

2023 H1 Global Threat Analysis Report

The 2023 H1 Global Threat Analysis Report explores changes in today's threat landscape as cybercriminals shift their attention from network DDoS attacks to more sophisticated, application-level Web DDoS attacks. Discover the latest targets, tactics and motivations so you can proactively protect your organization.



Executive Summary

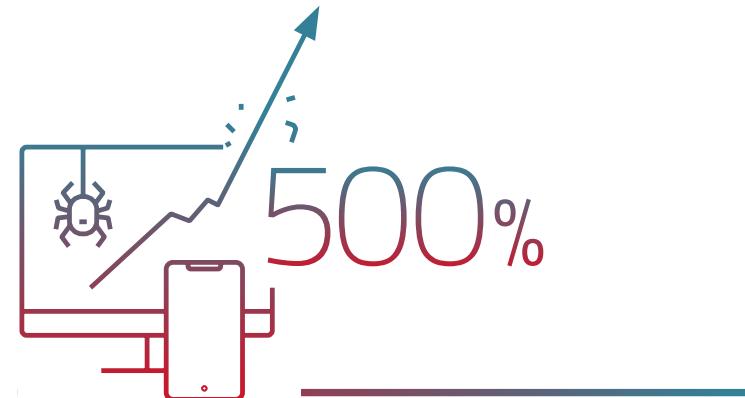
The cybersecurity landscape continued to rapidly evolve in the first half of 2023 (H1), when we observed a significant shift in Denial-of-Service (DoS) attack patterns. Increasingly, DoS attacks are progressing to layer 7 (L7), targeting not just the online applications and their APIs but also essential infrastructure such as the Domain Name System (DNS).

We noted a considerable surge in DNS query floods during H1 2023. Furthermore, Web Distributed Denial-of-Service (Web DDoS) attacks have become more sophisticated, utilizing high Request Per Second (RPS) traffic while randomizing multiple elements of the request to create seemingly legitimate traffic. This tactic has found favor with numerous hacktivist groups, including Anonymous Sudan and NoName057(16).

Hacktivists constitute a major part of the L7 DDoS problem. The effectiveness of these attacks has been significantly amplified by the use of patriotic volunteers in crowdsourced [botnets](#) or by providing them with custom attack tools and detailed tutorials on how to execute such attacks.

Network-layer attacks are better understood, and arguably easier to detect and mitigate compared to the new generation of HTTPS Floods organizations are facing in 2023. Since HTTPS Floods have been around for a few years, they are sometimes considered old news. However, the volume and intensity of the new generation of HTTPS Floods has increased dramatically while the sophistication and viciousness of attackers continue to grow. That is why we like to refer to these new-generation HTTPS Floods as Web DDoS attacks.

There's a discernible trend among malicious actors transitioning to cloud-based operations. By switching from compromised IoT devices to much more scalable and cost-effective cloud services providing high-speed internet connectivity, they can now orchestrate a limited number of very powerful



While in 2022 we observed a near linear growth per quarter, **in H1 2023 the number of malicious web application transactions skyrocketed by 500%**

nodes within their control. The advantages are considerable: they maintain control over their servers, suffer no loss from device reboots, and run a lower risk of detection by security researchers. Utilizing bulletproof hosting and proxy services that provide frequently rotating residential IP addresses creates the perfect platform to launch high-frequency, sophisticated attacks such as Web DDoS.

While the total number of [DDoS](#) events decreased by 33% compared to the first half of 2022 and the average attack volume per customer per month declined by 70%, the number of malicious web application transactions skyrocketed by 500%. In 2022 we observed a near linear growth in the number of malicious web transactions per quarter; in H1 2023 this growth accelerated exponentially. While the number of DDoS events in H1 2023 was below the number for H1 2022, it surpassed the total for the whole of 2021.

The narrative for 2023 is clear: as attackers ascend the network stack, they're increasingly targeting online applications and their infrastructure. Global DDoS activity hasn't reduced compared to 2022, but we observed a sizable proportion of network DDoS attacks shifting to more sophisticated application-level Web DDoS attacks. The task for organizations going forward is to proactively adapt to these evolving cyberthreats.

We noted a **considerable surge in DNS query floods during H1 2023**. Furthermore, Web Distributed Denial-of-Service (**Web DDoS**) attacks have become **more sophisticated**, utilizing high Request Per Second (RPS) traffic while randomizing multiple elements of the request to create seemingly legitimate traffic

Network-level DDoS Attack Activity

In H1 2023, UDP was the most abused protocol for volumetric network DDoS attacks, accounting for 63.8% of the total attack volume. TCP Out-of-State attacks followed with nearly 20%. DNS amplification produced the highest volume of amplification attacks at 61.6%. Resource exhaustion attacks, which exploit vulnerabilities in system resources and are characterized by high packet rates but low traffic volume, were also common. Attack vector distribution by packet rate showed a preference for TCP flag floods and DNS-A query floods in resource exhaustion attacks.

Compared with earlier years, the number of mid-sized attacks is growing very slowly. The number of small attack vectors is growing, but not as fast as last year. Large attack vectors in H1 2023 demonstrated a very steep growth compared to 2022.

In 2021 and most of 2022, less than 1% of all attack vectors were DNS Flood vectors, but this ratio doubled to almost 1.8% by Q2 2023. DNS Floods—application-layer attacks that overload a server's capacity to manage DNS requests—have also increased in scale since Q4 2022, with the largest attack in Q2 2023 reaching a rate of 1.29 million DNS queries per second. Despite this, the traffic volume of these attacks remained under the 1Gbps threshold as they aimed to overload servers rather than saturate internet connections. The most common DNS query used in DNS Floods in H1 2023 was the regular hostname to IPv4 query, accounting for 76.5% of all DNS Floods, followed by MX, TEXT, OTHER, and AAAA queries.

In terms of global DDoS events, the EMEA region (Europe, the Middle East and Africa), accounted for 66.2% of the attacks blocked in H1. Conversely, the Americas (North, Central, and South America) blocked a smaller number, 24.9%, but interestingly faced an almost equal attack volume to EMEA. This indicates that the threat level in the Americas is on par with EMEA, despite fewer blocked attacks. The APAC region (Asia and the Pacific) blocked 8.98% of DDoS events and faced approximately 5% of the global attack volume.

Network Level DDoS Attack Trends



UDP represented 63.8% of volumetric network DDoS attacks



TCP Out-of-State attacks represented roughly 20% of volumetric network DDoS attacks



DNS amplification produced the highest volume of amplification attacks at 61.6%

Estonia, Poland, Spain, the United Kingdom, and the Netherlands in the EMEA region, and the United States in the Americas, all emerged as major targets of DDoS attacks, suggesting continued focus by attackers on these countries.

To tackle DDoS threats, a global, decentralized approach is needed, preferably eliminating threats closer to their source. This reduces the malicious traffic burden on the larger internet infrastructure. Scrubbing centers, designed to filter out malicious traffic and ensure only legitimate data reaches its intended destination, play a pivotal role in this process. Distributed worldwide, these centers provide global DDoS protection, maintaining service continuity even during an attack. Interestingly, Ashburn (United States) handled nearly half of the total global malicious traffic. Frankfurt (Germany) blocked 20% of the attack volume, while London (United Kingdom) handled 10%. Together, Dallas and San Jose (United States) accounted for 12% of blocked global attack volume,

demonstrating the importance of each scrubbing center in mitigating global DDoS threats.

In H1 2023, DDoS attack volume distribution across industries was unevenly distributed, with the research and education sectors bearing almost a third of the attacks. Service providers faced close to 20%, while the technology sector accounted for 11.6%. Gaming and telecom were also frequently targeted, representing respectively 7.1% and 5.61% of total attacks. Compared to 2022, the gaming industry saw attack volume surge by almost 20%, with industries such as manufacturing, energy, and retail also experiencing increases. However, e-commerce, communications, telecom, utilities, and service providers observed a slight decrease. The number of attacks increased most in utilities (+18%), telecom (+3.1%), and energy (+2.7%), while there were slight reductions in the retail, transportation, finance, communications, and manufacturing sectors.



DNS Floods have also increased in scale since Q4 2022, with **the largest attack in Q2 2023** reaching a rate of 1.29 million DNS queries per second

DDoS Attack Volume by Industry

20%
Service providers
Tech

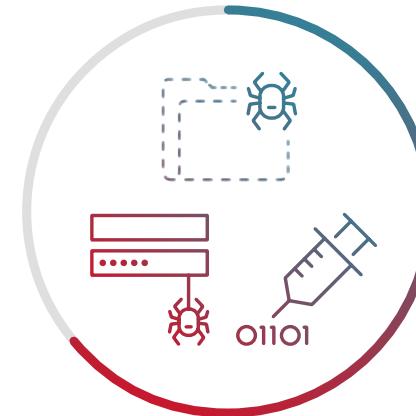
7.1%
Gaming
Telecom

Web Application Attack Activity

In H1 2023, the most significant security violation was predictable resource location attacks, accounting for a major portion of the total attack count. These attacks aim to uncover hidden web application resources by guessing common names for directories or files. Following this, SQL and code injection attacks were the second and third most common. Together, these three types of attacks accounted for 64% of the total attack activity on web applications and APIs. In Q2 2023, SQL injection attacks increased significantly, reaching almost the same frequency as predictable resource location attacks.

The majority of blocked web security events originated from the United States, with Germany, Russia, the United Kingdom and Italy completing the top five. While the United States has consistently dominated the attack landscape, it's crucial to note that the origin country doesn't necessarily reflect the nationality of the threat actors. Often, actors use cloud-hosted servers, VPNs, proxies, and compromised servers to conceal their real origins. The country from which an attack originates is usually chosen based on the victim's location to avoid potential geo-blocking or to misdirect attribution during false flag operations.

The retail industry was the most targeted by web application attacks, accounting for 35.5% of all attacks. Carriers and SaaS providers followed as the second and third most attacked industries, representing 10.6% and 8.08% of web application attacks, respectively. The transportation sector (5.12%), government entities (5%), educational institutions (4.77%), utility providers (4.65%), and healthcare sector (3.3%) also experienced significant web application attacks.



64%

Combined web app and API attack activity from **predictable resource location attacks, SQL injection attacks and code injection attacks**

Industry Share of Web Application Attacks

35% Retail

10.6% Carriers

5.12% Transportation

8.08% SaaS providers

Most Blocked Web Security Events

- 1. United States**
- 2. Germany**
- 3. Russia**
- 4. United Kingdom**
- 5. Italy**



Unsolicited Network Activity

In H1 2023, Radware's Global Deception Network (GDN), which collects unsolicited events or random scans and attacks that don't target known services or organizations, recorded a substantial rise in such activities. The network collected a total of 2.05 billion unsolicited events, representing a marked increase compared to the total 2.65 billion events gathered in all of 2022. On average, the network recorded 11.3 million events per day, an increase of 55% compared to the previous year. There was also a 15% increase in unique IPs per day, with an average of 60,775 recorded in H1 2023 compared to 52,860 in 2022. Although the number of malicious devices on the internet increased only slightly, their activities became significantly more aggressive.

The most attacked TCP service was SSH, followed by Telnet and VNC. Other frequently targeted services included HTTP, Redis, HTTPS, SMB, TR-069, RDP, and the popular IP camera web UI port, 8080. TR-069 emerged as a new entry in the top ten for H1 2023, a prominent protocol from the Mirai era that re-entered the global scanning activity six years after its first major exploit.

Most of the scanned and exploited UDP ports were also among the top contenders in 2022. LDAP, which had been in the top ten, was replaced by OpenVPN in the tenth spot. CoAP, which had secured tenth place in 2022, was also displaced during H1 2023. SIP (port 5060) was again the most targeted UDP-based service in H1 2023.

2.05B

Unsolicited events collected
by Radware's Global
Deception Network (GDN)

11.3M

Events tracked per day
up 55% from 2022

The United States was the top country of origin for unsolicited network activity, accounting for 41.2% of all activity in H1 2023. This is almost identical to 2022 when it accounted for 42.5% of all such activity. The Netherlands rose from the fourth position in 2022 to the second in H1 2023, accounting for 16.5% of activity. China remained in the third spot, while Russia dropped from second in 2022 to fourth in H1 2023. The United Kingdom held steady in the fifth position. However, again it's important to note that the apparent origin of an attack doesn't necessarily reflect the true location of the attacker, as locations can be spoofed to make it seem as if attacks are originating from different countries.

Many web service vulnerabilities exploited common weak password combinations or hard-coded credentials to gain unauthorized access. The majority of the top 10 abused credentials were simplistic and widely used defaults such as "admin", "password", and "1234567890", often remaining unchanged from the default settings during device installation. A standout in this list was "report:8Jg0SR8K50", a hard-coded credential found in digital video recorders (DVRs) from the manufacturer LILIN. This vulnerability was publicly disclosed in March 2020 and is notable due to the ubiquity of DVRs and associated security cameras in the Internet of Things (IoT) landscape.

↑15%

Increase in unique
IPs per day

Denial-of-Service Attack Activity

In H1 2023, the number of DDoS events per customer blocked by Radware's Cloud DDoS Protection Service decreased by 33% compared to H1 2022 but grew by 103% compared to H1 2021. The H1 period of 2023 represented 32% of the DDoS events observed in 2022 and saw 7% more events compared to 2021.

In H1 2023, on average, the service blocked 6,271 DDoS events per customer, per month. In 2022, the service blocked 10,266 events per customer, per month. In 2021, the number of events per customer per month was 4,258. The average number of events blocked per month for a customer decreased by 39% compared to 2022 but increased by 47% compared to 2021.

Figure 1: Evolution of blocked DDoS events per quarter over time

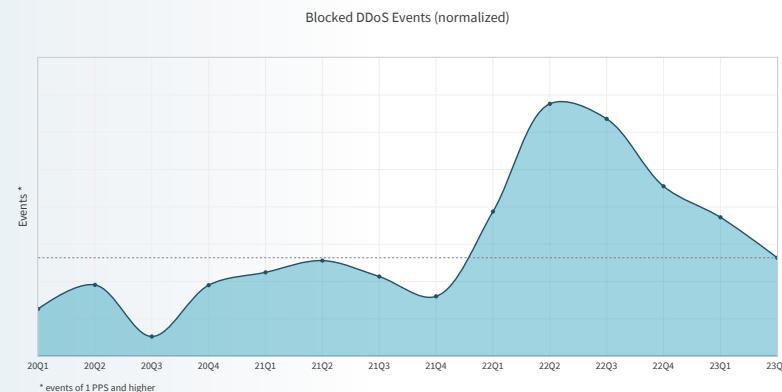
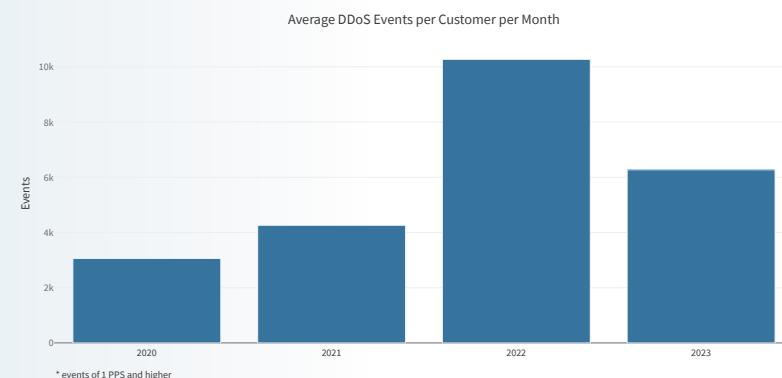


Figure 2: Average number of DDoS events blocked per customer per month



Regions and Industries

Regions

The EMEA region blocked 66.2% of global DDoS events. The Americas, while accounting for a lower 24.9% of blocked DDoS events, saw a similar attack volume compared to EMEA, 47.4% and 47.7%, respectively. This suggests that while the number of blocked attacks may be lower, the actual threat level in the Americas is comparable to EMEA.

The APAC region blocked 8.98% of DDoS events and faced about 5% of the global attack volume. Although these figures are lower than the other regions, they still represent a significant burden.

Organizations based in Estonia, Poland, Spain, the United Kingdom and the Netherlands experienced the highest attack volumes, indicating that organizations in these countries have the highest probability to be hit by volumetric DDoS attacks.

Despite EMEA's overall effectiveness in blocking a large proportion of DDoS events, the attack volume in these countries suggests that as attackers continue to focus on this type of attack they remain an area of concern.

On the other side of the Atlantic, the United States emerged as another hotspot for DDoS attacks. The attack volume in the United States was just behind that of the top five European countries. This aligns with the data indicating that the Americas region faced a similar attack volume as the EMEA region despite blocking fewer attacks.

Addressing DDoS attacks effectively necessitates a worldwide, decentralized strategy. The best method to mitigate distributed threats is by eliminating them as close to their source as possible, significantly reducing the strain of malicious traffic on the wider internet infrastructure.

Figure 3

Blocked DDoS events per region

2023 H1 Blocked Events* (normalized)

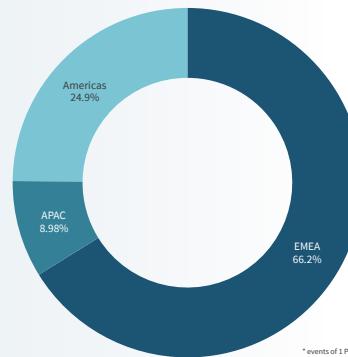


Figure 4

Blocked DDoS volume per region

2023 H1 Blocked Volume (normalized)

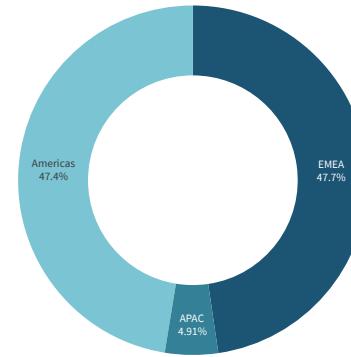


Figure 5: World map of DDoS attack volume per country

2023 H1 Attack Volume per Country (normalized per customer)



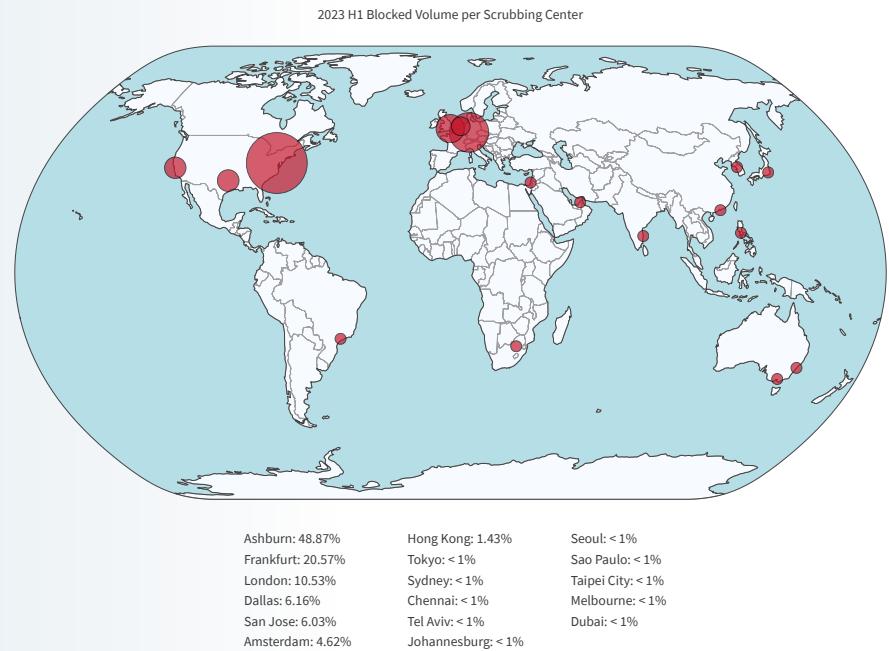
A scrubbing center is a data cleansing facility designed to help organizations protect their data and infrastructure from DDoS attacks. When incoming network traffic is directed through a scrubbing center, the role of the center is to “scrub” the data, that is to filter out malicious traffic and allow only legitimate traffic to be routed through the Cloud DDoS Protection Service backbone to its intended destination. This process involves the separation of clean data, which is allowed to reach the target server, from the “dirty” or harmful data, which is dropped.

Scrubbing centers should be distributed across the world to provide global DDoS protection and ensure uninterrupted service, even when an attack is underway. The quantity of attack volume intercepted by a scrubbing center offers a reliable indication of the origin of the hostile traffic.

Ashburn (United States) handled nearly 50% of the total global malicious traffic. Frankfurt (Germany) accounted for 20% of the attack volume while London (United Kingdom) consumed 10% of the global attack volume.

In the United States, the cities of Dallas and San Jose jointly accounted for 12% of the total global attack volume blocking. This diverse geographical distribution underlines the critical role of each scrubbing center in the collective fight against DDoS threats.

Figure 6: Blocked DDoS attack volume by scrubbing center



Industries

In H1 2023, certain industries faced a disproportionate share of the total DDoS attack volume. Notably, organizations within research and education bore the brunt with nearly a third of the total attack volume directed at them.

Service providers also faced considerable volumes, with almost 20% of the total attack volume aimed at their operations. Meanwhile, the technology sector experienced 11.6% of the total volume.

Other notable industries that found themselves frequent targets of these attacks included the gaming industry, with a 7.1% share of the attack volume, and the telecom industry, which accounted for 5.6% of the total.

Compared to 2022, during H1 2023 organizations in the gaming industry faced almost 20% more attack volume. Other significant growth industries in terms of attack volume were manufacturing (+14%), energy (+12%), industrials (+9.6%) and retail (+7.1%). Organizations in e-commerce, communications, telecom and utilities as well as service providers saw a slight (less than 1%) decrease in attack volumes during H1 2023 compared to 2022.

Figure 7
Blocked DDoS volume per industry

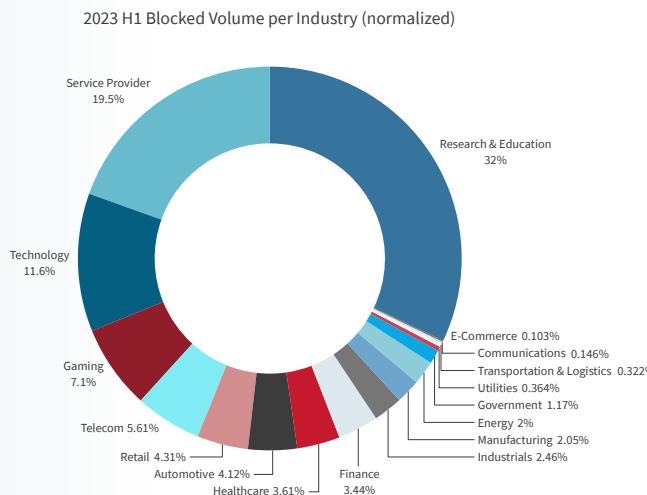
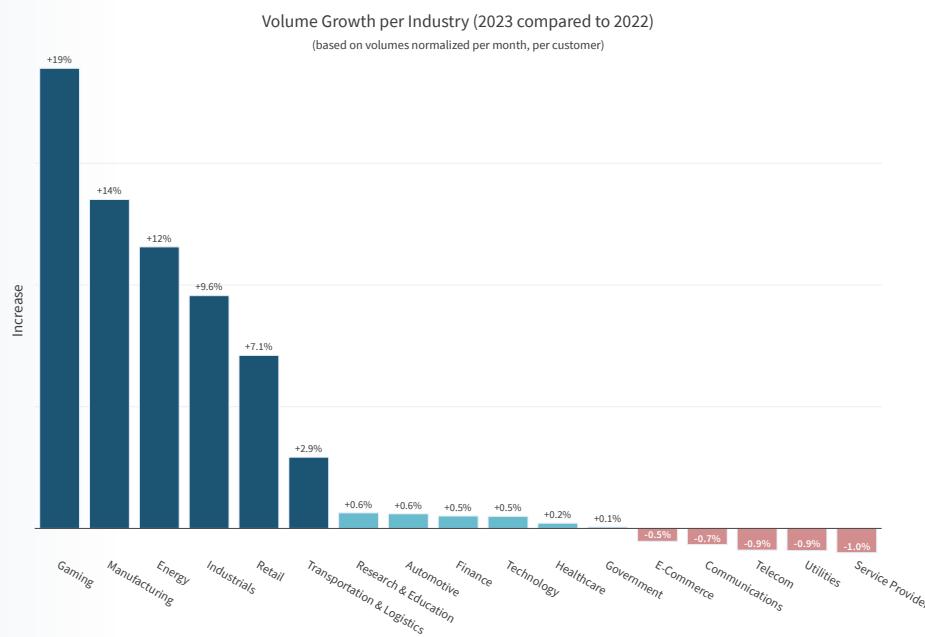
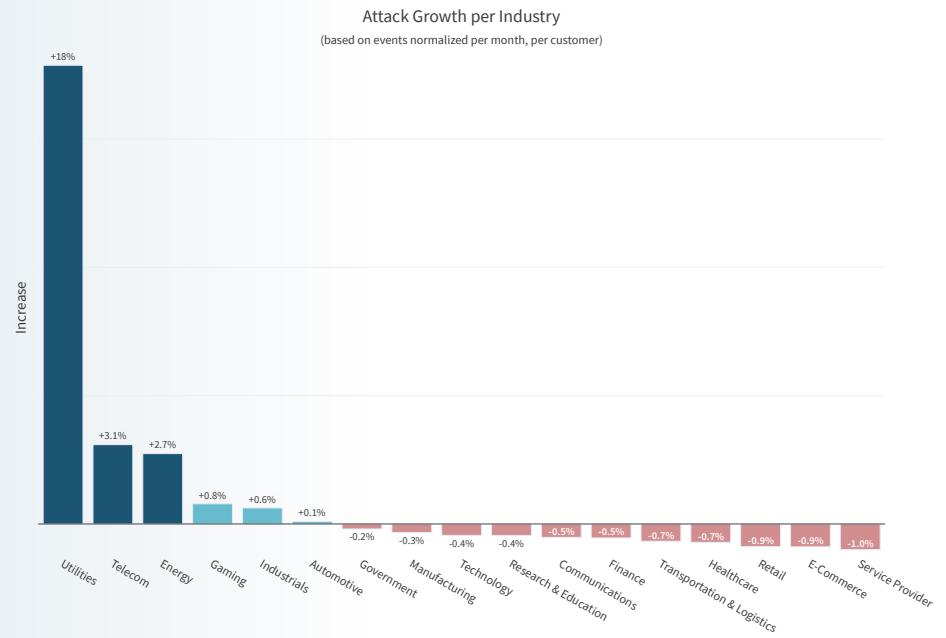


Figure 8
Growth of attack DDoS volume per industry from 2022 to H1 2023



In terms of DDoS attack events, utility organizations saw the largest increase (18%), followed by telecom organizations (+3.1%) and organizations in the energy industry (+2.7%). While the attack volumes targeting organizations in the retail, transportation and logistics, finance, communications and manufacturing industries increased in H1 2023, the number of attack events shrank slightly (between 0.3 and 1%).

