WEBROOT®
an opentext™ company

WEBROOT

THREAT REPORT

TABLE OF CONTENTS

FOREWORD

Hal Lonas, SVP and CTO, SMB and Consumer, OpenText

As we embark on a new decade, it's striking to think how many major changes have taken place in the very recent past. Consider this: we've been living in the smartphone era for over ten years. If we think back even further, the "cloud" grew from a mere concept in the 1960s to a buzzword in the early 2000s—then into the ubiquitous state of strategic computing today, in which public, private and hybrid clouds are everywhere. User expectations, in particular, challenge the way businesses operate around the world. For those of us who remember the days of dial-up: try to recall how long it took to connect, let alone download an image! Today, each of us expects to receive personalized, relevant, and immediate experiences, quickly and without lag, via cloud, mobile, social, and artificial intelligence—while simultaneously expecting our personal data will remain secured and private.

One thing that hasn't changed is the relentlessness with which hackers work to steal data, compromise systems, and generate profit. Many of the tactics remain the same; phishing has been around for ages and it's still a primary tool for dropping malware and gaining unauthorized access to sensitive information. Meanwhile, other tactics have evolved significantly; if we think back to ten years ago, we hadn't yet heard of ransomware, the effect of cloud computing on security was a big question mark, and only 28% of attacks used social engineering tactics.[1] The last couple of years, in particular, have made a remarkable impact on the threat landscape. For instance, malicious IP addresses, URLs that take unsuspecting users to dangerous sites, cryptojacking that mines for cryptocurrency without the user's knowledge or consent, ransomware in its variations, and increasingly vicious and stealthy malware—all of these are newer dangers to businesses and individuals alike.

In this year's Webroot® Threat Report, we take a deeper look into what we've seen in these and other categories, and include further context on targeted industries and common malware locations. With an in-depth view of massive amounts of both good and bad web traffic, we use our informed understanding of what has happened during the past decade to foreshadow what 2020 may bring, and help you make sense of these trends in a rapidly changing world.

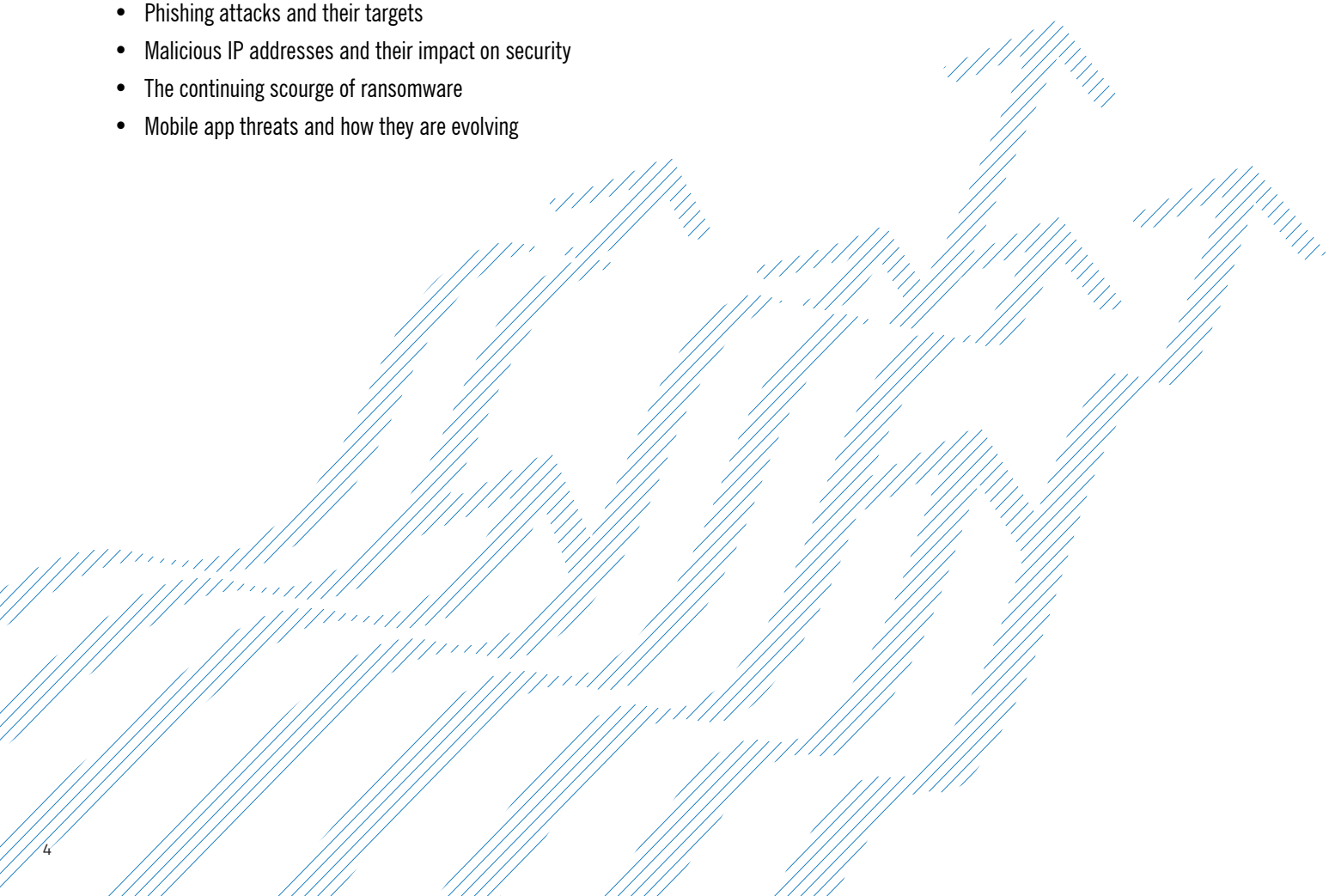
> Today, each of us expects to receive personalized, relevant, and immediate experiences, quickly and without lag, via cloud, mobile, social, and artificial intelligence—while simultaneously expecting our personal data will remain secured and private.

THE WEBROOT PERSPECTIVE

The statistics, trends and insights in this 2020 Webroot Threat Report are based on massive amounts of data continuously and automatically captured by our advanced machine learning-based architecture, the Webroot® Platform. This data—which comes from millions of real-world endpoints and sensors, specialized third-party databases, and end users protected by our technology partners—is then analyzed and interpreted on a continuous basis by our advanced machine learning engines and Threat Research team. The retrospectives, trends, and predictions in this report cover a broad range of threat activity, including:

- Trends in malware, who it affects, where it hides, and geographical and industry analysis
- URL classifications and security trends, including cryptojacking
- Phishing attacks and their targets
- Malicious IP addresses and their impact on security
- The continuing scourge of ransomware
- Mobile app threats and how they are evolving

Each of the aforementioned threats has wide reaching impacts across multiple industries, geographical regions, and user groups. We'll break it all down by the numbers, and also demonstrate how effectively employing end user awareness and training can mitigate risk of compromise. Finally, in the Predictions section, we'll look at how our comprehensive, global view informs what we expect to see in the coming year.



WEBROOT BRIGHTCLOUD® THREAT INTELLIGENCE

95+ Million real-world sensors

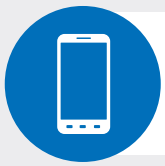
78+ Million end users protected through technology partners

842+ Million domains

37+ Billion URLs

4+ Billion IP addresses

36+ Billion file behavior records



31+ Million active mobile apps

MALWARE

Over the past ten years, we've seen that malware authors and attackers are highly adaptable and extremely focused. We only need to look at the rapid increase in malicious files found on only a single machine to see how authors have learned how to evade traditional cyber defenses via polymorphism.

*In 2019, **93.6% of malware** detected was only seen **on a single PC.** This is the highest yearly rate we've ever seen, although the number has been above 90% since 2014.*

Malware has become a favorite tool of nation-states, which employ (and, occasionally, lose control over) highly advanced, zero-day exploits to wreak havoc on businesses, governments, and organizations in general—witness the EternalBlue exploit.[2] Add to that the impact of the cloud, the ubiquity of mobile phones, and it's easy to see how much malware has evolved in the last decade.

One thing's for sure: Windows® malware hasn't gone away. Webroot-protected Windows endpoints see more than 1.6 million new malware and Windows applications each day. This number continues to grow, up from around 1.369 million per day the previous year. That tallies up to 500 million in 2018, and close to 600 million in 2019. In other words, we see a massive, growing, perpetual flow of file data.

CONSUMER VS. BUSINESS DEVICES

Of the endpoints reporting an infection, 62% were consumer (home user) devices, while 38% were business systems. This discrepancy is likely due to businesses having more layers of security in place, and also the increase in businesses providing security awareness training for their employees. Overall, the number of malware files per device is going down year over year for consumer PCs, but it remains roughly the same as last year for business PCs.

