

# 2023

## OpenText Cybersecurity Threat Report

Malware • Ransomware • High-Risk URLs • Phishing Attacks • Malicious IP Addresses • Harmful Mobile Apps

# Inside the report

<b>Foreword</b> .....	<b>3</b>
<b>Threat Intelligence Overview</b> .....	<b>4</b>
<b>Malware</b> .....	<b>6</b>
Infected Consumer and Business PCs.....	7
Infection Rates by Number of Licenses .....	8
Infection Rates by Region .....	9
Infection Rates by Industry .....	10
How Malware Reaches its Targets .....	10
Where Malware Hides .....	11
<b>Ransomware</b> .....	<b>12</b>
Rising Ransom Costs .....	14
Ransomware Gangs.....	14
Ransomware Methods.....	16
Thwarting Ransomware Through Cyber Resilience .....	17
<b>High-Risk URLs</b> .....	<b>18</b>
URL Classification .....	19
Malicious domains.....	19
Location-masking.....	20
Geographical Distribution .....	21
<b>Phishing Attacks</b> .....	<b>22</b>
Phishing Volume .....	23
HTTP and HTTPS Usage.....	23
Most Impersonated Companies.....	24
Email-Based Phishing Attacks .....	25
<b>Malicious IP Addresses</b> .....	<b>26</b>
Performing Multiple Bad Behaviors.....	27
Frequency of Convictions .....	28
Geographic Breakdown.....	29
<b>Harmful Mobile Apps</b> .....	<b>30</b>
<b>Security Awareness Training</b> .....	<b>32</b>
<b>Conclusion</b> .....	<b>36</b>

# Foreword

Cybersecurity professionals were kept on their toes throughout 2022. Russia's invasion of Ukraine sent shockwaves through organized cybercrime and disrupted ongoing operations by REvil and Conti. Global law enforcement continued to aggressively target threat actors, including the Hive ransomware gang. And discovery of critical vulnerabilities and exposures (CVE) continued at a record pace, with nine CVEs published with scores of 9 or higher.

In addition to these new developments, 2022 also saw a continuation of many of the trends first observed at the start of the pandemic. Attacks on manufacturing and supply chains remained common, disruptive, and profitable. By the end of the year, the average ransom demand was at its highest ever, with the median cost hitting just under \$200,000. Ransomware gangs increasingly targeted smaller businesses, which have fewer resources to prevent and manage the disruption. Simultaneously, many businesses faced tough security spending choices over the past year — exacerbated by rising inflation and economic uncertainties — brewing an ideal environment for cybercrime.

Meanwhile, phishing has evolved to take advantage of new social media platforms targeting younger users. And ever-advancing artificial intelligence (AI) capabilities look set to further fuel these kinds of attacks.

All of these issues combined make it more important than ever for businesses to embrace cyber resilience. In the 2023 OpenText Cybersecurity Threat Report, we dive into the inner workings of the threat landscape to highlight the situation facing businesses large and small. As OpenText Cybersecurity, we provide comprehensive security solutions for companies and partners of all sizes, helping customers build cyber resilience via a holistic security portfolio. Every year, we aim to improve the quality of our report data while providing broad coverage of threat activities. New to this year's report is the inclusion of data from Webroot Email Security (formerly Zix). Email is a core vector for many cyberattacks and we are excited to be able to include this information in our in-depth analysis of 2022. We hope the information in this report empowers you to build stronger and smarter defenses for the year ahead.



***Cyber bad actors, including nation-state players, continue to be persistent, innovative and effective. There is, however, some encouraging news. A decline in malware infections indicates comprehensive security measures are effective.***

***Prentiss Donohue  
Executive Vice President  
OpenText Cybersecurity***

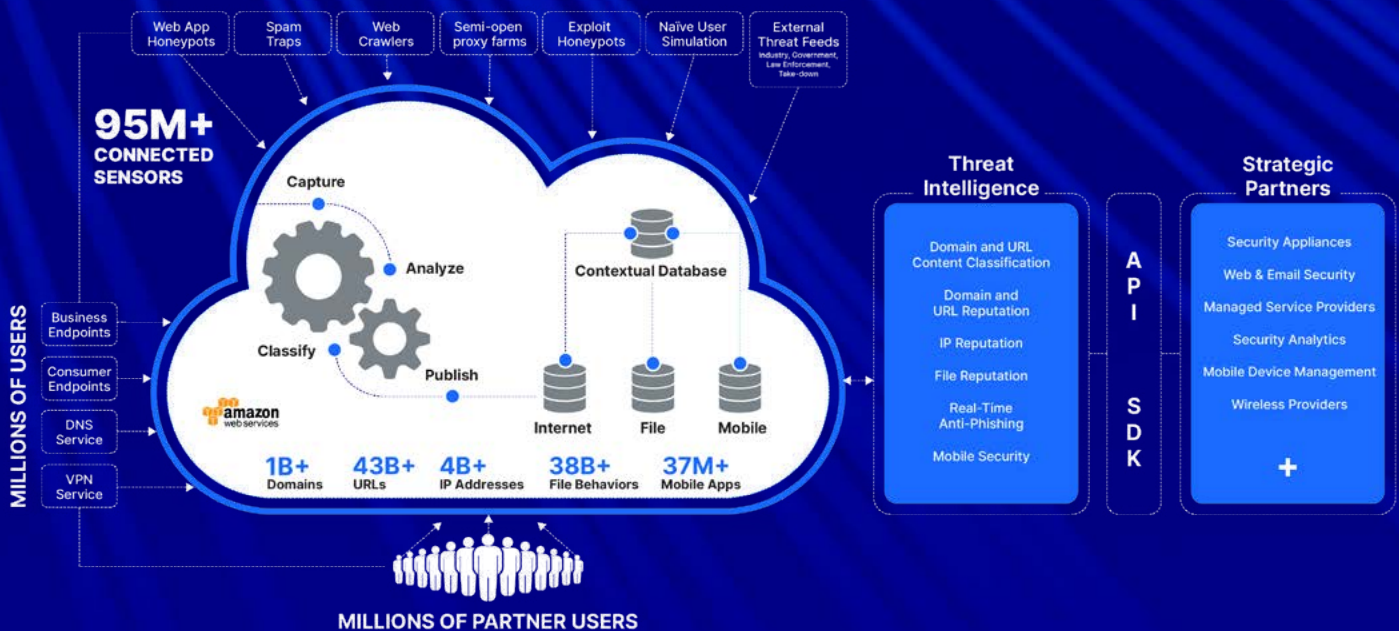


# Threat Intelligence Overview

The threat intelligence, trends, and details presented in the 2023 OpenText Cybersecurity Threat Report are based on data continuously and automatically captured by the BrightCloud® Platform — 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 then analyzes and interprets this data using advanced machine learning and AI.

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 for industries, geographies, companies, and individuals, and reveal what our threat experts expect to see in the coming year.



## Threat Intelligence by the Numbers



**95M+**

Real-world sensors



**78M+**

End users protected through  
technology partners



**1B+**

Domains categorized



**43B+**

URLs evaluated



**4B+**

IPs



**38B+**

File behavior records



**37M+**

Active mobile apps



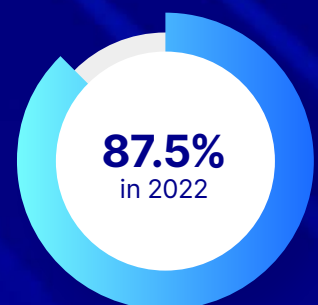
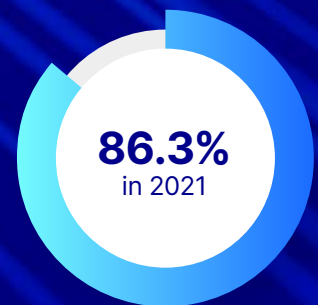
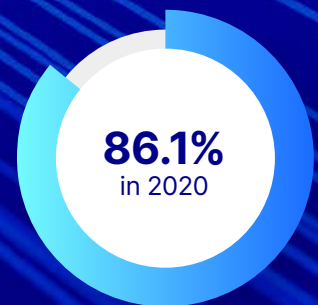


**This year, 87.5%  
of malware was  
unique to one PC**

# Malware

The stability of these figures (right) demonstrates that attackers are consistent in the techniques they use to evade detection.

In terms of tackling the issue of malware, the evidence recommends a layered approach to detect and protect against complex evasive threats. Our data showed that: First, the good news is that malware infection rates continue to decline. The number of malware files reaching Webroot-protected Windows endpoints has decreased year-over-year for the last three years, dropping by 16.7% between 2019 and 2020 and by 58% from 2020 to 2021. This decline in infections continued from 2021 to 2022 but at a slower pace. This doesn't mean that malware isn't still a very real threat. Our analysts encounter nearly a million new application files on a daily basis, and we continue to detect and block thousands of brand new malware variants each day.



There are three main reasons for the recent reduction in detected malware infections:

1. The ongoing migration from Windows 7 to newer Windows versions that experience significantly lower infection rates.
2. BrightCloud's upstream malware detection and blocking rates have continued to improve.
3. Attackers are changing their behavior. They're increasingly evading detection by "living off the land" (LotL) — running malicious commands on benign applications that are already present on endpoints rather than installing their own malware there.

Each year, we track the percentage of Windows malware that is only detected on a single PC. For the past few years, this number has hovered between 85% and 90%:

- Users who had implemented both Webroot SecureAnywhere and Webroot Security Awareness Training **saw a 4.5% average reduction** in the number of malware infections they encountered compared to those that only had Webroot SecureAnywhere.
- Those who used Webroot SecureAnywhere and Webroot DNS Protection experienced, on average, **27.1% fewer malware infections** than those that only had Webroot SecureAnywhere.
- Users who adopted all three layers of protection — Webroot SecureAnywhere, Webroot Security Awareness Training, and Webroot DNS Protection — rather than just using Webroot SecureAnywhere alone had the lowest infection rate, with an **average 40.3% reduction** in the number of devices that encountered malware.

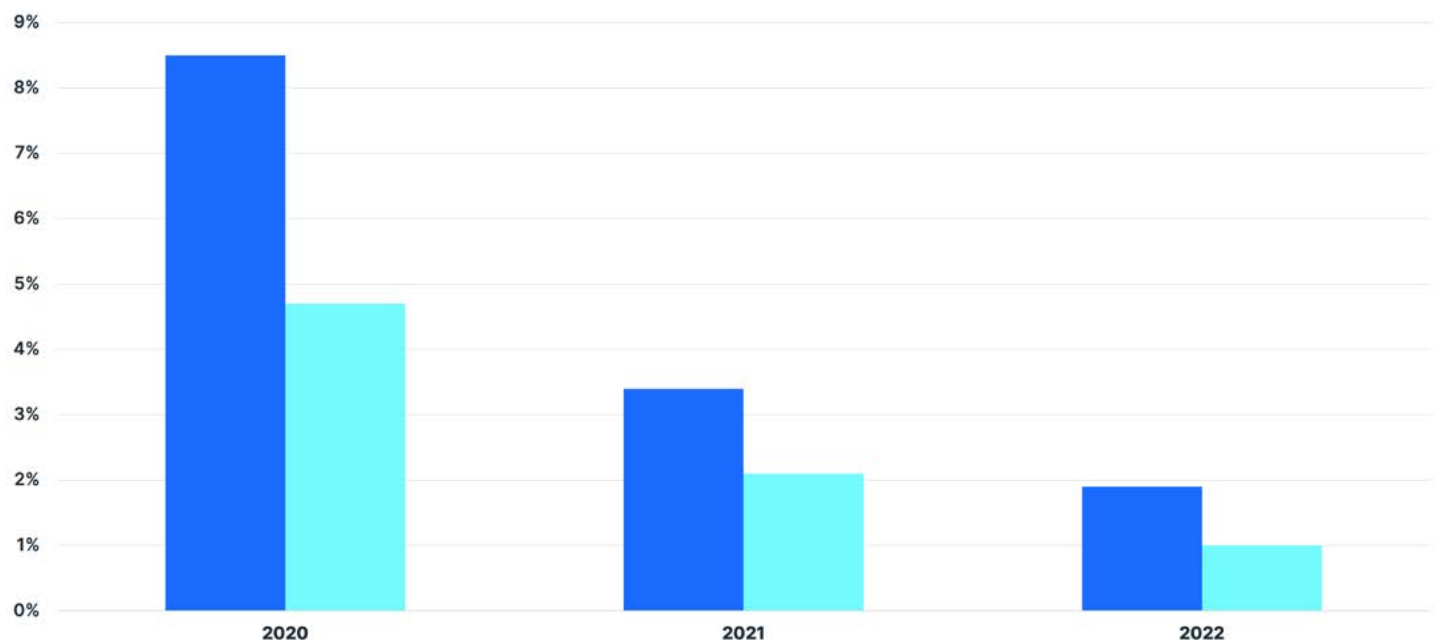


Figure 1: Infection rates for business and consumer PCs

## Infected Consumer and Business PCs

As in previous years, both consumer and business PCs are seeing decreases in rates of malware infections.

