
2024
OpenText threat perspective:
Strategies for a stronger SMB
opentext™ | Cybersecurity

Contents

Foreword

2023 was a year of geopolitical turmoil, rapid advance in the development of AI's capabilities, and persistent tug-of-war between law enforcement agencies and cybercriminal groups. All of these factors came together to challenge defenders in new ways, with ransomware attack volumes reaching an all-time high in the U.S., and malware infection rates creeping upwards for the first time after years of persistent decline.

Software supply chains remained a prime target for threat actors. The CL0P ransomware gang's MOVEit campaign exploited a zero day vulnerability in widely-used file sharing software to impact more than 60 million victims, driving the average ransom payment to a new peak, while illustrating just how effective the Ransomware-as-a-Service (RaaS) model continues to be.

After the relative restraint that some ransomware groups (notably LockBit) showed during the pandemic, it seems that the gloves are off in 2023. Last year, LockBit formally apologized when an affiliate attacked a children's hospital, issuing the victim a free decryption tool, and allegedly ending the relationship with the affiliate because of the rule violation.[1] This year, hospitals and health systems are among ransomware operators' prime targets.

In addition, LockBit has exemplified cybercriminal resilience, bouncing back swiftly from a high-profile takedown attempt conducted by an international law enforcement task force. Just a few days after law enforcement officials had dismantled its infrastructure, the group had reestablished operations and set up a new leak site on the dark web, with its leader publicly taunting the FBI.

Meanwhile, phishing has grown more prolific and more personalized. Attackers are leveraging generative AI and large language models (LLMs) to create more convincing phishing emails at scale, blurring the distinction between phishing (where large volumes of messages are sent) and spearphishing (where attackers invest time and effort in customizing communications in hopes of increasing open and click-through rates). Though AI continues to grow more capable quickly, it's likely that attackers' use of it is still in its earliest stages.

All of these trends are reflected in the threat intelligence we're presenting in this report. We'll explore the current threat landscape, highlighting the issues that are most relevant for small and midsized organizations. As OpenText Cybersecurity, we provide comprehensive security solutions to help companies of all sizes build cyber resilience with a holistic solution portfolio. Every year, we aim to improve the quality of our report data while providing broad coverage of threat activities. New this year is an audience-tailored approach, in which we specifically focus on the threats, trends, and advice that are of greatest interest to a particular market segment. Our goal is to empower you with the knowledge you need to build stronger and smarter defenses for in the year ahead.

1 https://www.theregister.com/2024/02/01/lockbit_ransomware_attack_hospital/

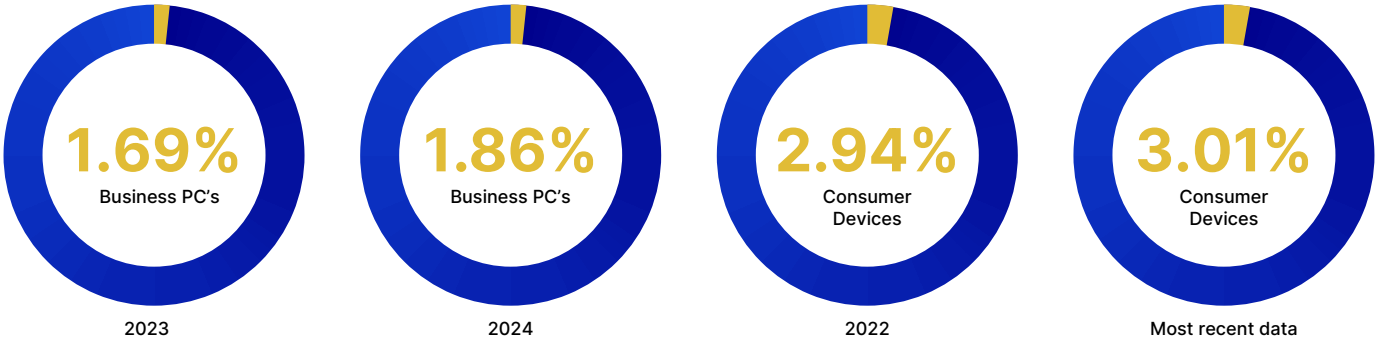
Threat intelligence overview

This report is based on threat intelligence data collected from millions of endpoints belonging to OpenText customers. We analyze files, email messages, and communications with malicious websites.

These endpoints encounter an average of 824,000 never-before-seen application files every day. We classify these files by source, with business PCs seeing 76% of all new files, and consumer devices encountering only 23%.

Malware

We've been tracking the number of malicious files reaching Webroot-protected endpoints for more than a decade now, but this year's data reveals that infection rates have reached a new—and not entirely welcome—inflection point. In our 2022 report, we celebrated a remarkable shift: malware infections of Webroot-protected Windows devices had dropped 58% year over year. The following year, we noted that the decrease continued, but its momentum had greatly slowed.

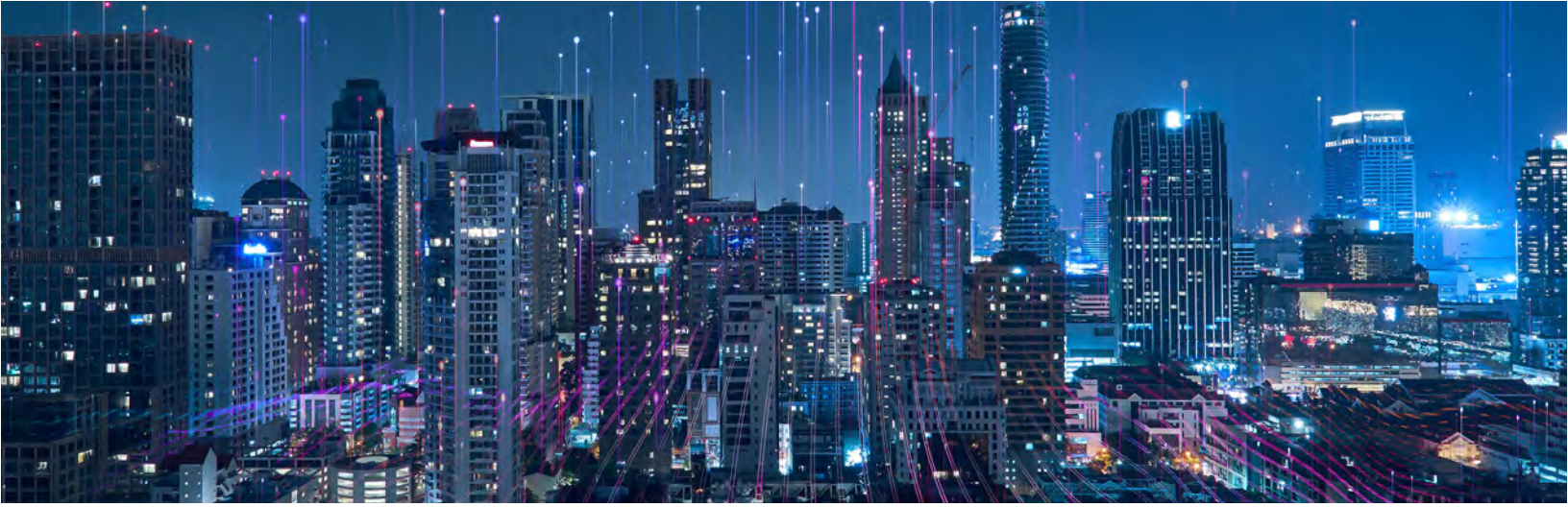


Now, we are observing—for the first time since 2017—an increase in both business and consumer PC infection rates. Last year, 1.69% of business PCs encountered a malware infection, while this year, 1.86% of business PCs were infected. Similarly, 2.94% of consumer devices were infected with malware in 2022, and 3.01% in our most recent data. This increase isn't large, but it's very different from the ongoing decline we saw in the past.

