ninja RMM | WEBROOT Smarter Cybersecurity™

2018 Webroot

What's inside

4 Webroot Perspective

6 Polymorphism: The Trend Continues

8 Trends in Polymorphism by Operating System

10 Ransomware, Cryptojacking, and Other Alarming Trends

12 Malicious IP Addresses

14 Incredible Number of High-Risk URLs

17 Phishing Attacks Become More Targeted and Dangerous

20 Universal Threat of Malicious Mobile Apps

22 Summary

Contributors:

Nicholas Duran | Jurijs Girtakovskis | Ken Jacobi | David Kennerley | Justine Kurtz | Grayson Milbourne | Tyler Moffitt | Cameron Palan | Steve Snyder

Foreword

Sal Sferlazza | CEO, NinjaRMM

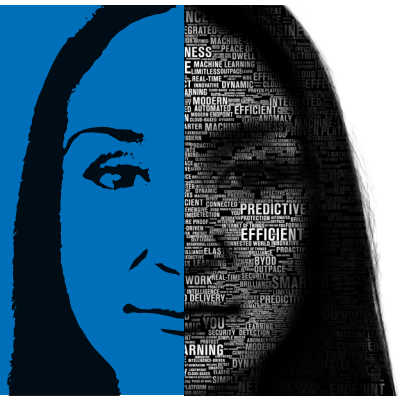
As wonderful as the internet is, it can also be a weird, treacherous place. Fraud attempts can come by email, phone, text, or even an innocuous-looking web page. As a security-centric CEO committed to keeping the cloud safe for business, I sleep better at night knowing that the engineers at Webroot are keeping a watchful eye on the ever-nimble cybersecurity threat.

And the agility of Webroot is what makes it a first-class product. As you'll learn from reading this report, cybersecurity was more like whack-a-mole than ever before in 2017. For example, most phishing domains were active for just a few hours before attackers moved on to another one. And 93% of malware variants were spotted on just one machine, because hackers have gotten so good at disguising the digital fingerprint of each attack.

In this type of environment, the old-fashioned tactics of site blacklists and virus databases are obsolete. Webroot's BrightCloud® Threat Intelligence Services offer a rich suite of tools to combat threats to your network as they emerge.

Tools like these make me so happy to partner with Webroot –we've been offering the product within our NinjaRMM platform since June of 2017. And you don't need to take my word for it. Over 2,000 of our managed service provider customers trust the product to keep their businesses protected and online. These customers are voting with their feet – and I hope you will too.

Webroot Perspective



The statistics in this report are based on threat intelligence metrics automatically captured, analyzed, and contextualized through the Webroot® Threat Intelligence Platform, which integrates billions of pieces of information from millions of real-time endpoints, sensors, third-party databases, and security partners. The Webroot Threat Research team has investigated data related to a broad range of threat activity, including:

- Trends in malware and potentially unwanted applications (PUAs)
- IP addresses and their impact on security
- Latest trends in ransomware and cryptojacking
- How URL reputations and classifications help combat attacks
- The evolution of phishing attacks
- Mobile application threats

This year's report includes several new sections. In addition to facts and predictions around today's threats, it incorporates an in-depth examination of the role that Windows® 10 migration is playing in overall security, and discusses the often-overlooked implications of home user device usage on enterprises. We cover the added value of ongoing end user awareness training to help organizations reduce risks and decrease the impact of social engineering, and examine recent trends in the increasing occurrence of cryptojacking, an alarming new extension of the threat landscape. We explore the impact of cryptojacking on mobile devices, web, and endpoint security, and even how malicious services are paid for.

The Webroot Threat Research team's findings and insights on threats and cybercrime trends shed light on the threats you face today, and help you become better prepared to handle them during the coming year.

WE CONTINUOUSLY CLASSIFY AND SCORE 95% OF THE INTERNET 3X PER DAY

27+

Billion URLs

600+

Million Domains

4.3+

Billion IP Addresses

15+

Billion File Behavior Records

62+

Million Mobile Apps

52+

Million Connected Sensors

Polymorphism: The Trend Continues

In the last few years, we have witnessed a dramatic increase in the prevalence of polymorphic malware and potentially unwanted applications (PUAs), indicating that these threats are the preferred system of malware delivery for cybercriminals. In fact, more than 94% of all malicious executables we encounter are polymorphic. Polymorphism is a tactic designed to circumvent traditional antimalware solutions, which use names, encryption keys, signatures, or hashes to detect a single instance of malware delivered to a large number of people. With polymorphic malware and PUAs, these identifiers are never the same, so an existing signature will not match the new variant. Attackers use polymorphism as an effective way to evade detection by pattern-matching security products, which cannot detect brand new variants before they compromise systems.

94% of malicious executables are polymorphic.

Webroot SecureAnywhere® endpoints see hundreds of millions of new executable files each year. Although the actual number of new executables is going up, the number of files determined to be malware or PUAs is decreasing. Of the never-before-seen files observed in 2017, just 2% were found to be malware, while <1% were PUAs. This is significantly lower than in previous years; in 2016, the relative percentages were 3% and 2%, respectively, while in 2015, 4% of new files were malware and 7% were PUAs.

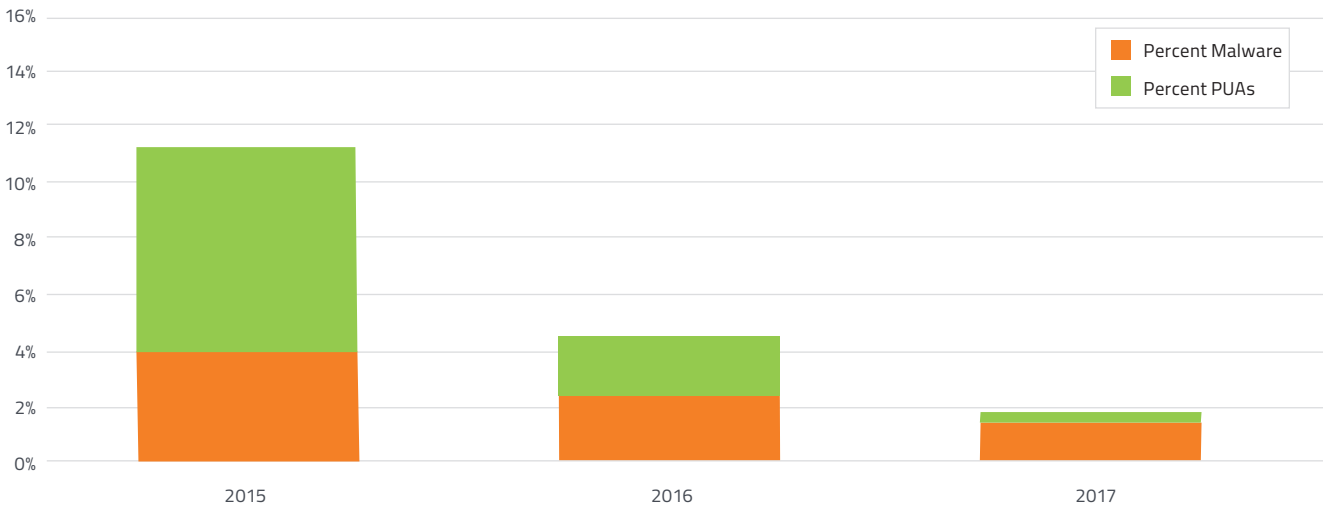


Figure 1: Percentage of new executable files determined to be malware or PUAs by year

In 2017, 93% of malware was unique.

