

2022

**BrightCloud[®]
Threat Report**



Contents

Mid-Year Update	3
Foreword	5
Threat Intelligence Overview	6
Malware	5
Infected Consumer and Business PCs	5
Infection Rates by Number of Licenses	7
Windows 7 versus Windows 10	7
Infection Rates by Region	9
Infection Rates by Industry	11
Where Malware Hides	12
Spotlight: Cobalt Strike	12
Ransomware	13
Rising Ransom Costs.....	13
Ransomware Gangs.....	14
Ransomware Methods	15
Thwarting Ransomware Through Cyber Resilience.....	16
Spotlight: The Future of “Stealth” Ransomware Attacks	16
Cryptocurrency	17
High-Risk URLs	18
URL Classification	18
Geographic Distribution	19
Phishing Attacks	20
Phishing Volume	20
HTTP and HTTPS Usage	21
The Most Impersonated Companies.....	22
Malicious IP Addresses	24
Performing Multiple Bad Behaviors	24
Frequency of Convictions	25
Geographic Breakdown	26
Security Awareness Training	27
Conclusion	28

2022

BrightCloud® Threat Report

— MID-YEAR UPDATE —

Our mid-year update provides contextual insights from the 2022 BrightCloud® Threat Report. These updates highlight the most recent trends in malware and phishing within the first six months of 2022.

The threat intelligence presented in the mid-year update is guided by our threat research team that analyzes data from over 95 million real-world endpoints and sensors to deliver cutting-edge insights into the cyber threats affecting consumers and businesses across various industries.

Malware

Malware steadily continues to permeate PCs

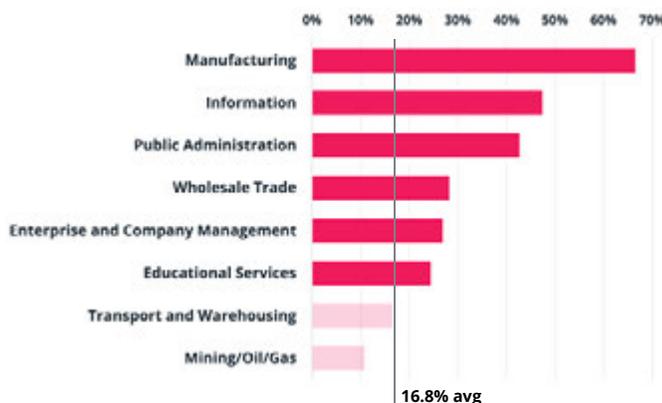
In the first six months of 2022, 89.3% of malware was unique to one PC, up from 86.3% in 2021. This slight uptick in the infection rate shows the evasive steps malware takes to ensure each attack variant is successful.

Infected consumer endpoints surpass their business counterparts

When it comes to endpoint infections, user behavior continues to be a leading factor, with 54.55% of consumer endpoints encountering more than one infection, which is higher than the business endpoint infection rate of 49.84%. Consumer endpoints also witnessed almost two times the infection rate for devices in comparison to business endpoints. This indicates that consumers are more likely to engage in riskier online behavior, increasing their likelihood of experiencing an infection.

Infection rates by industry

The Manufacturing vertical continues to experience the highest above-average infection rate, rising just over 12% since 2021 to 66.5%. The Information and Public Administration verticals also saw spikes in above average infection rates, 47.4% and 42.7%, respectively.



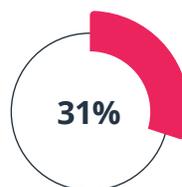
Infection rates by industry and deviation from average

Not only do infection rates vary by vertical, but they also differ by size of the business.

Within the first six months of 2022, we witnessed a 20% infection rate for businesses with 21-100 employees. This is 14% lower than what we saw in 2021. However, as the year progresses, we expect this rate to return to a similar level from the previous year.

Infection rates are also affected by operating systems.

Windows 11 adoption remains stagnant, only rising 4% for businesses and 15% for consumers within the first nine months of the release. Since the adoption of Windows 11 has been slow, these results highlight the importance of incorporating a layered security approach that includes DNS protection which helps reduce infection rates. Not only does DNS protection offer added privacy, but it also acts as a robust defense against malware.



fewer infections when endpoint and DNS protection are combined.



“Businesses operating in verticals with well above-average infection rates need to take note and ensure their security posture is properly prepared to handle potential threats. Cyber resilience is a great strategy to achieve this goal as it not only allows businesses to prepare for known and unknown attacks, but also recover (if an attack is successful) without significant effects on business operations.”

Grayson Milbourne, Security Intelligence Director

Phishing

Phishing is moving in one direction – up. Phishing activity has been exceptionally high in 2022. Nearly 20% of all phishing activity occurred in April. This is likely the result of tax season when cybercriminals prey on unsuspecting users looking for tax refunds.

HTTPS Use

Similar to what we witnessed in 2021, phishing sites continue to proliferate. So far this year, we've seen 46% of phishing sites use HTTPS, representing a 14% increase from 2021. This is steadily in line with the growth from 2020 (32%) and 24% in 2019.



“The most impersonated brands continue to be a favorite target by hackers. This means we need to become more vigilant and aware of what we click on, especially with these high-profile tech brands. There is just too much at risk and therefore a high return on investment for criminals. This means that business leaders need to prioritize ongoing security awareness training and phishing simulations with employees to ensure all users know how to spot and avoid becoming a victim of a phishing attack.”

Tyler Moffitt, Senior Security Analyst

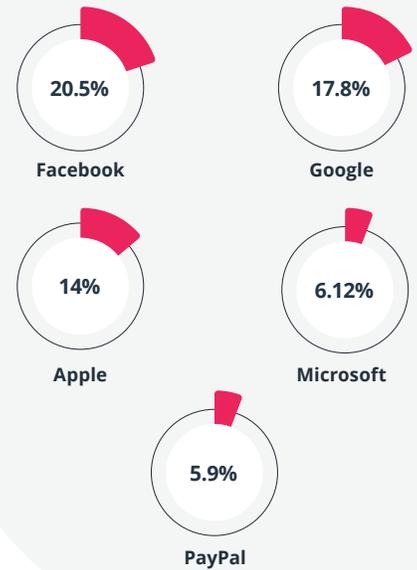
Conclusion

Combatting cyber threats like malware and phishing has become a must-have for businesses and consumers alike. Our latest insights reveal that consumers are more likely to experience an infection than their business counterparts, but that doesn't mean businesses should feel immune. Employees benefit from ongoing security awareness training to reduce the likelihood of successful attacks that can wreak havoc on a business network and affect continuity.

With phishing attacks steadily on the rise, cybercriminals continue to try and trick us into clicking on bad sites, exploiting household names like Microsoft, Google and Apple. Consumers should invest in a reliable antivirus solution that helps block malicious sites and offers trusted protection while shopping, banking and engaging online.

Phishing with your favorite brands as bait

Top 5 targeted brands in 2022



Increasing your cyber know-how and using trustworthy and dependable security solutions, like antivirus and DNS protection, helps enhance cyber resilience – the ability to recover files and keep businesses moving without experiencing downtime. Through our collective efforts, we continue to enhance security for businesses and consumers, so no matter what threats they face, businesses and consumers are prepared to tackle evolving threats as they emerge.

As expected, last year was marked by innovation from both cybercriminals and security professionals.



David Dufour
Vice President of Engineering & Cybersecurity

Foreword

In 2021, many cybersecurity incidents caused experts to shake their heads and left businesses, law enforcement agents and government officials in a state of constant catch-up.

Attacks on the supply chain? You bet. The takedown and resurrection of the Emotet botnet? Check. Enhancement of malware techniques to reduce the level of detection on devices? Absolutely. Massive infrastructure breaches that wreaked havoc from the United States to Belgium and beyond? They happened too.

Remote and hybrid working arrangements continued to evolve in the past year and will continue to alter how we work and interact with one another. These new realities opened easier and more lucrative avenues for bad actors to exploit. Phishing attacks across email, text and other communications platforms remain a common first step in breaches.

Malicious URLs have spiked. Browser-based cryptojacking may have practically disappeared, but cryptomining malware is becoming more mainstream. Cybercriminals remain hard at work looking for ways to compromise our data and personal information.

Though cybercriminals made headway in their stealth approaches to compromise organizations, cybersecurity analysts and threat researchers continued to pinpoint and prevent the proliferation of risks. An impossible challenge at times, but one that remains essential to address across all industries and sectors.

Individuals and businesses will never be fully immune. Small to medium-sized businesses (SMBs) remain particularly vulnerable to ransomware breaches. Though ransomware payments soared in 2021, countries banded together to thwart the efforts of ransomware

gangs like REvil. Top brands like Apple, Microsoft and Google continue to be used as phishing bait to lure unsuspecting users. The manufacturing sector remains a prime target for attackers to focus their efforts.

In this year's BrightCloud® Threat Report, we delve into the developments affecting businesses large and small and what these changes mean for businesses and individuals. Through our in-depth analysis, we provide insights, trend analyses and predictions for what lies ahead this year.

We hope our report can empower your defense and recovery strategies, and the information it contains helps keep you safe in the year ahead.

Threat Intelligence Overview

The threat intelligence, trends and details presented in the 2022 BrightCloud® Threat Report are based on data continuously and automatically captured by the BrightCloud® Platform, which is the proprietary machine learning-based architecture that powers all of our Webroot protection and BrightCloud services. This data comes from over 95 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.



95M+
Real-world sensors



78M+
End users protected through technology partners



1B+
Domains categorized



43B+
URLs evaluated



4.39B+
IPs
all IPv4 and in-use IPv6



38B+
File behavior records



37M+
Active mobile apps

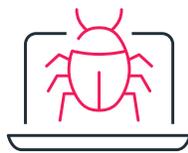


Malware

The number of malware files reaching Webroot-protected Windows endpoints dropped 58% from 2020 to 2021. That's an incredible shift. Throughout this section and other sections of the report, we'll look at several reasons that together led to this massive decrease, including the disruption of Emotet, DarkSide and REvil cybercrime operations, the continuing migration from Windows 7 to newer Windows versions and improvements to upstream malware detection capabilities by our BrightCloud technology.

Another major reason for the reduction hinges on attackers' behavior. They are increasingly evading detection through living off the land binaries—benign applications already present on endpoints—instead of transferring their own malware applications to endpoints. But don't think for a second that malware isn't still a huge threat. In 2021, Webroot-protected Windows endpoints witnessed over one million new malware and Windows application files per day on average.

We also tracked the percentage of detected Windows malware that was only witnessed on a single PC worldwide. This year, 86.3% of malware was unique to one PC. This is nearly identical to previous years—86.1% in 2020 and 86.2% in 2019—implying consistency in the techniques attackers use to evade detection. It also underscores the importance of using antivirus technologies with per-endpoint telemetry. [Endpoint Security Threat Report](#)



This year, 86.3% of malware was unique to one PC

Infected Consumer and Business PCs

Another trend continuing from previous years was a decrease in infection rates for consumer and business PCs. In 2019, 12.6% of consumer PCs and 7.8% of business PCs experienced at least one malware infection. In 2020, infection rates fell to 8.5% for consumer PCs and 4.7% for business PCs. In 2021, we witnessed an even sharper decline, down to 3.5% for consumer PCs and 2.1% for business PCs.

