X.

In addition to ransomware, organizations are also becoming increasingly concerned about adware. Adware is widely used, and, in many cases, it makes hidden modifications to the operating system. These modifications often affect the DNS application programming interface (API) that translates domain names into IP addresses. For example, when a user requests an address for a site, such as google.com, the adware intercepts the request and returns an address for a site controlled by the attacker. During 2015, approximately 15% of the adware examined by Webroot threat researchers exhibited malicious behavior, including DNS poisoning. These techniques are used for adware on multiple platforms, including Windows and Mac OS X.

Ransomware, malicious adware, and other malicious software pose a major threat to organizations. Although many have focused primarily on Windows hosts to date, there is increasing evidence that malware creators are expanding their attacks to target Mac OS X and other hosts.

More IP addresses to launch attacks

Automatically blocking inbound traffic from malicious IP addresses can be one of the most effective methods to prevent attacks. Webroot actively monitors the entire IPv4 space and in-use IPv6 to provide a dynamic list of high-risk IP addresses to protect Webroot customers and for integration into Webroot partners' security devices via BrightCloud IP Reputation services. IT security administrators can easily identify threats by type and protect their networks from malicious IP categories, including Windows exploits, web attacks, phishing, botnets, denial of service, scanners, proxies, reputation, spam sources, and mobile threats.

The Webroot Threat Intelligence Platform analyzes and correlates data across numerous dimensions to create a predictive risk score for IPs, ranging from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious, and High Risk (Figure 3). Numerically lower scores (higher risk) indicate that an IP is more likely to be involved in an attack, and are monitored at a greater frequency than trustworthy IPs. The reputation tiers enable enterprises to finely tune their security settings based on their risk tolerance and business needs. This enables them to proactively prevent attacks by limiting the exposure of their networks to dangerous or risky IPs.

Webroot's dynamic list of known malicious IP addresses contains up to 12 million addresses at a given time. Throughout 2015, approximately 32 million new malicious addresses were discovered—which is still less than 1% of the entire IPv4 address space. On an average day, approximately 5% of the list is changed through adding and removing addresses, and this percentage remains relatively consistent throughout the year. An IP address is only useful for attack-launching or attack-control purposes until it is detected as malicious.

Because blacklisting can occur within minutes of the appearance of new malicious IP activity, attackers must change hosts and IP addresses frequently. However, because the Webroot IP blacklist is constantly updated, these changes are rapidly detected and mitigated, minimizing the window of opportunity for malware designers and other attackers.

Figure 3. BrightCloud IP Reputation Index Tiers

Each day, 100,000 IPs that have never before exhibited harmful behavior are added to the blacklist.

While most IP addresses on the blacklist drop off and don't reappear, there is a core set of IPs that resurface repeatedly. In particular, the top 10,000 malicious IP addresses are reused quite often, dropping and reappearing on the blacklist approximately 18 times a year. Although this indicates that the same hosts tend to be reused to perform attacks, this reuse rate is over 60% lower than the one from 2014. A partial explanation for this is that the use of threat intelligence technologies has significantly improved detection of threats from these misused hosts, forcing attackers to abandon them and seek out other hosts to use. An additional cause is that many attackers are moving to the dark web and using IP anonymizing services, such as Tor, that preclude identifying attacks by a particular IP address.

Throughout 2015, the average number of net new IP addresses Webroot added per day was around 100,000, a significant increase from the 2014 average of 85,000 a day. This further supports the notion that attackers are starting to avoid IP address reuse. It also reinforces the importance of using a consistently updated IP list to proactively block threat actors behind those IPs based on advanced reputation data, such as stopping spam and distributed denial of service (DDoS) traffic by limiting the exposure to dangerous or risky IPs. For instance, a highly security conscious bank may choose to block anything with a score lower than 80, while others may choose to accept traffic from IPs with scores higher than 60, as long as the site being accessed is affiliated with a partner.

Malicious IP addresses come from all over the world, but they tend to be concentrated in just a few countries. Figure 4 shows the percentage of malicious IPs for the top 10 countries of origin in 2015, which hosted 75% of all malicious IPs globally. The other 25% represents over 200 other countries with detected malicious IP addresses.