We see a similar decline in the average number of malware files per device by year. In 2016, the average incidence of malware was 0.66 per device, but this figure dropped to 0.48 per device in 2017. The difference is even more striking when viewed in terms of business versus home user endpoints. In 2016, the average incidence of malware per home user device was 0.59, but it dropped to 0.53 in 2017. For business devices, the figures were 0.61 in 2016 and 0.42 in 2017.

Despite the impression these numbers may give, this decrease in the percentage of files determined to be malware does not indicate the malware threat is diminishing. There are a number of likely reasons that the volume of new malware and PUAs has stopped growing at the astronomical rates we had seen previously. First, during those years of incredible growth, attackers were changing from traditional malware and PUA creation to more automated, polymorphic file creation techniques, thereby creating many unique executables—rather than a single executable that could be blocked quickly due to its popularity. Once most attackers had switched to polymorphic techniques, the rate of growth abated. Second, Webroot has enhanced its techniques for detecting malicious activity earlier in the kill chain, such as blocking executable files from being transferred to endpoints via malicious URLs, and preventing malicious executable files on an endpoint from downloading additional malicious executables. Because Webroot is more effective at preventing additional executables from reaching endpoints, those executables are no longer included in the observed files. Although the decline in the volume of new malware reaching Webroot customers is certainly a positive trend, organizations must continue to treat malware as a major threat. Third, malware is becoming more difficult to distribute. Changes in exploit kits and major takedowns in 2017—such as the RIG Exploit Kit takedown in July and the February 2017 move by Gmail to disallow JavaScript—have created obstacles in the path of malware distribution.

Perhaps one of the most important reasons for the drop is due to the migration to the Windows 10 operating system, which is significantly more secure than its predecessors. Nevertheless, the highly variable nature of malware makes it impossible to predict when malware may spike; any big news story, seasonality (e.g. holiday shopping, back-to-school, or income tax season) or any other factor may impact the results.

To see that polymorphic malware and PUAs are still extremely prevalent, we need only look at the number of files found on a single machine, indicating that each was a unique variant and not seen again, even after Webroot created almost half a million rules to trap future instances. In 2017, 93% of the malware encountered was seen on only one machine, and 95% of PUAs. Clearly, the move toward creating slightly different variants of malicious or unwanted files has become mainstream. This data speaks to how quickly the hackers retire a variant and come up with a new one.

Trends in Polymorphism by Operating System

We've seen the strong trend toward the use of polymorphic attacks for several years, along with a steady decrease in the percentage of new files that are malware or PUAs. To help explain this decrease, this year, Webroot enhanced its analysis with deeper insight into the differences between business and home user data. Our research shows that one of the more important factors in the reduced percentage of new malware files and PUAs is the migration to Windows® 10, which appears to be a much safer operating system.

To date, more than half the systems (54%) observed by Webroot are running Windows 10, compared to 49% in January of 2017. Compare this with Windows® 7 (less than 33%), Windows® 8 (8%), Vista® (1%), and XP® (<1%). Overall, there has been a strong movement away from older, deprecated, or less secure operating systems. However, when we look deeper, we notice some striking differences between the adoption rates (and results) for businesses versus home users. It's important to track both environments, since so many business users bring personal devices to work, in addition to corporate-controlled and managed devices, all of which could access the corporate network.

Why Businesses Should Care about Home User OS Migration

It's good news that home users are adopting Windows 10 at a rapid clip, but not-so-good news that enterprises are moving at a slower pace. The reasons are understandable: any OS migration is a major endeavor and, according to a recent CIO Magazine article, migrating the entire organization to Windows 10 is considered a multiple-year project[i]. As long as corporate devices are running older versions of the operating system, the organization is at risk. Windows 7, the second-most-prevalent OS in the devices seen by Webroot, remains especially vulnerable.

> **Almost all the devices that fell victim to the WannaCry ransomware attack were running Windows 7, and that attack alone is estimated to have caused $4 billion in losses to businesses.**[ii]

Add to that the vulnerability from organizations' users who employ not only corporate-owned devices, but also their personal smartphones, tablets, etc., which can access corporate data and are often in vulnerable settings. These devices are subject to a much higher occurrence of malware per device (.55 infections per device on average over the year) than business-owned or managed devices (.42 infections) and the same holds true with respect to PUAs. Even organizations with strong BYOD policies are often unaware of the precise security status of a user-owned device. While Windows 10 won't solve all security woes, it's a step in the right direction. Combined with advanced endpoint protection that uses behavioral analysis and machine learning, adopting Windows 10 can greatly reduce enterprises' vulnerability to cyberattacks.

Windows 10 is almost twice as safe as Windows 7.

Business Devices

The business world is showing steady, if slow, adoption of Windows 10. In January 2017, only 20% of observed business computers were running Windows 10; that figure climbed to 32% by year end. In contrast, Windows 7 was running on 62% of the systems we saw in January, but had dropped to 54% share by the end of the year. Windows 8 was at 4% in December 2017, down from 5% in January, while Windows Vista™ (1%) and XP (<1%) both represented miniscule percentages at the end of 2017.

While fewer malware files were seen in 2017 than in 2016, the numbers are more striking when viewed by operating system. Only 15% of the total files determined to be malware in 2017 were seen on Windows 10 systems, while a full 63% were found on Windows 7, the next-most-common OS for businesses. On Windows 10 systems, we saw an average of .04 malware files per device, a strong contrast with .08 on Windows 7.

The volume of malware seen on Windows 10 devices was relatively consistent over 2017, with spikes in August (14% of the annual total) and December (12%).

When we look at PUAs within the context of the operating system, we see that PUA per device for Windows 10 dropped from a high of .06 in January 2017 to .01 in December. The overall incidence of PUAs per device, independent of operating system, fell from a peak of .69 PUAs per device in January to .06 at year's end.

The OS migration rate for enterprises has been quite slow; Webroot saw only 32% of corporate devices running Windows 10 by the end of 2017. Although the cost in terms of man hours and level of effort may contribute to enterprises' slower migration rates, their exposure to risk grows with each passing day.

Home User Devices

Home user OS migration to Windows 10 tells a very different story. By December 2017, almost 72% of home user devices had migrated to Windows 10, up from 65% in January while Windows 7 dropped from 17% in January to 15% in December, and Windows 8 fell from 14% to 11%. As with business devices, the use of Windows Vista (2%) and XP (<1%) remain insignificant.

The occurrence of malware per non-business device at the end of 2017 was .07 for Windows 10, versus .16 for Windows 7 and .17 on Windows XP. As with business devices, Windows 10 is more than twice as safe as Windows 7 for home user devices. The volume of malware per device remained constant throughout 2017, at an average of .55 files per device.

PUA volume has been steadily decreasing since its peak in February 2017; from a high of .33 PUAs per device, the rate dropped to .17 per device. Windows 10 sees about half the rate of PUAs per device as Windows 7.