Figure 9: Growth in the number of DDoS attack events between 2022 and H1 2023 by industry



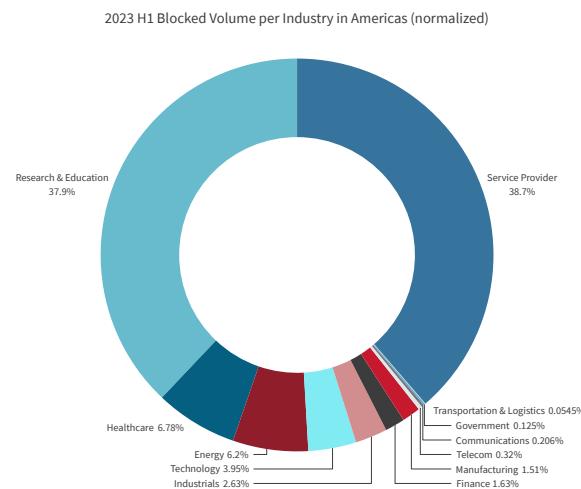
The Americas

(North, Central, and South America)

In H1 2023, service providers and research and education organizations were the main targets, constituting 38.7% and 37.9% of the total DDoS attack volume respectively. This indicates a significant cyberthreat focus on these sectors in the Americas.

Further down the list, healthcare organizations were subjected to 6.8% of the attack volume. Energy companies experienced a slightly lower proportion of attacks, receiving 6.2% of the total volume. Technology organizations, while also significantly affected, saw a smaller proportion of the overall attack volume at 3.95%.

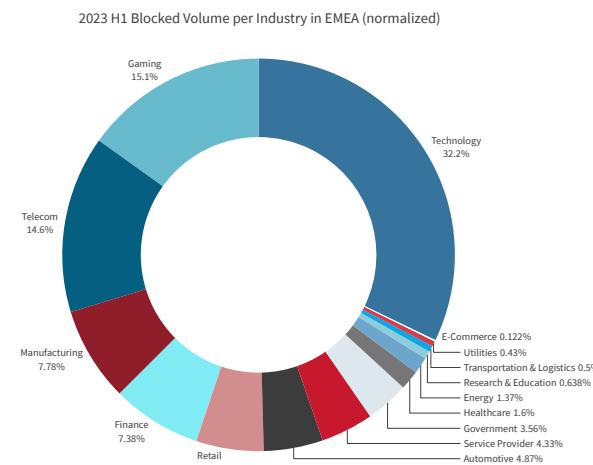
Figure 10: Blocked DDoS volume per Americas industry



EMEA (Europe, Middle East and Africa)

In the EMEA region, the distribution of DDoS attack volume during H1 2023 showed a broader spread across various industries. The technology sector was the most affected, accounting for 32.2% of the attack volume. This was followed by the gaming industry (15.1%), telecom (14.6%), manufacturing (7.78%), finance (7.38%), and retail (5.55%).

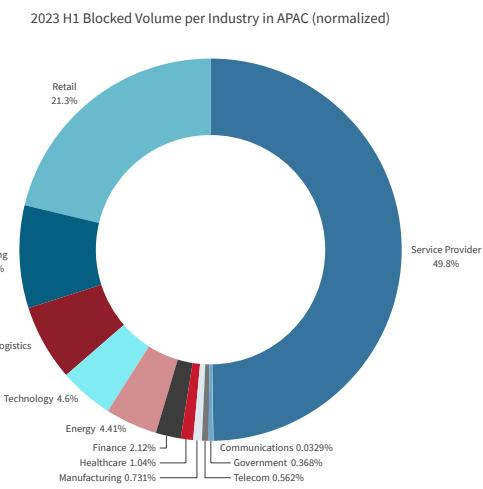
Figure 11: Blocked DDoS volume per industry in EMEA



Asia Pacific (APAC)

In the APAC region, service providers bore the brunt of DDoS attacks during H1 2023, with 50% of the total attack volume targeting this sector. The retail industry faced a significant proportion of the remaining volume, accounting for 21.3%, followed by the gaming industry at 8.68%, and transportation and logistics at 6.44%.

Figure 12: Blocked DDoS volume per industry in APAC



Attack Protocols

In 2023, UDP was again the most leveraged protocol for volumetric network DDoS attacks. UDP and UDP Fragment floods represented 63.8% of the total attack volume in H1 2023. TCP Out-of-State attacks represented almost 20% of the attack volume.

Volumetric network DoS attacks aim to saturate the connectivity of organizations or services by flooding the network with more traffic than it can handle. The use of UDP Floods in volumetric attacks is reflected in the attack vector distribution per vector size in Figure 14.

Attackers leverage reflection and amplification services that are publicly exposed on the internet. If it's UDP and is exposed to the internet, it can be weaponized for DDoS attacks. By reflecting malicious packets from legitimate services on the internet, the attackers hide the origin of their attacks while making them more resistant to simple mitigations such as IP blocklisting. Another motivation to weaponize specific protocols is amplification. Certain protocols are preferred as they provide more amplification. The amplification factor (AF), the ratio between the size of the request and the reply, and the number of available or exposed services on the internet will cause attackers to gravitate to vulnerable protocols and services. A higher AF means a more efficient attack. More exposed services represent a larger total aggregate bandwidth and a higher diversity in source IPs in the attack traffic, making detection harder.

Figure 13: Protocols leveraged by volumetric network attacks

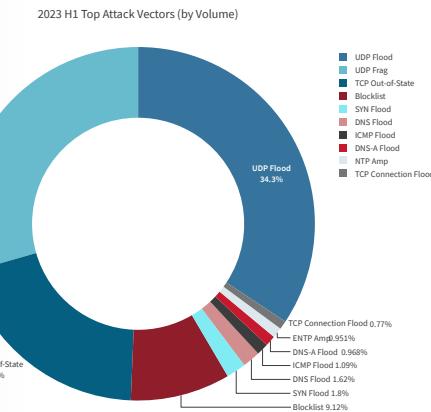
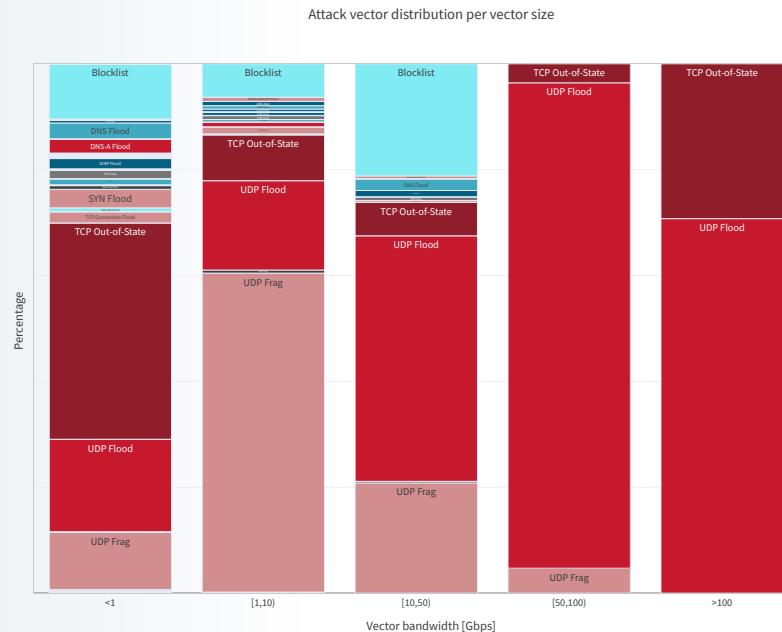


Figure 14: DDoS attack vector distribution per vector size



Some of the most important and top amplification vectors and their associated maximum amplification factors are listed in Table 1.

DNS amplification was the amplification attack vector that generated the most volume in H1 2023, representing 61.6% of the total amplification volume. NTP amplification was the second most abused amplification attack vector, accounting for 34.1% of the volume. Smaller volumes were generated by SSDP, ARMS, Memcached, DHCP Discover (IPv6), Chargen, CLDAP, SNMP and CoAP.

In addition to volumetric attacks, attackers also leverage resource exhaustion attacks. Unlike volumetric attacks, these do not rely on volume but rather on packet rates. Resource exhaustion attacks are designed to exploit vulnerabilities in system resources, such as memory, computing power, or even specific application resources. These types of attacks are characterized by a high packet rate, where a large number of small packets are sent to overwhelm specific elements of a network's infrastructure. As a consequence, the traffic volume associated with resource exhaustion attacks is typically limited.

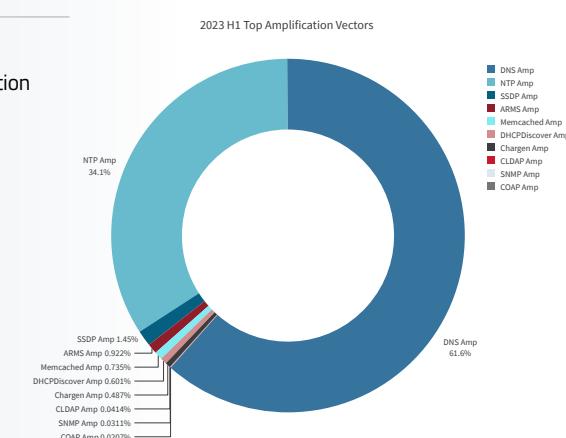
Even if the overall network bandwidth isn't overloaded, these attacks can render targeted systems unresponsive by causing server processes to consume too much CPU or memory, by filling up connection tables, or by filling up disk space or database connections.

Table 1: DDoS amplification attack vectors

Amplification Vector	Amplification Factor	Port
NTP	500x	UDP/123
DNS	160x	UDP/53
SSDP	30x	UDP/1900
Memcached	50,000x	UDP/11211
Chargen	1,000x	UDP/19
ARMS	30x	UDP/3283
CLDAP	50x	UDP/398
DHCPDiscover	25x	UDP/37810
SNMP	880x	UDP/161
RDP	80x	UDP/3389
CoAP	30x	UDP/5683
mDNS	5x	UDP/5353
WSD	500x	UDP/3702, TCP/3702
Plex (PMSSDP)	5x	UDP/32410

Figure 15

Top DDoS amplification attack vectors



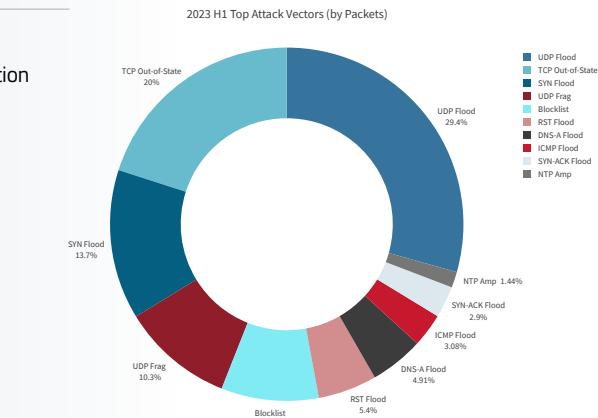
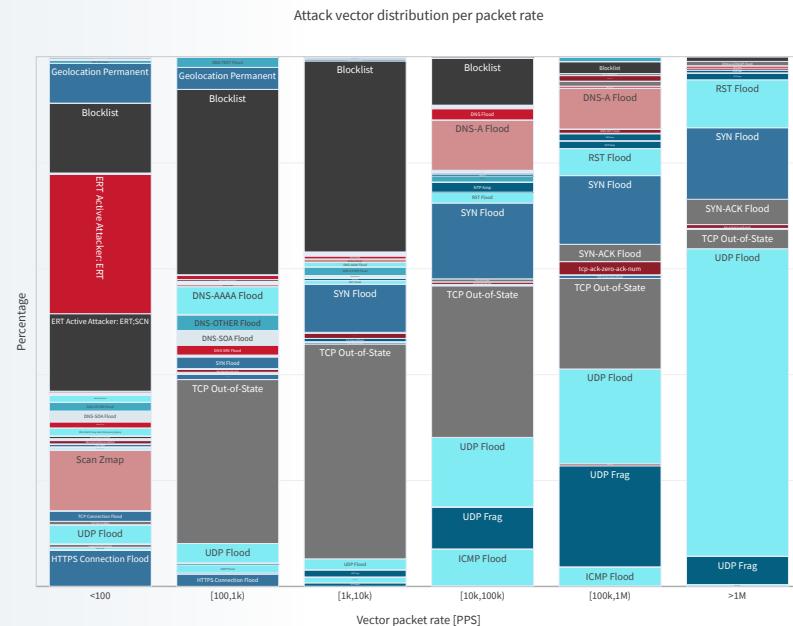
In H1 2023, 29.4% of all blocked packets originated from UDP floods. UDP floods are also responsible for most of the volume. Generating a large volume requires high packet rates. The maximum size of an internet packet is limited to less than 1500 bytes. To saturate high bandwidth connections with terabit per second attacks, attackers need to leverage high packet rates to reach such high traffic levels.

TCP Out-of-State (20%) and TCP SYN Flood (13.7%) attacks are resource exhaustion attacks, as are TCP RST (5.4%) and DNS-A (4.91%) Floods. While representing only about 5% of the malicious packets blocked in H1 2023, DNS query floods can cause disruption to the network infrastructure of organizations. It's a tactic that has been used more often by attackers in the last few months (see DNS Floods, page 20).

The attack vector distribution by packet rate demonstrates attackers' preference for TCP flag floods such as SYN, SYN-ACK, RST floods and TCP Out-of-State floods in all attack vectors with higher packet rates, including the highest packet rate attack vectors generating more than 1 million PPS. DNS-A query floods were typically leveraged in attack vectors between 10,000 and 1 million PPS. Other DNS query floods, such as AAAA, SOA and OTHER queries, are more significant for attack vectors between 100 and 1,000 PPS.

Figure 16

Top DDoS amplification attack vectors

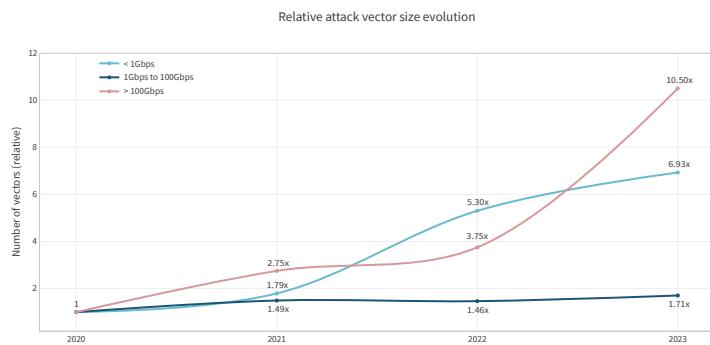
**Figure 17:** DDoS attack vector distribution by packet rate

Attack Vector Characterization

A DDoS attack campaign consists of one or more attack vectors running simultaneously or sequentially over the time of the attack. In this section, individual attack vectors are analyzed to understand and characterize the nature of the DDoS attack threat landscape during H1 2023.

To compare the size evolution, attack vectors are divided into three categories based on their attack size, expressed in bits per second. Small attacks are those below 1Gbps, while large attacks are those above 100Gbps. By normalizing the number of vectors in each size category against the number of vectors in 2020, the relative vector size evolution over time can be compared. For H2 2023, we assume an equal volume of attack vectors in the second half compared to the first half.

Figure 18
Relative DDoS attack vector size evolution



Compared to earlier years, the relative number of mid-sized attacks grew very slowly. The number of small attack vectors grew, but not as fast as their growth last year. In contrast, large attack vectors in H1 2023 demonstrated a very steep growth compared to last year.

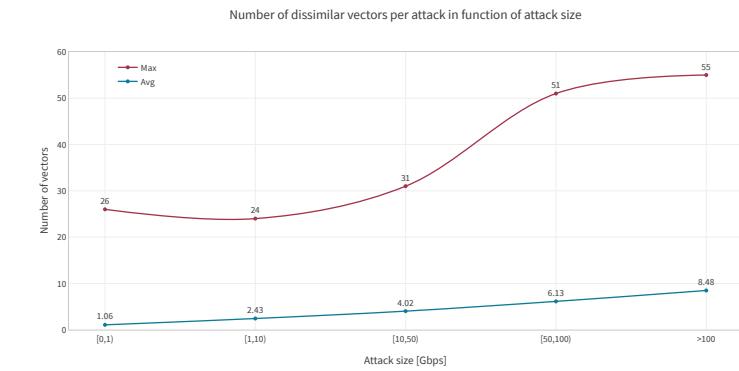
In conclusion, H1 2023 can be characterized as a period in which attack sizes rapidly grew larger.

Attack Complexity

While a single attack vector can be devastating, attackers will often leverage multiple and dissimilar vectors to increase the impact, confuse detection and make attack mitigation harder. When attackers leverage multiple amplification servers and protocols, a single attack will consist of several dissimilar concurrent attack vectors. Attackers will also change attack vectors over time to evade mitigation using manually crafted access control lists. While changing attack vectors is usually not sufficient to evade automated DDoS mitigation services, it can still be effective against targets that have inadequate DDoS protection in place.

An attack is considered more sophisticated or complex when it leverages a greater number of dissimilar attack vectors. Attacks using multiple concurrent or changing attack vectors are harder to mitigate. Fast shifts and high numbers of concurrent vectors are impossible to mitigate without automated mitigation solutions.

Figure 19
Number of dissimilar DDoS attack vectors per attack as a function of attack size



The average complexity of attacks in H1 2023 increased with attack size. Since the average number of attack vectors in a single attack can't be smaller than one, smaller attacks exhibited a more isolated character as their average vectors per attack came closer to this number. Attacks above 1Gbps on average had more than two dissimilar attack vectors per attack, which almost doubled in number for attacks above 10Gbps. Attacks above 100Gbps had on average more than eight dissimilar attack vectors with the most complex attacks leveraging 55 dissimilar attack vectors.

Application-layer Attacks

DNS Floods

The digital era has catalyzed rapid growth in online commercial activities, making e-commerce and online platforms a vital component of the global economy. However, this technological advancement is not without its vulnerabilities. A crucial and ubiquitous part of this digital ecosystem is DNS, which acts as the internet's phonebook, translating human-readable domain names into their underlying IP addresses. When a DNS service is subjected to a cyberattack, such as denial-of-service or distributed denial-of-service, the disruption caused can be catastrophic for businesses.

DNS denial-of-service attacks come in various forms, each with unique techniques and impacts. Here are the most common attack types:

DNS Amplification Attack

This is a type of network-level, reflection-based, volumetric DDoS attack where the attacker crafts a DNS query packet with a forged source IP address (the victim's). It sends it to a legitimate open DNS resolver which subsequently replies to the victim with a large amount of data. The goal is to overwhelm the victim's network with traffic.

DNS Flood Attack

A DNS Flood is a type of application-layer DDoS attack that seeks to overload a DNS server with a high volume of requests until it becomes unresponsive. The requests appear legitimate, making it difficult to filter out malicious traffic.

DNS NXDOMAIN Attack

In this type of DNS Flood attack the attacker sends a high volume of requests for non-existent or invalid domains, resulting in DNS recursion and NXDOMAIN (nonexistent domain) responses. The server must work hard to try and resolve these spurious requests, thereby consuming valuable resources instead of processing legitimate requests. When a DNS server is under NXDOMAIN attack, the cache of the DNS server will be flooded

with NXDOMAIN results, forcing the server to resolve legitimate requests repeatedly instead of fetching the answer from its cache.

Phantom Domain Attack

This attack involves the attacker setting up one or more phantom domains that do not respond to DNS queries and sending requests to the victim's DNS server to resolve the phantom domains. The victim's DNS server gets overwhelmed when it tries to resolve the phantom domains through non-responsive servers. This causes the recursive server to spend valuable resources waiting for responses that will never come.

Pseudo Random Subdomain (PRSD) Attack

Also known as water torture attacks, this attack is similar to the DNS NXDOMAIN attack. The attacker sends a massive number of requests for non-existent subdomains of a valid and existing domain through different recursive resolvers. This causes the authoritative server to consume resources trying to resolve these non-existent subdomains, eventually leading to a denial of service.

In each case, the attacker's objective is to disrupt the DNS service and make the websites and online services that rely on it inaccessible. These attacks exploit different aspects of the DNS protocol, making them challenging to defend against and highlighting the importance of implementing robust DNS security measures.

DNS amplification attacks are discussed in the Attack Protocols section (page 16). This section analyzes DNS Flood attacks or L7 DNS query flood attacks that aim to overwhelm a DNS server with a high volume of illegitimate requests.

By determining the proportion of DNS Flood attack events or vectors directed specifically at DNS services in relation to the overall event count, we can gauge the progression of DNS Floods over time, irrespective of the total activity or number of customers protected by the Cloud DDoS Protection service.

Throughout 2021 and most of 2022, fewer than nine out of every 1,000 attack vectors was a DNS Flood vector. However, from Q4 of 2022, we noted a marked increase in the proportion of attacks featuring a DNS Flood vector. The ratio experienced a twofold surge, rising to almost 18 attacks per 1,000 in Q2 2023.

The area chart depicted in Figure 21 traces the development of the count of DNS Flood attack vectors according to each query type. A description of the key DNS record types can be found in Appendix A: Common DNS Record Types. The total number of DNS Floods mitigated each month corroborates the escalating trend discerned in the previous DNS Flood attack ratio. From September 2022 onwards, the monthly number of DNS Floods consistently surpassed the figures recorded in the preceding months.

DNS Floods are application-layer assaults with the objective of compromising the server's capability to manage valid DNS requests. The pace of these requests determines the total effect on the server. The blue trajectory in Figure 22's chart illustrates the highest DNS query rate detected each quarter, denoted in queries per second (QPS). Aside from a notable DNS Flood attack in Q1 2021, which peaked at 1.59 million QPS, the DNS Floods since Q4 2022 were

Figure 20: DNS Flood attack vector ratio evolution over time

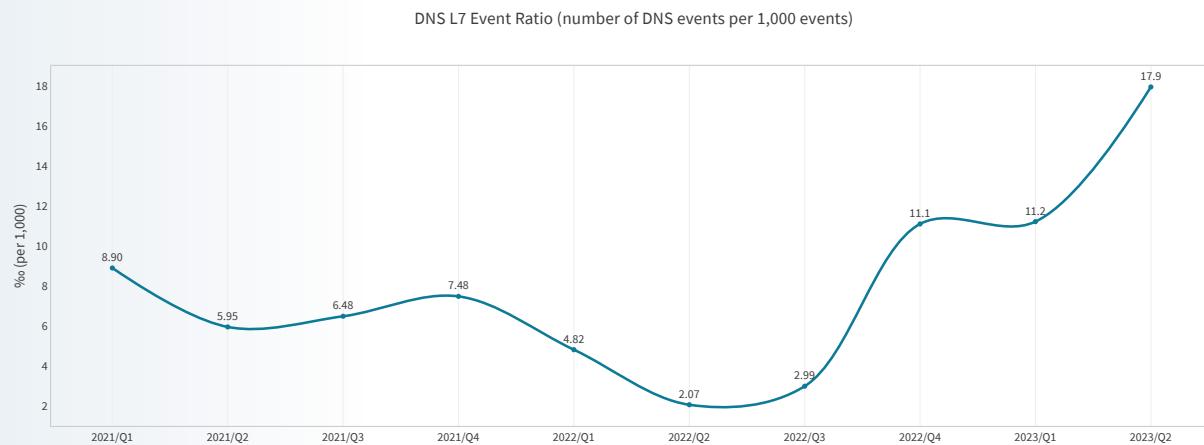
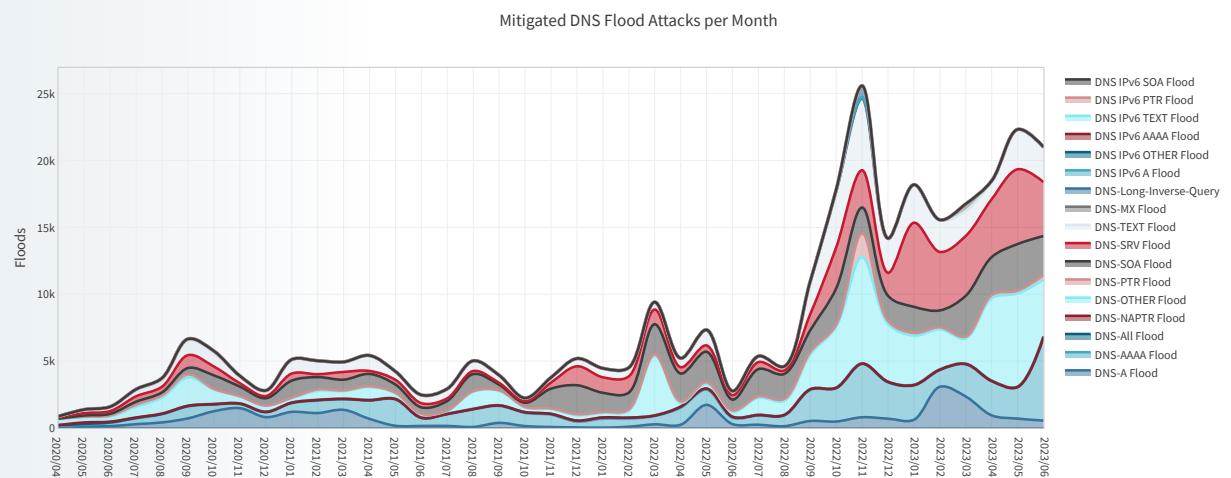


Figure 21: Number of DNS Floods per month



significantly larger in scale compared to previous quarters. The largest DNS Flood in the past two years was observed in Q2 2023, registering an attack rate of 1.29 million DNS queries per second.

The red trajectory in Figure 22's chart demonstrates the peak traffic of the most significant DNS Flood each quarter. The traffic rate shows a consistent pattern aligning with the maximum query rate. It is important to understand that application-level attacks focus on overloading the server, which does not necessarily equate to a traffic volume high enough to saturate the server's internet connection. The red line emphasizes this point; considering that the most substantial DNS Flood recorded a traffic volume of less than 1.3Gbps, all the DNS Floods monitored over the past two years remained under the 1Gbps threshold.

The most prevalent DNS query leveraged in DNS Floods in H1 2023 was the regular hostname to IPv4 query, accounting for 76.5% of all DNS Floods. The second most used was the MX query with 6.14%, followed by the TEXT (5.56%) and OTHER (4.89%) queries. The hostname to IPv6 address resolution query, AAAA, was the fifth most leveraged query type and represented 3.79% of all DNS query floods.