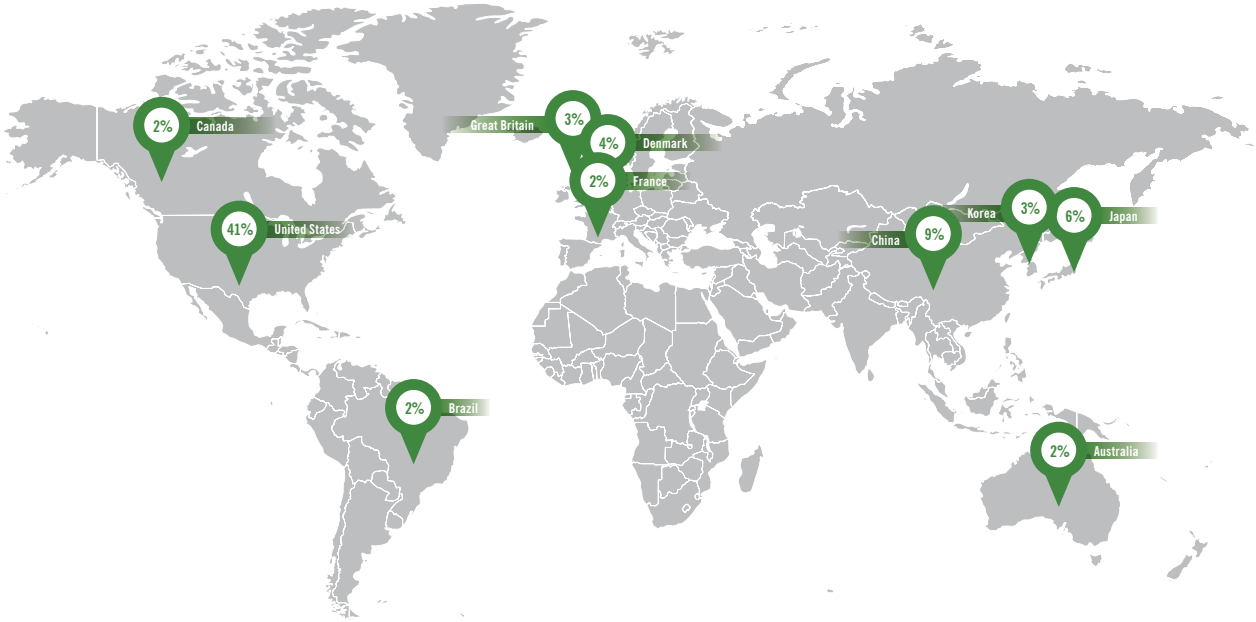

Figure 4. Top 10 malicious IP origin countries.

The United States continues to have the most malicious IP addresses of all countries. In 2015, it accounted for over 40% of all malicious IP addresses; a significant increase from 31% of malicious addresses in 2014. This enormous share in malicious IP addresses is unsurprising, given that the United States is typically the primary focus for attacks. In contrast, China had less than 10% of malicious IPs in 2015, which is a sharp decrease from 2014, during which Chinese addresses constituted 23% of malicious IPs. Similarly, Russia was third in the 2014 count, with 10% of malicious IPs; this declined to 1% in 2015, so Russia was no longer in the top 10. Japan, which did not make the top 10 in 2014, was third in 2015 with 6% of all malicious IP addresses. The most likely explanation for these changes is that attacks originating in countries such as China and Russia have had less success than those from countries such as the United States and Japan, and that attacks that appear to victims to be locally hosted are more likely to succeed.

Another interesting finding from this data involves threat types, such as spam sources, scanners, proxies, web attacks, and phishing. Based on the types of malicious activity that each IP address is involved in, it is categorized by its primary threat type. Spam sources make up the vast majority of all malicious IPs by threat type (approximately 94%). These threats are typically very short-lived, often existing for only hours or even minutes; however, by using continuously updated IP blacklists, organizations can successfully stop spam and related botnets by blocking the associated IP addresses.

The percentage of malicious IPs by threat type, excluding the predominant spam sources type, are shown in Figure 5. Scanners make up just over half of the remaining threats, with proxies following closely behind. The 2015 percentages show minimal change from their 2014 counterparts, with one notable exception: the percentage of web attacks has dropped from 6% to 1%, and scanners have increased by nearly the same amount. The web attacks threat type involves attacks against web servers themselves and does not include malicious websites attacking clients, such as drive-by download sites that push malware onto users' desktops, laptops, and other devices.

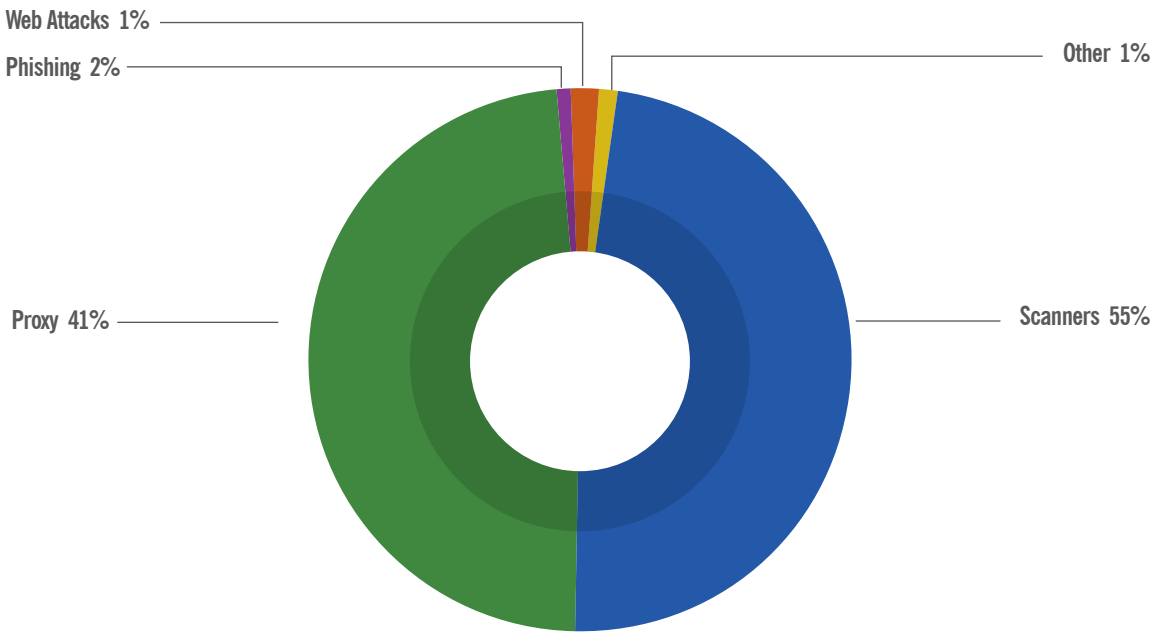

Figure 5. Malicious IPs by threat type in 2015, excluding spam sources.

Even good websites can be risky

New websites are emerging at astonishing rates, and many don't have sufficient security to protect themselves or their users. Others still are expressly designed to take advantage of visitors by delivering malware or executing phishing or other forms of attack. To keep up with the speed and volume of websites, Webroot continuously classifies and monitors the reputations of URLs, having analyzed over 27 billion URLs to date. This process occurs across 83 primary content categories to help enterprises secure users against online threats, control internet usage, and ensure compliance by implementing sensible web access policies. In addition, a reputation scoring system is used to assess the risk of a specific URL based on its site history, age, rank, location, networks, links, and real-time performance, as well as other contextual and behavioral trends, regardless of content category. This intelligence is available via the BrightCloud Web Classification and Reputation Services, and used in the rest of the Webroot security portfolio to protect users and provide a unique perspective into the realm of online security.