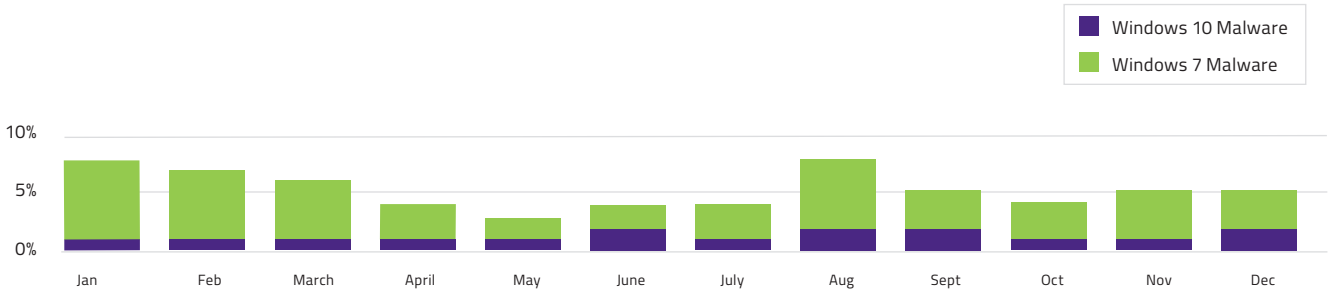


Figure 2: Malware on Windows 10 and Windows 7 devices by month, in 2017, as a percent of total malware seen across all operating systems

Ransomware, Cryptojacking, and Other Alarming Trends

Ransomware and its variants have become a serious threat around the world, and 2017 saw new, more virulent and destructive variants with a variety of purposes. The two most discussed and largest ransomware attacks in history—WannaCry and NotPetya—hit during 2017 and were the most prolific ever seen. Together, they infected more than 200,000 machines in more than 100 countries, all within just 24 hours. These attacks used the EternalBlue exploit to attack the server message block (SMB), which is essentially a file-sharing vulnerability on Windows XP and newer. The malware was then able to move laterally through the network just like a worm, reaching any computer running SMB, even those not connected directly to the network, but to another network-connected device.

NotPetya arrived a few months later, using the same exploit to eventually spread worldwide from its origin as an infected update to Ukrainian tax software. Rather than encrypting files, NotPetya modified the master boot record (MBR) and encrypted the entire hard drive, preventing the Windows OS from booting. The attack was designed to do as much damage as possible to Ukrainian infrastructure during a holiday, and it achieved its goal: power plants, banks, and supermarkets were shut down. After the attack spread across the world, estimated damages of more than $1.2 billion[iii] were reported.

Spam email campaigns have long been the preferred method for distributing ransomware, but an easier vector has emerged: using unsecured remote desktop protocol (RDP) campaigns to infect victims. A convenient way to control servers and other machines remotely, RDP suffers from several security weaknesses, such as leaving port 3389/TCP open to any inbound connection (more than 11 million endpoints do so); not requiring administrators to change the default admin account credentials; and allowing a very large number of login attempts before triggering an alert or account lockout. Cybercriminals can use specialized tools equipped with large username and password lists to eventually make their way in. Once inside, the hacker may use specialized tools or custom malware to get past or disable security solutions. The most common result of an RDP campaign is to deploy ransomware, an especially potent infection, since the attacker can also view other computers on the network and gather information for future campaigns. Whether for profit or destruction, new developments in ransomware are causing the industry to reevaluate the role and intentions of ransomware in future global attacks.

According to our data, cryptojacking is also gaining traction and could turn out to be even more profitable and anonymous, and require less effort than other attacks. Instead of stealing a victim's files and ransoming them for money, the cybercriminals steal victims' CPU power to mine cryptocurrency. Since there's no malware payload, the user often remains blissfully unaware they're being used. We first saw cryptojacking in September 2017, when CoinHive debuted JavaScript code to mine the cryptocurrency Monero. Claiming this was an ad-free way for website owners to generate enough income to pay their server costs, cybercriminals quickly began to hijack websites to host scripts that would pay into their own Monero wallets. (Monero is currently preferred to Bitcoin because it has the best mining performance on home user CPUs, as well as a private blockchain ledger that prevents tracking of transactions.) The recent surge in cryptocurrency prices has also contributed to the popularity of this type of attack vector for criminals. Since September 2017 there have been more than 5,000 websites that have been compromised to mine Monero through CoinHive[iv].

A third and extremely dangerous trend relates to the spread of government hacking tools. A group calling itself Shadow Brokers leaked government hacking tools, starting in 2016 and continuing throughout 2017. As these formidable tools get into the hands of bad actors, it's the cybersecurity equivalent of leaking not only the plans to build a nuclear weapon, but a shipment of enriched uranium at the same time.

WANNACRY AND NOTPETYA HIT DURING 2017 AND WERE THE MOST PROLIFIC EVER SEEN

100 countries

200,000 machines

$1.2 billion dollars

Damages estimated from NotPetya

Malicious IP Addresses

Every year, Webroot sees tens of millions of IP addresses that we determine to be malicious. These may be compromised computers that send out spam emails, open proxies that allow anonymous traffic to pass through, or unsecured home computers or IoT devices that are part of a botnet distributing malware or launching denial of service (DoS) attacks. The ideal defense is to block network traffic from these addresses automatically, before the damage is done.

Although we saw no significant increase in the number of unique malicious IP addresses in 2017 versus 2016, the number remained enormous. We track the various types of threats from malicious IP addresses, and categorize them as spam, Windows exploits, scanners, botnets, denial of service attacks, proxies (including anonymous and Tor), web attacks, phishing, and mobile threats. Figure 3 shows that the vast majority of malicious IP addresses on the list represent spam sites (65%), followed by scanners (19%) and Windows exploits (9%). Scanner attacks can be especially troublesome; hackers scan the network environment to learn its specifics, including the software being used, the network configuration, and even user data, so they can mount an attack specifically tailored to that environment. Windows exploits are an increasingly popular method for distributing malware, since many do not require active participation from the user, but rather exploit a vulnerability in the operating system, software, browser, or plug-in. As more users migrate to Windows 10, this vector may decrease in popularity.

Most malicious IP addresses came from a handful of countries. Figure 4 shows the 10 countries that accounted for almost 62% of all malicious IPs globally.

The United States, as in years past, had the highest percentage of malicious IP addresses (12%). This percentage dropped substantially from 2016 (22%), and even more significantly from 2015 (41%). China, in contrast, saw a big uptick in malicious IP address activity in 2017, reaching 12% in 2017,

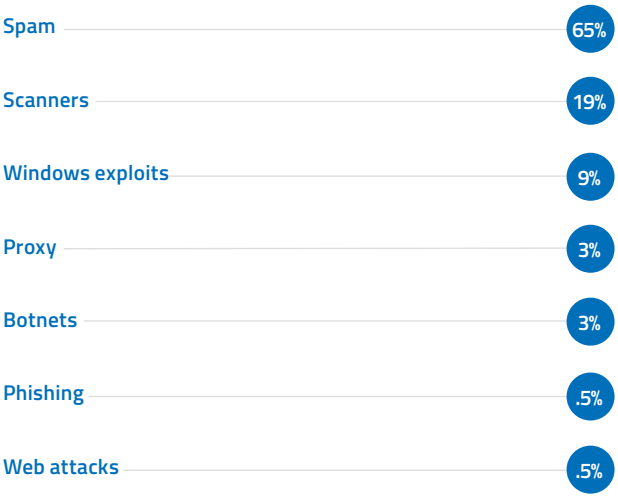


Figure 3: Malicious IP addresses

84% of malicious IPs represent spam and scanners.

