2021 Webroot BrightCloud® Threat Report

CARBONITE® + WEBROOT®

Backup • Train • Block • Protect • Restore

opentext™ Business Solutions

Contents

OpenText™

2021 Webroot BrightCloud® Threat Report

Mid-Year Addendum

Significant Mid-Year Threat Landscape Shifts Prevail

This mid-year report is a six-month update to the annual Webroot BrightCloud Threat Report*. It distills a broad range of threat activity since January 2021 and offers insights into the most recent trends that have impacted critical industries, geographies, companies and people. The threat research team analyzed over 285 million real-world endpoints and sensors, specialized third-party databases and intelligence from end users.

The mid-year update reflects changes in the malware landscape, including record phishing spikes, and the continued role of cryptocurrency in ransomware.

Malware

Device Infection Rate Stays Above 50% for Repeat Offenders — Who is Affected More?

Of devices that were infected once in 2021, 52.36% of consumer and 45.49% of business devices sustained at least one additional infection, revealing that the simplest of security hygiene practices were not implemented before, during or after an initial infection.

Malware Expert Insight

The significant and ongoing increase in malware infections for consumers and businesses that suffered a single prior infection grew, revealing that threat protection was not applied or readied, leaving critical gaps in security posture. Industries that saw increases in infection rates aligned with those making weekly news headlines, with oil, gas and mining increasing 47% so far in 2021, while manufacturing and wholesale trades have both increased 32%. However, the management of companies and enterprises industry has shown the most significant increase in malware infections–57% versus the global average–highlighting the fact that technology supply chains are under attack.

> *People aren't learning from their cyber mistakes, and more concerning, they aren't equipped with knowledge on how to prevent repeat mistakes. Organizations must take ownership of the issue and do all they can in leading their people to improve security awareness, knowledge and habits.*
>
> **Grayson Milbourne, Security Intelligence Director**

Phishing

The Driving Force Behind the Single Largest Phishing Spike in a Single Month—440% Increase

Though the total number of new phishing sites dropped by 83% from January to April 2021 compared to the previous quarter, Webroot observed a significant spike (440%) in sites created during May 2021. Interestingly, though it did not experience the above January-April decline, online gaming platform Steam was a top target, comprising 50% of all in-the-wild detections from January-May 2021. Of those detections, 99% of Steam-related phishing sites used HTTPS. This is extremely rare and unique to Steam; however, 46% of all phishing pages are using HTTPS, up from 32% in 2020.

Phishing Expert Insight

Phishing is back in full force. Big brands continue to suffer, with potential risks for user engagement. While PayPal only accounted for 1% of the top 200 phished brands, its 1,834% spike in May showed that online payment services and financial institutions remain top targets for phishing attacks.

Unfortunately, inexpensive and easy-to-use kits being sold on cybercrime forums for as little as a few hundred dollars, enables low-level scammers to conduct effective template-based phishing campaigns.

Dr. Nolen Scaife, Senior Manager, Advanced Threat Research

Crypto Exchanges

Is the Future of Your Money Secure?

Crypto exchanges and wallets are increasingly being targeted by phishing. The Coinbase IPO was immediately followed by a spike. During that time, there was a 75% increase in Coinbase phishing pages using HTTPS, according to our observations. Crypto jacking remains active but has declined since March 2020 when we saw the end of several crypto mining operations, including Minr, XMROmine and JSECoin, though activity can continue for several years.

Crypto Expert Insight

Crypto jacking activity saw a 32% increase in April 2020, and by June of 2021, there was a significant decline of 39%. Although the number of domains hosting crypto jacking scripts remained steady in May 2021, there was a spike in visits to these domains across all types except CoinIMP.

Cryptocurrency is like leaving behind digital breadcrumbs on blockchain, and while crypto jacking in the browser is dead, crypto mining using applications is still very profitable and might yield a higher reward over time than a ransomware demand.

David Dufour, VP of Engineering

Conclusion

With the significant spikes around ransomware, malware and phishing attacks, our global supply chain should be better armed to provide safe and secure protection for valuable business data. But questions remain: *Can businesses deliver on a more secure posture, and will consumers embrace better cybersecurity hygiene?*

Organizations worldwide must focus on people to remedy the security gaps in any data-centric environment, as we continue to remain our own worst vulnerability, and pose the greatest risk to any IT environment; from server to endpoint.

Management and IT must collectively share the responsibility and apply new business continuity and cyber resiliency plans to do the following:

1. Purchase hardware and software to thwart a variety of modern attack vectors
2. Identify network dependencies
3. Manage internal and external communications during the crisis
4. Conduct awareness training to reduce human vulnerabilities
5. Implement backup and recovery procedures to maintain systems after an attack

While the news and headlines paint a grim picture, the reality is that ransomware and other cybercrime can be and is prevented every day. Businesses that embrace a cyber resilient strategy become just that, resilient to attacks.

Foreword

By David Dufour | VP, Software Engineering

"Zoom parties."

Before 2020 happened, if you'd told me that Zoom parties would become one of the most exciting events on my social calendar, I'd never have believed it. Yet here we are, with much of the world having been in varying states of social restriction or lockdown for over a year.

Although remote work wasn't a new phenomenon when the COVID-19 pandemic began, little could have prepared us for the explosion in online activity that followed. It wasn't just that more people started working from home; suddenly, many of us had to move our entire lives online. And as we shifted practical activities like work and school to online modalities, the internet also became our only way to connect with loved ones, see friends' faces, share in celebration, and mourn loss. Without a doubt, the notion of "normal" wasn't just put on hold; it was obliterated.

Whenever there's a major event or hot topic in the news, you can bet there will be opportunists on standby somewhere, poised to exploit it. The pandemic has been no different, with cybercriminals working overtime to take advantage of individuals and businesses as they transitioned to a mostly online lifestyle. New social engineering tactics, phishing campaigns, record-breaking ransomware payouts, and other developments emerged at astonishing rates.

Between February and March, our data showed a 2000% spike in malicious files with 'zoom' in their filenames.

The cybercriminals certainly didn't sit 2020 out. But neither did we. Cybersecurity analysts and threat researchers the world over have been working tirelessly to discover and neutralize threats as quickly as they appear. Operating systems and web browsers are making effective improvements to their built-in security. Risk awareness training and phishing simulations for employees continue to improve security postures. Nations and companies are working together to break down cybercriminal infrastructure. Like COVID-19 numbers, at least at the time we're writing this report, many previously virulent online threats are actually trending downward.

The last year certainly tested our fortitude, and its unique circumstances are not yet over. But when challenges come, we adapt. In times that threaten to push us apart, we find new ways to come together. We have proven our resilience and we stand together, ready to face what the future may bring.

Threat Intelligence Overview

The threat intelligence, trends and details presented in the 2021 Webroot BrightCloud® Threat Report are based on data continuously and automatically captured by the Webroot® Platform, which is the proprietary machine learning-based architecture that powers all of our Webroot protection and BrightCloud services. This data comes from over 285 million real-world endpoints and sensors, specialized third-party databases, and intelligence from end users protected by our technology partners. Our threat research team analyzes and interprets the data using advanced machine learning and artificial intelligence.

In this report, we'll break down a broad range of threat activity, offer insights into the trends we've observed, discuss wide-reaching impacts across industries, geographies, companies and people, and reveal what our threat experts expect to see in the coming year.

Webroot BrightCloud® Threat Intelligence Numbers

Real-world sensors	285M+
End users protected through technology partners	269M+
Domains	999M+
URLs	43B+
IPs – All IPv4 an in-use IPv6	4.38B+
File behavior records	37B+
Active mobile apps	37M+

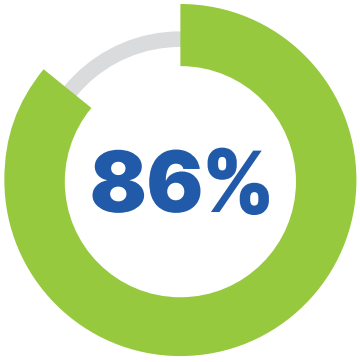
Malware

Something happened in 2020 that we've never seen before, and it's probably not what you think: the number of new malware and Windows® application files seen by Webroot-protected Windows endpoints dropped, and that's with more endpoints than ever before. This doesn't mean malware is on the decline, by any means, but it does merit a closer look.

Back in 2018, we saw around 500 million new malware and Windows application files. In 2019, this number climbed to nearly 600 million, but 2020 saw it fall to 2018 levels again. This decline seems to be due largely to the COVID-19 pandemic and the dynamic shift to work-from-home. During the earlier part of 2020, before the work-from-home transition had begun in full, numbers were on track for another record year. By April, there had been a significant decrease, and the numbers stayed at that level for the rest of the year.

Each year, we also track the percentage of detected Windows malware that is only seen on a single PC worldwide. We've recently enhanced our methodology for calculating this figure and updated our numbers accordingly. In 2020, it was a staggering 86.1% of malware, which is almost identical to the 86.2% detected in 2019. The highest rate we've observed was 89.1% in both 2018 and 2017.

Together, the new file count and the percentage of unique malware indicate that, although there's been a slight decline in volume, there hasn't been a major change in malware usage. As such, we expect the decline to be temporary.



of malware is unique to a single PC.

EXPERT INSIGHT

We believe the overall decline in malware is due to several factors. The first is improvements in our own technology, which includes layers of protection that can prevent an attack before the malware hits an endpoint device. The next factor is the rising adoption of Windows® 10, which is generally a more secure operating system. The third is a newer trend in which attackers use Living off the Land Binaries (or "LolBins"), which means exploiting applications that Windows systems already have by default, so there's less need to use malware executables in attacks. Finally, the TrickBot takedown likely played some part (more on this later), though it occurred late enough in the year that we believe we'll see greater impact from the takedown in next year's threat report.

Infected Consumer and Business PCs

In keeping with recent years' trends, consumer (home user) and business PCs were significantly less likely to become infected in 2020 than prior years. While 2019 saw 12.6% of consumer PCs and 7.8% of business PCs experiencing a malware infection at some point, these numbers plummeted in 2020 to 8.5% and 4.7% respectively. That's a 33% drop year-to-year for consumer and a 40% drop for business devices.

Of PCs that get infected, about half will get infected more than once.

Of consumer PCs encountering an infection in 2020, 53% saw more than one, and 17% saw more than five. Of business PCs encountering an infection, 48% saw more than one, and 13% saw more than five. These percentages are slightly higher than those from 2019.

Due to the way COVID-19 has altered the notion of work vs. home devices, it can be difficult to clarify these differences. For many, our homes have become our offices. We use business PCs on home networks and use consumer PCs to perform business tasks, blurring the boundary lines that, in years past, have helped delineate risk.

A Tale of Two Systems

Since its release, Windows 10 has generally been a more secure operating system than Windows® 7. In 2020, the Win7 rate was 0.09 infections per PC, while the Win10 rate was only 0.04. The previous year, these rates were 0.11 and 0.04, respectively.

The security gap between the two operating systems has continued to grow since Microsoft ended support for Win7 in January 2020 and stopped releasing patches for it. At that time, approximately 9.1% of consumer PCs were still using it, as were a surprising 21.7% of business PCs.

By the end of 2020, Win7 usage had dropped to 5.8% for consumer PCs and 10.0% for business PCs. Win10 runs on 87.4% of the consumer PCs and 79.1% of business PCs globally.

A full year after Microsoft stopped supporting Windows 7, 10% of business PCs were still using it.

Separating the infection rates for consumer and business PCs reveals that consumer Win7 PCs consistently have had higher infection rates than their business counterparts, and twice as high in 2020 (14% versus 7%). Similarly, consumer PCs running Win7 have had higher infection rates than consumer Win10 PCs, although the gap has closed (5% versus 4%).