Users and networks need to be kept safe from millions of malicious websites.

URLs vary widely in terms of their reputations. Figure 6 shows the breakdown of URLs scored by the Webroot Threat Intelligence Platform during 2014 and 2015. It is important to note that the moderate risk category includes all URLs for which insufficient information was available to accurately categorize them, such as newly created websites. For example, a new website might not have displayed any signs of malicious behavior, but it would be premature to declare it trustworthy until it has been monitored for a longer period of time. Thus, the fact that the percentage of moderate risk URLs increased by 30%, and the percentage of trustworthy URLs fell by nearly 20%, does not necessarily indicate a major change in malicious URLs, but rather a much larger number of new websites. Overall, Figure 6 shows stability in the nature of URL reputations throughout 2014 and 2015.

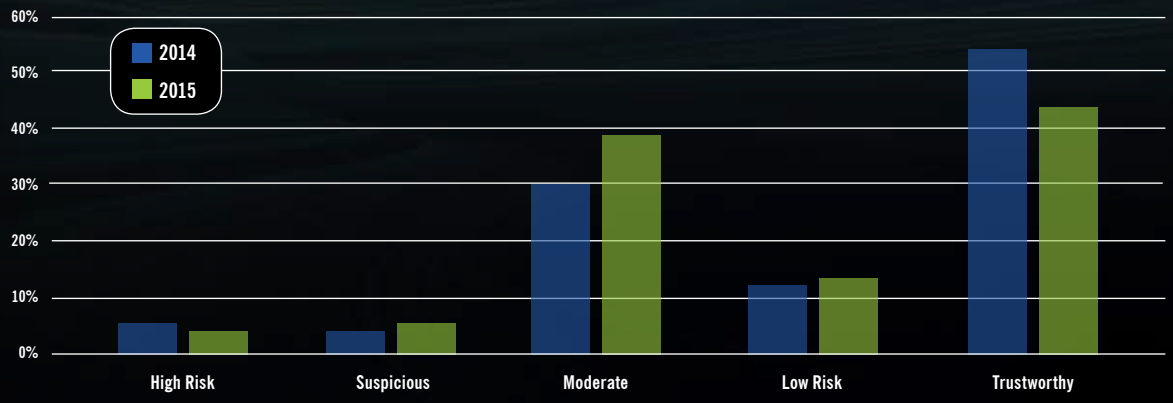

Figure 6. Risk categorization of URLs classified in 2014 and 2015.

Attackers in high-risk countries host malicious sites in more trustworthy countries.

Another important characteristic to consider is where URLs are hosted. Figure 7 depicts malicious URLs by host country. The percentages in this chart are somewhat different from those in Figure 4, but the top two countries, the United States and China, remain the same. The United States' predominance is likely due to attackers in high-risk countries hosting malware URLs in the United States to avoid automatic blocking by geo-filtering services. This underscores the importance of having URL reputation data independent of classification, as filtering purely by IP may not be enough to keep networks and users secure.

Figure 7. Top 10 countries that host malicious URLs.

To further analyze this data, Webroot looked at the 83 primary categories that are used to classify URLs, such as content delivery networks, online greeting cards, and translation services. The BrightCloud Web Classification Service includes six categories of high-risk URLs, which are known spam URLs, malware sites, phishing, proxy avoidance and anonymizers, spyware/adware, and botnets. Excluding those, Figure 8 shows the top 15 categories in terms of high risk and suspicious activity, and their relative distributions of high risk, suspicious, moderate risk, low risk, and trustworthy URLs. These are sites that may have been compromised and not remediated, or were correlated to other malicious URLs, IP addresses, files, or mobile apps.

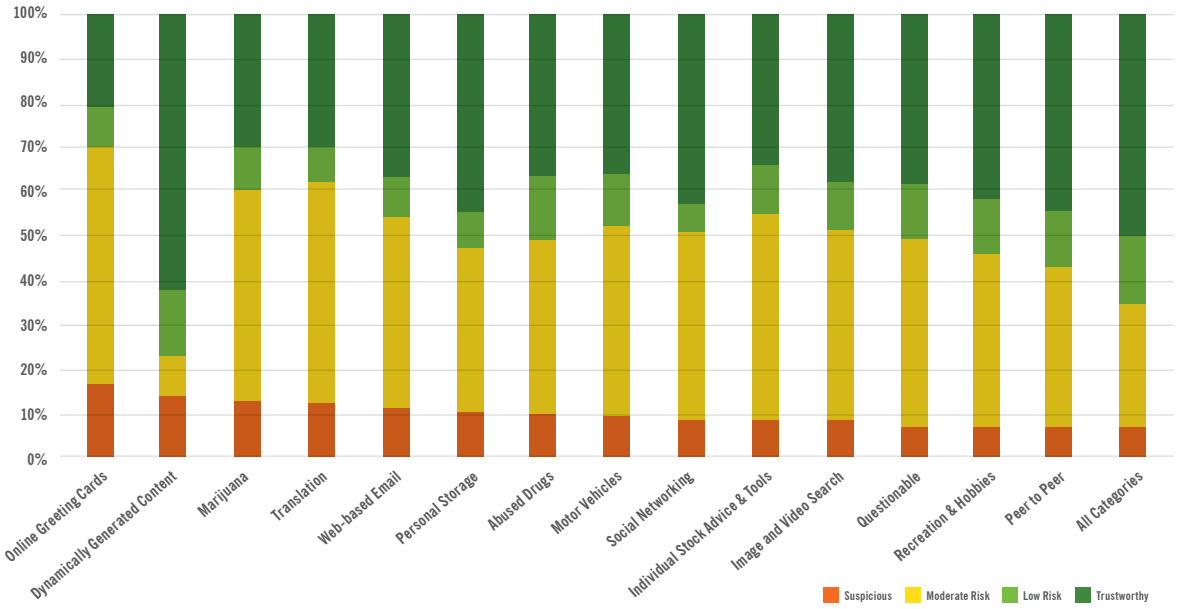

Figure 8. Top 15 Suspicious to High Risk URL categories, excluding Malicious.