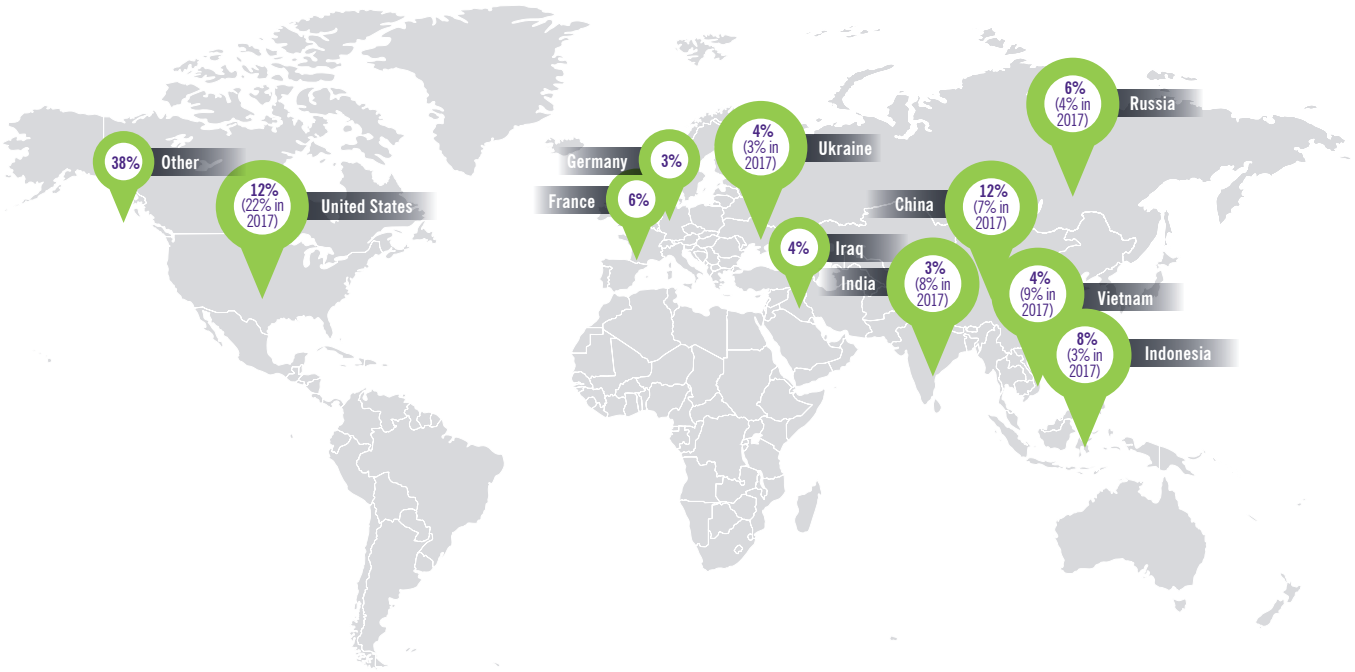


Figure 4: Malicious IP addresses by country

versus 7% in 2016 and 9% in 2015. Russia showed a significant spike, going from just 1% in 2015 to 6% in 2017. A similarly large increase was seen in Ukraine, which jumped to 4%. India in 2015 represented just 1% of the top offenders; the percentage increased to 8% in 2016, then dropped to 3% in 2017. Indonesia rose to 8%. Iraq, Germany, and France joined the top 10 list this year but were less prevalent in 2016.

The types of threats seen by country vary somewhat. Of the top 10,000 blacklisted IP addresses from the top 10 countries, 37% are scanners, followed by spam at 34%, and Windows exploits at 21%. Many (66%) pose multiple threats, e.g. acting as both a vulnerability scanner and a phishing site. Five countries (USA, China, France, Indonesia and Russia) accounted for more than 47% of the scanner attacks seen last year by Webroot, while Indonesia, China, and the USA were the country of origin for more than 31% of the spam attacks. China alone was responsible for just over 40% of the botnet attacks.

It's also important to remember that IP reputations are not static; they may appear on the malicious list, disappear, and then reappear. When we look at the blacklist contents from 2017, we see that the top 10,000 IP addresses most often associated with malicious activity were reused frequently, moving in and out of the list an average of almost 18 times a year, with some disappearing and reappearing more than 100 times each. This mirrors the rate for repeat offenders in 2016. With tens of millions of new IP addresses appearing on the blacklist in 2017, the need for continuous surveillance of the internet is clear. By identifying new malicious activity on an ongoing basis and updating blacklists in real time, we narrow the window of opportunity for attackers, as new malicious activity can be blocked early on.

Incredible Number of High-Risk URLs

Hundreds of thousands of new websites are created each day. Many are benign, but a sizeable number are compromised, or are created specifically to carry out cyberattacks. Since there are more than a billion websites in existence[v], an organization may be hard-pressed to safeguard its users against malicious sites. Compounding the difficulty is the fact that a benign site today could be malicious tomorrow, or even mere minutes from now. The only effective way for an organization to protect its users, data and brand is to use up-to-the-minute URL reputation data.

URLs can vary in terms of their relative risk to an organization, and the percentages can vary from year to year. Figure 5 shows the relative distribution of the categories in 2017. 25% of all URLs fall into the High Risk, Suspicious, and Moderate Risk categories, representing significant risk to organizations.

The 10 countries that hosted the most high-risk URLs in 2017 included a number of them that have appeared in the list in years past. The USA leads the list at 43%, virtually identical to the share it held in 2016. However, this number

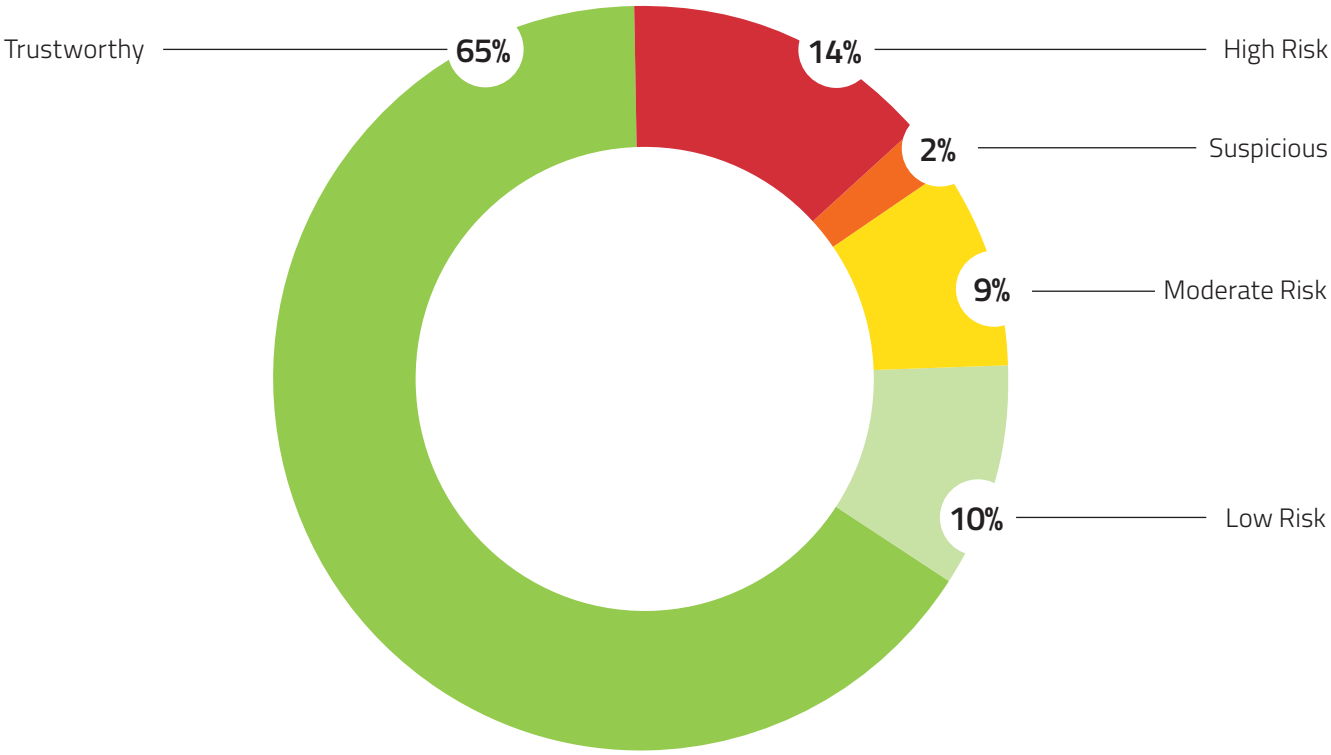


Figure 5: URLs by risk category

25% of all URLs in 2017 were malicious, suspicious or moderately risky.

can be misleading, since many bad actors host their sites in the USA, where websites are considered to be reliable, and geo-filtering services may not automatically block them as they do with sites from countries with more dangerous reputations. Webroot understands that geo-filtering is only one component to consider when trying to protect against bad sites; malicious categories, the IP address, and URL reputation must also be examined to make a strong security decision.