We don't have conclusive evidence about the reasons for the year-over-year increase in infections, but we do understand its implications. As attackers continue to innovate, in particular by leveraging tools like generative AI to increase the volume and customization of email-borne threats, it is mission-critical for businesses of all sizes to reassess the effectiveness of their cyber defenses.

Although overall infection rates have gone up, attackers remain consistent in the methods they're using to create and deliver unique variants. The percentage of malicious files seen only on a single PC was 85.7%, which is in the same ballpark as last year's number, 87.5%. The fact that the number of unique malware variants is fairly stable should remind stakeholders that it's important to implement antivirus protection with per-endpoint telemetry that can identify and block novel threats. It is also vital to follow a multi-layered cybersecurity approach.

Similarly consistent was the percentage of infections observed on two to ten PCs, which was 12.2%, slightly up from 11.1% last year, as well as the percentage of infections observed on 11 to 100 PCs (1.8%, up from 1.2% last year). These rates have remained relatively stable over the past few years.



The importance of a multi-layered approach for cyber resilience

There's solid evidence in our data that multiple layers of protection are more effective than a less comprehensive approach. Simply put, the more protections are applied, the fewer malware infections an organization or individual will experience.

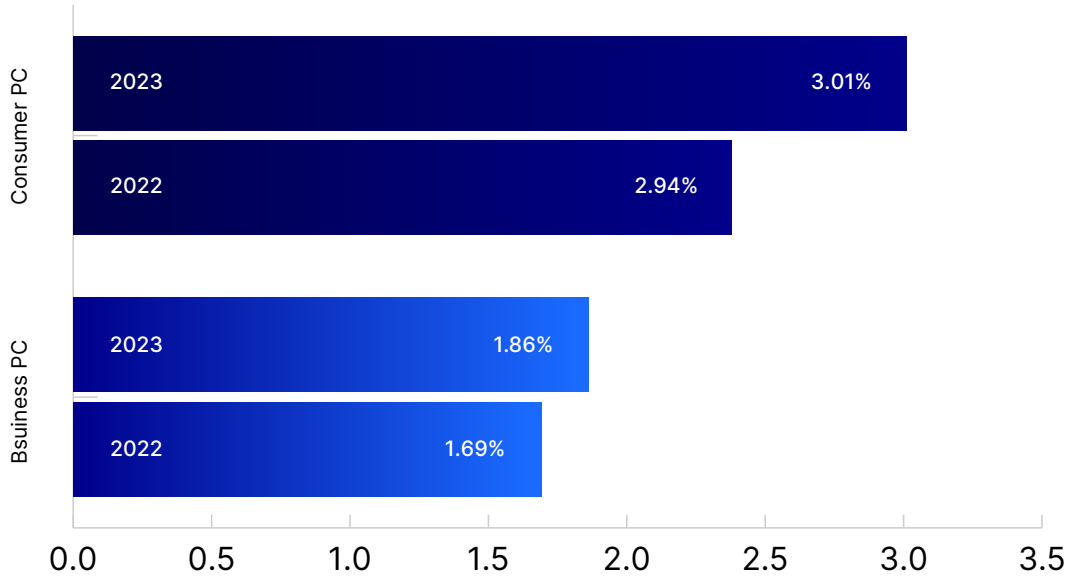
- Customers who implement security awareness training in conjunction with Webroot SecureAnywhere (WSA) see 11.4% fewer infections than those who rely on WSA alone.
- Customers who combine DNS protection with WSA see 19.8% fewer malware infections than those who use just WSA.
- Most notably, customers who leverage WSA, DNS protection and security awareness training experience the fewest infections of all, 30.7% less than those relying on only WSA.

It is absolutely critical to follow a layered approach if you want to mitigate today's greatest cyber risks. Endpoint protection works better in conjunction with DNS protection, because even if a machine gets infected, the DNS protection will block outbound connections to malicious sites. Adding security awareness training ups the ante even further. This is becoming even more important now that generative AI seems to be driving an increase in attack volumes. We are beginning to see cyber insurance companies require their clients to have security awareness training programs in place. This is new, but it's a growing trend.

—Kenneth Thon, Solutions Consultant, OpenText Cybersecurity

Infection rates: Consumer vs. business PCs

It has long been the case that business PCs see a much lower infection rate than consumer PCs, and that trend has continued into 2023. In keeping with this tendency, the infection rate for consumer PCs over the past year was again approximately 50% higher than the infection rate for business PCs.



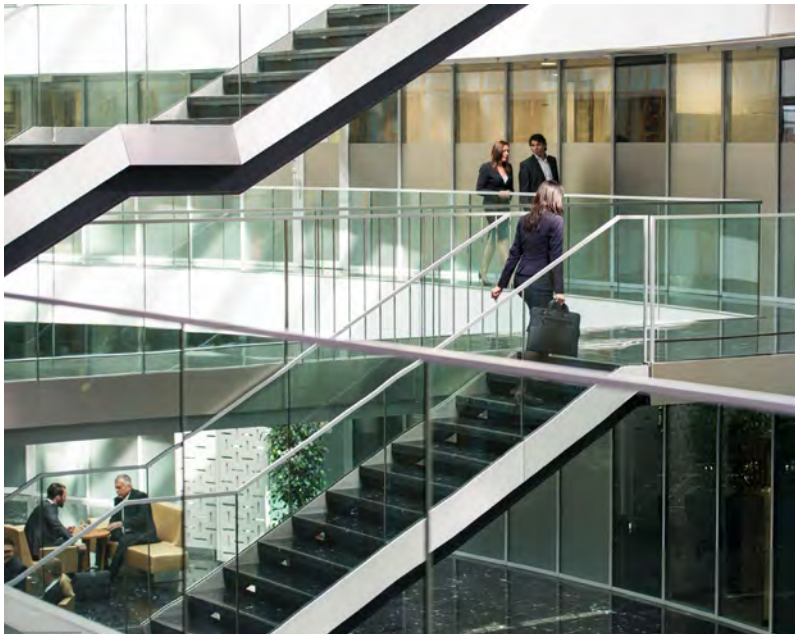
The overall infection rate for consumer PCs in 2023 was 3.01%, a slight increase (2.38%) from last year's infection rate of 2.94%. Though lower, the business PC infection rate saw a larger increase (of 10.01%). The overall business PC infection rate was 1.86% in 2023, up from 1.69% the previous year.

