

# 2017 Webroot

**ANALYSIS**  
CYBER-CRIMINALS  
SPYWARE HIGH RISK

**BENIGN**  
MONITOR NETWORK

**LWARE**  
BOTS  
NETWORK MALWARE

**RISK**  
EMERGING

**ANONYMIZER**  
BLACKLIST

**RANSOMWARE**  
COMPROMISED

**PHISHING**  
MALWARE

**PUA**  
LIFE CYCLE  
ANONYMIZER

**SPYWARE**  
SENSORS

**TARGETS**  
ADVARE

**MOBILE APPS**  
MALWARE

**ADVARE**  
HIGH RISK

**KILL CHAIN**  
MOBILE APPS

**PISHING**  
ADWARE

**MALWARE**  
KILL CHAIN

**PHISHING**  
SENSES UNIQUE

**BEHAVIORS**  
CROSS-CRIMINAL UNPREDICTED

**REMOTE**

**COMPROMISED CYBERSECURITY**  
**BLACKLIST**  
**DEBRISWARE**  
**ENCRYPT**  
**UNWANTED**  
**MALICIOUS BENIGN**  
**COMPROMISED**  
**KILL CHAIN**  
**CONTAMINATED**  
**BOTNET**  
**SPAM**  
**POLYMORPHIC**  
**MONITOR**  
**COMPROMISED**  
**KILL CHAIN**  
**BOTNET**  
**UNIQUE**  
**SENSORS**

**NETWORK INFECTION**

MALWARE SENSORS THREATS VARIANTS MONITOR UNWANTED SPAM

REPUTATION: SPYWARE HIGH RISK SPYWARE THREATS MALICIOUS SENSORS INFECTION CYBER-CRIMINALS POLYMORPHIC

ATTACKERS TARGETS

EMERGING REPUTATION KILL CHAIN

SUSPICIOUS ASYLUM GRISM REMOTE CALL CHAIN

RANSOMWARE ANONYMIZER SPYWARE THREATS CYBERSECURITY PHISHING HIGH RISK HIGH RISK UNSECURED KILL CHAIN RISK SENSORS PUA REMOTE

POSSIBLE SPAM

EMERGING INFECTION ANONYMIZED HIGH RISK EMERGING VARIANTS MAIWFAR

**BLACKLIST SUSPICIOUS**  
**RISK ATTACKERS DETECT**  
**SUSPICIOUS ENCRYPTION**  
**EMERGING CRITICAL**  
**THREATS MALWARE**

**DETECTION ZERO-DAY**  
**EMERGING SENSORS**  
**UNIQUE MALICIOUS**

**TRUSTWORTHY RANSOMWARE**  
**RANSOMWARE ZERO-DAY**  
**ANALYSIS BLACKLIST SUSPICIOUS**

**IMPERSONATED EMERGING**  
**ANALYSIS DETECT ENERGY CONSUMPTION**  
**POLYMORPHIC UNSECURED**

**BENIGN BEHAVIORS SENSORS**  
**DOMAINS POLYMORPHIC RISK**

**BLACKLIST RANSOMWARE ENCRYPTION**  
**MALWARE MONITOR**  
**REMOTE REPUTATION**

**POLYMORPHIC REMOTE**  
**CRITICAL BENIGN**  
**DETETION ADVANCED**  
**ATTACKERS POLYMORPHIC LIFE CYCLE**

**BOTNET ANALYSIS MONITOR**  
**LIFE CYCLE ENCRYPTION TARGETS**  
**UNSECURED POLYMORPHIC ATTACKERS**

**ATTACKERS MALICIOUS**  
**TRUSTWORTHY**  
**POLYMORPHIC ANALYSIS BOTNET**  
**UNSECURED DETECT CRITICAL PIA**  
**REMOTE BEHAVIORS**

**ADWARE** SPYWARE  
VARIANTS KILL CHAIN NETWORK LIFE CYCLE VARIANTS  
**CYBERSECURITY** SPAM ADWARE INFECTION  
**NETWORK** SPYWARE TARGETS  
**UNSECURED** VARIANTS  
**CRITICAL** SPAM NETWORK TRUSTWORTHY  
**ZERO-DAY** MALWARE  
VARIANTS REPUTATION  
**BLACKLIST** FULL  
POLYMORPHIC PHISHING BEHAVIORAL  
BEHAVIORS ZERO-DAY  
**MALWARE** POLYMORPHIC  
**DOMAINS**

UNSECURED  
MOBILE APPS  
BEHAVIORS TRUSTWORTHY BOTNET  
THREATS DETECTION POLYMORPHIC  
ZERO-DAY RISKS PUPPETIZING  
RISK APPS SPYWARE  
EMERGING AREA51 APPS  
RISK ZOMBIEWARE RANSOMWARE ANALYSIS  
APPENDIX REPUTATION  
SENSORS APPENDIX  
REPUTATION  
PUA ANALYSIS  
UNIQUE  
APPENDIX  
INVESTIGATIVE  
TECHNIQUES

**VICTIM**

- RANSOMWARE
  - LIFE CYCLE
  - BLACKLIST
  - PUSHING
  - RANSOMWARE
  - MALICIOUS
  - THREATS
  - PUAs
  - SPYWARE
- SPYWARE
  - LIFE CYCLE
  - ANONYMIZER
  - BENIGN
  - PHISHING
  - IMPERSONATED
  - HIGH RISK
  - ADWARE
  - SENSORS
  - UNIQUE
  - MOBILE APPS
  - KILL CHAIN
  - DATA LEAK
  - CRYPTOJACKING
  - MONITOR
  - RISK
  - VARIANTS
- ADWARE
  - LIFE CYCLE
  - ANONYMIZER
  - BENIGN
  - PHISHING
  - IMPERSONATED
  - CROSS-CHANNEL
  - BEHAVIORS
  - UNIQUE
  - MOBILE APPS
  - KILL CHAIN
  - DATA LEAK
  - CRYPTOJACKING
  - MONITOR
  - RISK
  - VARIANTS
- MALWARE
  - LIFE CYCLE
  - ANONYMIZER
  - BENIGN
  - PHISHING
  - IMPERSONATED
  - CROSS-CHANNEL
  - BEHAVIORS
  - UNIQUE
  - MOBILE APPS
  - KILL CHAIN
  - DATA LEAK
  - CRYPTOJACKING
  - MONITOR
  - RISK
  - VARIANTS
- PHISHING
  - LIFE CYCLE
  - ANONYMIZER
  - BENIGN
  - PHISHING
  - IMPERSONATED
  - CROSS-CHANNEL
  - BEHAVIORS
  - UNIQUE
  - MOBILE APPS
  - KILL CHAIN
  - DATA LEAK
  - CRYPTOJACKING
  - MONITOR
  - RISK
  - VARIANTS

# What's inside

- 1 The Webroot Perspective
- 3 Continued predominance of polymorphic malware
- 5 Still millions of malicious IP addresses
- 9 Incredible percentage of High Risk URLs
- 13 Escalating threats from phishing attacks
- 17 Alarming numbers of malicious apps
- 20 Conclusion
- 21 About Webroot

## **Contributors:**

Jurijs Girtakovskis | Ken Jacobi | David Kennerley | Kiran Kumar | Grayson Milbourne | Tyler Moffitt | Cameron Palan | Steve Snyder



# Foreword

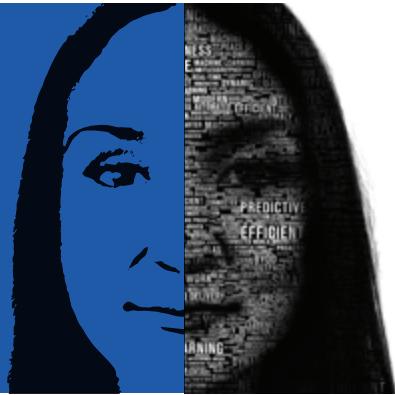
Hal Lonas | Chief Technology Officer

A year ago, we accurately predicted cybersecurity threats that have since been realized, from attacks that targeted the presidential election to the continued onslaught of ransomware. Awareness of cyber threats may be at an all-time high, but attacks are still both prevalent and successful. Nonetheless, for the first time ever, we witnessed a minor year-over-year decrease in the volume of malware. In part, the decline can be attributed to the increased security awareness mentioned, but it also reflects changes in cybercriminal tactics. We observed a drastic increase in malicious website encounters and significant changes to the malicious IP landscape, as well as an overall decrease in the average lifespan of phishing sites. These observations are evidence of a highly reactive threat landscape that adapts at a moment's notice to changes in the ways users try to protect themselves.

At Webroot, we know we need to operate smarter and faster than the cybercrime ecosystem to be effective. Our technology puts a premium on real-world, real-time visibility into various threat vectors as they are encountered. We use advanced machine learning to analyze and correlate billions of internet objects and daily events, and leverage that data to predict where threats will next emerge. This precise awareness and predictive capability powers all Webroot products, as well as dozens of partner integrations, and provides the quality of real-time threat intelligence necessary to prevent cyberattacks.

The 2017 Webroot Threat Report provides a uniquely insightful global view into the analysis and discoveries made by the Webroot® Threat Intelligence Platform to provide insights on key trends and risks as seen by our users over the past year.

# The Webroot Perspective



The Webroot® 2017 Annual Threat Report presents analysis, findings, and insights from the Webroot Threat Research team on the state of threats, including the following:

- » Malware and potentially unwanted applications (PUAs)
- » IP addresses associated with malicious activity
- » URL reputations and classifications
- » Phishing targets, sites, and URLs
- » Mobile app reputations and the threats mobile apps can contain

This report is intended to help you understand the current threat landscape and related trends so you can prepare your organization to better handle threats during the coming year.