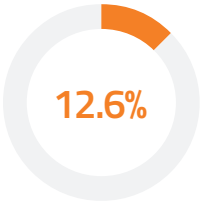
Consumer devices continue to become infected much more often than their business counterparts. For this reason, it's important to underscore the risk companies run when they allow their workers to connect personal devices to the corporate network. With a higher prevalence of malware and generally fewer security defenses in place, it's easier for malware to slip into the corporate network via an employee's personal device.

Consumer devices remain approx. 2x more likely to become infected than business systems.

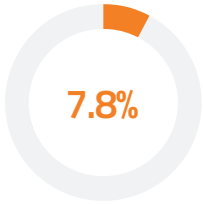
One thing that is especially interesting to note is the frequency with which PCs were re-infected.

In 2019, 12.6% of consumer PCs encountered an infection. Of these:

- 46.3% encountered only one infection
- 35.8% encountered 2-5
- 8.6% encountered 6-10
- 9.2% had more than 10 infections



Consumer PCs infected



Business PCs infected

In contrast, only 7.8% of business PCs encountered an infection. Of these:

- 50.4% saw just one infection
- 33.2% saw 2-5
- 7.9% saw 6-10
- 8.5% saw more than 10

There are several possible reasons for systems to encounter multiple infections; it could be the result of multiple polymorphic files attacking a single PC, or a single piece of malware dropping multiple files. It could also be due to occasions in which, when Webroot protection is first installed on a machine, it finds multiple current infections. Regardless, the message here is that administrators and individuals alike must remain vigilant.

WHY THE OS MATTERS

As we've seen in the past two years, the move to Windows® 10 (a generally safer OS) helps explain some of malware declines in the data. Overall, systems running Windows® 7 are nearly three times as likely to get infected as Win10 devices; each operating system sees an average of 0.11 and 0.04 infections per endpoint, respectively.

Malware targeting Windows 7 increased by 125%.

In general, we can say that Win10 sees fewer infections, with 0.06 per device for consumer PC and 0.02 per device for business PCs. The magnitude of the Win7 problem depends on how many consumer and business PCs are running that OS. In 2019, we saw that 82% of consumer PCs were running Win10, versus just 10% Win7, whereas business PCs stood at 63% for Win10 and more than 25% on Win7. We expect this percentage to decrease as Microsoft no longer supports Win7.

When looking at infection rates per endpoint, the differences between the consumer and the business world are clear. Infections per consumer system are steadily declining overall (from 0.11 in 2017, to 0.10 in 2018, and down to 0.08 in 2019) but the aggregate figures mask an important fact: Win7 rates grew from 0.17 to 0.20 infections per device. Although we expect the number of Win7 endpoints to decrease, the amount of malware specifically targeting Win7 is likely to increase for the same reason; if Microsoft no longer supports Win7, they will no longer patch vulnerabilities within the OS.

The slight drop in the annual total of malware files is likely due to several factors.

- **Security Awareness Training**
  Because users are the first line of defense, security awareness training is increasingly important. Gartner says end-user-focused security education and training is a rapidly growing market and estimates that "by 2022, 60% of large/enterprise organizations will have comprehensive security awareness training programs."[3]

- **Technological Effectiveness**
  The data we present is gathered from Webroot-protected endpoints. Our layered, multi-vector approach detects and blocks activity earlier in the kill chain. For example, by blocking executables from hitting endpoints via malicious URLs or preventing .exes from downloading additional malware files, we can reduce the incidence of malware executing on protected endpoints.

- **Changes in Cybercriminal Activity**
  Some cybercriminals have refocused on attack methods that generate profit from remote systems more easily than malware does, such as phishing or cryptojacking. In addition, criminals have moved to a more targeted malware business model, in which they launch fewer attacks and deploy less malware, but do so with a higher success rate.

- **Better Operating System Security**
  The mass adoption of Windows 10 (with antivirus always on) and efforts by the security community and the security industry at large have also been a factor.

INFECTIONS BY REGION AND INDUSTRY

If we track the rates of infection on Windows devices by geographical region, the view presents striking differences. At first glance, it's easier to see the rate of infected consumer devices versus business PCs.

Additionally, infection rates vary widely by geographical area. Nearly a quarter (23%) of devices in the Middle East encountered an infection in 2019; Asia was close behind, followed by Africa, and South America. In contrast, Europe, North America, and Japan saw much lower rates.

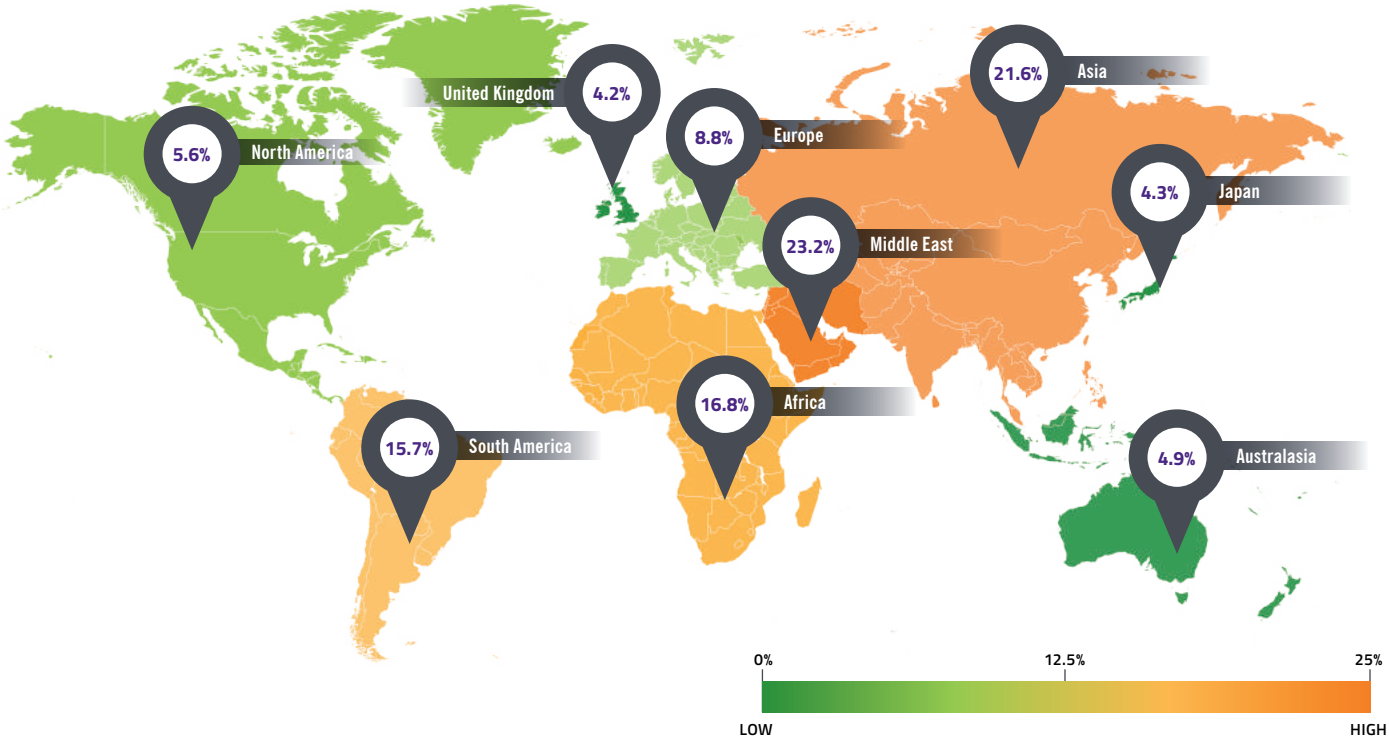


Figure 1a: Infected devices by region

	Consumer devices with infections	Business devices with infections
Africa	20.3%	15.7%
Asia	27.9%	16.6%
Australasia	11.6%	4.6%
Europe	21.5%	7.3%
Japan	4.6%	4.1%
Middle East	26.9%	16.6%
North America	6.9%	3.9%
South America	17.9%	10.5%
United Kingdom	9.6%	3.7%

0% 14% 28%

Figure 1b: Infected consumer and business devices by region

	Devices running Win7	Devices running Win10
Africa	31.5%	53.9%
Asia	33.4%	54.6%
Australasia	24.8%	62.0%
Europe	26.9%	59.2%
Japan	39.6%	51.3%
Middle East	35.3%	50.1%
North America	19.6%	69.8%
South America	22.5%	63.1%
United Kingdom	26.0%	62.2%

0% 35% 70%

Figure 1c: Infected Win7 and Win10 devices by region

To better understand the infection rates, we need to look at regional data by OS. In general, Win7 represents 21% of the base, while Win10 represents 68%. But if we look at regions with very high infection rates, we can correlate that to the prevalence of Win7. For example, in South America, more than 22% of the PCs are running Win7; in Africa the figure is 31.5%; in Asia it's 33.4%; and in the Middle East, it is 35.2%. All of these regions show high rates of infection per device, and regions with large volumes of Win7 PCs are subject to an increasing number of threats. Again, the threat rate is growing for Win7 while it remains flat or decreases for Win10. In contrast, in North America, almost 70% of PCs are running Win10, and the infection rates are low.