Re-infection rates were also higher among consumer devices, with 52.39% of the consumer devices that were infected at least once encountering one or more additional infections over the course of the year. Fewer of the business devices that were infected once were subsequently re-infected, at 42.8% of the total. This highlights the importance of user education, which can significantly reduce re-infection risk, especially if conducted after the initial incident is detected and remediated.

Also noteworthy: the overall rate of Windows 11 adoption is higher among consumers (23.5%) than among businesses (18.8%). All new PCs are sold with Windows 11, but a number of older systems don't meet the TMP 2.0 requirement needed to run it. Fewer business PCs (6.3%) are still running Windows 7 than consumer PCs (9.2%), but more business PCs (66.3%) are running Windows 10 than consumers (57.6%). Migration to Windows 11 is expected to continue, but at a slow pace over the next few years. In the past, migrations to the latest Windows version have tended to decrease malware infection risks, but the jury remains out on whether that trend will persist into the future.

Infection rates by business size

As has been the case in previous years, smaller businesses tend to experience fewer malware infections overall. Attackers may target larger organizations more frequently, assuming they are more likely to have funds available for extortion or more weaknesses on their attack surface that can be successfully exploited. It's important to keep in mind, though, that malware infections tend to have a greater impact on smaller businesses. They might see fewer infections, but they are more likely to experience full network disruption when an infection does occur.



Among the smallest organizations (those with 20 or fewer licensed PCs), 6.1% experienced an infection, with an average of 4.8 PCs impacted. Medium organizations (those with 21 to 100 licensed PCs) saw higher infection rates, with 30.5% experiencing infections and an average of 6.5 PCs affected. Rates were higher among larger organizations.

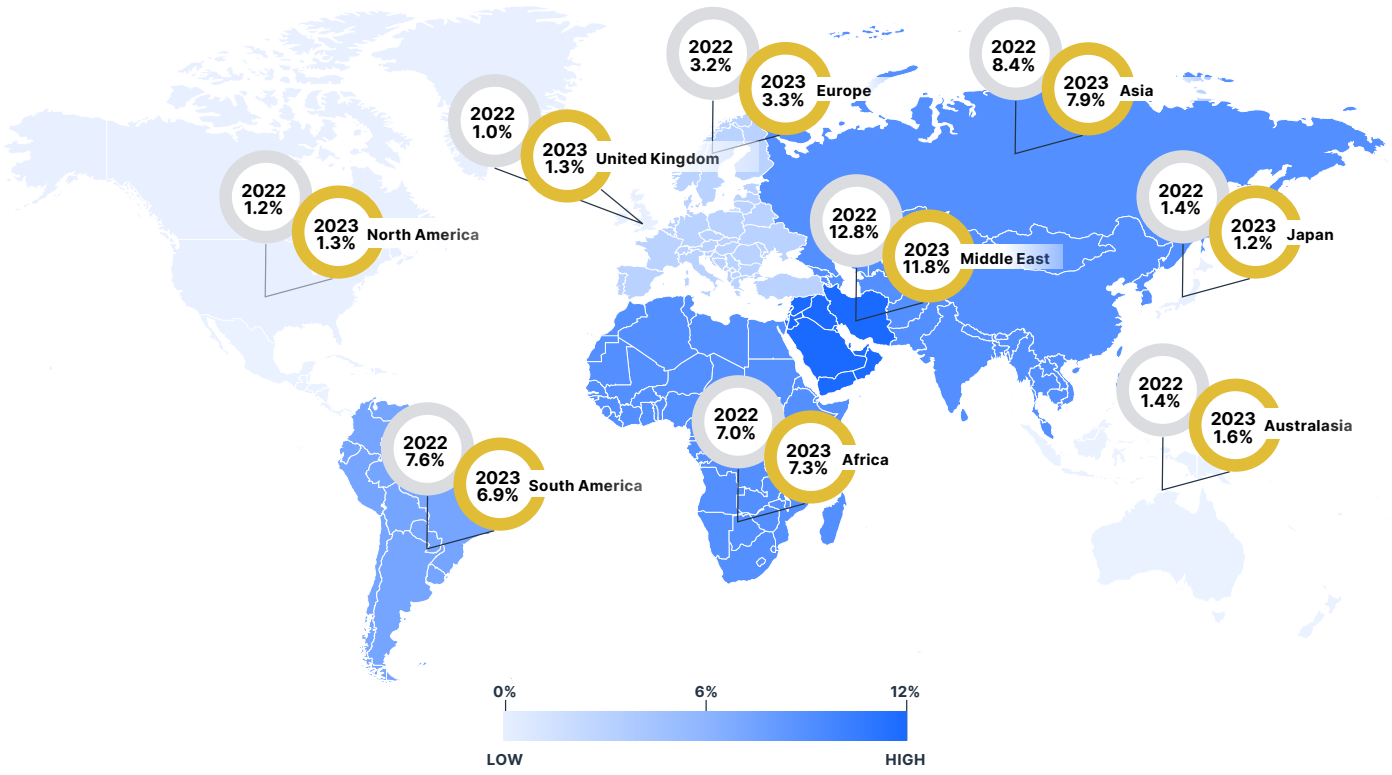
Those with 101 to 500 licensed PCs experienced a 61.8% infection rate, with an average of 15 PCs affected, while those with more than 500 licensed PCs saw an overall infection rate of 86.5%, with 40.9 PCs impacted on average.

Business Size by # of Licensed PCs	% of Businesses with Infections	Avg. Infections per Infected Business
1-20: Small	6.1%	4.8 PCs
21-100: Medium	30.5%	6.5 PCs
101-500: Large	61.8%	5 PCs
501: Very Large	86.5%	40.9 PCs

Infection rates by region

Geography has an enormous impact on infection rates. This has been true in the past, and was also the case in 2023. PCs located in Asia, Africa, South America, and the Middle East encountered more than five times as many infections as those in Australia, New Zealand, Japan, North America, the UK, and Europe, with an overall infection rate of 9.0% for the first group, and 1.7% for the second.

However, Europe differs from other less-frequently-infected regions when it comes to consumer device infection rates. For consumer devices, Asia, Africa, South America, Europe, and the Middle East averaged more than 380% more infections than Australasia, Japan, North America, and the UK (11.5% vs. 3.0%). Business PC infection rates resemble the overall regional rates. Asia, Africa, South America, and the Middle East average 439% more infections than Australasia, Europe, Japan, North America, and the UK (6.0% vs. 1.4%).



Infection rates by industry

Approximately 67% of our business customers provided data on which industry vertical they're in. Figure 1 shows the percentage of businesses in each industry that encountered at least one malware infection over the past year.