Figure 22: Queries per second and bandwidth consumption by DNS Floods

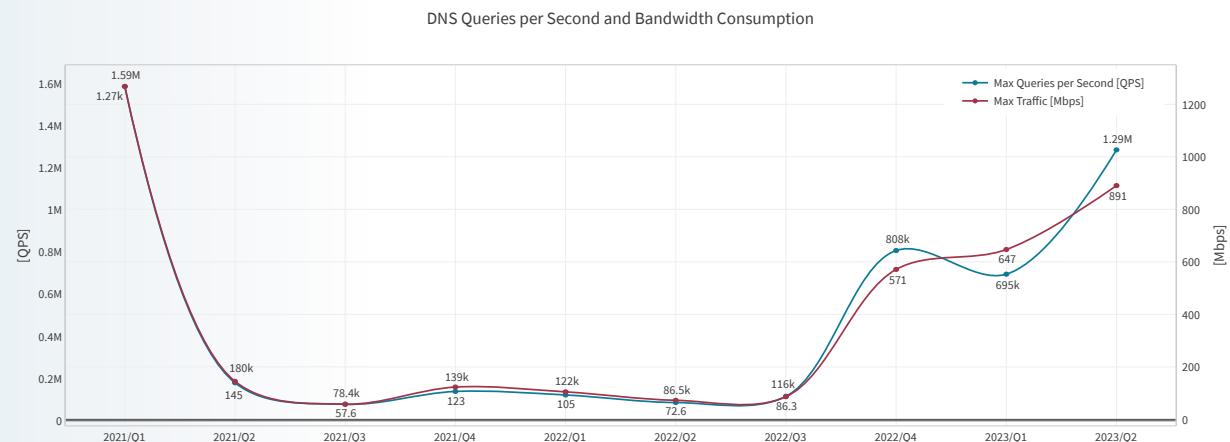
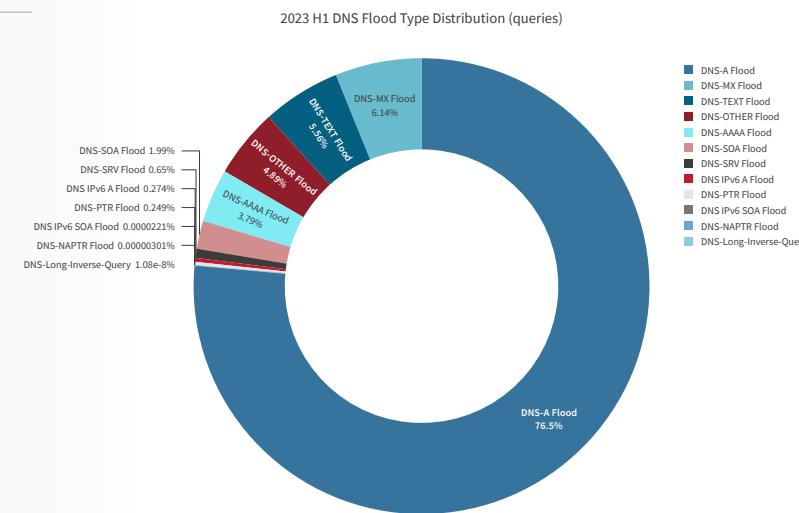


Figure 23
DNS Flood type distribution in H1 2023



Web DDoS

Network-layer attacks are better understood and arguably easier to detect and mitigate compared to the new generation of HTTPS Floods organizations are facing in 2023. Since HTTPS Floods have been around for a few years, they are sometimes considered old news. However, the volume and intensity of the new generation of HTTPS Floods has increased dramatically, and the sophistication introduced by attackers is growing quickly and viciously. That is why we like to refer to these new-generation HTTPS Floods as Web DDoS attacks.

A 2.8 million RPS Web DDoS Attack

As an example, one of our customers became the target of a Web DDoS attack consisting of multiple attack waves and alternating attack vectors. One of the most threatening attack vectors was a Web DDoS attack vector that performed 2.8 million seemingly legitimate encrypted web application requests per second. Radware's new Web DDoS Protection service was able to eliminate the threat and handle the attacks, ensuring the customer's online applications remained available and uninterrupted.

The campaign, which lasted a total of four days, targeted multiple customer applications and consisted of three significant attack waves. The waves lasted for 2.5, 1.5 and 0.5 hours, respectively. The cumulative attack duration across all applications amounted to 20 hours.

Figure 24: Three Web DDoS attack waves spread over four days

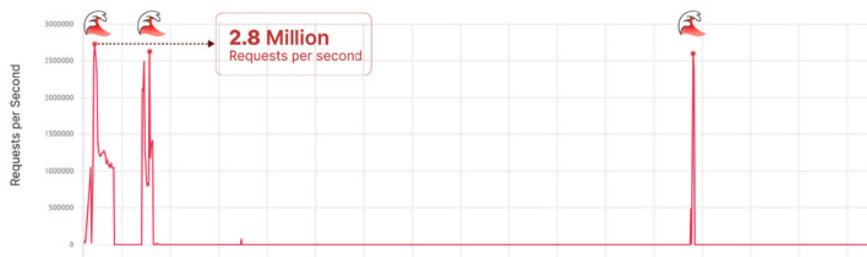


Figure 25: DDoS attack wave detail per single targeted application



The attack originated from a large-scale anonymizing proxy network spanning multiple countries, including, among others, Sweden, the United States, Denmark, Morocco, Poland and Italy. Approximately 30,000 unique source IPs participated in the attack. Before being proxied through the anonymizing proxies, the attack traffic was generated from an attack infrastructure consisting of several public cloud-hosted servers.

The attackers employed various methods to increase the impact of their attacks and evade regular security measures, including:

- ↗ Encrypted requests (HTTPS)
- ↗ HTTP GET requests designed to appear legitimate
- ↗ Techniques that included HTTP/2 multiplexing for improved effectiveness
- ↗ Alteration of request patterns at different stages of the attack

It's important to note that, despite these changing tactics, Radware's algorithm swiftly detected and updated security measures in real time.

Figure 26: Samples of crafted HTTP GET requests disguised as legitimate web requests

```
GET /en/ HTTP/2.0
host: [REDACTED]
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate, br
upgrade-insecure-requests: 1
sec-fetch-mode: document
sec-fetch-site: none
sec-fetch-user: ?1
te: trailer

GET /?u=fhsdfsf HTTP/2.0
host: [REDACTED]
user-agent: like
origin: https://[REDACTED]/?u=fhsdfsf
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
upgrade-insecure-requests: 1
sec-fetch-mode: navigate
sec-fetch-site: none
sec-fetch-user: ?1
cache-control: only-if-cached

GET /?u=qwefsd HTTP/2.0
host: [REDACTED]
user-agent: [REDACTED]
origin: https://[REDACTED]/?u=qwefsd
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
upgrade-insecure-requests: 1
sec-fetch-mode: navigate
sec-fetch-site: none
sec-fetch-user: ?1
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.5
cache-control: max-age=0
```

Network Scanning and Exploit Activity

Not all malicious events that target internet-exposed assets are DoS attacks. Network intrusion attacks consist of easy-to-execute exploits based on known vulnerabilities. These range from scanning using open source or commercial tools, information disclosure attempts for reconnaissance, and path traversal and buffer overflow exploitation attempts designed to render a system inoperable or provide access to sensitive information.

In H1 2023, half of the attack events were DoS attacks and 22% were network intrusion attacks. 27.4% of the blocked attacks were identified as known culprits in the Radware active attackers threat intelligence feed. The ERT Active Attackers Feed (EAAF) is a feed comprising devices found to be actively scanning or randomly exploiting the internet which were caught in the Radware Global Deception Network or GDN. See Unsolicited Network Activity section (page 43) for more information on the GDN and the type of activity caught in our honeypots.

The information disclosure exploit (DNS-named-version-attempt) is used by malicious actors to identify the version of the Bind-named¹ DNS service. This is the first period in which this DNS server information disclosure exploit has led the charts and it does so with three times as many attempts as the runner up.

Half of the top ten network intrusions were related to known log4j exploits. The December 2021 publicly disclosed log4j vulnerability, dubbed Log4Shell, attracted huge attention across the security community. This vulnerability in a commonly used Java logging library allowed an unauthenticated attacker to leverage publicly available exploit tools for remote command execution (RCE). Log4shell was the most critical vulnerability of 2021, and some even argued it was the worst vulnerability of the decade.

1. BIND is a suite of software for interacting with the Domain Name System. Its most prominent component, named, performs both of the main DNS server roles, acting as an authoritative name server for DNS zones and as a recursive resolver in the network (source: Wikipedia).

Figure 27

Attack categories by event count

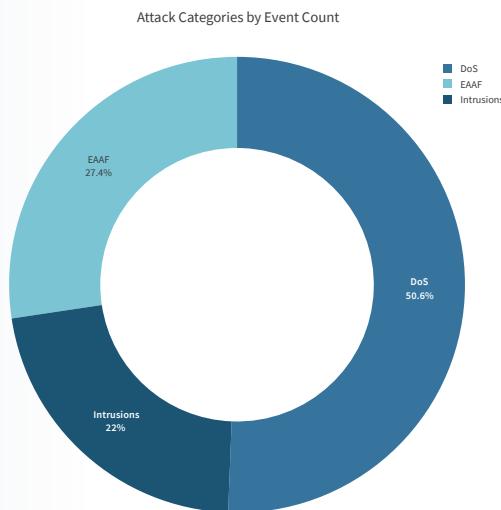
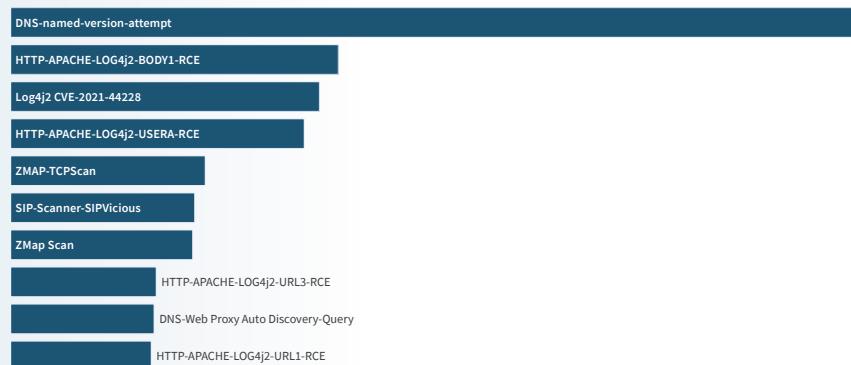


Figure 28: H1 2023 top network intrusions (see Appendix B: Radware Network Intrusion Signatures)

2023 Top Network Intrusions



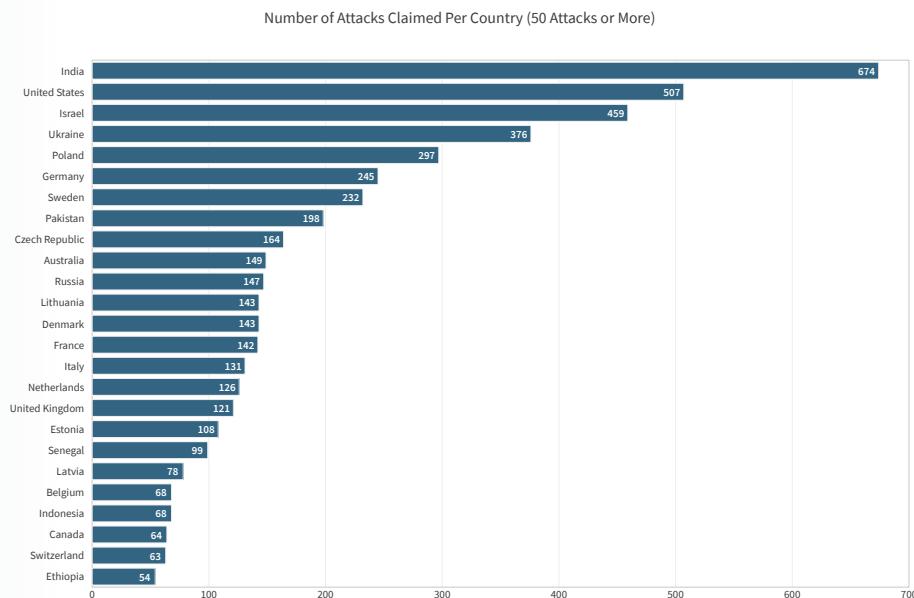
Most Targeted Countries

Most of the claimed DDoS attacks in H1 2023 targeted India, United States, Israel, Ukraine and Poland, in that order. India was a constant target for the same pro-Islamic actors that moved focus to Israel and Australia for #OpIsrael and #OpAustralia. Poland was the fifth most targeted country because of its ongoing support for Ukraine which displeases pro-Russian hacktivists.

Figure 32 demonstrates that the activity by hacktivists is a global threat. Organizations across the globe, willing or not, are now in the crosshairs of hacktivists. There are exceptions such as Alaska, the North and South Poles and parts of Africa, Latin America and Asia.

Figure 31

Number of DDoS attacks claimed per country

**Figure 32**

World heatmap of claimed DDoS attacks



Most Targeted Website Categories

Government, business/economy and travel websites were the most targeted categories, followed by those involved in financial services, health/medicine, society, news/media, education and the military.

Business/economy, government, travel and finance websites were the primary targets for NoName057(16). Government was also the most attacked category for Team Insane PK and Mysterious Team. Anonymous Sudan has an outspoken preference for health/medicine and travel websites.

Note that travel includes websites for airports and seaports, two categories that were often targeted by hacktivists.

Figure 34: Top website categories targeted globally

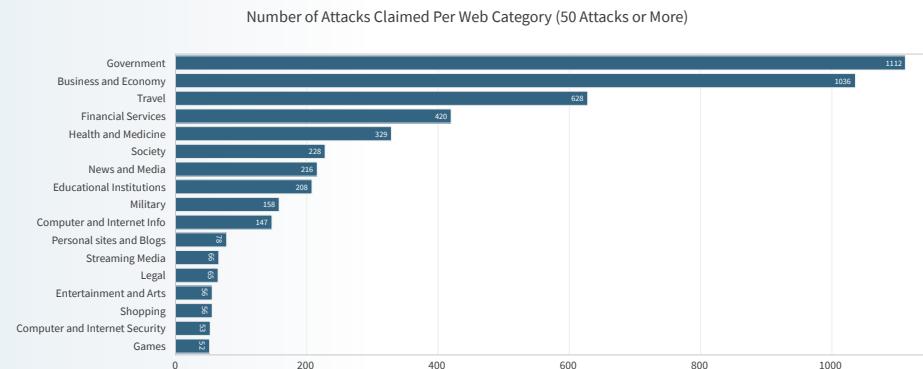
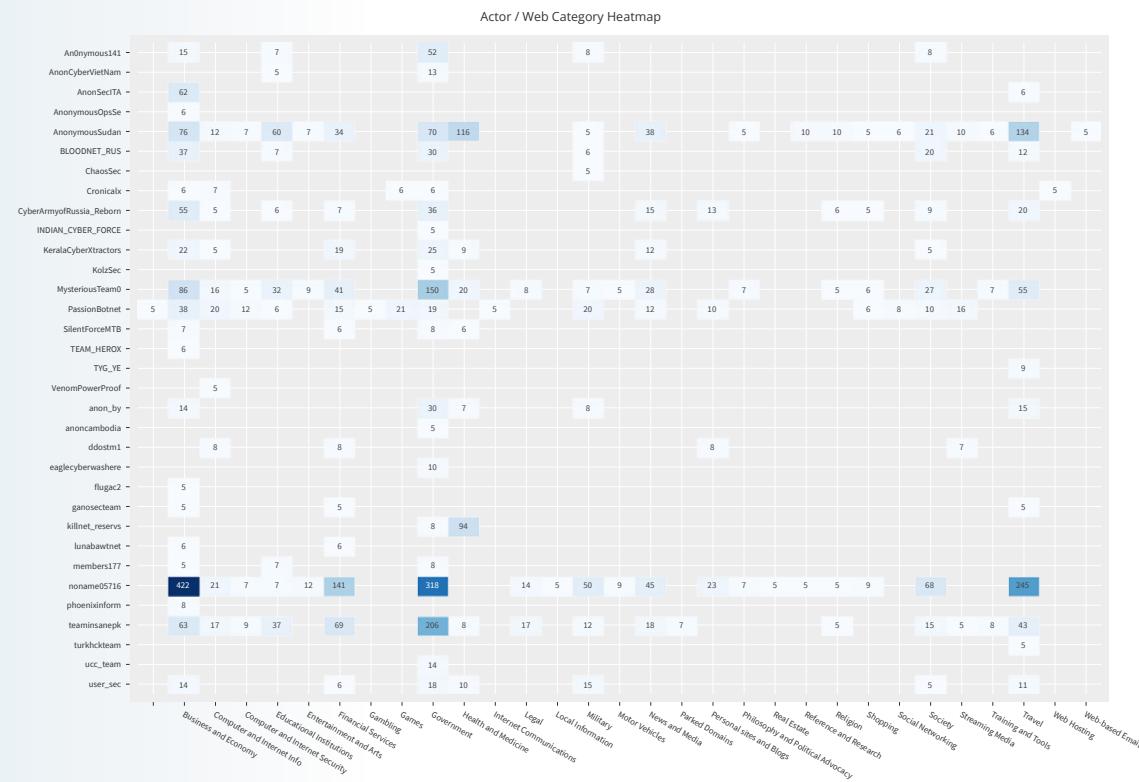


Figure 35: Number of DDoS attacks claimed by website category (> 5 attacks claimed)



Web Application Attack Activity

In H1 2023, the number of blocked malicious web application transactions grew by a staggering 500% compared to the first half of 2022. The high number of malicious web transactions underscores the earlier statement that DDoS attacks are moving to the application layer.

Compared to last year, malicious web transactions grew 366% in Q1 2023 and even faster in Q2 at 605%.

While in 2022 we observed a near linear growth in the number of malicious web transactions per quarter, in H1 2023 this accelerated to an exponential growth.

Targeted malicious web application attacks can be blocked by application-specific and custom rules, learned by inspecting the application and tuned by the Security Operations Center (SOC). The chart in Figure 45 shows that the share of targeted malicious transactions blocked by signature and behavioral detection modules remained mostly unchanged in the last three quarters. However, the bulk of malicious web transactions blocked were unsolicited and random attacks, not specifically targeting the application or a known web application exploit or vulnerability.

The remainder of this section considers attacks detected and blocked based on known malicious behavior, vulnerabilities, and exploits.

While in 2022 we observed a near linear growth in the number of malicious web transactions per quarter, **in H1 2023 this accelerated to an exponential growth**

Figure 42: Yearly blocked malicious web application transactions

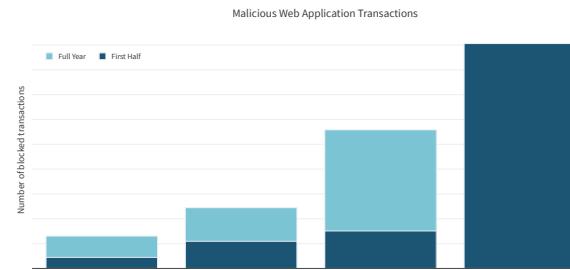


Figure 44: Blocked malicious web application transactions growth evolution

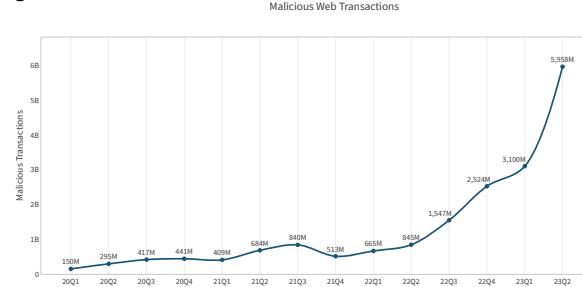


Figure 43: Quarterly blocked malicious web application transactions

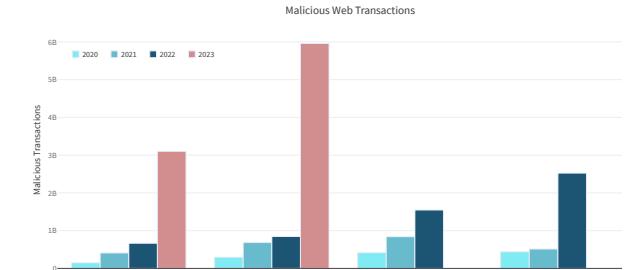
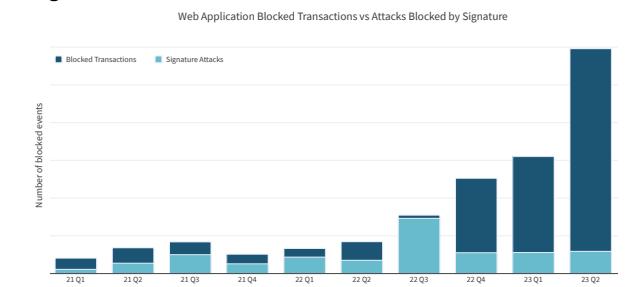


Figure 45: Web application transactions vs attacks blocked by signature



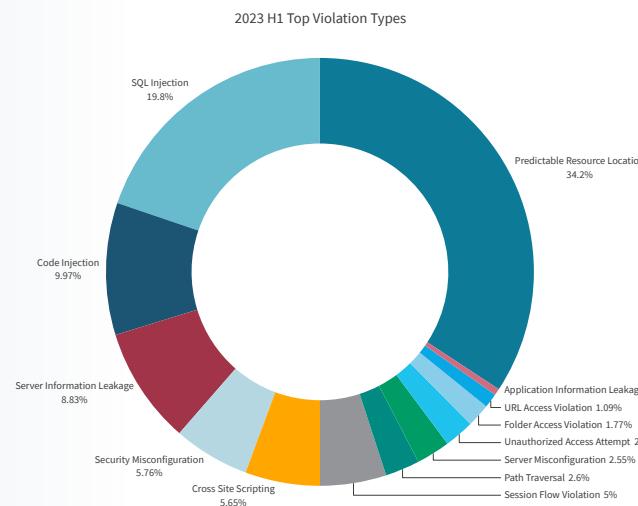
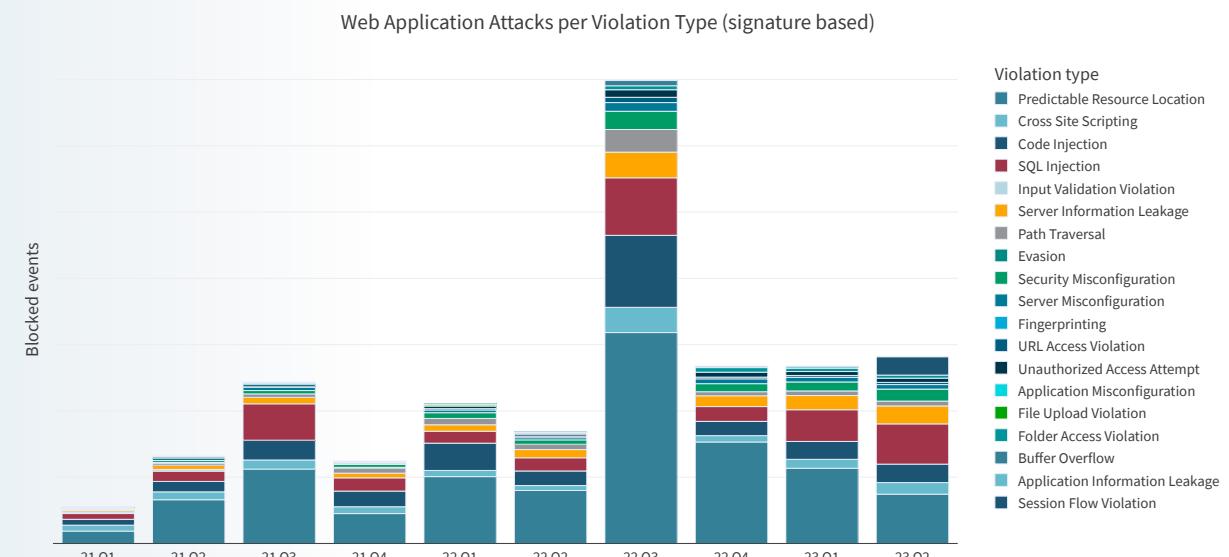
Security Violations

The most important security violation for H1 2023 (Figure 46), predictable resource location attacks, has always accounted for a significant part of the total attack count. Predictable resource location attacks target hidden content and functionality of web applications. By guessing common names for directories of files, an attack may be able to access resources that were not intended to be exposed. Examples of resources that might be uncovered through brute force techniques include old backup and configuration files and yet-to-be-published web application resources. SQL and code injection were, respectively, in second and third position. Combined with predictable resource location attacks, these three web application attacks were responsible for 64% of the total attack activity on web applications and APIs.

In Q2 2023 (Figure 47), SQL injections became more prominent and for the first time were leveraged for attacks almost as often as predictable resource location.

Figure 46

Top security violation types for H1 2023

**Figure 47:** Evolution of violation types over time

Attacking Countries

Most blocked web security events in H1 2023 originated from the United States with Germany, Russia, United Kingdom and Italy completing the top five. The United States has dominated the attack scene and has consistently taken the number one spot in most quarters (Figure 49). It is important, however, to note that the country where an attack originates from does not have to correspond to the nationality of the threat actor or group. Arguably, the country where the attack originates will most often not be the home country of the threat actor. Threat actors leverage public cloud-hosted servers, anonymizing VPNs and proxies, the Tor network, and compromised servers as jump hosts to conceal the real origin of their attacks. The originating country of an attack is typically chosen based on the location of the victim to circumvent potential geo-based blocking. It can also be based on the country the threat actor wants to see attributed during false flag operations.