Online Greeting Card URLs have the highest likelihood of being suspicious or high risk, followed by Dynamically Generated Content, Marijuana, Translation, and Web-Based Email URLs. The top URL categories for 2015 are nearly identical to those in 2014, with no notable changes. This indicates stability in the distribution of suspicious and high-risk URLs, even as the total number of these URLs has skyrocketed.

In Figure 9, the left column shows the top 10 most commonly visited URL categories in 2015, while the right column reflects the top 10 suspicious to high-risk URL categories. Naturally, URLs in malicious categories, such as Malware Sites and Spam URLs, pose the most risk. When excluding those, the greatest percentage of suspicious to high risk URLs are Business and Economy, Society, Shopping, Travel, and Health and Medicine, which match the categories and order from 2014 exactly.

Top 10 Categories for URLs		Top 10 Categories Suspicious to High Risk URLs	
1 Business and Economy	29%	1 Malware Sites	23%
2 Society	14%	2 Business and Economy	10%
3 Malware Sites	13%	3 Spam URLs	8%
4 Adult and Pornography	6%	4 Proxy Avoidance and Anonymizers	7%
5 Shopping	5%	5 Society	6%
6 Travel	3%	6 Phishing and Other Frauds	4%
7 Personal Sites and Other Blogs	3%	7 Shopping	4%
8 Phishing and Other Frauds	3%	8 Travel	3%
9 Religion	2%	9 Health and Medicine	2%
10 Legal	2%	10 Entertainment and Arts	2%

Figure 9. Breakdown of top 10 URL Categories in 2015.

Somewhat counterintuitively, some categories that might be assumed suspicious or unwanted due to their nature are relatively reputable when compared to average scores. An example is URLs tied to the Gross category, for which 83% are Trustworthy or Low Risk, as compared to the average for all URLs at 56%. Other such categories include Cheating (80% Trustworthy or Low Risk), Hate and Racism (80%), Violence (71%), Illegal (67%), Adult and Pornography (65%), and Nudity (65%). While enterprises—and households, for that matter—may not want their users to visit these types of sites, access and limitations thereof must be based on reliable classifications, as reputation scores alone cannot cover these sites based solely on preference. Further support for relying on classifications is that suspicious and high-risk URLs are often delivered through malicious or compromised ad services, which provide the URL to the user without their action or choice.

A list of categories used by Webroot can be found at www.brightcloud.com.

Shifts in phishing targets

The lifespan of phishing sites is now typically measured in hours and minutes. The window of time during which a phishing site is active is known as its Time to Live; the shorter the Time to Live, the harder it is to protect against it using static blacklists. The BrightCloud® Real-Time Anti-Phishing Service provides time-of-need website analysis to automatically determine, within milliseconds, if a site is a phishing threat.

During 2015, approximately 50% of Webroot customers experienced a first contact with a zero-day phishing site. All subsequent contact attempts by Webroot customers were automatically blocked. This demonstrates how important real-time anti-phishing security controls are for preventing such attacks from succeeding. It also indicates that zero-day phishing attacks are becoming more effective, since the percentage of users being tricked into visiting a zero-day phishing site increased by two-thirds since 2014.

Figure 10 shows the number of unique zero-day phishing URLs identified during each month of 2015. Although there is considerable variation in the numbers from month to month, both halves of the year saw nearly the same number of zero-day phishing URLs overall, with 49% in the first six months and the other 51% in the remaining half of the year.

50% of internet users will fall for a zero-day phishing attack in a year.

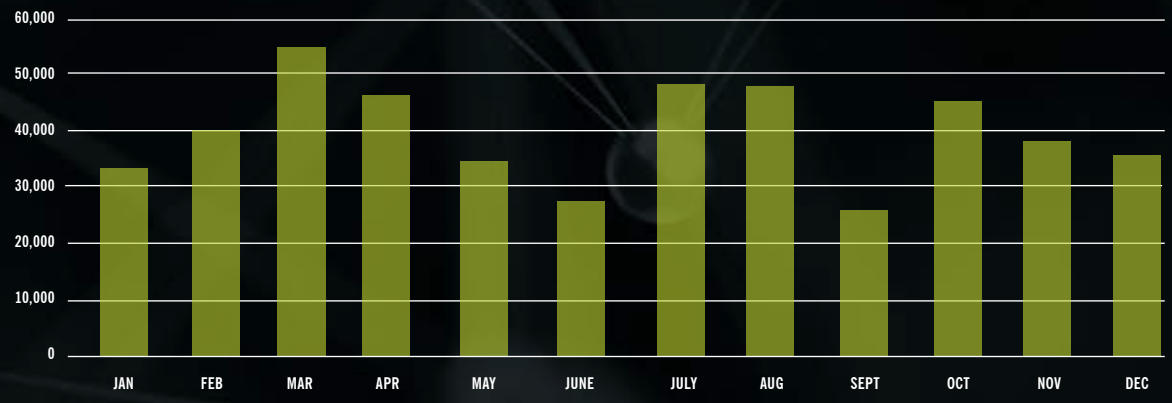

Figure 10. Monthly unique zero-day phishing URLs for 2015.

Examining zero-day phishing data to discover which types of websites are being targeted yields interesting results. Webroot inspected data from companies impersonated by phishing sites in 2015. Figure 11 shows that technology companies were targeted by over twice as many phishing sites as financial institutions (68% to 32%).