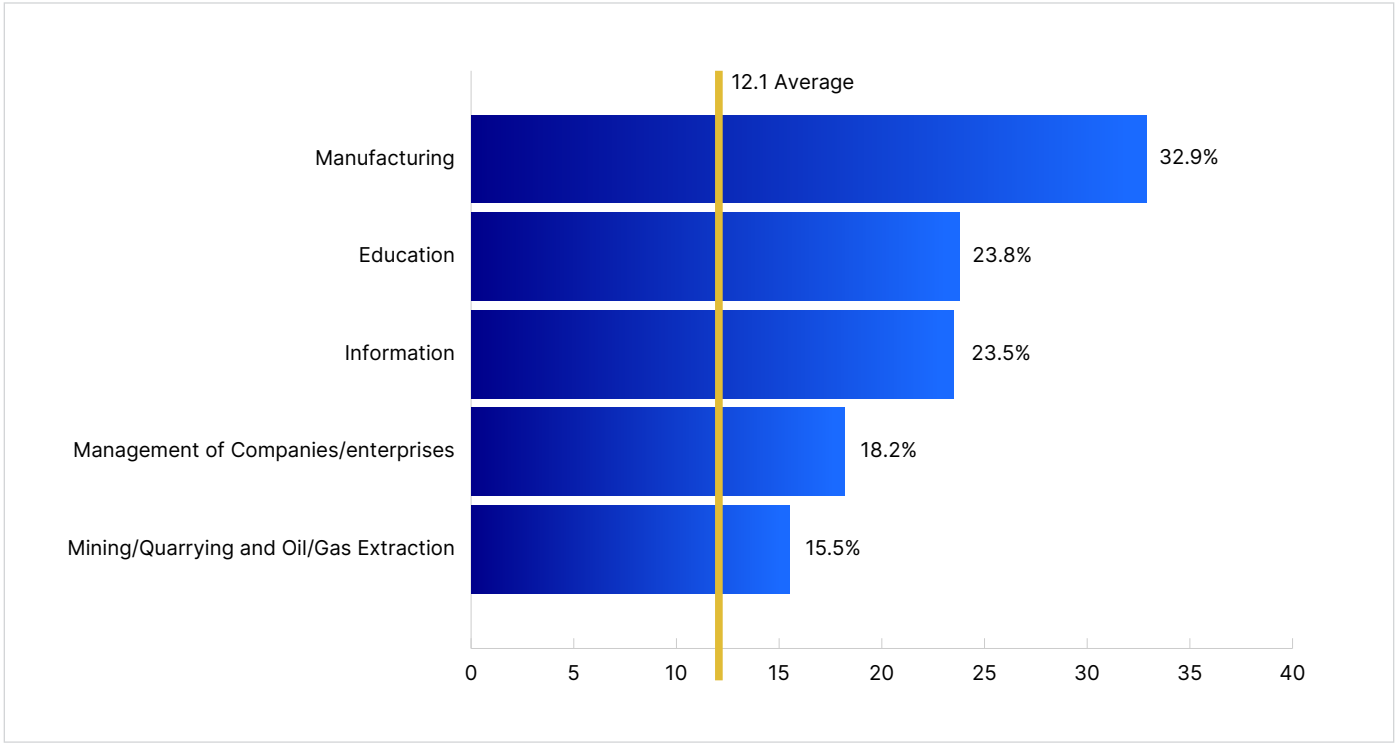


Figure 1 shows the percentage of businesses in each industry that encountered at least one malware infection over the past year.

The average infection rate across all verticals was 12.1%, but this percentage isn't highly representative of real-world risks, since there were major differences across industries. This year, the verticals with the highest infection rates were:

1. **Manufacturing**—32.9% above average.
2. **Education**—23.8% above average.
3. **Information**—23.5% above average.
4. **Management of Companies and Enterprises**—18.2% above average.
5. **Mining, Quarrying and Oil & Gas Extraction**—15.5% above average.

Both Education and Mining, Quarrying and Oil & Gas Extraction are new to the top five this year, displacing Public Administration (which still experienced an infection rate 14.8% above average) and Wholesale Trade (which experienced an infection rate 13.6% above average).

Manufacturing was the most frequently infected industry again in 2023, a trend that continues from previous years. Manufacturers are notoriously intolerant of downtime because of the high costs associated with production stoppages. As a result, they may be more willing to pay ransoms than victims in other verticals.

Education is new to the top five this year. Its inclusion may represent the "gloves off" approach that we're seeing attackers take, where all ethical constraints are abandoned and no prospective victim is spared.

Ransomware

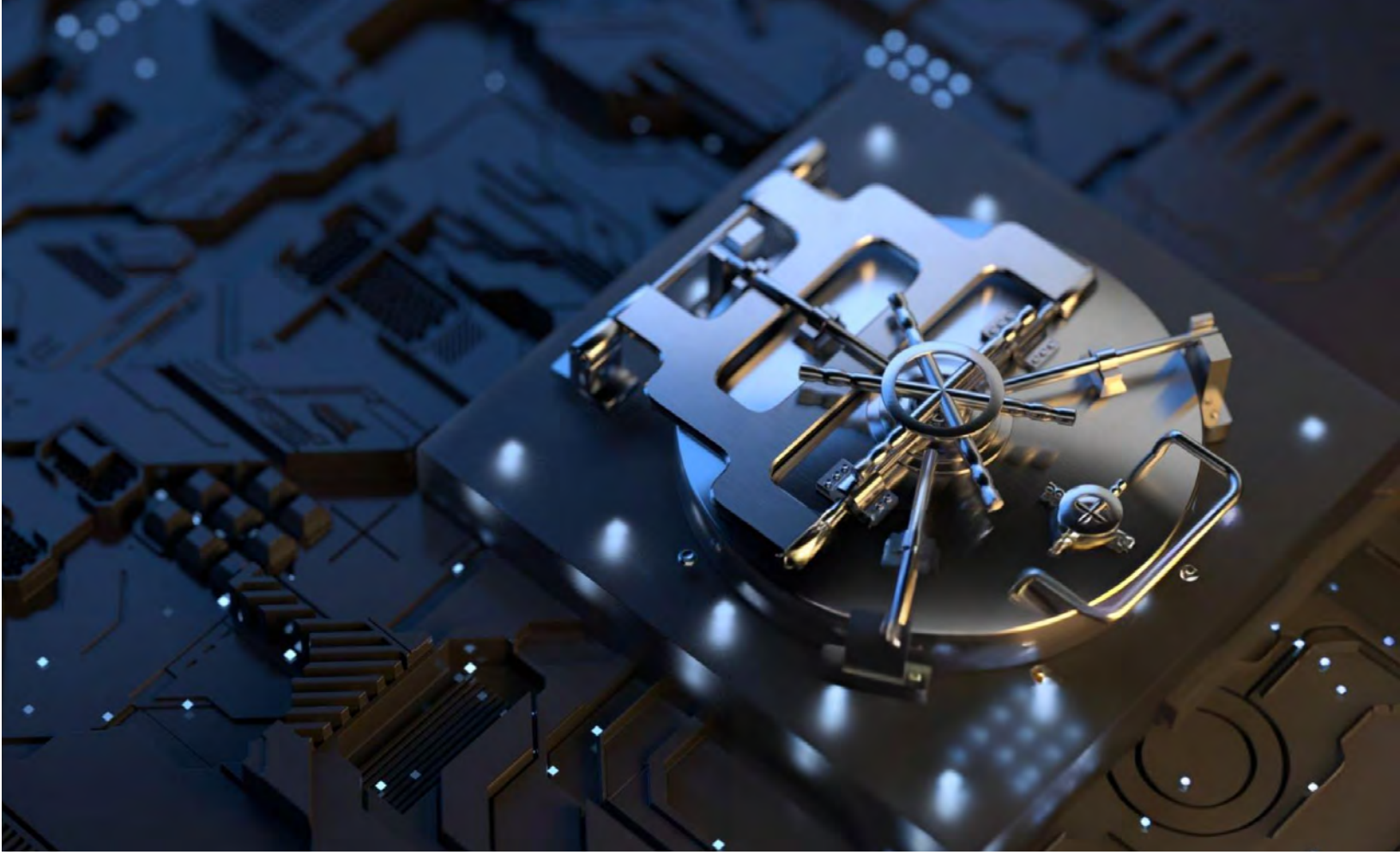
Developments across the ransomware landscape over the past year demonstrate that the pace of change is as fast as ever. It's long been the case that a ransomware gang takedown will result in a short-term decrease in activity, followed by a surge as the group rises anew. 2023 saw this pattern repeat itself, though law enforcement leveraged innovative tactics and had some successes, while governments continued to contemplate the benefits (and potential consequences) of payment bans.[1] Crackdowns on illicit cryptocurrency movement forced attackers to seek out new ways to collect payments.[2]