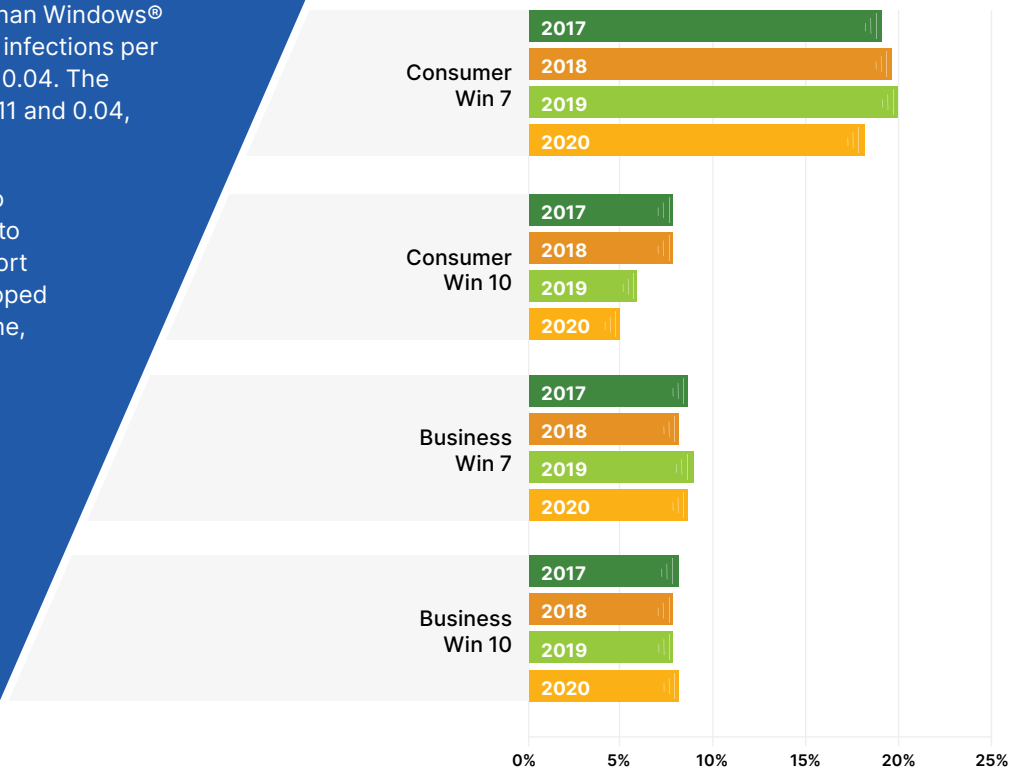


Figure 1: Infection rates by operating system across business and consumer devices

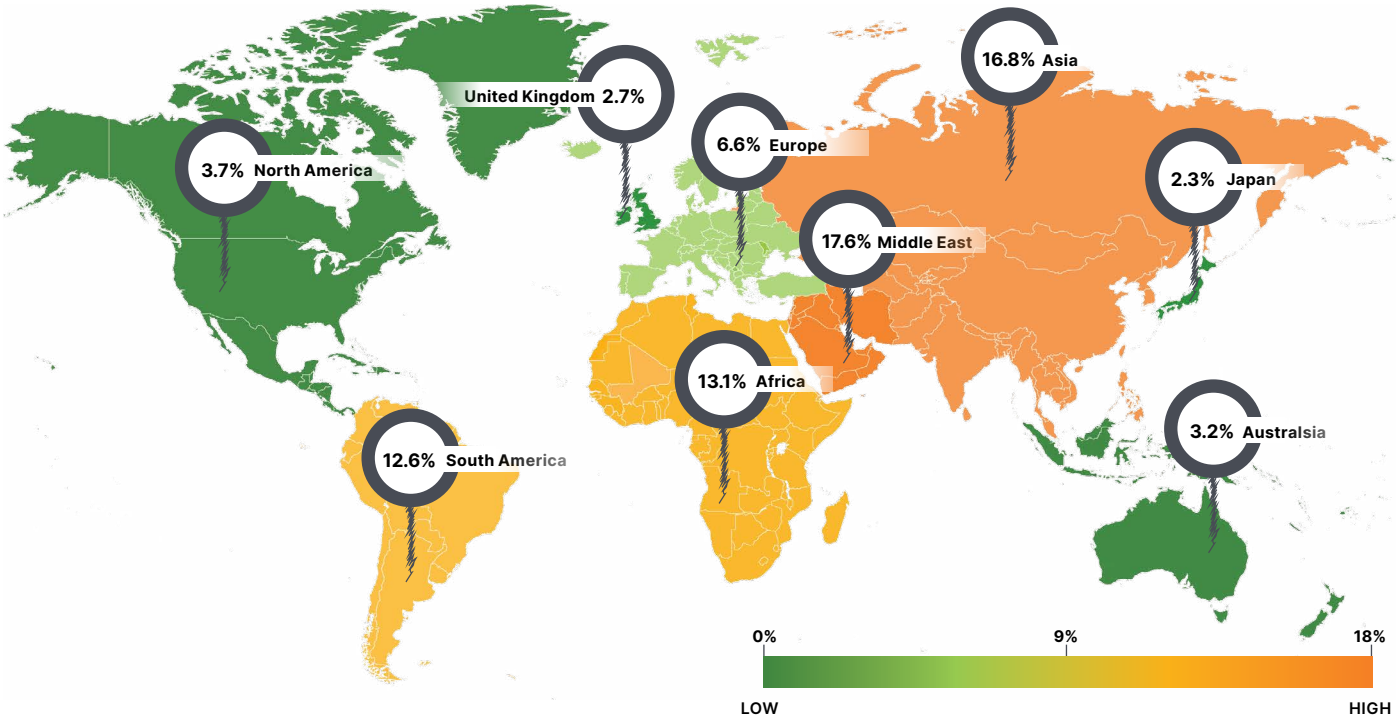


Figure 2: Infected devices by region

Infection Rates by Region

There's more to the Win10/Win7 story than consumer vs. business. Separating the infection rates by geographic region reveals additional trends.

When we look at infection rates for all PCs, without accounting for Windows version or consumer/business role, we see that PCs in Africa, Asia, the Middle East, and South America were four times as likely to be infected during the year than PCs in Australasia, Europe, Japan, North America, and the UK (15% versus 3.7%).

When we add Windows OS version back into the calculus, it explains much of the difference in these global infection rates. In the above groupings, PCs in the first set were almost twice as likely to be running Win7 as those in the second (23.7% to 12.7%).

Infections by region also vary between consumer and business PCs. On average, 18.8% of consumer PCs in Africa, Asia, the Middle East, and South America were infected during 2020, compared to 8.2% for Australasia, Europe, Japan, North America, and the UK.

Making the same comparisons for business PCs, those in the first set of regions had an average infection rate of 11.2%, while the second set of regions had a much lower rate: 3.0%.

Breaking out the numbers by region included a few surprises:

- Japan had the lowest rates of infected PCs at just 2.3%. It is important to note, however, that Japan is a unique region targeted by malware that is typically not seen in other regions.
- In Europe, 17.4% of consumer PCs had infections during 2020, but only 5.3% of business PCs did, meaning home devices were more than three times as likely to encounter an infection as business devices.

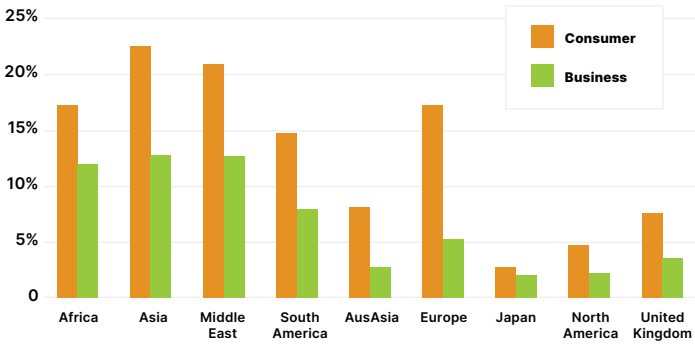


Figure 3: Infections by region for consumer and business PCs

Infection Rates by Industry

Nearly 40% of our business customers have reported their industry verticals to us. Although businesses in each industry saw lower infection rates in 2020 than in 2019, it's worth noting how the targets shifted. For example, in previous years, businesses in the Health Care and Social Assistance category were among those hit hardest by attacks; this year, their infection rate was a full 41.4% lower.

Based on reported data, the industries with the highest infection rates were as follows, where the percentages shown represent the deviation from the average number of attacks by industry: Wholesale Trade (attacks up 32.2% over average), Mining/Oil/Gas (up 32.0%), Manufacturing (up 25.9%), Public Administration (up 25.0%), and Information (up 22.1%). On the other end of the spectrum, the industries with the lowest infection rates were Health Care and Social Assistance (down 41.4% from the year-over-year average), Non-Profit (down 31.5%), Arts, Entertainment, and Recreation (down 20.7%), Educational Services (down 20.2%), and Finance and Insurance (down 16.5%).

EXPERT INSIGHT

Why did the targeted industries shift?

Cybercriminals often choose targets based on how easy it is to infiltrate them, i.e., they pick the lowest hanging fruit. Industries like health care, non-profit, entertainment, and education have been big targets for several years, so it's reasonable to expect that organizations in these industries would have taken steps to improve their security. As such, the definition of "lowest-hanging fruit" has changed, highlighting different industries whose less-secure or aging systems can be exploited. Additionally, the Maze ransomware group specifically swore to avoid targeting hospitals, emergency and public services, and promised to decrypt files for any such institutions targeted (more on this in the Ransomware section).