Switzerland, Japan, and Brazil joined the top 10 list of countries this year, albeit with relatively low percentages, replacing three countries/territories (Great Britain, Hong Kong and Australia) that had been on the top 10 list in 2016. Six of the countries, USA, China, Russia, France, Ukraine, and Brazil, are on both the list of top 10 countries with malicious IP addresses, and those with High Risk URLs. It is important to understand that attackers, to increase the chance of infection, typically try to localize the payload server to the country of attack.

Webroot has found that certain types of sites are more likely to be high-risk or suspicious, relative to others; these include business and economy, shopping, society, streaming media, and shareware and freeware sites. Those most likely to be trustworthy, based on the URLs observed by Webroot in 2017, include health and medicine, news and media, and society sites.

High-risk URLs fell into two major categories: malware sites (33%) and proxy avoidance and anonymizers (40%). The rest were phishing and other fraud sites (15%), botnets (10%), and spyware and adware (2%).

Keep in mind: although a given site's category might not be considered malicious, the organization may choose to restrict its users from accessing it, such as the shopping category.

Figure 6: High-risk URLs by country

Webroot continually monitors URLs and has examined more than 27 billion URLs to date. The process of analysis takes into consideration the website's history, age, rank, location, networks, links, real-time performance, and behavioral information. The analysis results in each URL being labelled as belonging to one of 82 primary content categories defined by Webroot, indicating its primary purpose such as real estate, shopping, gambling and the like, or malicious intent such as keyloggers and monitoring, spyware or phishing. Independent of category, each URL is assigned a risk score of 1-100, which falls into one of five categories: High Risk, Suspicious, Moderate Risk, Low Risk, or Trustworthy. This information, made available through the BrightCloud® Web Classification and Reputation Services, can be used by organizations to set up web access policies that will protect their users from online threats, control internet usage, and ensure compliance.

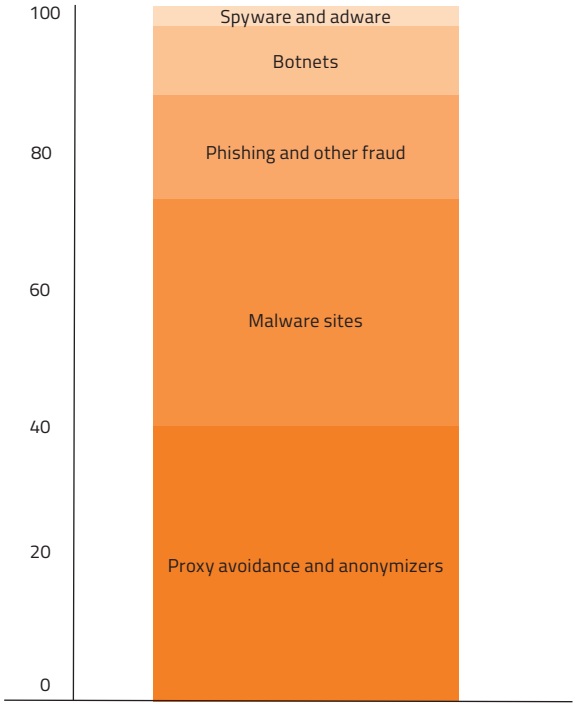


Figure 7: High-risk URLs by category

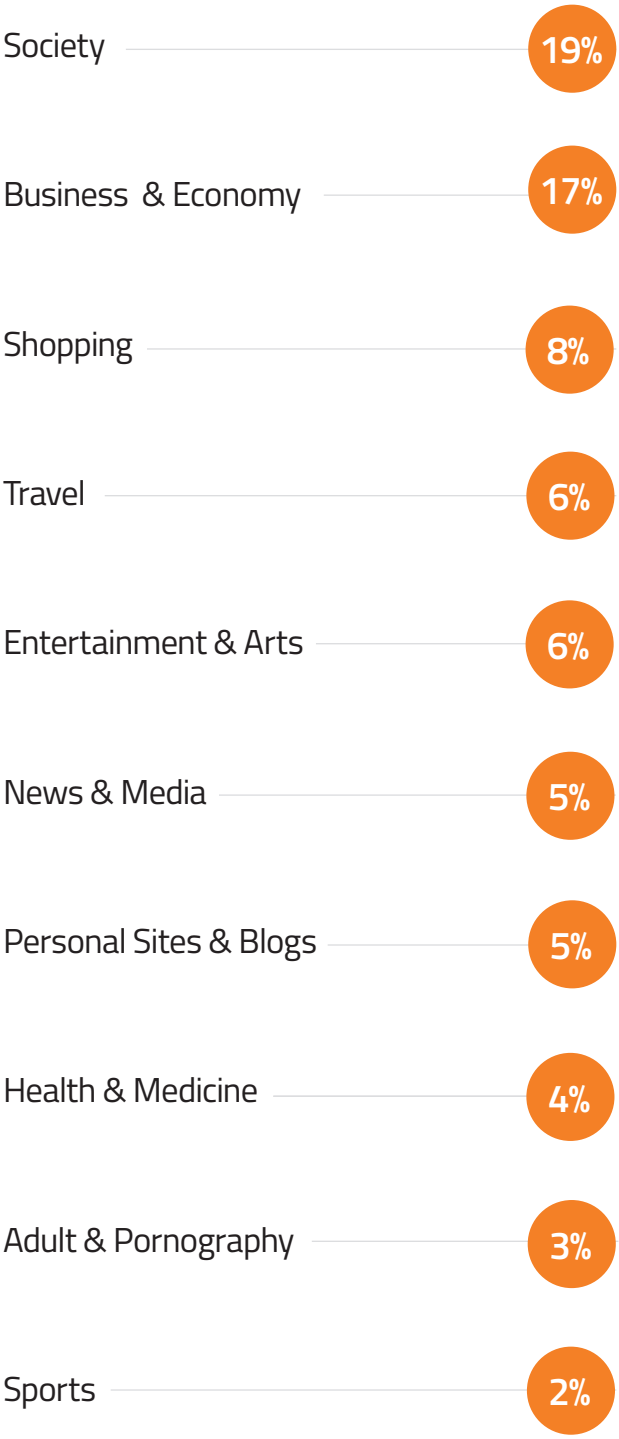


Figure 8: Top 10 non-malicious URL categories in 2017

Phishing Attacks Are More Targeted and Dangerous

Phishing remains one of the most used and most successful attack vectors. Highly targeted attacks use social engineering, relying on themes that are relevant, interesting, or appropriate to the targeted individual. When the user clicks a link in a phishing email that takes them to a malicious site, or opens an attachment carrying malware, they invite the attacker into the network.