Early in 2024, an international task force spearheaded by law enforcement operatives from the US and UK delivered a major blow to the LockBit ransomware group, seizing control of the criminals' infrastructure, source code, cryptocurrency accounts, and custom tooling.[3] Law enforcement used LockBit's own dark web leak site to disseminate decryption keys to victims, a creative reversal that may have permanently tarnished the group's reputation. Nonetheless, LockBit had reestablished operations and created a new dark web leak site within days of the takedown.[4] The group's leader published a rambling statement alleging that the FBI had pursued the group only because LockBit had documents stolen from government systems in Fulton County, Georgia, which were relevant to Donald Trump's trial—and thus, U.S. election security. The statement also boasted that the takedown would "show… vulnerabilities and weaknesses" that would ultimately "make [LockBit] stronger."[5]

Meanwhile, 2023 saw ransomware attack volumes reach a new peak, especially in the U.S., while the average ransom payment soared to an all-time high of $850,700 in Q3 of that year.[6] At the same time, the percentage of ransomware attacks in which the victim made a payment to the criminals fell to a record low of 34%. This likely represents a shift in attacker strategy as ransomware operators begin to move away from the data-exfiltration-only tactic, which had gained prominence over the past few years, towards more targeted attacks incorporating encrypting malware as well as data theft.[7] Encrypting a victim's data requires more time and effort from ransomware operators, but the potential payoff is greater, since the business impact caused by massive operational disruption increases the chances that victims will hand over a large ransom.

Among the most successful ransomware operations of 2023 was the CL0P gang's MOVEit campaign, which exploited a zero day vulnerability in widely-used file transfer software to infect systems and exfiltrate data en masse.[8] More than 2,000 organizations—and 62 million individuals—were impacted by these attacks, including multiple high profile public and private sector entities.[9] The campaign, which ultimately yielded over $100 million in criminal profits, demonstrated that software supply chain risks remain pervasive. If ransomware operators can take advantage of a vulnerability in widely-used but little-known middleware, the payoff can be enormous. Relatively few MOVEit victims paid the very large ransoms that CL0P demanded, but those that did likely drove the global average ransom payment up dramatically.[10]

1 https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying
2 https://www.wired.com/story/ransomware-payments-2023-breaks-record/
3 https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant
4 https://www.cybersecuritydive.com/news/lockbit-revives-operations/708507/
5 https://krebsonsecurity.com/2024/02/fbis-lockbit-takedown-postponed-a-ticking-time-bomb-in-fulton-county-ga/
6 https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments
7 Ibid.
8 https://therecord.media/clop-moveit-zero-day-dustin-childs-interview
9 https://www.engadget.com/clop-ransomware-gang-obtained-personal-data-of-45000-new-york-city-students-in-moveit-hack-204655820.html
10 https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments



Ransom payment amounts stabilize

Within the past half-decade or so, the average ransom payment amount has increased more than tenfold. In late 2018, it averaged just $6,733, and by late 2023, had climbed to $850,7000. However, at only $200,000, the median ransom payment lags far behind the average—demonstrating that only a small number of victims end up paying such large amounts.[1]

Notably, the number of data-exfiltration-only attack victims opting to pay ransoms dropped to a new low of 26% in Q4 of 2023.[2] Stories of how ransomware gangs failed to delete victims' data after promising to do so abound, increasing suspicions that even well-established criminal groups cannot be trusted. During law enforcement's takedown of LockBit, for instance, officials revealed that they had discovered large stores of data that the gang had pledged to delete after receiving payments to destroy it.[3]

2023 saw somewhat of a bifurcation in ransomware gangs' targeting strategies as SMB-focused actors leveraged tactics like email phishing and Remote Desktop Protocol (RDP) exploitation to launch large volumes of undifferentiated attacks, while major enterprise-focused actors focused on CVEs and sophisticated social engineering campaigns.[4]

1 https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals
2 Ibid.
3 https://therecord.media/lockbit-lied-about-deleting-exfiltrated-data-after-ransom-payments
4 https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying

Tactics and strategies

Ransomware-as-a-Service (RaaS), a business model in which ransomware operators sell or lease access to tools they've built to launch ransomware attacks, continued to dominate the ransomware ecosystem for yet another year in 2023. The RaaS model brings advantages for ransomware developers and their affiliates alike. It makes it simpler for would-be cybercriminals with little technical skill to launch attacks, and it's enormously profitable for established ransomware operators. LockBit, for instance, earned more than $200 million in affiliate fees—even though this is just 20% of the full amount of ransoms paid out.

2023 also saw an increase in the number of initial access brokers, cybercriminals who specialize in facilitating access to corporate IT environments.[1] These brokers make compromised credentials available on the dark web, or offer step-by-step pathways into victim environments. Initial access brokers often operate in tandem with RaaS groups, making it faster and easier for them to gain a foothold in a victim environment. The collaboration enables greater volumes of attacks, particularly against SMBs and lower-profile targets.

Infostealer malware—software designed to covertly harvest high-value information such as login credentials or financial data—has also become more widely available on the dark web. This also allows less-sophisticated criminals to execute the early stages of a ransomware attack. Organizations in healthcare and financial services are particularly likely to be targeted by infostealers.[2]

Major ransomware attacks

In the immediate aftermath of the COVID-19 pandemic, when sympathies for healthcare workers were running high, several ransomware operators (including LockBit) promised not to target hospitals or provider organizations. Such principles have long since fallen by the wayside, with some of the last year's biggest attacks targeting hospitals and healthcare organizations.