While the distribution of phishing sites is quite different among technology companies and financial institutions, the number of companies within each category that are being attacked is actually very similar. Figure 12 demonstrates that 56% of the companies impersonated were financial institutions, while 44% were technology companies.

When the numbers in Figures 11 and 12 are considered together, there are many more phishing attempts per technology company than per financial institution. On average, for every phishing attempt detected per financial institution, there are over 2.6 attempts detected per technology company. Although it might seem that there would be greater value in a financial institution account than a technology company account, the opposite is often true. For example, compromising a technology company account may be easier to accomplish, and in turn it may lead to compromises of one or more financial accounts, providing a larger return on investment for the attacker.

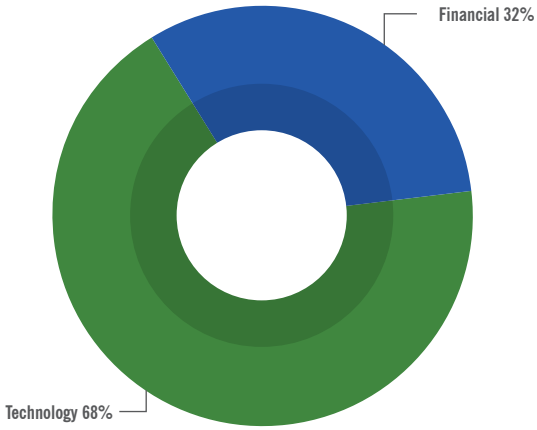

Figure 11. Phishing sites by target (% of website category).

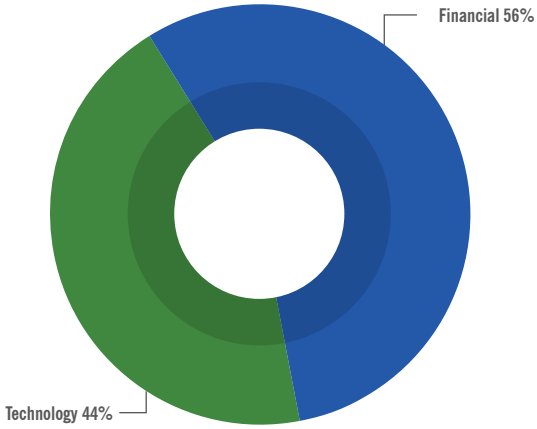

Figure 12. Phishing sites by target (% of companies within each website category).

Over 83,000 fake Google sites in 2015.

The top five impersonated technology companies are listed in Figure 13. These are the same five technology companies that were most targeted in 2014, but their relative rankings have changed somewhat. Phishing sites targeting Google still make up the largest percentage, having increased from 36% in 2014 to 44% in 2015. Of the other top five technology company targets, Dropbox has more than doubled its percentage in the past year, while Yahoo, Apple, and Facebook have all seen a relative decline.

Figure 14 shows the top five impersonated financial institutions. It is important to note that the percentages shown in this table and the previous table are respective to their particular sectors. They cannot be directly compared because they are percentages of different numbers of phishing sites. Although PayPal was targeted in 40% of 2015 financial industry phishing sites, the actual count of these sites, over 36,000, is still less than half the number of phishing sites that targeted Google (over 83,000).

The relative percentages of sites targeting these financial institutions has also changed from 2014 to 2015. For example, PayPal was targeted by over 52% of financial institution phishing sites in 2014. Attackers appear to be shifting their interest away from PayPal users and onto others; Navy Federal, for example, has more than doubled its relative percentage in the past year.

1	Google	44%
2	Dropbox	16%
3	Yahoo	15%
4	Apple	14%
5	Facebook	8%
	Other notables: Adobe, Blizzard, and Microsoft	

Figure 13. Top 5 impersonated technology companies.

1	PayPal	40%
2	Wells Fargo	21%
3	Bank of America	13%
4	Navy Federal	9%
5	Chase	7%
	Other notables: USAA, Lloyds Bank, and NatWest	

Figure 14. Top 5 impersonated financial institutions.

Figure 15 illustrates the top 10 countries that host the most phishing sites in 2015. The United States hosts, by far, the largest number of phishing sites (56%). Although this is a significant drop from 2014, when 75% of all phishing sites were hosted in the United States, this number is over ten times the phishing site count for any other country. The next largest hosts of phishing sites are the UK and Germany, each with a 4% share. The United States' share in our analysis can be accounted for, in part, by the fact that a larger percentage of Webroot customers is based in the United States. Additionally, phishing attacks often target victims based on economic ranking for a higher return on investment, so they typically focus on more developed nations. The year-to-year decline in the percentage for the United States likely indicates increased interest in phishing attacks against other countries, rather than decreased interest in United States-based phishing.

Figure 15. Largest hosts of phishing sites by country.

Mobile apps are riskier than ever

Between the prevalence of smartphones and tablets and the continued popularity of Bring Your Own Device (BYOD), mobile applications and compromised devices have become a preferred target to attack individuals and the networks they connect to. Webroot continuously analyzes new and updated applications from app stores and other online sources. This intelligence is used to help protect Webroot mobile customers, and is available to vendors who provide mobile management and security solutions via the BrightCloud® Mobile App Reputation Service and Mobile Security SDK. These help those vendors address the security vulnerabilities that mobility and the BYOD trend create by restricting access to applications and compromised devices.

Webroot has streamlined the process of analysis to provide concise classification and other information on mobile apps. A five-tiered classification system enables Webroot partners to implement effective mobile app usage policies. This provides flexibility for partners to decide how to use the app information and adapt it for specific management requirements.