- In 2020, the malware infection rate fell to 8.5% for consumer PCs and to 4.7% for business PCs.
- In 2021, the decline was even sharper, with the infection rate falling to 3.4% for consumer PCs and 2.1% for business PCs.
- In 2022, this momentum continued but slowed, with the infection rate for consumer PCs falling to 1.9% and to 1.0% for business PCs.

---

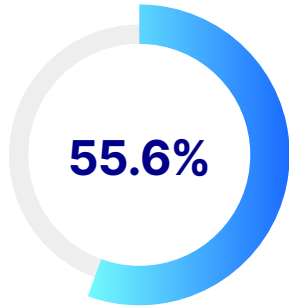
**Lower infection rates are always good news — but the rate of infection for consumer PCs is still nearly double the rate for business PCs.**

---

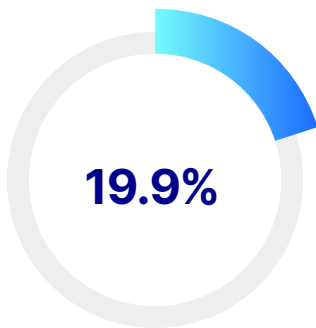
As hybrid work becomes increasingly popular, organizations need to think carefully about the best strategies for protecting employees who are using their own PCs for work purposes. In many cases, requiring employees to use corporate-owned and managed devices can contribute to cyber resilience.

Besides examining infection rates, we also look at re-infection rates — that is, how often PCs were infected more than once during the year.

**Among infected consumer PCs**

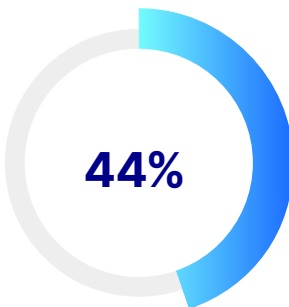


were infected at least once



were infected more than five times

**Among infected business PCs**



saw more than one infection, a significantly lower rate than what we observed for consumer devices.

These findings highlight the importance of user education, especially in the wake of a compromise, because training end users can significantly reduce their risks of re-infection.

**Infection Rates by Number of Licenses**

To see whether larger or smaller organizations were more likely to experience malware infections, we analyzed infection rates according to the number of licensed PCs owned by a business (Figure 2).

Among the smallest organizations (those with 20 or fewer licensed PCs) only 6.4% experienced an infection, with an average of six PCs infected.

Medium organizations (those with 21 to 100 licensed PCs) saw higher infection rates, with 28.5% hit with an infection and an average of seven PCs affected.

Larger organizations (with 101 to 500 licensed PCs) experienced infection rates that were higher still, with 58.7% encountering an infection and an average of 17 PCs affected.

The largest organizations (those with more than 500 licensed PCs) saw the very highest infection rates. Among those businesses, 85.8% experienced a malware infection, and an average of 63 PCs were impacted.

*The larger a business grows, the more likely it is to become a target for malware infection.*

Attackers assume a large business has access to more data and money than a small business — and the more employees and systems a business has, the more weak points. But it’s noteworthy that malware infections tend to have a greater impact on smaller businesses. Though small businesses tend to see fewer infections overall, when they do experience them, it’s likely that a higher proportion of their end users will be infected. And this can have repercussions for the entire organization. Many of these smaller organizations also lack in-house cybersecurity and technology expertise, leaving them in a more vulnerable position, with limited response capabilities if an infection should occur.





Business Size by # of Licensed PCs	% of Businesses with Infections	Avg. Infections per Infected Business
 <b>1-20: Small</b>	6.4%	6
 <b>21-100: Medium</b>	28.5%	7
 <b>101-500: Large</b>	58.7%	17
 <b>501: Very Large</b>	85.8%	63

Figure 2: PC infection rates by number of licenses



## Infection Rates by Region

The infection rates of both business and consumer PCs vary depending on where in the world they're located (Figure 3). In 2022, PCs in Africa, Asia, South America, and the Middle East encountered over five times as many infections as PCs in Australia and New Zealand, Europe, Japan, and North America. The average rate of infection for PCs in the least-infected regions was 1.7%, compared to 9.0% in the most-infected regions. In our data, geographic location was the single most significant factor in determining an individual PC's probability of becoming infected with malware.

There were also pronounced regional differences in the infection rates of consumer versus business PCs.

- Africa, Asia, South America, the Middle East, and Europe saw 474% more infections in consumer PCs than Australia and New Zealand, Japan, North America, and the U.K.

- Consumer PCs in Africa, Asia, South America, the Middle East, and Europe saw an average malware infection rate of 12.1%. That's compared to 2.5% in the regions where infections were less prevalent (Australia, New Zealand, Japan, North America, and the U.K.).
- Business PCs in Africa, Asia, South America, and the Middle East averaged 447% more malware infections than those in Australia and New Zealand, Japan, North America, the U.K., and Europe.
- 6.0% of business PCs in Africa, Asia, South America, and the Middle East suffered malware infections, compared to only 1.3% of business PCs in Australia and, New Zealand, Japan, North America, the U.K., and Europe.

As these results show, Europe (minus the U.K.) is an interesting case study. Although it's among the group of regions with the lower infection rates when it comes to business PCs, it was one of the regions with the highest infection rates among consumer PCs.

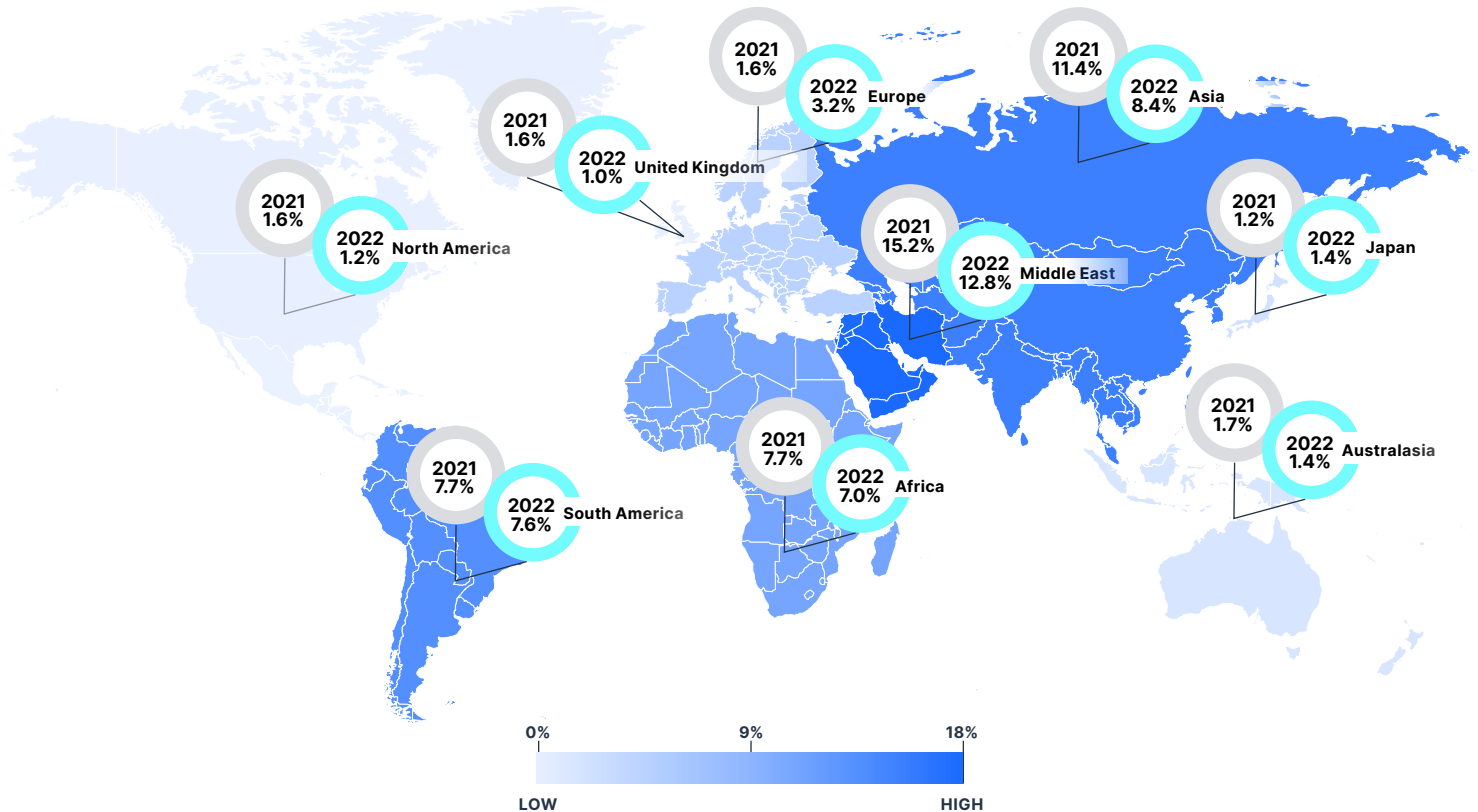


Figure 3: PC infection rates by region

## Infection Rates by Industry

About 34% of our business customers provided data on which industry vertical they're in. Figure 4 shows the percentage of businesses in each industry that encountered at least one malware infection in the last year. The average infection rate across all verticals was 13.1%, representing a minor decrease from last year's average of 16.8%. This year, the verticals with the highest infection rates were:

1. Manufacturing — 55.6% above average
2. Information — 33.3% above average
3. Public Administration — 32.0% above average
4. Management of Companies and Enterprises — 27.1% above average
5. Wholesale Trade — 25.1% above average

All except Management of Companies and Enterprises were also in the top five in our 2022 report, based on data from 2021. That year, Educational Services took the fifth spot.

Manufacturing was also the most frequently infected industry in 2021, and we expect to see this trend continue in 2023. Manufacturers may be more willing to pay ransoms than businesses in other verticals because of the high costs associated with downtime and production stoppages in that industry.

Management of Companies and Enterprises entered the top five for the first time in 2022. This may be part of a growing trend of attacks focused on service providers and supply chains. By targeting a single company, attackers can potentially gain access to systems belonging to many or even all of the client organizations the victim serves. With so many companies now reliant upon third-party software or services to support their operations, we expect these types of attacks to continue.

## How Malware Reaches its Targets

New to this year's report is an analysis of how malware reached the PCs it infected. Data collected by Zix reveals that email attachments remain a very popular vehicle for delivering malware. In total, 165 million emails were quarantined with malware attachments, representing 3.4%

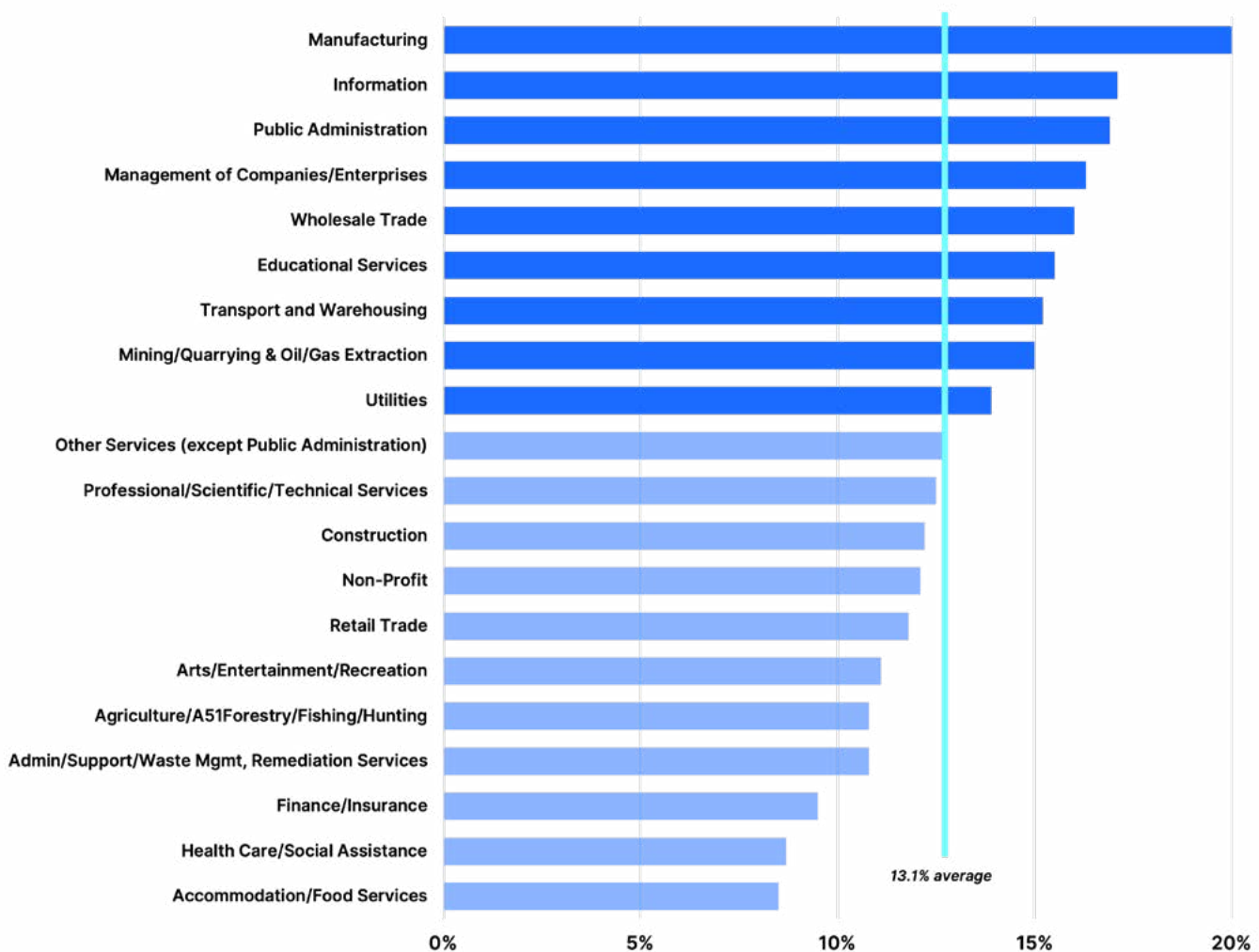


Figure 4: Infection rates by industry and deviation from average

of unwanted emails — a slight increase from 2021. The United States was the most common point of origin for these malicious emails.