Figure 48
H1 2023 top attacking countries

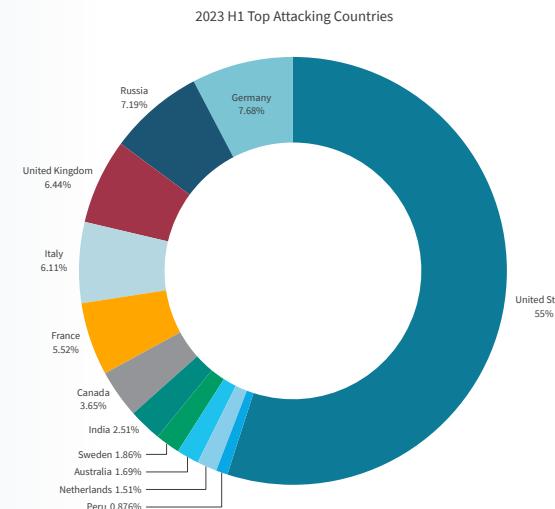
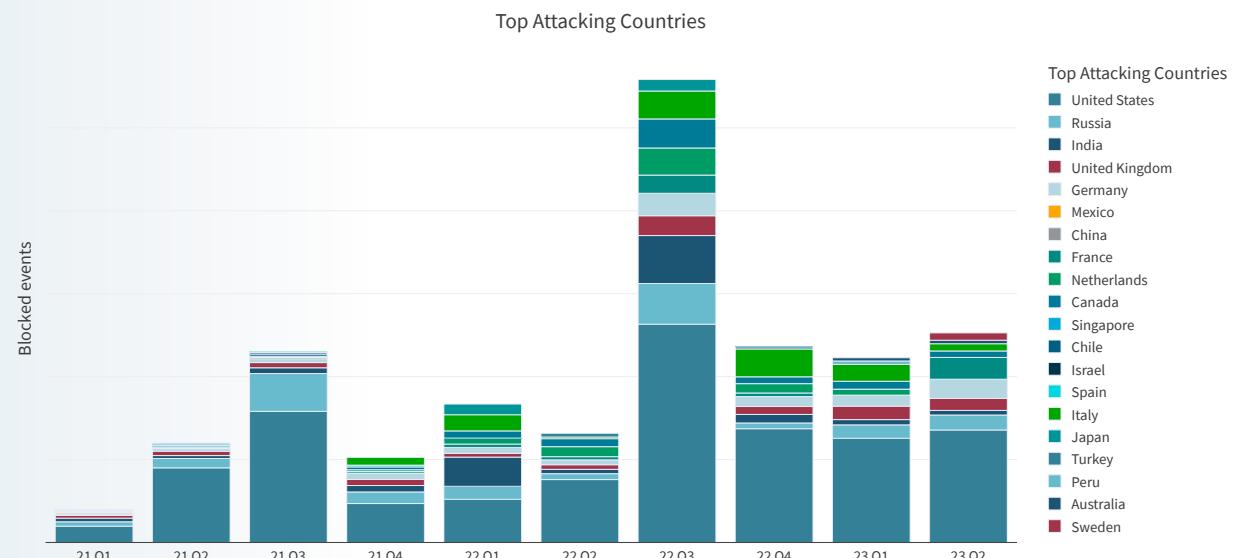


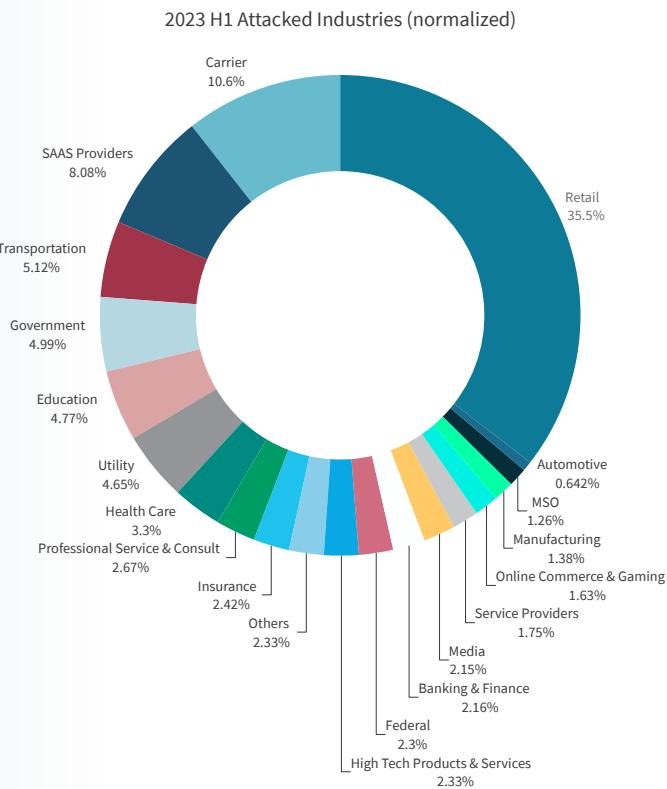
Figure 49: Top attacking countries over time



Attacked Industries

The most attacked industry in H1 2023 was retail, accounting for 35.5% of web application attacks. Carriers and SAAS providers were in second and third place, respectively representing 10.6% and 8.08% of web application attacks. Transportation was fourth (5.12%), followed by government (5%), education (4.77%), utility (4.65%) and health care (3.3%).

Figure 50
Web application attacks
by industry



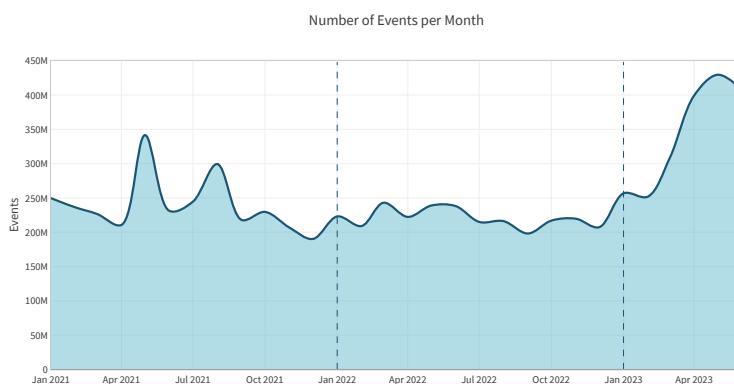
Unsolicited Network Activity

The Radware Global Deception Network (GDN) consists of a network of globally distributed sensors that collect data on unsolicited traffic and attack attempts. Unsolicited events include DDoS backscatter and spoofed² and non-spoofed scans and exploits.

The major difference between the GDN events discussed in this section and the web application and DDoS attack events in previous sections, is the unsolicited nature of the events. Web application and DDoS attack events were collected from real-world services accessible via the internet. In the latter case, attackers were targeting a particular organization or a specific application or service. By contrast, the unsolicited events recorded by the GDN are random acts. The scans or attacks were not targeting known services or a particular organization. The IP addresses of the sensors in the GDN are not published in DNS and do not provide accessible applications or services. No client, agent or device has a legitimate reason to reach a Radware GDN sensor.

2. IP address spoofing is the crafting of Internet Protocol (IP) packets with false source IP addresses for the purpose of impersonating another originating computing system and geolocation.

Figure 51: Number of events per month recorded by Radware's GDN

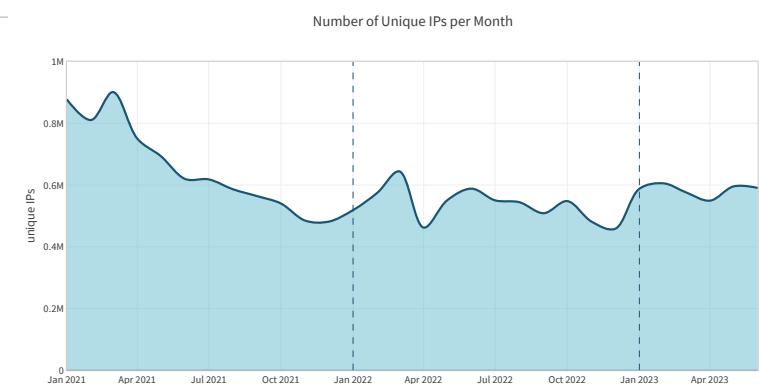


In H1 2023, the GDN collected a total of 2.05 billion unsolicited events. This represents a significant increase compared to the total 2.65 billion unsolicited events collected in the full year 2022. The network collected an average of 11.3 million events per day. Compared to 2022, the average events per day increased by 55%.

The number of unique IP addresses provides a measure for the evolution of the number of malicious hosts and devices randomly scanning the internet and exploiting known vulnerabilities. In H1 2023, the deception network registered an average of 60,775 unique IPs per day. This was an increase of 15% compared to 2022, which had an average of 52,860 unique IPs per day.

While the total number of events per day grew significantly (55%) in H1 2023, the number of unique IPs per day increased only slightly (15%). In conclusion, the number of malicious devices on the internet increased slightly, but their actions became much more aggressive compared to earlier years.

Figure 52: Number of unique IP addresses per month recorded by Radware's GDN



Most Scanned and Attacked TCP Ports

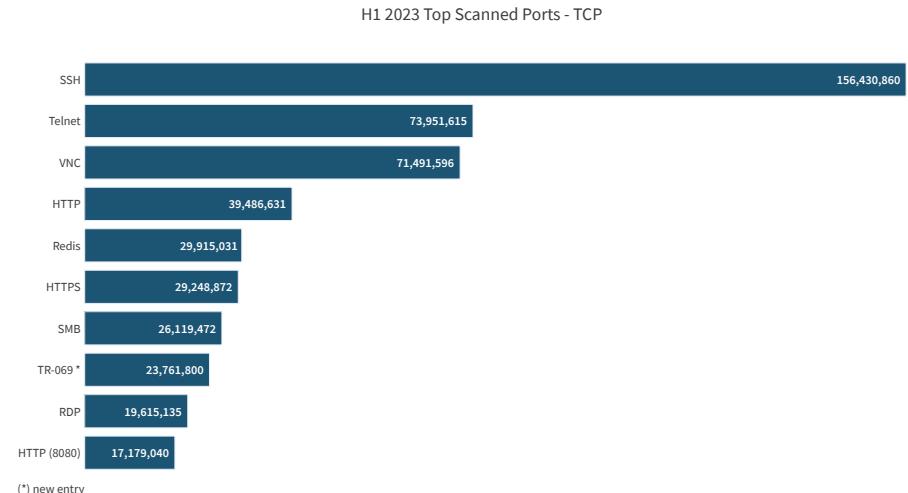
For TCP services, the most attacked service was SSH on port 22, followed by Telnet and VNC. The top 10 was completed by HTTP, Redis, HTTPS, SMB, TR-069 and RDP, followed by the popular IP camera web UI port 8080. TR-069 was a new entry in the top ten for H1 2023 compared to 2022. Leaving the top ten in H1 2023 was HTTP port 8088, another popular IP camera web UI port.

While Telnet was a favorite of the Mirai botnet for a long time, the number of access attempts on SSH surpassed Telnet by a good margin. SSH attacks are leveraged in account takeover and brute force attempts. Leveraging default or leaked credentials, attackers try to gain unauthorized access to devices and systems to move laterally across organizations' networks. This is used for abuse of cloud instances for cryptomining, as a jump host to anonymize targeted attacks, to plant cryptolocking malware during ransomware campaigns, and to hijack device connectivity to perform DDoS attacks.

Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the Remote Frame Buffer (RFB) protocol to remotely control another computer. It transmits the keyboard and mouse input from one computer to another, relaying the graphical screen updates over a network. In 2022, VNC took the eighth spot on the top ten most scanned ports. This year VNC scans were even more prominent, moving VNC up to the third most scanned TCP port in H1 2023.

Redis (TCP port 6379) is an open source (BSD licensed) in-memory data structure store used as a database, cache and message broker. In March 2022, the Muhstik malware gang started actively targeting and exploiting a Lua sandbox escape vulnerability in Redis (CVE-2022-0543) after the release of a proof-of-concept exploit. In December 2022, a previously undocumented Golang-based malware, dubbed Redigo, targeted Redis servers to take control of systems with this vulnerability, most likely to build a botnet. The malware mimicked the Redis protocol to communicate with its command & control (C2) infrastructure. In 2022, Redis took fourth place, just behind HTTP. In H1 2023,

Figure 53: Top scanned and exploited TCP ports



both HTTP and Redis were surpassed by VNC, with each dropping down one place.

Server Message Block (SMB) is a popular file and printer sharing protocol leveraged by Microsoft in Windows and many Linux implementations through Samba or the more recent ksmbd kernel service. In December 2022, a critical vulnerability with a CVSS score of 10 was disclosed that could enable remote attackers to execute arbitrary code on Linux servers exposing the SMB protocol on Linux servers with ksmbd enabled. SMB remained in seventh place in the top ten for H1 2023, unchanged from 2022.

Technical Report 069 (TR-069) is a technical specification of the Broadband Forum that defines an application-layer protocol for the remote management and provisioning of customer premises equipment (CPE) connected to an IP network. TR-069 uses the CPE WAN Management Protocol (CWMP) which provides support functions for auto-configuration, software or firmware

Most Scanned and Attacked UDP Ports

Most of the scanned and exploited UDP ports during H1 2023 were the same as the top scanned UDP ports in 2022. The exception was LDAP which left the top 10 in favor of HTTP, and CoAP, which took tenth place in 2022, replaced during H1 2023 by OpenVPN in the same spot.

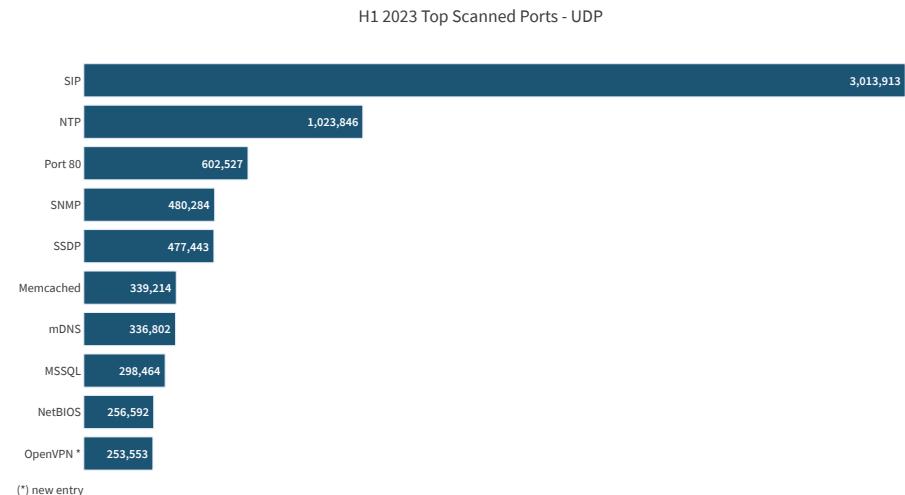
SIP (UDP port 5060) was again the most targeted UDP-based service in H1 2023. Port 5060 is used by many SIP-based VoIP phones and providers. VoIP remains critical to organizations and for this reason it also made the charts as one of the most targeted services for DDoS attacks in 2021. Vulnerabilities and weak or default passwords in VoIP services allow attackers to abuse them for initial access, spying, and moving laterally inside organizations' networks.

NTP (UDP port 123), SNMP (UDP port 161), SSDP/UPnP (UDP port 1900), Memcached (UDP port 11211) and mDNS (UDP port 5353), are among the most abused protocols for DDoS amplification attacks. Many black and white hat actors are continuously scanning and cataloging the internet's addressable range to abuse for DDoS attacks (black hat) or assess the risk in the DDoS threat landscape (white hat).

MSSQL (UDP port 1434) is used by the Microsoft SQL Server database management system monitor. It is abused through remote code execution vulnerabilities and is known for the W32.Spybot.Worm that spread through MSSQL Server 2000 and MSDE 2000 from the early 2000s onwards. It remained a very solicited port in 2021, 2022 and also H1 2023.

NetBIOS (UDP port 137) defines a software interface and a naming convention. NetBIOS includes a name service, often called WINS on Microsoft Windows operating systems. The NetBIOS name service is needed only within local networks and for systems prior to Microsoft Windows 2000 which require name resolution through WINS. Otherwise, internet name resolution is done via DNS. Openly accessible NetBIOS name services can be abused for DDoS reflection attacks against third parties. Furthermore, they allow

Figure 54: Top scanned and exploited UDP ports



potential attackers to gather information on the server or network for the preparation of further attacks.

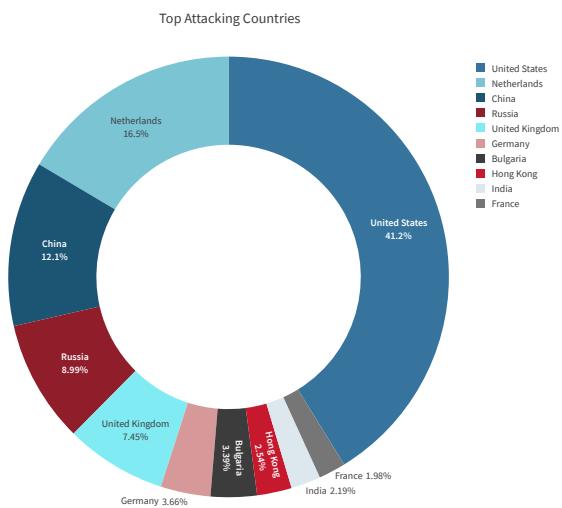
OpenVPN (UDP port 1194) is a virtual private network (VPN) system that implements techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations providing remote access for clients. It makes extensive use of the OpenSSL encryption library as well as the TLS protocol and contains many security and control features. It uses a custom security protocol that utilizes SSL/TLS for key exchange and is capable of traversing network address translators (NATs) and firewalls. OpenVPN has been ported and embedded in many router firmware platforms including DD-WRT which has an OpenVPN server function.

Attacking Countries

The United States was the country from which the most unsolicited network activity originated during H1 2023. The United States was also the number one in 2022 with 42.5% of all activity and remained so with 41.2% of all activity in H1 2023. The Netherlands moved from fourth spot in 2022 to second place in H1 2023 with 16.5%. China remained in the third spot in H1 2023 while Russia moved from second in 2022 to fourth position in H1 2023. The United Kingdom remained unchanged in fifth place. That said, as discussed earlier, the origin of an attack often does not align with the home country of the attacker and can be spoofed to impersonate a different country.

The real origin of an attack often does not align with the home country of the attacker and can be spoofed to impersonate a different country

Figure 55: Top attacking countries

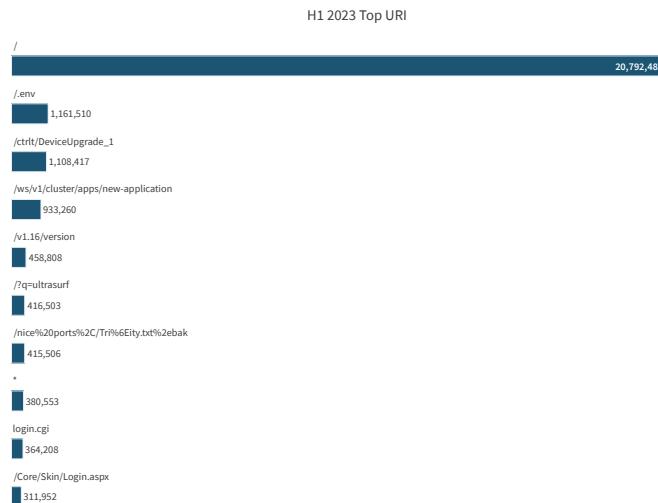


Web Service Exploits

The top attacked HTTP Uniform Resource Identifiers (URI) were led by “/”, the universal URI for testing the presence of a web service and collecting information from header fields in server responses. There is a significant difference in the top targeted URIs for unsolicited events compared to the top targets in web application attacks where services are supporting real applications. This section covers unsolicited events, meaning there is no real application or service running on the targeted server and the IP address of the targeted server is not published in DNS or referred by any services on the Internet. The top URIs should be interpreted as the top services and applications that are targeted by actors that are randomly scanning and exploiting the internet. Typically, a URI will conform with a known and disclosed vulnerability.

Figure 56

Top scanned URIs



Most important and known vulnerabilities based on top scanned URIs are listed in the following table:

[/.env](#)

A predictable resource location access exploit attempting to find configuration information of the service in the hidden file “.env”. Moved from a fourth spot in 2022 to second place in H1 2023.

[/ctrlt/DeviceUpgrade_1](#)

Huawei HG532 routers Remote Code Execution vulnerability, CVE-2017-17215. Moved from tenth place in 2022 to third place in H1 2023.

[/ws/v1/cluster/app/new-application](#)

A known vulnerability used to exploit Hadoop YARN services and schedule arbitrary workloads on Hadoop clusters. An exploit abused by many cryptojacking campaigns that try to illegitimately leverage the cloud instances of enterprises and research institutions. This was the second most exploited URI in 2022 but moved down to third place in H1 2023.

[/v1.16/version](#)

Used by threat actors to identify the available Docker API version by invoking a command for an old version. Used by cryptocurrency miners for abusing containers through the Docker API. This was in seventh place in 2022 but moved to fifth place in H1 2023.

[/q=ultrasurf](#)

UltraSurf is a freeware internet censorship circumvention product created by UltraReach internet Corporation. The software bypasses internet censorship and firewalls using an HTTP proxy server, employing encryption to ensure privacy. The software works by creating an encrypted HTTP tunnel between the user's computer and a central pool of proxy servers, enabling users to bypass firewalls and censorship. UltraReach hosts all of its own servers. The software makes use of sophisticated proprietary anti-blocking technology to overcome filtering and censorship online. The tool was originally designed for internet users in mainland China, where the internet is heavily censored and Internet activities are monitored. With the advent of Ultrasurf and other circumvention tools, these internet users are provided a lifeline to access and share information freely. After nearly two decades of development, the technology has proven extremely resilient and adaptable in the face of increasingly advanced censorship techniques and aggressive blocking. Its success in helping internet users in China to surf the web in freedom has attracted the attention of internet users beyond China's borders. Today, Ultrareach has millions of users from over 180 countries. Radware assumes that “/q=ultrasurf” is leveraged in attempts to identify the locations and addresses of Ultrareach proxies. Ultrasurf is a new entry in the top scanned URI list.

[/nice%20ports%2C/Trinity.txt%2ebak](#)

Request for “/nice ports,/Trinity.txt.bak” is used by Nmap’s service detection routine to test how a server handles escape characters within a URI.

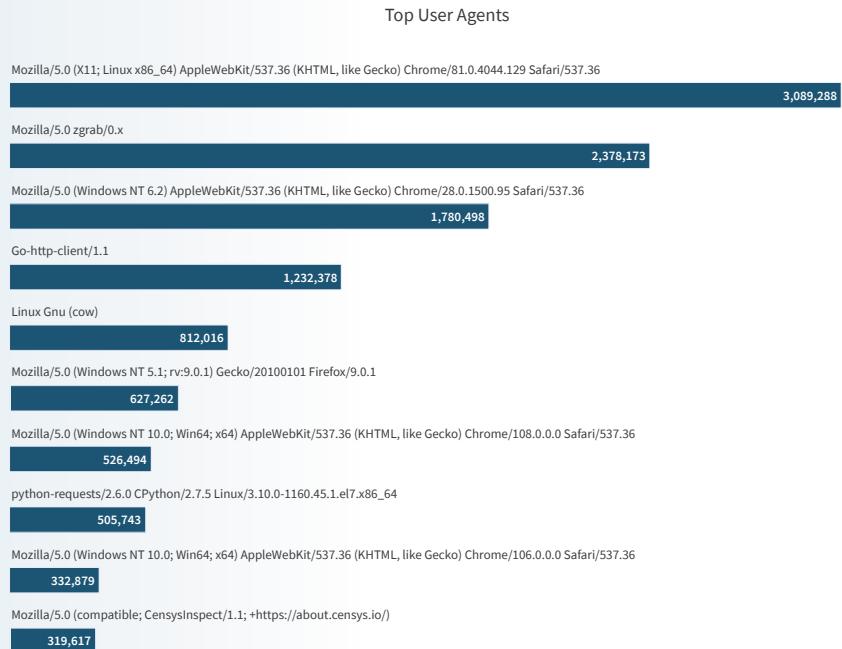
Top User Agents

In HTTP, the user-agent string is often used for content negotiation, where the origin server selects suitable content or operating parameters for the response. For example, the user-agent string might be used by a web server to choose variants based on the known capabilities of a particular version of client software, and to differentiate its interface for smartphones or desktop browsers. The concept of content tailoring is built into the HTTP standard in RFC1945.

As such, the user-agent field in a web request can be used to identify the client agent that makes the request. Some malicious actors are aware of this identifying feature being used to score the legitimacy of a web request by web security modules. This causes them to mask their origins by randomly generating and changing the user-agent to known legitimate values.

Commercial and open source web service vulnerability scanning tools and programming language implementations can be identified through their user agent. For example, zgrab is the application-layer network scanning component of the Zmap open source scanning tool and “Go-http-client” is the default user agent header when using the Golang net/http package.

Figure 57: Top user agents



Top HTTP Credentials

Not all web service vulnerabilities can be exploited without authentication. Some web services embed widely used defaults and some even have hard-coded secrets to protect access from unauthorized users or devices. Typically, weak passwords are combined in credential pairs such as "admin", "password", "1234567890", or no password. These weak password permutations make up nine of the top 10 credentials. These are universally agreed to be the worst credentials and are abused because they provide access to devices that have not had their default credentials changed during installation.

The credential "report:8Jg0SR8K50" is hard coded in digital video recorders (DVRs) from vendor LILIN and was publicly disclosed in March 2020. DVRs are ubiquitous in the IoT landscape, as are the security cameras that feed them.

Top SSH Usernames

The top usernames used during SSH authentication give an indication of the services most vulnerable to brute forcing. Amongst the top 10 are "postgres", "oracle", "ftpuser", "git", "root", "pi" (Raspberry Pi default username) and "ubnt" (Ubuntu default username). The others are the most leveraged usernames by administrators or default accounts, for example, "admin", "user", and "test". Appendix A

Figure 58: Top HTTP credentials

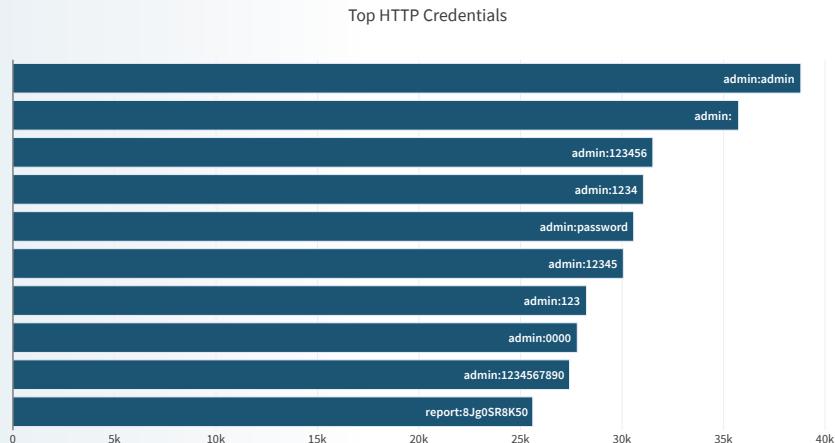
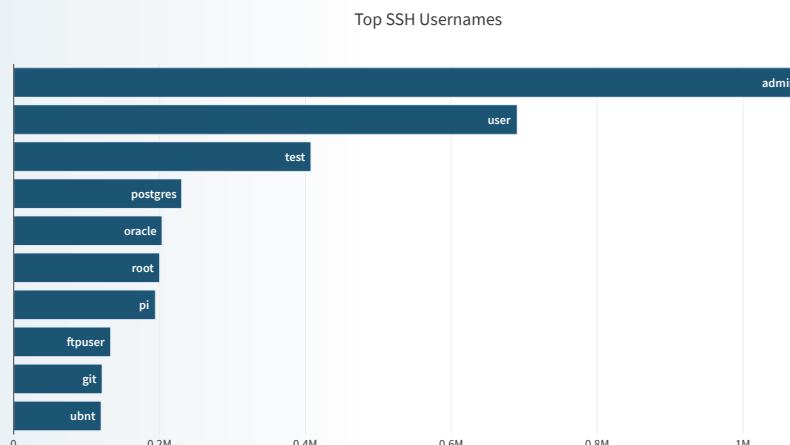


Figure 59: Top SSH usernames



NEXUSGUARD®

Distributed Denial of Service (DDoS) Trend Report 2024

Key Observations for 2023

- In 2023, the total attack count and average attack size decreased by 54.74% and increased 233.33% respectively compared to the figures registered in 2022.
- Compared to 2022, the maximum attack size increased by 93.42%, with the maximum attack size clocking in at 700 Gbps.
- UDP based attacks remained the most predominant type of attack in 2023, decreased by 58.29% YoY. The number of TCP based attacks decreased by 37.20% in the same period a year ago.
- Amplification attacks decreased YoY by 54.94%, while Application attacks decreased by 19.20% YoY.