In 2015, Webroot added over 10 million new and updated Android™ apps to its App Reputation service, which now includes over 20 million apps. Figure 16 shows the distribution of these new and updated apps by reputation over the course of 2014 and 2015 by half year, and the overall change is striking. In the first half of 2014, 27% of new and updated apps were benign, 51% were moderate or suspicious, and 21% were malicious or unwanted. In contrast, during the second half of 2015, only 18% of new and updated apps were benign, 30% were moderate or suspicious, and the remaining 52% were unwanted or malicious.

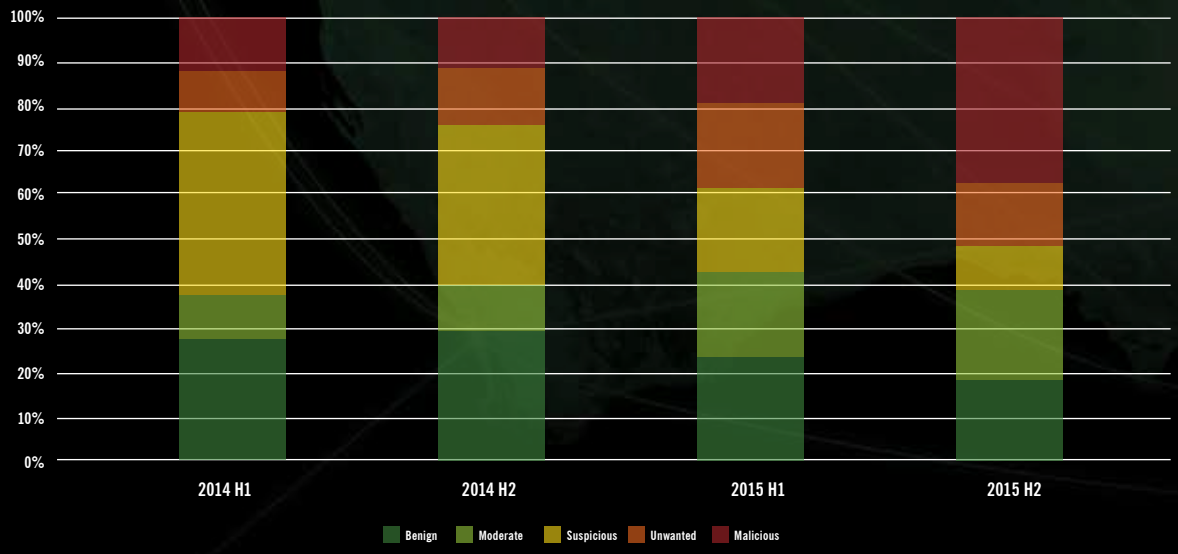

Figure 16. Distribution of mobile app reputation in 2014 and 2015.

Although these percentages might imply that most apps have nefarious intent, keep in mind that these numbers are generated by analyzing apps from certain feeds—some of which are dominated by malware. Regardless, these numbers clearly indicate a shift toward malicious and unwanted apps. A reason for this may be that the market for new apps that offer what existing apps already provide is shrinking. Another reason for this is that malicious, suspicious, and unwanted apps are increasingly installed at the factory, particularly on devices geared for emerging markets.

It is also important to be aware that malware may be more prevalent in certain app stores. For example, Android app stores in the United States generally offer more robust processes for ensuring that apps are legitimate before making them available for download. In other countries, such as China, many Android app stores are managed by third parties, and their standards for security may vary greatly, allowing attackers to fill app stores with malware. A presentation at the 2015 Association of Anti-virus Asia Researchers (AVAR) conference demonstrated that over 30% of apps in Android app stores in China are actually malware. Another reason behind this trend is that, in China and many other countries, people are much more likely to have an Android device than a traditional desktop or laptop computer. Attackers typically target their malware creation at the most popular platforms, i.e. the Android OS, in this case.

Figure 17 shows the relative frequency of types of mobile app threats within the malicious category, including adware, PUAs, rootkits, spyware, system monitors, Trojans, and worms. Trojans make up the vast majority of malicious threats, averaging 77% for 2014 and 60% for 2015. Trojans are a very broad category that includes SMS infections, which are the largest family of malicious Android apps, and fake installers. The next most prevalent categories are PUAs, which were only 10% in 2014 but are over 28% in 2015, and spyware, which has slightly risen from 9% in 2014 to 11% in 2015. The most likely explanation for the sharp increase in Android PUAs is that free mobile apps often support themselves through ad networks, some of which are malicious.

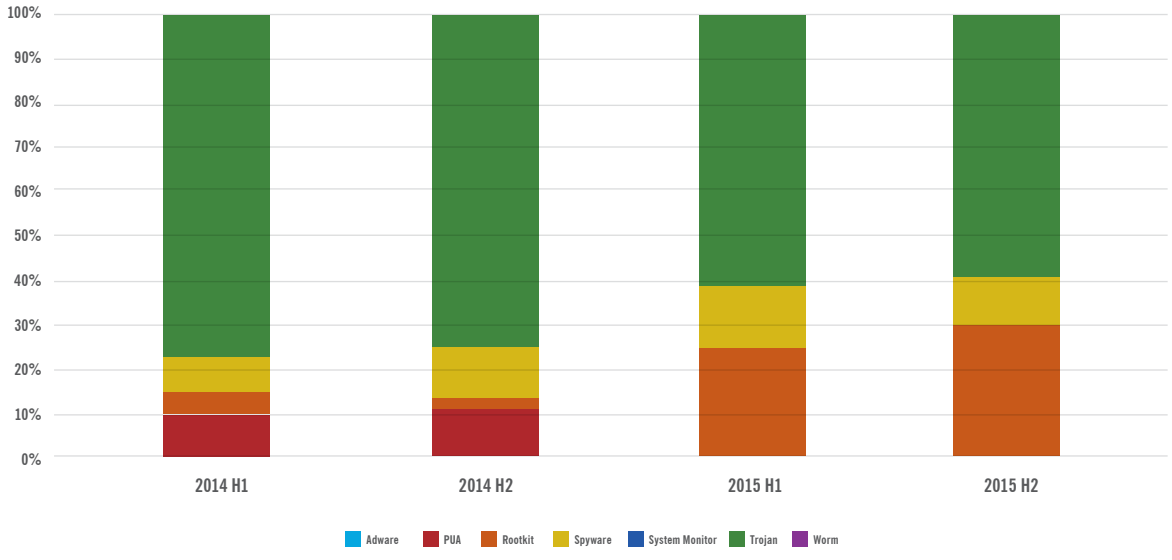

Figure 17. Frequency of Android™ application threat types.