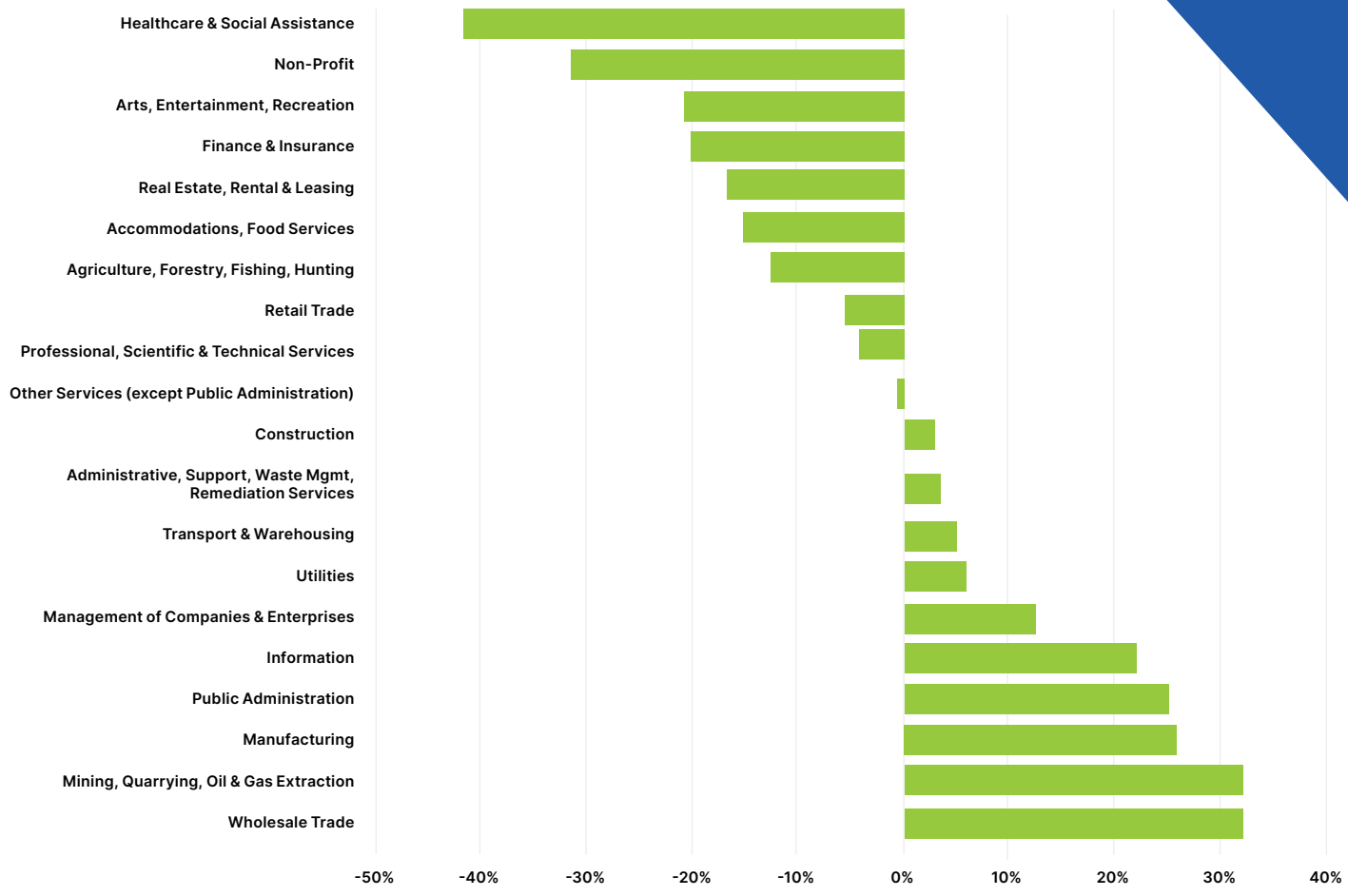


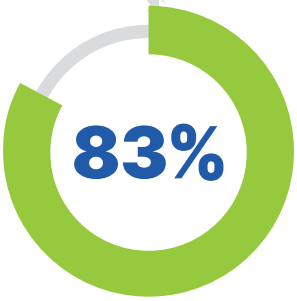
Figure 4: Change caption to: Infection rates by industry and deviation from average

Where Malware Hides

Malware can hide in many places on PCs, but some locations tend to get more use than others. In 2019, 85% of malware was found in one of the following folders: %temp% (38.2%), %appdata% (22.9%), %cache% (12.8%), or %windir% (11.2%). In 2020, the numbers were similar, with 83% of malware infections found in one of four locations: %temp% (28.4%), %appdata% (26.1%), %cache% (19.7%), or %desktop% (9%). Usage of the %windir% directory has fallen out of favor for the time being, dropping from 11.2% to 4.9%.

These changes in where malware is located continue the trends that we saw during the year before: usage of %temp% and %appdata% is declining and use of %cache% and %desktop% is rising.

Increasingly, companies are realizing the value in setting up Windows policies that prevent executables (including malware) from running in directories like %temp%. In 2019, 54.4% of business PC infections were in %temp%, compared to only 21.7% in 2020. Unfortunately, attackers have adapted by using %appdata% instead, where the infection rate has jumped from 16.7% in 2019 to 41% in 2020. The work is never done.



of Windows® malware hides in one of four locations.

The changes in where malware tends to hide prove it's possible to 'break' malware by preventing execution from certain directories. It's pretty easy to set up Windows policies that prevent executables from running out of %temp% or %cache%, but the other directories present more of a challenge, since execution from them can't be blocked by location alone. We recommend disabling macros, as well as any LolBins that are not in use. A good rule of thumb is: if it's not strictly necessary, disable it.

Grayson Milbourne | Security Intelligence Director

Ransomware

It was truly an astonishing year for ransomware, largely due to growing ransom payment amounts and the newer trend of data extortion.

Thought to have been pioneered by the Maze ransomware group, the extortion tactic involves not only preventing computers and files from being accessed, but also stealing a copy of the data and threatening to expose or misuse it if the victim doesn't pay. This new ransomware business model specifically targets sensitive data to increase the likelihood of payment.

In these situations, ransomware victims have verry few options. If a targeted business doesn't pay the ransom, the data may be disclosed publicly. Depending on the nature of the data stolen, the consequences of a breach could include costly fines for violating privacy regulations, such as the General Data Protection Regulation (GDPR) or California's Consumer Privacy Act (CCPA). These fines can add up to a major financial burden, starting at $100 USD per customer per record lost and increasing up to flat percentages of revenue.[1] As if the fines weren't enough, one must also consider the costs of downtime and recovery, like the $67 million loss that Universal Healthcare Services reported from its September 2020 ransomware incident.[2] Finally, there's the question of the brand's reputation and customer trust, which could be so irreparably damaged that the business might not survive.

For many businesses, the most attractive option (and the quietest) is to pay the ransom.

Although there's no guarantee that the criminals won't release the data anyway, some ransomware cartels conduct themselves as businesses, working to develop a reputation for keeping their word so that future victims are more likely to pay them. In fact, before permanently closing up shop in late 2020, the Maze group went so far as to state not only that they would avoid targeting hospitals, emergency services, and other public services, but that if anyone used Maze's ransomware against such institutions, Maze would decrypt the ransomware for free. But other ransomware gangs have no such scruples, as we saw when attackers targeted hospitals[3] and clinical vaccine trials[4] during the pandemic.

Rising Ransom Costs

As a result of the evolution of the ransomware business model, ransoms skyrocketed in 2020. At the end of 2018, the average ransom payment was $6,733.[5] At the end of 2019, it had increased over 1100% to $84,116.[6] By September 2020, the average peaked at $233,817; and by the end of 2020 it had dropped to $154,108.[7] Whether this drop is a temporary blip or a long-term trend remains to be seen.

2020 was also a year of record-breaking ransom demands. Here are a few examples:

- Attackers reportedly stole data from and encrypted a large number of servers at Foxconn, then demanded approximately 1804 Bitcoin (around $34 million USD at the time, but worth approximately $100 million now) to prevent the stolen data from being disclosed.[8]
- Attackers infected Garmin's systems with ransomware and demanded (and reportedly received) $10 million to destroy the stolen data.[9]
- Attackers infected numerous systems at CWT, a travel management firm, and demanded $10 million in ransom, ultimately receiving $4.5 million.[10]

Some companies now consider paying ransoms to be a cost of doing business. They prepare in advance for inevitable ransomware attacks, such as having Bitcoin on hand or being able to acquire it immediately, so they can pay ransoms quickly. For companies with cyber insurance policies, their insurance companies may pay their ransoms, typically after an evaluation of the security protocols and some negotiation to bring down the ransom cost.

Ransomware-as-a-Service Business Model

Ransomware-as-a-Service has become increasingly robust. Attackers have become more specialized, with each providing an individual service, like customizing ransomware code, providing a botnet for performing an attack, or collecting money from victims. Ransomware-as-a-Service customers can then use these individual services in series to issue ransomware attacks and collect the money. The attackers who provide the individual services are in business against each other, so the competition has made them highly innovative, and they're constantly testing new ways to refine their services.

Repeatedly, we're seeing evidence that botnets like Emotet (which was taken down this year), Trojans like TrickBot and Dridex, and ransomware like Conti/Ryuk are related to or working with each other. By examining shared code, shared infrastructure, money trails, and dark web forums, we can start to discern the relationships between seemingly disparate attack types. In many cases, there may be a single group or individual at the center of these pieces.

Ransomware cartels have also become more deliberate in how they target their victims so as to maximize their profits. The groups that carry out these attacks have typically done recon on their targets to discover exactly how to breach them and which systems to encrypt to cause maximum disruption.

Multi-stage Malware Attacks

As previously described, most ransomware victims are actually infected by more than just the ransomware payload. The ransomware is often the last stage of an attack, which could have been going on without the victim's knowledge for months or longer. What follows is a progression of how a multi-stage attack might unfold.

- First, a user clicks a malicious email attachment or a malicious link in an email and downloads a Microsoft document, typically Word or Excel.
- When they try to open the file, the user gets a notification asking them to enable macros. If they enable macros, a botnet or Trojan payload, such as Emotet, will infect the computer and act as a backdoor into the system for follow-up malware.
- Emotet (or whichever malware variant is acting as the backdoor) then drops TrickBot onto the computer. In this case, TrickBot serves as the payload that "cases the joint," moving laterally throughout the environment and using tools like Mimikatz to steal credentials when they are typed into the computer. Eventually, this process will give malicious actors domain controller credentials, arming them with the right access permissions to tamper with protections or backups and take other actions to ensure their eventual ransomware payload will cause as much devastation as possible.
- Finally, after the reconnaissance phase is complete, TrickBot drops Conti/Ryuk ransomware, for which the way has been paved to do maximum damage.

All of these threats can spread from the user's computer to other business systems, where they gather information for attackers. Eventually, the ransomware steals the business' sensitive data and encrypts its systems, and the attackers demand payment.

In most cases, ransomware isn't the beginning of a compromise. It's actually the end state, where the criminals cash in after an extended period. By the time you realize you've got ransomware on your network, the criminals may have been in there, watching, listening, and tampering with things for weeks or months without your knowledge. They might've even checked out your financials, so they know what kind of ransom to demand.

Kelvin Murray | Sr. Threat Research Analyst

These combined attacks aren't rare; rather, they are becoming the norm. The good news is that we're starting to see coordinated strikes against attackers, with nations and organizations acting together to break the Ransomware-as-a-Service infrastructure. For example, Microsoft and several partners requested and received a court order to stop TrickBot. This takedown was largely successful, although TrickBot has made a bit of a return since the takedown.[12] Additional takedowns are expected in the coming year and could cause some churn in how ransomware attacks are performed.

Thwarting Ransomware

Attackers like to target businesses with single points of failure—for example, SMBs that may have weaker security and few security personnel compared to large companies. They may also target much larger, better secured organizations, not only for the chance of a larger payout but also, effectively, for the bragging rights among their peers. Despite the shifts we detected in targeted industries, attackers continue to target the government, transportation, education, and health care sectors, which may also have fewer security resources compared to institutions in other sectors.

Combating the risks from ransomware requires layering your protection. No layer will ever be 100% effective at stopping threats, but by using several layers together—an 80% effective one, a 50% effective, a 95% effective one, etc., you build a far stronger solution than any single layer can provide.

One of the most important layers is user education. Time and time again, attackers enter company networks and systems by tricking users into clicking on a link or opening a file that leads to compromise. We've even seen a surge in telephone-based phishing with the COVID-related shift to remote work, in which the attacker calls the intended victim and impersonates a member of their corporate IT team to gain access.

Providing effective security awareness training and education for your users, especially on avoiding phishing attacks and other forms of social engineering, can significantly reduce compromises.

Another layer that's become particularly important during the time of COVID-19 is securing the Remote Desktop Protocol (RDP). RDP is a Microsoft remote access system that has become one of the most common ways for attackers to deliver ransomware because it provides desktop access to a machine in the environment, offering one of the most robust footholds to launch an infection. Millions of companies are using RDP without securing it properly, many of them because of hasty transitions to work-from-home due to COVID-19. Attackers can readily find unsecured RDP using scanning tools or by buying access from other attackers. From there, attackers are inside the company and able to wreak all sorts of havoc.

The best approach to thwarting ransomware is to make your business more resilient—in other words, prepared across all areas of your company where you might encounter risk.

David Dufour | VP, Software Engineering

High-Risk URLs

During 2020, there was an incredible increase in malicious URLs at the beginning of the year that coincided with the beginning of the COVID-19 pandemic. Between January and February, we saw an 88% increase in malicious URLs, largely due to increased phishing activity. By the end of the year, the number of malicious URLs had technically dropped 49% since the beginning of the year.