The statistics throughout this report come from threat intelligence metrics automatically captured and analyzed by Webroot through our threat intelligence platform. The Webroot® Threat Intelligence Platform is an advanced, cloud-based machine learning architecture that continuously produces threat intelligence used by Webroot SecureAnywhere® endpoint security products, FlowScape® analytics, and by technology partners through Webroot BrightCloud® Threat Intelligence Services. Unlike traditional list-based or single-vendor threat intelligence, Webroot threat intelligence is highly effective for identifying and stopping even the most sophisticated zero-day, never-before-seen, and advanced persistent threats.

We believe there are four key elements to producing and delivering timely, accurate, and predictive threat intelligence:

## 1. Visibility

Provide unmatched worldwide threat visibility by utilizing a wide range of high-quality input sources, and continuously scanning the entire internet and incorporating data from millions of real-world endpoints

## 2. Advanced Machine Learning Techniques

Predict the expected behavior of each observed object (executable file, mobile application, URL, IP address, etc.) at impressive speed and with high accuracy by using patented contextual analysis methods and other proprietary adaptive machine learning techniques

## 3. Real-Time Scoring with Confidence Intervals

Make threat intelligence actionable by leveraging the massive processing power of the cloud to create a reputation index value for each observed object

## 4. Continuous Updates

Ensure that the latest threat intelligence is available in real time to Webroot customers and partners

The elements involving machine learning and real-time scoring merit additional explanation. Webroot has a unique approach to machine learning based on using an extensive range of characteristics for each internet object observed to evaluate its nature. Some of Webroot's machine learning applications can capture up to 10 million characteristics per observed object. This enables Webroot to analyze practically any information pertaining to an object and determine if it poses a threat at the precise time of analysis. Webroot's machine learning techniques automate the research and classification of over half a trillion objects a day.

To make the machine learning results actionable, Webroot assigns every object a reputation score between one and one hundred. The lower the score, the more likely the object is to behave maliciously. Reputation scores are critical because they allow Webroot customers and partners to consider the shades of gray in cybersecurity, rather than relying on a basic good/bad determination. Customers and partners can then fine-tune the score thresholds at which their devices will block objects.

Another important part of the machine learning is the use of Webroot-patented contextual analysis methods. Contextual analysis is, fundamentally, “guilt by association.” For example, if a specific URL has been serving malware every day for the last five years, Webroot has already assigned that URL a poor reputation score. When a new file becomes available from that URL, Webroot would automatically reduce that file’s reputation score because of the associated URL’s score. Another example is a user launching a new mobile app that immediately tries to access the user’s contact list and transfer it to an IP address that appears ready to accept that contact list. Since the mobile app is exhibiting malicious behavior, the IP address it wants to use would have its reputation score reduced immediately.

The power of contextual analysis is the ability to correlate current associations between objects, combined with insights on past behavior, which results in the predictive nature of Webroot threat intelligence.

The big data processing capacity used in this platform, coupled with the massive scale of Webroot’s machine learning models and proprietary implementation of a powerful contextual analysis engine, enables the Webroot® Threat Intelligence Platform to:

- » Scan the entire IPv4 space and monitor in-use IPv6 addresses to continuously update a list of 8 to 12 million malicious IP addresses
- » Classify and score the reputations of billions of URLs
- » Detect new phishing sites in real time
- » Analyze behaviors to classify over one million new, unique executable files each day
- » Assess the risk of tens of millions of new and updated mobile apps

Webroot threat intelligence helps protect millions of organizations and individual consumers around the world. Webroot SecureAnywhere® endpoint security products also provide an exceptional vantage point on the threats customers currently face. Although the primary purpose is so Webroot can help its customers stay ahead of emerging threats, it also enables Webroot to analyze activity observed on Webroot endpoints in order to create the portrait of the threat landscape documented in this report.



**27+**

Billion URLs



**600+**

Million Domains



**4+**

Billion IP Addresses



**13+**

Billion File Behavior Records



**50+**

Million Mobile Apps



**40+**

Million Connected Sensors

# Continued predominance of polymorphic malware



For several years, the most important trend in malware and potentially unwanted application (PUA) executables has been polymorphism. Polymorphic malware and PUAs, such as spyware and adware, are generated by attackers in ways that make each instance unique. Attackers do this to defeat traditional security approaches, which rely on the relative ease of detecting one instance of malware delivered to a large number of people. Detecting a million unique instances of malware as they are delivered to the same number of people quickly enough to prevent a breach requires a completely new approach to analyzing executables.

When Webroot SecureAnywhere protection is installed on an endpoint, it creates a digital fingerprint of every executable file it encounters. During 2016, approximately 94% of the malware and PUA executables observed by Webroot were only seen once, underscoring how prevalent polymorphism is. Webroot's threat intelligence and discovery model, along with its use of digital fingerprints from real-world files, was developed specifically to identify and stop polymorphic malware and PUA executables before they can damage their targets. In addition to using this model to protect its customers, Webroot also makes it available to partners through BrightCloud File Reputation intelligence. The same advanced machine learning models also power the new BrightCloud Streaming Malware Detection solution for security vendors. In several independent tests during 2016, Webroot SecureAnywhere Business Endpoint Protection protected against 100% of new malware tested within a 24-hour period.<sup>1</sup>

Webroot endpoints observe hundreds of millions of new instances of executable files each year. Of the new executable file instances in 2016, around 2.5% were malware and 2.2% were PUAs. As Figure 1 shows, there have been major changes in the relative percentages of malicious executables out of all new executables over the past three years.

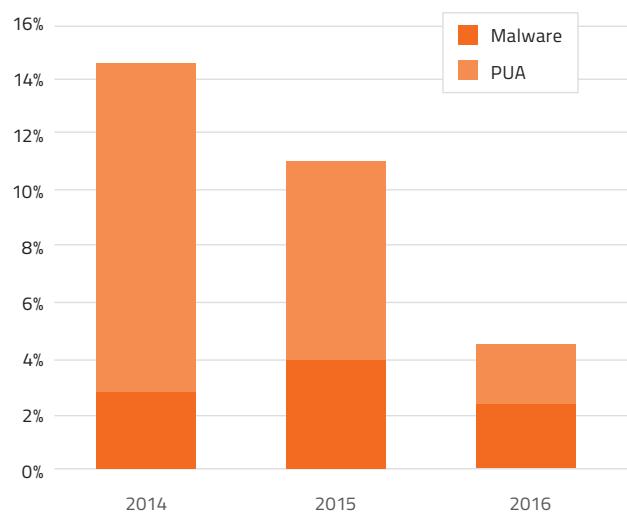


Figure 1: Percentage of malware and PUAs out of all observed new and unique executable files

Malware's share has dropped by 23%, while PUA's share has plummeted almost 81%.

More detailed analysis of the 2016 data reveals that the monthly counts of new PUAs dropped throughout 2016; the volume in December was less than 20% of January's volume.

There are two likely reasons that the volume of new malware and PUAs has stopped growing at the astronomical rates we had seen so far. 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.

Approximately one in every 40 new executable file instances observed in 2016 was malware. These files are highly customized, often to target individuals, and they cannot be stopped by traditional malware detection technologies.

During 2016, Webroot classified 56% of previously unseen malware executables as malicious within the first hour of encounter, and the vast majority were caught and blocked in real time. This rate increased to 90% over a 12-hour period. Webroot is able to accomplish this in part because of its record of digital fingerprints for every executable file encountered by Webroot SecureAnywhere solutions, combined with automated systems that use those fingerprints to create new detection rules to stop similar files in real time. Even though attackers continue to innovate and use low-volume attacks to avoid detection, Webroot also continually innovates to stop them from breaching systems and data.

## The Risks of Ransomware

Ransomware is malware that encrypts files or a device's storage and demands payment to restore access. Recently, there have been countless news stories about hospitals and other institutions effectively being shut down by ransomware. The FBI estimated that cybercriminals would collect over \$1 billion in ransoms during 2016.<sup>2</sup> Actual losses suffered by organizations are certainly higher than that due to disruption of productivity and business continuity, and we must also account for a general reluctance to report ransomware incidents. In 2017, we expect ransomware to become an even larger problem. The Webroot Threat Research team closely monitors ransomware and has identified the most important trends of 2016 and predicted likely 2017 trends.

The first trend is the rise of Locky. Locky was the most successful ransomware of 2016. In its debut week in February, it infected over 400,000 victims, and has been estimated to have earned over \$1 million a day since then.<sup>3</sup> Locky was one of the first ransomware variants to encrypt unmapped network drives, which has been particularly devastating to small businesses. At first, Locky propagated through email attachments with macros that, when run, would download and execute the ransomware. Throughout 2016, Locky evolved not only to use many other delivery methods, but also to camouflage itself to avoid detection and to make analysis more difficult for security researchers. Locky shows no signs of slowing down, and will likely be just as prolific in 2017.

Another important trend is the frequent changes in the exploit kits used by ransomware. For example, in the first half of 2016, most exploit kit ransomware was distributed using Angler or Neutrino. In May, Webroot saw a huge drop in Angler-based ransomware, and by early June it had virtually disappeared. Cybercriminals who were using Angler began switching to Neutrino, and the Neutrino authors were able to double their price for the lack of competition. A few months later, Neutrino followed in Angler's footsteps and disappeared. At the end of 2016, the most commonly used exploit kits were variants of Sundown and RIG, the majority of which support Locky.

The final trend to discuss is ransomware-as-a-service (RaaS). Although it emerged in 2015, it wasn't until 2016 that RaaS had truly carved out its niche in the ransomware landscape. Ransomware-as-a-service enables cybercriminals without the knowledge or resources to create their own ransomware to easily generate customized attacks to meet their needs. The original authors of whichever RaaS variant is used automatically get a percentage of all paid ransoms. Ransomware-as-a-service offerings very similarly to legitimate software, with frequent updates and utilities to help ransomware distributors get the most from their service. The availability and ease of ransomware-as-a-service are likely to mean even greater growth in ransomware incidents.