In February 2023, the Lehigh Valley Health Network (LVHN) was attacked by the BlackCat ransomware group, which obtained patient information from the organization's systems. Though LVHN's CEO reported that operations had not been impacted, the group published nude photos of cancer patients undergoing treatment in an effort to increase the pressure to pay up.[3] LVHN was subsequently sued by patients alleging that its refusal to pay the ransom was not in their best interest, since it led to a violation of their privacy.[4]

One of the most disruptive ransomware attacks of 2023 took place when CharterCare Health Partners, an affiliate of California-based Prospect Medical Holdings, announced that its systems were down, disrupting inpatient and outpatient care. The Rhysida ransomware gang claimed responsibility for the attack, in which, it was subsequently revealed, patients' personal, financial, and treatment information was taken.[5]

Las Vegas casino giant MGM suffered a major attack later in the year, when its hotels' digital room keys, slot machines, and even websites stopped working. The company subsequently reported that customer data was compromised during the attack, for which the group ALPHV (also known as BlackCat) claimed responsibility in a detailed summary published on their dark web leak site. Total losses stemming from the business disruption topped $100 million.[6]

1 https://www.cisecurity.org/insights/blog/initial-access-brokers-how-theyre-changing-cybercrime
2 https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/bbcomv4/blackberry-com/en/solutions/threat-intelligence/2023/threat-intelligence-report-august/Blackberry-Global-Threat-Intelligence-Report-August-2023.pdf
3 https://www.lehighvalleylive.com/business/2023/03/gang-leaks-lehigh-valley-health-network-cancer-patient-photos-as-part-of-data-hack.html
4 https://www.wsj.com/articles/patient-seeks-to-force-hospital-network-to-pay-hackers-ransom-to-remove-naked-photos-online-46ee754
5 https://www.fiercehealthcare.com/providers/ongoing-cyberattack-prospect-medical-holdings-forces-facilities-offline-disrupts-services
6 https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware

Defending against ransomware: Cyber resilience is key

Ransomware can infect systems in multiple ways, and we're confident that attackers will continue diversifying their techniques in the months and years to come. No organization—large or small—can expect to avoid all infections, since threat actors take advantage of human error, zero day vulnerabilities, and other entry points that cannot be completely shielded. Even with the strongest-possible preventative measures in place, every organization is likely to encounter an infection at some point.

This is not to say that prevention is no longer important, but in and of itself, it is no longer adequate for mitigating business risk effectively. Instead, organizations must adopt a multi-layered, defense-in-depth strategy, one that incorporates security awareness training for employees, preventative blocking of threats, protections for devices and networks, and a backup and recovery solution that enables rapid restoration. With these elements combined, you've set a firm foundation for cyber resilience.

In today's world, a layered approach is essential, since ransomware attackers have repeatedly demonstrated that they can breach each individual layer—but usually not all of them at the same time. A thorough cyber resilience strategy will combine overlapping protections in ways that can significantly reduce ransomware risks.

At a minimum, every organization should have:

- An email security solution that can detect and quarantine malicious attachments.
- An active vulnerability management program covering all servers and PCs.
- Antivirus and endpoint protection software on every PC within the organization.
- Security awareness training for all end users.
- Frequent, immutable backups for all critical files and systems.
- A disaster recovery plan that includes testing backup and restore processes.

This strategy will not prevent all ransomware infections. Cyber resilience also entails preparing your organization to respond to ransomware attacks that slip through the cracks. This means maintaining robust incident response capabilities, so that security teams can act quickly to stop an initial infection from spreading. It also means testing your backup systems so that you can be confident that you could restore critical systems and data in time to protect the continuity of your operations, should the worst-case scenario occur. Finally, you should re-evaluate your cyber resilience plan on a regular basis to ensure that it has been updated to reflect the most prevalent current threats.

Internal auditing is an incredibly important—and often overlooked—part of cyber resilience. Too few organizations test their backup and recovery processes as often as they should. Automation can help with this, but nothing can substitute for vigilance. Testing, auditing, reviewing policies and procedures regularly—all of these are ways to keep your eyes open.

—Mike Jackson, Senior Technical Sales Engineer, Carbonite/OpenText

Phishing

Tried and true but perennially effective, phishing remains one of the most popular methods for distributing malware, capturing credentials, and drawing traffic to malicious URLs. The threat landscape is ever-shifting, and phishing attacks continued to evolve throughout 2023. In particular, there was a notable move towards greater customization, likely driven by broad adoption of generative AI and large language models (LLMs).

In 2023, we quarantined approximately 7.7 billion email-based threats, exemplifying a wide variety of attack tactics. Among these, about 817 million were phishing or spearphishing attempts. This represents a significant decrease in volume, about 25% less than the previous year. However, it should not be interpreted to mean that phishing now poses less of a threat. In fact, the opposite is true: threat actors appear to be taking a much more intentional and targeted approach to tricking their victims.

Generative AI and LLMs make it far cheaper and easier to send large volumes of messages that are individually tailored and highly convincing. These technologies also facilitate the creation of fluent-sounding communications in multiple languages, expanding the global reach of phishing attacks. These capabilities are enabling attackers to scale up spearphishing operations, which used to require far more time, effort, and labor to conduct. In essence, the widespread availability of generative AI is beginning to blur the distinction between phishing (a volume-based undertaking) and spearphishing (where attackers invest in greater message personalization in hopes of increasing open and click-through rates.)

"As threat researchers, what we're seeing is better wording, increased customization and more realistic spoofing of companies and brands in email attacks," says Troy Gill, Senior Manager of Threat Intelligence at Zix and OpenText. "Phishing emails are using company language, corporate logos and landing pages that are almost impossible to distinguish from a legitimate business's login portal. The quality of the content has been getting better and better, too. It's becoming more difficult for end users to spot, which is important, because they're the last line of defense. This makes security awareness training more important than ever."

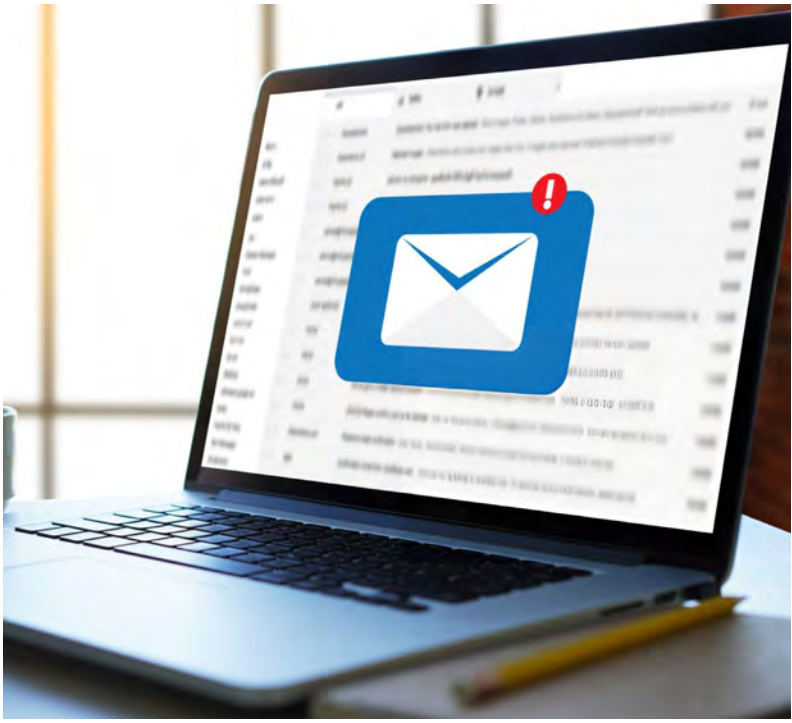
As threat researchers, what we're seeing is better wording, increased customization and more realistic spoofing of companies and brands in email attacks

This year, email threat researchers have also observed a greater focus on supply chains, both digital and physical. Shippers and operators of maritime vessels have been experiencing highly targeted attacks. And software supply chains remain an attractive target because they represent the opportunity to exploit a trusted relationship to potentially infect thousands of victims at the same time.