Another trend we saw was a significant decrease in malicious URLs being hosted on non-malicious sites. Although this figure was as high as 25% in 2019 and 40% the year prior, it's all the way down to 8% for 2020. What's not yet clear is the cause of this drop. During 2020 we enhanced some of our threat collection methods, which undoubtedly affected our data on the types of threats seen. Another cause could be overall improvement in website security. Some organizations may be becoming more diligent about the patching and configuration of their web servers and websites, while others may have switched from hosting their own websites to using cloud-based providers that provide security fundamentals for them.

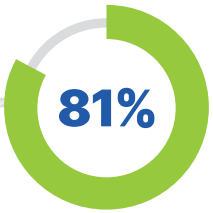
Approximately 1 in 10 malicious sites is hosted on a benign domain.

We'll be watching closely to see if the percentage of malicious URLs on non-malicious domains continues to decline and will continue to categorize individual URLs to more comprehensively identify threats and evaluate risk, compared to domain-only approaches.

Webroot BrightCloud Web Classification averages over 3 billion requests a day to categorize URLs based on their websites' behavior, history, age, popularity, location, networks, links, and real-time performance. We are constantly updating our categorizations to determine which URLs are high-risk and what nefarious behavior is associated with each URL.

URL Classification

The following categories comprise what we call high-risk URLs: botnets, keyloggers and monitoring, malware sites, phishing, proxy avoidance and anonymizers, spam, and spyware and adware. Over 81% of all high-risk URLs we discovered in 2020 were for phishing, which continues the trend we've witnessed in previous years. We'll dive deeper into this increase in the Phishing Attacks section of this report, but we believe much of this increase was due to criminals generating phishing emails that capitalized on COVID-related topics.



of high-risk URLs were in the phishing category.

COVID-19 had other impacts on cybersecurity, based on additional trends we saw in high-risk URL classification in the first several months of 2020. For example, categorizations of proxy and anonymization services increased 173% in March, as might be expected since so many people shifted to remote work and activities. Spyware and adware also shot up 269% in March, which may indicate attackers taking advantage of hurried work-from-home transitions with less-than-optimal security in place.

It's not uncommon to see shifts of this nature as malicious actors quickly pivot tactics to take advantage of the most current trends in internet use. At different points later in the year, we observed even more drastic swings in the spyware/adware and proxy avoidance/anonymizer categories, detailed in Figure 5.

Geographical Distribution

Every year, we see that only a small number of countries host most of the high-risk URLs in existence. 2020's list of countries is nearly identical to the one from 2019, with the United States far ahead of all others: 64.3% this year, down slightly from the previous year's 71.3%. (The U.S. figures are to be expected, since the U.S. is the most targeted nation for phishing and Webroot also has a greater number of end customers in the U.S.) The other countries in the top 10 remain largely the same, without significant changes to percentages or order (see Figure 6)—with one notable exception: Denmark. Denmark was in 16th place on the list in 2019, with just 0.5% of all high-risk URLs. Suddenly, in 2020 Denmark is second on the high-risk URL list, with 10.3% of those URLs. Although there are several factors that could contribute to this change, such as the amount of personal information required for hosting contracts, we have not determined a definitive cause at this time.

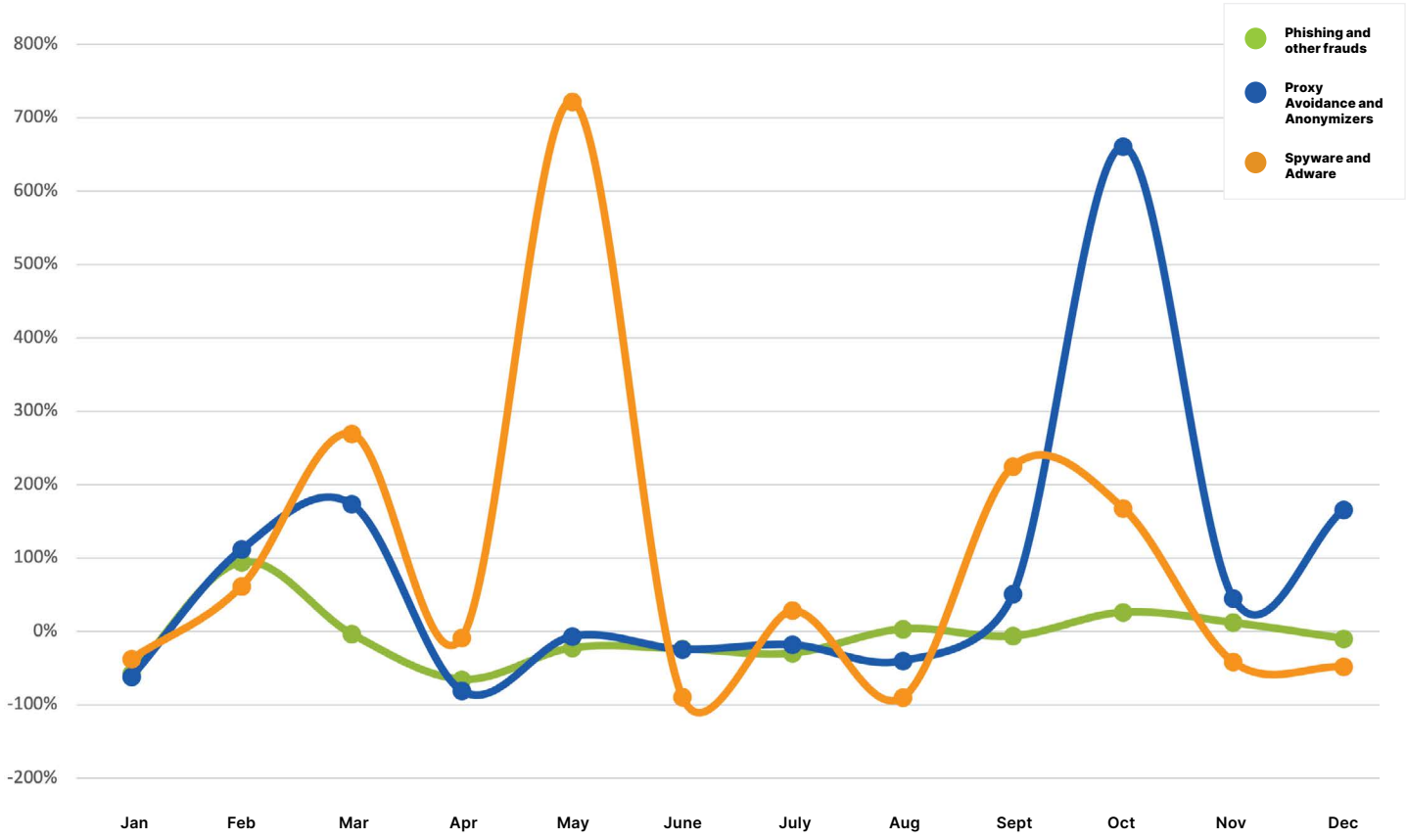


Figure 5: Trends in high-risk URL classifications

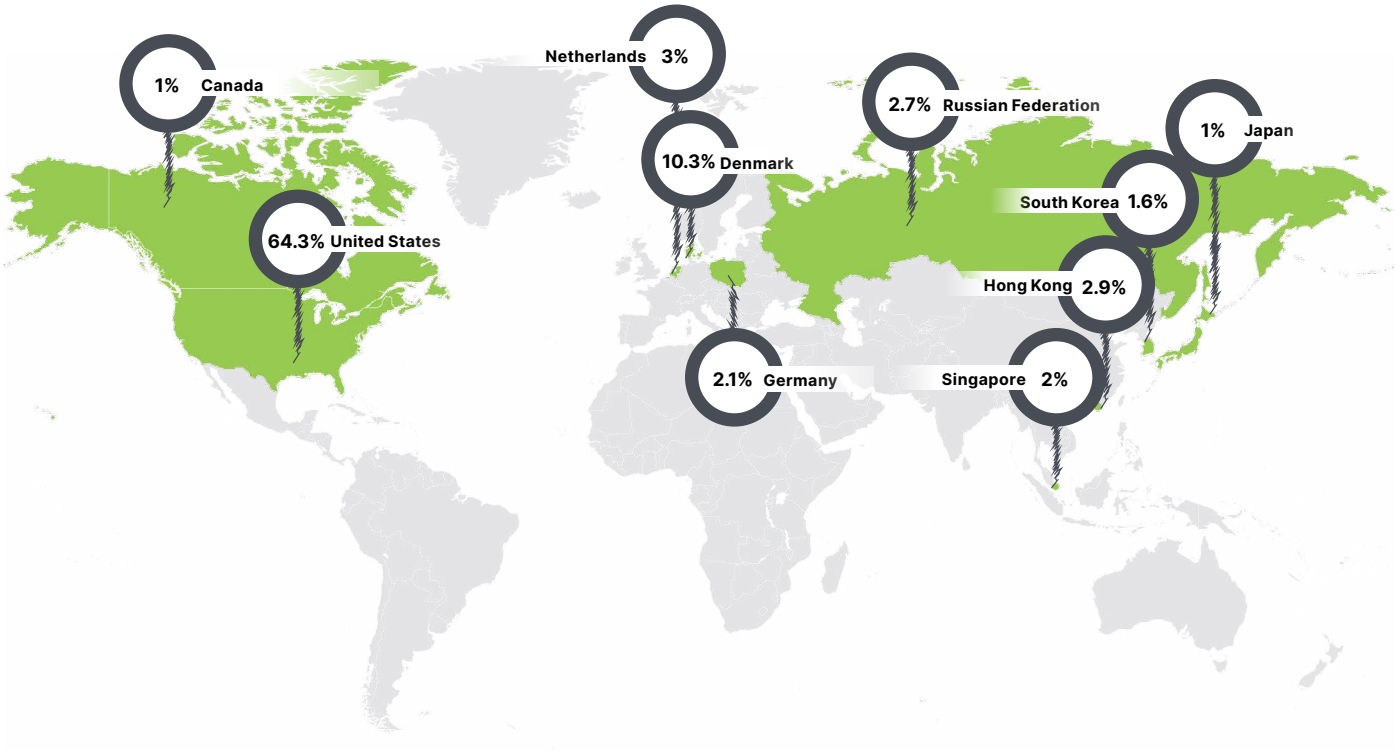


Figure 6: The top 10 countries hosting the majority of high-risk URLs in 2020

SPOTLIGHT: TrickBot

Once a humble banking Trojan that used web injects to steal login credentials, TrickBot has gotten quite the upgrade. Now, it is typically deployed as the second stage from a botnet and eventually leads to ransomware. Once on a machine, TrickBot spreads laterally through the network with the aim of stealing domain credentials to do the maximum possible damage.

In 2020, Webroot observed TrickBot endpoints downloading malware configuration files from a central repository service, then running on the endpoint with that configuration. This configuration information can be used to decode encrypted command and control channels, allowing malicious bot operators to steal credentials as users enter them into web pages. The malware may also initiate requests for additional access information, such as PINs or security codes, that are not requested by the legitimate website, or use web injection techniques to redirect victims to malicious servers when attempting to visit a legitimate site.

At the peak of activity from September to October, Webroot confirmed over 12,000 unique code repositories created each day being contacted by TrickBot endpoints, and we suspect there could have been as many as 50,000.

This volume indicates that TrickBot endpoints were contacting numerous dynamically-generated and short-lived command and control centers using rapidly updated configuration files.

To protect against common bots like TrickBot, it's best to adopt a comprehensive strategy toward cyber resilience that includes multiple types of protection at the endpoint, network and user layers, and that include threat intelligence that can automatically identify botnets and blocks these malicious domains.

Browser-Based Cryptojacking

For the past few years, many malicious URLs have been used for browser-based cryptojacking. Browser-based cryptojacking is when attackers inject malicious JavaScript code into improperly secured websites without the knowledge or consent of the website owners. Then all traffic to those webpages mines cryptocurrency for the criminal who put that script on those pages, using unknowing end users' computer processing power to do it.

1.4 million URLs still host cryptojacking scripts. Of these, about half are hosting defunct Coinhive code.