<sup>1</sup> [https://www.mrg-effitas.com/wp-content/uploads/2015/12/Webroot\\_vs\\_Sophos\\_report.pdf](https://www.mrg-effitas.com/wp-content/uploads/2015/12/Webroot_vs_Sophos_report.pdf)

<sup>2</sup> <http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html>

<sup>3</sup> <http://www.smartdatacollective.com/david-balaban/412688/locky-ransomware-statistics-geos-targeted-amounts-paid-spread-volumes-and-much>

# Still millions of malicious IP Addresses



At any given time, millions of IP addresses are associated with malicious activity. For example, unsecured home computers and Internet of Things (IoT) devices may be compromised and then remotely directed by attackers to launch attacks on others. Automatically blocking network traffic from these IP addresses can prevent many attacks from reaching their targets.

To facilitate this, Webroot actively scans the entire IPv4 space and monitors in-use IPv6 addresses for signs of malicious activity. Combining this with other data, then analyzing and correlating the data across numerous dimensions, the Webroot Threat Intelligence Platform creates a predictive risk score between 1 and 100 for each IP address. The lower the score, the greater the risk associated with that IP address, and the more often Webroot monitors that IP address' activity compared to other addresses.

To make the risk score values more meaningful, Webroot maps each score to one of the five tiers in the BrightCloud IP Reputation Index (Figure 2.) These tiers—High Risk, Suspicious, Moderate Risk, Low Risk, and Trustworthy—enable organizations to establish proactive policies that account for their risk tolerance and business needs. For example, an organization with a great deal to lose from a compromise might prohibit all activity involving IP addresses in the High Risk and Suspicious tiers, while an organization with lesser security concerns might allow use of its services from all IP addresses, while prohibiting system administration from addresses in the High Risk, Suspicious, and Moderate Risk tiers.

01-20 High Risk		These are high risk IP addresses. There is a high predictive risk that these IPs will deliver attacks – such as malicious payloads, DoS attacks, or others – to your infrastructure and endpoints.
21-40 Suspicious		These are suspicious IPs. There is a higher than average predictive risk that these IPs will deliver attacks to your infrastructure and endpoints.
41-60 Moderate Risk		These are generally benign IPs but have exhibited some potential risk characteristics. There is some predictive risk that these IPs will deliver attacks to your infrastructure and endpoints.
61-80 Low Risk		These are benign IPs and rarely exhibit characteristics that expose your infrastructure and endpoints to security risks. There is a low predictive risk of attack.
81-100 Trustworthy		These are clean IPs that have not been tied to a security risk. There is very low predictive risk that your infrastructure and endpoints will be exposed to attack.

Figure 2: BrightCloud IP Reputation Index tiers

Throughout 2016, Webroot identified malicious IP addresses from nearly 150 countries. The number of active malicious IP addresses in Webroot's constantly updated blacklist at any time ranges from 8 to 12 million. Over the course of 2016, 33 million unique malicious addresses appeared on the blacklist, a slight increase from 2015. This indicates that the trend seen in previous years is continuing; attackers are changing IP addresses to avoid detection. Once an IP address is associated with malicious activity, security vendors add it to their blacklists. The time needed to identify the malicious activity and provide the updated blacklist to customers varies

by vendor, but Webroot constantly identifies new malicious activity and updates its blacklist, enabling real-time detection of activity from new malicious IP addresses. The Webroot approach makes the window of opportunity for attackers as small as possible.

When analyzing our 2016 blacklist contents, we discovered some interesting patterns. For example, over 88% of the IP addresses appeared on the blacklist only once. Such an address might be from a host that was briefly compromised, then recovered and not used for malicious activity again. The address might also be from a host that was compromised the entire year and used for generating attacks all that time. Of the 12% of IP addresses that appeared more than once, a small group were added and removed from the blacklist repeatedly. The 10,000 IP addresses most often associated with malicious activity were added and removed from the blacklist an average of 18 times each in 2016.

This rate of change in repeat offenders underscores the importance of a constantly updated IP address blacklist. This blacklist enables an organization to be proactive in blocking threats that are likely to launch attacks. The Webroot blacklist not only lists malicious IPs, but also provides the risk score and reputation tier for each IP address, allowing organizations to set blocking thresholds that make the most sense for them.

To get a better understanding of the repeat offenders, Webroot identified the countries of origin for the 10,000 IP addresses blacklisted most often during 2016. Figure 3 shows the percentage of the top 10,000 addresses for each country.

Another view of the countries hosting the top 10,000 blacklisted addresses is shown in Figure 4, on page 7. This chart shows the relative percentages of these addresses for the countries with the largest totals in 2015 and 2016 combined. The United States continues to have far more malicious IP addresses than other countries, averaging



Figure 3: Repeat Offenders, Top 10 malicious IP origin countries

32% over the past three years, but the percentage varies significantly from year to year. The United States' share dropped by almost half from 2015 to 2016. Since approximately 55% of all registered IP addresses are in North America, the drop in the US share indicates an increase in attacks from other countries.

Figure 4 shows some of the countries responsible for these increases. Other than China's percentage, which remained relatively consistent during 2015 and 2016, all other countries in Figure 4 have seen major changes. For example, Vietnam has gone from a minuscule share that rounded down to 0% in 2015 to a 9% share in 2016, while India's share has increased almost as much as Vietnam's. Other countries, such as Japan, Germany, and the United Kingdom, have undergone large drops in their shares during 2016.

Webroot analysts also examined information from the blacklist on the types of threats each IP address poses. Many addresses pose multiple threats, such as acting as both a spam source and a vulnerability scanner. This information allows

organizations to be more granular in their blacklist use, such as setting policies that prohibit vulnerability scanner addresses from contacting any of the organization's addresses, while permitting all other malicious addresses not associated with denial of service threats to contact public-facing web servers.

Figure 5 shows the relative representation for the types of threats associated with the top 10,000 blacklisted IP addresses from the top 10 countries during 2016. Even though Webroot can identify many types of threats, the majority of them are spam sources and vulnerability scanners. This has been the case for years. Thirty-nine percent of the addresses pose more than one type of threat, so Figure 5 counts each of those addresses multiple times and lists the percentage of multi-threat addresses on the left side for each country. Over 98% of the addresses primarily act as spam sources. Historically, spam sources have been difficult for organizations to stop because they are so short-lived, lasting for hours or even just minutes. They can best be stopped by using continuously updated IP address blacklists.