Key Observations for 2023

Metrics

Total Attacks

vs. 2022

-54.74% ▼

Attack Sizes

Maximum

700.00 Gbps

vs. 2022

93.42% ▲

Average

0.80 Gbps

vs. 2022

233.33% ▲

Top 3 Attack Types

1

NTP Amplification Attack

vs. 2022

-62.58% ▼

2

HTTPS Flood

vs. 2022

-19.67% ▼

3

DNS Amplification Attack

vs. 2022

165.58% ▲

DDoS Attack Category

Volumetric (Amplification)

vs. 2022

-54.94% ▼

Application Attack

vs. 2022

-19.20% ▼

Volumetric (Direct Flood)

vs. 2022

-68.74% ▼

2023 Attack Statistics

Attack Vector Distribution

In 2023, the landscape of DDoS attacks was dominated by a trio of methods: NTP Amplification, HTTPS Flood, and DNS Amplification attacks, each playing a distinct role in shaping the cyber threat environment.

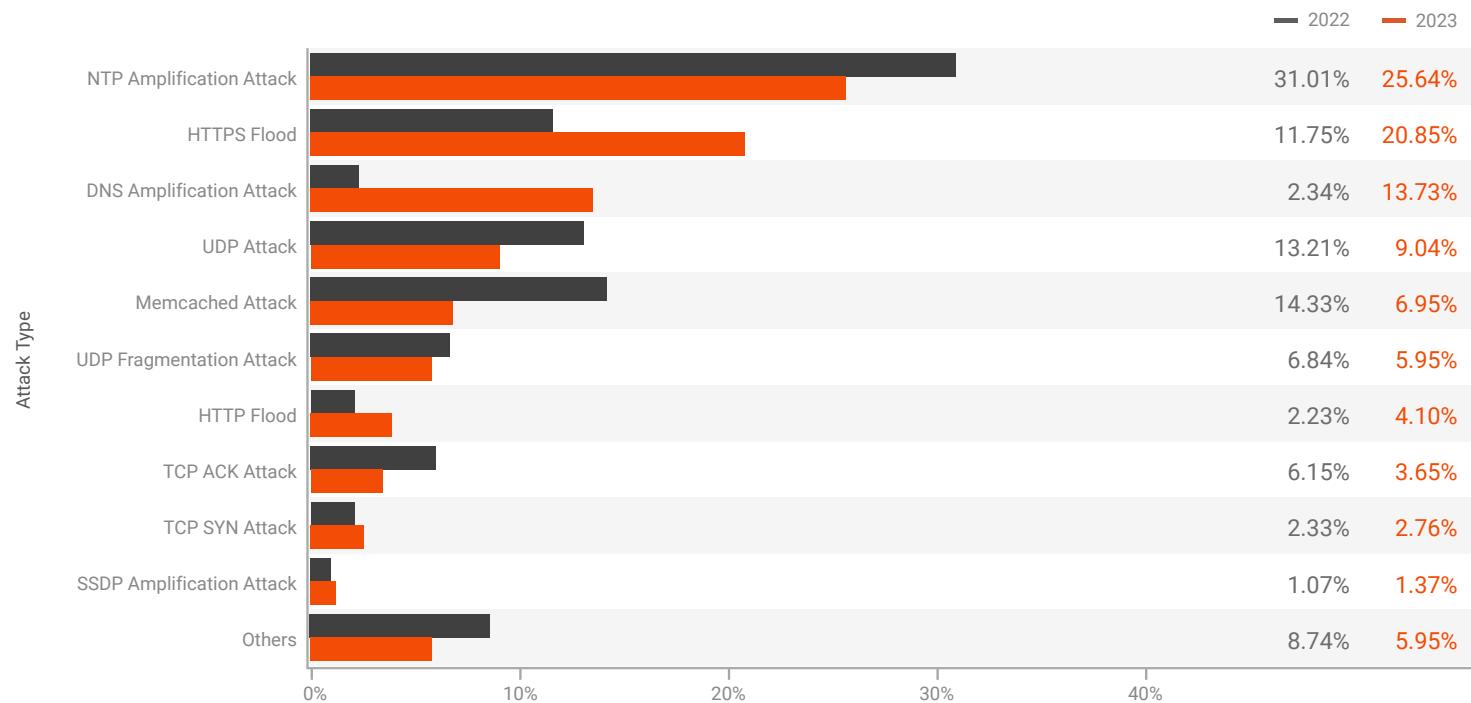


Figure 2 - Distribution of Attack Vector in 2022 and 2023

2023 Attack Statistics

Attacks by Category Distribution

The landscape of DDoS attacks showcased significant trends and real-world incidents, particularly in the categories of Volumetric (Amplification) attacks, Application attacks, and Volumetric (Direct Flood) attacks.

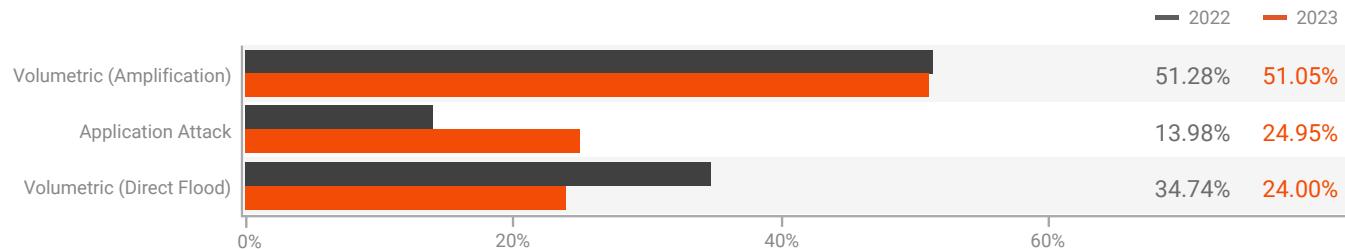


Figure 3 - Distribution of Attacks by Category in 2022 and 2023

Amplification attacks

-0.44%

Application attacks

+78.51%

Direct Flood attacks

-30.93%

2023 Attack Statistics

Attacks by Protocol Distribution

In 2023, the DDoS attack landscape was significantly shaped by UDP and TCP-based attacks, while ICMP attacks were relatively less prominent. UDP-based attacks, known for sending numerous UDP packets to overwhelm targets, were the most dominant, accounting for 66.81% of the total attacks.

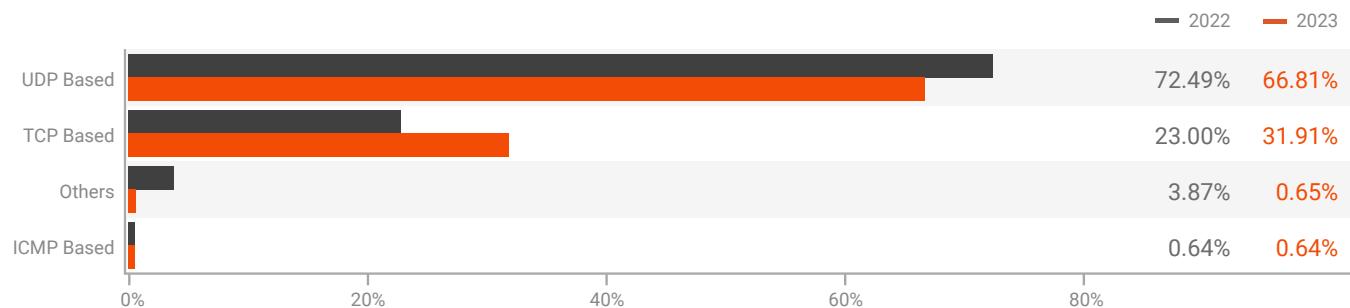


Figure 4 - Distribution of Attacks by Protocols in 2022 and 2023

UDP based attacks

-7.84 %

TCP based attacks

+38.75 %

ICMP based attacks

-0.95 %

2023 Attack Statistics

Quantity of Attack Vectors

The prevalence of single-vector attacks at 92.70% of total DDoS attacks, compared to multi-vector attacks in 2023, suggests a significant trend in the cyber threat landscape. There are several potential reasons for this predominance of single-vector attacks:

Simplicity and Cost-Effectiveness: Single-vector attacks are generally simpler to execute and require fewer resources. The simplicity also means that less technical expertise is required, making these attacks more accessible to a broader range of attackers.

Sufficient Effectiveness: For many targets, a single-vector attack can be sufficiently effective to disrupt operations or services. If the primary goal of the attack is to cause disruption or downtime, even a straightforward attack method like a UDP flood can be effective without the need for more sophisticated multi-vector approaches.

Detection Evasion: While it might seem counterintuitive, single-vector attacks can sometimes be more difficult to detect and mitigate due to their straightforward nature. They can more easily blend in with legitimate traffic, making it harder for defense systems to identify and block the attack without affecting normal operations.

Shift in Attacker Priorities: The prevalence of single-vector attacks could also reflect a shift in attacker priorities or strategies. As cybersecurity defenses evolve, attackers might be adapting their methods, possibly finding that single-vector attacks meet their objectives with lower risk or effort.

Resource Allocation: Conducting multi-vector attacks requires more resources, coordination, and technical know-how. Attackers might reserve such complex attacks for high-value targets or specific campaigns, whereas single-vector attacks are more broadly utilized for a range of targets.

Evolution of Defense Mechanisms: The evolution of defense mechanisms against multi-vector attacks might also be a contributing factor. As multi-vector attacks have historically posed significant threats, organizations might have developed more robust defenses against them, leading attackers to pivot back to single-vector attacks.

It's important to note that while single-vector attacks dominate, the presence of multi-vector attacks, though in the minority, indicates a continued need for comprehensive and adaptive defense strategies. Multi-vector attacks, due to their complexity, can be particularly challenging to defend against and may be employed in more targeted and sophisticated cyber campaigns.

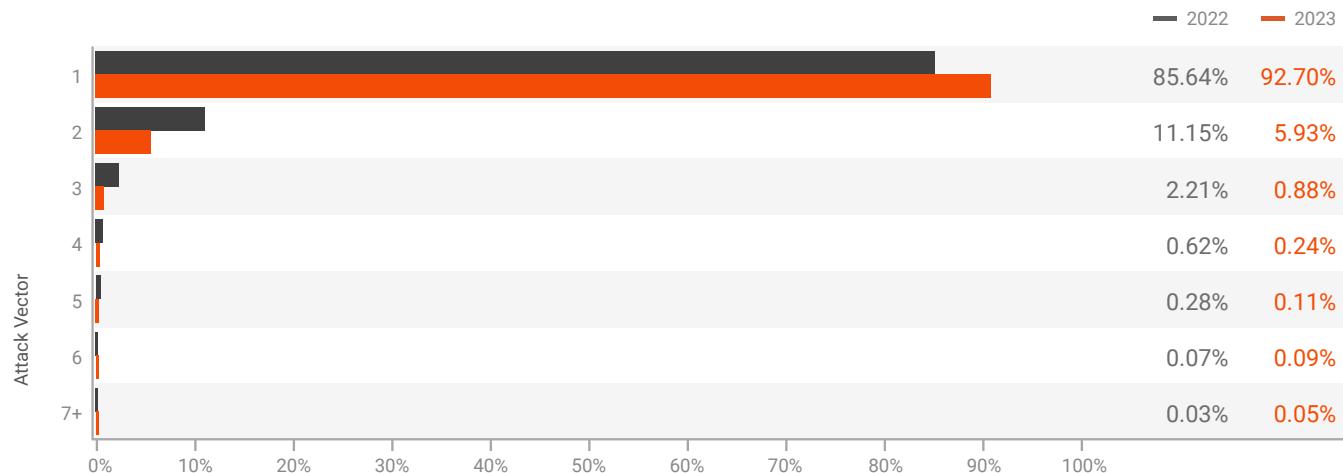


Figure 5 - Distribution of DDoS Attack Vectors in 2022 and 2023

Single-vector attacks
93%

Multi-vector attacks
7%

2023 Attack Statistics

Multi-Vector Attack Combinations

The data in this section illustrates the distribution of common multi-vector DDoS attack combinations. Multi-vector DDoS attacks leverage multiple attack vectors simultaneously, making them more complex and harder to defend against compared to single-vector attacks.

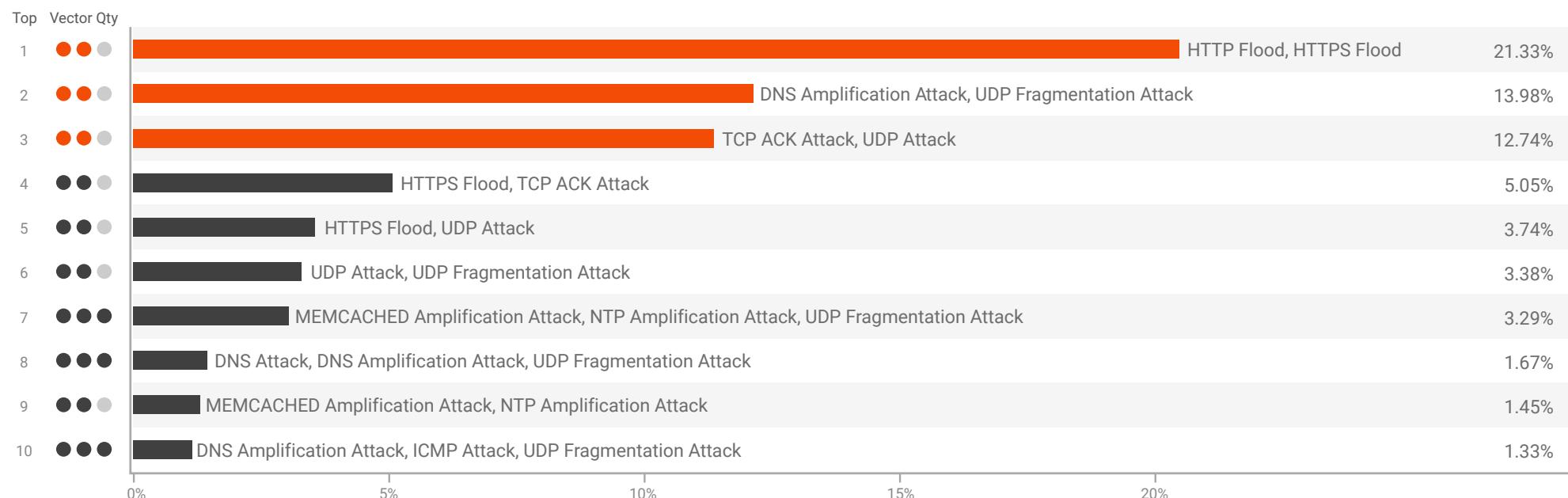


Figure 6 - Top 10 multi-vector combinations in 2023

2023 Attack Statistics

Attack Duration Distribution

In a comprehensive analysis of Distributed Denial of Service (DDoS) attack durations for the years 2022 and 2023, notable trends emerge that reflect the evolving cybersecurity landscape. DDoS attacks, designed to overwhelm websites and online services, rendering them inaccessible, have long been a tool for cybercriminals. However, the data from these two years provides insight into how the nature of these attacks is changing, likely influenced by advancements in defense mechanisms, shifts in attacker tactics, regulatory impacts, and increased organizational preparedness.

Key Findings:

- Attacks lasting 90 minutes increased by 22.20%.
- There was an increase in the proportion of attacks falling within the 90-240 minute range, which accounted for 2.11%.
- Attacks in the 240-420 minute range increased from 67.96%, indicating a possible shift in attacker preferences or tactics within this range.
- The occurrence of attacks lasting between 420-720 minutes and 720-1200 minutes decreased by 2.19% and increased 32.53% respectively.
- Lastly, the duration of the longest attacks (1200+ minutes) saw a reduction from 95.03% of the total event count.

Duration (Minutes)	2022	2023
Maximum	27642.12	24267.33
Average	82.76	101.10

Table 1 - Maximum and Average duration between 2022 and 2023

These trends suggest several underlying factors at play in the cybersecurity arena:

Enhanced Security Measures: Organizations worldwide have ramped up their cybersecurity defenses, incorporating sophisticated detection systems, strengthening infrastructure resilience, and deploying swift response strategies to mitigate DDoS attacks effectively.

Evolving Attacker Strategies: Cybercriminals may be adjusting their approaches, possibly pivoting from prolonged assaults to shorter, more intense bursts of activity or other forms of cyber threats that are more challenging to defend against and potentially more damaging.

Regulatory and Enforcement Actions: Increased regulatory scrutiny and proactive law enforcement efforts against cybercrime networks have likely disrupted the operations of many would-be attackers, curtailing their ability to launch extended DDoS campaigns.

Greater Awareness and Preparedness: The cybersecurity community's heightened awareness and preparedness for DDoS threats have likely led to improved mitigation capabilities. This proactive stance enables organizations to quell attacks more swiftly, thus reducing their overall duration.

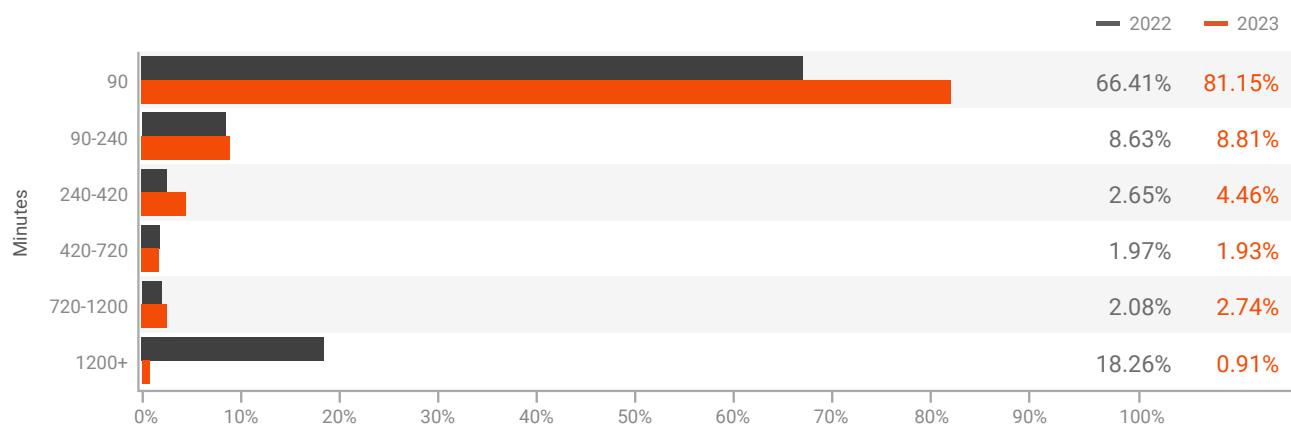


Figure 7 - Attack Durations Distribution in 2022 and 2023

81%
of attacks were shorter than 90 minutes

Gaining grounds in the Eternal Cyber Conflict

As major service providers and hosting companies invest heavily in DDoS mitigation technologies, often partnering with leading cybersecurity firms to bolster their defense, attacks are finding it increasingly difficult to sustain prolonged disruptions. Collaborative efforts by international law enforcement have also led to significant takedowns of botnets and individuals behind them.

The reduction in DDoS attack durations from 2022 to 2023 signals a positive trend in the ongoing battle against cyber threats. It underscores the importance of continued investment in cybersecurity defenses, the need for international cooperation in combating cybercrime, and the effectiveness of regulatory measures in protecting online spaces.

2023 Attack Statistics

Attack Size Distribution

In 2023, the landscape of Distributed Denial of Service (DDoS) attacks underwent notable changes compared to 2022. This section delves into the size of DDoS attacks observed during these years, highlighting trends, drawing comparisons, and exploring the underlying reasons for these shifts.

Data analysis reveals a significant shift in the distribution of DDoS attack sizes from 2022 to 2023. While the overall number of attacks decreased, there was a marked increase in the proportion of larger-scale attacks (≥ 10 Gbps). Specifically, attacks under 1 Gbps still constituted the majority but saw a decrease in their total count, indicating a possible shift towards more potent attacks.

Key Findings:

Decrease in Total Attacks: The total number of DDoS attacks saw a reduction in 2023. This 24.6% decrease suggests an evolving threat landscape where attackers might be opting for quality over quantity.

Shift Towards Larger Attacks: The most significant change was observed in the ≥ 10 Gbps category, which saw an increase for 2023. This dramatic rise (over 450%) in larger-scale attacks signifies a concerning trend towards more disruptive and powerful attacks.

Proportional Changes: While smaller attacks (< 1 Gbps) still dominate, their proportion slightly increased from 88.1% to 90.9%. Conversely, mid-sized attacks (≥ 1 and < 10 Gbps) saw a decrease in both count and proportion, highlighting a polarization towards either end of the scale.

Several factors could contribute to the observed shift in DDoS attack sizes:

Advancements in Attack Technology: Attackers are leveraging more sophisticated tools and techniques, enabling them to launch larger and more effective attacks with less effort.

Increased Attack Surface: The expansion of IoT devices and cloud services provides attackers with more targets and opportunities to amplify their attacks.

Motivation and Impact: Larger attacks often generate more media coverage and can fulfill various motives, including extortion, political activism, or demonstrating capability.

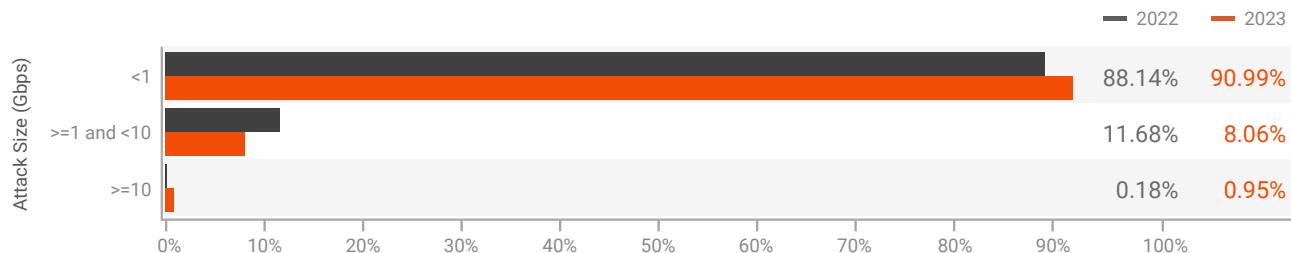


Figure 8 - Attack Size Distribution in 2022 and 2023

91%
of attacks were smaller than 1Gbps

The year 2023 marked a turning point in the nature of DDoS attacks, with a clear move towards larger, more destructive efforts. This evolution demands heightened awareness and enhanced security measures from organizations worldwide. As attackers continue to refine their strategies, the need for robust defense mechanisms and international cooperation becomes ever more critical.

2023 Attack Statistics

The State of Bit- and- Piece DDoS Attacks in 2023

In 2023, Distributed Denial of Service (DDoS) attacks notably evolved in complexity and impact, with Bit-and-Piece (BNP) attacks emerging prominently. These attacks employ small data packets from diverse sources to flood systems, challenging to detect and mitigate. Data shows 214 Autonomous System Numbers (ASNs) were hit by 1,177 BNP DDoS incidents, leveraging amplification methods like CHARGEN, SSDP, DNS, and NTP, impacting various countries including Australia, Bangladesh, Brazil, and Bulgaria.

Summary 1 - Bit-and-Piece Attacks in 2022 and 2023

		2022	2023	Difference
No. of Targeted ASN		240	214	-10.83%
No. Target Geolocations		20	30	50.00%
Total IP prefixes under attack(Class C)		3,079	1,177	-61.77%
No. of targeted IP addresses per IP prefix	Minimum	30	30	0.00%
	Maximum	256	256	0.00%
Attack Duration(Minutes)	Minimum	2.00	13.18	599.0%
	Maximum	2,577.00	1,571.65	-39.01%
Attack Count per IP	Minimum	40	40	0.00%
	Maximum	74,570	8,124	-89.11%
Attack Count per IP Prefix	Minimum	441	1,278	189.80%
	Maximum	3,366,723	63,245,641	1778.55%
Attack Size by IP (Gbps)	Minimum	0.0004	0.0020	400.00%
	Maximum	21.38	49.82	133.02%
Attack Size by IP Prefix /24 (Gbps)	Minimum	0.0297	0.0245	-17.51%
	Maximum	123.72	178.06	43.92%

Targeted ASNs

214

Total No. of IP Prefixes (Class C) Under Attack

1,177

Summary 2 - Bit-and-Piece Attack Types

2022	2023
SSDP Amplification Attack(44.75%)	CLDAP Reflection Attack(0.27%)
NTP Amplification Attack(20.14%)	HTTPS Flood(0.19%)
Memcached Attack(10.89%)	BITTORRENT Amplification Attack(0.19%)
CHARGEN Attack(6.86%)	L2TP Amplification Attack(0.16%)
UDP Fragmentation Attack(6.15%)	IP Fragmentation Attack(0.11%)
DNS Amplification Attack(2.50%)	DNS Attack(0.05%)
UDP Attack(1.62%)	SIP Flood(0.03%)
TCP ACK Attack(1.59%)	STEAM PROTOCOL Amplification Attack(0.03%)
ICMP Attack(0.88%)	
TCP SYN Attack(0.69%)	
SNMP Amplification Attack(0.52%)	
IP BOGONS(0.47%)	
TCP RST Attack(0.44%)	
TCP Null Attack(0.38%)	
TCP Fragmentation Attack(0.38%)	
HTTP Flood(0.36%)	
WS-DISCOVERY Amplification Attack(0.36%)	
	CHARGEN Amplification Attack(46.67%)
	SSDP Amplification Attack(18.39%)
	NTP Amplification Attack(11.58%)
	UDP Fragmentation Attack(8.28%)
	MEMCACHED Amplification Attack(6.52%)
	DNS Amplification Attack(4.25%)
	UDP Attack(1.47%)
	TCP SYN Attack(1.25%)
	WS-DISCOVERY Amplification Attack(0.81%)
	TCP SYN-ACK Attack(0.37%)
	TCP ACK Attack(0.15%)
	L2TP Amplification Attack(0.15%)
	ICMP Attack(0.07%)
	DNS Attack(0.07%)

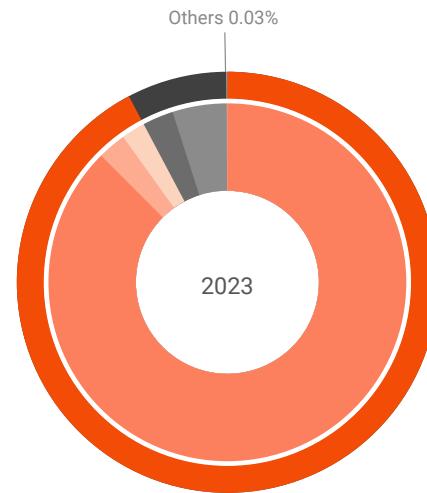
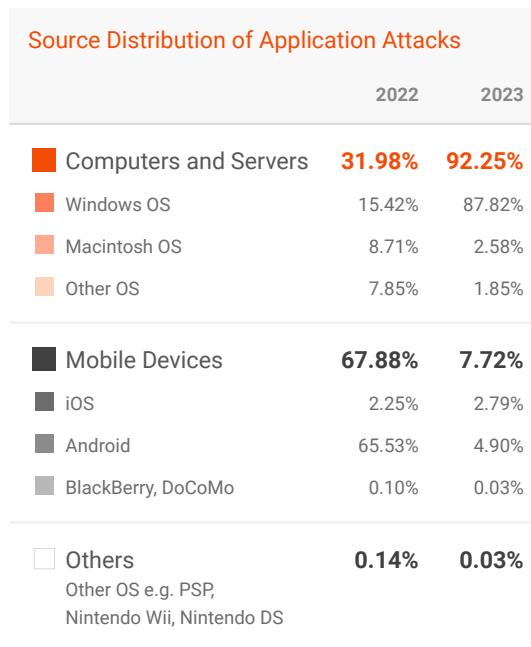
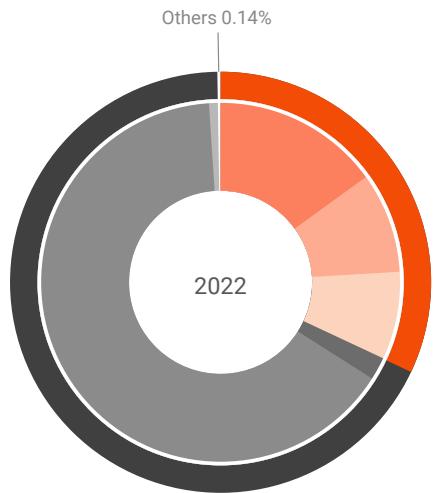


Figure 9 - Source Distribution of Application Attacks in 2022 and 2023

No system is Infallible

The shift in primary attack sources to Windows OS devices, reflects the dynamic nature of cyber threats. It emphasizes the need for ongoing vigilance, software updates, and reinforced cybersecurity defenses for all systems and networks. Real-world examples in 2023, such as the exploitation of Microsoft Exchange Server vulnerabilities and the rise of ransom DDoS attacks, serve as stark reminders of the tangible impacts of these attacks. As attackers evolve, we must adapt our defense and resilience strategies against DDoS attacks.