This type of attack has typically scaled with the price of Bitcoin, but exclusively mines the Monero cryptocurrency due to its profitability on consumer-grade hardware. After cryptocurrency prices fell in 2018 and 2019, most cryptojacking campaigns declined and some of the major players, like Coinhive, completely shut down. Although we expected to see some increase when cryptocurrency prices rose again, this form of cryptojacking continues to die off.

Despite declines, browser-based cryptojacking remains in use. It peaked in April, shortly after the start of the pandemic, but was falling sharply by June. Overall, it declined 35% from March to December. The number of domains found hosting a cryptojacking script also fell from 146,000 in 2019 to 66,000 in 2020. Also, the top domains had a bigger share of the business; the top 20 cryptojacking domains represented 25% of customer traffic in 2019, but they exceeded 40% in 2020. By themselves, the top three domains hosting cryptojacking scripts had a full quarter (24.75%) of the traffic.

The 66,000 domains resulted in 1.4 million URLs (down from 7.9 million in 2019) hosting a cryptojacking script tracked across the seven most prevalent cryptojacking services, including those no longer in operation: Coinhive (now defunct), CoinImp, CryptoLoot, JSECoin, Minr, XMROmine, and deepMinerAnonymous. Although the number of domains hosting these scripts did not increase in May, we saw a spike in visits to these domains across all types except CoinImp. 2020 ushered the end of Minr, XMROmine, JSECoin, and other cryptomining operations, but activity can still continue for several years to come, as we saw with Coinhive code.

As cryptocurrency values continue to fluctuate, we expect to see a return of this type of website monetization. However, it faces something of an uphill battle as web browsers are currently against the technique.

The number of sites continuing to host defunct malicious code and outdated, highly vulnerable plugins indicates how many website and domain owners do not adequately audit the code they host.

Cathy Yang | Lead Product Manager

dedmen.de	14.73%
smokingarchive.com	7.38%
oklahomaball.com	2.64%
hd-world.org	1.20%
ass1st.com	1.19%
aahora.org	1.18%
olavarriatv.com	1.17%
hollywoodmeasurements.com	1.07%
ganaycobra.com	1.01%
atk-exotics.com	0.98%

nedrobin.net	0.98%
digitaldredger.com	0.97%
vidics.to	0.96%
greenground.it	0.82%
getmypopcornnow.pw	0.81%
gdstudiogame.com	0.67%
datacenter-digiarty.com	0.65%
tfdmarket.com	0.55%
ukpassbay.org	0.55%
sirshanksalot.com	0.53%

Figure 7: Top 20 cryptojacking domains

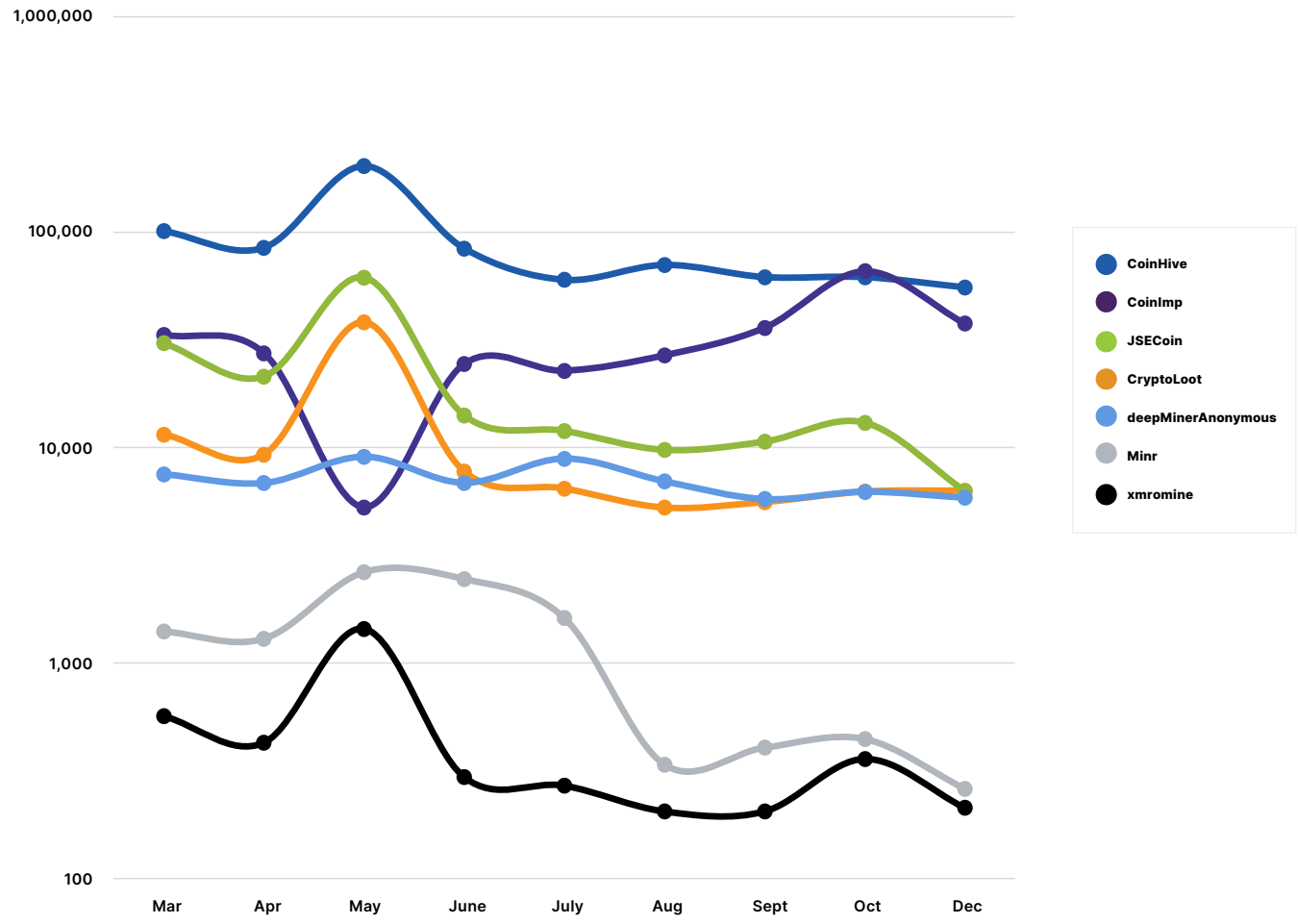


Figure 8: Visits to prevalent cryptojacking services

EXPERT INSIGHT

How do Bitcoin values affect cryptomining activity?

After every 210,000 blocks mined, or roughly every four years, a cryptocurrency event occurs in which the reward for Bitcoin miners is cut in half. Called "the halvening" by some crypto enthusiasts, this event typically brings steady increases in cryptocurrency values over the year or so immediately following. This is part of the normal market cycle and we're coming up on a bull market.

Executable-Based Cryptojacking

With cryptocurrency values soaring again, executable-based cryptojacking has been on the rise. As a general term, cryptomining refers to the practice, legal or otherwise, of mining cryptocurrencies using consumer or enterprise-grade hardware like CPUs and GPUs; cryptojacking refers to the type of cryptomining that occurs by hijacking another person's CPU/GPU power without their knowledge or consent. Many attackers who would have used browser-based cryptojacking services have shifted their focus to executable-based practices, in which they implant a malicious executable to run in the background on a victim's computer or server. This type of mining doesn't rely on website visitors to mine cryptocurrency; the mining is constant and can scale down its resource usage based on current legitimate CPU/GPU usage to evade detection.

Unlike browser-based cryptojacking, executable-based cryptojacking can be done on any device that has a processor and an internet connection, including many Internet of Things (IoT) devices, such as routers and smart TVs. Typically, people are unaware that their computers, servers, IoT devices, or other systems are running the malicious executable and have no idea their resources are being used without their consent. If a victim notices the effect of the mining, it's more likely because their systems slow down and their power bills skyrocket; otherwise, CPU usage scaling can effectively conceal the compromise.

Executable-based cryptojacking is now among the more popular choices for criminals to monetize a breached environment in cases where ransomware isn't deemed viable, since the payout starts immediately and no consent or knowledge of the breach is required. XMRig is the most popular mining executable currently used by criminals since it yields the most amount of money while running on consumer-grade hardware. We expect malicious cryptomining payloads to continue to grow in popularity as crypto market values increase.

Browser-based cryptojacking has largely died down as web browsers have improved their built-in protections. Site owners and visitors no longer need to take extra actions to stop these threats as Chrome and Firefox have embedded security. Since this model just isn't viable anymore, executable-based cryptojacking is getting more popular.

Tyler Moffitt | Sr. Threat Research Analyst

Phishing Attacks

Phishing attacks are still one of the most popular ways, if not the most popular, to insert ransomware and other types of malware into an organization's network. Getting a targeted victim to fall for a phishing attack is often the first step, giving attackers a jumping off point to perform reconnaissance, acquire credentials, interfere with protections, deploy malware payloads, and more as they decide what to do with any data they steal. Attackers are constantly improving their tactics, underscoring the importance of security awareness training to keep users up to date on the most current tactics.

Phishing and COVID-19

With COVID-19 dominating headlines all year, it's no surprise that criminals have targeted the topic in their phishing. In fact, the pandemic has meant big business for criminals. Most of the malicious spam (malspam) emails we've seen have used COVID-related phishing lures. The most common lures involved guidelines on how to protect yourself from COVID-19, typically pretending to be from reputable organizations like the CDC, WHO, NHO, or even the White House. There were also many lures claiming to offer details on pandemic stimulus money and vaccines.

Phishing spiked by 510% from January – February 2020 alone.

Most of the malspam asked users to download a Microsoft® Word document. Once the document was downloaded and opened from the email attachment or link, Word would ask the user to "Enable Content." This action allows macros, meaning a user who clicked to enable content would, in fact, be enabling delivery of malware like Emotet.

Just one click can be the catalyst that starts the infection process, eventually leading to ransomware or other forms of malware. If the user doesn't open the Word document or doesn't enable macros, the malspam poses no threat. This is why it's so important for users to be educated on the latest trends in phishing tactics.

Briana Butler | Sr. Technical Project Manager

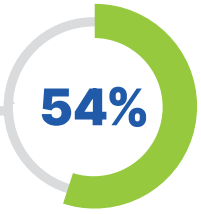
The rates of phishing attacks throughout 2020 largely coincided with the early months of the pandemic. Attacks increased 510% from January to February, with eBay and Apple being the brands most often targeted. Attack volume continued to grow into March, then dropped off as we moved into the summer. A more modest spike occurred in the months leading up to the U.S. election: up 34% from September to October, and another 36% from October to November. Although we typically note an increase in phishing activity in December due to the holiday shopping season, December of 2020 constituted one of the lowest rates of the whole year, underscoring the correlation between spikes and current events.

Phishing URLs with HTTPS

Another trend in phishing URLs is the use of HTTPS versus HTTP. Many users have learned to expect their websites to use HTTPS to protect communications, making them less likely to fall for phishing scams using HTTP. While switching to use HTTPS requires a bit more effort and expense on the attackers' part, it's well worth it, as using the HTTPS protocol gives unsuspecting victims a false sense of security, and the encryption can also prevent many web filtering solutions from identifying and blocking malicious communications. Throughout 2020, approximately 32% of phishing attempts used HTTPS. Keep in mind, this is the full year's average; in December of 2020, a full 54% of phishing sites used HTTPS. We expect the majority of phishing attempts to use HTTPS during 2021.