Six common file types account for 88% of the files used as malicious email attachments. These include:

- .htm — 25.0% of malicious file attachments
- .zip — 22.5% of malicious file attachments
- .doc — 11.5% of malicious file attachments
- .pdf — 11.1% of malicious file attachments
- .xls — 10.8% of malicious file attachments
- .rar — 10.1% of malicious file attachments

Taken together, .htm and .zip files account for nearly half of the malicious files attached to emails. This marks a sharp turn away from .doc and .xls files, likely driven by Microsoft’s decision in early 2022 to automatically block the execution of macros from Microsoft Office files downloaded from the internet. With this in mind, it’s also notable that 40.4% of emails with malicious attachments sent in 2022 were sent within the first three months, compared to only 37.2% sent in the second half of the year. This could indicate that this move by Microsoft made it significantly more difficult for attackers to deliver malware as an email attachment.

## Where Malware Hides

Malware operators often try to conceal malware in places where it’s less likely to be noticed — typically in accessible locations that have many other applications or files stored within them.

In 2021, 83% of infections across all Windows PCs used one of four paths:

- %temp% — 37.8%
- %cache% — 18.7%
- %appdata% — 14.2%
- %desktop% — 12.6%

2022’s numbers were similar across two paths but significantly different for the other two:

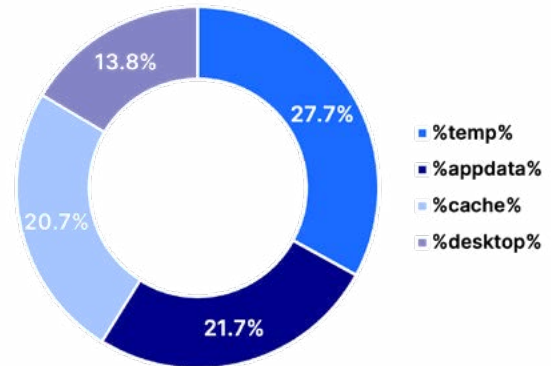
- %temp% — 30.4%, a 7.4% decrease since 2021
- %appdata% — 21.8%, a 7.6% increase since 2021
- %cache% — 18.4%
- %desktop% — 12.3%

Interestingly, uses of %temp% decreased by almost the same percentage as the use of %appdata% increased.

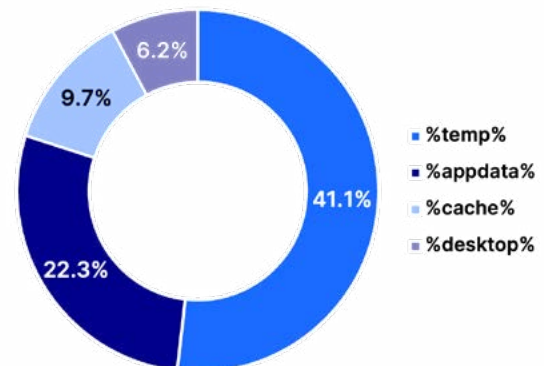
Taken together, this data suggests that users are being tricked into downloading malware voluntarily.

We observed significant differences in where malware hides on consumer PCs in comparison to those belonging to business users. The top four locations are the same as on all Windows PCs — but the order is different.

On consumer PCs, the most common paths used by malware in 2022 were:



In contrast, the most common paths used on business PCs in 2022 were:



This means that about half as many malware infections are found in %desktop% on business PCs as on consumer PCs. This is evidence that business users — particularly those who’ve had the advantage of security awareness training — are less likely to click on malicious links or agree to install malicious files where they can see them.

In 2021, %temp% was slightly more prevalent among malware infections impacting business users, used in 50.9% of infections. For context, last year, 19.7% used the %appdata% path, 8.4% used the %cache% path, and 5.6% of infections used the %windir% path. Use of %desktop% is on the rise even among business PCs — but malware infections targeting business PCs are still far more likely to use %temp% than any other file path, and infections making use of %desktop% remain a minority.



# Ransomware

Law enforcement secured several major successes in the ongoing international fight against ransomware platforms in the past year. In January 2022, the U.S. and Russia collaborated to shut down prolific cybercriminal gang REvil.<sup>1</sup> Almost exactly one year later, the FBI infiltrated the ransomware platform Hive and worked with international partners to shut it down.<sup>2</sup> In May 2022, ransomware group Conti voluntarily shut down and restructured after its support of Russia's invasion of Ukraine made it harder to secure ransoms.<sup>3,4</sup>

Meanwhile, stakeholders across several industries have claimed that the volume of new attacks being launched against them is on the decline, and some sources suggest that the rate of ransomware incident responses has decreased slightly. However, there's no evidence of a corresponding decrease in the number of organizations whose names are listed on public ransomware leak sites,<sup>5</sup> and the average ransom payment remains remarkably high. Despite these victories against high profile gangs, a decade since it first emerged, ransomware remains the most significant cyber threat facing small and midsize organizations. Ransomware groups continue to experiment and evolve their tactics amidst an ever-changing and very active threat landscape.



*With Ransomware now turning 10 years old, it's been a wildly successful 'business model' for cybercriminals. The growth of extortion leak sites among ransomware gangs is a worrying trend showcasing the chase for profits. The damage to victims is twofold as the cost of non-compliance with data privacy regulations and damage to the brand can be even more devastating than disruption from ransomware, especially for larger organizations. It has become more attractive to just pay the ransom and sweep the entire incident under the rug.*

**Tyler Moffitt**  
Senior Security Analyst  
OpenText Cybersecurity



Geopolitical unrest often fuels cybercrime. Russia’s invasion of Ukraine and political tensions over the Taiwan Strait and North Korea provided a tumultuous backdrop that may well escalate and will likely have repercussions in the ransomware world for some time to come.

In the weeks after Russia invaded Ukraine in February 2022, there was widespread concern that pro-Russian cybercriminals would attempt to interfere with critical Ukrainian infrastructure and that these threats would subsequently spread beyond Ukraine’s borders, as happened with NotPetya in 2017.<sup>6</sup> Although this didn’t come to pass in 2022, it’s possible that the masterminds behind currently inactive ransomware groups have already redirected their attention to Russia’s war effort, planning attacks and misinformation campaigns against the Ukrainian government and its supporters, including the U.S. and members of NATO.

With as many as 84% of ransomware attacks now including threats of data leakage,<sup>7</sup> a growing number of cybercriminal groups appear to be foregoing encryption entirely and simply stealing data and threatening to publish it. This strategy eliminates the need for expertise in cryptography, storing and managing decryption keys, and the ability to deploy file-encrypting malware across an organization’s entire infrastructure.

The Lapsus\$ group rose to prominence as an extortion-only operator. Their first major target was Brazil’s health ministry in late 2021, and in 2022 they targeted major technology companies, including Nvidia, Samsung, Microsoft, and Okta.<sup>89</sup> They stole and occasionally leaked data, including product designs and source code.

At around the same time, data extortion group Karakurt emerged as a threat, using similar tactics. Rather than encrypt the files they hack into, they typically send their victims screenshots of the confidential data as proof of the hack and attempt to extort payments ranging from \$25,000 to \$13 million in Bitcoin.<sup>10</sup> Unlike Lapsus\$, Karakurt has so far focused on smaller organizations, which allows them to move faster.<sup>11</sup>

Victims of these attacks often find themselves weighing impossible trade-offs. On the one hand, paying criminals encourages them to continue their nefarious activities. On the other, paying the ransom may be the only way to prevent the attackers from leaking the data, and to avoid public disclosure of the breach, which can have painful consequences. For example, a data breach can damage a brand’s reputation and erode customer trust — sometimes so irreparably that the company may not survive. Data regulators may also fine companies for failing to protect their customers’ data. In some cases, these fines are higher than the ransom. Unsurprisingly, there’s little to no evidence that fines for breaches or ransomware attacks do anything other than incentivize victims to reward attackers by paying the ransom.



Figure 5: Ransom Payments by Quarter<sup>17</sup>

## Rising Ransom Costs

Over the past few years, average and median ransom payments have skyrocketed, hitting record highs by the end of 2022.

---

*At the end of 2018, the average ransom payment was \$6,733.<sup>12</sup> Over the next 12 months, it multiplied to \$84,116,<sup>13</sup> only to grow to \$154,108 by the close of 2020<sup>14</sup>. A year on, at the end of 2021, the average ransom payment had more than doubled, reaching \$322,168.<sup>15</sup>*

---

Interestingly, that number dropped dramatically over the next few months, to just over \$200,000 by the end of the first quarter of 2022. It rose again — to \$288,125 — in the middle of the year.<sup>16</sup> And by the end of Q4, average ransom payments had hit their peak of \$408,643. This volatility somewhat mirrors the price of Bitcoin, which is often used to pay ransoms. However, whereas ransom prices rose over the course of 2022, Bitcoin hadn't recovered its value by the end of December.

It was a similar story for median ransoms, which rapidly increased from \$49,450 in 2020 to \$117,116 in 2021 before sinking to \$36,360 in Q2 of 2022 and then shooting up to an all-time high of \$185,972 by the end of 2022.<sup>17</sup>

This volatility does not necessarily indicate fluctuations in the severity of the threat posed by ransomware. Rather, it's evidence that ransomware groups and their affiliates are increasingly targeting smaller companies, against whom they can launch less risky, lower-profile attacks. Even if each individual payment is smaller, launching such attacks can be enormously profitable if done at great volume. These lower numbers may also indicate that some larger organizations are simply refusing to pay ludicrously high ransoms.

For many ransomware attackers, small and mid-sized organizations are now the most attractive target. With their budgets under pressure from rising inflation, many of these companies have been forced to cut costs on their cybersecurity programs, leaving them potentially ill-equipped to deal with an attack — but still with enough cash to make it worthwhile to the criminals. Ransomware operators may also believe that smaller organizations are less likely to involve law enforcement than major enterprises, which are more likely to be familiar with reporting mechanisms and better aware of how to get support from authorities.

---

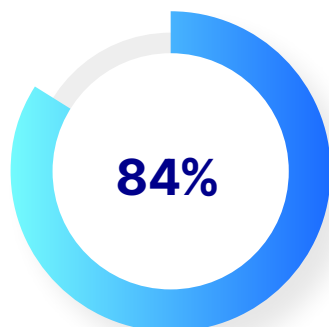
*In response to the skyrocketing mean cost of ransom payments, cyber insurance also climbed in price.<sup>18</sup>*

---

The increased costs associated with both ransoms and losses have insurers asking tougher questions about security controls, internal processes, and risk mitigation efforts before issuing a policy. They're also looking at relationships with third-party contractors and vendors. Some insurers are exiting the market entirely, with the CEO of Europe's largest insurance company warning that cyber risks are on the verge of becoming "uninsurable."<sup>19</sup>

## Ransomware Gangs

In 2022, cybersecurity professionals celebrated the apparent end of two of the highest-profile ransomware gangs. REvil, also known as Sodinokibi, was reported to have ceased operations after Russian law enforcement authorities — acting on information from the U.S. — announced the arrest of 14 alleged members of the group.<sup>20</sup> However, that was in January, before Russia invaded Ukraine, and it's thought that the subsequent breakdown of cooperation between the U.S. and Russia may have prompted the latter to release the suspects.