Lower infection rates are positive developments, but the rate for consumer PCs is still nearly double the rate of business PCs. This highlights a pressing need for organizations to protect remote employees who are using their own PCs for work purposes.

One reason for decreased infections is more widespread use of layered defenses. More prevention is taking place, resulting in less malware reaching the endpoint. Another compelling reason is continued migration from Windows 7 to Windows 10 and Windows 11.

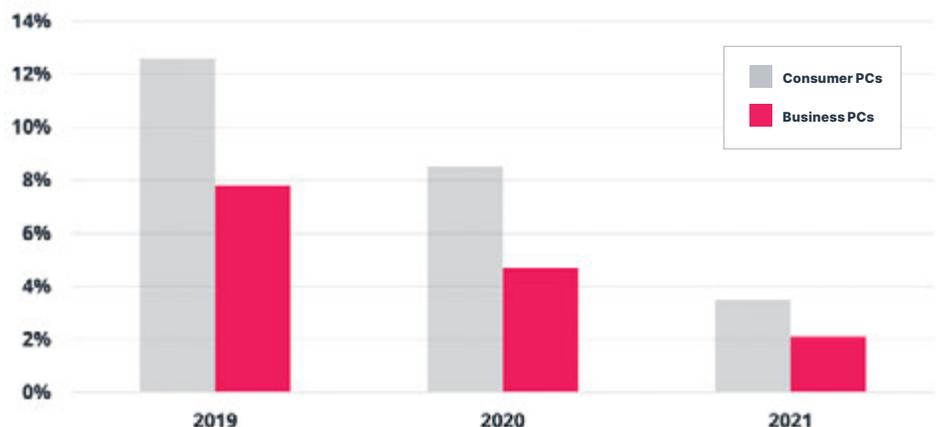


Figure 1: Infection rates for business and consumer PCs

Improved security features available on these newer versions make infections less likely.

As threats become more widely recognized, more proactive and offensive measures against organized cybercrime have begun to take shape.

In addition to examining infection rates, we also looked at reinfection rates—that is, how many times a PC is infected within the year. Among infected consumer PCs, 53% were infected more than once, and 19% were infected more than five times. For infected business PCs, 45% had multiple infections, and 12% were infected more than five times. These percentages are roughly the same as those from 2020. These reinfection rates emphasize the importance of user education, especially after a compromise occurs.

Among infected consumer PCs



were infected more than once, and



were infected more than five times

Infection Rates by Number of Licenses

New to this year's report is an analysis of infection rates by the number of licensed PCs a business has. Only 8.3% of the smallest organizations, those with 20 or fewer licensed PCs, experienced an infection on any of their PCs this year. On average six PCs were involved in an infection. When we look at medium-size organizations (21 to 100 licensed PCs), the infection rate sharply increased to 34.1% of organizations, affecting nine PCs on average. Infection rates were

Business Size by # of Licensed PCs	% of Businesses with Infections	Avg. Infections per Infected Business
 1-20: Small	8.3%	6
 21-100: Medium	34.1%	9
 101-500: Large	65.1%	23
 501: Very Large	89.7%	86

Figure 2: PC infection rates by business size

even higher for organizations with 101 to 500 licensed PCs—65.1% of organizations affected—and at 89.7% for organizations with over 500 licensed PCs. As you would expect, as your business grows, so does your risk of infection.

What's even more compelling are the differences in the relative impact of infections to smaller businesses versus larger ones. When a small business experiences an infection, it typically hits a much larger percentage of that business's PCs compared to an infection at a large business. Though the infection rate is much lower for small businesses, the impact of an infection is likely to be greater. The lack of IT and highly trained cybersecurity professionals to support these small businesses leaves them in a vulnerable position.

Windows 7 versus Windows 10

We've monitored the infection rates for Windows 7 and Windows 10 PCs for several years, and Windows 7 has consistently experienced significantly higher infection rates than Windows 10. This year the trend continues. In 2021, Windows 7 PCs experienced 0.06 infections per PC, and Windows 10 PCs averaged only 0.03 infections per PC, half the Windows 7 rate.

With a dwindling number of Windows 7 devices in use, the number of infections involving Windows 7 should continue to drop over time. Microsoft stopped releasing patches for Windows 7 in early 2020, when Windows 7 hit its end-of-life. At that time, around 16% of all PCs were still running Windows 7. By the end of 2021, that number had plummeted to 5%, with 86% of all PCs using Windows 10. We're also starting to see Windows 11 systems coming online, so we expect Windows 7 numbers to continue to decline.

We witnessed more dramatic differences between Windows 7 and Windows 10 when we split out consumer and business PCs. First, we saw that businesses continue to lag behind consumers in moving away from Windows 7, with 6% of business PCs but only 4% of consumer PCs still on Windows 7 at the end of 2021. Windows 10 is overwhelmingly the favorite Windows version, with 88% of consumer PCs running Windows 10 compared to 84% of business PCs.

We also witnessed consumer PCs continue to have much higher infection rates than their business PC counterparts. Consumer PCs running Windows 7 have 0.11 infections per PC,



Figure 3: Infection rates by operating system across business and consumer PCs

over three times the 0.03 rate of business PCs running Windows 7. For Windows 10, the difference between consumer and business PCs is less dramatic—0.04 versus 0.02. All of these rates are still significant improvements over the rates from just a few years ago. These findings indicate improvements in protecting endpoints from malware, but consumer PCs are clearly still at much greater risk than business PCs.

Infection Rates by Region

Windows 10 and Windows 7 PC infection rates also vary greatly depending on where in the world the PCs are located. Separating the infection rates by geographic region showcases discrepancies among regions. Japan and the UK have Windows infection rates less than one-tenth of the Middle East's. This discrepancy has also widened since 2020, when Japan's rate was approximately one-seventh of the Middle East's.

The four regions with the lowest rates—Japan, the UK, North America and Australia and New Zealand—saw their rates drop by an average of 51% from 2020 to 2021, to a collective 1.4%. In contrast, the other regions only experienced a 33% drop year-over-year to an average of 9.2%.

Splitting these rates out for Windows 7 and Windows 10 paints a somewhat muddled picture. In the five regions with the highest infection rates, 16.7% of their consumer PCs and 14.3% of their business PCs are still running Windows 7, but in Japan, which had an infection rate of 1.2%, a whopping 21.7% of their consumer PCs and 9.2% of their business PCs are running Windows 7! So, while regions with higher percentages of Windows 7 PCs tend to have higher infection rates, Japan is a glaring outlier.

Across all regions, Windows 10 adoption rose 11.2% from 2020 to 2021. All regions except North America had increases of at least 9%, while North America's counts stayed relatively steady. What's even more impressive is the massive migration from Windows 7 across all regions, from a 23.5% drop in the Middle East and a 26.5% drop in Asia to a 49.0% drop in North America and a 50.1% drop in the UK.