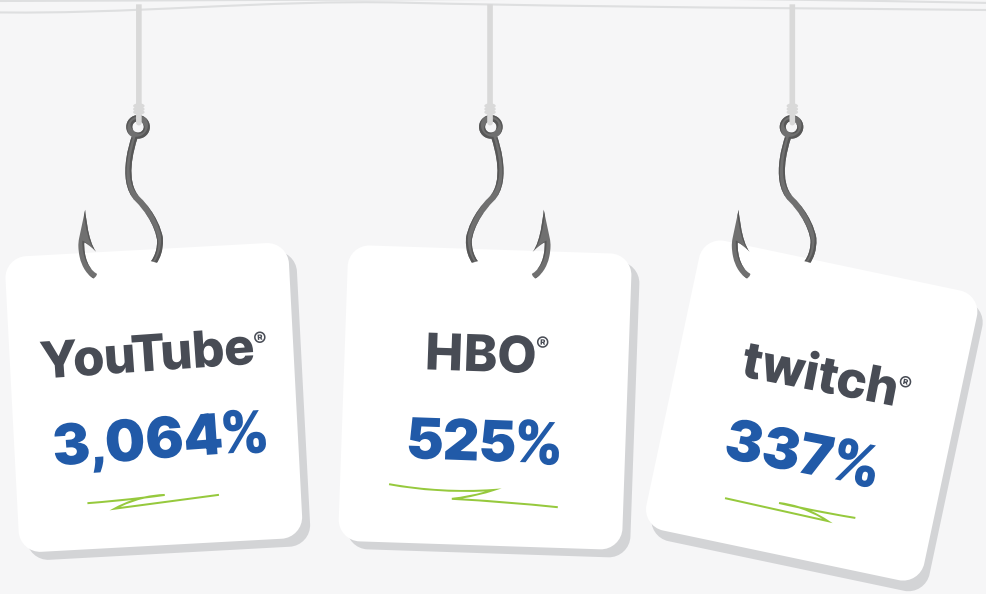
By the end of 2020,

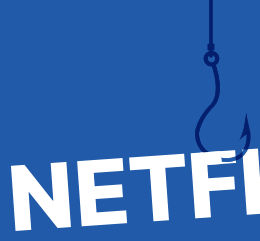
of phishing sites used HTTPS.



In spite of these rising figures, the use of HTTPS varies considerably based on the industry being targeted. It's most heavily used when spoofing cryptocurrency exchanges (70% of the time), ISPs (65%), and gaming (62%). Meanwhile, for other industries, like delivery services and social media, the rates are just over 30%. Education is the lowest sector at 26%.

In March 2020, these services saw massive increases in phishing activity





From March to July, phishing URLs targeting Netflix jumped 646%

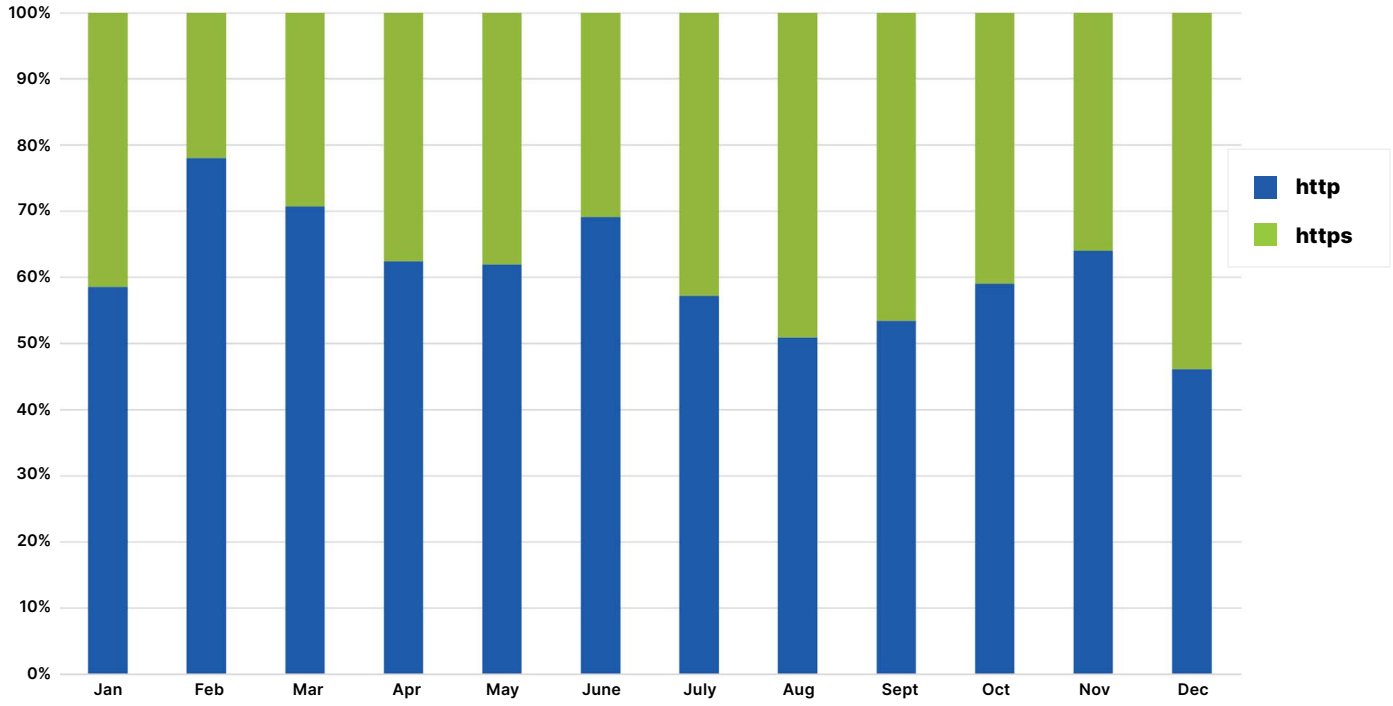


Figure 9: HTTP/S phishing attacks by month

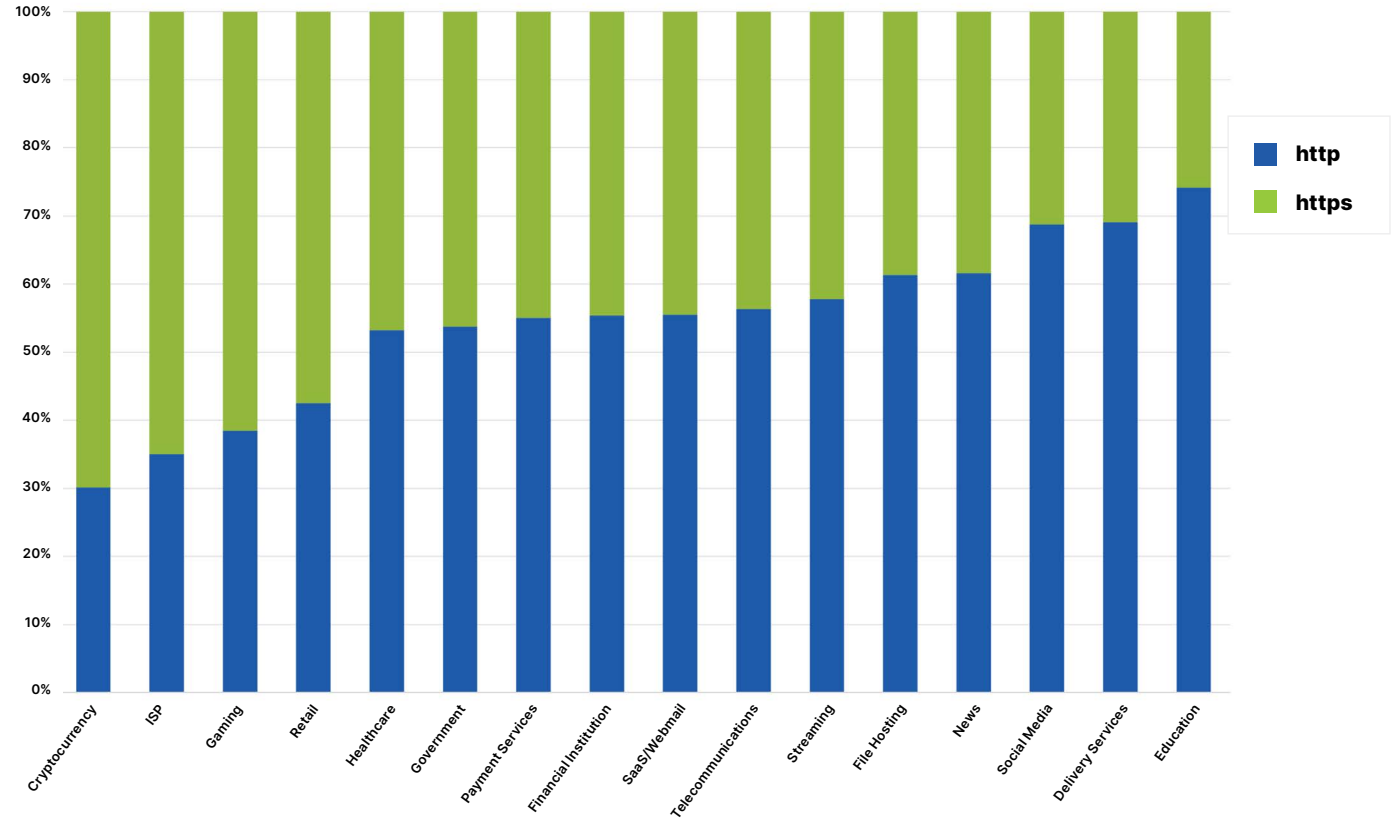


Figure 10: HTTP/S phishing sites by target industry

The Most Impersonated Companies

From year to year, we've learned to expect only minor shifts in the companies that are most often impersonated in phishing attacks. For example, 2018 and 2019 shared eight of the top 10 targets. Comparatively, 2020 was a year of flux; only six of the top 10 targets from 2019 made the 2020 list. Once again, these shifts were largely due to COVID-19.

The top 5 phishing targets were eBay, Apple, Microsoft, Facebook and Google.

2020 was the first year we've measured where brands like eBay and Amazon made the top 10, and eBay was the most targeted brand of the year. During the first half of the year, when there were widespread product shortages and huge increases in online purchasing, phishing attempts were 80% higher than in the second half of the year. It would make sense, then, that impersonating eBay, Amazon, and other online retailers, particularly those where resale by individuals is also common, would be a highly successful strategy.

For the first time, eBay was the most-impersonated brand in phishing attacks.

During the height of the product shortages, eBay was by far the most often impersonated. In February, a staggering 31.1% of all phishing attacks impersonated eBay. The percentage declined through July, then dropped sharply, reaching a paltry 0.4% in December.

> *It's not uncommon to see big shifts in the companies targeted by phishing campaigns based on how people are likely to shop and interact online. During the pandemic, people who would have shopped in person at malls and brick-and-mortar stores turned to resources like eBay and online retailers. Cybercriminals follow these trends. They took advantage of eBay early in the pandemic and then pivoted, as the year went on, to other trending topics.*
>
> **Grayson Milbourne | Security Intelligence Director**

Top 10 in 2019		Top 10 in 2020		Top 10 in 1H 2020		Top 10 in 2H 2020	
Facebook	12.8%	**eBay**	13.2%	eBay	18.8%	Microsoft	15.4%
Microsoft	10.6%	Apple	10.2%	Apple	13.3%	Facebook	11.9%
Apple	8.4%	Microsoft	9.5%	Steam	9.9%	Google	9.4%
Google	7.7%	Facebook	8.8%	Google	8.2%	Amazon	8.8%
PayPal	6.2%	Google	8.6%	Facebook	7.0%	Apple	4.8%
Dropbox	3.2%	**Steam**	7.9%	Yahoo	6.9%	Steam	4.3%
Chase	3.1%	Yahoo	5.4%	Microsoft	6.2%	PayPal	4.0%
Yahoo	2.9%	**Amazon**	4.7%	Netflix	2.5%	Netflix	4.0%
Adobe	2.8%	**Netflix**	3.0%	Amazon	2.4%	eBay	3.0%
Wells Fargo	2.8%	PayPal	3.0%	PayPal	2.4%	Instagram	3.0%

Figure 11: Companies most often impersonated in phishing attacks

Malicious IP Addresses

During 2020, the average number of malicious IPs decreased from 4.85 million to 4.18 million. While this roughly 15% decline is welcome, the sheer number of malicious IPs is still enormous. For the purposes of this report, we do not analyze all of the billions we track. Instead, we study the behavior of the top 50,000 malicious IPs, meaning the IP addresses associated with the highest number of observed malicious transactions during the year.