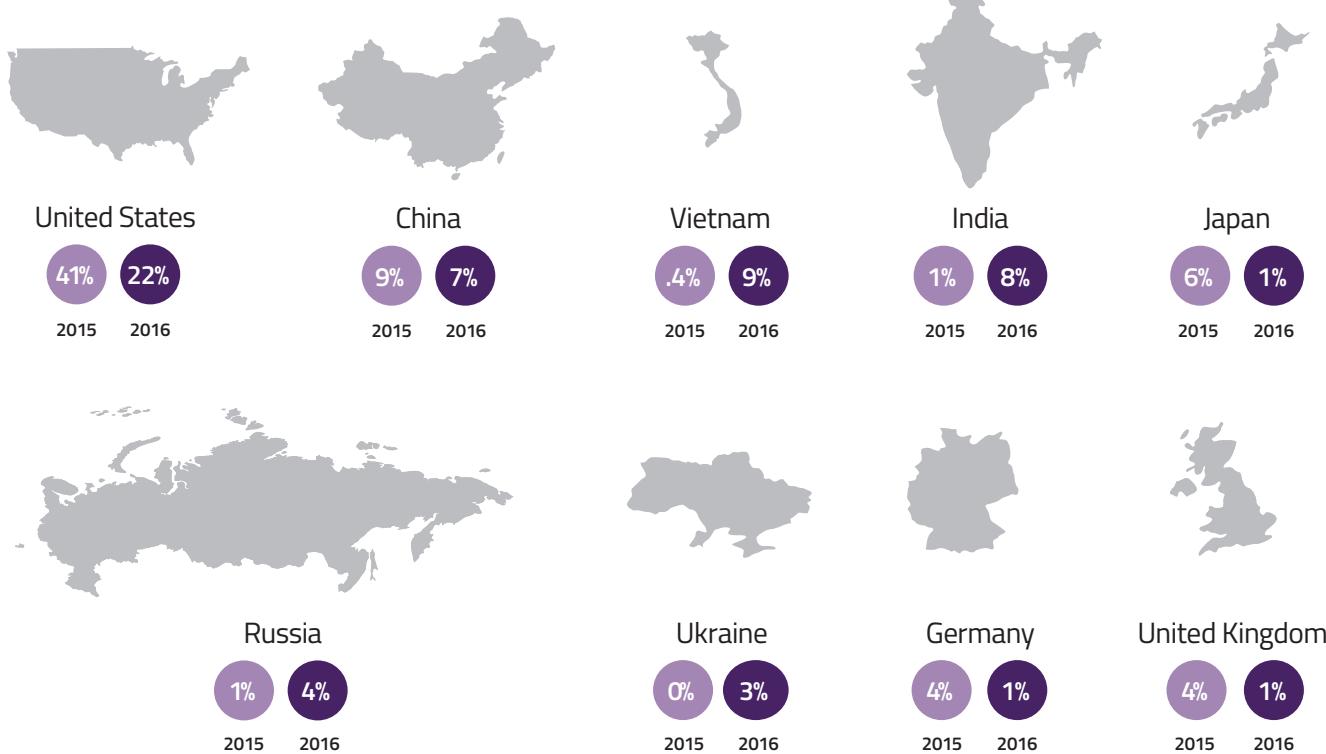


Figure 4: Top malicious IP origin countries for 2015 and 2016 total

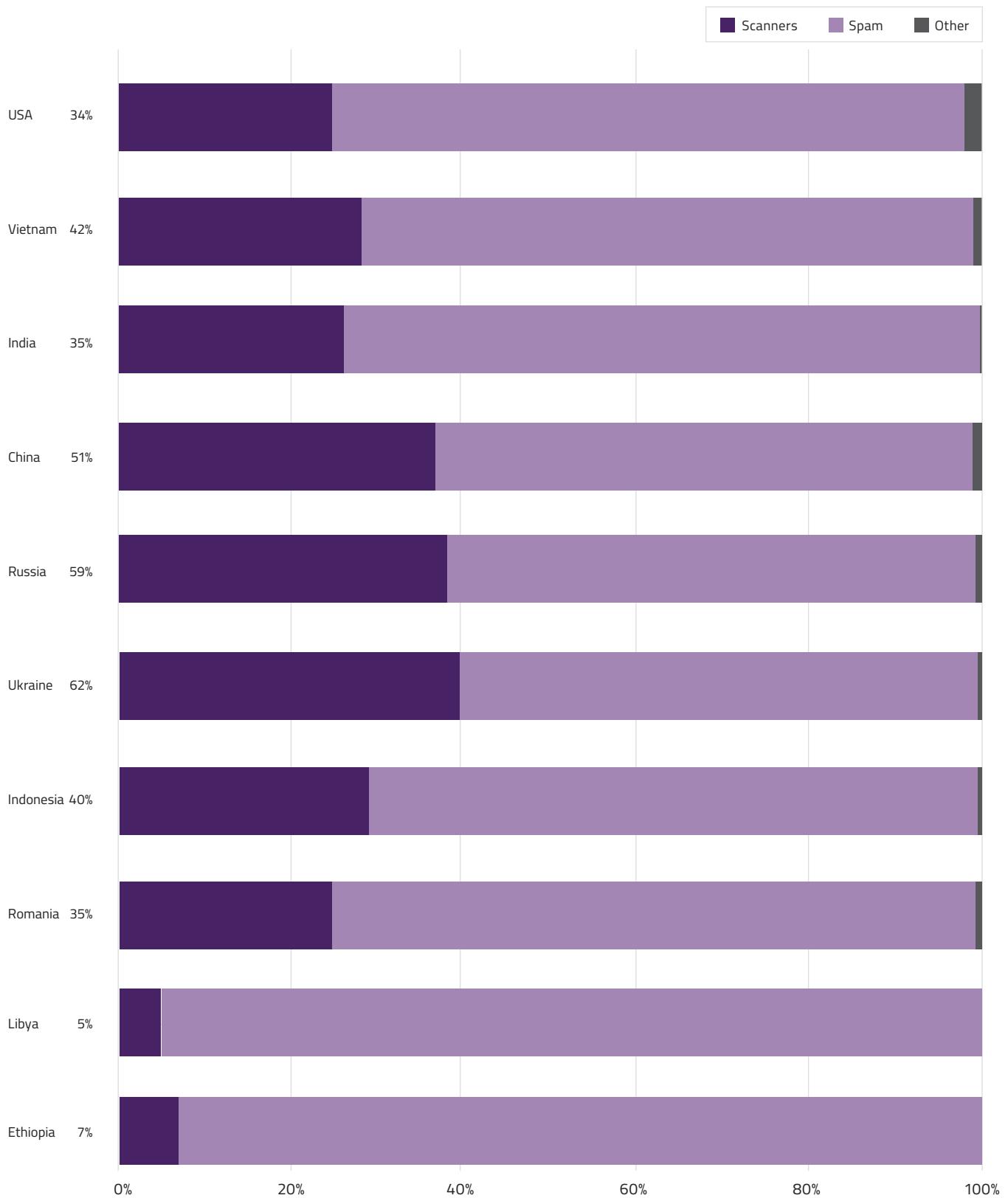


Figure 5: Threat types for top 10,000 blacklisted IP addresses from top 10 malicious IP origin countries

# Incredible percentage of High Risk URLs



Between benign websites that are compromised and malicious websites created specifically to attack the systems and users that access them, businesses must safeguard their organizations and users against website threats. The sheer volume of websites continues to rapidly increase, and the speed of exploitation means that the website or webpage that is benign one minute may be malicious the next. The only way organizations have to thwart these threats is to use the latest reputation data for URLs.

Webroot continually monitors URLs, and has analyzed over 27 billion URLs to date. This analysis includes labeling each URL with a risk category—High Risk, Suspicious, Moderate Risk, Low Risk, or Trustworthy—based on numerous factors, such as the website's history, age, rank, location, networks, links, real-time performance, and behavioral information. Each URL is also labeled as belonging to one of 82 primary content categories defined by Webroot. The risk and content categories enable organizations to create web usage policies that reflect which URLs may or may not be accessed. Webroot uses its URL threat intelligence in its products and also makes it available through its BrightCloud Web Classification and Reputation Services.

Figure 6 shows the distribution of risk categories assigned by the Webroot Threat Intelligence Platform to URLs during 2016. Note that the Moderate Risk category's percentages may be misleading because the category includes all URLs that could not be accurately categorized due to a lack of information. Many of these URLs point to new websites that may not yet have enough activity associated with them to determine their true nature. URLs falling in High Risk, Moderate Risk, and Suspicious categories pose a great deal of risk to organizations and represent nearly 70% of the URL distribution.

Figure 7 shows the ten countries that hosted the most High Risk URLs during 2016. Although the percentages change from year to year, the top ten countries stay fairly consistent, and the United States is always first. This is due in part to attackers in other parts of the world hosting their malicious websites and URLs in the United States to avoid automatic blocking by geofiltering services. Geofiltering alone only accounts for the location of the IP addresses being used, which is why it is important to consider both IP address and URL reputations when making security decisions.

Figure 8, on page 11, shows another way to look at the High Risk URL data. It demonstrates the relative distributions for the major categories of High Risk URLs—malware, phishing, spam, proxy avoidance and anonymizer, and botnet—for the countries from Figure 7. The most common type of High Risk URL is malware, followed by phishing and proxy URLs. Spam and botnet URLs are by far the least common types. Other items of interest from Figure 8 include the following:

- » Nearly 75% of Germany's High Risk URLs are associated with proxies. This is more than twice the relative share of any other country in the top 10.
- » Over 65% of Australia's High Risk URLs are for phishing. This is almost double the share of the second-highest country in the top 10.
- » All top 10 countries other than Germany and Australia have their most common High Risk URL type as malware, followed by either proxy or phishing.
- » The three countries in the top 10 with the highest relative percentages of malware URLs are China (86%), the Ukraine (84%), and Hong Kong (80%).