2023 Attack Statistics

Application Attack Source Distribution (IP Reputation)

Top 10 Attack Sources Ranking in APAC (2023)		Top 10 Attack Sources Ranking in Europe (2023)	
	2023		2023
China	91.49%	Russian Federation	21.93%
Singapore	3.12%	United Kingdom	15.37%
Thailand	0.97%	Germany	14.53%
India	0.87%	Netherlands	8.96%
Indonesia	0.76%	France	8.06%
Hong Kong	0.66%	Spain	3.20%
Taiwan	0.39%	Poland	3.20%
Japan	0.25%	Ukraine	2.95%
Australia	0.22%	Italy	2.69%
Malaysia	0.22%	Ireland	2.12%
Others	1.05%	Others	16.99%

Top 10 Attack Sources Ranking in Middle East and Africa (2023)

	2023
Turkey	66.89%
Tanzania, United Republic of	5.46%
Iran	5.11%
Mozambique	3.32%
Israel	3.27%
Kenya	2.65%
South Africa	1.95%
Nigeria	1.17%
Morocco	0.96%
Egypt	0.96%
Others	8.26%

Top 10 Attack Sources Ranking in America (2023)

	2023
United States	60.43%
Brazil	29.83%
Canada	3.66%
Mexico	1.12%
Argentina	1.08%
Colombia	0.74%
Ecuador	0.40%
Belize	0.38%
Peru	0.34%
Venezuela	0.32%
Others	1.70%

Geo-Political Undercurrents Drive DDoS Attacks

The prominence of these countries in DDoS attack distribution is not solely a matter of technological infrastructure but also reflects socio-economic factors, cybersecurity practices, and geopolitical considerations. For instance, lax cybersecurity regulations, inadequate defense mechanisms, and the presence of large numbers of unsecured devices contribute to the volume of attacks originating from these regions. This 2023 data on DDoS attack sources underscores the complex, multifaceted nature of cyber threats. Understanding the reasons behind the geographic distribution of these attacks is crucial for developing effective countermeasures.

2023 State of the Phish

An in-depth exploration of user awareness,
vulnerability and resilience

Key Findings

44%

of people think an email is safe when it contains familiar branding



300-400K

telephone-oriented attack delivery attempts daily, with a peak of 600k per day in August 2022

1/3



of people took a risky action (such as clicking links or downloading malware) when faced with an attack



Increase in direct financial loss from successful phishing



30 Million

malicious messages sent in 2022 involved Microsoft branding or products



> 1 in 10

threats were blocked as a result of user reporting

1/3+

can't define "malware," "phishing" and "ransomware"

Even basic concepts are misunderstood



ONLY 35% of organizations conduct phishing simulations

64%

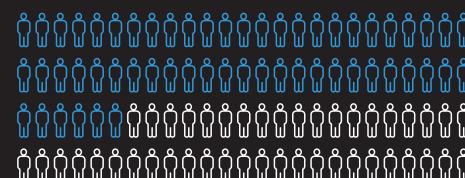
of organizations infected with ransomware paid a ransom

90%

of organizations affected by ransomware held a cyber insurance policy

65%

of organizations reported at least one incident of insider data loss



ONLY 56% of organizations with a security awareness program train all their employees

90%

of security professionals consider security a top priority at their company

VS.

33%

of employees say cybersecurity is not a top priority of theirs at work

COMING TO TERMS:

Even basic concepts are still not fully understood—more than a third can't define "malware," "phishing" and "ransomware"

40%

of users know what ransomware is, a 9-point jump from 2019—the biggest increase among the terms we asked about

29% and 30%

of users knew the relatively new terms smishing and vishing, respectively

58%

of users knew what phishing is, a 5-point increase from last year but 3 points below 2019

Security Habits and Knowledge Gaps

Last year's *State of the Phish* described 2021 as "the year of the new normal." The pandemic started to recede, and many workplaces permanently adopted a hybrid model. Those macro trends have continued in 2022, cementing an expanded attack surface that cyber criminals can target both in and out of the office.

The increased risks of a hybrid workplace are well understood by CISOs, and many told us in our 2022 *Voice of the CISO* report that they planned to take steps to enhance security awareness programs to meet this challenge.

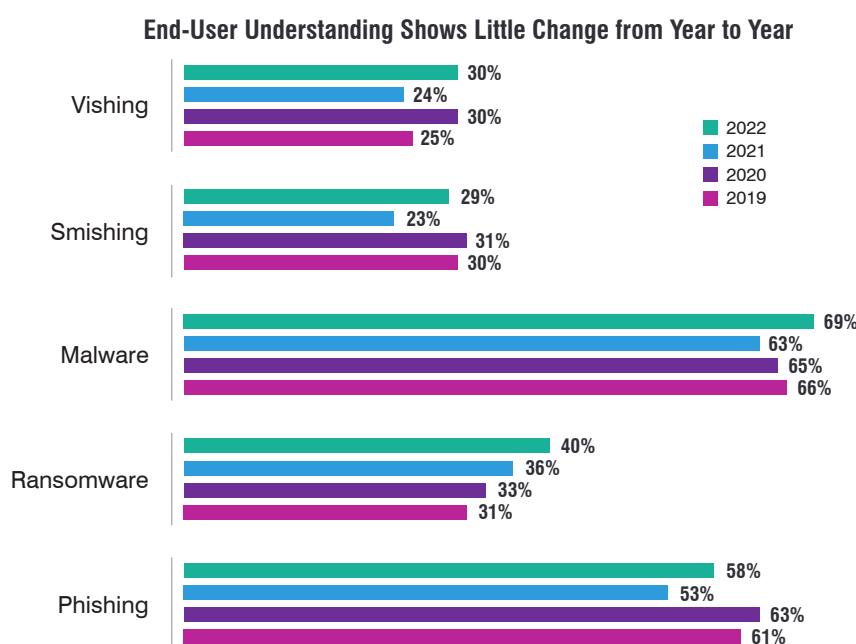
All of which begs the question: has the basic level of security awareness and understanding increased since last year?

Unfortunately, the short answer is "no."

Terms and concepts: the same gaps remain

Common threats are still not well understood across organizations. Nearly a third of survey participants were unable to correctly define terms like "phishing" and "malware." For more advanced attacks like "ransomware," "smishing" (SMS phishing) and "vishing" (voice phishing) around two-thirds answered incorrectly.

Data from the past four years shows only modest gains or no gains at all.



IMPOSTER SYNDROME:

21%

of users don't know that an email can appear to be from someone other than the sender

44%

of users don't know that a familiar brand doesn't make the email safe

63%

of users don't know that an email link text might not match the website it goes to

Moving on from terminology to security fundamentals, the story is more encouraging. Some 80% to 90% of respondents said they understood basic email security concepts. Numbers here have increased by 2 to 3 percentage points year over year.



know to be cautious of unexpected emails



know email attachments can have damaging software



know an email can appear to come from someone other than the sender

We saw a similar degree of improvement for more advanced email security concepts, though overall understanding was lower at just 40% to 50%. Notably, people have become more aware that cyber criminals can send multiple emails to build trust. This evolution of this tactic has been a point of focus for our threat researchers this year, particularly with state-sponsored attacks.



know a familiar company brand doesn't make an email safe



know a link or attachment can affect computers beyond theirs



know their email provider can't automatically block all malicious emails



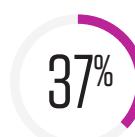
know exchanging multiple emails doesn't mean a sender is safe



know that files stored in the cloud are not always safe



know internal emails at work are not always safe



know an email link might not match the website it goes to



know their company can't automatically block all malicious emails

THE UNCERTAINTY PRINCIPLE:

Nearly 30% of respondents said that they weren't sure if files stored in the cloud are always safe. This was by far the highest percentage of "not sure" answers; others ranged between 8% and 20%. In security terms, "not sure" and "don't know" both describe a knowledge gap. Instead of just focusing on incorrect answers, training programs should also aim to address blind spots.

Security habits: blurred lines

In the last four years of tracking security habits both at home and at work, we've seen a noticeable shift. It's now the case that over three-quarters of people use their work devices for personal activities, with almost the same proportion using personal devices for work.



use work devices for personal activities



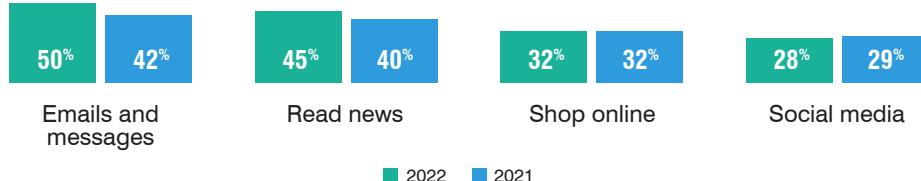
use personal devices for work devices



let family and friends use their work devices

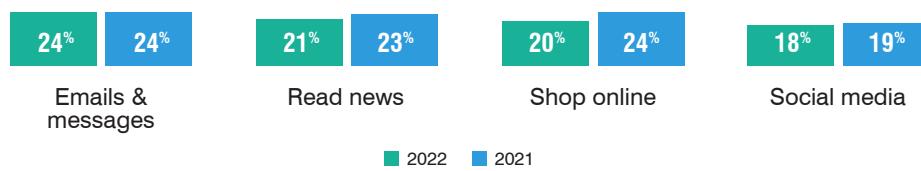
Personal use of work devices for social media and online shopping held steady from year to year. However, email, messaging and reading news all increased.

Personal Use of Work Devices



Nearly half of respondents said they allowed friends and family to use their work devices. This number has fallen slightly year on year (from 56% to 48%), possibly because of people returning to offices for more days during the week. Most categories of use by friends and family remained static year on year, with email and messaging the most common activities.

Friends & Family Use of Their Work Devices



Unfortunately, a small percentage of respondents (3%) said they didn't know what their friends or family did on their work device. This clearly represents an unacceptable level of risk.

PASSWORD UNPROTECTED:

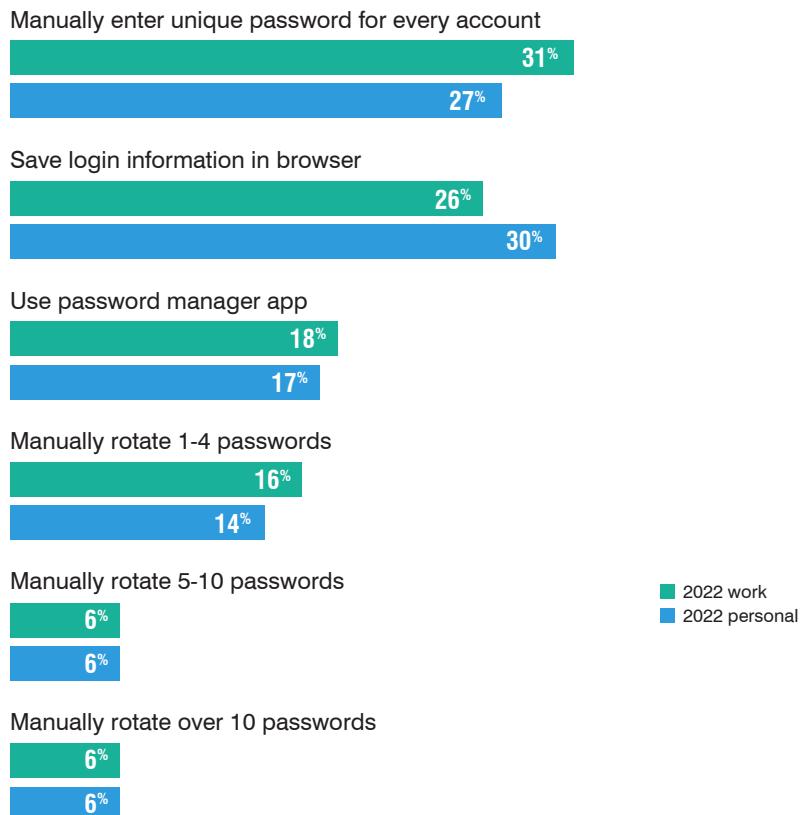
28%

of users reuse passwords for multiple work-related accounts, jeopardizing all of them if even just one is compromised

Security habits: password hygiene

Another area where behavior has remained disappointingly unchanged is password management.

Use of Home and Work Passwords



The most common method is the most secure: using a single unique password, entered manually per account. In second and third place, less-secure browser password managers are still more popular than dedicated apps. While the least secure options are to be found in the long tail of responses, more than a quarter of respondents admitted to reusing a limited number of passwords.

WIRELESS WEAKNESSES:

71%

of users don't change the default network name on work Wi-Fi routers

80%

of home and work Wi-Fi users didn't change the default admin password for their routers in 2022—worse than the previous year

Security habits: Wi-Fi woes

Password problems aren't just limited to email and cloud accounts. We also found that numbers are low when it comes to Wi-Fi password best practices.

Percentage of Actions to Protect Home Wi-Fi

Password protect the network



Change default network name



Change default network password



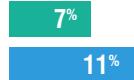
Change default admin password



Check router software updates



Don't take any security measures



Over two-thirds of people password protect their home network. But the number of people who change default wireless and administration passwords is much lower, at less than a third each. Most alarming of all, 7% of respondents said they took no home Wi-Fi security measures at all.

ACTIONS SPEAK VOLUMES:

34%

of users did something in 2022 that put themselves or their organizations at risk

63%

of working adults think an email link always goes to the matching website brand

11%

of recipients fell for phishing simulations mentioning “DocuSign document for review” and “FedEx delivery failure”

As part of our survey, we asked people why they don't take these necessary steps to secure their home networks. The range of answers is revealing:

Feel security is already in place (“That's what my network provider does.”)

Think there is built-in safety (“I thought it was safe enough.”)

Never think about security (“I have never thought to change any of these things.”)

Security handled by someone they know (“My spouse looks after this.”)

Made security changes previously (“I made changes when it was set up.”)

Made some changes but not others (“I have modified the ones I thought appropriate.”)

Don't know how to change settings (“I was worried I would mess it up.”)

Security habits: risky business

With these gaps in knowledge and best practices, it's no surprise that many people continue to take risky actions when faced with a cyber attack. And with many risky actions not being recognized in the moment (or admitted to after the fact), these numbers are almost certainly lower than the reality.

Risky Actions Taken by Working Adults in Threat Situations

Any type of risk action

34%

Clicked phishing link to fake website

18%

Downloaded malware from smish

13%

Downloaded malware from phishing link/site

11%

Gave personal information to a scammer

9%

Gave password to untrustworthy source

8%

More than a third of respondents took at least one risky action during the year, with clicking on malicious links being the most frequent. With email overwhelmingly the most common vector for distributing phishing links and malware, training users on the correct action to take should remain a key part of ongoing security awareness initiatives.

84%

of organizations faced at least one successful phishing attack

54%

faced three or more attacks

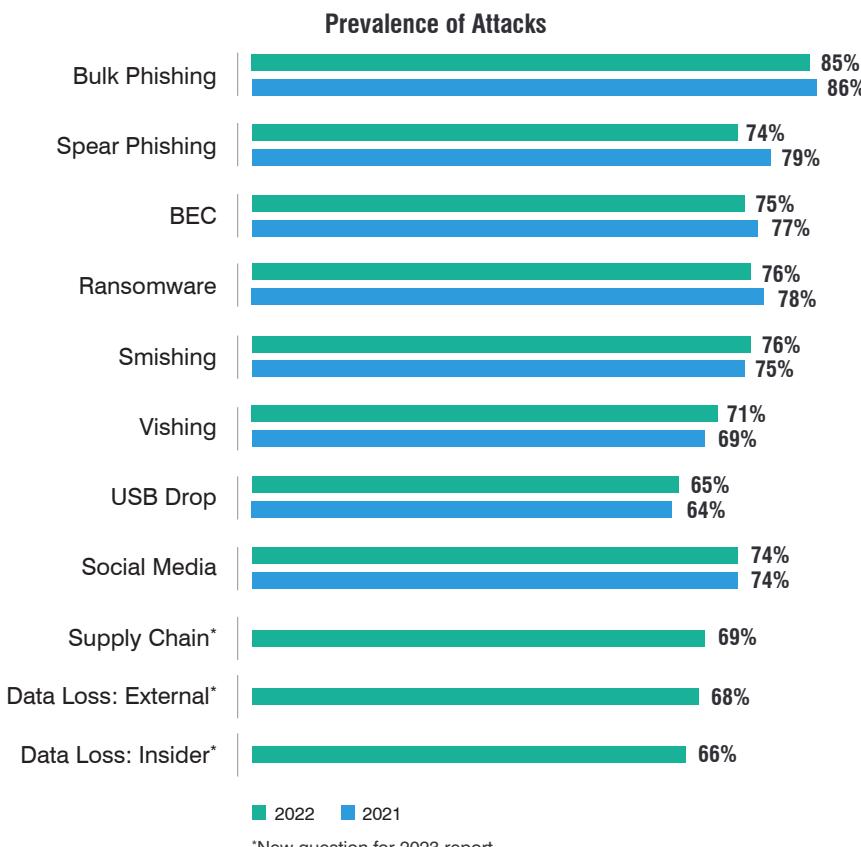
Recognizing Risk

Cyber criminals know that most people have gaps in their security awareness. Their own campaign dashboards provide the evidence, with phishing kits, botnets and malware-as-a-service often showing click rates, downloads and other common digital “success” metrics.

Despite many techniques remaining effective, attackers aren’t standing still. They have refined their social engineering tactics and introduced entirely novel attacks. When the threat landscape moves this quickly, security teams—and security awareness programs—need to be agile to keep up.

The incidence of most attack types has remained constant year on year, with high levels across the board. Threats arrive at an unrelenting pace and are almost as likely to appear from inside an organization as from an external attacker.

In total, 84% of survey respondents said that their organization had experienced at least one successful email-based phishing attack during 2022. And 54% said that they had dealt with three or more attacks.

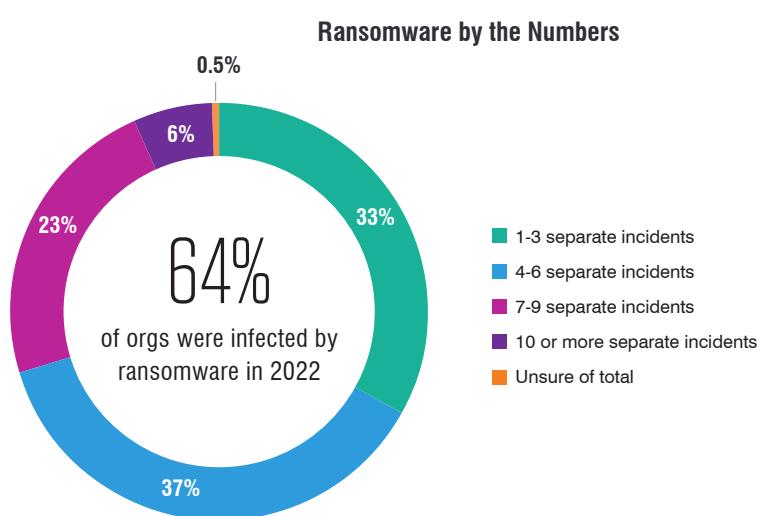


90%
of organizations that were infected by ransomware had cyber insurance

99%
of ransomware victims in the U.S. had cyber insurance, the highest percentage among countries surveyed

Ransomware remains

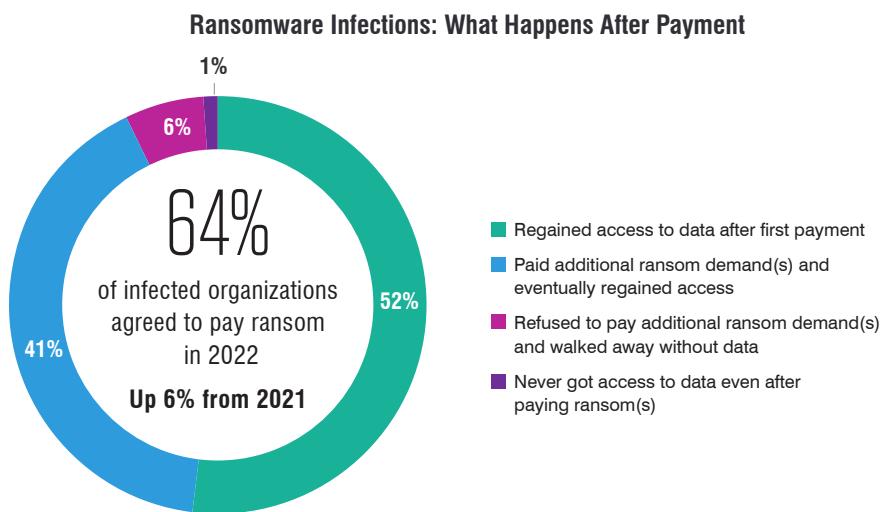
BEC might be the most lucrative form of cyber attack, but ransomware can inflict massive operational, reputational and financial damage. About 76% of organizations experienced an attempted ransomware attack, with 64% experiencing a successful infection. Alarmingly, over two-thirds of respondents said their organizations experienced multiple separate incidents of infection.



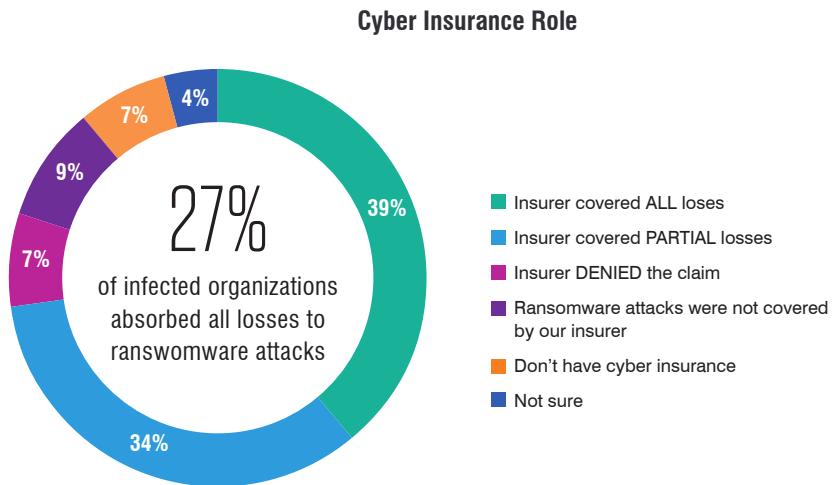
The FBI's latest Internet Crime Complaint Center (IC3) report shows that ransomware attacks have continued to rise, increasing by 51% year over year. The Bureau recommends that organizations refrain from paying, as this only contributes to the threat's growth.

There is also no guarantee that payment will result in a positive outcome. About 52% of victims—slightly better odds than a coin flip—regained access to their data after making a single ransomware payment. Nearly as many were obliged to make further payments, and some still never regained access to their data. Still, most infected organizations paid up, and many did so more than once—usually with the help of cyber insurance.

The overwhelming majority of organizations that faced a ransomware attack had cyber insurance (90%), and most of those insurers were willing to help (82%). This perhaps explains the high propensity to pay, with 64% of organizations infected with ransomware paying at least one ransom—a six-point increase from last year.



Some 41% said they paid more than one ransom before regaining access to their data. The majority of companies taking out cyber insurance (73%) said that their insurer covered some or all the losses incurred.



25%

of users said they had changed jobs within the past two years

44%

of those who left a job took data with them

The insider threat

According to 1,400 global CISOs surveyed in our 2022 *Voice of the CISO* report, insider threats are their biggest security concern. And today's job market has made data protection an even bigger challenge. Pandemic-related job mobility coupled with post-pandemic economic uncertainty has resulted in large numbers of people changing or leaving jobs. And data shows that people often take sensitive data and credentials with them when they go.

In this year's survey, we asked end users if they had changed jobs within the past two years. A quarter said that they had, and, of those who left their jobs, nearly half admitted to taking data with them when they left.

We also added questions about insider data loss to our survey of security professionals. Nearly 65% reported that their organization had experienced data loss because of an insider. The number was even higher for the U.S., the U.K. and the Netherlands at around 85%.



report one to 10 data loss incident(s) via insider



report 11 to 25 data loss incidents via insider



report 26 to 50 data loss incidents via insider



report over 50 data loss incidents via insider

The most common cause of data loss to insiders is the result of carelessness or negligence. But that isn't the only type of insider threat. In general, they fall into three main categories:



A “**careless user**” might cause accidental harm, such as a Japanese city contractor who lost a USB stick with the personal data of almost half a million residents.



A “**malicious user**” takes actions for deliberate harm or personal gain, such as an outgoing Pfizer employee who allegedly uploaded over 12,000 confidential files to a Google Drive account.