Android apps can also be classified by their apparent purpose, based on the 45 categories defined by the Google Play store. Webroot found malicious apps in each of the purpose categories, but they were not evenly distributed. As Figure 18 illustrates, the Tools category, which includes a wide range of utilities, ranging from calculators to battery management apps, was by far the leading category for malicious apps, with 24% of all malicious apps, although this is just over half of the 44% noted for 2014. Note that apps in the tools category often require additional access to the device, making them better suited for malicious purposes. The other categories in the top 10, which are nearly identical to the 2014 percentages, are Arcade & Action (10%), Personalization (5%), Casual (5%), Entertainment (5%), Communication (4%), Social (4%), Lifestyle (3%), Health & Fitness (3%), and Brain & Puzzle (3%). The remaining 35 categories constitute 34% of all malicious apps, a major increase from the 20% seen in 2014. Based on the reduced focus on tools and the increased attention to other categories, this indicates that malware authors are changing their tactics by widening the scope of the apps they target.

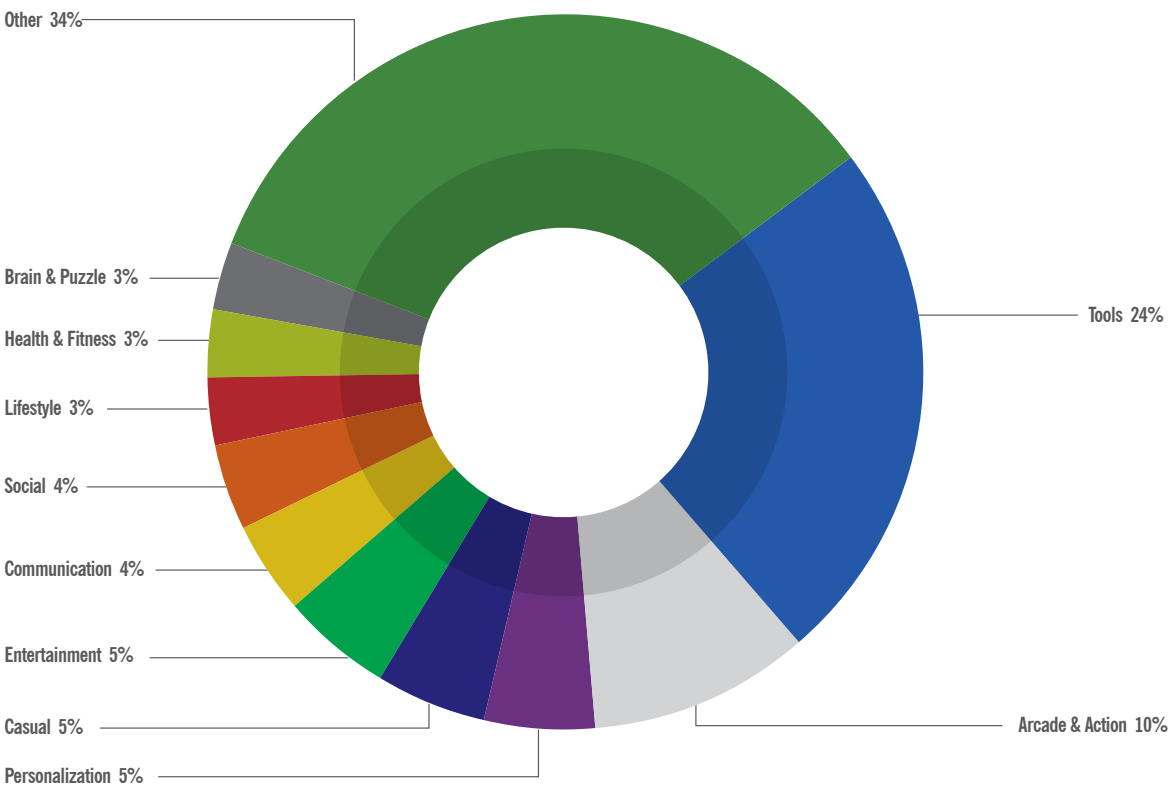

Figure 18. Top 10 malicious Android apps by category in 2015.

1	Tools	24%
2	Arcade & Action	10%
3	Entertainment	5%
4	Personalization	5%
5	Casual	5%

Percentages of top 5 malicious Android apps by category

1	Tools	10%
2	Arcade & Action	9%
3	Entertainment	8%
4	Personalization	8%
5	Casual	6%

Percentages of top 5 Android PUAs by category

Worth noting is the difference between the percentages for the top 10 malicious Android apps by category (Figure 18) and the percentages for the top 10 Android PUAs by category. The top five categories are the same: Tools (10%), Arcade & Action (9%), Entertainment (8%), Personalization (8%), and Casual (6%). However, upon closer inspection, Tools made up 24% of malicious apps, but only 10% of PUAs. Other categories have percentages closer to the Tools number. This indicates a more even distribution of Android PUAs by category than malicious Android apps.