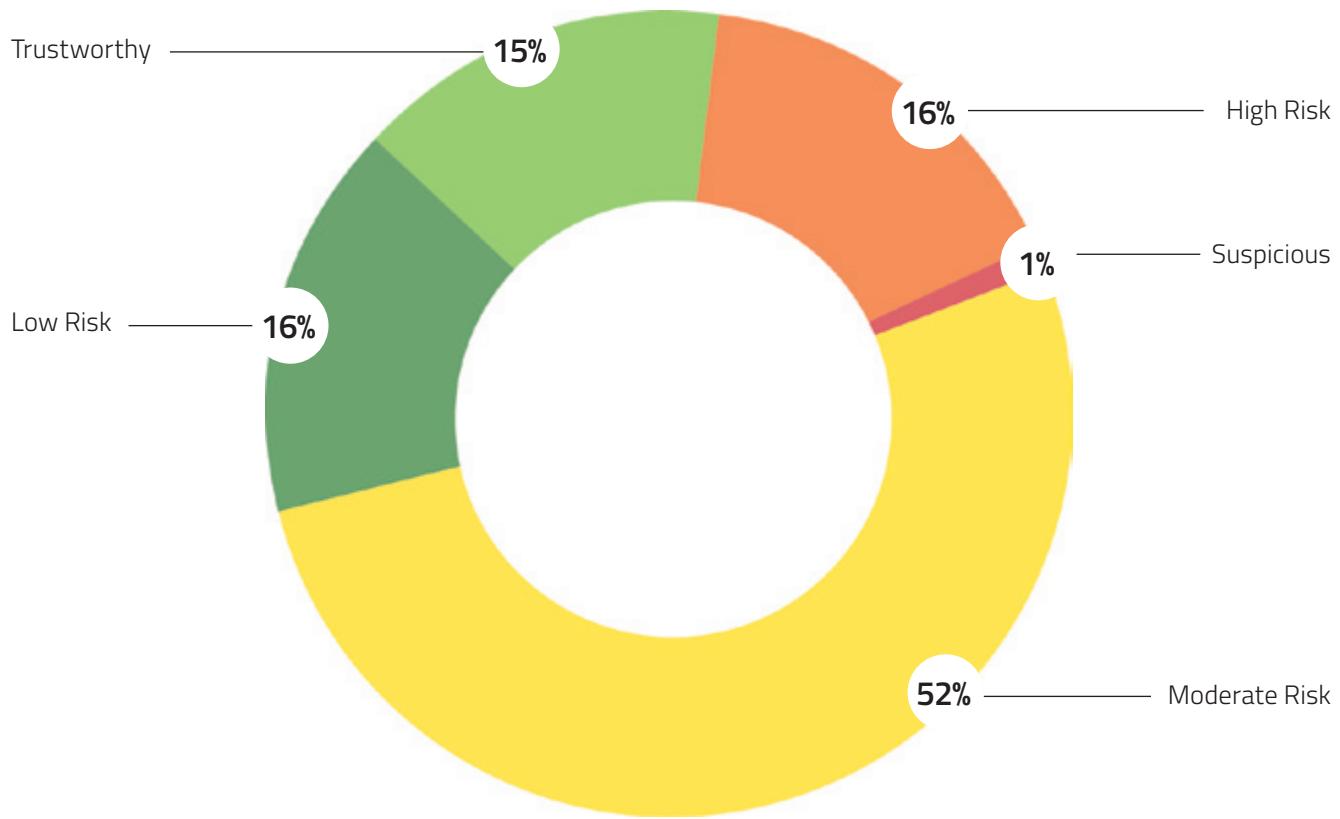


Figure 6: Distribution of URL risk categories during 2016

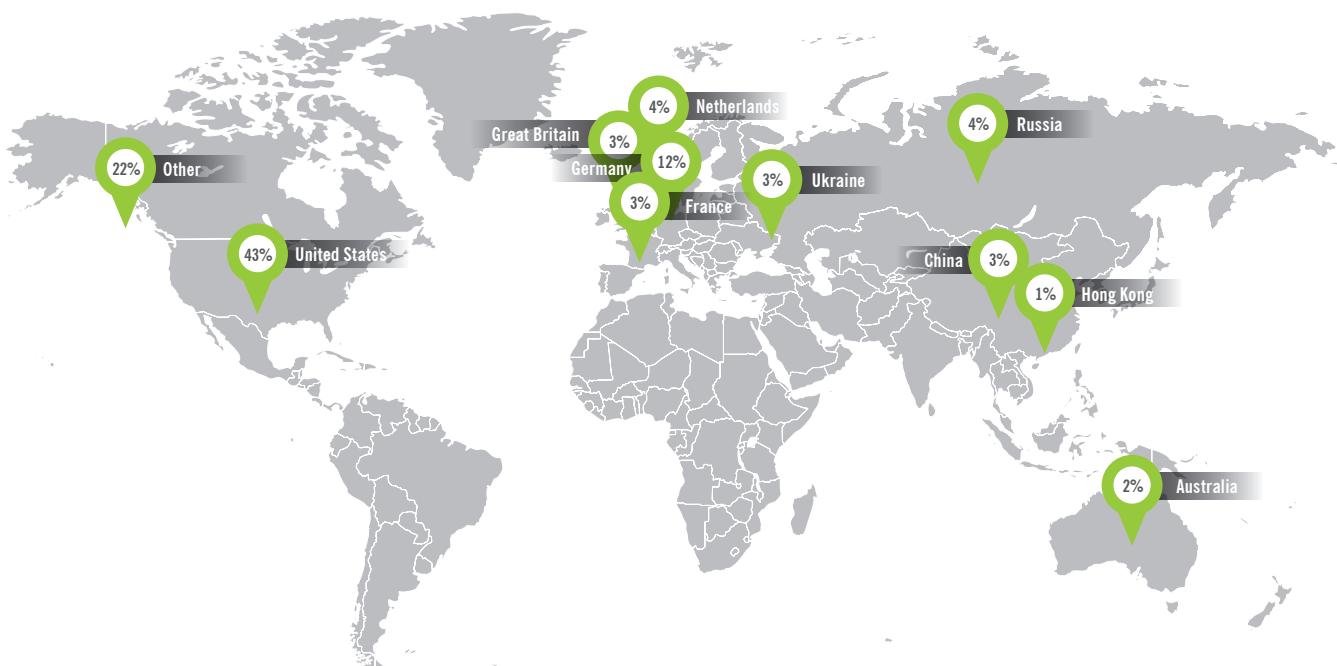


Figure 7: Top 10 countries that host High Risk URLs

It is also important to consider the other URL content categories besides those falling solely within the High Risk URL type. Webroot analyzed the data from these other content categories. The top three that were far more likely to be High Risk or Suspicious compared to average are:

1. Content Delivery Networks (11.6 times as likely)
2. News and Media (7.6 times as likely)
3. Web Advertisements (4.1 times as likely)

These content categories indicate that the use of malicious ads for attack delivery has significantly increased.

Likewise, some categories of URLs are far more likely to be Trustworthy than average. The top three are:

1. Personal Storage (5.4 times as likely)
2. Keyloggers and Monitoring (4.9 times as likely)
3. Gross (4.8 times as likely)

These statistics clearly show that while a URL category may generally be considered reputable, that does not mean its URLs are also reputable. Likewise, URL categories considered undesirable by many organizations do not necessarily pose additional danger. Organizations should set their policies based on reliable risk classifications for each URL.

A final area we analyzed for the URLs observed is how the most popular non-malicious URL categories have changed during the past two years. Figure 9 shows the top 10 categories in 2015 and 2016. The categories have not changed significantly, but the top 10 categories comprised 78% of all non-malicious URL categories in 2016 as compared to 71% in 2015. This indicates a tighter focus by attackers on a small group of URL categories.

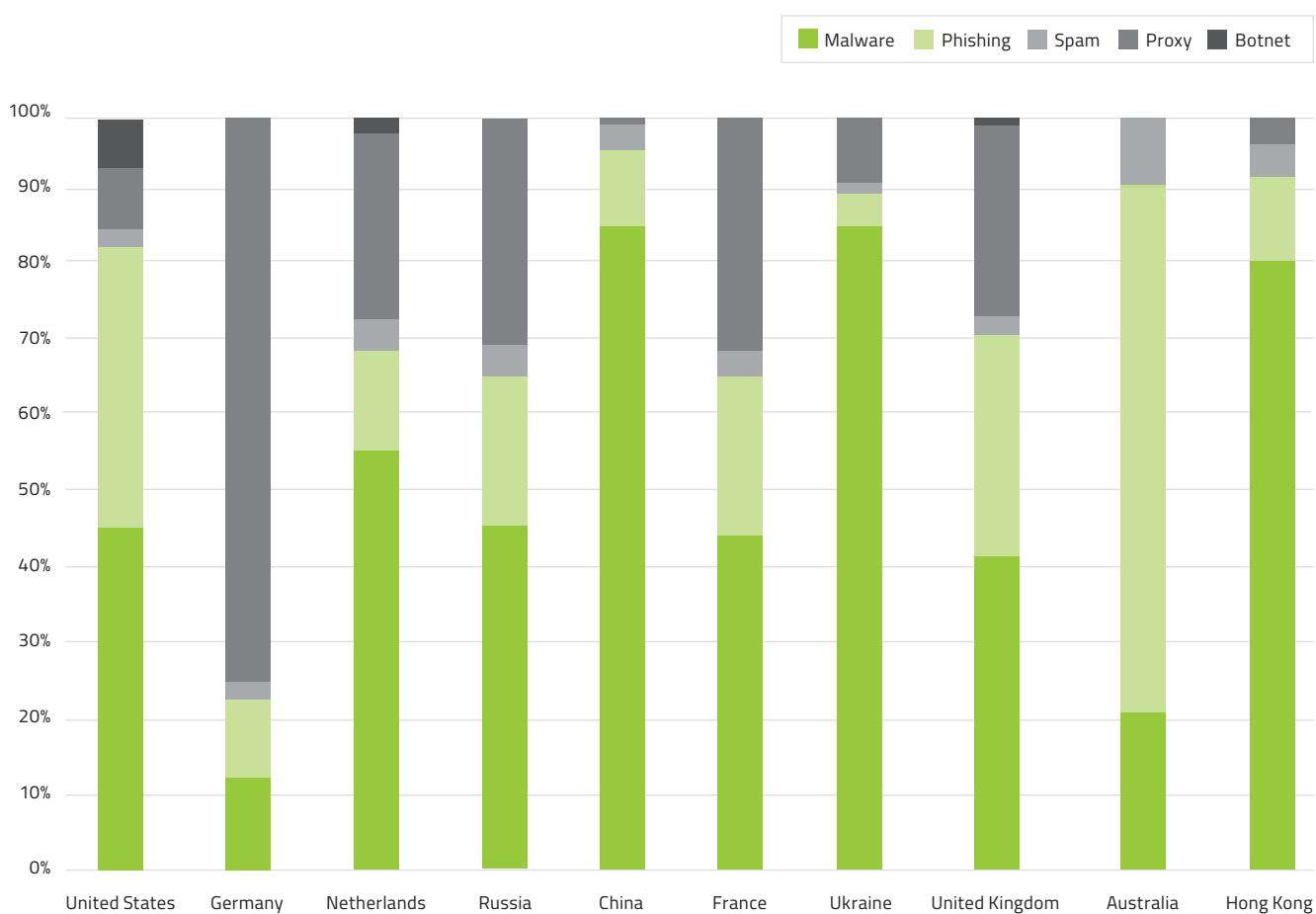


Figure 8: High Risk URL types for top 10 countries

## Top 10 Non-Malicious URL Categories in **2015**



## Top 10 Non-Malicious URL Categories in **2016**



Figure 9: Top 10 non-malicious URL categories in 2015 and 2016

# Escalating threats from phishing attacks



Webroot Threat Researchers keep a close eye on phishing attacks because of their prevalence and their increasing use as a starting point for more grievous attacks. The team has observed a dangerous trend in phishing over the past several years: the shortening of phishing attack life cycles, i.e. the length of time each phishing site is active. To quantify the current state of this trend, the team selected a representative sample of over 800 of the phishing sites detected during September and October 2016. Figure 10 shows the results of the analysis. The longest-lived site had a life cycle of less than two days (44 hours), while the shortest-lived site lasted only 15 minutes. Nearly 5% of the sites in the sample had a life cycle of less than an hour, 84% of all phishing sites last less

than 24 hours. On average, a phishing site was online for less than 15 hours. This trend is important because anti-phishing technologies based on static blacklists cannot keep up with such short life cycles, rendering them more or less ineffective at stopping attacks.