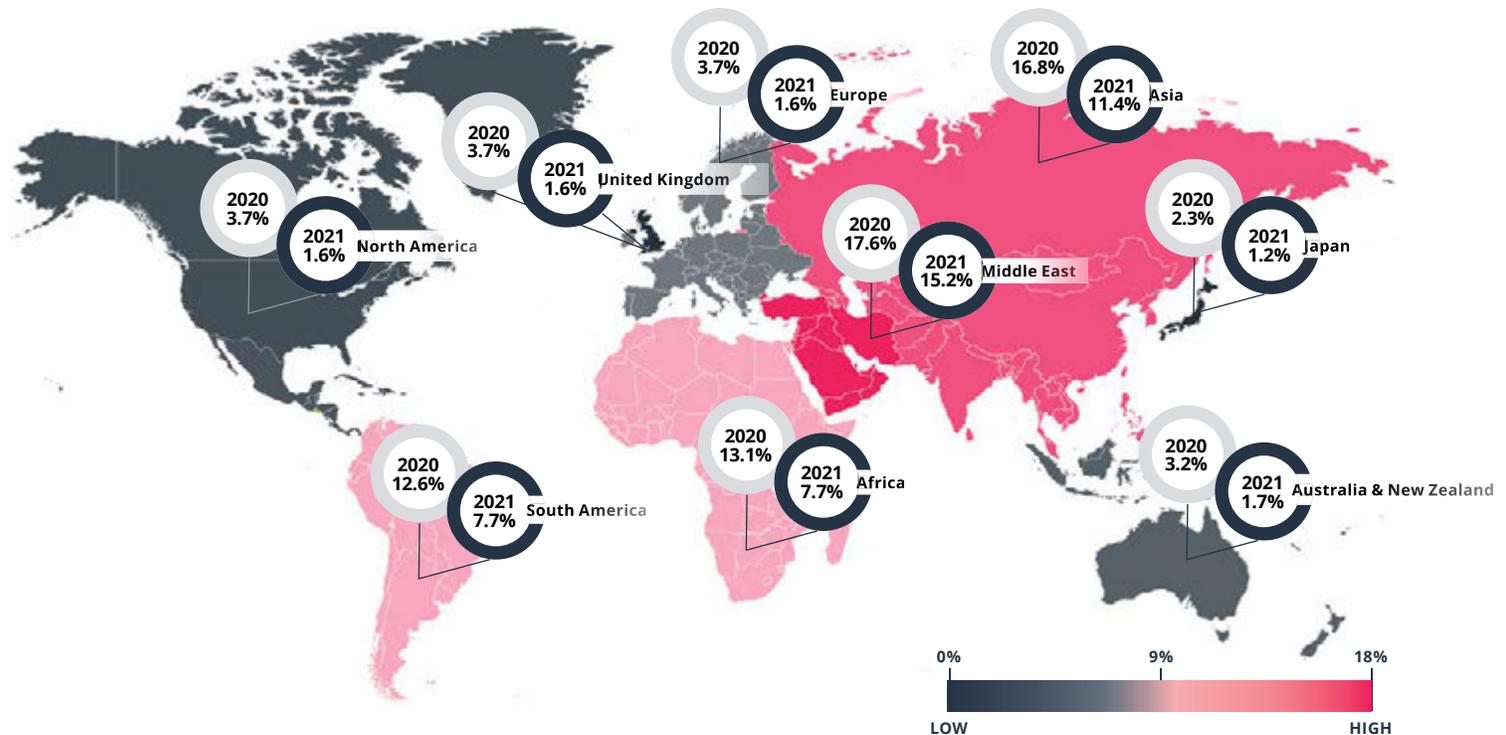


Figure 4: PC infection rates by region

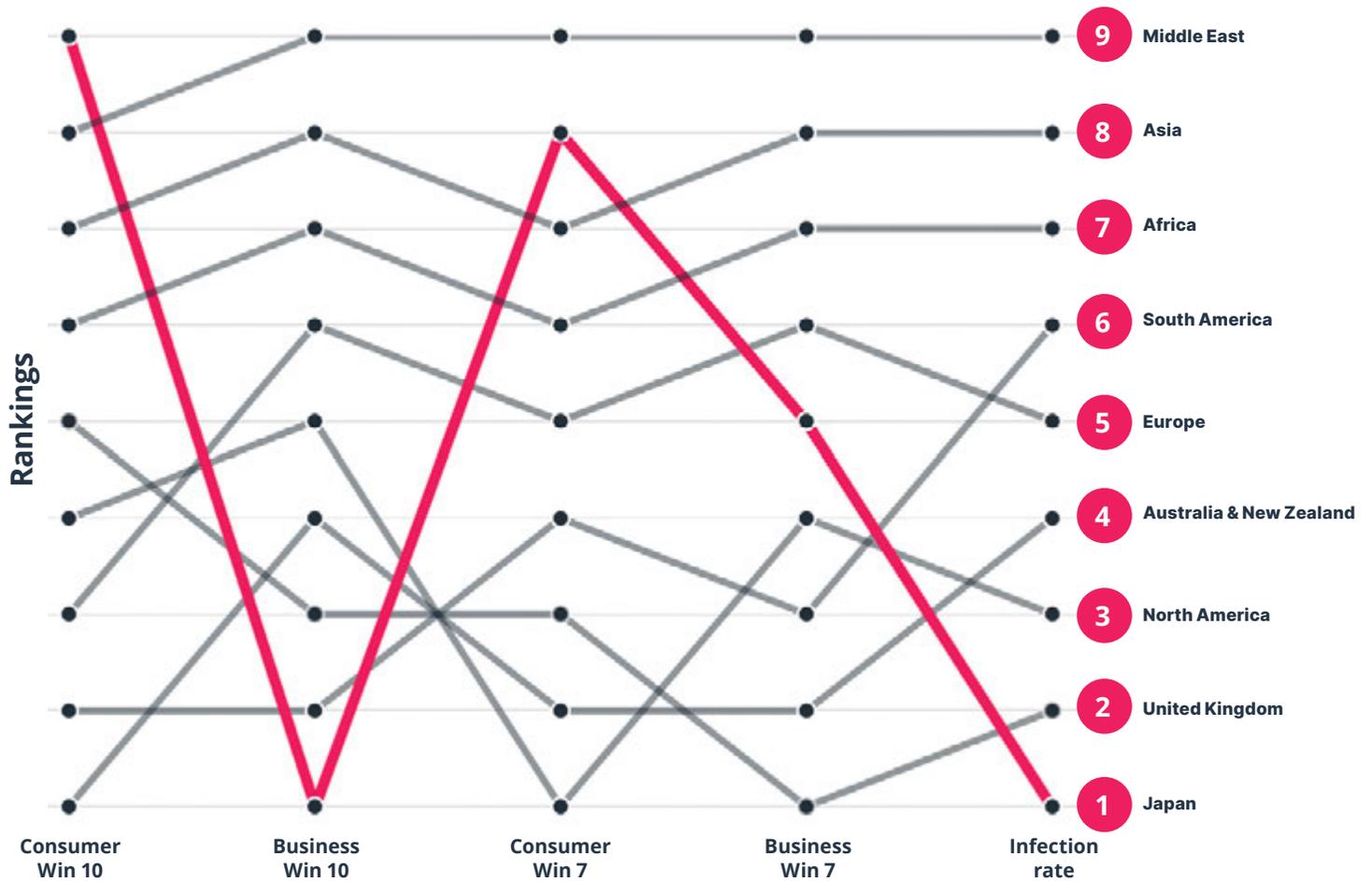
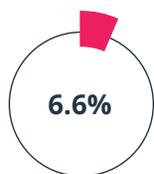


Figure 5: Rankings of consumer and business PC adoption of Windows 7 and 10 with overall infection rates

Increase in Windows 10 usage



worldwide for business PCs



worldwide for consumer PCs

Last year's shifts from Windows 7 to Windows 10 were, in most regions, due primarily to business PCs.

The increase in Windows 10 usage was 13.8% worldwide for business PCs, but only 6.6% for consumer PCs. Similarly, the drop in Windows 7 usage was mainly from business PCs, which fell by 42.1% year-to-year, with consumer PCs showing a slightly less impressive drop of 29.3%.

Another way to look at the data is to rank each of the nine regions from 1 (best) to 9 (worst) in terms of their consumer and business PC adoption of Windows 7 and Windows 10, as well as their infection rate. Ranking the data by region illustrates the difference in the numbers for Japan compared to the rest of the world. Japan ranks first in Windows

10 adoption by businesses and last in Windows 10 adoption for consumers.

For remaining Windows 7 usage, it is average for business PCs compared to other regions and next-to-worst for consumer PCs. But somehow it has the lowest overall infection rate. Most countries have fairly steady rankings across the categories, including their infection rates.

Likely explanations for the differences in rates among regions include the effectiveness of layered defenses that prevent malware from reaching endpoints in the first place and the effectiveness of security awareness training that helps prevent users from being tricked by social engineering into unwittingly infecting their own PCs.

Infection Rates by Industry

Nearly 40% of our business customers provide data on their industry vertical. Figure 6 illustrates the average percentage of businesses with at least one infection last year for each industry vertical. The gray line indicates the average infection rate across these verticals, 16.8%. Based on this data, the verticals with the highest rates were Manufacturing (54% above average), Public Administration (41% above average) and Information (37% above average), followed by Wholesale Trade and Educational Services. Four of these five verticals were also in the top five in 2020.

These numbers shift each year, and it is not surprising that Manufacturing was the industry most likely to be infected compared to all others this year; it was third highest the year before. We expect to see more attacks targeting manufacturers in 2022, since they may be willing to pay ransoms in order to avoid causing supply chain disruptions.

Trusted software distribution attacks were arguably the biggest cybersecurity story of 2021. These affected SolarWinds, Kaseya and Log4j, to name a few, making headlines around the world. Cybercriminals love these attacks because they can breach the software once and then sit back

and watch as that breached software is sent to thousands or millions of systems. With many companies including third-party software in their products or services, it's to be expected that third-party software will continue to be heavily targeted by attackers.

At the other end of the industry spectrum, we saw several verticals with infection rates significantly below the average, including Accommodation and Food Services (35% below average), Health Care and Social Assistance (31% below), Real Estate and Rental and Leasing (27% below), Finance and Insurance (22% below) and Agriculture, Forestry, Fishing and Hunting (16% below).

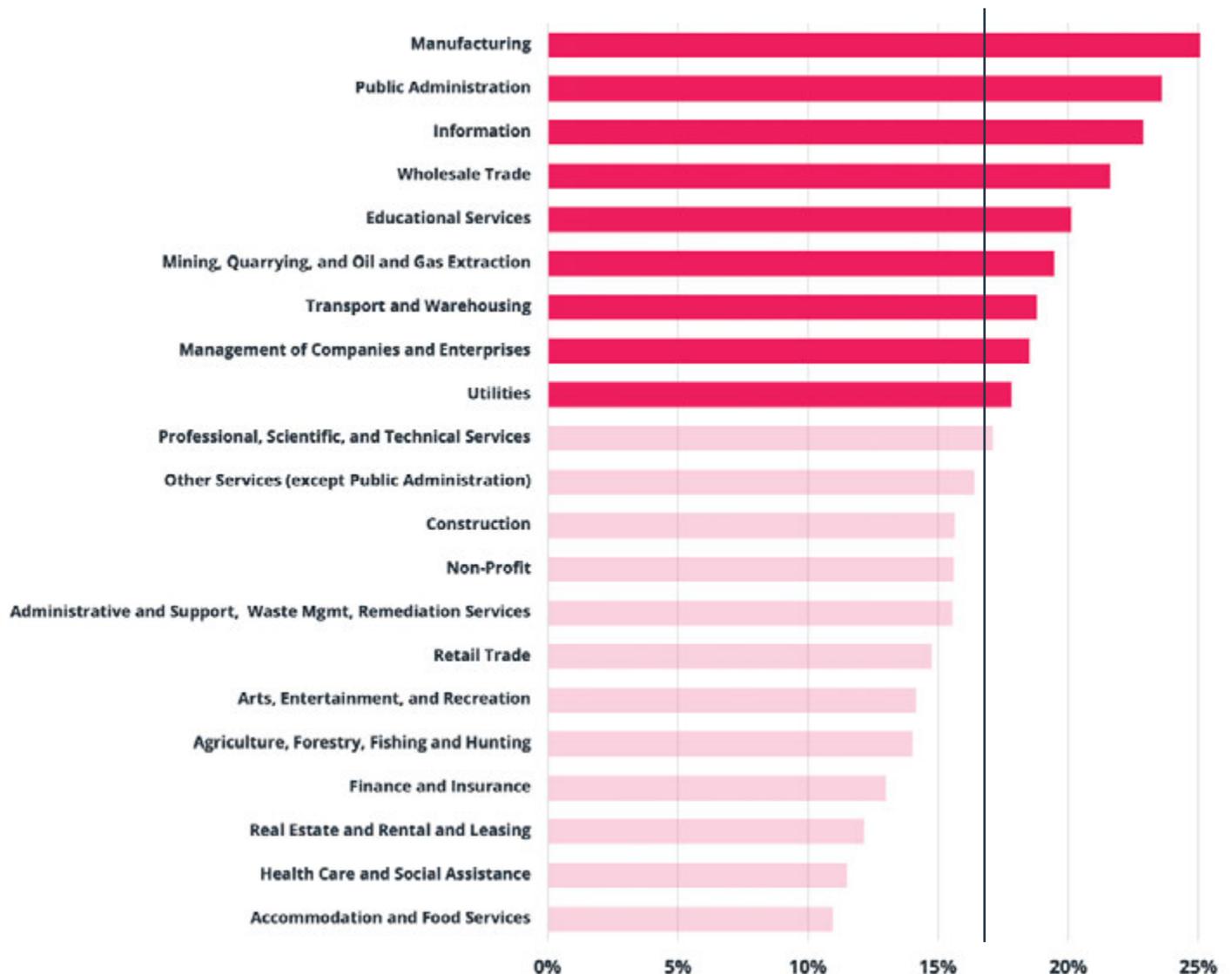


Figure 6: Infection rates by industry and deviation from average

Where Malware Hides

We track where Windows malware hides. It tends to use just a few locations, even though there are many possible places within which it can lurk. Malware tends to hide in these locations because they're accessible and there are many other applications or files stored within them.

In 2020, 83% of malware infections used one of four paths: %temp% (28.4%), %appdata% (26.1%), %cache% (19.7%) or %desktop% (9.0%). The 2021 numbers are similar, with 83% of infections using the same four paths, but with a big shift toward %temp% (now 37.8%, a 33% increase) and %desktop% (now 12.6%, a 40% increase) and away from %appdata% (now 14.2%, a 46% decrease). The year-to-year change in %cache% (now 18.7%, a 5% decrease) was relatively small in comparison to the others.