Malware and attachments

The volume of email with malware attachments increased significantly in 2023, up 35% from 2022's numbers. In total, we quarantined about 223 million messages that included malicious attachments. Reasons for the increase might include geopolitical conflict and unrest, but it's also possible that generative AI is making it easier to write both malicious code and email content.

Email remains a simple and efficient method for threat actors to deliver malware, though the file types most commonly used have changed in recent years. Since Microsoft Office 365 began blocking the download of macros from the internet by default, attackers have adjusted their tactics, more often delivering .htm files that supply a link inviting prospective victims to download a file. This tactic requires that victims complete multiple steps in sequence before the malware can be delivered, making infection somewhat less likely—or requiring a greater number of attempts before attacks can succeed.



Obfuscation tactics

Naturally enough, threat actors don't want to advertise the fact that they're sending email messages with malicious links or attachments. They've become progressively more creative when trying to conceal deceptive content. Today, these often appear in the form of QR codes that, once scanned by the victim's mobile device, direct them to a malicious website. Though it's not new, this form of phishing, dubbed quishing, exploded in popularity over the course of 2023.

Attackers are also inviting their victims to cross communication channels, including voice calling. In what's known as telephone-oriented attack delivery (TOAD), the phishing email includes a telephone number to call, usually accompanied by the claim that there's an urgent issue in need of attention. This malicious omnichannel strategy isn't new, but recently attackers have inserted images into the body of the email message (usually in PDF form) to better avoid detection while credibly imitating brand logos and imagery. Figures 2 and 3 show two recent examples of malicious callback emails observed by our threat researchers.

We also observed a significant increase in the use of legitimate services to conduct phishing attacks. When employing this tactic, known as "living off the land" (Lotl) phishing, threat actors make use of a known and trusted URL that redirects to a malicious site or hosts the phishing payload itself. Because these services are also used for a legitimate business purposes, they cannot simply be blocked outright.

In last year's report, we remarked upon the significant increase in Lotl phishing activity that we'd observed, but this year's numbers are even larger. In total, we observed 199.7 million instances in which this tactic was employed

Figure 2

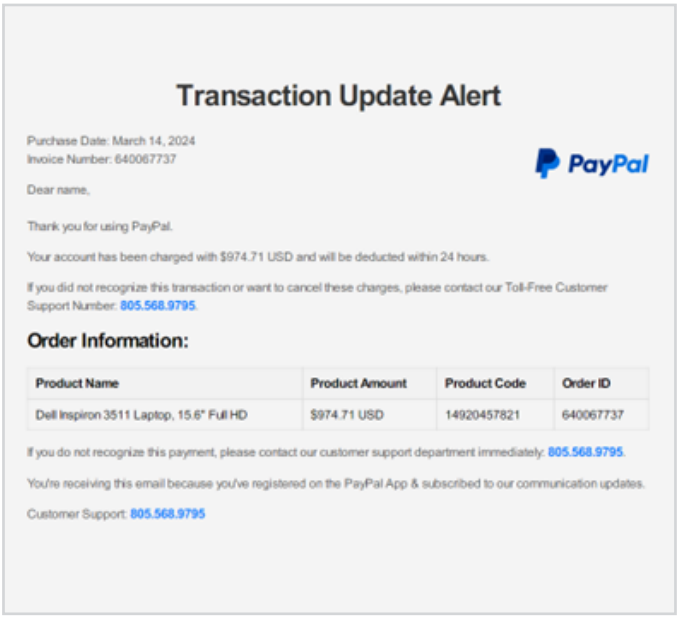
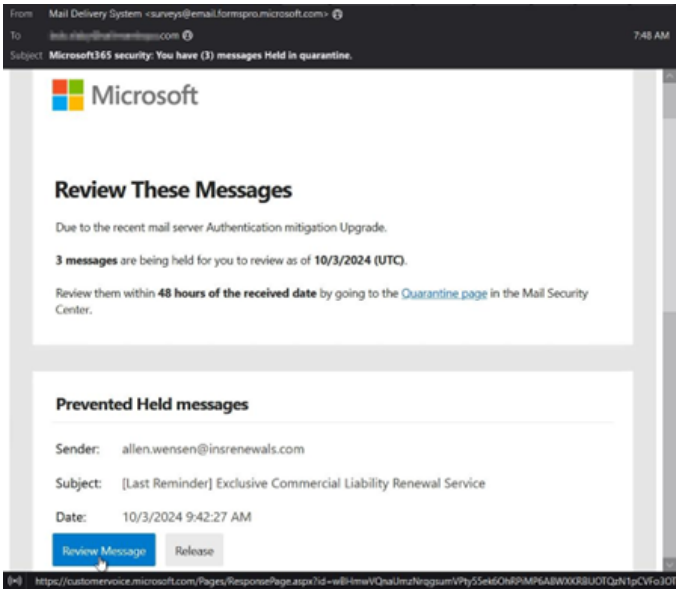


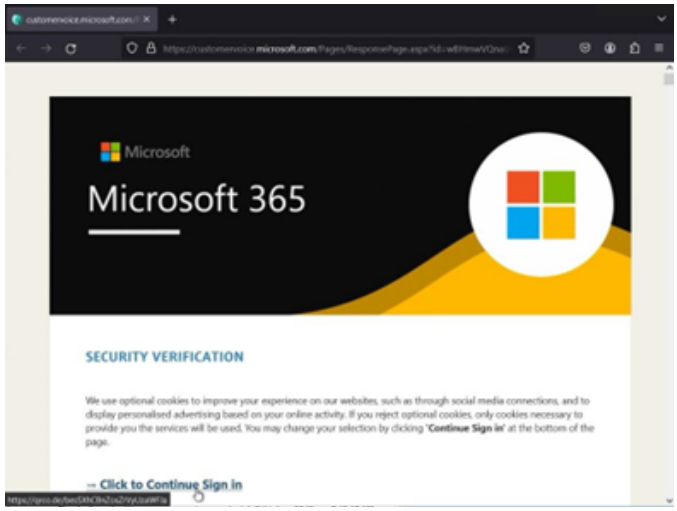
Figure 3

in 2023, an increase of 48.7% year over year. The most commonly abused services in the LotI phishing attacks that we observed in the last quarter of 2023 were Google APIs and Windows.net.