A second important trend confirmed by Webroot analysis is the use of existing benign domain names in phishing attacks. At one time, when the average phishing attack life cycle was measured in weeks or months, it was common for each phishing campaign to use a new domain name dedicated to that campaign. Today, few phishing attacks do this because domain names used only for phishing can be identified quickly

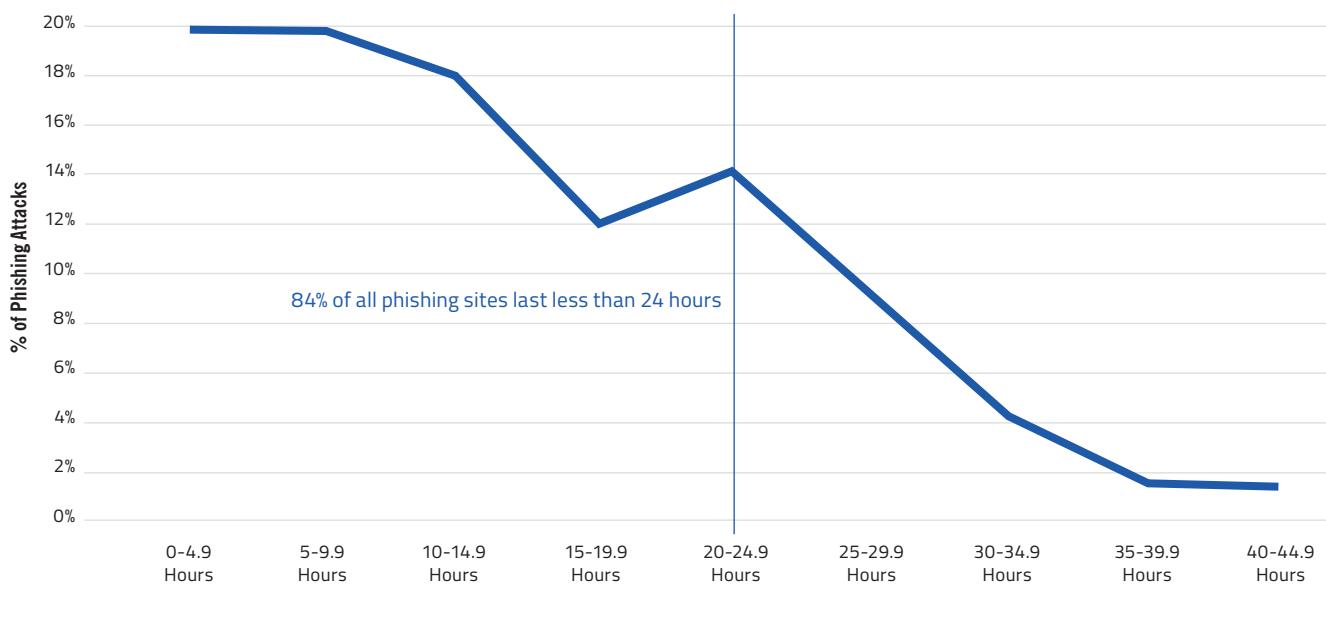


Figure 10: Phishing attack life cycle lengths

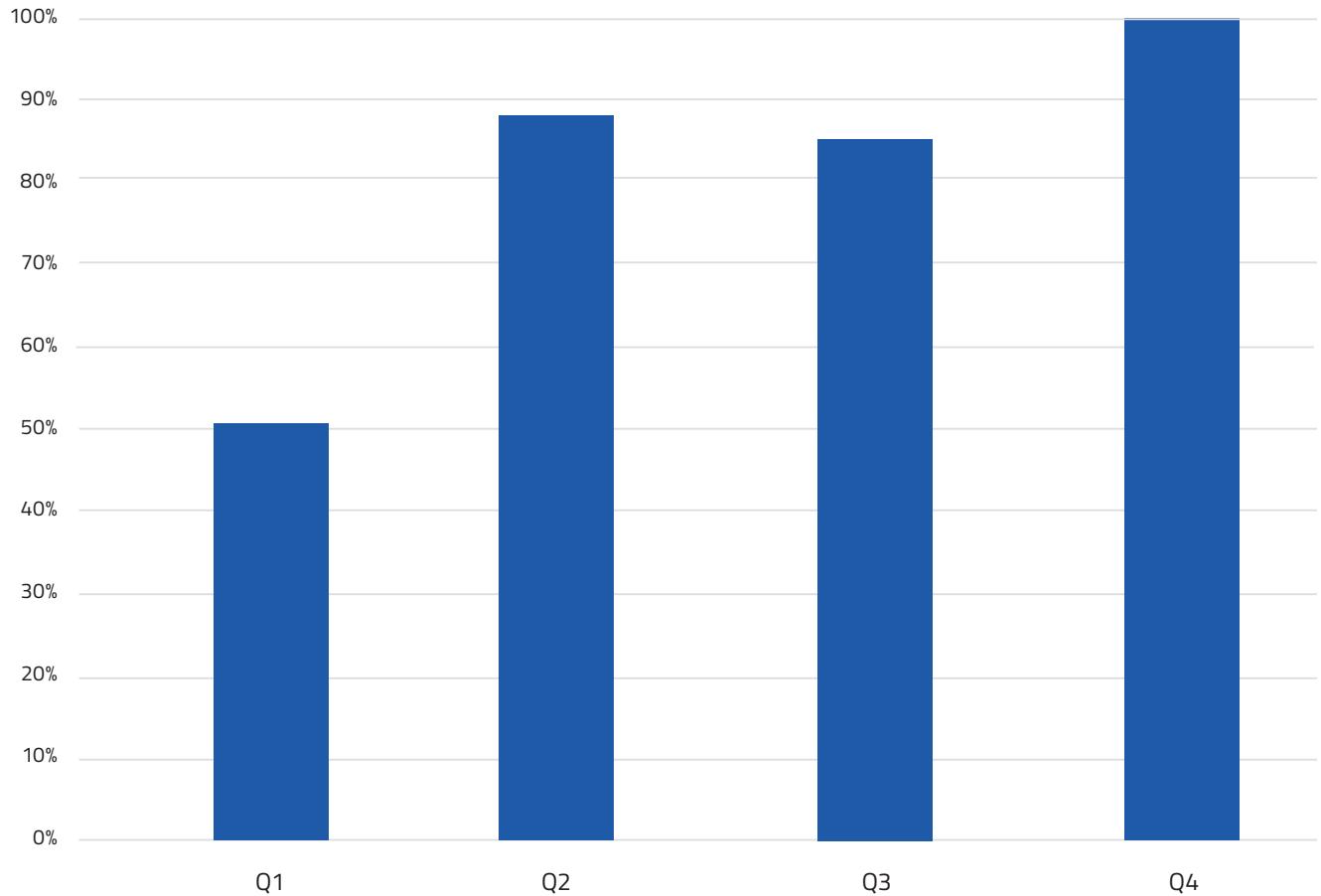


Figure 11: Unique zero-day phishing URL counts

and all traffic associated with that domain blocked. Instead, attackers use domains meant for benign usage; for example, an attacker may compromise a website and replace one page with phishing content. Recent Webroot analysis showed that almost 100% of phishing URLs were pointing to malicious pages or sites within benign domains.

With shrinking attack life cycles and increasing use of benign domain names, detecting and stopping phishing attacks has become more complicated, requiring new approaches. Webroot has developed the BrightCloud® Real-Time Anti-Phishing Service to automatically determine in milliseconds if a page or site being requested is part of a phishing attack. This time-of-need analysis is necessary to ensure that the site is benign right now, regardless of whether it was benign or malicious a minute ago. Real-time anti-phishing security controls are absolutely necessary for stopping phishing attacks.

Figure 11 depicts how many unique zero-day phishing URLs were detected by Webroot during each quarter of 2016. The 100% on the left axis indicates the URL total in the peak quarter, Q4. The average number of URLs increased over the course of the year. For example, 57% of the URLs were observed in the second half of the year. More striking is that almost twice as many URLs were detected in the fourth quarter compared to the first quarter. The most likely explanation for this is attackers taking advantage of the holiday shopping season.

Another way to examine the unique zero-day phishing URLs is to categorize each URL by the type of website being impersonated. Webroot analyzed observed URLs to identify those impersonating the 20 most targeted companies in 2016.