The numbers throughout this section don't effectively show the real-world impact a single malicious app could have. For example, in mid-2015, an easily exploitable vulnerability in Android phones forced an update for over a billion devices.[2] An attacker could send a crafted MMS message that would root the recipient's phone if it wasn't updated, giving the attacker full device control. This attack, known as Stagefright, is not an isolated instance; almost every year there is a new major vulnerability and corresponding exploit that puts hundreds of millions or even billions of phones at serious risk of compromise.

Fortunately, Android version 6.0 (Marshmallow) includes enhanced security and privacy features that reduce the risk of compromise and the impact of compromises that do occur. For example, Marshmallow offers a dynamic permissions model that allows a user or administrator to enable or disable individual permissions, such as deciding whether or not a particular app may have access to the user's contacts. The new model also makes it clearer to the user why a particular permission is being requested for an app. This allows users to make more informed choices related to the security and privacy of sensitive information, potentially preventing compromises of that information. Additionally, Marshmallow offers other beneficial features, such as encrypting stored data by default.

Although the emphasis throughout this section has been on Android apps, this is not to imply that other mobile platforms, such as iOS® devices, are without security issues. Historically, iOS devices have not been compromised as frequently as their Android counterparts, which has led many to conclude incorrectly that iOS devices are not at risk. As a counterexample, a recent attack against Apple's integrated app development and creation environment, Xcode, occurred.[3] A developer distributed a Trojan version of the Xcode software, which was acquired and used by many other developers. Every app created using the infected Xcode included hidden commands. It is estimated that approximately 2 million iOS users were impacted by the Trojan that was started with the single altered copy of the coding platform. This illustrates the potential for weaknesses within iOS security and the risk that many users typically discount.

[2] "Stagefright: It Only Takes One Text To Hack 950 Million Android Phones." Forbes Magazine. July 2015. www.forbes.com/sites/thomasbrewster/2015/07/27/android-text-attacks

[3] "Apple iOS Virus May Have Affected Almost 500 Apps, 2 Million Users." Forbes Magazine. October 2015. www.forbes.com/sites/hnewman/2015/10/06/apple-ios-virus-may-have-affected-almost-500-apps-2-million-apple-users

Conclusion

The data collected by Webroot throughout 2015 clearly shows that today's threats are truly global and highly dynamic. Many attacks are staged, delivered, and terminated within a matter of hours, or even minutes, having harvested user credentials and other sensitive information, encrypted devices through ransomware, or otherwise acquired the means to achieve financial gain. Countering these threats requires an innovative approach to attack detection that leverages advanced detection techniques and threat intelligence.

Malware and PUAs have become overwhelmingly polymorphic, and over 97% of all malware instances during 2015 were observed on a single endpoint device each. The average number of file instances per PUA family plummeted from nearly 30,000 in 2014 to just over 260 in 2015, while malware file instances per family dropped from nearly 700 to less than 100, underscoring increased polymorphism. Although PUAs were twice as common as malware during 2015, the frequency of malware increased by 29%, even as PUAs decreased by 30%. The decrease in PUAs is primarily due to consumers becoming increasingly conscious of installing applications from legitimate sources.

Webroot continuously updates a list of approximately 12 million high-risk IP addresses, with around 5% of the entries changing every day. Of the IP addresses added each day, around 40% have never before been associated with malicious behavior. Malicious IP addresses come from all over the world, but they are heavily concentrated in just a few countries, including the United States (41%) and China (9%). The vast majority of malicious IP addresses (94%) are associated with spam generation, which are quite short-lived and are nearly impossible to detect using traditional, static blacklists. However, they can be stopped using dynamically updated IP address lists and advanced relationship scoring.

During 2015, Webroot analyzed and scored millions of URLs and discovered that the distribution of URL reputations was similar to 2014, except for a single shift attributable to an increase in brand new websites for which sufficient classification data is not yet available. Webroot also noted that, as with malicious IPs, malicious URLs are largely hosted in the United States (30%) and China (11%). Overall, there was minimal change in URL reputations, categories, and hosting countries from 2014 to 2015.

The average likelihood of a user encountering a true zero-day phishing site over the course of a year was only 30% in 2014, but climbed sharply to 50% in 2015, testifying to the increased efficacy of zero-day phishing attacks. Of the companies targeted by phishing sites in 2015, technology companies were targeted by over twice as many phishing sites as financial institutions. However, financial institutions were impersonated 56% of the time and technology companies only 44% of the time. This means that there were over two and a half times more phishing attempts per technology company than

continued on next page »

per financial institution. Google alone was targeted by over 83,000 phishing sites during 2015. Phishing sites are also hosted primarily in the United States, although the number itself has declined somewhat in the past year. In 2014, 75% of all phishing sites were in the US, whereas this share dropped to 56% for 2015. However, the countries with the next biggest shares, the UK and Germany, only have a 4% share each.

Webroot analyzed over 10 million new and updated Android mobile applications during 2015 and classified them as benign, malicious, moderate risk, suspicious, or unwanted. By the end of 2015, 52% of all new and updated Android apps were determined to be unwanted or malicious, while only 18% were benign. This is a striking change from the beginning of 2014, when only 21% of new and updated apps were found to be unwanted or malicious, and 27% were classified as benign. Although all these numbers are somewhat slanted because many of the analyzed apps come from sources dominated by malware, the changes indicate a disturbing shift. Most mobile app threats discovered involve Trojans (60%) or PUAs (28%).

With the various increases in polymorphism and other malware trends, it is more apparent than ever that organizations need to bolster their security posture with real-time, highly accurate threat intelligence and proven next-generation endpoint security to protect themselves, their users, and their customers from cybercriminal activity. Dynamic intelligence enables them to set proactive policies to automatically protect networks, endpoints, and users as part of a defense-in-depth strategy. This is especially necessary when security teams consider the threat landscape as a whole, in addition to conducting in-depth analysis on the threats targeting them. Furthermore, individuals also need to be more vigilant than ever about the websites they visit, the URLs they follow, and the applications they download and use.

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