A variety of factors may contribute to these rates of infection. For instance, regions that have greater economic resources, better access to up-to-date technology, and stronger awareness of cybersecurity concerns and risks (such as the US and Europe) tend to show fewer infections per device, especially for business PCs. Regions with fewer up-to-date devices, i.e. large numbers of Win7 PCs, show a greater number of threats.

Another way to look at infection rates is to compare the rates of various industries with the overall average. Of the Webroot customers who have reported their industry verticals to us, all have seen a lower percentage of malware per device in 2019 than 2018. However, the targets who experience more malware than others are shifting. For instance, Manufacturing, Public Administration, Resource Mining/Extraction, and Transport and Warehousing report higher-than-average encounters with malware per device. Meanwhile, more traditional targets for attack, such as Finance and Insurance, Healthcare and Social Assistance, Nonprofits, and Education Services, are experiencing lower-than-average malware rates. (Since these latter industries have been in cybercriminals' crosshairs for the last several years, and many of them have, consequently, made massive investments to improve security, it's unsurprising that their percentages would improve.)

WHERE MALWARE HIDES

Malware is everywhere, but the system locations in which it hides differ between consumer and business PCs. Take %appdata% as an example. For consumer PCs, 26.5% of all infections are found in this folder.

In contrast, 16.7% of the threats detected in %appdata% for business PCs are malware. One of the reasons appdata is often popular for consumer systems is because the user does not need the services of a local admin to install a program with Win8 and above. The majority of consumer devices have a single user, who is the device admin. This is different in business environments, where the user often has restrictions for where new applications can be installed.

85% of threats hide in 1 of 4 locations: %temp%, %appdata%, %cache% and %windir%.

Other examples include %temp% which accounts for 54.4% of bad files for business PCs, and 28.7% for consumer PCs. Temp is twice as likely to be a hiding spot for business PC infections as for consumer PCs. (There is good news: it's easy to set up a Windows policy to prevent programs from running from the %temp% directory, regardless of whether they are malicious or benign. This is good cyber hygiene and, coupled with user security awareness training, can go a long way to ensure protection.)

We continue to see the positive impact of a cleaner operating system, Win10 especially. It's important to keep in mind that, when consumers buy a new PC, they will generally get Win10 as the default operating system, especially since Microsoft intends to move everyone off Win7. However, for businesses, it's harder to do a massive upgrade; there may be legacy apps that require Win7, and there are costs associated with upgrading.

RANSOMWARE

Ransomware didn't show up in force until 2015. Before that, we saw a fair amount of fake antivirus software in which a popup alarmingly informed the user that their system had been compromised, and they needed to click a link to "clean" their system. This action typically incurred some sort of cost and further compromised the system. By the mid-2010s, hackers began using cryptocurrency to make it more difficult for legal authorities to track their activities. This advantage coupled with the high value of the currency made it a booming business. With the evolution of ransomware came offers for free single-file decryption, multi-language support and customer service—all from the bad actors who had perpetrated the attack in the first place.

In 2017, ransomware attacks spread panic around the world. Organizations scrambled to safeguard mission-critical data and often paid the ransoms—but they didn't always receive the keys to decrypt their lost files. We saw fewer ransomware attacks succeed in 2018, partially because better backups, more awareness, and evolving defenses have made it more difficult to pull off productive campaigns.

Although Webroot has seen a further decline in ransomware attacks over the last year, they certainly haven't gone away. Instead, ransomware has become more targeted, better implemented, and much more ruthless, with criminals specifically targeting higher value and weaker targets. Additionally, this threat has continued to target RDP to breach systems, particularly compromised remote desktop protocol (RDP) tools commonly used by managed service providers (MSPs). Breaching a single MSP can provide give criminals access to an entire client base of businesses, making providers especially lucrative targets.

Examples of notably successful exploits used by ransomware during the past decade include EternalBlue, originally developed by the US National Security Agency and later leaked by a hacker group. The worldwide WannaCry ransomware attack, which began as a supply chain attack on Ukrainian targets through tax software, used this vulnerability to attack unpatched systems, and, in spite of a kill switch, the attacks caused billions of dollars of damage and downtime. The same exploit was used later to carry out the NotPetya attack on still more unpatched systems.

THE LATEST RANSOMWARE TRENDS

MORE RECON

Attackers are focusing their efforts on learning about a company and its infrastructure, including critical servers and backup locations. That way, they know which malware and exploits to use to increase the likelihood of success. These types of recon attacks are especially effective when targeting small and medium-sized businesses (SMBs) who are less prepared (i.e. no contingency plans, risk assessment structures, cyber insurance, etc.)

RISING RANSOM COSTS

The average ransom amount is increasing. In Q3 2019, it reached $41,198, up from $36,295 in Q1.[4] These figures are reported by Coveware, a company specifically set up to help ransomware victims pay their ransom. The existence of such a company in the first place is a testament to the ongoing success of ransomware attacks.

DOUBLE TROUBLE

As it was in 2018, the one-two punch of Trickbot-Emotet prevailed in 2019. Emotet is a botnet delivery network that allows you to deploy other infections; it often drops Trickbot (a banking Trojan that steals data, but also gathers info about the organization). Recently such attacks have targeted larger companies, attempting to find lucrative victims who would pay large ransoms. In 2019, Trickbot delivered a two-pronged attack, stealing information and then dropping Ryuk, another type of ransomware. In addition to stealing personal data and credentials, Trickbot was able to go back to the same victims and attack them again later via ransomware.

These attacks rely heavily on phishing emails to get a toehold in the network. They take advantage of timely topics, such as healthcare enrollment or climate change, to increase the chances someone will click a link and download a Trojan, ransomware, or other malware.

Another extremely successful ransomware organization, "Evil Corp", is the target of a US Justice Department hunt—with a $5M bounty offered for information leading to the conviction of Maksim Yakubets, the hacker believed to be responsible. The Russian organization has stolen some $100M from businesses and consumers. The group uses Dridex malware to steal banking credentials from employees at small to mid-sized companies, then recruits "money mules"—unwitting or complicit collaborators—to assist in laundering the money obtained through the scheme. The group is also responsible for BitPaymer, a ransomware attack that hit several companies in Spain in late 2019.[5]

HIGHER STAKES

A recent trend in ransomware is to not just steal or lock an organization's data, but to threaten the victim with leaking or otherwise abusing the data. This increases the likelihood that victims will still pay, even if they have adequate backups in place.

SHIFTING TARGETS

2019 saw an epidemic of ransomware attacks on US cities, as well as systematic attacks on favored targets, such as transportation, healthcare, education, and SMBs. Many of these attacks make use of Ransomware-as-a-Service malware, which is freely available on the dark web and easy to use by even inexperienced cybercriminals.

HIGH-RISK URLs

Webroot has examined billions of URLs over the years, continuously scrutinizing their behavior, history, age, popularity, location, networks, links, and real-time performance. This year we saw a slight increase in the volume of high-risk URLs. However, the number of malicious URLs found on non-malicious sites decreased; it's now 24% (down from 40% in 2018). Still, the figure is not insignificant.

1 in 4 malicious URLs is hosted on an otherwise non-malicious site.

Making a website more secure calls for due diligence, staying on top of patching and having a review process for existing content, as well as reviewing access control over who can publish content. While it's clear many organizations have taken the trouble, 24% remains a high number, testifying to the fact that cybercriminals know it's difficult to block bad content on otherwise good domains. Keep in mind that, because HTTPS traffic is encrypted, there is less visibility into the pages hosted on HTTPS sites. In addition, adoption of HTTPS has increased, limiting visibility to the domain level within devices that cannot or don't decrypt traffic. These devices are typically meant for home or small-business use, but also can span into the enterprise arena, meaning the impact may be widespread. Ultimately, solutions that only look at the domain to evaluate risk are not as effective as those that evaluate the pages within the site.