**of ransomware attacks now including threats of data leakage**



Later in the year, the highly professionalized ransomware-as-a-service (RaaS) operator Conti took its platform and negotiation infrastructure offline after an archive of its internal communications was leaked to Twitter.<sup>21</sup>

But that's likely not the end of either group. Although crackdowns on cybercriminal groups may result in a brief lull in activity, they often reform as new outfits. Conti may have dismantled its operations, but it's more of a rebranding than a disbanding. Ransomware gangs bolstered by former Conti members include BlackCat, AvosLocker, and Hive, which was shut down by the FBI and its partners in early 2023. Meanwhile, other former Conti members are involved with extortion-only operations, such as BlackByte and Karakurt.<sup>22</sup>

REvil looks to be similarly slippery-yet-robust. Threat researchers have since identified REvil samples in the wild, including during a period when group members were still purportedly being held by Russian authorities.<sup>23</sup> Some have suggested that the members who were apprehended were probably lower-level affiliates and distributors rather than top-level masterminds. By now, it's likely that they're back in action, and they may even have been deployed by

Russia in its war against Ukraine. As we have seen with TrickBot and Emotet, there's little reason to believe that these apparent shutdowns will be permanent.

---

*Threat researchers have reported that the LockBit RaaS scheme was the most active ransomware operation in 2022, publishing the names of nearly 900 victims to its public leak site in the first half of the year.<sup>24</sup>*

---

Not only have LockBit's operators targeted more victims per month than any other named malware strain in the past year, but they've also displayed a remarkable flair for innovation. After their own servers were taken offline by a distributed denial-of-service (DDoS) attack, LockBit's operators pioneered the use of triple-extortion tactics, in which data encryption is combined with both data leakage and DDoS attacks to increase the pressure on the victim.<sup>25</sup> This tactic has yet to gain widespread traction, but it's still relatively new and may become more mainstream in 2023.



Hive waws shutdown by a multi-national law enforcement collaboration

---

*LockBit also became the first known ransomware gang to start a bug bounty program. The bounties on offer for new zero-days and other vulnerabilities range from \$1,000 all the way to \$1 million, with the top reward reserved for anyone who can dox the gang's leader.*

---

These values dwarf those of legitimate software vendors and crowdsourced software testing services, potentially incentivizing security researchers with questionable ethics to use their talents for evil.<sup>26</sup> As long as legitimate technology companies are unwilling to match these bounties, criminals will have early access to exploits, giving them time to perfect their tactics before the vulnerabilities are made public, and cybercrime will retain its allure.

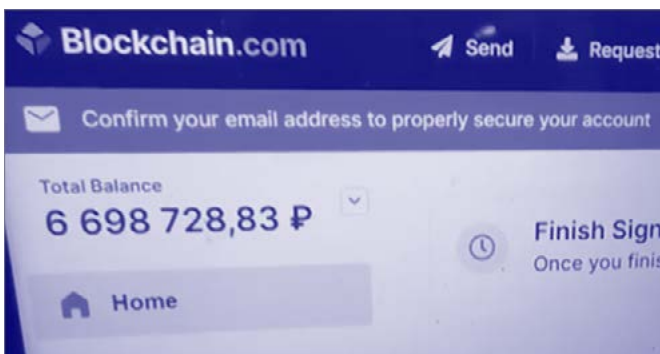
Unlike many of its cybercriminal peers, LockBit did display a degree of compassion and discrimination in selecting their targets. When an affiliate targeted the pediatric teaching and research hospital, the Toronto Hospital for Sick Children (SickKids), the ransomware gang apologized, announcing that they'd provide the organization with the decryptor for free and would expel the perpetrator from their affiliate program.<sup>27</sup>

## Ransomware Methods

As in previous years, the bulk of ransomware continues to spread through multi-stage malware attacks. In most cases, the malware is delivered through phishing campaigns. In the first stage, the user is tricked into clicking on a malicious attachment or link, which infects the computer with a botnet client that gives the attacker command and control capabilities. In the next stage, the attacker leverages the botnet client to install malware that enables them to move laterally and perform reconnaissance within the organization before infecting the environment with ransomware.

However, in 2022, threat researchers observed increased usage of living off the land (LotL) techniques, in which threat actors abuse otherwise benign applications to execute malicious payloads disguised as legitimate processes.<sup>28</sup> Another technique that grew in popularity was the dynamic-link library (DLL) side-loading, in which the attackers execute malicious DLLs from within legitimate, trusted applications, often with elevated system privileges.

Threat researchers have also observed that ransomware attackers are further diversifying their tactics. Some groups have embraced the use of new programming languages, such as Rust and Go, which can make file detection more difficult. It can also make it easier to compile the malware so that it will run on different operating systems or platforms.



*Russian authorities arrested members of the REvil gang and seized their computers and other assets*

This speaks to the fact that ransomware no longer focuses exclusively on Windows. Researchers have observed new ransomware families (including RedAlert and Luna) and a LockBit variant that can all encrypt both Windows and Linux-based systems.<sup>29</sup>

In 2022, ransomware gangs also concentrated their efforts on developing malware that can encrypt files at record speed.

---

*LockBit's operators have boasted that their ransomware can encrypt files faster than any other, a claim that security researchers have validated. It took just four minutes and nine seconds for LockBit to encrypt 53.83 GB of files across different Windows operating systems and hardware configurations.*<sup>30</sup>

---

When ransomware performs encryption at such blazing speeds, the amount of time between gaining an initial foothold in an environment and full deployment shrinks from weeks to days or even hours. This means that once adversaries are inside a network, it can be near-impossible for defenders to prevent large-scale encryption.

Ransomware groups have also maintained their focus on unpatched vulnerabilities. While we have not seen exploits at the scale of WannaCry and NotPetya in 2017, we have seen ransomware spread through exploitations of critical vulnerabilities and exposures (CVEs). After CVE-2022-41080 and CVE-2022-41082 were published in November 2022, the authors of Play ransomware began leveraging these vulnerabilities to achieve remote code execution on unpatched Microsoft Exchange Servers.<sup>31</sup> The impact was widespread, with cloud computing company Rackspace becoming the best-known victim.<sup>32</sup> This tactic is nothing new, and there's little doubt that it will continue to be effective for the foreseeable future.

# Thwarting Ransomware Through Cyber Resilience

Ransomware can infect systems in many different ways, and we're confident that attackers will continue diversifying their techniques in 2023. Organizations must adopt a multi-layered strategy to protect themselves from as many potential attack strategies as possible. Ransomware attackers can often breach individual layers – but usually not all of them at the same time. By tactically combining overlapping protections, companies can significantly reduce the risk that an attack will succeed.

At a minimum, every organization should:

- Inspect all incoming emails for malicious attachments and block potential threats.
- Keep all PCs and servers fully patched.
- Run effective antivirus and endpoint protection software on every device on the network and within the organization.
- Train users on how to spot phishing emails and avoid other types of social engineering.
- Back up all critical systems and files regularly.

Even organizations with exceptionally thorough vulnerability management programs cannot expect to avoid all infections. That doesn't mean there's no point trying — it means shifting the focus to cyber resilience, not just prevention. Cyber resilience involves taking steps to avert attacks while also preparing your organization to respond to ransomware attacks that slip through the cracks. For this reason, cybersecurity teams should:

- Have a robust incident response plan ready, so they can act quickly to stop an initial infection from spreading.
- Develop and test backup capabilities, so you can be confident that you can restore your critical systems and data in time to protect the continuity of your operations.
- Re-evaluate your cyber resilience plan on a regular basis to ensure that it reflects the most prevalent current threats.



# High-Risk URLs

Online cybersecurity threats continue to emerge at an alarming pace. New malicious websites come online daily, while legitimate sites are occasionally compromised and co-opted for nefarious purposes.

High-risk URLs host phishing sites, keyloggers, botnets, spyware, drive-by malware, and other types of malicious software. They can also receive traffic relayed from spam messages, and may be hidden behind proxy servers or anonymizers in order to bypass URL filtering.

We collected data on more than 87 billion unique URL visits in the past year. The BrightCloud® Web Classification Service averages more than 4.5 billion requests per day and constantly categorizes URLs based on their website's behavior, history, age, popularity, location, networks, links, and real-time performance. The service constantly updates its categorizations to determine which URLs are high-risk and what nefarious behavior is associated with each one.



“

*Smishing will continue to rise because mobile phones are higher risk from a BYOD perspective. Attackers typically use a familiar sender name and use shortener links that redirect to malicious pages, eliminating the ability to gauge legitimacy without clicking on them. We've seen smishing attacks contain accurate PII, likely obtained via a dark web sale, as well as health-related smishing. There is also smishing that uses long-known techniques like User-Agent blocking, which when opened on a web browser do not load, and therefore are more difficult to detect and verify.*

**Serena Peruzzi**  
Sr. Manager, Research & Development  
OpenText Cybersecurity

”

## URL Classification

Of the malicious URLs we observed, 90.9% fell into one of three categories:

1. Phishing
2. Hosting malware
3. Proxy avoidance and anonymization

The graph below shows month-to-month fluctuations in the number of malicious URLs used for each of these three purposes over the past year. The values indicate how much the actual number of URLs exceeded or fell below the average for the year, which is indicated by 0%.

As was also the case in 2021, the number of phishing URLs remained relatively stable, fluctuating by no more than 30% above or below the average. Approximately 74.9% of the high-risk URLs we discovered were used for phishing, which is fairly consistent with last year's numbers. However, the total number of URLs used for phishing increased by 29.6% between 2021 and 2022 — from 2.7 million to 3.5 million. The number of malware URLs was more dynamic, peaking more than 60% above average early in the year and plummeting to more than 50% below average by midyear.

The number of URLs used for proxy avoidance and anonymization was less dynamic, remaining within 15% of the average for most of the year, with the exception of a period of less activity in late summer and early fall, when the number of URLs used for proxy avoidance fell as low as 50% below average.

We can't pinpoint specific events that might have caused these shifts. We do know, however, that attackers are quick to pivot, rapidly changing their tactics to take advantage of newly-discovered vulnerabilities, capitalize on trends, or make use of changing user habits.

## Malicious domains

2022 was the first time we collected data on the number of high-risk URLs found on each malicious domain. On average, each malicious domain hosted 2.9 malware URLs, compared to only 1.9 phishing URLs per domain. This apparently reflects the fact that it takes more effort and investment to host malware than to set up a phishing site. Plus, phishing site operators are constantly shifting to new URLs to avoid detection, resulting in a rapid churn rate.