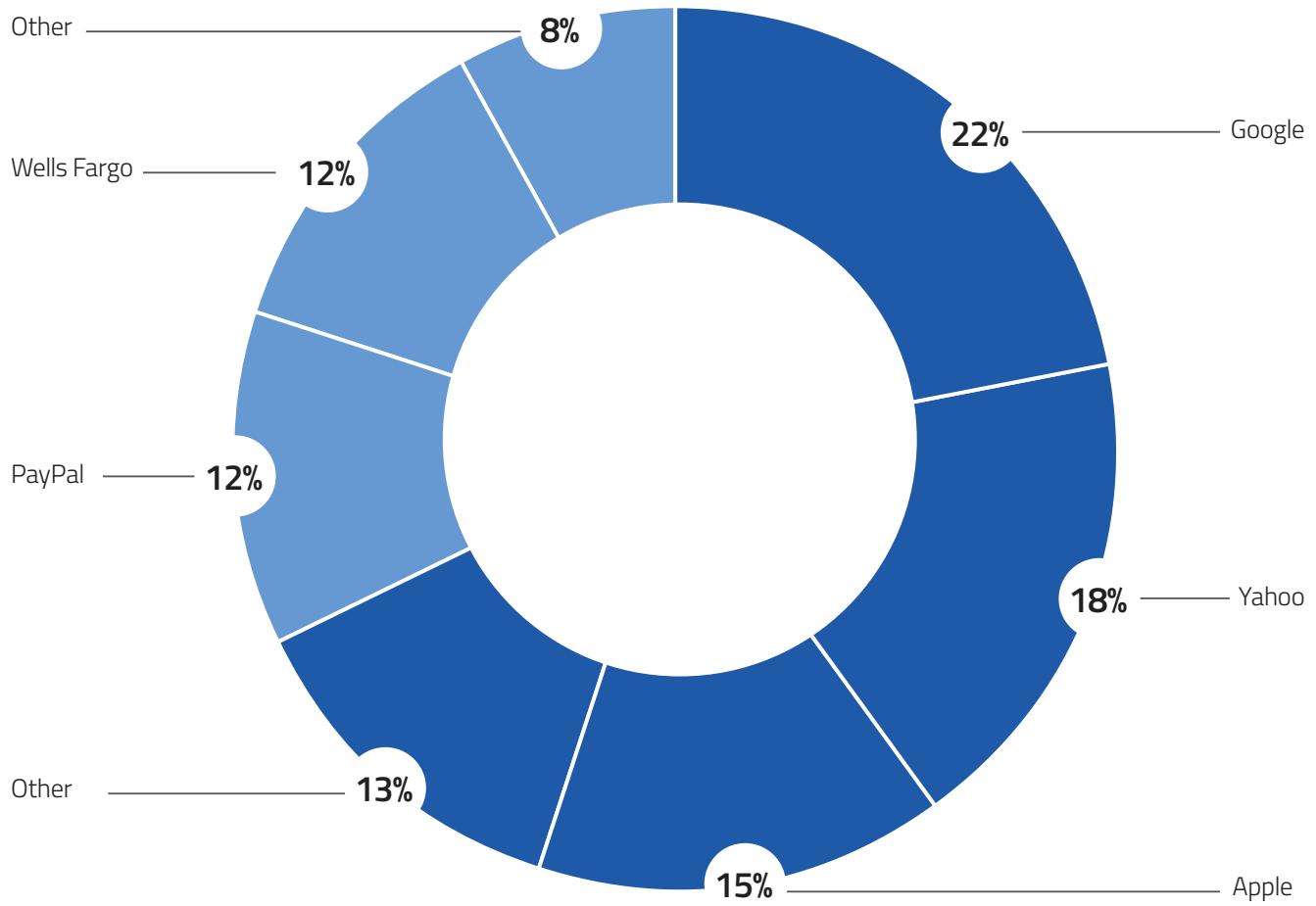


Figure 12: Share of phishing sites for the most impersonated companies

## *The average lifespan for a phishing site is less than 15 hours.*

Figure 12 shows the relative number of these URLs for each technology and financial company within the top 20. The graph indicates that there were over twice as many unique zero-day phishing URLs impersonating technology companies as financial institutions (67% to 33%). However, there were over three times as many financial institutions targeted by those URLs than technology companies (78% to 22%).

The Webroot Threat Research team determined that during 2016, for every new phishing URL impersonating a financial institution, on average there were over seven new phishing URLs impersonating technology companies. This ratio has changed greatly since 2015, when it was approximately 2.6. The change is probably due to a combination of factors, but the most important ones are how much easier it is to phish a technology account compared to a financial account, and how the compromise of a technology account often enables

compromising other accounts, including financial accounts, because of password reuse. Attackers who target technology accounts can get a much larger return on investment than those targeting financial accounts.

Figure 13 takes a closer look at the four companies covering technology and financial sites that are in the top five impersonated targets in both 2015 and 2016. The graph shows the share of the total unique zero-day phishing URLs impersonating each company each year. Google has consistently been at the top of the list for several years, but its relative share of phishing URLs dropped from 30% to 22% from 2015 to 2016, while Yahoo's relative share nearly doubled during the same period. Apple's share also rose from 9% to 15%. To summarize, phishers are targeting Google, Yahoo, Apple, and PayPal more evenly than they had in previous years, but Google is still their top target.



Figure 13: Comparison of most impersonated companies between 2015 and 2016

# Alarming numbers of malicious apps



As more people adopt mobile services, it's not especially surprising that smartphones and tablets are increasingly targeted by attackers. Because many attacks are in the form of malicious mobile apps, Webroot consistently monitors app stores and other app repositories to identify new and recently updated Android® and iOS® apps and analyzes them for malicious behavior. The results of this analysis are incorporated into Webroot products to protect mobile customers, and they are also available through the BrightCloud Mobile App Reputation Service and Mobile Security SDK to Webroot partners providing mobile management and security solutions.

Webroot's analysis classifies each mobile app as having one of the following reputations: Trustworthy, Benign, Moderate, Suspicious, Unwanted, or Malicious. In 2016, Webroot analyzed approximately 20 million new and updated Android and iOS apps, bringing the total number of classified Android and iOS apps to over 50 million. Figure 14 shows the distribution of Android app reputations over the past three years by half year. (Note: because so few apps were classified as Trustworthy, they are not shown in the graph.)

The changes during 2016 are striking. For example, Malicious apps fell from 45% of all new and updated apps in the first half of the year to only 17% in the second half. The percentages of Benign and Moderate apps roughly doubled, and the percentage of Suspicious apps more than tripled. The largest change was seen in Unwanted apps, which fell from 22% to 5% in 2016. Looking at the three-year period, the classifications from the second half of 2016 seem to be more similar to the distributions seen in 2014 and the first half of 2015 than the data from late 2015 and early 2016.

Figure 15 provides additional information on what has happened. The four leftmost columns show the average monthly distributions for 2014 and 2015 by half year. The twelve rightmost columns show the monthly distributions from 2016. Analysis of the data in Figure 15 along with Webroot Threat Research team insights indicates the following:

1. In 2016, over four times as many new and updated mobile apps were observed and analyzed as in 2015. Starting in February 2016, every month's app volume was more than double the 2015 averages.
2. February through July 2016 were relatively stable in terms of volume except for March, which was much higher. A detailed examination of the March data showed an unusually large volume of SMS malware and PUAs. Several large phishing and malware campaigns based on SMS were occurring at that time, which would explain the spike in the data.
3. Nearly 50% of the new and updated mobile apps analyzed in 2016 were classified as Malicious or Suspicious. That means nearly 10 million Malicious and Suspicious mobile apps were made available during the year. In contrast, just over 2 million such apps were made available during 2015.

It is also important to note that the distributions in Figures 14 and 15 are not fully representative of mobile app reputations in the real world. For example, some of Webroot's sources of mobile apps are dominated by bad apps. Another example is that app stores in some parts of the world may make greater efforts to identify malicious apps before making them available to download, or respond more quickly when an app is reported as malicious. Webroot focuses its analysis on app stores in regions with Webroot customers, so the mobile app reputation distributions in other parts of the world may be significantly different.