URL CLASSIFICATION

We classify high-risk URLs in several categories: phishing, botnets, keyloggers and monitoring, proxy avoidance and anonymizers, malware sites, spam sites, and spyware and adware. Phishing represents 45% of the high-risk URLs found this year; we saw big spikes in July and August (26% of the annual total phishing sites found), and another ramp-up toward the end of the year. In fact, 62% of the phishing URLs were seen in the second half of the year. This may be related to the rise of online activity during back-to-school and holiday time periods.

The upward trend in high-risk URLs is a continuation from previous years, and the growth in 2019 is largely driven by phishing sites. Phishing continues to grow in prevalence with a notable uptick before the holiday season: visits to phishing sites spiked to 21% on Black Friday and to 58% on Cyber Monday, while visits to spam, questionable, spyware and adware, and proxy sites increased on Cyber Monday.

Phishing URLs grew by 640% throughout the year.

In contrast, we saw a gradual decline in the percentage of URLs that appear to be related to malware hosting. While rates varied between 1-1.5%, we saw a significant drop from 1.45% at the beginning of the year to 1.06% by the end of the year.

We also saw a steady decline in the incidence of URLs related to spam, proxy avoidance and anonymizers, adware, and spyware.

SPOTLIGHT: MALICIOUS CONTENT DISTRIBUTION

More than a quarter (28%) of URLs classified in the Security category in 2019 were malware content distribution sites. When we examine the categories of malicious content distribution, we see that URL shorteners and cloud storage are, as in the past year, the top two ways to obfuscate where content really originates. If we consider the top ten thousand most popular domains as published by Alexa Internet, more than 20 different content categories were found to be hosting malicious URLs, and 96% of them were doing so via URL link modifiers/shorteners. While URL shorteners are easy to use and popular, enabling users to communicate with a limited number of characters (e.g. for Twitter), they obfuscate where the user is really being taken.

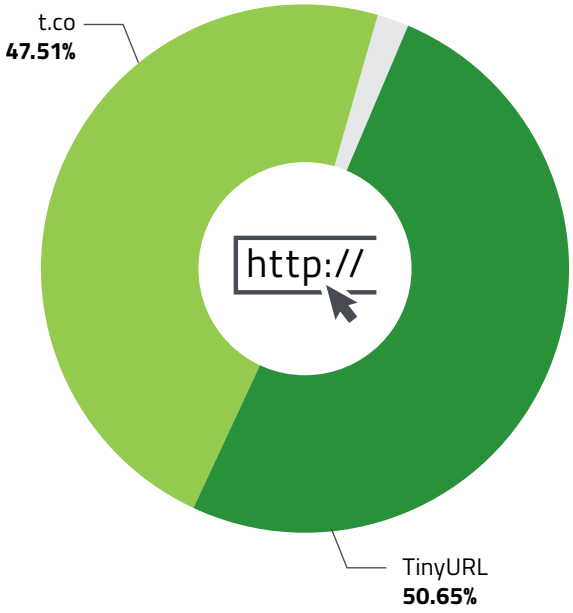


Figure 2: The top two culprits for malicious URLs in the URL Link Modifier category

Cloud storage can also pose a risk to users. While the domain itself may not be classified as malicious, the path of the URL could be. For example, the user might receive a link to the cloud service, but the file the URL points to is malicious. Last year, 3% of cloud storage URL paths were malicious, a significant increase from the 1.28% seen in 2018.

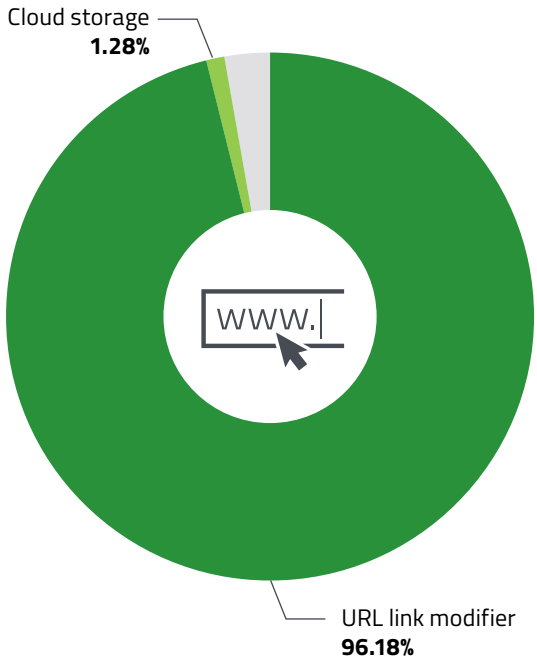


Figure 3: Malicious content distribution across benign domains in the Alexa top 10k

Malicious content distribution occurs across many types of benign domains as seen in the Alexa top million most popular domains.

URL category	Percentage hosting a bad URL
Manufacturing	19.87%
Shareware / Torrents	11.84%
Adult	9.43%
Social Networking	8.71%
Entertainment	8.63%
Medicine	7.66%
URL Link Modifier	5.81%
Other	28.06%

Figure 4: Top site categories hosting malicious URLs in 2019

While it is easy to understand how shareware/torrents, adult sites, and social networking would be obvious vehicles for malicious content distribution, it's not so obvious why others appear in the list. Manufacturing, for example, tops the list as the most-targeted category. This may be because manufacturing sites are less likely to be patched and fully up to date, making them more vulnerable. Manufacturing organizations also have complicated supply chain relationships, often driven by APIs that can be attacked. As noted in the Malware section, manufacturing devices saw a slightly higher rate of infection than the overall average for Webroot customers who reported their industries, reinforcing the notion that cybercriminals may be targeting that industry. Rounding out the top 10 are Real Estate, Food and Beverage, and Blogs.

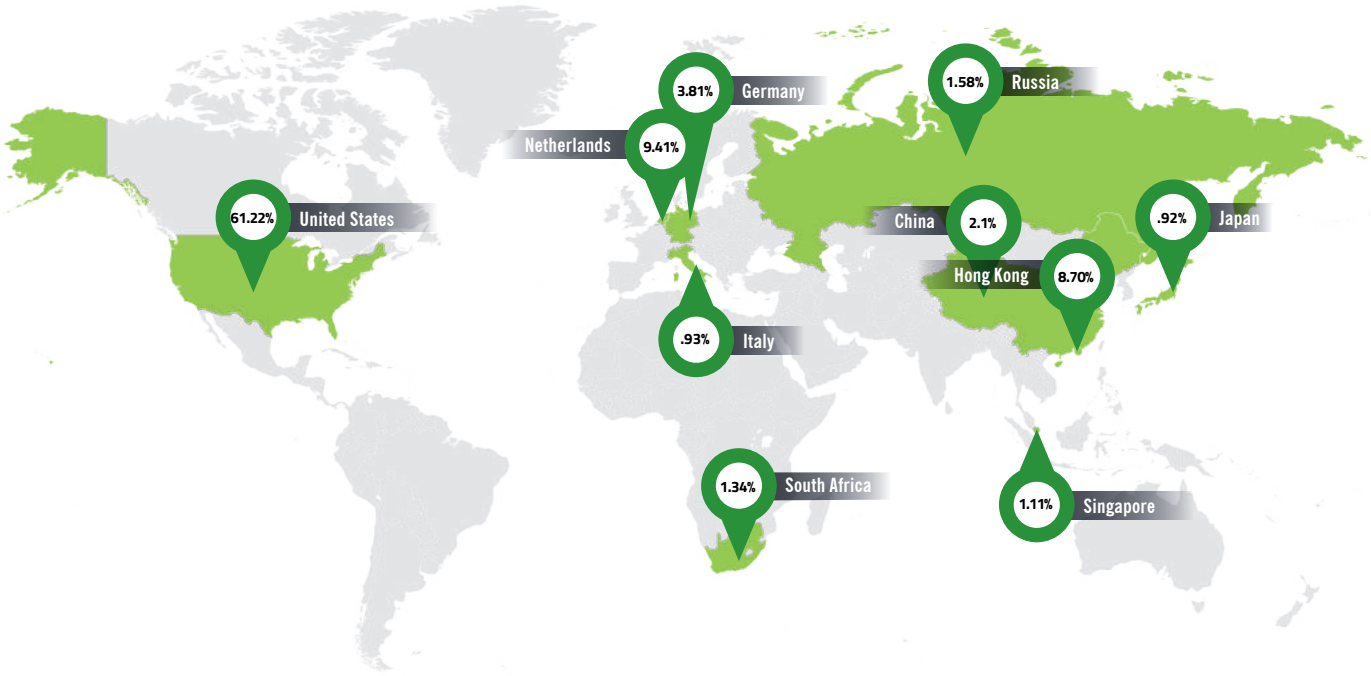


Figure 5: The top 10 countries hosting the majority of high-risk URLs in 2019

GEOGRAPHICAL DISTRIBUTION

In 2019, the ten countries that hosted the majority of high-risk URLs were fairly similar to those from 2018, but the UK, Canada, and France dropped off the list. These were replaced by South Africa, Singapore, and Italy (all representing less than 5% of the total).