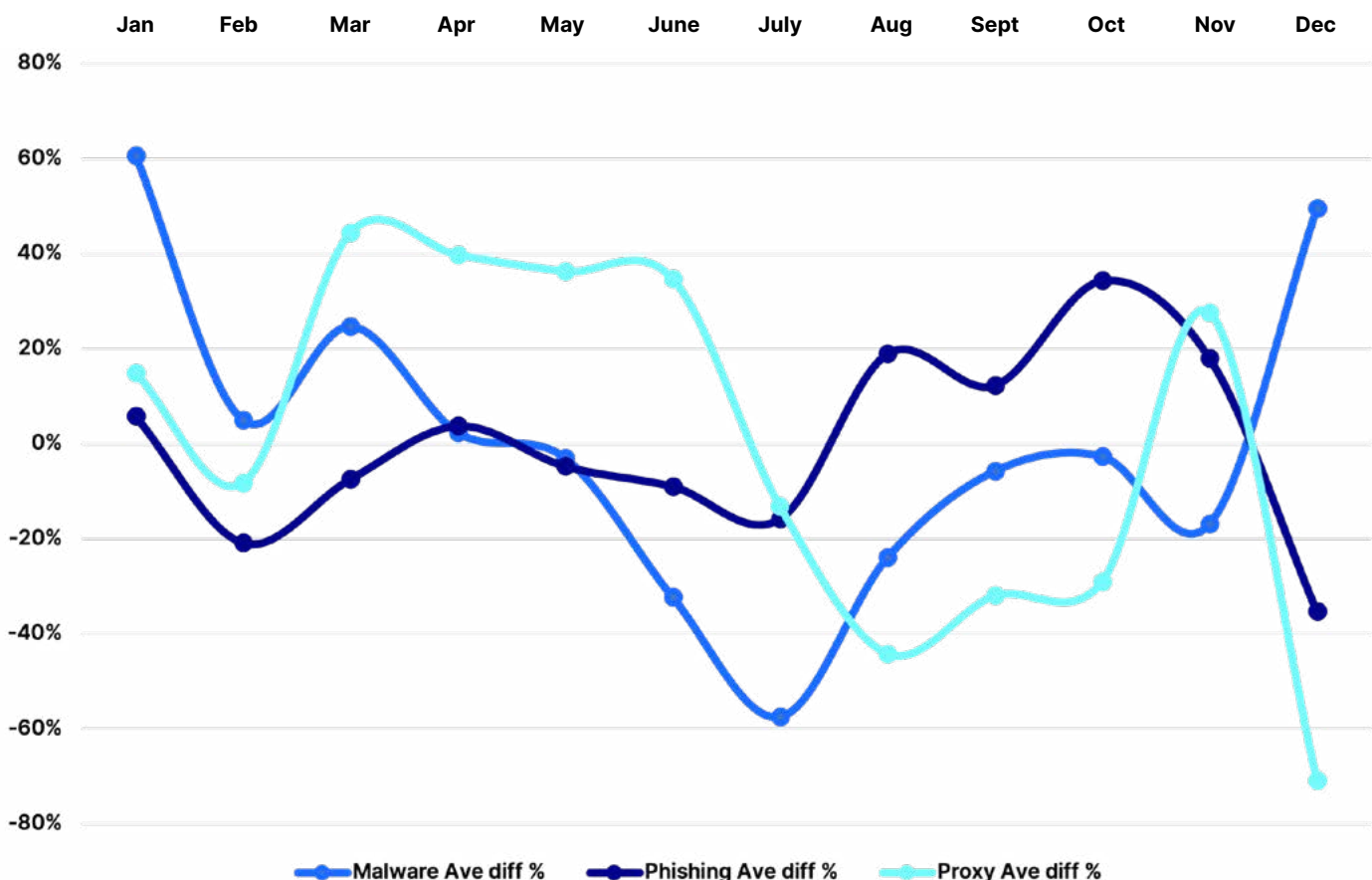


Figure 6: Trends in high-risk URL classifications

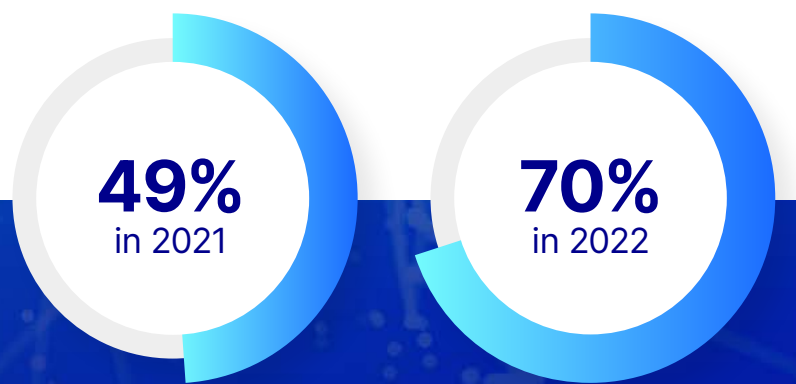


## Location-masking

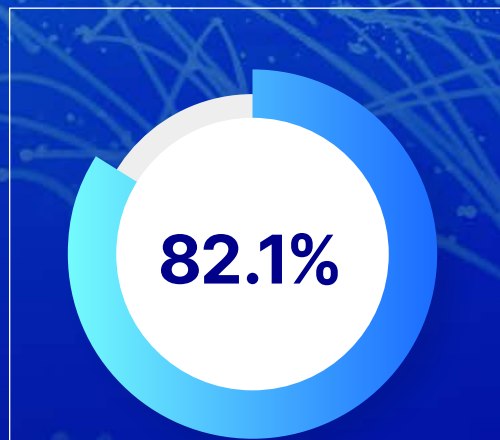
One notable trend from the past year is a significant increase in evasive techniques concealing the location of URLs hosting malware and phishing sites.

The percentage of malicious URLs hidden behind a proxy or geolocation-masking service increased 36% over 2021's numbers. That year, only 49% of high-risk URLs were obfuscated in this way, compared to 70% in 2022. This increase indicates that masking a malicious URL's location is now easier than ever — and that more attackers may have learned how to do it.

Location-masking is especially prevalent among high-risk URLs hosting malware. Among the high-risk URLs we observed, 82.1% of those hosting malware were concealing their geolocation, compared to two-thirds of phishing sites. It's likely that at least some phishing sites deliberately advertise their location — particularly if hosted in a "known-good" country like the U.S. — so that traffic to them won't be blocked by geography-based filtering.



**The percentage of malicious URLs hidden behind a proxy or geolocation-masking service increased 36% over 2021's numbers.**



**of malware hosting URLs mask the geo location**



## Geographical Distribution

Whenever we discover a new high-risk URL, we try to identify the country hosting it. For a long time, the majority of high-risk URLs have been hosted within a small number of countries. Now, however, it's difficult to determine whether that's still the case since, today, the majority of malicious or suspicious URLs are hidden behind proxies or location-masking services.

Of all the malware-hosting URLs detected, we were able to determine the country of origin in 16% of cases. Of these, the top five countries hosting the most were:

1. The U.S. — 56.7%
2. India — 5.4%
3. Germany — 4.9%
4. China — 4.3%
5. Russia — 2.2%

These five countries collectively hosted nearly three-quarters (72%) of all the malware URLs for which we could determine the country of origin. As you can see, the vast majority were located in the U.S. — a trend that's been consistent over the past few years. That proportion has increased from 44.3% in 2021.

The U.S. also stands out when it comes to hosting phishing sites. Of the phishing sites with a known location, most were in these five countries:

1. The U.S. — 63.0%
2. Germany — 5.0%
3. Netherlands — 4.3%
4. Russia — 3.2%
5. Hong Kong — 2.4%

---

*It's not surprising that the majority of these phishing sites are hosted in the U.S. since that's where most of our customers are based, and attackers operating phishing campaigns may deliberately choose U.S.-based hosts in order to evade location-based filtering.*

---

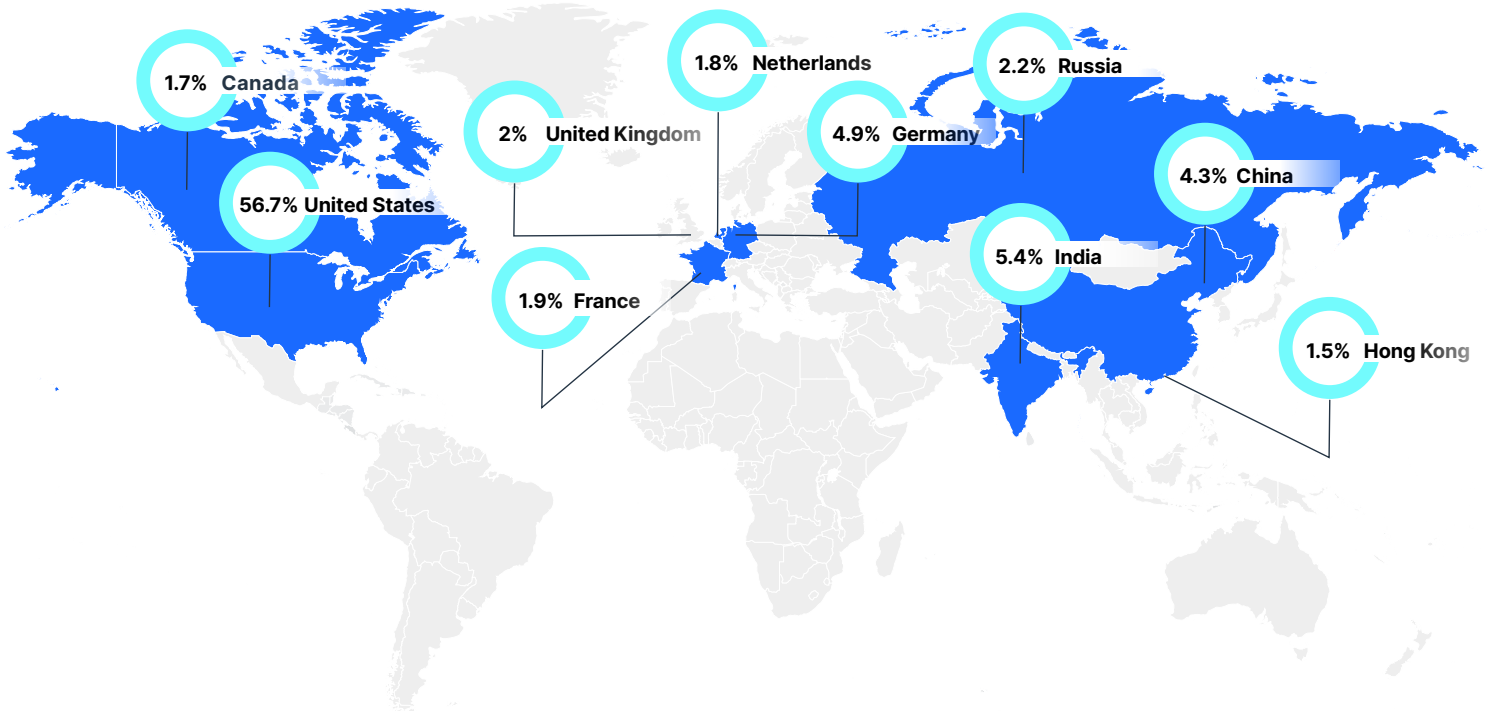


Figure 7: The top 10 countries hosting the majority of high-risk URLs in 2022

# Phishing Attacks

Phishing attacks enable threat actors to acquire credentials, deploy malware payloads, and evade security protections in order to gain a foothold within a victim's environment. Phishing campaigns remain among the most popular methods for delivering ransomware and capturing credentials, often via email, text messaging (SMS), and call center communications. As we mentioned in the previous section, just under three-quarters of the new high-risk URLs we observed over the past year were being used to host phishing sites. In 2022, phishing attackers were as creative, persistent, and skillful as ever.

As phishing messages and websites have become more sophisticated, it's gotten increasingly difficult for users to tell them apart from legitimate communications. Although phishers continue to use common tactics such as business email compromise (BEC), they also continually look for new ways to deceive their victims.



*With the increased use of voice-based technology and AI, phone-based social engineering scams will become even more convincing and therefore, more effective. We expect to see an increase in call center scams, similar to what happened to Uber, as it is easier than ever to pre-assess vulnerable employees.*

**Serena Peruzzi**  
Sr. Manager, Research & Development  
OpenText Cybersecurity



For example, growing numbers of phishing attacks are weaponizing legitimate services, a tactic known as living off the land (LotL). In these attacks, threat actors make use of a known and trusted URL that redirects to a malicious site or hosts the phishing payload itself. Since these services are used for a broad array of legitimate purposes, they cannot be blocked outright. Plus, names like Google and Amazon Web Services (AWS) lend an air of credibility to the phishing email.

In another example of creative phishing, threat actors continue to capitalize on current events to pressure victims into complying. For example, they send malicious emails posing as security patches after highly-publicized software supply chain attacks and use pandemic-related shipping delays to pose as major shipping companies.

---

*Given how much phishing relies on deceiving recipients, a multilayered approach is the most effective way to reduce risk, combining security awareness training for end users with anti-phishing technologies.*

---

In 2022, the Webroot Web Threat Shield browser extension evaluated more than 87 billion URLs. It was able to protect the 7.2% of our users who unwittingly tried to access a phishing site, and the 14.0% who unknowingly tried to access malicious content by blocking them from proceeding.

## Phishing Volume

Figure 8 shows the volume of phishing attacks we observed during each month of 2022. The results are similar to what we saw last year.

Phishing attack volumes typically follow a seasonal pattern. As with 2021, 2022 got off to a fairly slow start, with only 23.4% of the year's

total phishing activity taking place during the first quarter. Activity often peaks around income tax filing deadlines in the U.S., and this trend continued in 2022, with 10.0% of the year's phishing activity observed during April alone.

As expected, most of the summer was relatively quiet, aside from the back-to-school shopping season in August. This prompted the third-highest peak of phishing attacks, with 9.6% of 2022's phishing activity taking place during that month.

As we'll see, phishing attacks often spike in periods of high online consumer spending. To attackers, more people shopping means a higher chance of finding victims who will fall for their scams. The increase in legitimate email marketing activity around these times can make people less cautious about opening emails, and attackers also use SEO-based tactics to place fake shopping sites high in search results. In both cases, they lure victims in with deals that look too good to miss but are really too good to be true -- scams aiming to collect credit card numbers and account details.

Given this, it's not surprising that another common seasonal pattern sees October and November — the start of holiday shopping — among the most active phishing months of the year. This pattern continued in 2022, with 10.3% of the year's phishing activity taking place in October and 9.4% in November. It's also worth noting that the U.S. held its midterm elections on November 8, 2022. Phishing attackers have responded to increasing political polarization by incorporating election-related messaging into their websites and campaigns.

## HTTP and HTTPS Usage

In our analysis, we keep track of which phishing URLs use HTTP and which use HTTPS. Many users incorrectly believe that HTTPS sites are "secure" and that the padlock displayed in the browser is evidence that the site is legitimate. Attackers are well aware of this popular perception, so they register domains, acquire certificates for them, and establish malicious websites using these certificates.