We also saw significant differences in where malware hides on consumer versus business PCs. The top four locations for consumer PCs were the same four as those on all Windows PCs, with similar percentages: %temp% (33.8%), %cache% (21.9%), %desktop% (15.0%) and %appdata% (12.5%). The only noteworthy difference from the 2020 locations is that the use of %desktop% has become much more likely and the use of %appdata% has dropped sharply.

On business PCs, the top four locations look a bit different from consumer PCs: %temp% (50.9%), %appdata% (19.7%), %cache% (8.4%) and %windir% (5.6%).

Of all the places where malware could hide on business PCs, it uses %temp% more than half the time!

And this is a striking change from 2020, where only 21.7% of business PC malware used %temp%. In 2020 the top location was %appdata% at 41.0%, which has dropped by over half from year-to-year. Interestingly, the 2019 percentages for %temp% and %appdata% were much closer to 2021 numbers—54.4% and 16.7%, respectively.

Spotlight: Cobalt Strike

It seems like the most notorious attacks in 2021 all utilized the same tool: Cobalt Strike. Cobalt Strike was originally intended to be used by white hats and red teams for penetration testing purposes. It's a highly sophisticated collection of hacking tools in a single package that's easy to use and lowers the bar in terms of necessary technical knowledge needed compared to most other tools. It's designed to use these hacking tools to conceal itself, identify vulnerabilities, spread laterally and perform privilege escalation and credential and hash harvesting. It also leaves little or no trace behind within the systems it infiltrates.

These characteristics made Cobalt Strike irresistible to attackers, who have made cracked versions of Cobalt Strike available and created their own versions to sell to affiliates. During 2021, a lot of effort focused on enhancing attackers' versions. A Linux port was even found in the wild in mid-2021.

Attackers especially love using Cobalt Strike to remotely access and control endpoints, to distribute and control ransomware and to do other activities requiring command and control capabilities. It's safe to assume that we'll see attackers continue to make heavy use of Cobalt Strike during 2022.



"Despite the improvement in infection rates this year, consumer PCs continue to have higher rates of infection in comparison to business PCs. With the introduction of Windows 11, bad actors won't think twice about engaging in new and dangerous exploits that leverage new features not previously available."

Grayson Milbourne, Security Intelligence Director



Ransomware

Ransomware continues to be the biggest cyber threat facing SMBs. The primary vector for infecting SMBs is Remote Desktop Protocol (RDP), followed by email phishing. During 2021, 82% of ransomware attacks targeted organizations with less than 1,000 employees. The smallest organizations, with 100 employees or less, comprised 44% of the ransomware victims. And 84% of all ransomware attacks now include threats of data breaches, a modest increase from a year before.ⁱ

In 2021, most ransomware attacks left many computers unusable and stole sensitive data, with the attackers threatening to disclose the data unless the organization paid a cryptocurrency ransom in time. Before the ransomware as a service (RaaS) model became commonplace, organizations could recover their data and avoid paying a ransom.

Now there's a tougher choice facing victimized organizations. Do they refuse to pay the ransom and instead focus on remediation? Or do they pay the ransom and hope attackers keep their word? And even if the attackers do keep their word, will the organization, as required by data privacy laws, still disclose the data breach that already happened when the attackers gained access to the data?

Attackers are also being more selective in the organizations they target. That's bad news for SMBs. Attackers don't want to pursue another high-profile victim,

like Colonial Pipeline, because such attacks are finally being answered with disruption and arrests.ⁱⁱ

So they're increasingly going after smaller organizations because it's less risky. They're also demanding—and getting—higher and higher ransom payments.ⁱⁱⁱ The increase in ransoms is likely due in part to the declining value of the U.S. dollar and in part to the rising fines for General Data Protection Regulation (GDPR) violations.

No one knows what's going to happen in 2022. Will more aggressive prosecution of ransomware gangs finally lead to a downturn in phishing?

Will ransomware gangs come up with more innovative ways to coerce targets into paying even higher ransoms?

Let's take a closer look at the trends during 2021 and what this means for the year ahead.

Rising Ransom Costs

Average ransom payments increased at an astonishing rate in 2021, far faster than previous years. At the end of 2018, the average ransom payment was only \$6,733.^{iv} A year later, it was \$84,116,^v and at the end of 2020 the average was \$154,108.^{vi} That's an increase of roughly \$73,500 a year. The year-end average for 2021 more than doubled the 2020 average, hitting \$322,168.

Median ransoms have also more than doubled since 2020, increasing from \$49,450 to \$117,116.^{vii} We expect ransom costs to continue increasing in 2022, based on the trends of the past few years combined with rising inflation.

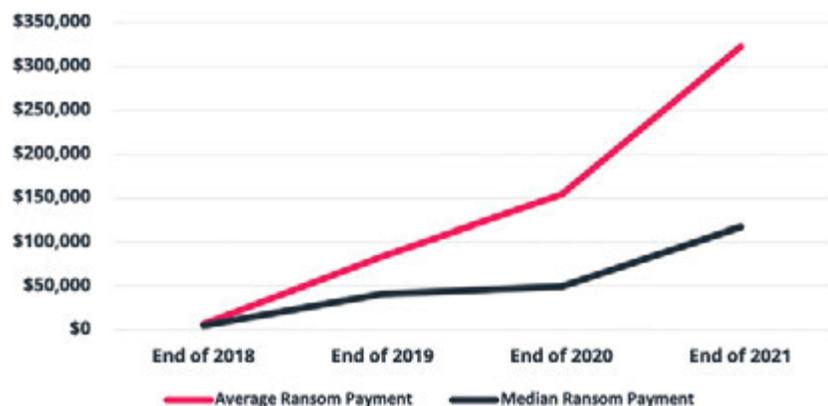


Figure 7: Average and median ransom payments as of year end

In 2021, we saw the largest ransom demands ever. Here are a few examples:



\$70M RANSOM

In a high-profile supply chain attack, the REvil ransomware gang compromised Kaseya's IT management software. They then used that compromise to infect not only companies using that software, but also the customers of those companies, estimated at 800 to 1,500 SMBs. REvil demanded \$70 million in ransom.^{viii}



\$50M RANSOM

Another REvil target was Quanta Computer. REvil claimed that they had stolen blueprints for computer components that Quanta manufactured for Apple. To show proof of their claim, they published some files. They demanded \$50 million in ransom, but not from Quanta—from Apple. REvil also said the ransom would increase to \$100 million if Apple didn't provide payment in a matter of days.^{ix}



\$40M RANSOM

CNA Financial was infected by the Phoenix ransomware gang. It took down CNA websites, email and other systems. Phoenix also compromised a large profile of sensitive employee and customer information. After two weeks of recovery efforts, CNA decided to pay \$40 million in ransom to regain access to their systems and data.^x

Not surprisingly, insurance companies are raising their rates for cyber insurance policies. They're also making it tougher to get cyber insurance. For instance, insurance companies may require a series of technical controls to be implemented. That may be particularly challenging for SMBs because of the complexity and cost of such controls.^{xi}

As a result, many organizations are shifting from relying on cyber insurance policies to increasing the strength of their layered defenses in order to be more resilient against ransomware attacks.

Ransomware Gangs

2021 was the year law enforcement agencies started striking back against ransomware gangs. At the beginning of 2022, Russian authorities arrested members of the REvil gang and seized their computers and other assets.^{xii} This is noteworthy for several reasons, including the unprecedented cooperation between U.S. and Russian

authorities and a ransomware gang's members being arrested instead of their affiliates. The REvil shutdown represents a positive sign for 2022 as law enforcement agencies develop more robust capabilities to arrest, prosecute and incarcerate ransomware gangs.

That's the good news. Unfortunately, RaaS business model is thriving. Ransomware gangs such as DarkSide and REvil were taken down, only to resurface later in a reduced or re-branded form. There's simply so much money to be made from ransomware that there are always others willing to risk imprisonment for a lucrative payday. The RaaS model also reduces the risk for ransomware coders and leaders at the top of the ransomware gangs. Those individuals still aren't being caught or prosecuted, only the ransomware distributors and affiliates lower in the hierarchy.

But there's hope: in November 2021, the U.S. State Department offered up to \$10 million for information about those at the top of the DarkSide ransomware gang.^{xiii}

Ransomware gangs are also using new tactics to coerce victims into paying ransoms. For example, if stolen data includes personal information, an organization may be required to report it and pay fines under the GDPR and other laws and regulations. Ransomware gangs are using this in their extortion tactics to victims, telling them that if they don't pay the ransom, they'll be the next on the list of GDPR violators, which will damage their reputation. So instead of the GDPR being a mechanism to pressure organizations into improving their security practices, the GDPR is being used to encourage organizations to pay ransoms.

When victims pay ransoms, it encourages attackers to continue using ransomware and to raise their ransom demands. Many governments are facing increasing pressure to either require organizations to disclose all ransomware payments or to make it illegal to pay ransoms, in hopes that this would reduce the number of ransoms that are paid. That, in turn, would hopefully make ransomware a less profitable business and cause a downturn in ransomware activity.^{xiv}

The GDPR at Article 33 requires that, in the event of a personal data breach, data controllers should notify the appropriate supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.



This is the rebranded "Grief" AKA Doppelpaymer/BitPaymer ransomware groups extortion page on the dark web. Here they use GDPR code and marketing materials to pressure victims into paying to keep the breach quiet

It seems inevitable, however, that some organizations will still pay ransoms to expedite their recoveries and avoid bad publicity, even if paying ransoms becomes illegal. It would be difficult at best for governments to identify violations of such laws.

Government agencies are also working to improve cybersecurity information sharing. For example, the Cybersecurity & Infrastructure Security Agency in the U.S. has launched a Cyber Information Sharing and Collaboration Program (CISCP). Sharing helpful information and other resources with those who most need it may be a big positive step in making ransomware crimes a lot riskier and less profitable.

Ransomware Methods

Ransomware continues to be spread largely through multi-stage malware attacks. The first stage is a phishing attack—tricking a user into clicking on a malicious attachment or link—and in most cases it's a document that asks the user, often through highly creative language, to enable macros. Doing so infects their computer with a botnet client, which provides the attacker with command and control capabilities over the computer.

In the second stage, the attacker uses the botnet client to install malware like Trickbot or Cobalt Strike to begin the reconnaissance inside the organization, moving laterally

from system to system and stealing credentials. Finally, the attacker uses their already-installed malware to download ransomware and infect the organization's systems.

In 2021 law enforcement agencies took actions to shut down some of the components that many ransomware attacks rely upon. A prime example is Emotet, a trojan that's been widely used for its botnet command and control capabilities and its ability to distribute ransomware and other malware within organizations. A massive effort coordinated across law enforcement agencies took the Emotet botnet down in early 2021.