As we saw last year, the majority of sites hosting malware are coming from the US. This percentage has remained relatively steady, up slightly from last year's 63%.*

CRYPTOJACKING AND CRYPTOMINING

In 2018, cryptojacking (the practice of using browser-based programs to mine cryptocurrency without the user's knowledge or consent) and cryptomining (malware that usurps a user's CPU to mine cryptocurrency) grew to be major threats. Cybercriminals could use them to easily monetize their attacks, and the extremely high value of crypto coins made the practice quite lucrative. Huge robberies, hacks and mining operations made the news.

Cryptojacking remained prevalent in 2019. Millions of dollars in cryptocurrency was stolen from crypto exchanges during the year.[6] An extremely dangerous type of router attack, which can result in every web page having a script on it, became prevalent. The problem grew large enough to attract the attention of law enforcement; a five-month-long operation coordinated by INTERPOL caused the number of routers infected with coin miners in Southeast Asia to drop by 78%.[7]

During 2019, Webroot encountered more than 146,000 domains hosting cryptojacking scripts, resulting in 8.9 million URLs hosting a cryptojacking script.

Although 2019 finished with a significantly lower number of cryptojacking URLs in December than in January, there were numerous notable spikes throughout the year, and sites continue to take advantage of this technique. One major event that affected the numbers occurred when the biggest player, Coinhive, shut down. At the start of 2019, Coinhive represented 84.5% of cryptomining activity. By the end of the year, the shutdown notwithstanding, it still represented 60.67% of activity. In March, there were almost 700,000 URLs running the script. By the end of the year, Coinhive was still running, but not mining. The fact that the Coinhive scripts remain active on so many domains suggests they were likely placed there by bad actors, and the website owners are not aware the scripts are there.

8.9 million URLs were found hosting a cryptojacking script.

* Note: this figure includes phishing sites, which may account for the large percentage coming from the US. Bad URLs are often in the same geographical region as their targets, and the highest density of Webroot customers is in the US.

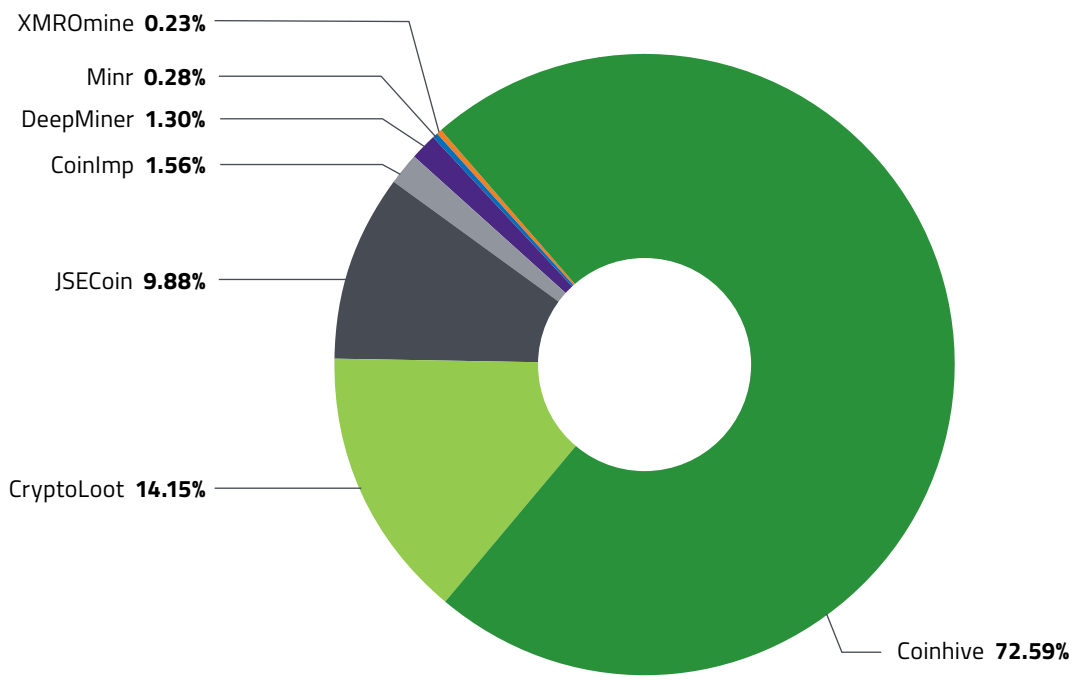


Figure 6: URLs hosting a cryptojacking script, tracked across the seven most prevalent cryptojacking services (Note: Coinhive no longer mines.)

Some of the gap left by the Coinhive dissolution is being filled by CryptoLoot (14.15% of traffic to crypto sites), JSEcoin (9.88%) and CoinImp (1.56%). Overall, almost all cryptojacking services showed a decline throughout the year, with the exception of CoinImp which showed a slight increase. The top 20 domains represent 25% of all customer traffic to cryptojacking domains.

Similar to last year, we saw a gradual decrease in detections on endpoints throughout the year; 22% of the year's cryptojacking incidents were found in the early months of the year, dropping to 7-8% by the end of the year. This is likely due to improved browser-based security against web-based cryptominers.

ass1st.com	5.64%
tpbproxyone.org	2.48%
rotate4refs.com	1.93%
propertiesyoulike.com	1.66%
smokingarchive.com	1.63%
anddev.org	1.32%
cheatcodesgalore.com	1.10%
vidics.to	1.05%
koinohajimari.com	0.98%
erogifs.com	0.94%
airproxyunblocked.org	0.89%
warly.ir	0.77%
svobdoska.ru	0.73%
oklahomaball.com	0.71%
themelike.net	0.62%
nepallist.com	0.60%
coinhive.com	0.60%
boya.com.sg	0.59%
pepitos.tv	0.59%
thepiratebay.bet	0.57%

Figure 7: The top 20 cryptojacking domains

PHISHING ATTACKS

Although phishing has been around for much longer than just the past ten years, it has evolved significantly. Early attempts were broad-brush, sent to huge numbers of recipients indiscriminately. But hackers later learned that, if they could target their victims selectively via spear phishing, they could increase their success rate. The wealth of personal information freely shared over social networks made it much easier for them to learn about a given victim's online habits, which, in turn, made it easier to craft a targeted phishing email specifically intended for that person.

A recent example of the continuing evolution of phishing is hijacked email reply chains. A hacker gains access to a person's email and takes over a legitimate conversation, then forwards it to one of that person's friends or colleagues with a malicious payload attached. The email is likely to get through any email filtering, and the recipient is likely to open it, since the conversation details are convincing—because they are real. However, opening the file could result in infection with Emotet or another banking Trojan, such as Ursnif/Gozi.

Year over year, we continue to see growth in phishing attacks, which remain an effective vector for capturing credentials and other sensitive data. The threat is ever-present; 1.6% of Webroot customers encounter a phishing page each month, representing some 20% of Webroot endpoint protection customers annually. Overall, the number of known phishing sites grew six-fold from January through December 2019: from 0.15% to 0.96% of all sites. The biggest difference we saw in phishing in 2019 is the surge in the number of HTTPS phishing sites. In 2018, 15% of phishing sites used HTTPS to trick the user into thinking the site was safe; by 2019 the percentage had risen to 27%.