The Webroot Threat Research team found that phishing attacks continue to be short-lived. Most phishing sites were online for 4-8 hours. Of the sites observed, the longest-lived was up for just 44 hours, and the shortest-lived was only up for 15 minutes. This brief duration demands that organizations use real-time anti-phishing solutions that can assess if a site's phishing risk level in real time, rather than putting faith in static blacklists that can't keep up with such short lifecycles.

Most phishing sites were online for 4-8 hours.

In 2017, Webroot saw millions of phishing attempts and tens of thousands of unique IPs hosting phishing sites. Despite the huge numbers, a deeper dive reveals intriguing information:

- 50 of the unique IPs hosting phishing sites produced over 1.5 million phishing attacks.
- A single IP was responsible for more than 400,000 phishing sites.
- 90% of the phishing attacks observed in 2017 came from a scant 62 domains.

Attackers take several steps to evade detection. Domain names are used only once or infrequently to avoid being blocked by static IP lists. We also found that almost 25% of phishing sites used IP masking, which makes it more difficult to discern the actual IP address of the domain. Another common tactic is to use benign domain names and replace a single web page with phishing content. When inserted as a disconnected, isolated page (i.e. no pages on the site point to the phishing page, nor does the phishing page point to any other pages on the site), it is nearly impossible for crawlers to detect the phishing threat.

Almost 25% of phishing sites used IP masking to hide the domain.

The sites targeted for impersonation change from year to year. The most impersonated sites in 2017 included some recurring names, such as Google, Microsoft, Dropbox, Facebook, PayPal, and Yahoo, as well as some new ones: shipping company UPS, money transfer service Ria, Israel's Bank Hapoalim, and entertainment software provider Blizzard.

Of the URLs that impersonated the 20 most-targeted companies in 2017, all but one were either impersonating financial services websites or technology company websites.

At the top of this list in 2017 was UPS, an impersonation responsible for 52% of the phishing attacks. Next was another new entrant, Ria, at 23% of the attacks. As more and more business is conducted online, it's reasonable to assume that services aimed at online purchases, such as package delivery and money transfers, would rise to the top of the targeted sites.

Technology companies represent a large percentage (26%) of the top 20 targeted companies, but 74% of the companies impersonated during the year were financial institutions. Although fewer in number, the volume of attacks on technology companies was substantial: more than 356,000 attacks were carried out using impersonated UPS pages, compared to a little more than 161,000 for Ria. Technology company phishing can be lucrative; they are sometimes easier to break into than a financial company account, and reused credentials frequently allow attackers to break into multiple accounts at a time.

Of the countries that host the impersonated sites, 36% of the phishing sites were hosted in the USA, and 13% in the Netherlands. Brazil and Russia each accounted for 2%, with Denmark and Lithuania hosting 1% each.

Very short lifecycles and the use of seemingly-innocent domain names make it increasingly difficult to detect and stop phishing attacks. Webroot addresses this growing problem. The BrightCloud® Real-Time Anti-Phishing Service, which helps power Webroot SecureAnywhere® protection for endpoints, automatically determines, in milliseconds, if a website being requested poses a phishing risk. Immediacy is necessary; a site that was benign a minute ago may now be malicious, and the user must be prevented from accessing it.

Webroot® Security Awareness Training, a training platform that helps organizations reduce the risks and costs of cyber threats through end user education, can boost a company's ability to deter phishing attacks. Due to the very high percentage of users that click through to a simulated phishing site and try to enter credentials, time-of-need training is a must. Based on Security Awareness Training figures from late 2017, roughly 42% of users who opened a phishing simulation email clicked through to the simulated phishing web page, and 65% of people who clicked through tried to enter their credentials. Education presented at the time the user falls for the simulation helps reinforce the lesson.