Unfortunately, Emotet returned later in 2021.^{xv} So far, takedowns have temporarily made things more difficult for attackers but haven't caused any overall slowdowns.

In an attempt to avoid detection, ransomware attackers are more frequently using living-off-the-land tactics as part of their multi-stage attacks instead of relying solely on malware components.

For example, misuse of RDP, a Microsoft remote access system, is endemic, and in 2021 RDP was used to spread ransomware as often as phishing was. RDP has been a common target for several years, but RDP attacks have spiked since the sudden and massive transition to remote work in 2020.

Ransomware attacks still usually rely on at least one malware component to provide command and control capabilities.

While multi-stage malware attacks are still favored, in 2021 we saw an increase in single-stage attacks. Attackers directly delivered ransomware executables to users through avenues like email attachments in carefully crafted phishing emails.^{xvi} Single-stage attacks have the advantage of happening more quickly than multi-stage attacks and with fewer malware components that an organization might detect and stop. However, single-stage attacks don't provide attackers with the visibility and access within the organization that multi-stage attacks can.

There's one final trend in ransomware methods to keep an eye out for in 2022: cryptomining. Some attackers are deploying cryptomining software instead of ransomware, which then consumes the victim organization's resources while making profits for the attackers. We'll discuss this in more detail in the Cryptocurrency section of this report.

Thwarting Ransomware Through Cyber Resilience

Ransomware can enter and infect your systems in many ways, such as phishing emails, malicious links and unsecured RDP. Many organizations, especially SMBs, lack the budget and skilled staff needed to keep up with today's threats. And unfortunately, no matter what you do in terms of prevention, a ransomware infection somewhere in your organization is inevitable.

What's needed is a strategy for combating ransomware and other types of cyber threats—and for recovering when a threat succeeds. That strategy is cyber resilience. Cyber resilience works by developing a layered defense in depth strategy that zeros in on training your personnel, blocking threats, protecting your devices and networks, backing up your data and recovering from data loss quickly.

Layered approaches to stopping ransomware are essential. There's no such thing as a 100% effective layer. By combining layers, like inspecting all incoming emails for malware, keeping PCs fully patched, using antivirus software and endpoint protection tools on all PCs and educating users on how to avoid phishing attacks and other forms of social engineering, you can make it less likely that attacks will succeed. Each layer blocks some of the attacks that other layers miss.

Cyber resilience also prepares your organization to handle any ransomware attacks that slip through these layers and succeed in infecting your systems. Preparation involves having incident response capabilities ready to act at all times and regularly testing your resilience plan, especially backup and restore capabilities for your organization's critical systems and data. Being prepared means you can act more quickly to stop a ransomware incident from spreading, minimize the likelihood of a major data breach and restore your operations.

Spotlight: The Future of "Stealth" Ransomware Attacks

In 2022, we will see "stealth" ransomware attacks: in order to persuade companies to quickly pay ransoms, ransomware gangs will give their victims the option to pay the ransom *before* the data is encrypted and exfiltrated.

They will ensure multiple strong footholds on the target beforehand, with sophisticated, failsafe automated encryption and exfiltration routines in place—essentially a ticking time-bomb if the target tries to remove or block the implanted malware. There will be a very short window of time in which the ransom can be paid before all critical data and backups are encrypted and key data is exfiltrated. Targets will be motivated to pay at this early stage to avoid the need to declare that a full-scale attack occurred and to avoid any compliance fines or negative media attention, let alone all the work needed to restore encrypted data and recover their operations.

Cybercriminals in their ransom demands will offer to encrypt a particular system or otherwise show strong evidence that they have deeply infiltrated the network and systems of their target. Cybercriminals will use DDoS attacks during the initial persuasion phase if payment does not arrive quickly enough. Some attackers will also claim much deeper infiltration than they've achieved and use well-targeted DDoS attacks to make it appear they've compromised websites and other important systems.

With cybercriminals increasingly coming under scrutiny from international lawmakers, they are keen to avoid drawing unnecessary attention to themselves. This "stealth" approach will help them to stay under the radar and get paid more quickly. It may also help them to bypass legislation prohibiting ransomware attack payments that may come into law in some countries or states in 2022.



"We will continue to see shorter times from initial compromise to ransomware deployment. We will also see attackers engage in rebranding to make attribution more difficult. As attackers become more strategic about who they attack, SMBs become a highly lucrative option. Attackers assume these types of businesses have little in the way of protection and are more willing to pay their ransom demands."

Matt Aldridge, Principal Solutions Consultant



Cryptocurrency

We observed significant shifts in attacks involving cryptocurrency during 2021. First, we witnessed the demise of browser-based cryptojacking. This form of attack relies on exploiting unsuspecting visitors on websites where JavaScript has been maliciously injected. Visiting such a site runs cryptomining scripts from the user's browser without the user's knowledge. Browser-based cryptojacking had been in decline before 2021, but this year it nearly disappeared.

Unfortunately, cryptojacking has been replaced with other, more effective approaches to cryptomining that aren't dependent on website traffic. Attackers are spreading cryptomining executables through phishing attacks and exploiting software vulnerabilities. A prime example of the latest wave of cryptomining malware is LemonDuck. LemonDuck uses numerous techniques to infect systems and to spread itself from an infected system to others.^{xvii}

As cross-platform malware, LemonDuck has the ability to infect both Windows and Linux computers. Expansion to less secure platforms has helped LemonDuck spread more quickly, leading to more mining and more revenue generation. LemonDuck also "safeguards" the platforms it infects by patching vulnerabilities and purging other malware variants.

This is because, in order to succeed, cryptomining malware needs to avoid detection for an extended time, typically weeks or months, so it can run long enough to be worthwhile for the attacker.

With cryptocurrencies becoming more valuable and popular, some attackers are running scams to steal cryptocurrency itself.

These scams don't always use the traditional methods like phishing someone into depositing cryptocurrency into an attacker-controlled account. Attackers do everything from distributing bogus mobile wallets to using DNS poisoning attacks that redirect victims to malicious lookalike exchange sites. We also see malware that includes clipboard skimmers, which look for an address and replace it with an address of the attacker's choosing.

There is also increasing interest in money laundering for cryptocurrency. Attackers who collect sizable payments from ransomware or steal cryptocurrency through scams often need to conceal the source of the cryptocurrency to avoid detection and prosecution. Law enforcement is cracking down on cryptocurrency laundering, and the U.S. Justice Department launched a National Cryptocurrency Enforcement Team (NCET) in late 2021. NCET will investigate and prosecute cryptocurrency-related crimes, as well as help victims recover their funds.^{xviii}

Whether this will lead to a decrease in this type of criminal activity remains to be seen. However, in February 2022 the Justice Department announced the seizure of \$3.6 billion in stolen cryptocurrency and the arrest of suspects. This cryptocurrency had been stolen several years earlier and tracked by investigators, leading to the remarkable recovery.^{xix} Hopefully more cryptocurrency seizures and arrests will be forthcoming.



"New and emerging threat actors will likely do cost-benefit analysis of long-term versus short-term mining and turn to social media platforms for price manipulation. By becoming more calculated in their approach, bad actors will look to maximize their potential financial windfalls."

Kelvin Murray, Senior Threat Research Analyst



High-Risk URLs

High-risk URLs encompass several categories of URLs that are malicious or suspicious, including:

- Botnets
- Keyloggers and monitoring
- Malware sites
- Phishing and other frauds
- Proxy avoidance and anonymizers
- Spam, spyware and adware

The BrightCloud® Web Classification Service averages 4.5 billion requests a day to categorize URLs based on their websites' behavior, history, age, popularity, location, networks, links and real-time performance. It constantly updates its categorizations to determine which URLs are high-risk and what nefarious behavior is associated with each.

One trend we closely monitor from year-to-year is how many malicious URLs are hosted on non-malicious (trusted) domains. This percentage indicates how frequently attackers have been able to set up malicious websites on otherwise-benign servers, such as exploiting a web server vulnerability to compromise the server and use it for hosting phishing sites. A few years ago, the percentage had bounced between 25% and 40%, then fell to 8% in 2020. We weren't certain if that large drop was related to the pandemic, improved web server and website security practices or changes in some of our threat data collection methods.

Now we have our answer. In 2021, the percentage jumped back up to 16% of malicious URLs. It's quite likely that the temporary drop in 2020 was primarily related to the pandemic.

Organizations likely focused more resources on securing their externally accessible resources like web servers or attackers changed their own plans.

URL Classification

We discovered over four million new high-risk URLs in 2021, almost two-thirds of them involved phishing.

That's a large percentage, but it's a significant drop from 2020 when 81% of high-risk URLs were for phishing. Most high-risk URLs are for phishing, malware sites and proxy avoidance and anonymizers and this report focuses on those three types.

The graph shows the month-to-month fluctuations in each of them during 2021, based on how much the actual count exceeded or fell below the average for the year, which is indicated by 0%. Interestingly, the graph indicates that there is relatively little fluctuation in the number of phishing URLs throughout the year, with maximum changes around 20% above and below the average. Malware sites are more dynamic, with changes reaching over 40% above and below the average.