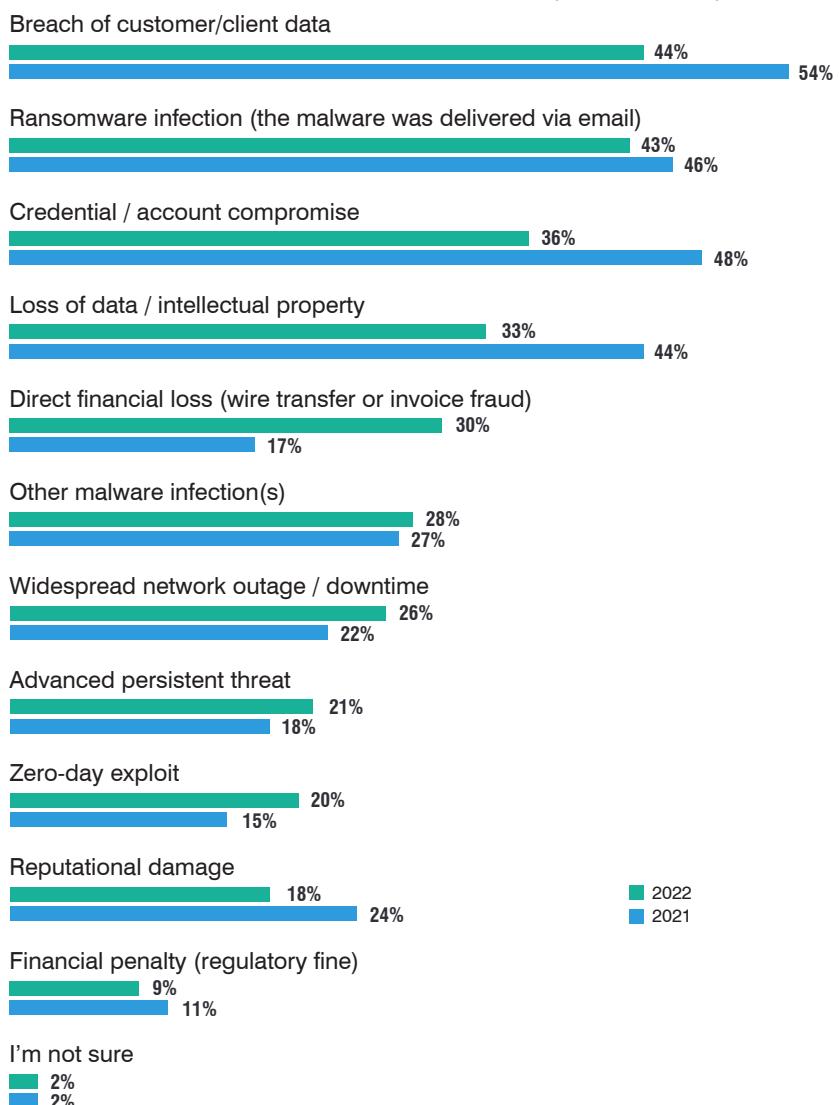
A “**compromised user**” is enticed by reward or coercion to infiltrate or exfiltrate data, such as a former SoftBank chief accepting ¥400,000 to leak confidential information to a Russian diplomat.

Counting the cost

For most threat actors, the goal of an attack is financial. And according to our data, 30% of organizations that endured a successful attack experienced a direct monetary loss, such as a fraudulent invoice, wire transfer or payroll redirection. This is an increase of 76% year over year.

The three most common consequences of attack were data breach (44%), ransomware infection (43%) and account compromise (36%). As all three of these actions can be readily monetized by cyber criminals, the financial incentives driving attacks are clear to see.

Results of Successful Phishing Attacks (Global Average)



PHISHING SIMULATION BY THE NUMBERS:

135 million+

simulated phishing attacks sent by our customers in 2022. An increase of 39 million over the 2021 number (96 million).

~410 million

simulated phishing messages have been sent since we started counting.

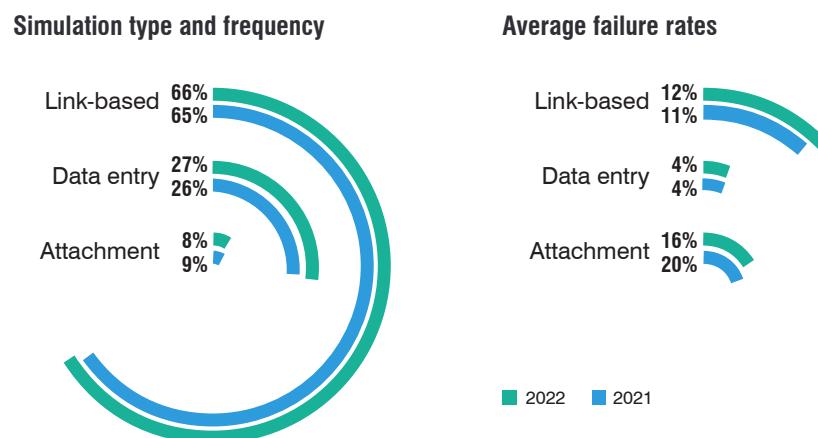
Benchmarks: Failure Rates, Reporting and Resilience

In addition to surveys and threat research, *State of the Phish* also compiles data from our phishing simulation tool to help identify areas of risk and areas for improvement.

The first headline to note is that users continue to display a major vulnerability to, well, headlines. Trending topics from news or social media are often engaging and can cause people to ignore red flags. Beyond regularly targeting seasonal events like holidays and the tax deadline, threat actors moved quickly to adopt the COVID-19 pandemic as a favored lure subject. Cyber criminals are nimble and opportunistic—so security awareness programs should use real-world threat intelligence and be modelled on real-world lures. Our researchers even saw a campaign making use of the death of Queen Elizabeth II to distribute malware.

Template failure rates

Attackers are adaptive, so phishing simulations should cover a range of templates and themes to reflect the current landscape. In real-world terms, attacks using unsafe URL links are between three to four times as common as those containing attachments. So the current ratio of link and attachment templates needs rebalancing. Especially as attachments still have an appreciably higher failure rate than links (though this has fallen by 4% since last year).



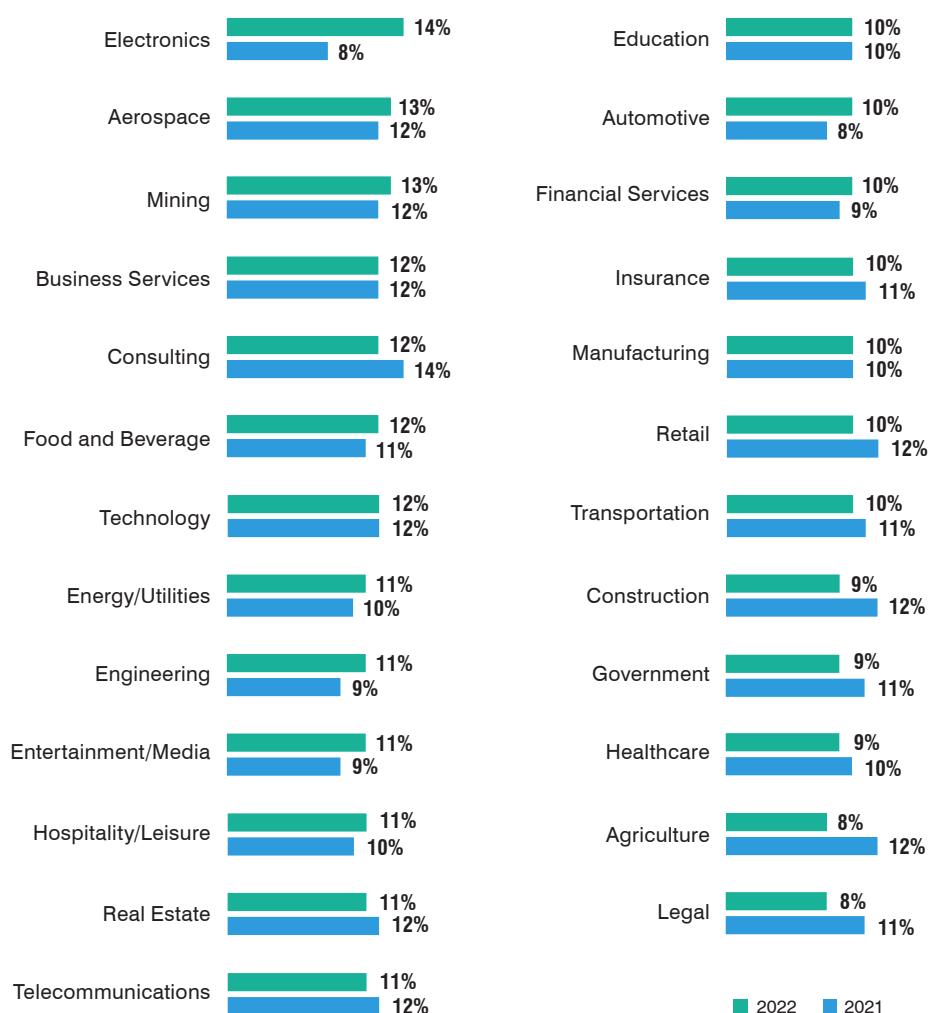
FAILURE RATE COMPARISON:

Each industry represented in our failure rate comparison includes data from at least 20 organizations and at least 300,000 simulated phishing attacks.

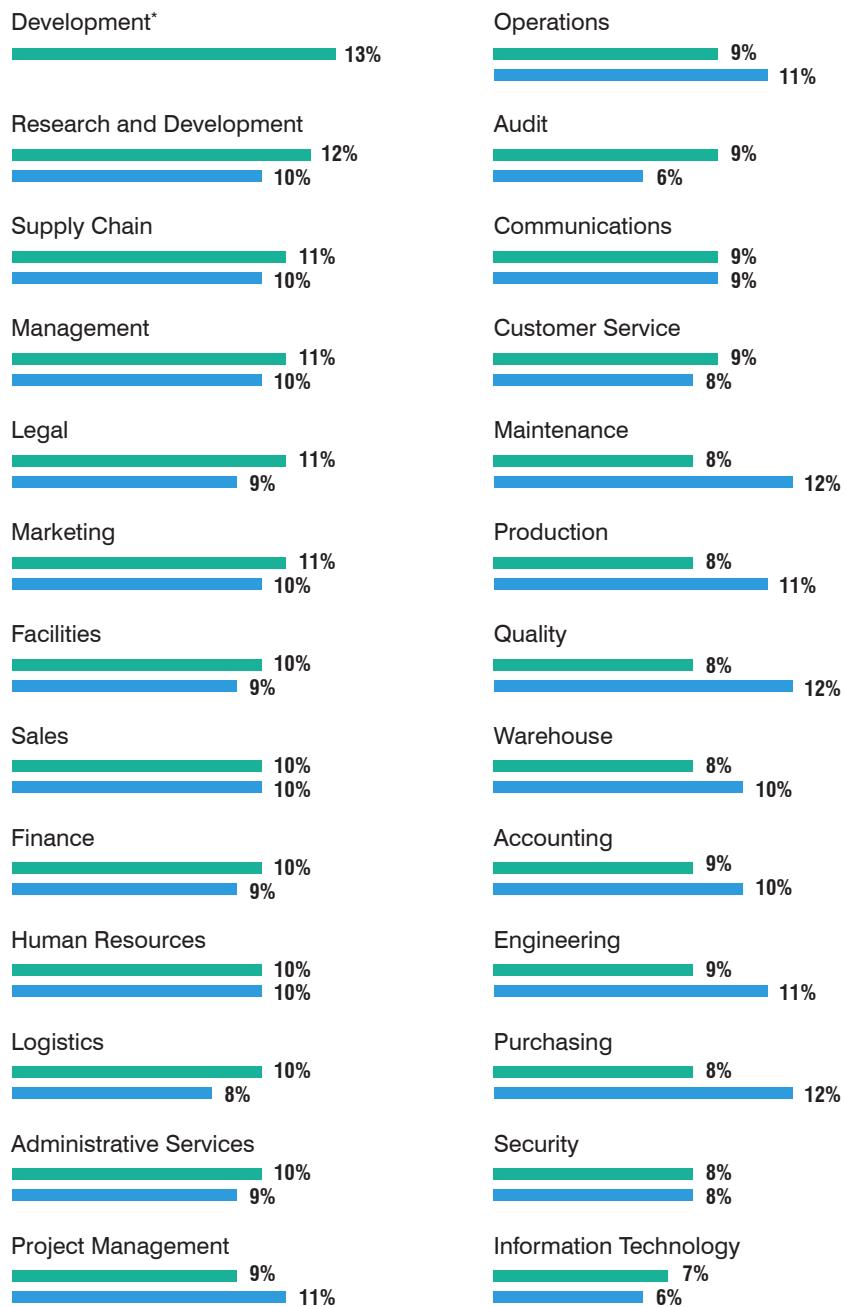
Failure rates by industry

Below are the industry average failure rates for phishing simulations. The data is in aggregate and contains all template types. Legal has the lowest overall failure rate, and electronics has the highest.

Failure Rates by Industry



Failure Rates by Department



■ 2022 ■ 2021

*New question for 2023 report

FAMILIAR FAKES:

Microsoft was the most-used template category in phishing simulation campaigns in 2022, including subjects across Microsoft OneDrive, Teams, and O365 Auth.

Template effectiveness

As we've seen, newsworthy topics are highly effective, both as real-world threats and simulation templates. Among the 10 most-used template themes in 2022, the failure rate for a COVID-19 lure was more than 50% higher than the next closest theme.

Subject	Failure Rate %
Coronavirus: COVID Update	17
Cloud Services: DocuSign document for review	11
Shipping: FedEx delivery failure	11
Microsoft: OneDrive contract shared	7
Email Account Alert: Email disconnect	7
Email Account Alert: Undelivered email	6
Email Account Alert: Queued email	4
Shipping: Amazon shipment	2
E-commerce/Retail: Amazon mismatch	1

COVID-19 was also represented twice in our list of “trickiest” themes—those with the highest failure rate regardless of how many times the template was used. Corporate internal communications/HR comms also appeared on the list multiple times. This suggests that employees are particularly vulnerable to messages alluding to disciplinary or other work-related issues that raise anxiety and reduce attention. Also surprising was people’s tendency to fall for entertainment-themed attacks, where messages related to personal interests in sport or television landed in their corporate inbox. This perhaps reflects the reality of how often work email is used to sign up for personal accounts.

Subject	Failure Rate %
E-commerce/Retail: E-Gift card	27
Entertainment: Squid Games next season early access	25
Banking/Financial Services: Purchase problems and funds removed	24
Coronavirus: COVID data cases report	23
Travel: Room confirmation	23
Corporate Communications: Dress code	22
HR: Code of Conduct—Reported incident	21
Coronavirus: COVID—List of infected users	20
Corporate Communications: Building evacuation plan	20
Entertainment: NBA Finals brackets	20

Most of the simulated campaigns our customers ran used two or three templates, with the average being 2.4. This is slightly higher than last year. Threat actors change their email lures from day to day, so using more templates reduces the chance of a simulation becoming widely discussed and increases the accuracy of the test.

Reporting and resilience

Reporting suspicious email is key to both defending against cyber attacks and to evaluating the effectiveness of an organization's security awareness efforts.

Overall, reporting rates for simulated phishing increased to 17% (vs. 15% in 2021). Failure rates for attacks remained at 10%. From these two numbers, we calculate a "resilience factor," which provides a quick way to gauge how resistant industries and departments are to attack. Note: the failure rates below are a subset of totals used previously, limited to customers who use our PhishAlarm in-client reporting tool.

$$\frac{17\%}{10\%} = 1.7$$

average reporting rate average failure rate resilience factor

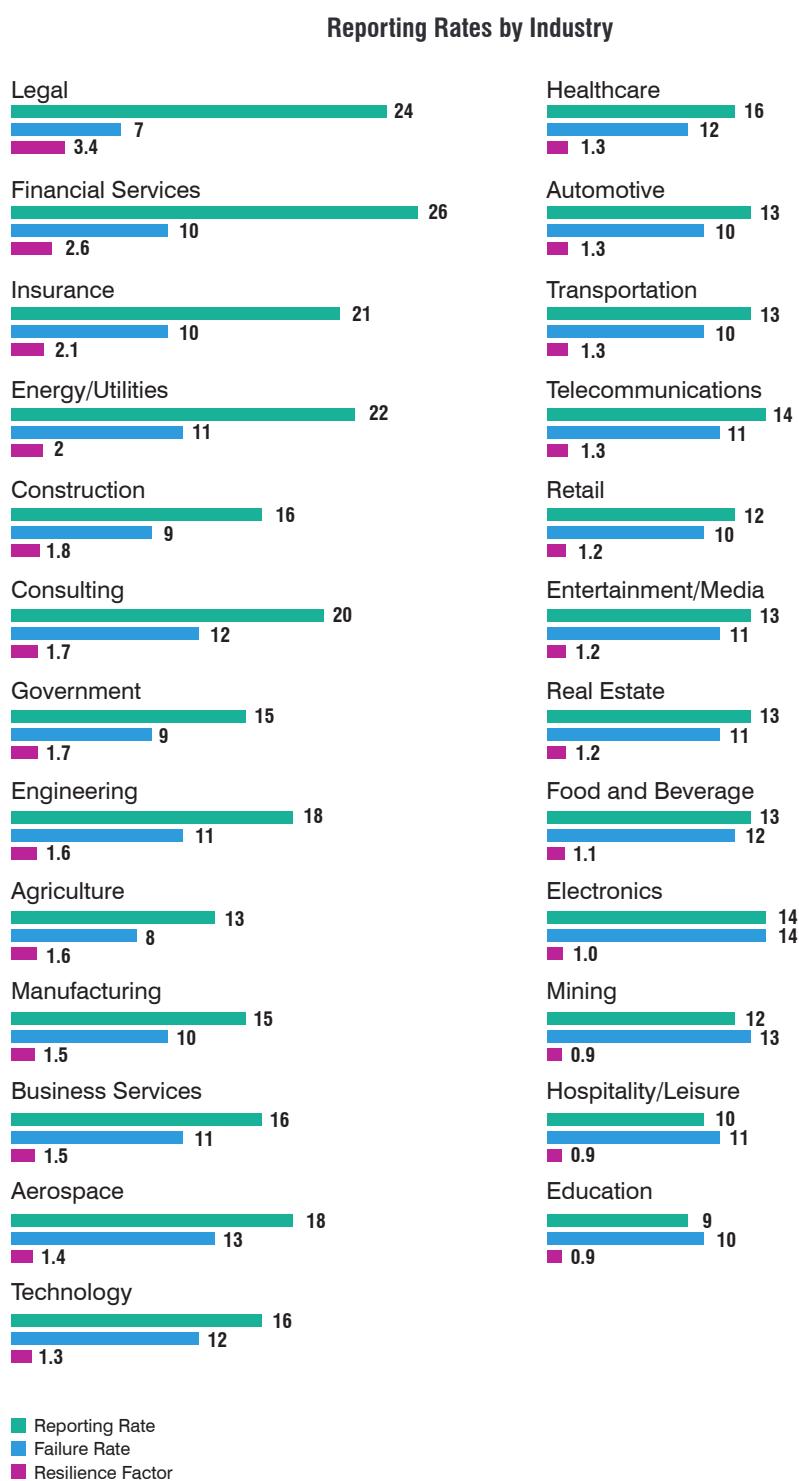
Last year the average resilience factor was 1.5, meaning that people have become slightly better at reporting and resisting attacks. This is reflected across all three template types:

	2022	2021
Link-based	17%	16%
Data entry	19%	17%
Attachment	19%	18%

At industry level, there is a broad span of resilience scores, ranging from 3.4 in legal to 0.9 in education. While the relatively strong performance of high-stakes industries like financial services and energy is heartening, several critical pieces of infrastructure fall below average, including agriculture, healthcare and transportation. As ransomware attacks on healthcare services over the past few years have shown, the consequences of low cyber resilience in these organizations can be severe.

INDUSTRY REPRESENTATION

Each industry represented in our failure rate comparison includes data from at least 20 organizations and at least 300,000 simulated phishing attacks.



75 million
malicious messages were blocked
by Proofpoint as a result of
user-reported suspicious emails

Our PhishAlarm button is ultimately designed to let users report suspicious real-world messages, not just phishing simulations. Beyond giving security teams a way to measure user response, user-reported emails are one of the signals that power our threat detection engines. In fact, we blocked an additional 75 million malicious messages in 2022 based on intelligence from user-reported attacks.

Between them, those malicious messages contained:

47 million+
credential phishing emails

~600,000
downloaders

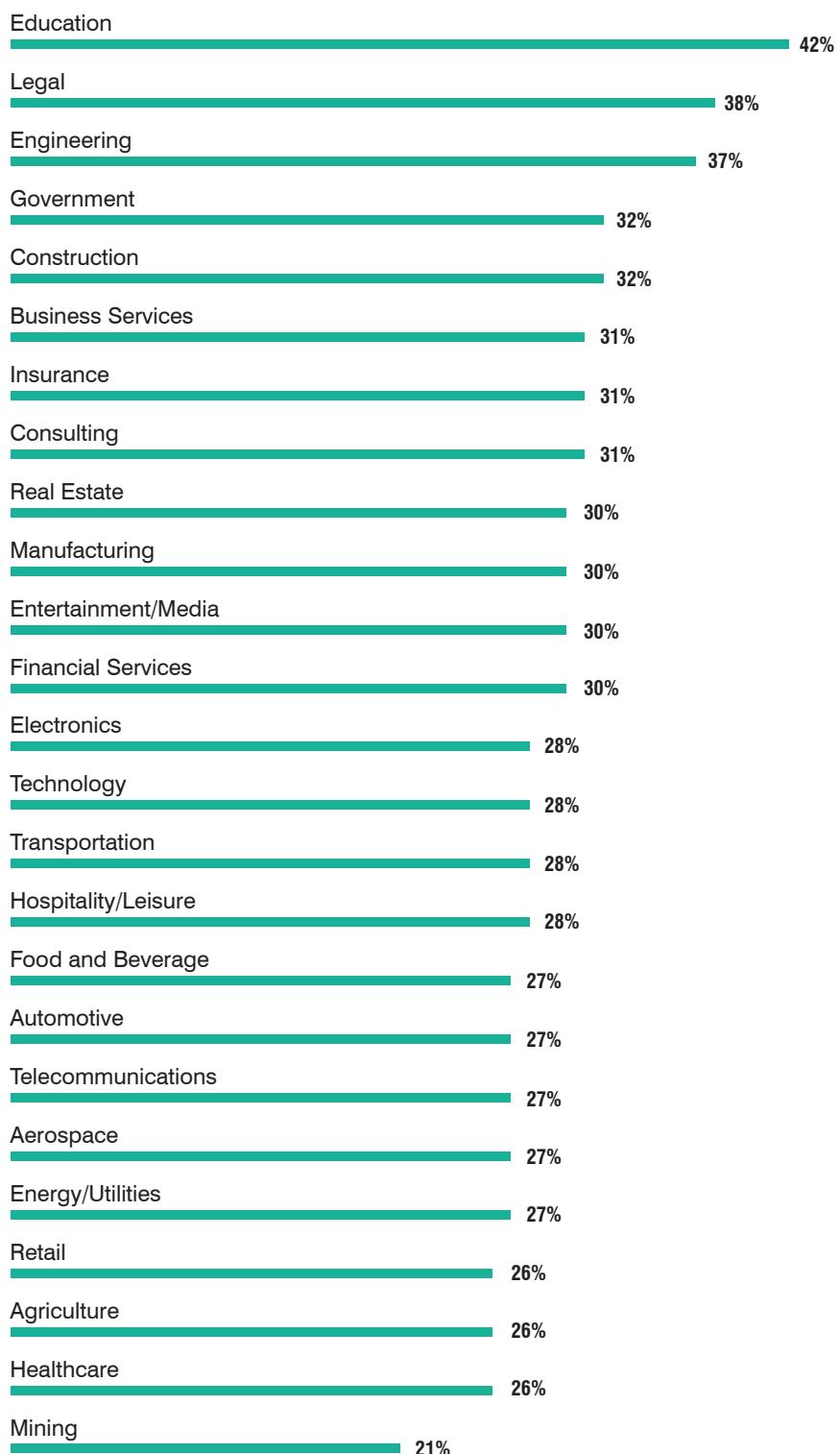
1.5 million+
emails containing malware

260,000+
keyloggers and stealers that could
lead to account compromise

1.2 million+
banking Trojans

680,000+
botnet malware

Of course, not every reported email turns out to be malicious. So we also benchmark real-world reporting accuracy for customers who use our PhishAlarm report button. Notably, while education had the lowest resilience among named industries, its real-world reporting accuracy is highest.

Accuracy Rate by Industry

98%

of organizations had a training program of some sort

but...

Only 56%

trained everyone in the organization

and...

Only 35%

ran phishing simulations

Security Awareness: Insights and Opportunities

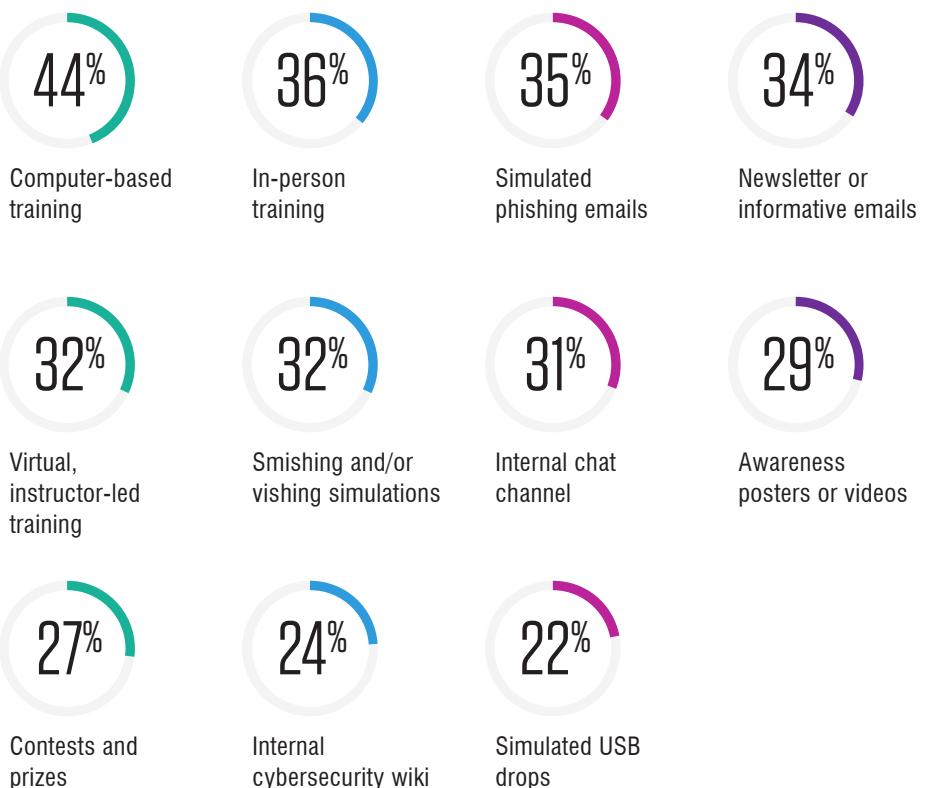
The majority of organizations covered by our surveys have security awareness programs. But most struggle to make them effective.

In fact, 27% of respondents said that failure rates had remained the same, even after introducing training. This is a big untapped opportunity. Time is already being dedicated to training, and, with a few key improvements, resilience and awareness could increase significantly.

Almost every organization offers a training program of some sort, with 74% conducting formal security awareness training. So far, so good. But only 56% train everyone in the organization—a figure which hasn't improved much since last year. And while training is the foundation of security awareness, it can only do so much.