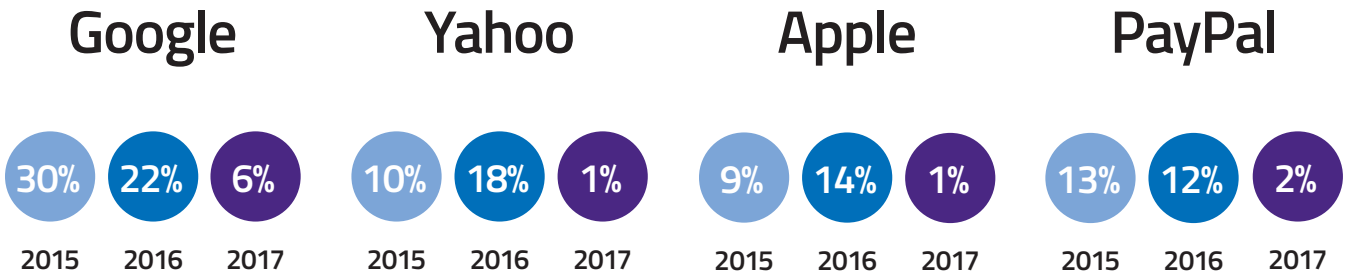


Figure 9: Changes in most heavily impersonated brands

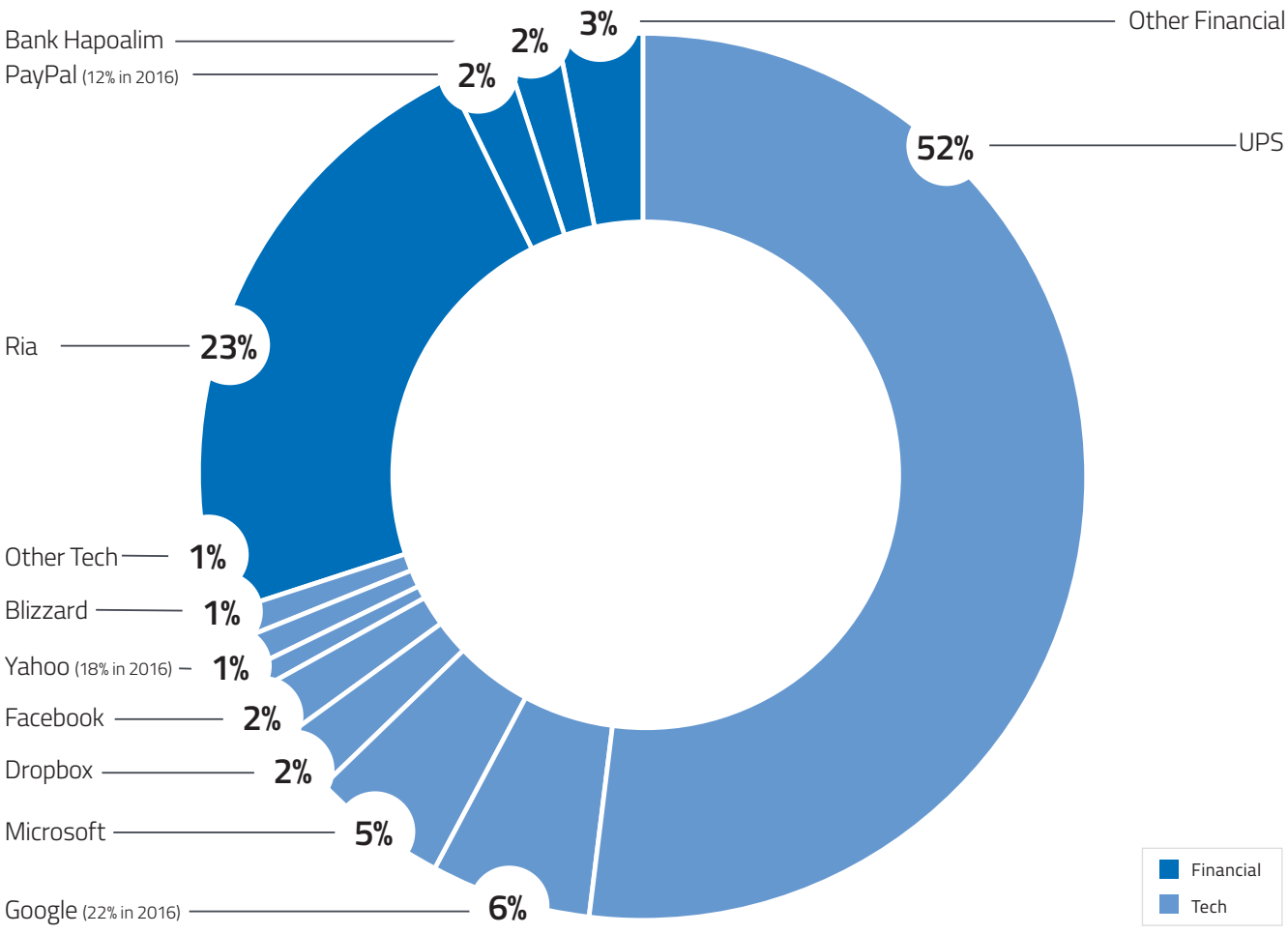


Figure 10: Top 10 sites impersonated in phishing attacks during 2017

Universal Threat of Malicious Mobile Apps

Smartphones and tablets are the devices of choice for most people. In fact, the total number of smartphone users worldwide is expected to pass the two and a half billion mark by 2019[vi]. As the world increasingly connects to the internet while on the go, these devices become a prime target for attackers. The malicious mobile app is the most common form of attack. Legitimate apps can be downloaded from official app stores, but similar apps and ones virtually identical in appearance are also available on many other sites. These can be malicious apps that masquerade as popular games, corporate utilities, and a wide variety of other application types.

Webroot is constantly monitoring app stores and other repositories; when we find new or recently updated apps, we analyze them for malicious behavior. This intelligence is available to customers through Webroot mobile protection applications and also through the BrightCloud® Mobile Security SDK.

Webroot analyzed millions of new or updated mobile apps in 2017, bringing the total number of apps analyzed to more than 62 million. Results of the analysis placed each mobile app in a reputation category ranging from highest to lowest risk: Malicious, Unwanted, Suspicious, Moderate, Benign or Trustworthy.

The percentage of mobile apps classified as malicious was a bit higher in 2017 as in 2016 (32% vs. 29%); unwanted apps came in lower in 2017 (8% vs. 11%) while suspicious apps stayed relatively the same (18% vs. 21%). A lower percentage

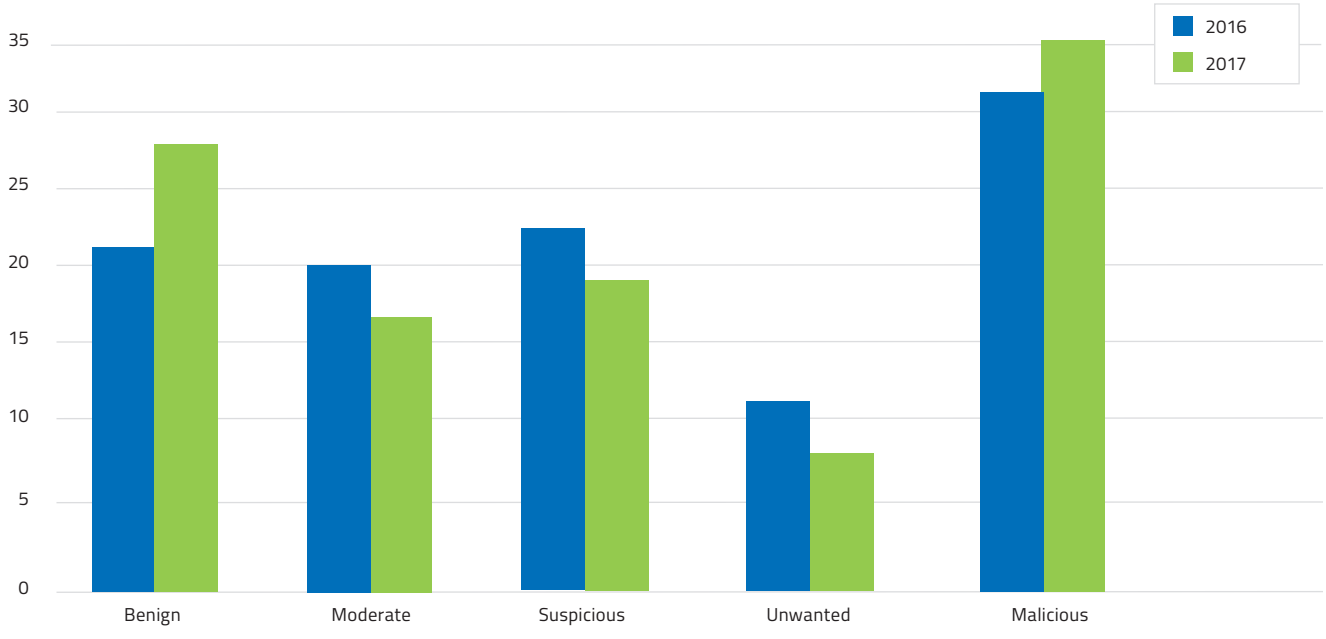


Figure 11: Distribution of Android™ app reputations over the past two years

32% of mobile apps were malicious.

of apps seen in 2017 was classified as Moderate (16% vs. 19% in 2016), while Benign apps accounted for more than one-quarter of all mobile apps evaluated 26% in 2017 contrasted with 20% in 2016.

When examined on a month-by-month basis, April saw the largest percentage of malicious apps (more than 60% of the total mobile apps seen by Webroot that month were deemed malicious) and December the second-largest (41%). The lowest months were January (14%) and February (25%). The percentage of suspicious mobile apps stayed relatively constant throughout the year, with an upsurge in October and November to 25% and 23%, respectively, while the other months remained between 15-18%. In terms of absolute numbers, the highest incidences of malicious apps were seen in May and July 2017. This may correlate to the Cloak and Dagger attack on Android devices that was first seen in May and lasted for several months, as well as the Judy malware that was discovered in May.

Webroot classified malicious apps in 2017 based on their primary activity, as shown in Figure 12, which compares 2017 to 2016. Trojans continue to be the most prevalent form of malicious mobile app. At 67% for the year, they are more common than in previous years where the figure was just above 60%, but continue to far outpace other types of malware. Second-most prevalent was the PUA, representing one-fifth of mobile apps analyzed, down from the 26% seen in 2016. While these can be annoying, especially when they are loaded with ads, the app is still functional. Webroot has found, however, that some seemingly-annoying apps can, in fact, be multi-purpose malware. For example, the Trojan known as Loapi displays an unending series of ads, which distract the user while the malware participates in DDoS attacks, sends messages, and can silently subscribe the user to paid services.

Malicious apps can be devastating, especially when they steal information or download ransomware. LeakerLocker ransomware was found hiding inside two Android apps in 2017: Booster & Cleaner Pro, and Wallpapers Blur HD. Rather than encrypt files, the malware threatened to extort a payment to prevent the spread of the victim's private information. Cryptojacking also hit mobile devices, draining smartphones so drastically that, in some cases, it overworked the hardware, actually damaging the device.