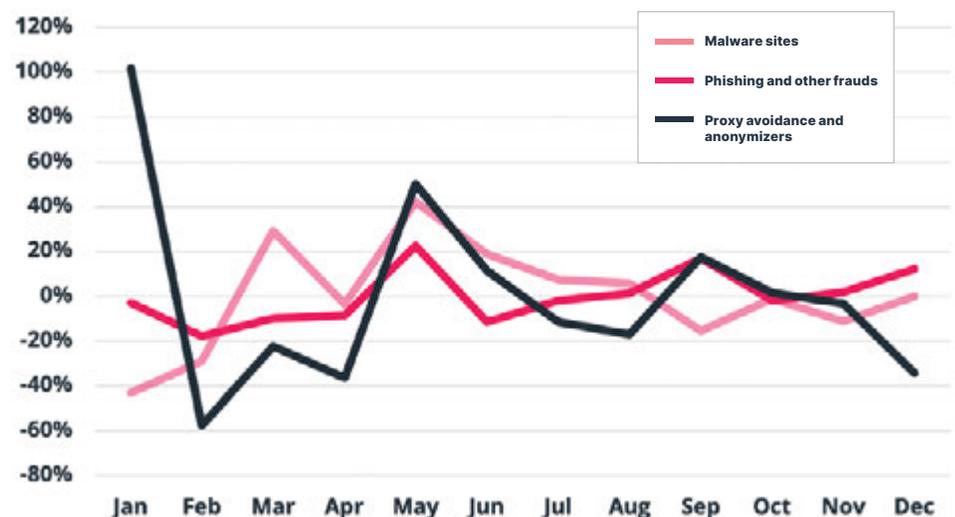


Figure 8: Trends in high-risk URL classifications

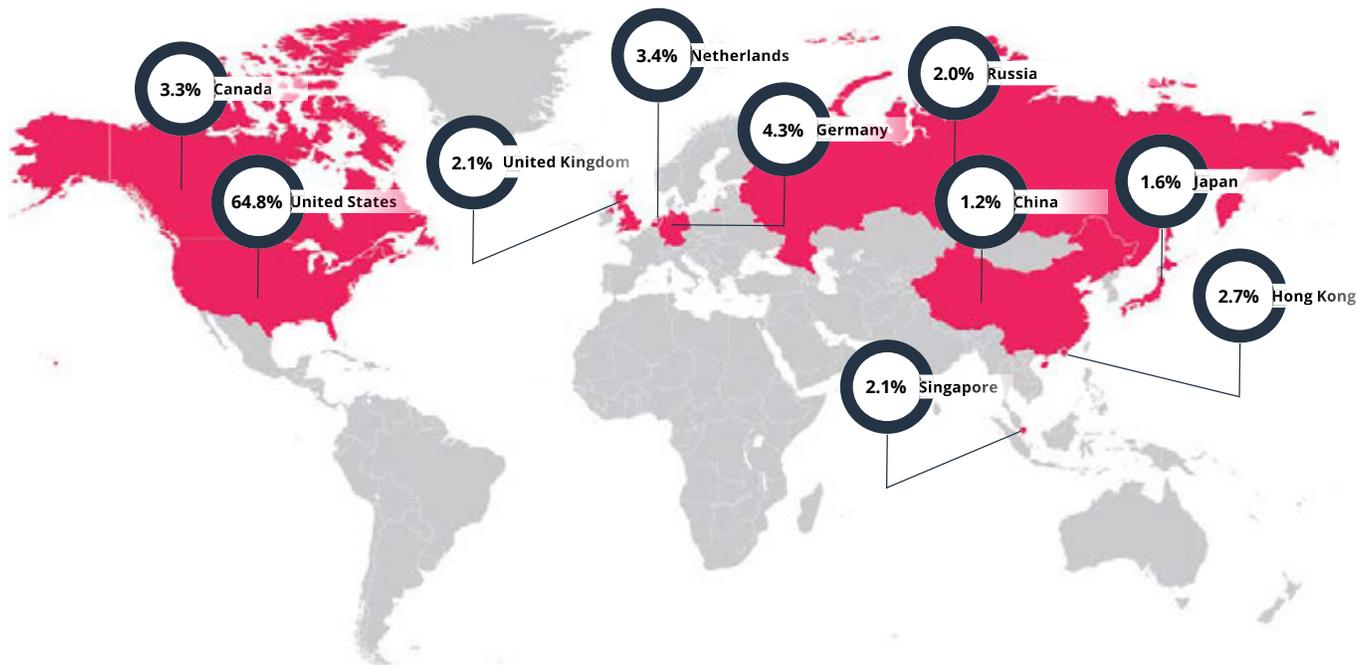


Figure 9: The top 10 countries hosting the majority of high-risk URLs in 2021

By far the majority of changes occurred with proxy avoidance and anonymizers. The January value was over 100% above the average, then plummeted in February to nearly 60% below average. In May, proxy avoidance and anonymizer URLs were 50% above average. Most notably, we saw big spikes in all three types of high-risk URLs during the month of May.

We can't point to specific events that would have caused all of these ups and downs. What we do know, from years of monitoring these trends, is that attackers will rapidly change what they do and how they do it in order to take advantage of new vulnerabilities, current events, changes in user habits and anything else that increases their likelihood of success.

Geographic Distribution

Every time we find a new high-risk URL, we try to identify the country that is hosting it. In 2021, around 48.5% of the time, a new high-risk URL was hiding behind a proxy or an anonymizer like Tor that obfuscated the URL's origin. For malware site URLs, a whopping 84.7% of the sites were hidden behind proxies or anonymizers.



84.7%
of malware site URLs were hidden behind proxies or anonymizers

Figure 9 shows the ten countries that were most often identified as hosting high-risk URLs. The rankings and percentages for most of these countries haven't changed much from 2020 to 2021. The U.S. is still hosting the majority of high-risk URLs, especially for phishing sites, and its share has even increased some since 2020. In that same timeframe, Germany's share more than doubled and Canada's more than tripled. Denmark and South Korea have dropped off the top 10, replaced by China and the United Kingdom.

For malware site URLs where the country of origin could be tracked, the United States was by far the leading location (44.3%). The rest of the top five countries were China at 10.5%, Hong Kong at 9.1%, Singapore at 5.7% and Russia at 5.4%. Together, these five countries hosted 75% of all malware site URLs found in 2021 with a known country of origin.

The U.S. is also the world leader in hosting phishing URLs: an overwhelming 59.6% of all phishing URLs where the origin could be tracked. Other countries in the top five were Germany (5.3%), Canada (4.5%), the Netherlands (4.3%) and Hong Kong (2.7%). The top five collectively hosted 76.4% of all phishing URLs with a known country of origin.

"We predict the percentage of high-risk URLs in existence will continue to grow, but attackers will use these URLs strategically based on what's happening at any given time during the year. Whether it's in proximity to the holiday season, after tax time or prior to an election, we foresee attackers timing their attacks to take advantage of unsuspecting users willing to click for updates. This will pose greater risks for businesses and consumers."

Grayson Milbourne
Security Intelligence Director



Phishing Attacks

Phishing attacks through emails, texts and other communication platforms remain the first step in many other attacks. As we discussed in the High-Risk URLs section, almost two-thirds of new high-risk URLs we detected in 2021 were for phishing attacks. Malware and ransomware attacks and cryptocurrency scams all make extensive use of phishing.

Phishing messages and websites continue to become more sophisticated and therefore more unlikely for users to notice. Some attackers are even adding CAPTCHAs to their phishing sites to make them seem more realistic.^{xx}

It's more important than ever to combine security awareness training for users with anti-phishing technologies to detect and stop these threats.

Phishing Volume

Figure 10 shows the volume of phishing messages we detected during each month of 2021. The year got off to a slow start for phishing, as it usually does, with the first four months only having a total of 9% of the phishing activity for the year.

*Then there was a **770% increase in May** compared to the average for the previous months.*

Phishing activity often skyrockets around income tax filing time in the U.S. Some of this can be attributed to attackers taking advantage of consumers with tax refunds to spend.



Security awareness training helps users understand the importance of examining URLs before clicking on them. To try to counteract this, some phishing attacks are now using URL shorteners, such as bit.ly, tinyurl.com and is.gd, to generate benign-looking URLs that redirect to phishing URLs. Since these shorteners are widely used for legitimate purposes, most organizations can't block them.^{xxi}

To thwart these types of phishing attacks, users need to be trained to recognize shortened URLs and to find out where they redirect before clicking on them. For example, adding a plus sign to the end of a URL from bit.ly or tinyurl.com will take you to a safe page showing when the shortened URL was created and what URL it redirects to. There are also websites where users can enter a shortened URL and get redirect information. Awareness of shortened URLs and options for handling them should be another tool in your users' toolboxes.



"Cybercriminals like to use tax season as an opportunity to execute attacks like spear phishing and spoofing. Be wary of suspicious emails that are attempting to lure you into providing your personal information to unlock your credentials, confirm your tax return details or refund eligibility. Businesses and individuals alike can easily fall for such attempts. Always ensure that any communication you receive comes from a legitimate source. Never respond to unsolicited emails asking you to provide personal information."

Grayson Milbourne
Security Intelligence Director

In 2021, 17.5% of all phishing activity occurred in the month of May.

That's nearly 20%. After fairly high volumes in June and July as well, phishing activity plummeted in August and September. We call these the "hacker holidays" because phishing activity is typically low during this time of the year. We imagine bad actors are likely taking a vacation.

October and November are usually the most active months of the year for phishing, and this year we saw a huge spike again. November was by far the most active month for phishing with 34.3% of all activity for the year, and October had 11.6% of the year's phishing. October and November are typically active because they lead into the holiday shopping season. Also, as U.S. elections have become more polarizing and of greater interest, attackers have incorporated elections into their phishing messages and websites. The timing coincides with the primary elections, which are mostly in May and June, and the general election in early November.

HTTP and HTTPS Use

As we detect phishing URLs, we also track whether they use HTTP or HTTPS. Many users associate HTTPS with "secure"—denoted by the familiar padlock in the browser—so they incorrectly assume any site is legitimate if it displays a padlock. Attackers have, of course, figured this out, so they register domains, acquire certificates for them and establish websites which use the certificates.

Of all the phishing URLs detected during 2021, 32% of them used HTTPS. This percentage would probably be much higher if it wasn't for the efforts by domain registrars and certificate authorities to prevent criminals from using their services, and if certificate reputation wasn't tracked as part of threat intelligence.

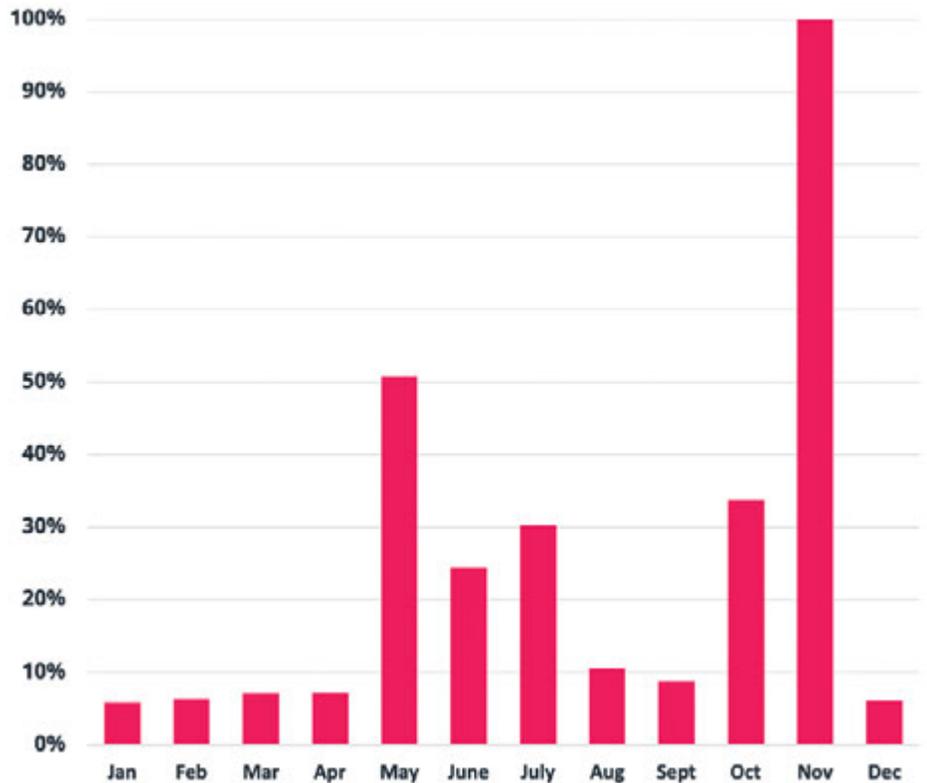


Figure 10: Phishing attacks by month



Figure 11: HTTP/HTTPS usage in phishing attacks by month

The Most Impersonated Companies

We typically see the same companies impersonated in phishing attacks from month-to-month and year-to-year, with some shifts in their order. The top five targeted brands in 2021 accounted for over 54% of detected phishing URLs. Apple (13.0%), Facebook (12.1%), YouTube (11.8%), Microsoft (9.1%) and Google (9.1%) were the favorite lures for phishing attacks, and all of these except YouTube were also in the top five in 2020. YouTube's rise in the rankings is likely due to its accounts being linked with Google since they are both Alphabet-owned companies.