THE MOST IMPERSONATED COMPANIES

In general, of the companies that were the most often impersonated in phishing attacks in 2019, eight of them were holdovers from the top ten most impersonated in 2018. Chase (at 3.1%) replaced Bank of America, which dropped out of the top 10, but remained in the top 20 at 2.4%.*

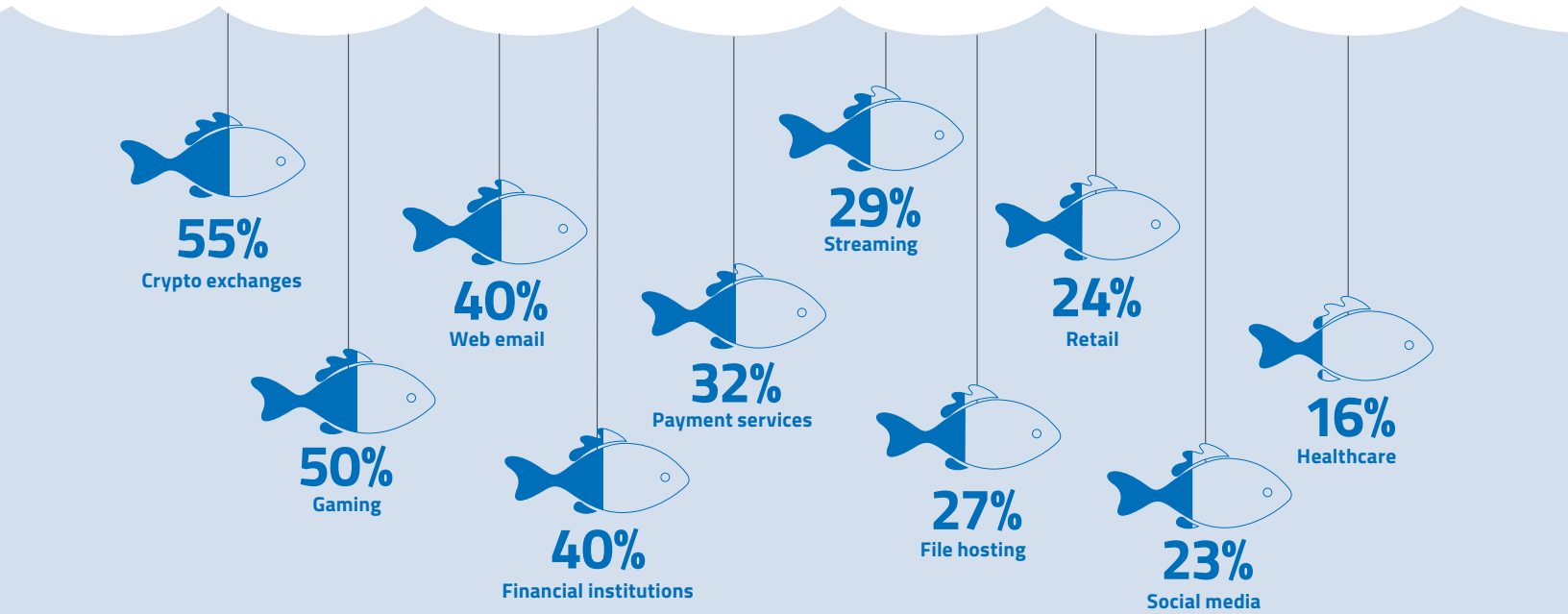


Figure 8: Top 10 industries targeted by HTTPS hosting

*Webroot data comes from our endpoint protection customer base, which is largely US-centric, so the following data is skewed toward US online habits.

Last year, Google topped the list at 15.6%, followed by Microsoft, Dropbox, and PayPal. When we expand the list to the top 20, we find many other household names, such as Amazon and Netflix, as well as DocuSign, Instagram, and Steam. DocuSign is a particularly interesting entrant due to its frequent use as a means of electronically signing important documents; impersonating DocuSign could lead an unsuspecting victim to fill in a form with personal information, thinking the data is going to a legitimate user. Likewise, the video game digital distribution service Steam, which enables automatic updates for games, could be impersonated to download malware to a device.

On a monthly basis, attacks on the top ten most impersonated brands tell an interesting story. Microsoft actually started the year with more than twice as many phishing attacks impersonating the company than Facebook. The number peaked from March through May, then declined dramatically until a jump in October. Attacks impersonating Apple quadrupled in March, dropped, then spiked again in October. (This is most likely tied to Apple® product release dates.) Google attacks started slow in the year, but saw a steady increase until the number of attacks was on a par with Microsoft and Apple. Additionally, Office 365 and Google Cloud have both been targeted with cyber threats. Examples include a recent phishing threat that use stolen passwords as scare tactics for spam campaigns. Rampant password reuse and heavy social media activity contribute to hackers' ability to target victims and frighten them into revealing their credentials. In addition, use of AI to create multi-faceted campaigns has made it more difficult for users to distinguish phishing emails from legitimate communication.

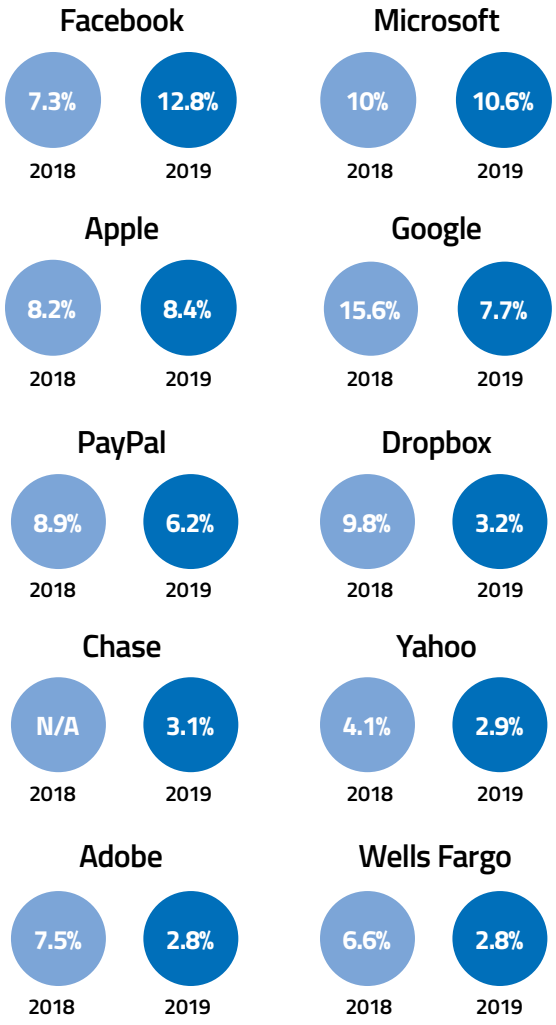


Figure 9: Top 10 companies most impersonated in phishing attacks

BUSINESS EMAIL COMPROMISE STILL NOT SLOWING DOWN

As in years past, business email compromise (BEC) continue to be prevalent. This type of email fraud targets commercial, government, and nonprofit organizations by fraudulently representing a senior colleague or a trusted customer. The email typically contains instructions to send money (especially via wire transfer) or release client data. BEC relies heavily on the inherent trust of employees in their senior executives and valued customers. Publishing giant Nikkei lost roughly $29 million after an employee of the Nikkei America subsidiary was tricked by scammers into sending funds to a bank account they controlled (Nov 2019). A Lithuanian man pleaded guilty to a BEC scam that tricked Google and Facebook employees into wiring him $112 million (March 2019).[8] According to the FBI, BEC is a $26 billion scam, and showed a 100% increase in the identified global exposed losses between May 2018 and July 2019.[9] AIG Insurance claims that BEC has overtaken ransomware and data breaches as the main reason companies filed a cyber-insurance claim in EMEA last year.[10]

MALICIOUS IP ADDRESSES

Over the past ten years, we have seen the impact that Tor has had on cybersecurity. We've witnessed layered proxy networks being used to protect malicious actors from attribution, and have seen the rise of malware hosting-as-a-service. In 2019, we saw large amounts of malicious IP reuse in the IPv4 space, since it is entirely allocated and assigned. However, IPv6 will completely change the game. So far, IPv6 is making it easier for attackers to use new, never-before seen addresses when launching their attacks.

We see over 26 million IP-related security incidents each day.

Webroot tracks IP addresses by the malicious activities they carry out (e.g., scanners or proxies, spam, Windows exploits, web attacks, botnets, phishing, and mobile threats), so they can be blocked proactively. Overall, 88% of total malicious IP addresses in 2019 were malicious because of repetitive spam triggers. The total number is truly massive; in one day, we saw as many as 4.6M spam IPs. For the purposes of this report, however, we do not present the millions we track, but instead show what we saw from the most reoccurring top 50,000 malicious IPs, i.e. those with the highest number of observed malicious transactions.

GEOGRAPHIC BREAKDOWN

Malicious IPs are a global phenomenon. The top 50,000 malicious IPs span 184 countries. In fact, measuring by convictions, 80.6% come from 23 countries, and more than half come from just six countries.