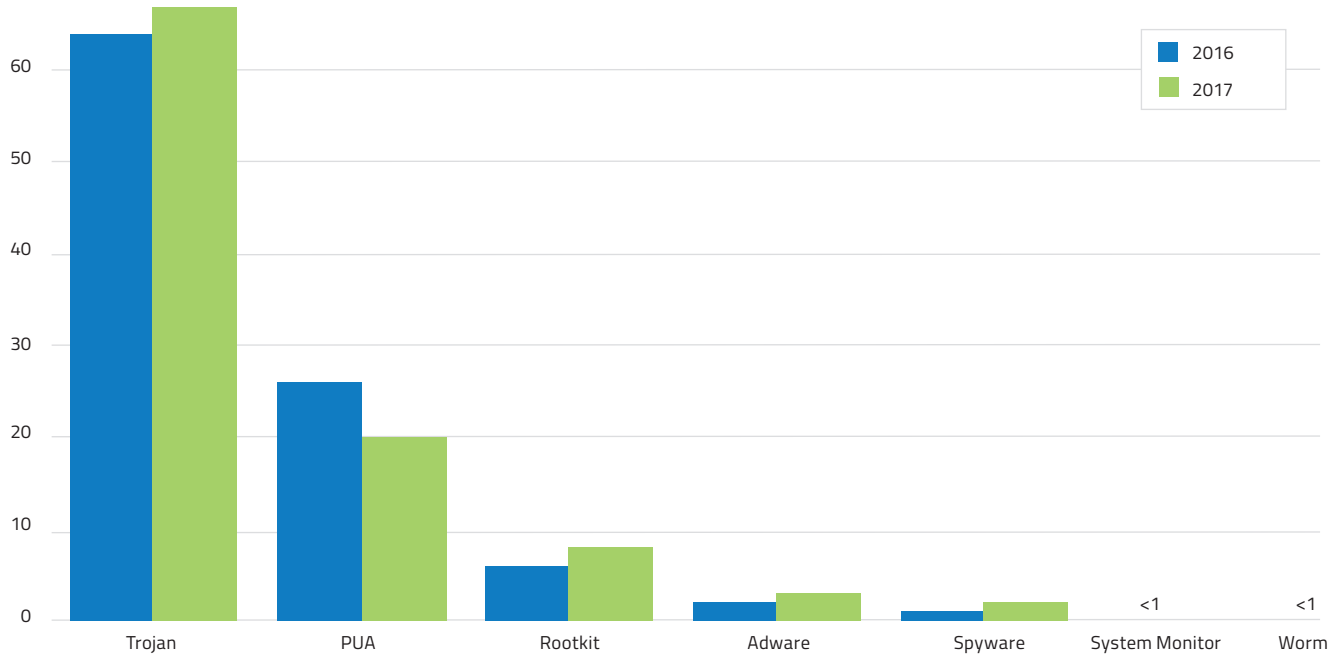


Figure 12: Malicious apps by primary activity over the past two years

Summary

The data collected and analyzed by Webroot throughout 2017 shows that the threat landscape is continuing to evolve rapidly. Attackers quickly learn what works and what doesn't, and they're constantly trying new ways to get around established defenses.

» Polymorphic attacks continue to be the favorite for malware (more than 94% of all bad executables seen by Webroot).

» Ransomware grew in 2017. Two of the biggest attacks ever seen caused billions of dollars in damages and employed novel ways of spreading throughout corporate networks.

» Cryptojacking is a rapidly emerging threat. Stealing CPU power to mine cryptocurrency provides a profitable path to easy money.

» High-risk IP addresses continue to cycle from malicious to benign and back again. Webroot saw 10,000 malicious IP addresses continuously reused in 2017, moving on and off the list an average of 18 times each. The majority represent spam sites (67%), which are very difficult to detect without dynamically-updated IP address lists and contextual analysis.

» One-fourth of URLs monitored in 2017 fell into the High Risk, Suspicious and Moderate Risk categories, representing significant risk to organizations and individuals alike.

» Phishing attacks are increasingly targeted, using social engineering and IP masking to trap their victims. Just a few domains (62) were responsible for 90% of the phishing attacks we observed.

» Malicious mobile apps continue to pose a serious threat: 32% of the apps analyzed by Webroot in 2017 were found malicious.

The rising prevalence of polymorphism, ransomware, and cryptojacking, the growing volume of malicious URLs, more sophisticated phishing attacks and malicious mobile apps, all paint a picture of a dangerous, dynamic threat landscape that calls for multi-layered defenses. While migration to more secure operating systems like Windows 10 can help mitigate the threat, it's only a small part of the solution. Today, it is crucial for organizations to use automated, real-time decision-making based on continuously-updated threat intelligence, contextual analysis and advanced endpoint and network protection. When coupled with strong user security training, any organization can materially reduce its exposure to unacceptable risk.

About the Data

The statistics presented in this annual threat report are derived from metrics automatically captured and analyzed by the Webroot Threat Intelligence Platform, our advanced, cloud-based machine learning architecture. This system provides proactive protection for users and networks against both known and zero-day, never-before-seen and advanced persistent threats. Threat intelligence produced by the platform is used by Webroot SecureAnywhere® endpoint security products and by technology partners through Webroot BrightCloud® Threat Intelligence services. Our threat intelligence is based on visibility of the entire IPv4 and in-use IPv6 space, billions of URLs, tens of millions of new and updated mobile apps, and all Webroot SecureAnywhere endpoints worldwide. Advanced machine learning techniques, real-time scoring with confidence levels, and continuous updates enable Webroot threat intelligence to be highly effective at identifying and stopping even the most sophisticated threats.

Webroot takes a unique approach to machine learning, based on massive data processing capacity, a proprietary implementation of the most advanced technology available, and a powerful contextual analysis engine. Contextualization is a "guilt by association" model that links internet objects. Capturing an extensive range of characteristics for each internet object observed (up to 10 million characteristics per object) enables Webroot to determine if the object poses a threat at the precise time of analysis. Our patented approach maps attack and threat behavior across vectors, analyzing the relationships among URLs, IPs, files and mobile apps. For example, if a user runs a mobile app that tries to access the contact list and transfer it to an IP address, the malicious behavior of the app would impact the reputation score of the IP address. This ability to correlate current associations among objects with history on how millions of objects have behaved over time is what makes Webroot threat intelligence predictive in nature.

[i] Why Enterprises Are Upgrading to Windows 10 Faster Than Expected. CIO, April 2017. Retrieved from https://www.cio.com/article/3187503/windows/why-enterprises-are-upgrading-to-windows-10-faster-than-expected.html

[ii] "WannaCry" ransomware attack losses could reach $4 billion. Moneywatch, May 2017. Retrieved from https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

[iii] NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion in Revenue. Cyberreason, Nov. 2017 Retrieved from https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue

[iv] Hackers are using YouTube Ads to Mine Monero Cryptocurrenty. HackRead.com, Jan 2018. Retrieved from https://www.hackread.com/hackers-using-youtube-ads-to-mine-monero-cryptocurrency/

[v] October 2017 Web Server Survey, Netcraft, 2017. Retrieved from https://news.netcraft.com/archives/2017/10/26/october-2017-web-server-survey-13.html

[vi] Number of smartphone users worldwide from 2014 to 2020 (in billions). Statista, 2018. Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

CloudPost Networks. Inc.
Prashanth Kalika
2445 Augustine Drive, Suite #601
Santa Clara, CA 95054
408-564-2367
support@cloudpostnetworks.com

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 webroot.com