What's missing from this year's top five is 2020's number one impersonated brand: eBay. eBay was heavily impersonated in early 2020 during the height of pandemic-related product shortages, when many were turning to the site to find goods they needed.

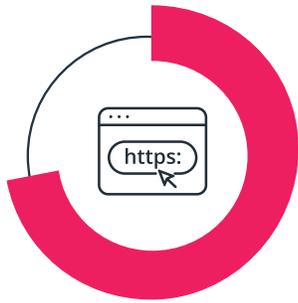


"We foresee an increase in the complexity of social engineering tactics as cybercriminals advance their tactics to become more deceptive and difficult to detect. Business email compromise (BEC) attacks will become more common. Deepfakes will continue to develop as a weaponized tool for clickbait that will help spread disinformation, particularly when it comes to elections and political developments."

Tyler Moffitt, Senior Security Analyst

Top 10 in 2019		Top 10 in 2020		Top 10 in 2021	
Facebook	12.8%	eBay	13.2%	Apple	13.0%
Microsoft	10.6%	Apple	10.2%	Facebook	12.1%
Apple	8.4%	Microsoft	9.5%	YouTube	11.8%
Google	7.7%	Facebook	8.8%	Microsoft	9.1%
PayPal	6.2%	Google	8.6%	Google	9.1%
Dropbox	3.2%	Steam	7.9%	Amazon	8.9%
Chase	3.1%	Yahoo	5.4%	PayPal	3.3%
Yahoo	2.9%	Amazon	4.7%	La Banque Postal	2.7%
Adobe	2.8%	Netflix	3.0%	Target	2.5%
Wells Fargo	2.8%	PayPal	3.0%	Instagram	1.9%

Figure 12: Companies most often impersonated in phishing attacks



In 2021, the top 10 brands comprised nearly 72% of all detected phishing URLs.

As the worst of the shortages passed, eBay fell out of favor with phishers. This year eBay barely made the top 20. This is a prime example of changes in attacker behavior based on current events.

In 2021, the top 10 brands comprised nearly 72% of all detected phishing URLs. However, we detect phishing attacks utilizing hundreds of other brands each year, many of those a single phishing URL for a brand during the entire year. Also, there's actually quite a bit of variation in which companies are being impersonated at any given time.

Figure 13 reflects the relative number of brands impersonated each month, with May being the highest month against which all other months are measured.

November involved nearly as many brands as May, while June and July were also high. For comparison, the graph also shows the relative volume of phishing URLs detected each month. Notice that in November, the diversity in brands and the volume of phishing were both high. In May, we saw the same volume of phishing, but with only half as many brands impersonated.

Comparing the two lines more closely, they track each other well throughout the year except for October and November. It appears that during that time period, there was a sudden and dramatic increase in how many brands were being impersonated, which returned to normal levels in December. The most likely reason for this is the holiday shopping season.



Figure 13: Number of brands impersonated by month



Malicious IP Addresses

BrightCloud tracks malicious activities by their associated IP addresses to help block repeat offenders and prevent attacks from reaching the endpoint. During 2021, the average number of malicious IPs at any given moment was nearly four million. This number has been consistent for the past few years, indicating a potential plateau for malicious IP activity.

As part of malicious IP tracking, BrightCloud monitors what types of nefarious activities originate from each address. We refer to each detected instance of bad behavior as a *conviction*. In this report, we take a closer look at the 50,000 malicious IPs associated with the most convictions during the year. The top 50,000 in 2021 had 11.6 million convictions, a 10% increase from their counterparts from 2020.

Performing Multiple Bad Behaviors

Bad behaviors for malicious IPs come from a variety of sources: scanners, spam sources, Windows exploits, botnets, Tor proxies, other proxies, web attacks, phishing and mobile threats. For the top 50,000 malicious IPs in 2021, each IP was convicted in at least two of these categories throughout the year. Of these same IPs, 96.5% were convicted in either three or four of the categories.

This illustrates an enduring trend: the most active malicious IPs are used for multiple malicious behaviors.

However, this conviction trend weakens when we examine malicious IPs with five or more categories, dropping to only 3.5% of the top 50,000. This rate has fallen from previous years, indicating that attackers may be attempting to avoid detection by performing fewer types of malicious behaviors from a single place.

Figure 14 reflects the number of convictions by category for the top 50,000 malicious IPs. Four categories are far more prevalent than others.

Scanners are the front-runner of the categories with 26%, followed closely by Spam Sources and Windows Exploits at 25% each and Botnets at 20%. Those four categories comprise 96% of all convictions, which is similar to what we witnessed in 2020.

BrightCloud also tracks exit nodes for the Tor network because Tor proxies are often used in an attempt to conceal the source of attacks. The number of Tor exit nodes we detected increased by approximately 40% from 2020 to 2021.

The 2021 total is nearly three times what we observed for 2019. This continued growth indicates rising use of the Tor network, both because of the shift towards remote and hybrid work and increased concerns about privacy.

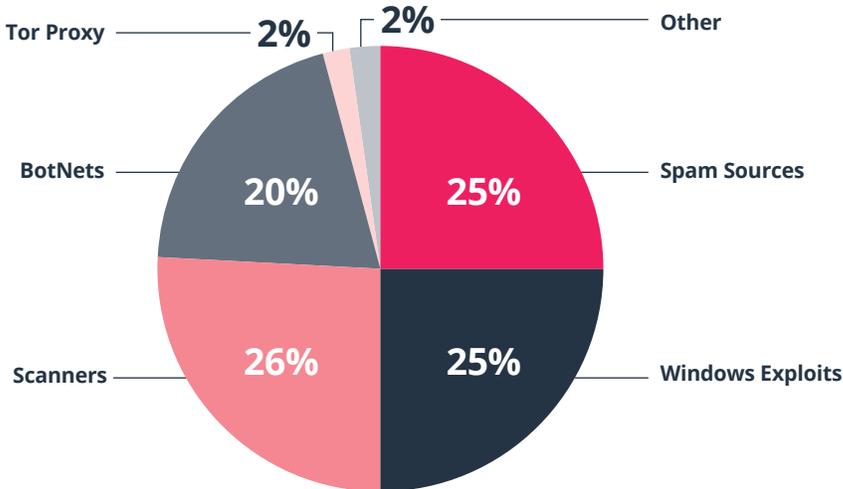


Figure 14: Convictions by category for the top 50,000 malicious IP addresses

Frequency of Convictions

The conviction numbers we've been looking at so far don't indicate how frequently each behavior occurs. Let's delve a little deeper and examine how often each of the top 50,000 malicious IP addresses is caught performing each bad behavior.

Only 6.0% of the top 50,000 were observed performing malicious actions in every month of 2021, although they had nearly 34% of all convictions. It's much more common for IPs to be used for malicious purposes for a short time and then not used for a few months before being active again. This fluctuating strategy allows attackers to avoid being blocked and provides ample time to be removed from blocklists before striking again.

Of the top 50,000, 54.1% were only active for three months or less during 2021.

Spam is the most common type of conviction, accounting for 86.3% of the total last year. This is nearly identical to the rates in 2020 and 2019 (87.0% and 87.6%, respectively). Spam rates were relatively consistent for all months of the year.

To better understand changes in the rest of the conviction data, we've removed the spam data. Figure 15 shows the monthly conviction numbers for the top categories (excluding spam) for the top 50,000, including proxies, Windows exploits, scanners and botnets. While proxy activity was fairly even throughout the year, there were significant changes in other categories, especially botnets. We saw a spike in botnet convictions during July. The likely explanation for this is that one or more massive DDoS attacks were performed at that time, and members of the botnet that had been quiet for months suddenly roared to life and were detected all at once.

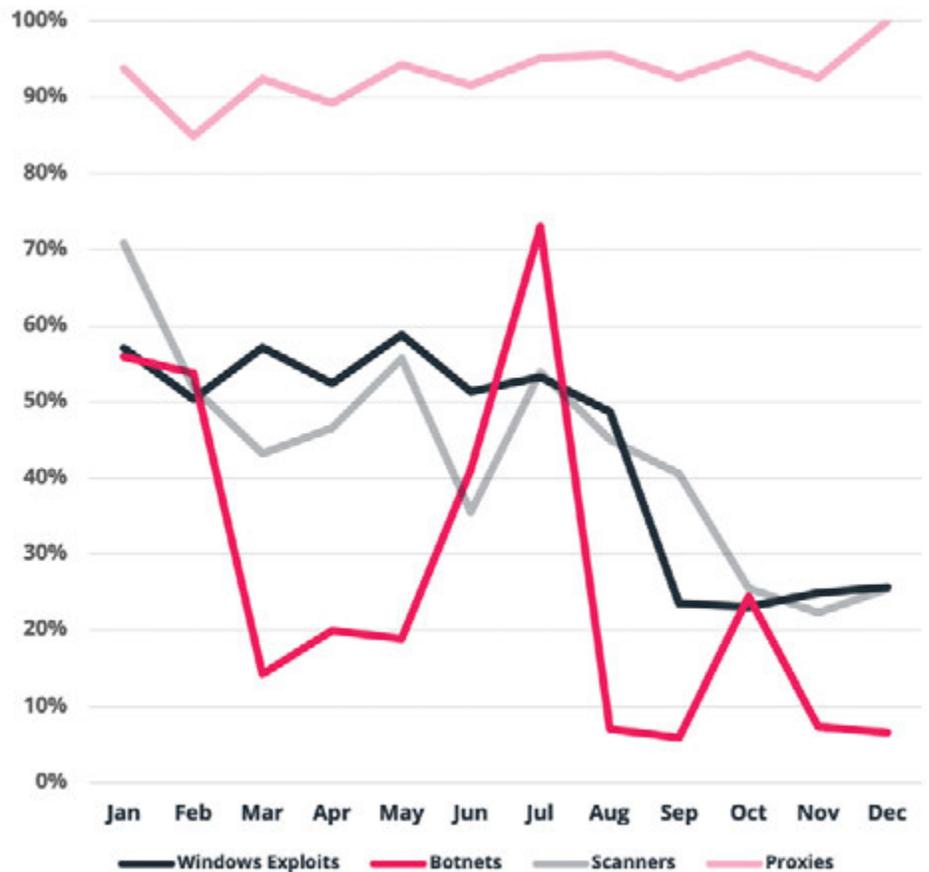


Figure 15: Monthly convictions by category for the top 50,000 malicious IP addresses, excluding spam



The number of IoT devices we will own and operate in our homes, in our workplaces and even our bodies will continue to rise. Many IoT devices that consumers use regularly lack security features common among other devices^{xxii} and they're rarely deployed in a secure state, let alone maintained. Consumer IoT devices have a lot of processing capabilities and bandwidth available, making them lucrative targets.