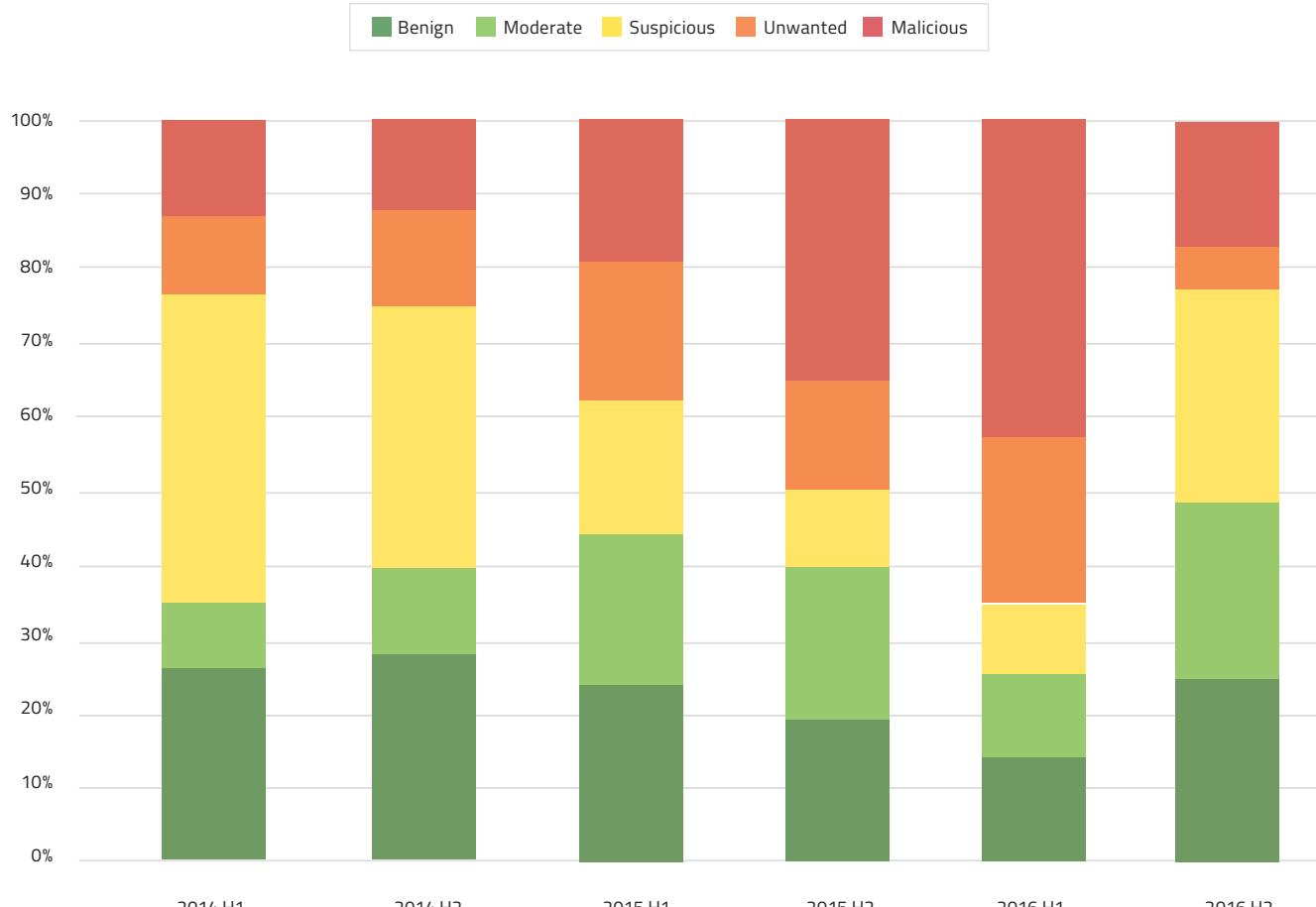


Figure 14: Distribution of mobile app reputations

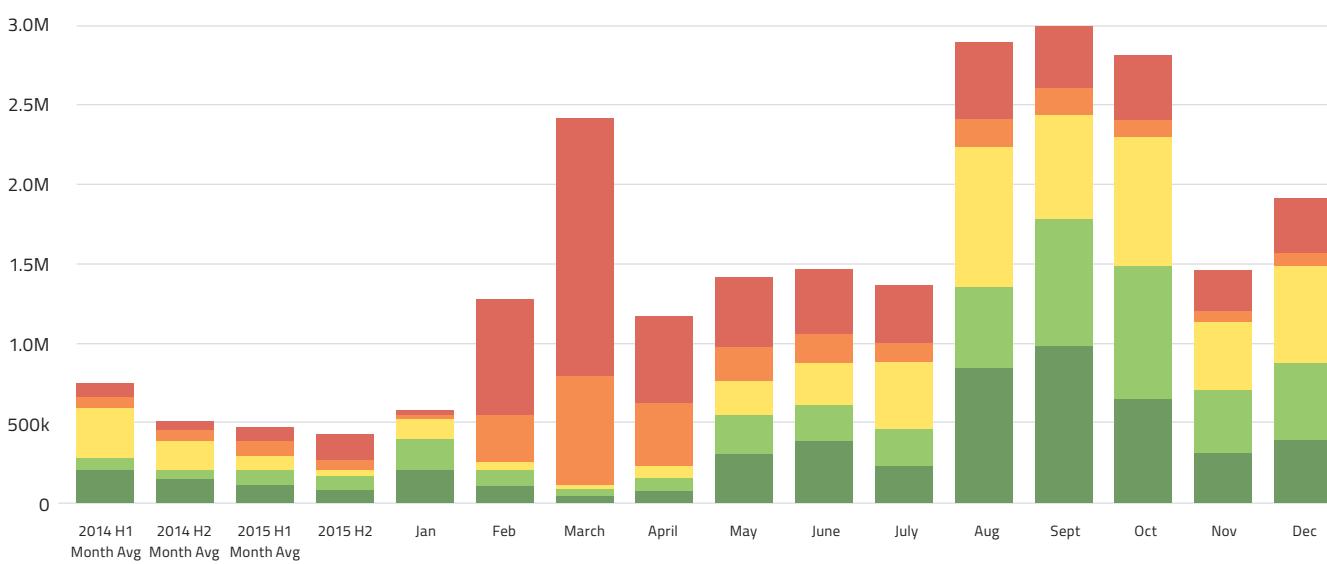


Figure 15: 2016 monthly distribution of Android app reputations and semi-annual 2014 and 2015 averages

For the mobile apps identified as Malicious in Figure 14 and Figure 15, Webroot categorizes each based on its primary malicious activity: adware, PUA, rootkit, spyware, system monitor, Trojan, or worm. Figure 16 shows the relative categorizations for the past three years, grouping rootkits, system monitors, and worms as Other because they are infrequent compared to the other categories. Throughout this time, Trojans comprised the majority of malicious mobile app threats, with a steady share of roughly 60% during 2015 and 2016. The next most common category has been PUAs, which have also kept a steady share—approximately 28%—over the past two years. The biggest change during 2016 has been an increase in adware, going from a negligible share in 2014 and 2015 to a nearly 10% share in the second half of 2016. This change is likely due to the Android operating system's growing popularity, which makes it a more attractive target for adware.

Another way of analyzing malicious Android apps is to look at their alleged purpose. The Google Play store defines dozens of categories based on app purpose. During 2016, Webroot found malicious apps and PUAs across more than 50 categories.

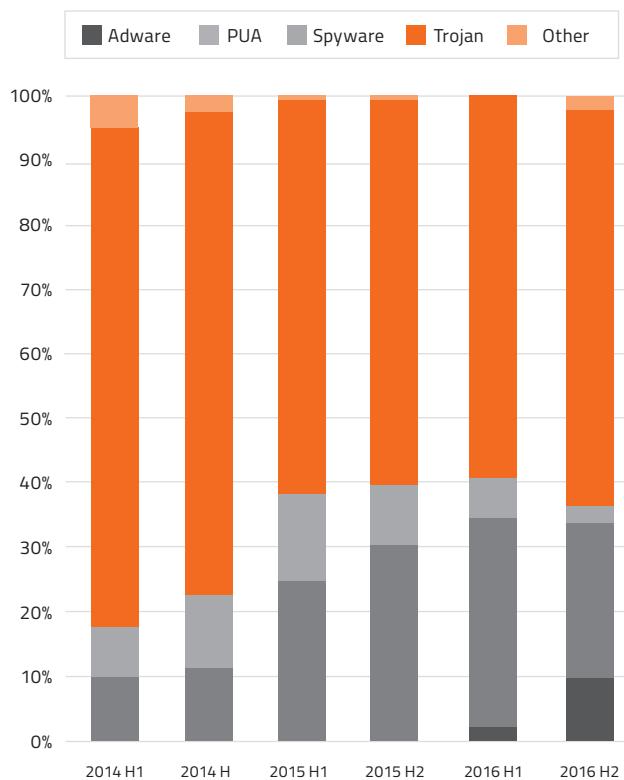


Figure 16: Frequency of Android application threat types

Figure 17 shows the distribution of malware and PUAs in these categories, highlighting the 10 used most often for malicious Android apps, while the rest are grouped under "Other". Observations of note for this graph include the following:

- » Almost all the top 10 categories have more malware apps than PUAs. Categories such as Entertainment and Personalization tend to have a higher percentage of PUAs because they naturally lend themselves to being PUAs. For example, most Personalization PUAs simply provide a few ringtones or wallpapers along with their malicious content.
- » The top five categories alone—Tools, Arcade & Action, Entertainment, Productivity, and Personalization—represent almost 50% of all malicious apps.
- » There have been no significant changes in the top 10 categories and their relative percentages from 2015. This is important because from 2014 to 2015, there were major shifts in the categories attackers focused on, indicating changes in tactics. The stability from 2015 to 2016 implies that attackers are no longer attempting to exploit previously neglected categories.

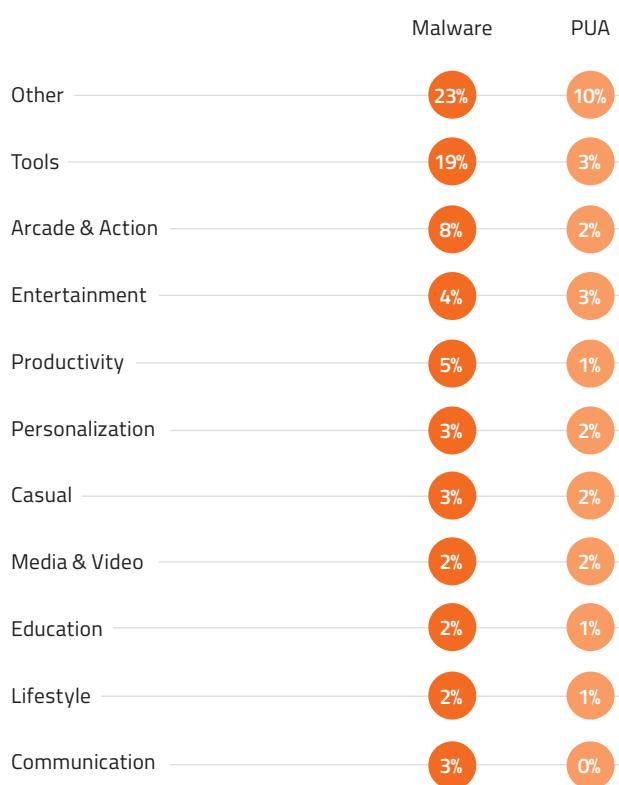


Figure 17: Top 10 Android malware and PUA categories

# Conclusion

Throughout 2016, Webroot continuously produced threat intelligence based on its broad and deep understanding of current and emerging threats. The Webroot Threat Research team analyzed this entire body of threat intelligence at the end of 2016 to identify the most important trends that organizations need to be aware of during 2017.

The notable positive trends involved executable files. Of the hundreds of millions of new executable files observed during the year, only 2.5% were malware and 2.2% were PUAs—both significant reductions from previous years. Also, the monthly counts for new PUA executable files dropped over 80% from January to December.

The notable exception in the positive executable file trends is ransomware; incidents involving ransomware caused largely unreported losses estimated in the billions during 2016. Ransomware is expected to be an even larger problem in 2017, given the continued success of Locky ransomware and the availability of numerous exploit kits and ransomware-as-a-service offerings. To mitigate ransomware and other executable file-based threats, organizations should continue to use innovative technologies for detecting and stopping both known and previously unseen malicious executable files in real time.

Unfortunately, there were numerous negative trends in 2016:

- » Approximately one-third of URLs with sufficient information available to determine a risk category were identified as high risk.
- » Phishing attack life cycles continue to drop; some phishing attacks now last just minutes, while the average phishing attack life cycle is under 15 hours.
- » Phishing attacks rarely use dedicated domain names anymore; instead, they rely on attackers acquiring and using webpages in established benign domains.
- » The number of unique zero-day phishing URLs Webroot observed each month grew throughout 2016, with almost twice as many URLs detected in the fourth quarter as in the first quarter.
- » The number of new and updated Android apps Webroot classified as malicious or suspicious each year dramatically increased from ca. 2 million in 2015 to nearly 10 million in 2016.

Considered together, these trends indicate a major increase in attacks based on malicious Android apps and malicious URLs. It is critical that all organizations implement strong strategies for detecting and stopping these threats. With the incredibly dynamic nature of today's websites, benign one minute and compromised the next, as well as the sheer volume of URLs and Android apps, organizations must adopt technologies that use threat intelligence that is constantly updated with the latest information on malicious and suspicious activity. This type of threat intelligence is the only solution for automated, real-time, highly accurate decision making to protect organizations from the rapidly increasing number of attacks they face each day.



## About Webroot

Webroot delivers next-generation network and 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, BrightCloud® Threat Intelligence Services, and FlowScape® network behavioral analytics protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Citrix, 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](http://www.webroot.com).

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 [webroot.com](http://webroot.com)

© 2017 Webroot Inc. All rights reserved. Webroot, BrightCloud, SecureAnywhere, FlowScape, and Smarter Cybersecurity are trademarks or registered trademarks of Webroot Inc. in the United States and/or other countries. All other trademarks are the properties of their respective owners. REP \_ 030217 \_ US