Top six countries representing 50% of malicious IPs:

- USA
- China
- Vietnam
- Russia
- India
- Indonesia

Rounding out the top 10 are:

- Netherlands
- Taiwan
- Ukraine
- Germany

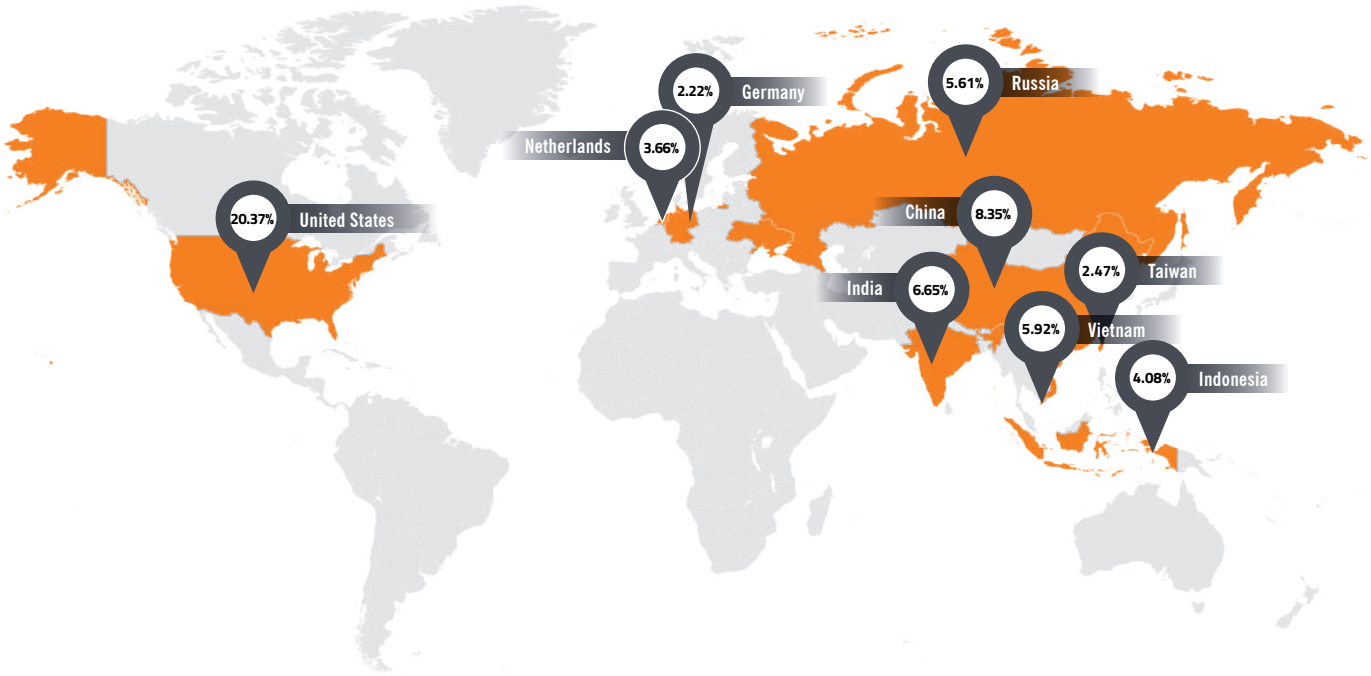


Figure 10: Malicious IPs by geographical region

Webroot tracks malicious IPs in several ways: by the IPs themselves, by the total number of IPs in each category, and by convictions. The term "convictions" refers to the number of times malicious behavior resulted in the IP being categorized as malicious or risky, rather than benign. (Multiple types of behaviors can be exhibited by the same IP, such as spam, botnet, and Windows exploit.) When looking at IP counts, 60% of malicious IPs are spread across 10 countries. But all the top 10 countries had IPs that exhibited malicious behavior five or more times, and 25 countries had IPs that were convicted in six or more categories.

AN IN-DEPTH LOOK AT IPs

Spam continues to occupy the top position in malicious IPs for another year. However, botnets rose from just 3% last year to 8% this year, and scanners still represent a significant percentage of the total seen in the top 50,000 (16%), down somewhat from last year's 19%.

The incidence of malicious IPs used for scanning dropped somewhat, but scanners still represent a significant threat. Hackers scan environments to learn details about network configurations, applications in use, and user behavior; armed with this information, they can select more lucrative targets and tailor attacks to that specific environment.

Windows exploits, while a much smaller category, present an alarming trend. For example, hackers might scan for systems that contain Windows vulnerabilities that have not been updated (such as the aforementioned EternalBlue), and exploit them by deploying targeted malware. The number of IPs associated with Windows exploits saw the biggest growth of any category in 2019, going from approximately 26,000 in January to more than 120,000 in December. That's a 360% increase.

MULTIPLE BAD BEHAVIORS

Malicious IPs are responsible for more than one type of bad behavior. In fact, all of the top 50K malicious IP addresses have been convicted in four or more categories. Additionally, they appear multiple times; 96% of bad IP addresses showed malicious activities more than once.

Malicious IP Fast Facts

- 92.9% have been convicted in at least 4 categories
- Just 3.4% of malicious IPs were convicted only a single time during the year
- Over 7 million IPs have been convicted more than 37 times during the year
- The top 1% of IPs convicted in 2019 were convicted more than 337 times that year alone

IP addresses associated with Windows exploits grew by 360%.

Figure 11: Malicious IP activity by category

HARMFUL MOBILE APPS

Since their introduction, Android™ devices have had a particularly rough time with security; several critical vulnerabilities were discovered over the past decade, with yet another major vulnerability found in November 2019. Google continues to fight malicious mobile apps, but the nature of their open OS hampers their efforts.

While Android malware is not nearly as prevalent as Windows malware, it remains a real, growing threat to the approximately 120.5 million Android users in the US.[11] To date, hundreds of malicious apps have been pulled from the Google Play Store through a review process that involves both computer algorithms and human review teams. Having implemented new, more stringent vetting for developers who want to publish their apps on Google Play for the first time, Google estimates the probability of downloading a potentially harmful app (PHA) was 0.64% in 2018, and much lower if the apps are downloaded from Google Play.[12]

Nevertheless, there are still many apps with security issues. Google found Joker malware (a.k.a. Bread) in 17,000 Android apps, which it subsequently removed from the Play Store. An analysis of the code showed that Joker's operators have used virtually every obfuscation technique available to evade detection. Since the average Android device comes with between 100 and 400 apps pre-installed, the potential for security holes remains high.

For Webroot-protected mobile users, the infection rate was 4.6% in 2019. The infections fell into several categories, with Trojans and malware representing the vast majority.

A recurring issue with Android devices is that more than 40% are using an OS version older than v9. As with Windows devices, older unpatched devices are more vulnerable to malicious applications. As an example, the exploit Bad Binder allows a malicious app to root and gain full control of a device. Android 9 and previous versions are impacted by this exploit, and older OS versions are susceptible to even older exploits. Apps crafted to take advantage of older exploits would continue to succeed on older devices that are unable to update to a more secure version.

Regardless of the method of attack or intent, malicious mobile code can spell trouble for users because the hacker can gain access to voice, text messages, and email; monitor all keystrokes; access the camera; track the device's location via GPS; and more. It's easy to see why mobile phones are highly sought after for compromise.

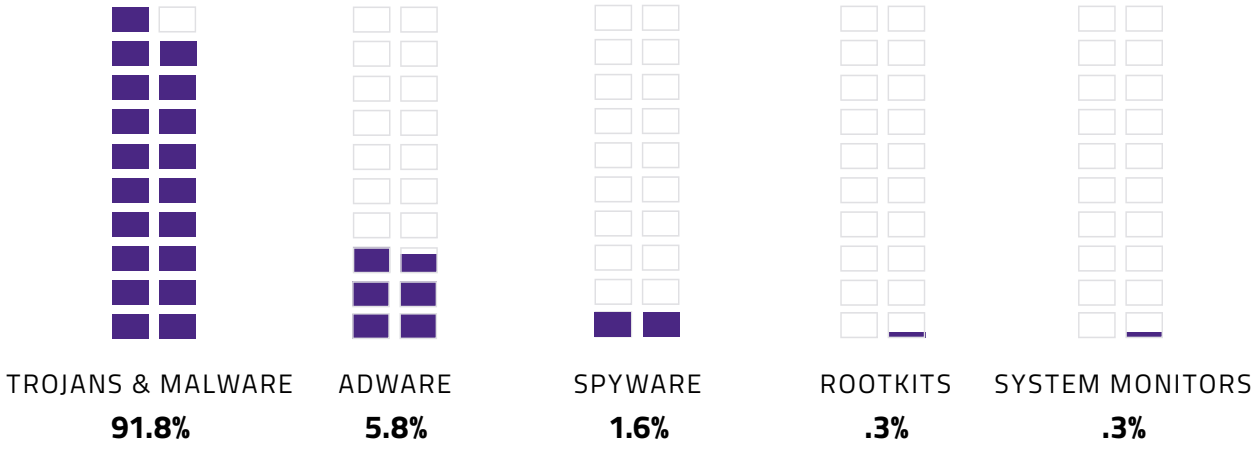


Figure 12: Malicious app breakdown (Note: of these, 12.5% were classed as potentially unwanted applications, or PUAs.)