EXPERT INSIGHT

Webroot tracks IP addresses that carry out malicious activities so those activities can be blocked proactively. This includes monitoring which types of malicious activities each IP address is being used for at any given time.

Performing Multiple Bad Behaviors

Bad behaviors we look for fall into these categories: spam, Windows exploits, web attacks, botnets, scanners, phishing, proxy, mobile threats, and Tor proxies. We refer to these observed malicious activities as "convictions." Every single member of the top 50K had convictions in at least four of these categories, meaning they each exhibited different types of malicious activities and did so more than once. 19.1% were caught in five categories, and another 2.7% with six or more categories. During 2020, the top 50K generated 10.4 million convictions.

Malicious IP addresses are largely used for Windows exploits, spam, scanners and botnets.

The vast majority of the top 50K are being used for Windows exploits (99%), spam (99%), scanners (98.5%), and botnets (nearly 95%). Interestingly, while there are numerous malicious activities to be observed and classified, top 50K IP addresses performing bad behaviors beyond these categories, such as proxies, are relatively uncommon. It's important to note that these numbers don't indicate how often each behavior occurs; just because an IP address performs several bad behaviors doesn't mean that each one happens with the same frequency.

Webroot tracks exit nodes for Tor because they are often used to conceal the origin of attacks. While there are relatively few Tor exit nodes, the number of these nearly doubled in 2020, from roughly 1000 to 2000. This implies that the Tor network has grown and is being used more. Much of that growth may be due to COVID-19 causing people to work and conduct other activities from different locations, as well as increasing privacy concerns.

Frequency of Convictions

When we look at how often each type of conviction occurs, the most prevalent bad behavior by far is still spam. In 2019 it was 87.6% of all convictions, and in 2020 the rate is almost unchanged at 87.0%. Other common convictions include proxies (4.3% in 2019, 3.3% in 2020); scanners (2.9% in 2019, 3.2% in 2020); botnets (2.4% in 2019, 2.0% in 2020); and Windows exploits (1.1% in 2019, 2.2% in 2020).

The frequency of various convictions changed during 2020 in the following ways:

- Spam declined by 13% from January to December.
- Botnets plummeted in March and April, but climbed in May and June, returning to January levels.
- Windows exploits dropped in February and March, then increased in April and May.
- Scanners declined from January through August, falling by nearly 50% before rebounding somewhat.

We also saw many changes in the IP addresses that were causing the most convictions. Of the top 50K, 45.8% of them were convicted in two or three different months. We continue to see malicious IPs being used for bad behavior for a short period of time, then exhibiting benign behavior for a few months before being reused to perform attacks. This on-again, off-again pattern allows the addresses to drop off static allow/block lists, making them effective threats once more. Only 3.9% of the top 50K were convicted in all 12 months, but those 3.9% of the addresses created 25.8% of all the convictions.

The IP addresses in the top 50K come from 177 countries. However, 80% of the top 50K are hosted in 18 countries, and more than half of the top 50K are located in just five countries: China (15.4%), the United States (10.5%), Taiwan (10.3%), Vietnam (9.1%), and India (8.5%).

Because IP addresses can go from malicious to benign and back so quickly, it's not possible to keep a static allow/block list as updated as it must be to be effective. To prevent these threats, you need real-time intelligence that can assess risk at the exact moment an IP is encountered.

Cathy Yang |
Lead Product Manager

Some countries, such as the United States, were overachievers in terms of conviction rates. The U.S. had 10.5% of the IPs in the top 50K, but 19.5% of the convictions, meaning that the U.S. addresses produced nearly twice as many observed attacks as the average.

Just 6 countries accounted for half of the top 50k malicious IP convictions.

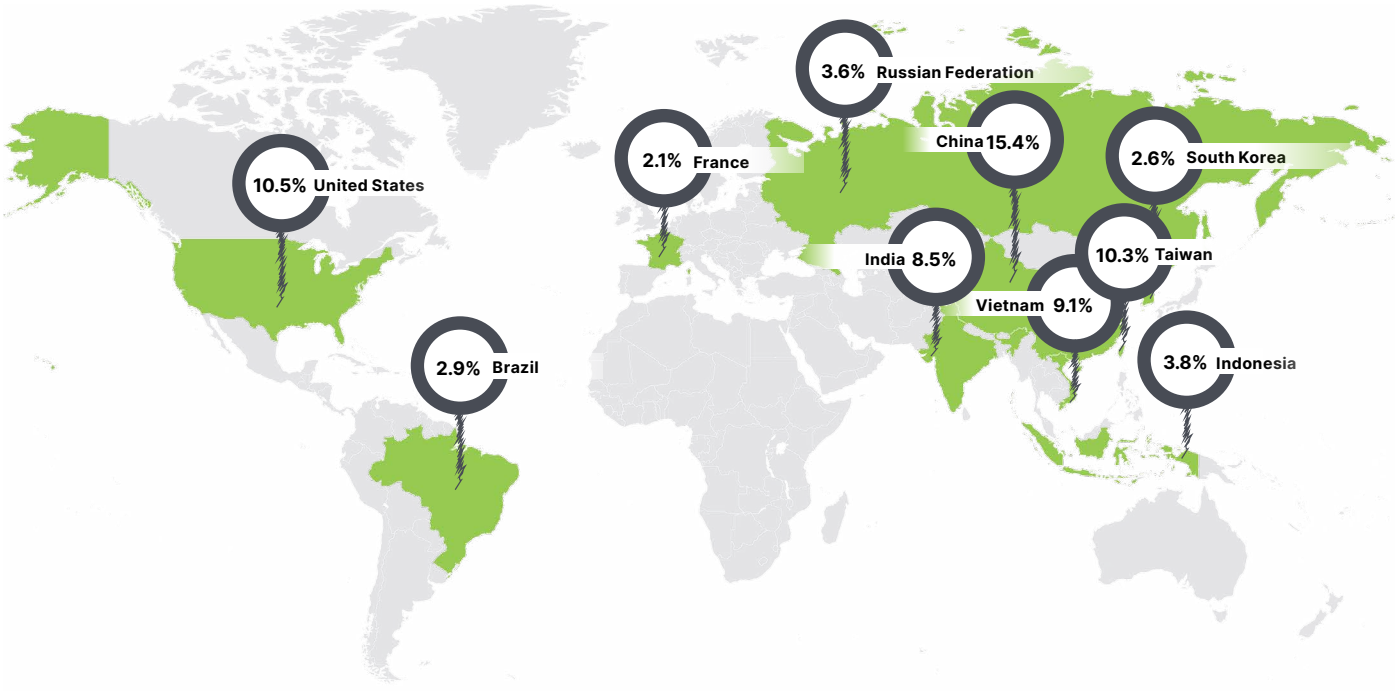


Figure 12: Countries of origin for top 50K malicious IPs

Harmful Mobile Apps

While not nearly as prevalent as Windows malware, Android™ malware is a real and growing threat, with hundreds of malicious apps having been pulled from Google Play. One example of common Android malware, the Joker Trojan, has been around since 2019, simulating legitimate apps to steal credit card information and banking credentials. Regularly throughout 2020, new variants of Joker and other info-stealing Trojans, such as MobOk, appeared in apps on the Play Store.

Hundreds of malicious Android apps were pulled from Google Play in 2020.

During 2020, 2.8% of Webroot-protected mobile users encountered an infection on their Android devices. This rate is down nearly 40% from 2019 levels. Of the threats detected on Android devices in 2020, Trojans and malware accounted for 95.9% of it, an increase from their 92.2 share in 2019.

Many of the recent malicious Android apps have masqueraded as COVID-19 contact tracing apps. Examples include CryCryptor, a form of ransomware that encrypts files but doesn't lock the device, and Banker and Spy Agent. These are not new malware; just older malware being repurposed.

Another trend in malicious Android apps is the increasing use of fleeceware. Fleeceware offers a legitimate service, but at an outrageous price. It usually starts with a short, free trial period, then tricks the user into paying a large monthly fee. One recent example is fleeceware in Minecraft Mod apps.

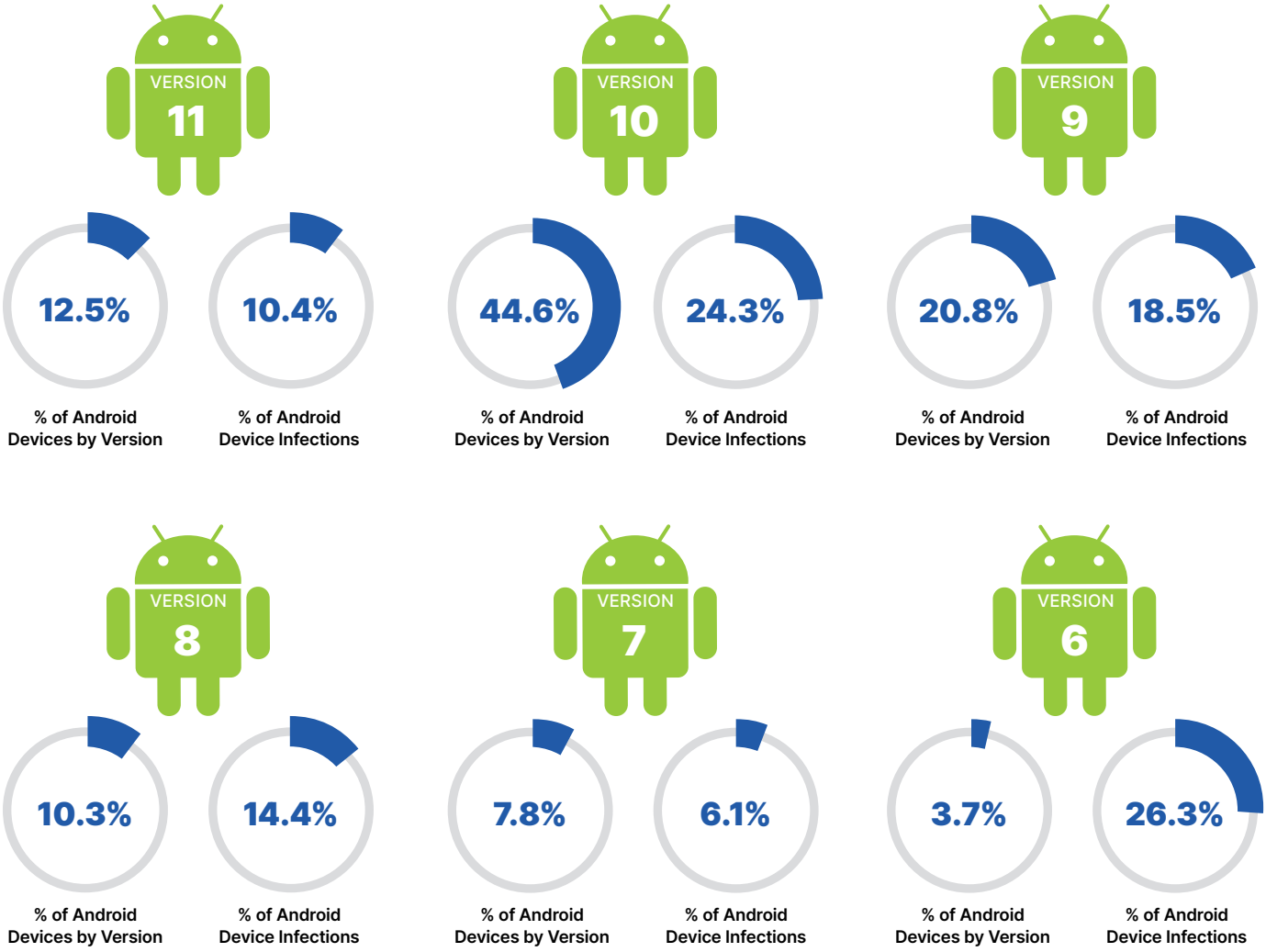
OS diversity remains a major challenge for Android devices, with over 42.8% of them using a version older than 10 or 11, including 20.8% on 9, 10.3% on 8, 7.8% on 7, and 3.7% on 6. All of these older OS versions have known vulnerabilities that aren't patched because the versions aren't supported anymore. This problem particularly affects populations who purchase older, used phones to save money.