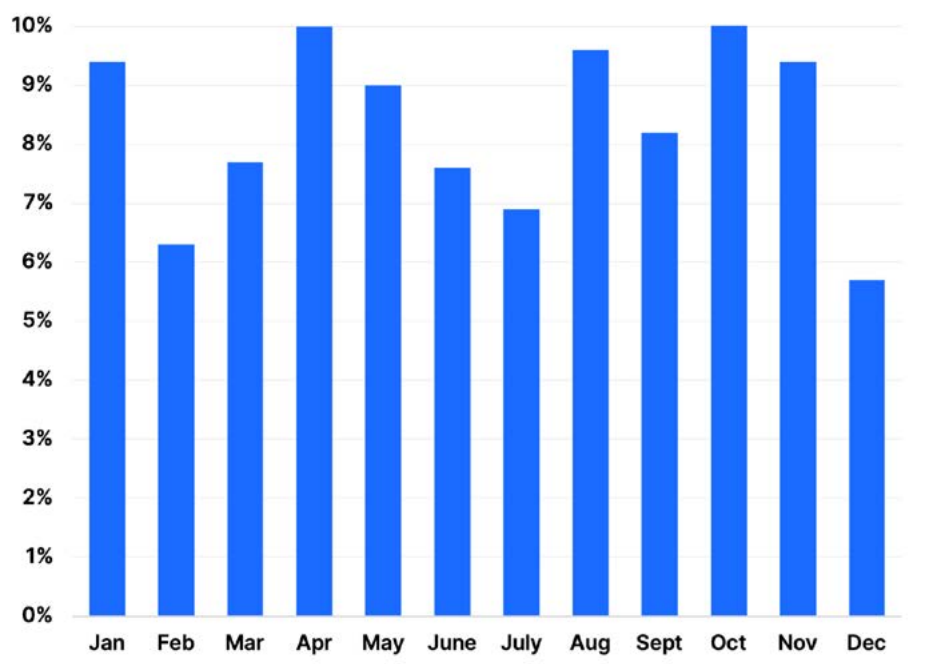


Figure 8: Phishing attacks by month in 2022



This explains why the number of phishing sites using HTTPS grew sharply in 2022. Figure 9 shows a month-by-month breakdown of the percentages of HTTP and HTTPS sites used in phishing attacks each month. On average, in 2021, only 32% of the phishing sites we detected used HTTPS, whereas in 2022, this average percentage grew to 49.3%. This marks a 55.5% year-over-year increase. The uptick in phishing sites with HTTPS URLs proves that domain registrars and certificate-issuing authorities are becoming less effective at preventing criminals from obtaining these credentials.

It's worth noting that with a few exceptions, the ratio of HTTPS to HTTP sites climbed throughout 2022. From this trend, we can extrapolate changes in the ways attackers are approaching phishing. While the April spike in phishing activity was accompanied by a corresponding drop in HTTPS usage, the October and November increases in phishing activity also saw the years' highest

HTTPS adoption rates. This may indicate that during the course of the year, attackers recognized the value in playing on users' perception of HTTPS URLs as secure and started to rely on these URLs over HTTP URLs during periods of peak phishing activity.

### The Most Impersonated Companies

We keep track of more than 200 brands in order to identify which are being imitated on phishing sites. Phishing attackers sometimes mimic real brands' communications to trick customers into thinking they're interacting with a trusted organization. That said, although we observed millions of real-world phishing attempts in 2022, in 88.2% of attacks, we didn't detect a brand that matched the 200+ that we track.

Phishing campaigns that work by impersonating particular brands typically imitate the same handful of companies every year, although

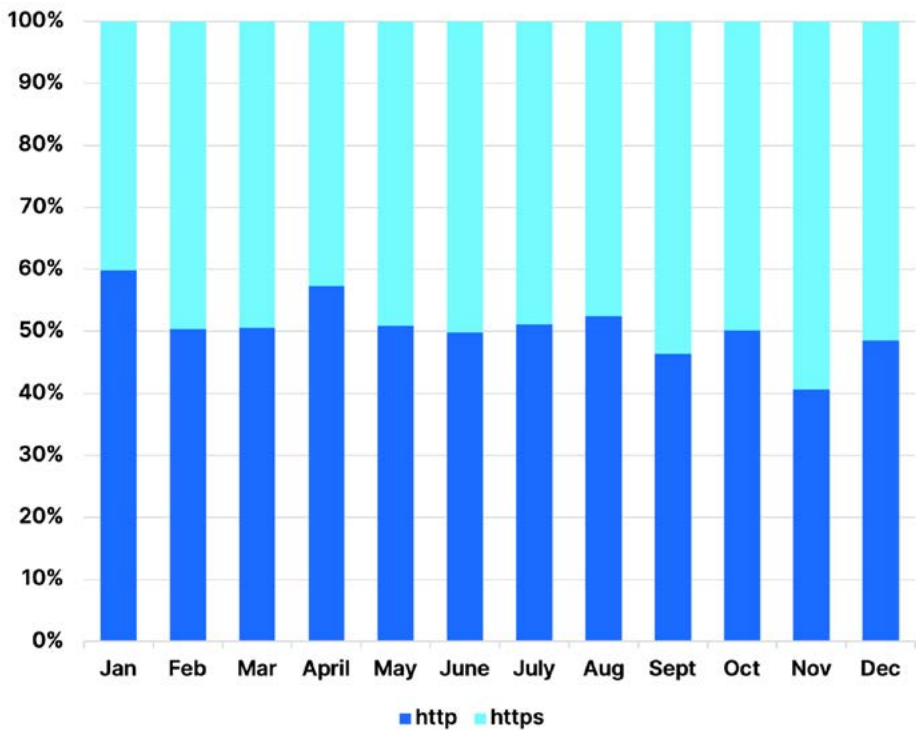
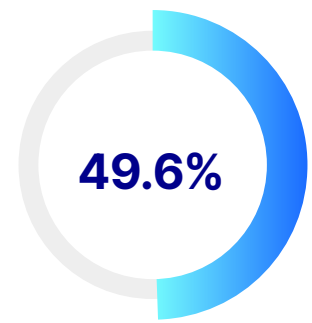


Figure 9: HTTP/HTTPS usage in phishing attacks by month



**In 2022 the top five brands accounted for 49.6% of attacks that were associated with a recognizable brand.**

there are notable changes in the order of popularity. The top five targeted brands in 2022 were:

1. Facebook — 14.9% of detected attacks
2. Google — 12.9%
3. Apple — 10.0%
4. Instagram — 7.1%
5. Microsoft — 4.8%

Taken together, these five brands accounted for 49.6% of attacks that were associated with a recognizable brand. All except Instagram were in the top five in 2021 as well. That year, Instagram was the tenth most-impersonated brand in phishing attacks, accounting for only 1.9% of detected attacks associated with a brand. The increase in Instagram imitations appears to correlate with increases in the number of monthly active users on the platform.

In contrast, YouTube accounted for 11.8% of the phishing attacks associated with a known brand in 2021, placing it in the top five, but fell out of the top 10 in 2022. Attackers track trends and imitate the brands that are gaining the most traction at a given moment, pivoting quickly as circumstances change.

Figure 10 shows how many HTTP and HTTPS sites were used in phishing campaigns in which a particular brand was impersonated. Facebook was both the most-impersonated brand and the one most often associated with HTTPS sites. Of all the sites impersonating Facebook, 61.6% used HTTPS. In fact, six of the top 10 most-impersonated brands were associated with a larger number of HTTPS sites than HTTP sites. This is another indication that HTTPS hosting is inexpensive and easy for cybercriminals to achieve. The certificate authorities who issue TLS certificates are somewhat to blame for this lapse. Stricter regulations will likely be needed before we see improvements in this area.

## Email-Based Phishing Attacks

For the first time, this year’s report considers data collected by the email security platform Zix in its analysis of phishing attacks. The Zix platform examined more than 13 billion emails in 2022. Approximately 56% of that traffic was unwanted emails, including spam, phishing, and email with attached malware. This represents an increase of 12.5% over 2021’s numbers. Of those 7.3 billion unwanted emails, over 1 billion were classified as phishing. Even though this means phishing represents a minority of unwanted emails, this is still an incredibly high number, demonstrating the enormity of the scale at which phishing activities are conducted today.

Email-based phishing attacks tend to also follow a seasonal pattern, with activity peaking between September and November. However, the highs and lows vary less dramatically than is seen with overall phishing attack volumes. This reflects the fact that email-based phishing requires minimal effort, so attackers can maintain relatively consistent levels all year.

The top three months for email-based phishing attacks in 2022 were:

- November — 9.9%
- October — 9.2%
- March — 9.1%

Spear phishing — highly targeted phishing campaigns tailored to specific individuals or groups — increased significantly in 2022. We observed a 16.4% year-over-year increase in spear phishing email traffic, which now accounts for approximately 8.3% of all email traffic.

Where possible, we also looked at the country of origin for email-based phishing attacks. The top five most common locations were:

1. The U.S. — 50.0%
2. China — 12.6%
3. The Netherlands — 9.4%
4. Brazil — 5.2%
5. Russia — 4.4%

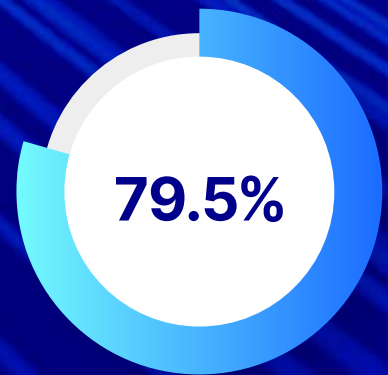
It’s likely that U.S.-based companies are the top target for email-based phishing attacks because there are so many of them, and because they are perceived as having deep pockets, meaning a successful breach will potentially generate large profits. In addition, phishing attackers often favor the U.S. as a launch location because it’s harder to defend against attacks from here since simple geography-based blocking doesn’t work.

Top 10 in 2020		Top 10 in 2021		Top 10 in 2022	
<b>eBay</b>	13.2%	<b>Apple</b>	13.0%	<b>Facebook</b>	14.9%
<b>Apple</b>	10.2%	<b>Facebook</b>	12.1%	<b>Google</b>	12.9%
<b>Microsoft</b>	9.5%	<b>YouTube</b>	11.8%	<b>Apple</b>	10.0%
<b>Facebook</b>	8.8%	<b>Microsoft</b>	9.1%	<b>Instagram</b>	7.1%
<b>Google</b>	8.6%	<b>Google</b>	9.1%	<b>Microsoft</b>	4.8%
<b>Steam</b>	7.9%	<b>Amazon</b>	8.9%	<b>PayPal</b>	4.3%
<b>Chase</b>	5.4%	<b>PayPal</b>	3.3%	<b>Target</b>	2.9%
<b>Amazon</b>	4.7%	<b>La Banque Postal</b>	2.7%	<b>Netflix</b>	2.4%
<b>Netflix</b>	3.0%	<b>Target</b>	2.5%	<b>Amazon</b>	2.3%
<b>PayPal</b>	3.0%	<b>Instagram</b>	1.9%	<b>Steam</b>	2.2%

Figure 10: Companies most often impersonated in phishing attacks

# Malicious IP Addresses

BrightCloud tracks IP addresses that have been associated with malicious activities, so we can prevent them from committing further attacks. The average number of active threat IPs in existence in 2022 was 7.9 million, an increase in 2021's numbers. Churn was up, too, with approximately 1.3 million malicious IPs appearing and disappearing each month. This reflects the fact that attackers often bounce between different IPs to evade block lists. They use each IP for a short period, then pause activity on it and switch to another, and later return to the original. The theory is that during each pause, the lack of malicious activity will be enough to convince cybersecurity services that the IP is now safe so they will remove it from block lists — hence churn. Although we expected results along these lines, these numbers nonetheless represent an enormous amount of nefarious activity.



**of malicious IPs observed in 2022 were convicted in only two or three categories**



We've honed in on the 50,000 most active IP addresses — i.e. the ones associated with the highest number of malicious behaviors, including hosting spam, Windows exploits, web attacks, botnets, scanners, phishing, proxies and anonymizers, mobile threats, and Tor proxies. We refer to each detected instance of one of these behaviors as a conviction. Over the course of 2022, the 50,000 IP addresses associated with the most convictions had 46.4 million convictions, a 12.8% increase from what we observed among the IP addresses associated with the most convictions in 2021.

### Performing Multiple Bad Behaviors

The rate of malicious activity attributable to the top 50,000 malicious IPs continues to grow — but most of these malicious IPs are limited to just a few bad behaviors. Although all of these 50,000 IPs were convicted in at least two different behavior categories over the course of 2022, 79.5% were convicted in only two or three, and just 1.75% were observed performing malicious behaviors in five or more categories.

The trend towards fewer behaviors per top malicious IP address has been consistent over the past few years. In 2021, 3.5% of the IPs in the top 50,000 were convicted for activities in five or more behavior categories. This suggests that attackers are trying to avoid detection by conducting fewer types of malicious activity from each individual IP address.

Figure 11 shows the number of convictions by category for the top 50,000 malicious IPs. The five most prevalent behaviors were:

- Serving as a source of spam — 24.9%
- Hosting phishing sites — 23.6%
- Hosting Windows exploits — 17.8%
- Hosting scanners — 16.2%
- Operating proxies — 9.5%

Spam has been the most common malicious behavior for a few years now, but the figure for 2022 is down quite significantly since 2021 when it accounted for 30.0% of convictions. More stable were the proportions of the top 50,000 most active malicious IP addresses hosting Windows exploits, proxies, and botnets:

- In 2022, Windows exploits accounted for 17.8% of convictions among the top 50,000 malicious IPs, compared to 19.7% in 2021.
- In 2022, 9.5% of the top 50,000 malicious IP addresses were convicted for hosting proxies, compared to 11.5% in 2021.
- In 2022, 4.5% of the top 50,000 malicious IP addresses were convicted for hosting botnets, compared to 4.4% convicted in 2021.