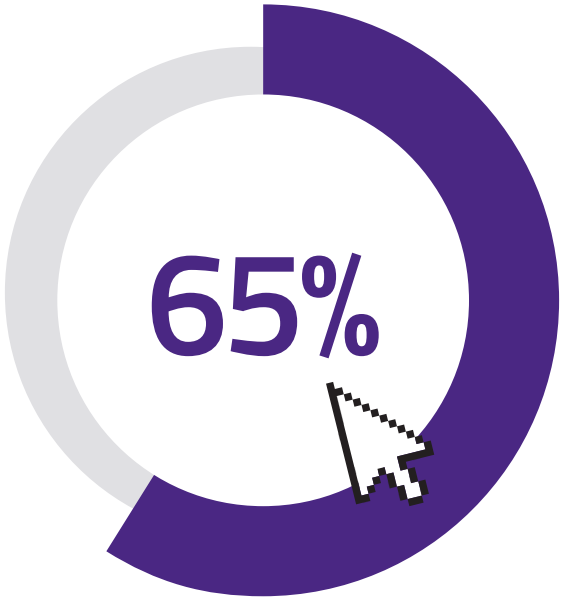
SECURITY AWARENESS TRAINING

New innovations always introduce new risk, but training goes a long way to reduce that risk. The growing field of preventive cybersecurity education (security awareness training) is highly effective at reducing security incidents related to social engineering, such as phishing, which are often the starting point for serious breaches. The first line of defense, trained individuals help protect sensitive data, intellectual property, and the viability of the organization itself.

In 2019, we saw that organizations running 1-5 security awareness campaigns over a one to two-month period showed an average click rate of 37% on phishing simulations. But running 6-10 campaigns and training over a period of three to four months reduced the click rate to 28%. The numbers improved even further when the organization ran 11 or more courses over a 4 to 6-month period: the rate dropped to 13%. This type of training is especially relevant in combatting BEC (see Phishing section) where large sums of money could be at stake.

One of the reasons behind the increased success of regular training is that users must be armed against highly variable, increasingly sophisticated, targeted phishing attacks, especially as these attacks rely heavily on current events and trends. Recent examples include package delivery notifications, warnings that social media passwords need to be changed, or that your credit card has expired and needs to be updated to continue to receiving a particular service. Anything that is current or popular is fair game to hackers, who can pivot quickly and modify their spam methods. Users need continuous, relevant training to help them avoid falling victim.

Running 11 or more training courses over 4-6 months reduces phishing click-through by



PREDICTIONS

Webroot security experts are leveraging the lessons of the past to forecast what we will see in 2020 and the coming years. Here are a few of their predictions:

WHAT THREATS WILL WE SEE?

"Expect to see more attacks against less-developed nations—not to generate revenue, but rather to disrupt and destroy," says Grayson Milbourne, Security Intelligence Director. He predicts that phishing will become even more targeted, as data collected from breaches is incorporated into phishing emails.

"We will continue to see Emotet as the front-runner in terms of both botnet size and malspam distributed. Ransomware will continue to be a threat. Less sophisticated actors will mimic the tactics used by larger, more successful operations."

Jason Davison | Advanced Threat Research Analyst

Eric Klonowski, Manager of Advanced Threat Research, foresees that ransom-motivated attackers will carefully observe automatic backup solutions and attempt to remove and/or alter the backed-up data or the task itself. Tyler Moffitt, Security Analyst, adds that, with privacy regulations like GDPR and CCPA in full effect, we are likely to see ransomware threatening to leak important customer data to increase the likelihood businesses will pay, even they have adequate backups in place and don't need the files back.

WHO WILL BE TARGETED?

Tyler Moffitt believes SMBs will continue to be targeted: they have lower budgets and scarce security staff, making them attractive targets. Kelvin Murray, Senior Threat Research Analyst, advises that user education is the main defense against BEC attacks. No reasonable amount of email filtering can stop all fake emails from getting through.

"All forms of the energy sector will continue to be at serious risk. In addition, service providers make very lucrative targets for attackers, as they are a single point of entry into many businesses. Executives will continue to be the targets of BEC attacks, which will continue to evolve in sophistication."

Matthew Aldridge | Principal Solutions Architect

WHAT ROLE WILL AI/ML PLAY?

Hal Lonas, SVP and CTO, warns that we will see more AI experimentation by cybercriminals, which will drive an increase in the scale and severity of attacks in 2020. Along similar lines, Joe Jaroch, Senior Director of Cybersecurity Strategy, believes adversarial attacks on AI-based security products will grow both in scope and complexity.

One of the scarier scenarios involves the use of AI in the production of deepfakes. In 2019, we saw the first examples of deepfake-style AI synthesis technology being deployed successfully to add a convincing new dimension to social engineering attacks.

"Deepfakes are going to become a major threat. As the technology develops, anyone could make a fake video of someone else saying something they did not, and could effectively weaponize it for malicious (or political) purposes."

Grayson Milbourne | Security Intelligence Director

IS CRYPTOJACKING DEAD?

Tyler Moffitt expects that, while we have seen cryptojacking decrease over the past year or so, the decline reflects the overall price of the cryptocurrency market. If we see another pump of cryptocurrency prices to an all-time high in the coming year, we're likely to see a resurgence in this type of attack. Matthew Aldridge anticipates that cryptojacking will continue in 2020, as a low-key way for criminals to make money by exploiting the resources of others. He predicts that attackers will find new types of computing devices and networks to target, to get a greater return on their invested attack time, using increasingly clever ways to avoid detection.

CONCLUSION

As we look back at 2019 and the preceding years, the changes are clear. We've seen a massive move to the cloud; evolving (and sometimes conflicting) user demands for privacy, security and convenience; the relentless innovation of cybercriminals; and an ever-expanding attack surface.

In terms of protection efforts, the sheer volume and variation of attacks necessitate a comprehensive, multi-layered approach. It should start with people. Educate them, train them to avoid risks and report suspicious incidents quickly and correctly, then introduce other defense layers to ensure that, if users do inadvertently click a bad link, they will be stopped preventively. (After all, even the best-trained users make mistakes.) If they try to visit a malicious IP address, there should be a layer of security in place to stop them from visiting it. If they attempt to visit a phishing site, yet another layer should be in place to protect them. If they should happen to run a malicious script, it should be prevented from executing. If they attempt to run a malicious program, or if an apparently benign application becomes malicious, this should be blocked.

And if all other methods should fail, all critical data should be securely backed up as part of a complete protection and disaster recovery strategy.

Ultimately, there is no silver bullet, there never has been, and there never will be. But by implementing security layers that protect users and data though all the stages of an attack, it's possible to achieve a state of "cyber resilience", in which businesses and end users can bounce back—even in the face of massive security breaches, cyberattacks, and data loss.

Hal Lonas | SVP & CTO, SMB and Consumer

[1] Verizon. "2010 Verizon Data Breach Investigations Report." (July 2010) https://www.wired.com/images_blogs/threatlevel/2010/07/2010-Verizon-Data-Breach-Investigations-Report.pdf

[2] The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved from www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

[3] Magic Quadrant for Security Awareness Computer-Based Training. Retrieved from www.gartner.com/doc/reprints?id=1-1OAYVTNP&ct=190723&st=sb

[4] Ransomware Payments Rise as Public Sector is Targeted, New Variants Enter the Market. Retrieved from www.coveware.com/blog/q3-ransomware-marketplace-report

[5] Spanish companies' networks shut down as result of ransomware. Retrieved from arstechnica.com/information-technology/2019/11/spanish-companies-networks-shut-down-as-result-of-ransomware/

[6] Bitcoin remains strong as 160 million stolen from crypto exchanges in 2019. Retrieved from cryptoslate.com/bitcoin-remains-strong-as-160-million-stolen-from-crypto-exchanges-in-2019

[7] Cryptojacking Drops by 78% in Southeast Asia After INTERPOL Action. Retrieved from www.bleepingcomputer.com/news/security/cryptojacking-drops-by-78-percent-in-southeast-asia-after-interpol-action

[8] Tech Duo Stung for $122m by BEC Attacker. Retrieved from www.infosecurity-magazine.com/news/tech-duo-stung-for-122m-by-bec-1?

[9] Business Email Compromise Is a $26 Billion Scam Says the FBI. Retrieved from bleepingcomputer.com/news/security/business-email-compromise-is-a-26-billion-scam-says-the-fbi/

[10] BEC overtakes ransomware and data breaches in cyber-insurance claims. Retrieved from www.zdnet.com/article/bec-overtakes-ransomware-and-data-breaches-in-cyber-insurance-claims

[11] Number of Android smartphone users in the United States from 2014 to 2021. Retrieved from www.statista.com/statistics/232786/forecast-of-andrioid-users-in-the-us

[12] To Stop Shady Apps, Google To Scrutinize First-Time Developers. Retrieved from uk.pcmag.com/news-analysis/120501/to-stop-shady-apps-google-to-scrutinize-first-time-developers

About Webroot

Webroot, an OpenText company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

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