Microsoft remains the most frequently-spoofed brand in a broad array of attacks. In the example shown below, the malicious message appears to be a Microsoft 365 security notification informing its recipient that their email messages are being held in quarantine. Because the message was sent from a Microsoft server, it appears more authentic than it otherwise would.
In this case, the email was sent from a compromised Dynamics 365 customer account, a service that's intended to provide survey capabilities. The payload URL in the message body was also hosted on the microsoft.com domain, increasing the apparent legitimacy of the communication.

Victims who click the sign-in link would then be redirected to a malicious site that closely resembles the actual Microsoft 365 login page. This site is not hosted by Microsoft.





Expert advice for SMB stakeholders

One challenge that small to mid-size organizations face is that threat actors don't discriminate. SMBs encounter the same attacks that large enterprises do. With businesses large and small moving to the cloud, there's greater emphasis on single sign-on (SSO), and Microsoft has been pushing for federated identity. Attackers are working hard to compromise those credentials, because it gives them access to multiple applications—often containing sensitive data—all in one place. They don't need to go to salesforce.com, and then to SAP, and then Workday, etc.

At the same time, the most devastating attacks—like the zero day, software supply chain attacks—remain very rare. Organizations that maintain a strong focus on the basics can prevent all of the most common attacks. If you do the right things—like vulnerability management and security awareness training—you'll be very difficult to compromise.

—Paul Reid, Global Head of Threat Intelligence, OpenText Cybersecurity

Conclusion

With the broad adoption of LLMs and generative AI, greater ruthlessness among attackers, and geopolitical unrest adding fuel to the fire, 2023 proved to be a challenging year for cyber defense. As phishing campaigns got personal, ransomware attack volumes reached a new peak, and malware infection rates trended upward for the first time in years, cyber adversaries once again demonstrated their apparently limitless capacity to evolve, adapt, and innovate.

What does this mean for stakeholders in small and mid-sized organizations? In the 2024 OpenText Threat Perspective, we've presented the most relevant insights from our threat research for this audience, but we also want to equip our readers with insights that will help them protect themselves against today's most prevalent threats.

Attackers continue to seek out novel ways to bypass defenses, infect victims' devices, and commit fraud, extortion, and data theft. They're constantly on the lookout for new strategies to employ, such as inserting QR codes into phishing emails or varying the attachment types used to disseminate malware. It often seems like every step forward that law enforcement takes in their efforts to stop cybercrime is quickly countered by the group in question, which then re-forms, recruits fresh talent, and changes its approach. The resulting cat-and-mouse game is one we've seen law enforcement officials and cyber adversaries playing for decades now.

Given that this is the case, it's unrealistic to expect that any organization—especially one without limitless resources and funding—can prevent all present and future cyberattacks. But this doesn't mean that the situation is hopeless. By maintaining a strong focus on cyber resilience, it is possible to prevent the great majority of attacks from succeeding. It's also possible to limit the damage and disruption that your organization would experience, and accelerate recovery if an incident should occur.

To build the most effective defenses possible for your organization, the key is to adopt a multi-layered approach. With multiple overlapping tools, systems, and processes in place to safeguard your data and improve your ability to recover, you can decrease the likelihood that attackers will compromise your organization, and reduce the impact that a successful attack would have on your operations.

We recommend that organizations improve their ability to prevent, detect, and recover from malware and ransomware infections across all areas of the attack lifecycle. Every organization should be able to, at a minimum:

- Inspect all incoming emails for malicious attachments, and block potential threats.
- Keep all PCs and servers fully patched at all times
- Run effective antivirus software and endpoint protection on every device on the network and in the organization.
- Maintain robust identity governance processes, including role-based access controls.
- Implement multi-factor authentication (MFA) for all organizational accounts and resources.
- Train users to spot phishing emails and malicious communications.
- Back up all critical systems and files regularly
- Develop and practice an incident response plan, so that all stakeholders know what to do in case of a cyber incident.
- Test backup capabilities to ensure that you can restore critical systems and data to protect the continuity of your operations.

When building out these capabilities, it's important to remember that not all solutions are created equal. Those that leverage threat intelligence, machine learning, and behavioral analysis to detect and block malware attacks are likely to be more accurate and effective than solution relying on yesterday's signature-based methods.

Immutable backups offer greater protection for your data, while backups that are stored in a place that's separate from the network are less vulnerable to threats (but slower to restore from). Security awareness training that incorporates threat intelligence will be able to teach users to spot current attack tactics, not those that were popular three or six months ago.

Cyber criminals are inventive and resourceful, but cybersecurity decision-makers are too. By reading this report—and thus making yourself aware of recent trends in the threat landscape—you've taken a key step towards cyber resilience for your own organization. That kind of awareness is exactly what's needed to stay ahead of attackers.

What our experts are saying

In recent years, we've seen security practices and data backup strategies become more and more closely intertwined. Today's advanced backup solutions, for instance, have built-in ransomware detection capabilities, so that they can immediately notify security teams or administrators if suspicious file characteristics are observed. When it comes to protecting end users, it just makes sense to integrate intelligent file behavior analysis into backup tools. It's efficient and effective, and that's the way the industry is headed.

—Vladimir Holly, Senior Solutions Consultant, OpenText Cybersecurity

AI is still only in its infancy, but it's maturing really quickly. There are already AI engines out there that can launch denial of service attacks in an instant, and that's just the beginning. The landscape is changing fast, and it's only going to get faster. It's always good to start planning for the future before it's upon us. It will probably take AI to battle AI, so companies and vendors will have to think about how to best make use of these technologies."

—Mike Jackson, Senior Technical Sales Engineer, Carbonite/OpenText

One of the benefits of working with a security awareness training vendor who also offers a broad portfolio of other products and services is that vendor will have a deeper understanding of the threat landscape. We directly integrate content from our threat researchers' observations into our security awareness training, and we've been doing that for years now. This way, our phishing simulation templates are based on the latest attacks—they're really at the bleeding edge. You don't want to train your users on the attacks that were prevalent three years ago. You want the ones that are prevalent this week."

—Troy Gill, Senior Manager of Threat Intelligence, Zix/AppRiver/OpenText

A focus area for us in our efforts to expand the scope and effectiveness of security awareness training is assigning risk scores to individual users. How much of an employee's personal information is exposed on the open web, how much is for sale on the dark web—these are pieces of the equation. Other factors include that person's job role and what their access permissions are. And how they've performed in security awareness training is important, too. Ultimately, I think these scores will be combined with other data sources feeding extended detection and response solutions that will help security teams rapidly solve puzzles and quickly figure out which anomalies are truly malicious. "

—Kenneth Thon, Solutions Consultant, OpenText Cybersecurity

Attackers are always practicing deception—attacking one part of the network openly while their real attention is focused on slipping into the back door while you're distracted. That's where behavioral analytics really shines: it can highlight unexpected changes in customer environments. When we threat hunt using behavioral analytics, we have no idea what we're going to find, what attacks we're going to see. But we know the system will give us a series of behavioral indicators we can use to figure out what's really taking place. Human-machine teams that leverage artificial intelligence and machine learning to identify behaviors are much better at protecting our customers than simply looking for tools, tactics, and procedures would be."

—Paul Reid, Global Head of Threat Intelligence, OpenText Cybersecurity

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.