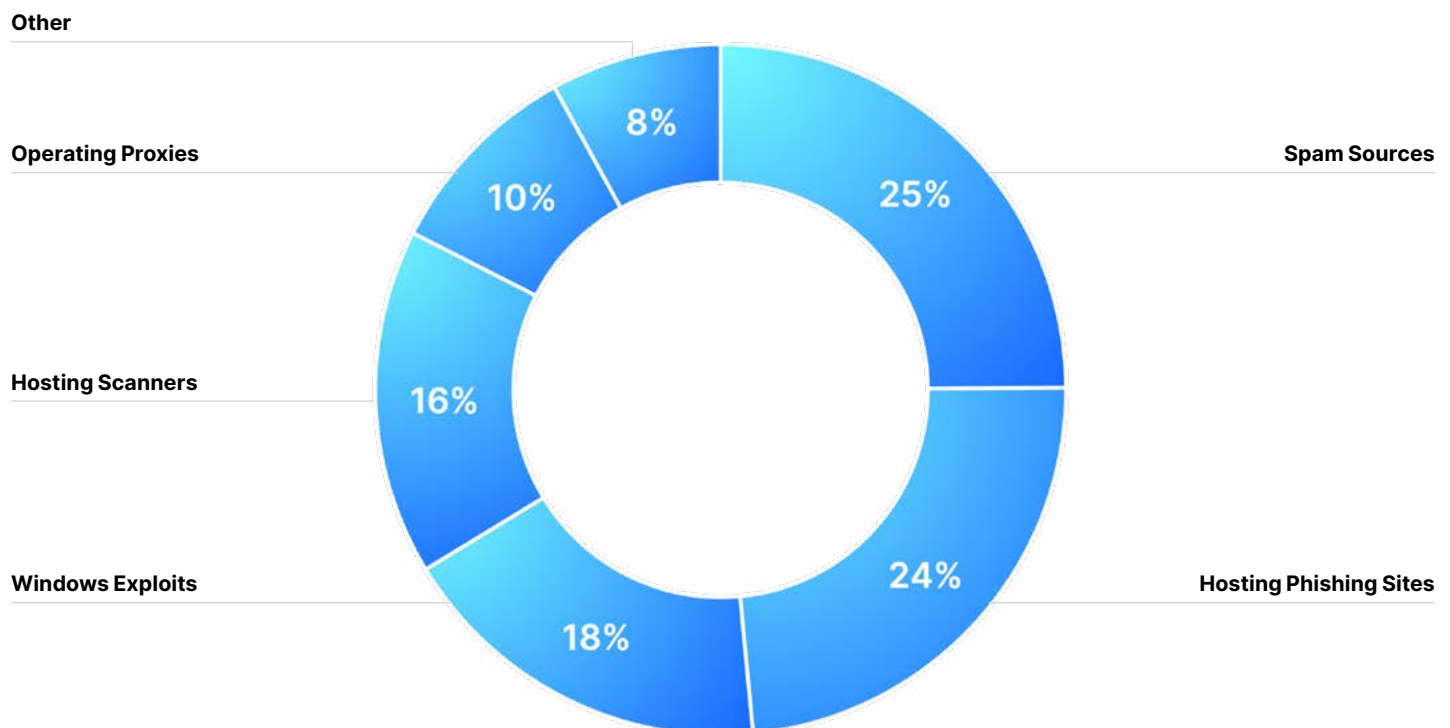


Figure 11: Convictions by category for the top 50,000 malicious IP addresses

---

*One notable change is the proportion of the top 50,000 malicious IPs that are hosting phishing URLs. In 2021, only 10% were convicted for this, but in 2022 that percentage more than doubled to 23.6%. This indicates that threat actors are finding more value in hosting phishing sites, perhaps because of the popularity and ready availability of phishing kits.*

---

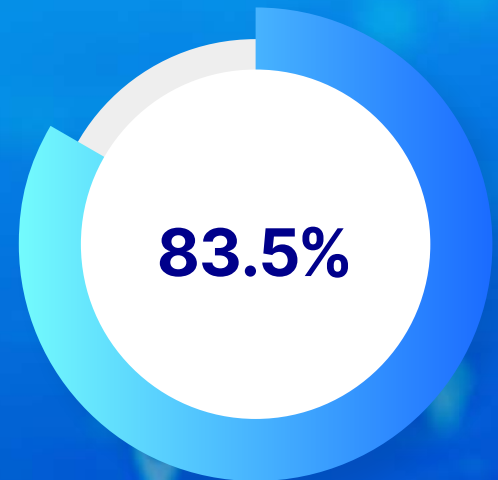
Another change we observed is that the proportion of the top 50,000 malicious IPs that were convicted of hosting scanners decreased significantly, down from 25.1% last year to 16.2% this year.

BrightCloud® also tracks exit nodes for the Tor network because Tor proxies are commonly used to conceal the source of attacks. The number of Tor exit nodes edged upward slightly, from 1.2% in 2021 to 1.5% in 2022. Although the rapid growth in the adoption of the Tor network that we first observed in 2020 has stabilized, its usage has not declined.

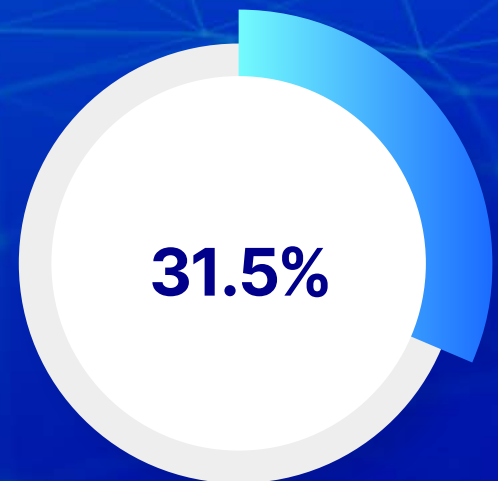
### Frequency of Convictions

The data that we've been looking at so far shows how prevalent each type of malicious behavior is in relation to all the other categories — that is, a relative comparison. We'll also delve deeper into the absolute number of times each of the top 50,000 malicious IP addresses was convicted of performing each bad behavior. In addition, we'll examine the month-by-month trends we observed among the top 50,000 malicious IPs.

Most of these IP addresses were active throughout the entire year. Of the top 50,000 most-active malicious IP addresses, 83.5% were observed performing malicious activities in every month of 2022. This is unusual because attackers typically use an IP address for malicious purposes for a short time, pause for a while to avoid being blocked or until they've been removed from blocklists, and then start using it again.



**of the most-active malicious IP addresses were observed performing malicious activities in every month of 2022**



**of convictions worldwide were found in the U.S. in 2022**

---

*The number of times each of the top 50,000 most active malicious IP addresses was convicted of performing bad behaviors significantly increased over the past year. We observed 903 malicious behaviors per IP address — a 5.8% increase from 2021 when we observed 852 malicious behaviors per IP address in the same group.*

---

## Geographic Breakdown

In 2022, the top 50,000 most-active malicious IP addresses originated from a total of 164 different countries. Similar to 2021, 90% were hosted in only 24 countries (last year, a similar percentage was hosted in 22 countries). Figure 12 shows the 10 countries with the highest relative share of the top 50,000 malicious IP addresses. As we can see, 66% of the total 50,000 were hosted in just five countries:

1. The U.S. — 31.5%
2. China — 18.0%
3. The Netherlands — 7.8%
4. Vietnam — 4.4%
5. Germany — 4.2%

As was also the case in 2021, the U.S. had the largest number of convictions in 2022. In the chart, the United States is shown to have the largest number of malicious IP addresses as well as the greatest share of convictions.

---

*The key changes from 2021 to 2022 are the movement of the Netherlands and Germany into the top five and Russia's drop out of the top five.*

---

2022 saw a number of countries impose sanctions on Russia following its invasion of Ukraine. As a result, it's possible that Russian IPs were more likely to be placed on blacklists, especially after Moscow set up its own TLS certificate-issuing authority to provide HTTPs certificates to Russian websites impacted by the sanctions.<sup>33</sup> This increased burden may have motivated at least a few operators of malicious IP addresses to set up shop in other parts of Europe or elsewhere.

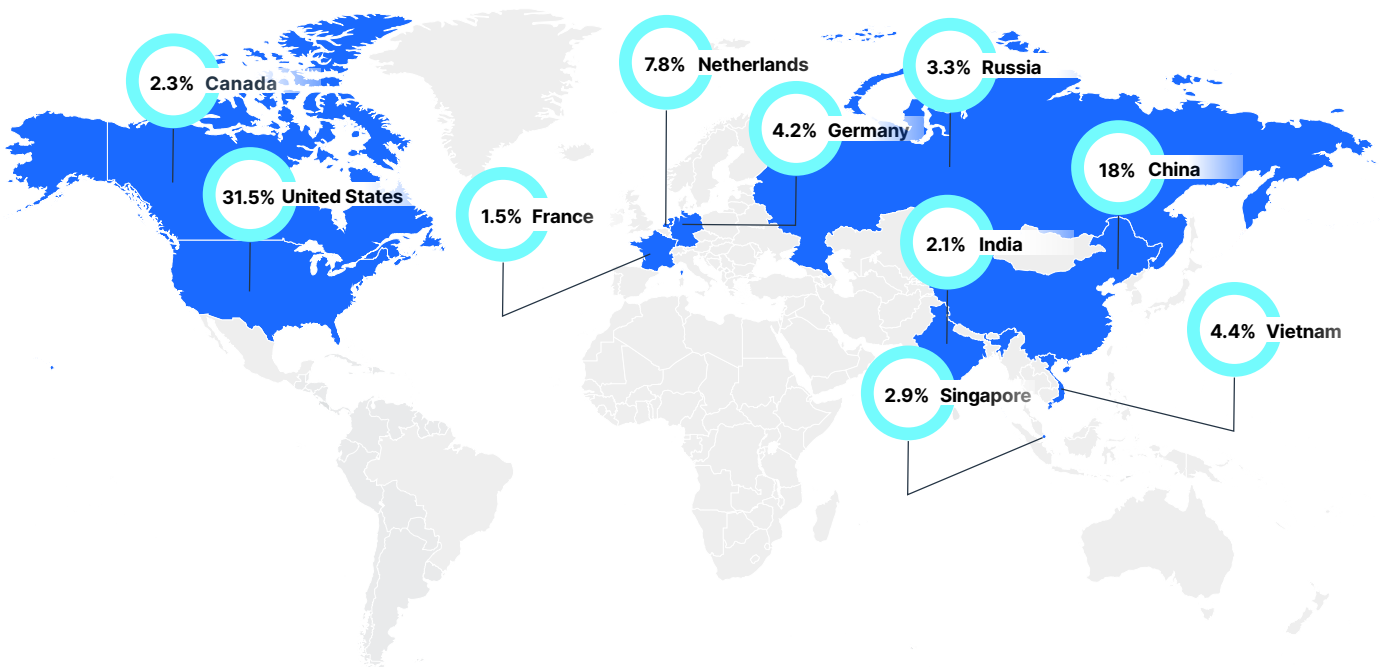


Figure 12: Malicious IP addresses and convictions by countries of origin for top 50K malicious IPs



# Harmful Mobile Apps

Although not yet as pervasive as malware targeting Windows PCs, Android malware is a real and growing threat — one with significant ramifications for businesses with employees who use personal mobile devices for work. Google has removed thousands of malicious apps from Google Play, including some that were downloaded more than one million times. These apps infected devices with malware and bombarded them with malicious ads before they were made unavailable.<sup>34</sup>

The recent phenomenon of vendor certificate compromise is also concerning. The Android operating system determines apps' privileges and levels of OS access on the basis of certificates provided by app developers and device manufacturers that prove the software is legitimate. A number of these certificates have been leaked, including some by Samsung, LG, and Mediatek.<sup>35</sup>

“

*It's worth noting that the total number of Trojans spiked 310% between July and September when a new Joker variant infected many apps on Google Play.*

”

Malware apps can use these leaked certificates to access permissions within the Android operating system. Vendor certificate compromise remains the biggest challenge within the self-certified security model the Android app ecosystem relies on. It will continue to be a challenge until all vulnerable apps and devices are updated or phased out.

In 2022, our threat research team tracked the types of infections Webroot-protected mobile device users encountered on their Android devices. Among the threats we observed, Trojans and malware were the most prevalent, together accounting for 89% of mobile infections.

One of the most common strains of Android malware is the Joker Trojan, first detected in 2019 and still dominant within the Android ecosystem. While Joker steals credit card information and banking credentials, a newer variant, Harly — named for another DC Comics character and the Joker’s sometime girlfriend — signs its victims up for paid subscriptions without their knowledge.

Joker has been very successful at infecting legitimate apps. It continues to evolve to incorporate new functionalities, like recording SMS conversations and other device activity. The recordings can then be used to bypass multi-factor authentication (MFA).

It’s worth noting that the total number of Trojans spiked 310% between July and September when a new Joker variant infected many apps on Google Play.