Outdated operating systems accounted for nearly 90% of Android™ infections.

For each major Android version, we compared the percentage of devices running that version with the percentage of devices running that version which were infected at least once during the year. It's clear from this comparison that older Android devices are much more likely to get infected than newer ones. While only 3.7% of devices ran version 6, they had a whopping 26.3% of all the Android infections. Meanwhile, 44.6% of the devices ran version 10, but as a group they had fewer infections than the version 6 devices, which they outnumbered by more than ten to one.

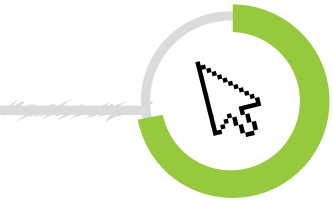
Malware for Android-based IoT devices is also increasing. For example, a new variant of the InterPlanetary Storm malware was found in 2020 that can attack Android devices, not just Linux and Windows devices. This new variant can run on ARM-based architectures, which are common with IoT devices, so it targets things like TVs running an Android operating system.

InterPlanetary Storm usually gains access by running a brute-force password guessing attack against the devices' SSH servers. Infected IoT devices join the InterPlanetary Storm botnet and are used to conduct attacks. This type of threat underscores the importance of securing all Android devices, even beyond smartphones and tablets.



Security Awareness Training

Companies needed layered defenses to stop threats, and the first layer of that defense should be security awareness training for users. We've highlighted several times throughout this threat report how a single user is often the entry point for a large incident. Preventive cybersecurity education, such as security awareness training, has been proven effective at reducing the success of phishing attacks and the rates of security incidents.



Regular phishing simulations can reduce click-through by up to 72%.

When organizations conduct security awareness campaigns for their users, these often include phishing simulations. Globally, the typical click rate for the first phishing simulation is 11%. Running a second phishing simulation shows an immediate improvement, with click rates just above 8%. As you run more phishing simulations over a period of several months, click rates will continue to fall, potentially dropping to 3 or 4%, which is a 72% reduction in phishing click-through.

It's unrealistic to expect users to stop falling for social engineering attacks altogether. But by reducing the click rate, you're making it harder for attackers to gain a foothold in your company. You're also increasing the chances that their failed attacks will be detected, and your technical controls will be able to stop additional attempts before they reach other users. You're strengthening the user layer of your layered defense.

The more phishing simulations you run, the less end users fall for them.

As we've already seen in this report, phishing attacks frequently take advantage of current events and trends, such as the COVID-19 pandemic and the U.S. elections. There are also all the typical phishing attacks, which include tactics like prompting you to update your personal information, warning you that a password needs to be changed, or informing you of a missed package delivery. Users need to be prepared to detect all phishing attempts, not just the run-of-the-mill ones. They also need to be aware of how sophisticated and targeted phishing attacks have become and must receive ongoing security awareness training to keep them up to date as phishing methods continue to evolve.

SPOTLIGHT: Business Email Compromise

Business email compromise (BEC) continues to plague organizations all over the world. This type of scam targets commercial, government, and nonprofit organizations by fraudulently representing a senior colleague, IT team member, or a trusted customer. The email typically contains instructions to send money (especially via wire transfer), provide credentials, or release client data. BEC relies heavily on the inherent trust of employees in their members of management, fellow employees, and valued customers.

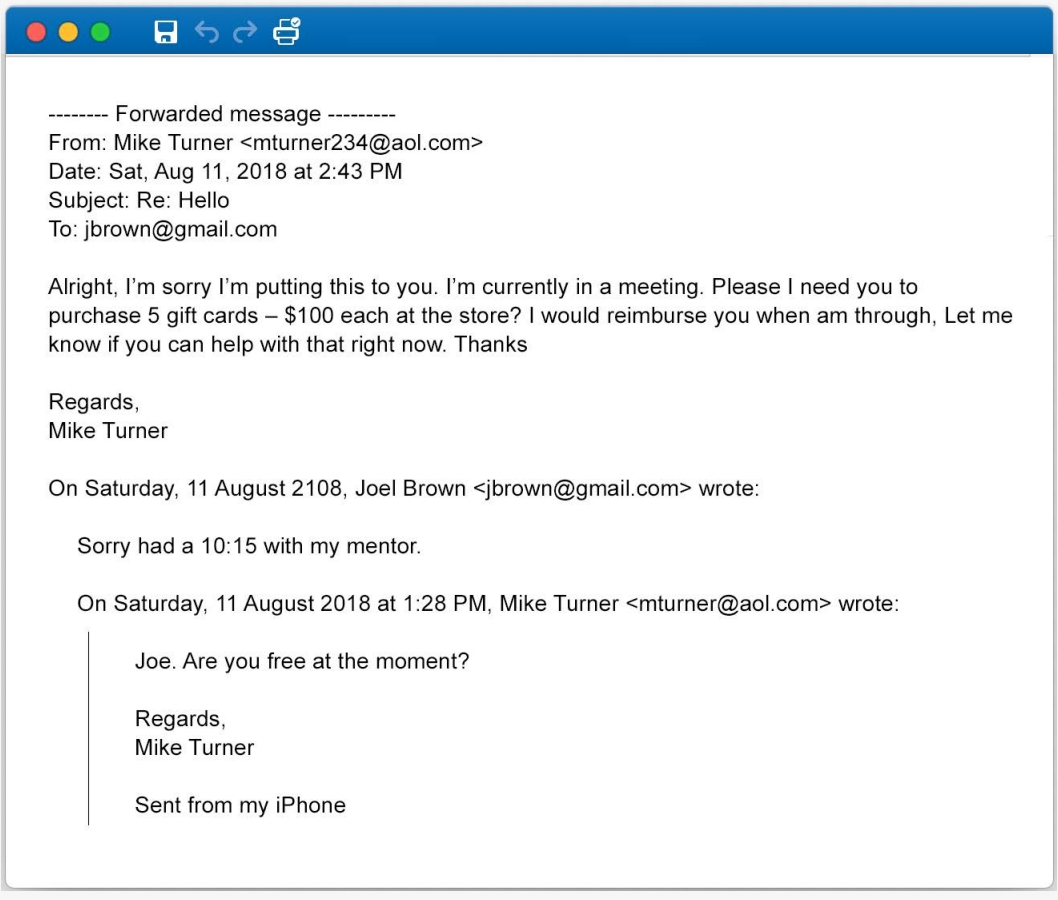
According to the FBI, the Internet Crime Complaint Center (IC3) received 19,369 complaints of business email compromise or email account compromise in 2020.[12]

The adjusted losses from BEC attacks reported to IC3 in 2020 were $1.8 billion USD.

Like phishing prevention, successfully preventing BEC involves a combination of robust training for end users and appropriately designed and publicized business policies around how to handle financial or technical requests.

Grayson Milbourne, Security Intelligence Director

Example of a BEC email



-------- Forwarded message ---------
From: Mike Turner <mturner234@aol.com>
Date: Sat, Aug 11, 2018 at 2:43 PM
Subject: Re: Hello
To: jbrown@gmail.com

Alright, I'm sorry I'm putting this to you. I'm currently in a meeting. Please I need you to purchase 5 gift cards – $100 each at the store? I would reimburse you when am through, Let me know if you can help with that right now. Thanks

Regards,
Mike Turner

On Saturday, 11 August 2108, Joel Brown <jbrown@gmail.com> wrote:

Sorry had a 10:15 with my mentor.

On Saturday, 11 August 2018 at 1:28 PM, Mike Turner <mturner@aol.com> wrote:

> Joe. Are you free at the moment?
>
> Regards,
> Mike Turner
>
> Sent from my iPhone

Predictions for the Year to Come

I think we'll see a ransom demand of $100 million or more, and I expect we'll experience an escalation in the code wars between nations.

Grayson Milbourne, Security Intelligence Director

Ransomware with data extortion will continue to be an issue, and the record-breaking ransoms we've seen in the last year will likely be surpassed as criminals keep upping the ante. I also think executable-based cryptojacking will explode as the amount of profit they make today will triple or more by the end of the year.

Tyler Moffitt, Sr. Threat Research Analyst

Supply chain and infrastructure attacks, such as the SolarWinds hack, will grow in prevalence.

David Dufour, VP, Software Engineering

Ransomware will become a top political concern. The damage caused and amount of money being made are too high to be ignored by world governments.

Briana Butler, Sr. Technical Project Manager

Criminals are still adapting to the work from home model and have yet to fully exploit the situation. I expect we'll see a whole host of new attacks on home-based employees involving home routers, IoT devices, social engineering and more.

Kelvin Murray, Sr. Threat Research Analyst

Conclusion

The COVID-19 pandemic brought unforeseeable surges in threat activity as cybercriminals capitalized on chaos and security gaps caused by the worldwide exodus to remote work. Particularly by targeting COVID-19 trackers, hospitals, vaccine production and distribution, videoconferencing and streaming applications, and other pandemic-related topics in their scams, criminals raised the stakes on what we expect would've been a record year regardless.

Although we can all take heart that 2020 is over and numerous security improvements have occurred, it's clear we haven't seen the last of the pandemic-related increases in cyberattacks. Our experts agree; as employees around the world continue to work from home, we're likely to see another banner year in terms of phishing, ransomware, malicious domains and more.

As we all continue adapting to new circumstances as they arise, our focus must remain on resilience.

After all, the most important lesson we can learn is not that we might fall; but that even if we fall, we can stand again. While we will likely never see an end to cybercriminals and their exploits, the more we understand their tactics, the more we can anticipate their movements, prepare, and protect. By training end users and individuals to avoid scams; preventing malware and network-layer attacks using threat intelligence and machine learning; and backing up all systems and files to ensure your data is always available where you need it, when you need it; we can all become more resilient against cybercriminal efforts, now and in the future.

[1] www.thematrixpoint.com/resources/articles/ccpa-fines-penalties-and-violations

[2] healthitsecurity.com/news/uhs-ransomware-attack-cost-67-million-in-recovery-lost-revenue

[3] www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

[4] www.nytimes.com/2020/10/03/technology/clinical-trials-ransomware-attack-drugmakers.html

[5] www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases

[6] www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

[7] www.coveware.com/blog/ransomware-marketplace-report-q4-2020

[8] www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/

[9] www.wired.com/story/garmin-ransomware-hack-warning/

[10] www.wired.com/story/garmin-ransomware-hack-warning/

[11] www.csoonline.com/article/3600457/trickbot-explained-a-multi-purpose-crimeware-tool-that-haunted-businesses-for-years.html

[12] www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf


RANSOMWARE
PHISHING
MALICIOUS IPS
HIGH-RISK URLS
HARMFUL MOBILE APPS
MALWARE

CARBONITE® + WEBROOT®

Backup ✪ Train ✪ Block ✪ Protect ✪ Restore

opentext™ companies

carbonite.com webroot.com

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.