Consumer IoT devices are perfect avenues for attackers to exploit and compromise when combined with botnets to perform DDoS attacks. They can also be called upon to generate traffic that conceals other attacks being performed simultaneously. We expect to see botnet IP counts increase in 2022, but with the same kinds of fluctuations we witnessed in 2021.

Geographic Breakdown

The IP addresses in the top 50,000 originated from 175 countries. However, a large majority, 80%, were from 20 countries. What we found most striking is over half of the top 50,000 were located in one of five countries: China (17.6%), the United States (15.0%), India (8.6%), Vietnam (6.7%) and Russia (3.9%).

Figure 16 depicts the relative shares of the top 50,000 IP addresses from the top ten countries. China's share is represented as 100% since it's the highest. The chart also illustrates the number of convictions for each country. The U.S. had the largest number of convictions in 2021: 24.3% of the top 50,000's. That's a 25% increase from 2020.

Of these top five, the Netherlands had the highest number of convictions per bad IP address: an average of 526. This means that each malicious IP address in the Netherlands performed more malicious activity on average than the average malicious IP address in other countries.

The U.S. was second with 375 and Germany was third with 350. Throughout the top 50,000, the average number of convictions per IP address was 241.



The remaining top five for 2021 were China (13.1%), the Netherlands (8.2%), India (5.2%) and Germany (3.6%). These five countries collectively had over 54% of the convictions but only 47% of the top 50,000 IP addresses, so they were mild overachievers.

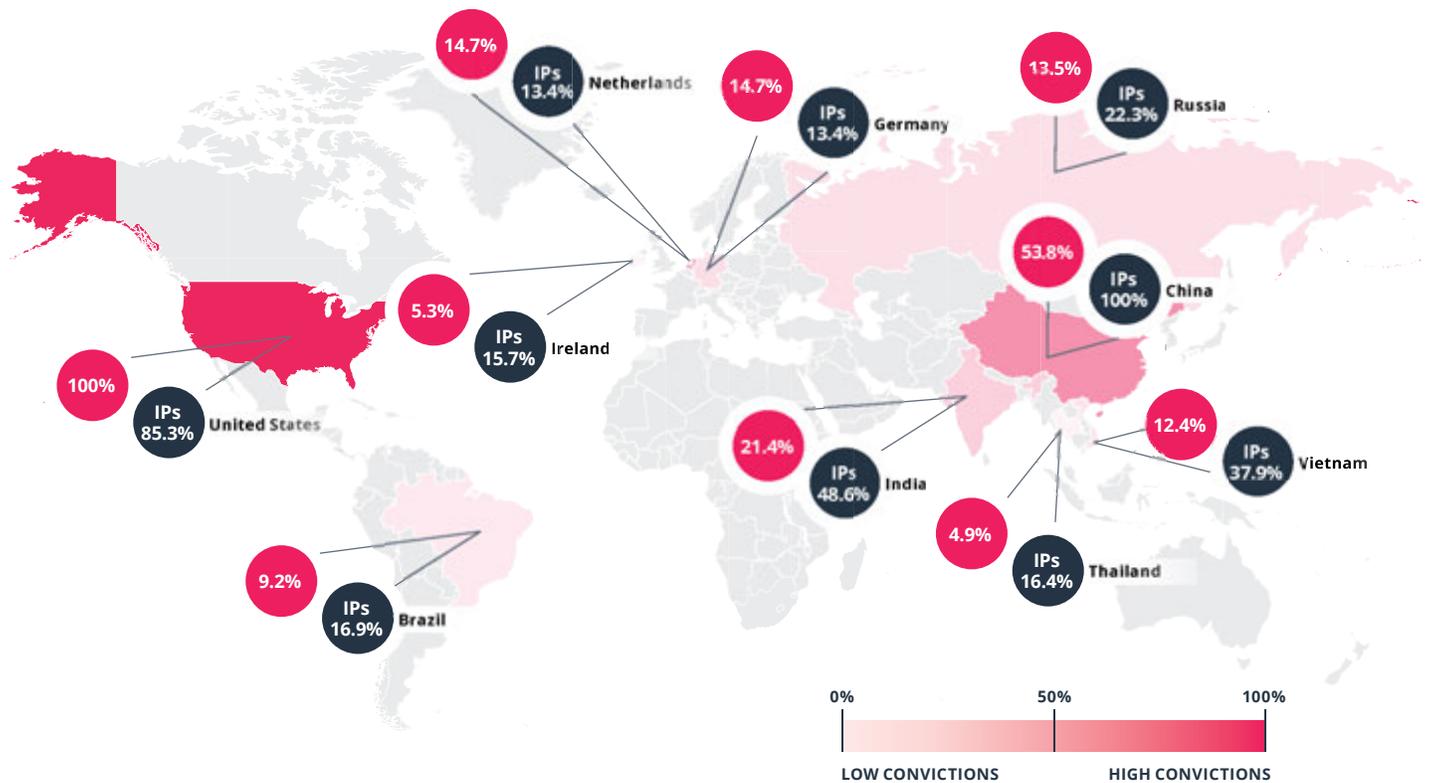


Figure 16: Malicious IP addresses and convictions by countries of origin for top 50K malicious IPs



Security Awareness Training

Layered defenses are absolutely essential for stopping threats. Attacks are becoming increasingly sophisticated. As a result, attackers are securing record-high profits from ransoms and cryptocurrency thefts. The best defense has several layers that complement each other. Security awareness training is the only layer that exclusively focuses on changing user behavior, and there's no other layer that can take its place.

With security awareness training, we see significant reductions in devices with malware when users are properly trained. Webroot® Security Awareness Training customers see a 10% reduction in devices with malware than those with Webroot® Business Endpoint Protection alone. And customers who use Webroot® DNS Protection along with Webroot® Security Awareness Training experience a 15% reduction. Webroot® Security Awareness Training also educates users on BEC attacks, which remain highly prevalent.

BEC attacks don't necessarily have a malware component, so user education is particularly important for spotting and stopping them.

Many incidents of data loss begin with a single mistake made by a single user. A 15% reduction in infected devices can make a real difference, especially for SMBs. While there is no guarantee users won't be tricked by phishing attempts or other social engineering tactics, providing the right training helps reduce successful attempts and make them easier to detect.

Users need to be updated frequently on the latest trends in phishing, especially when they concern topics like elections or major sporting events. They also need to know about other threats, like fake personas on social media and the use of deepfakes, used to fool users. The more educated your users are, the more they can be active participants in safeguarding your organization.



Conclusion

We made it through 2021, the year where everything security-related that could go wrong did go wrong. So what's next?

More of the same, unfortunately. The permanent reality of a highly distributed and hybrid workforce will continue to shape how bad actors strategize and execute their attack plans. With more devices operating remotely, endpoint protection and awareness training become vital for protection and for preventing attacks. This becomes all the more relevant as malicious actors continue to make their attacks more sophisticated. To make matters worse, bad actors are coalescing into larger criminal organizations, making it almost

certain they will continue looking for avenues to generate big profits from ransomware, cryptocurrency theft, the sale of stolen data and other means. Supply chain attacks, attacks against critical infrastructure and the rebirth of botnets that were taken down all hint at things to come...2022 is going to be another challenging year for all of us.

Our ability to prepare and recover from these threats will come from focusing our efforts on integrating cyber resilience into our technologies, our processes and our people. Compromises are inevitable, so we need to plan for them and be prepared to recover quickly when they happen.

To reduce the likelihood of compromises and to establish the ability to restore normal operations swiftly, we need to have strong layered defenses in place. That includes preventing malware and network-layer attacks by using solutions backed by industry-leading threat intelligence and machine learning. It requires backing up all systems and files to ensure your data is always available where and when you need it and testing your restoration capabilities under simulated attack scenarios. It also means frequently training your users to identify and avoid phishing attacks and scams. These collective measures are at the heart of cyber resilience.

Adopting cyber resilience allows you to prepare and recover from attacks. Through a defense in depth approach, you can act more quickly to thwart malicious threats from spreading, minimize the likelihood of a major data breach and restore your operations. Only through cyber resilience can we truly make progress in our fight against cybercrime.



Sources

- ⁱ <https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021>
- ⁱⁱ <https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/>
- ⁱⁱⁱ <https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021>
- ^{iv} <https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases>
- ^v <https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate>
- ^{vi} <https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020>
- ^{vii} <https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021>
- ^{viii} <https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/>
- ^{ix} <https://www.wired.com/story/apple-ransomware-attack-quanta-computer/>
- ^x <https://www.zdnet.com/article/us-insurance-giant-cna-financial-paid-40-million-ransom-to-wrestle-back-control-of-systems/>
- ^{xi} <https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/22/with-rising-cyber-insurance-costs-and-requirements-consider-new-alternatives-to-fight-ransomware/?sh=8eef096e140e>
- ^{xii} <https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/>
- ^{xiii} <https://www.reuters.com/technology/us-offers-reward-up-10-mln-information-darkside-cybercrime-group-2021-11-04/>
- ^{xiv} <https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts>
- ^{xv} <https://www.zdnet.com/article/emotet-once-the-worlds-most-dangerous-malware-is-back/>
- ^{xvi} <https://zix.com/resources/threat-report>
- ^{xvii} <https://www.zdnet.com/article/microsoft-warns-over-this-unusual-malware-that-targets-windows-and-linux/>
- ^{xviii} <https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts>
- ^{xix} <https://www.wsj.com/articles/justice-department-says-it-seized-3-6-billion-in-stolen-cryptocurrency-exchange-hack-11644339381>
- ^{xx} <https://zix.com/resources/threat-report>
- ^{xxi} <https://zix.com/resources/threat-report>
- ^{xxii} <https://doi.org/10.6028/NIST.IR.8267-draft>

About BrightCloud® Threat Intelligence

BrightCloud was the first threat intelligence platform to harness the cloud and artificial intelligence to stop zero-day threats in real-time. The platform is used to secure businesses and their products worldwide with threat intelligence and protection for endpoints and networks. With more than 10 years of experience in building and analyzing the industry's most robust internet threat database, BrightCloud has the strongest coverage model, fewest uncategorized objects and the most historical records which others cannot replicate.

In 2019, BrightCloud was acquired by OpenText, a global leader in Enterprise Information Management. As a whole, we are a market leader in cyber resilience, offering total endpoint protection and disaster recovery for businesses of any size.

brightcloud.com