Trojans like Joker and Harly are a constant plague on Google Play, where they proliferate by virtue of the user trust they’ve gained simply by being available on the official Google app store.

Other types of malicious Android apps we observed in 2022 include:

- Potentially unwanted applications (PUAs) — 8%
- Spyware — 2%
- Adware — 1%

Mobile devices are ubiquitous, and everything done on them can be tracked and captured. This makes them an ideal spyware vector, fueling an entire cybercriminal enterprise that’s likely to remain viable for the foreseeable future.

With more businesses — from grocery stores to banks to medical providers — now relying on mobile apps to support their offerings, the mobile app ecosystem has become an enormous attack surface that continues to grow. Problems that arise from this include:

- More apps that have been abandoned by their developers but which still exist on devices and have vulnerabilities attackers can leverage.
- Persistent vulnerabilities in app development frameworks.
- The common practice of copying and pasting code, which can potentially replicate vulnerabilities.

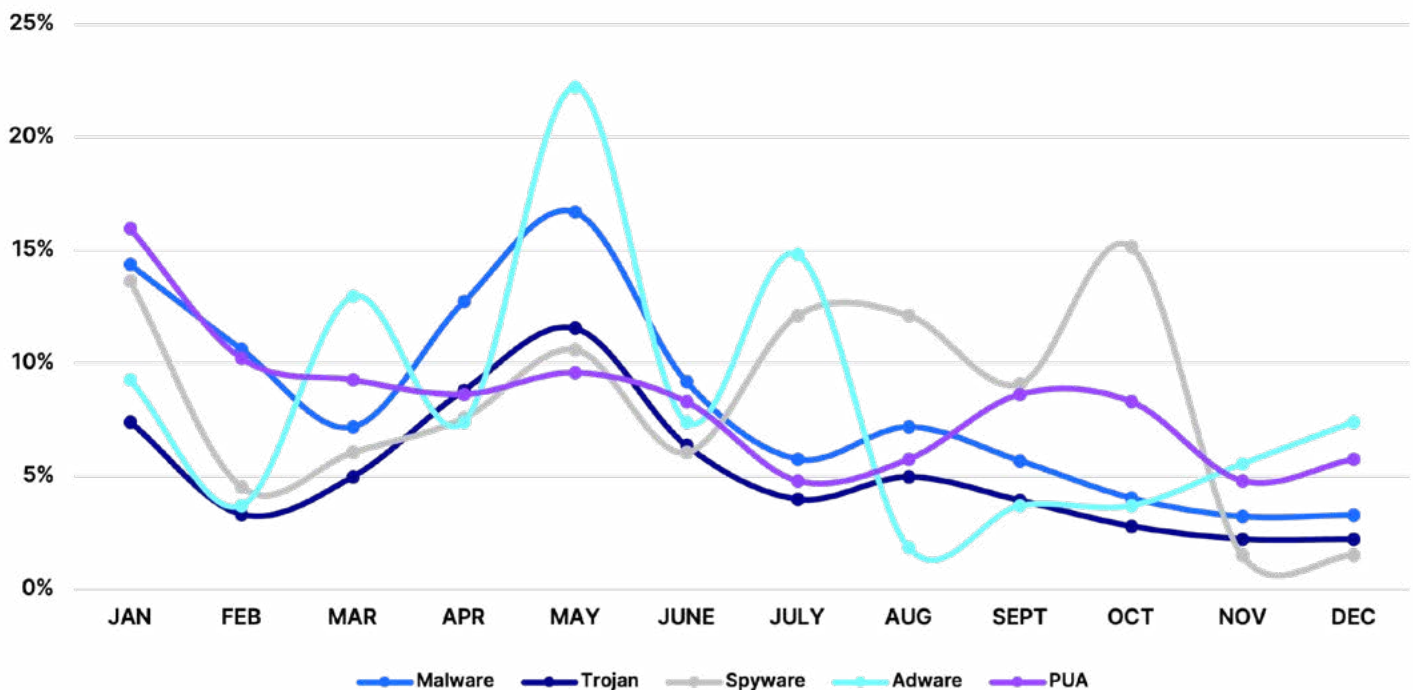


Figure 13: Malware family monthly changes



# Security Awareness Training

Cyber attackers don't just rely on technology to get around security protocols. Many use social engineering to deceive users into unintentionally creating an opening malicious software can squeeze through. Therefore, security awareness training should be a core component of every organization's multi-layered defensive strategy for preventing cyber attacks.

End users who have been trained on how to spot cybercrime can be a major asset to a cybersecurity program. Some forms of attacks specifically require unwitting user intervention to work — which also means that training people to spot these attacks can be a highly effective way to prevent them.

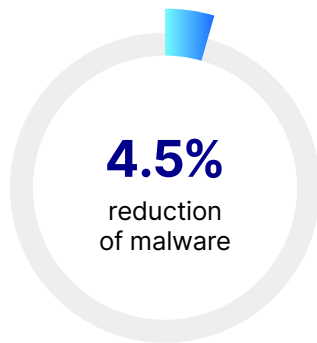


For example, email and endpoint protection solutions often struggle to detect business email compromise (BEC) attacks since they don't involve malware. This means you're relying on recipients to notice suspicious messages and report them. Even phishing emails that do contain malware — and this is still the most common malware delivery method — rely on the end user to click on the malicious link or attachment in the message. While it's impossible to guarantee that end users will never be tricked by social engineering tactics, training them to spot and report messages containing malicious links can significantly reduce the risk of infection, especially when combined with other security procedures.

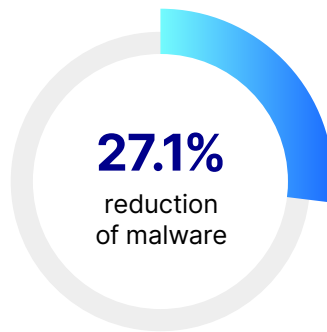
Our data indicates the value of adding cyber security training to your other protective tools. In 2022, customers who used Webroot® Security Awareness Training in combination with Webroot® Business Endpoint Protection experienced 4.5% fewer infected devices than those who relied on Webroot® Business Endpoint Protection alone. Although this represents a decrease from 2021's numbers, this most likely reflects the overall decrease in malware infections.

Cybersecurity training has to be ongoing and updated in order to remain effective. As this report makes clear, attackers like to combine tried-and-true tactics with new tricks. For example, attackers have a long history of referring to trending topics like elections, holidays, or major sporting events when crafting phishing emails. But more recently, they've also started creating customized social media personas and even using AI-generated deepfakes. Users need to be prepared to recognize all of these tactics, so it's vital to continually update your cybersecurity awareness training in line with the latest trends, as well as classic techniques.

The most advanced security awareness training solutions base the material they present to users upon the very latest threat intelligence. This is why we infuse insights gathered by our Advanced Email Threat Protection solution into our Webroot Security Awareness Training platform. We take the most novel and creative attack tactics and use them as templates for phishing attack simulations. This way, organizations can train their people to recognize the newest — and trickiest — threats.



Users who had implemented both **Endpoint Protection** and **Security Awareness Training** saw a **4.5% average reduction in the number of malware infections** they encountered compared to those that only had Endpoint Protection.



Users who used both **Endpoint Protection** and **DNS Protection** experienced, on average **27.1% fewer malware infections** than those that only had Endpoint Protection.



Users who adopted all three layers of protection – **Endpoint Protection**, **Security Awareness Training**, and **DNS Protection** over Endpoint Protection alone had the lowest infection rate, with **an average of 40.3% reduction in the number of devices that encountered malware**.

# Conclusion

The 2023 OpenText Cybersecurity Threat Report shows that cyber attackers continue to be resilient, innovative, and effective.

In 2022, they doubled down on longstanding tactics — including increasing the volumes of phishing emails and ransomware attacks — while also adapting to new trends. For example, they continued to ramp up attacks against supply chains and the relatively unprotected personal devices and home WiFi networks used by remote workers and took advantage of businesses that cut back on cybersecurity spending.

Attackers continued to look for novel ways to evade defenses, using improving technology such as deepfakes and AI; honing social-engineering tactics; and rethinking the way they carry out attacks, e.g. using ransomware to access and copy data rather than locking the user out.

Although international law enforcement agencies have had some recent successes targeting the cybercriminal organizations behind many of these attacks, these groups often reform under a different banner. They recruit fresh talent with new ideas, which are harder to defend against because there's no information on how they work.

Given these continued challenges, it's unrealistic to expect that we'll be able to prevent all cyberattacks. Instead, our focus should be on building cyber resilience: Doing our best to defend against attackers and prevent breaches while also preparing a strategy that will limit damage and speed up recovery should an attack occur.

Building a multi-layered approach to defense is core to cybersecurity and cyber resilience. The more processes, tools, and systems you have in place to protect and recover data, the less likely an attack will succeed — and if it does, the less impact it will have on your business.

Examples of these layers of defense and resilience include:

- Solutions that use threat intelligence and machine learning to detect and block malware attacks
- Backing up all critical files and systems in a separate and secure location
- Testing your restoration capabilities under simulated attack scenarios
- Training end users to spot and report phishing attacks and scams

Resilience and resourcefulness are not limited to cyber criminals. Seeing the sheer scope of the threats out there can feel intimidating — but by staying aware of these trends and applying multiple security measures, it's possible to stay one step ahead of the attackers.

## Footnotes

- <sup>1</sup> <https://www.bbc.com/news/technology-59998925>
- <sup>2</sup> <https://www.scientificamerican.com/article/fbi-takes-down-hive-criminal-ransomware-group1/>
- <sup>3</sup> <https://www.securityweek.com/conti-ransomware-operation-shut-down-after-brand-becomes-toxic/>
- <sup>4</sup> [https://www.cyber.nj.gov/garden\\_state\\_cyber\\_threat\\_highlight/conti-ransomware-group-announces-shutdown-proliferation-continues-via-affiliates](https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/conti-ransomware-group-announces-shutdown-proliferation-continues-via-affiliates)
- <sup>5</sup> <https://www.secureworks.com/resources/rp-state-of-the-threat-2022>
- <sup>6</sup> <https://www.secureworks.com/resources/rp-state-of-the-threat-2022>
- <sup>7</sup> <https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021>
- <sup>8</sup> <https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/>
- <sup>9</sup> <https://www.zdnet.com/article/who-are-lapsus-and-what-do-they-want/>
- <sup>10</sup> <https://www.hhs.gov/sites/default/files/karakurt-threat-profile-analyst-note.pdf>
- <sup>11</sup> <https://threatpost.com/extortion-karakurt-threat-ransomware/176911/>
- <sup>12</sup> <https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases>
- <sup>13</sup> <https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate>
- <sup>14</sup> <https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020>
- <sup>15</sup> <https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021>
- <sup>16</sup> <https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022>
- <sup>17</sup> <https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments>
- <sup>18</sup> <https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf>
- <sup>19</sup> <https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d>
- <sup>20</sup> <https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil/>
- <sup>21</sup> <https://www.cisecurity.org/insights/blog/the-conti-leaks-a-case-of-cybercrimes-commercialization>
- <sup>22</sup> <https://www.bleepingcomputer.com/news/security/google-says-former-conti-ransomware-members-now-attack-ukraine/>
- <sup>23</sup> <https://www.cyberscoop.com/revil-prosecutions-reach-a-dead-end-russian-media-reports/>
- <sup>24</sup> <https://www.secureworks.com/resources/rp-state-of-the-threat-2022>
- <sup>25</sup> <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/>
- <sup>26</sup> <https://venturebeat.com/security/lockbit-bug-bounty/>
- <sup>27</sup> <https://www.bleepingcomputer.com/news/security/ransomware-gang-apologizes-gives-sickkids-hospital-free-decryptor/>
- <sup>28</sup> <https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf>
- <sup>29</sup> Ibid.
- <sup>30</sup> [https://www.splunk.com/en\\_us/form/an-empirically-comparative-analysis-of-ransomware-binaries.html](https://www.splunk.com/en_us/form/an-empirically-comparative-analysis-of-ransomware-binaries.html)
- <sup>31</sup> <https://www.crowdstrike.com/blog/owassrf-exploit-analysis-and-recommendations/>
- <sup>32</sup> <https://www.bleepingcomputer.com/news/security/rackspace-confirms-play-ransomware-was-behind-recent-cyberattack/>
- <sup>33</sup> [https://www.theregister.com/2022/03/11/russian\\_ca/](https://www.theregister.com/2022/03/11/russian_ca/)
- <sup>34</sup> <https://www.zdnet.com/article/android-warning-these-malicious-apps-had-over-a-million-downloads-from-google-play/>
- <sup>35</sup> <https://www.bleepingcomputer.com/news/security/samsung-lg-mediatek-certificates-compromised-to-sign-android-malware/>



The background of the entire page is a deep blue color. It features a complex, abstract pattern of thin, light blue lines that flow and curve across the frame, creating a sense of motion and depth. Small, light blue dots are scattered throughout, particularly along the lines, resembling data points or particles in a network.

# opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

Copyright © 2023 Open Text Corporation. All rights reserved.