As we've seen, the threat landscape moves fast. Threat actors are always innovating. An effective way to assess user vulnerability to new threats in a secure environment is to use phishing simulations drawn from real-world lures. But only 35% of organizations use simulations—down from 41% in 2021. Times are hard, and budgets are shrinking, but the cost of a breach makes skimping on security a risky trade.

We asked respondents about their use of a range of training options:



In addition to regular, formal training, 79% of organizations offered training for people who fell for real-world or simulated phishing attacks. This was a six-point drop from last year. Overall, time given to training was low, with 80% of respondents saying their organizations only offered two hours or less per year.

When it comes to training topics, malware, email-based phishing and Wi-Fi security were the most covered subjects, followed by ransomware. This aligns with the results of our end-user survey, which found that malware, phishing and ransomware were the terms users were most likely to correctly define.

Most organizations say that they use threat intelligence to inform their training, though this wasn't something we found reflected in more specific questioning about content. And when it comes to aligning with top CISO concerns, only 23% of programs covered supplier risk. Likewise, only 31% cover BEC, despite this being the most financially damaging form of cyber crime.

Building a security culture

Finding the right balance between reinforcement and punishment is an perennial problem. Since last year, we've seen a few changes at both ends of the spectrum, with decreases in both the most lenient and the harshest actions for people who fail simulated or real-world attacks.

Overall, 52% of organizations have formalized consequences in place for employees who interact with real or simulated attacks (55% in 2021). And 26% of those who don't have such a model in place say they are considering it or will implement one soon. About half of organizations say they won't discipline employees until they have failed at least three phishing tests.

Discipline Model for Employees

Counseling from manager



Counseling from information security team



Disciplinary actions by HR (warning, probation)



Impact to yearly performance review



Removal of access to systems



Monetary penalty



Termination



■ 2022
■ 2021

Weighing the impact of these consequence models, security professionals say they've seen good results.



said consequences had increased end users' overall phishing awareness



think security is considered a top priority for their company



feel employees think security is a top priority at work



report feeling positive about the security culture at their org

On the other hand, employees take a less positive outlook:



complain about the consequence model



said cybersecurity is not a top priority of theirs at work



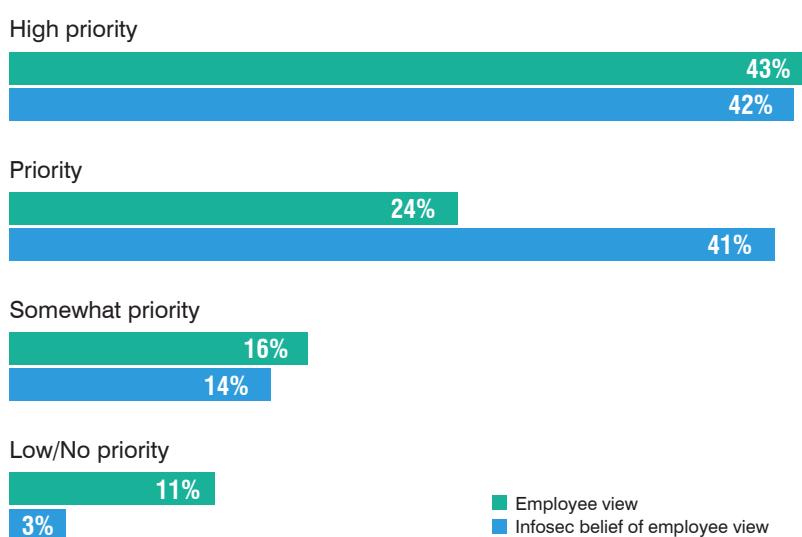
don't feel confident that their IT team will handle cybersecurity incidents



don't think company's security tools will block all dangerous emails

The data shows an obvious discrepancy in perception between security teams and end users, which possibly hints at lack of two-way communication. To build a strong, sustainable security culture, security teams need to do more than just measure how people respond to real and simulated threats. They also must understand how employees feel about the company's security culture and their place within it.

Tangled View of Cybersecurity Priority



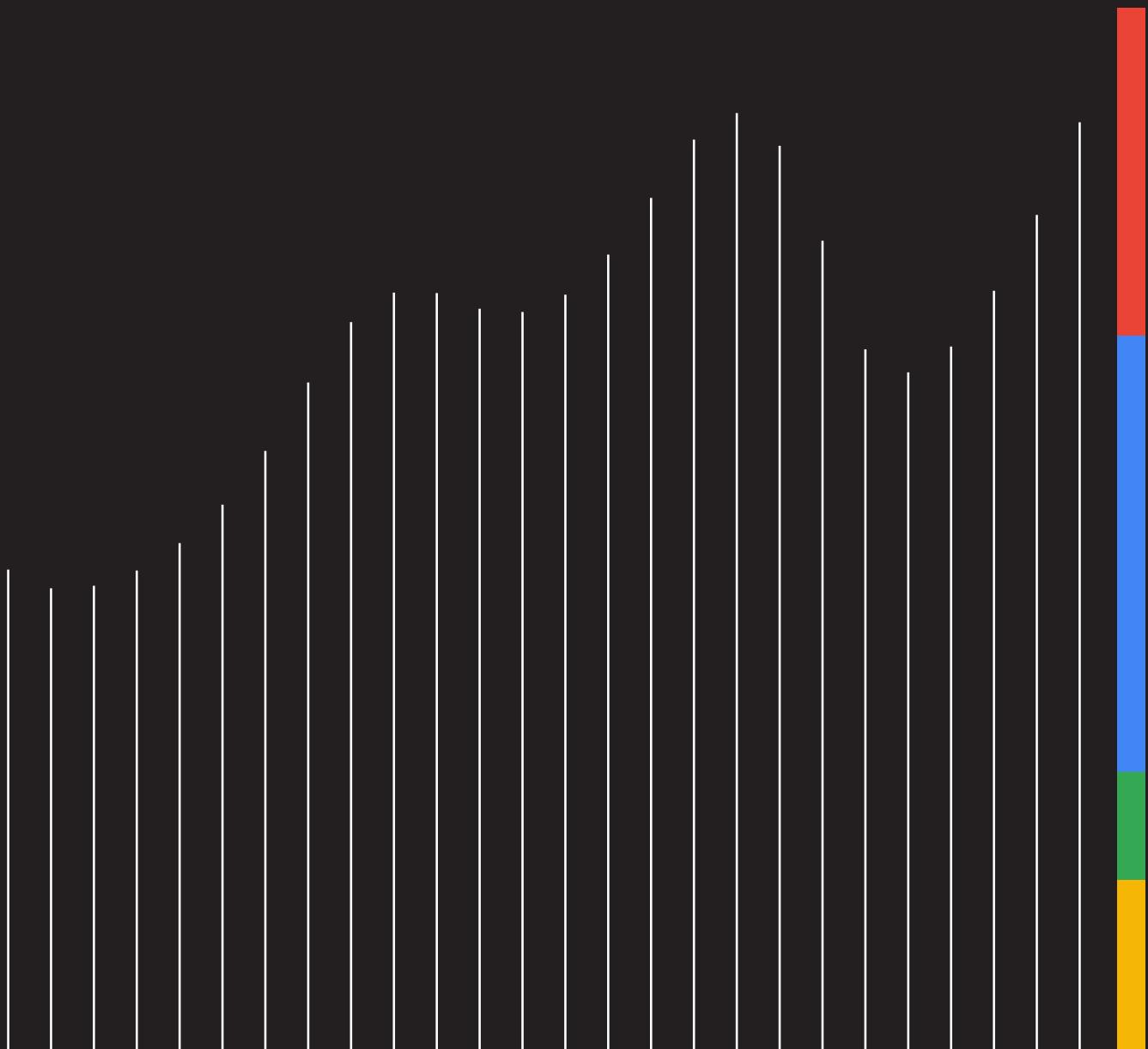
Taken together, the conflicting views of employees and security teams suggest that security culture is at a crossroads. But there is a way forward. With the right training and threat intelligence, employees can learn to understand the threat landscape and the dangers it poses. With a fair and thoughtful consequence and reward model in place, security teams can encourage and direct employees to embody the right security behaviors. And with strong executive sponsorship, company culture can reinforce the importance of protecting people and defending data.



Google Cloud Security

M-Trends

2024 Special Report



Global Trends

Special Report: Mandiant M-Trends 2024

6

The metrics reported in M-Trends 2024 are based on Mandiant Consulting investigations of targeted attack activity conducted between January 1, 2023 and December 31, 2023.

Internal detection is when an organization independently discovers it has been compromised, such as through an internal security appliance alert or internal personnel notification of suspicious activity.

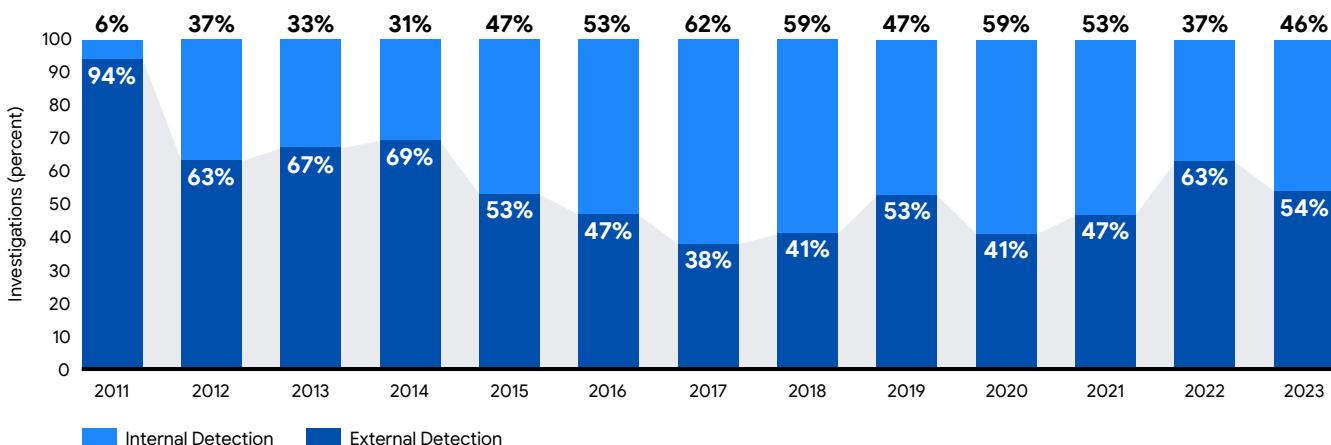
External notification is when an outside entity, such as law enforcement agencies, cybersecurity companies, or industry partners, informs an organization it has been compromised. In some cases, attackers will perform this notification, such as through a ransom note.

Detection by Source

In 2023, more than half of compromised organizations (54%) first learned of a compromise from an external source, while 46% first identified evidence of a compromise internally. However, separating out ransomware-related intrusions reveals that it was much more common for an organization to learn of a ransomware-related incident from an external source. For ransomware-related intrusions, 70% of organizations were externally notified, in most cases, via a ransom demand from the attacker. For intrusions that were not linked to ransomware, the ratio of internal versus external discovery was even, 50% to 50%. Of the internally discovered intrusions, 85% did not involve ransomware.

The percentage of externally notified intrusions decreased from 63% in 2022 to 54% in 2023. Mandiant also responded to more ransomware-related intrusions in 2023 than in 2022. Ransomware events are most often discovered through external means. Despite this, Mandiant observed a nine point drop in external notifications. This year-over-year shift, along with the high proportion of internally discovered compromises in cases other than ransomware, suggests that organizations are experiencing higher rates of success in detecting malicious behavior on their networks.

Detection by Source, 2011-2023

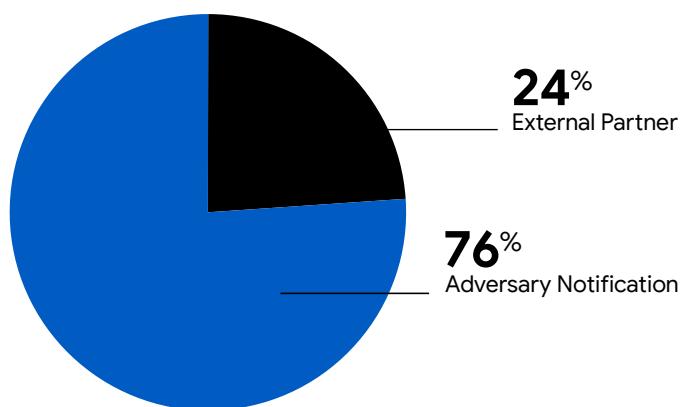


A ransomware-related intrusion provides access for or is associated with an attacker that has the primary goal of encrypting data, with the intention of extracting payment from the target in order to avoid further harm or to undo the malicious action.

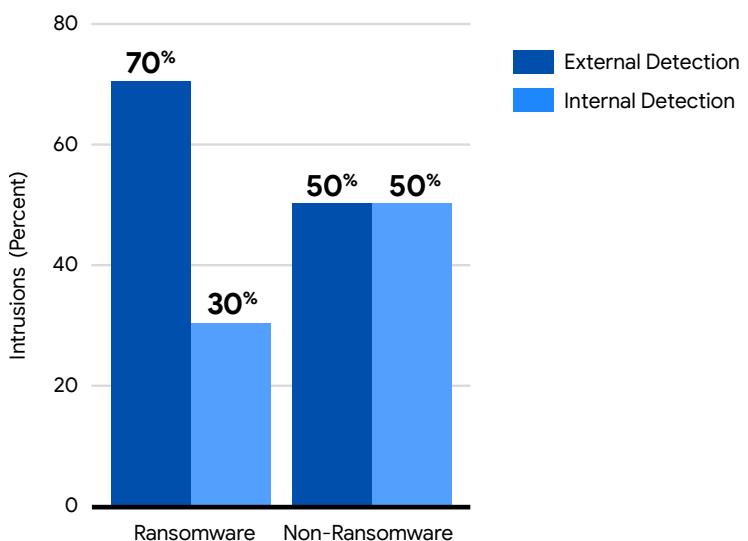
Ransomware-Related Intrusions

In 70% of cases, organizations learned of ransomware-related intrusions from external sources. Organizations were notified of a ransomware incident by an attacker ransom note in three fourths of those intrusions. This is consistent with the extortion business model in which attackers intentionally and abruptly notify organizations of a ransomware intrusion and demand payment. The remaining quarter of external notifications for ransomware intrusions came from external partners, such as law enforcement or security companies. In 2022, attacker notifications represented two thirds of external notifications for ransomware intrusions, compared to one third coming from external partners.

Ransomware External Notification Source, 2023



Detection by Source, 2023



Dwell time is calculated as the number of days an attacker is present in a compromised environment before they are detected. The median represents a value at the midpoint of a dataset sorted by magnitude.

Change in Median Dwell Time

16
days in 2022



10
days in 2023

Dwell Time

Global median dwell time continued a downward trend marking another notable shortest time period between initial intrusion and detection for all M-Trends reporting periods. In 2023, most organizations detected intrusions within 10 days of the initial intrusion. This is a decline of nearly one week compared to 16 days in 2022.

Mandiant defenders observed notable improvements in global median dwell time in 2023 across all notification sources. With the shortest periods across the board, global median dwell time for external notification sources decreased to 13 days in 2023 from 19 days in 2022. This likely indicates improved communication between organizations targeted and external parties making notifications. Another likely explanation for this decrease could be the increase of ransomware-related adversary notifications.

Maintaining the ongoing trend, when defenders detect adversary intrusions internally, they do so faster than the overall median dwell time. The global median dwell time for intrusions detected internally was nine days in 2023, down from 13 days in 2022 and from 18 days in 2021.

Global Median Dwell Time, 2011-2023

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
All	416	243	229	205	146	99	101	78	56	24	21	16	10
External	—	—	—	—	320	107	186	184	141	73	28	19	13
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9

Global Dwell Time Distribution

Dwell time distribution measures the percentage of Mandiant-investigated intrusions with a specific range of dwell time. In 2023, Mandiant experts continued to see intrusions detected earlier, with 43% of intrusions being detected in one week or less. Nearly two thirds of all intrusions in 2023 were detected within 30 days. This likely indicates that detection capabilities continue to improve across organizations, allowing defenders to be notified of threats during the initial infection or reconnaissance phases of the targeted attack lifecycle, similar to previous M-Trends reports.

Mandiant observed a decrease in intrusions that remain undiscovered for long periods of time compared to previous years. In 2023, 6% of investigations identified activity that remained undetected for between 1 and 5 years, compared to 11% in 2022 and higher percentages prior to 2020. Although organizations are still facing intrusions that go undetected for longer periods of time, defenders will likely see the distribution of dwell time move to the left as external parties, such as security vendors and law enforcement, increase their involvement and pace of notifications. However, detection capabilities and continuous hunting throughout environments have been effective at unearthing long-standing intrusions. As actionable information is shared, detection capabilities will continue to improve.

Broadly, the long-term trends of declining median dwell time and increasing rates of internal discovery of compromises indicate that organizations have made meaningful, measurable improvements in their defensive capabilities.

Global Dwell Time Distribution, 2018–2023

	1 week or less	30 days or less	6 months or less	1 year or less	5 years or less	5 years or more
2018	15.0%	16.0%	36.0%	13.0%	18.0%	1.1%
2019	22.2%	18.5%	29.2%	9.3%	18.5%	2.3%
2020	35.3%	17.2%	26.7%	6.6%	13.0%	1.2%
2021	37.4%	17.7%	26.2%	10.7%	7.8%	0.3%
2022	42.0%	16.0%	24.0%	7.0%	11.0%	0.0%
2023	43.3%	22.7%	22.3%	5.4%	6.0%	0.2%

Change in Global Investigations Involving Ransomware

18%  **23%**
in 2022 in 2023

Change in Global Dwell Time—Ransomware

9  **5**
days in 2022 days in 2023

Change in Global Dwell Time—Non-Ransomware

17  **13**
days in 2022 days in 2023

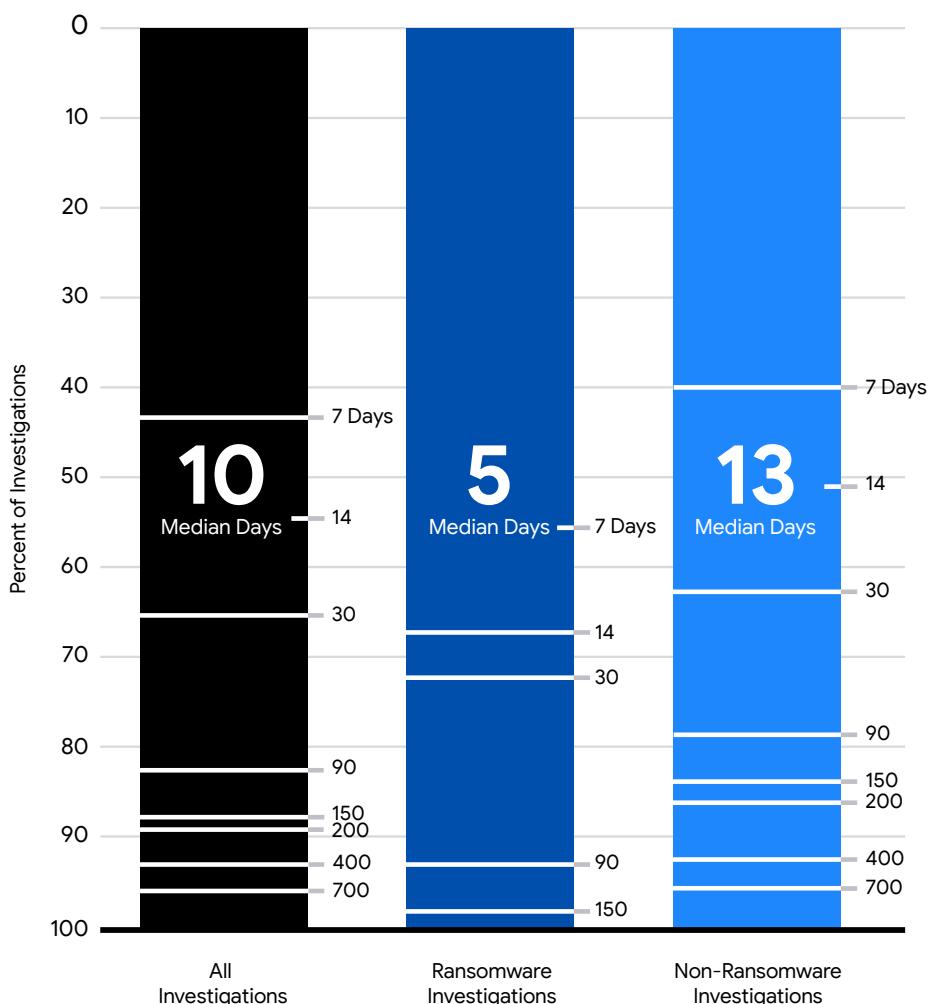
Investigations Involving Ransomware

In 2023, global investigations involving ransomware increased five percentage points to 23% of investigations in 2023 compared to 18% in 2022. This brings the percentage of ransomware-related intrusions back to where it was previously in 2021.

Globally, organizations detected ransomware or received a ransom demand faster in 2023—in five days compared to nine days in 2022—regardless of notification source. Non-ransomware-related intrusions were detected in 13 days, compared to 17 days in 2022.

Intrusions involving ransomware were detected in six days when the notification came from an internal source, compared to 12 days in 2022. Defenders were notified of ransomware-related intrusions from an external party in five days in 2023, two days quicker than what was observed in 2022.

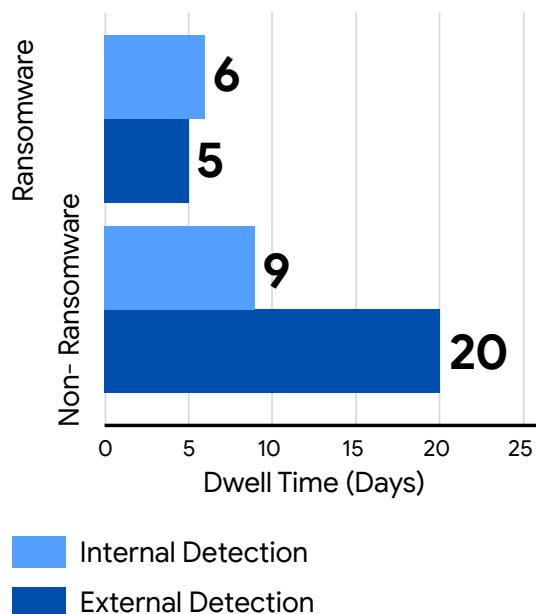
Global Dwell Time by Investigation Type, 2023



Ransomware attacks have continued to be a driving factor in reducing dwell time over the years. However, in 2023, Mandiant experts observed notable improvements in decreased dwell time across all notification sources and investigation types.

Intrusions that did not involve ransomware were identified in a shorter period of time in 2023. Notably, intrusions that occurred in 2023 were identified internally in little over a week, with nine days between initial intrusion and detection, compared to 13 days in 2022. Organizations were notified by an external party of an intrusion one week faster in 2023, resulting in a 20-day median dwell time for externally notified, non-ransomware-related intrusions, compared to 27 days in 2022.

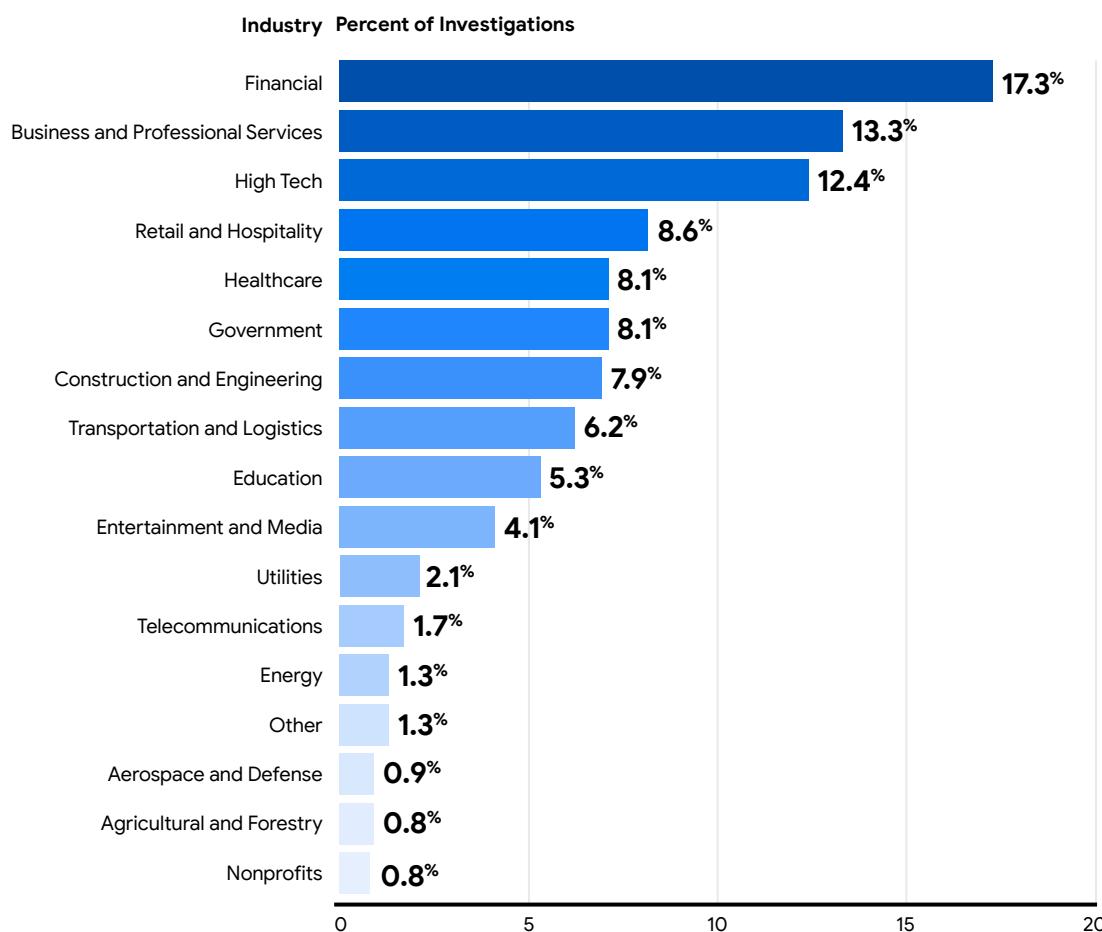
Global Median Dwell Time by Detection Source



Industry Targeting

In 2023, Mandiant most frequently responded to intrusions at financial services organizations, followed by business and professional services, high tech, retail and hospitality, and healthcare. All of these sectors have access to a variety of sensitive information, including proprietary business information, personally identifiable information (PII), protected health information (PHI), and financial data. Attackers have also abused service providers and technology organizations to facilitate third-party compromises or to obtain access to data or networks belonging to many organizations through a single compromise. Mandiant consistently finds these sectors toward the top of the list for share of investigations. Government sector investigations declined from first to tied for fifth with healthcare in 2023, potentially reflecting fewer new investigations related to the war in Ukraine compared to 2022.

Global Industries Targeted, 2023



Targeted Attacks

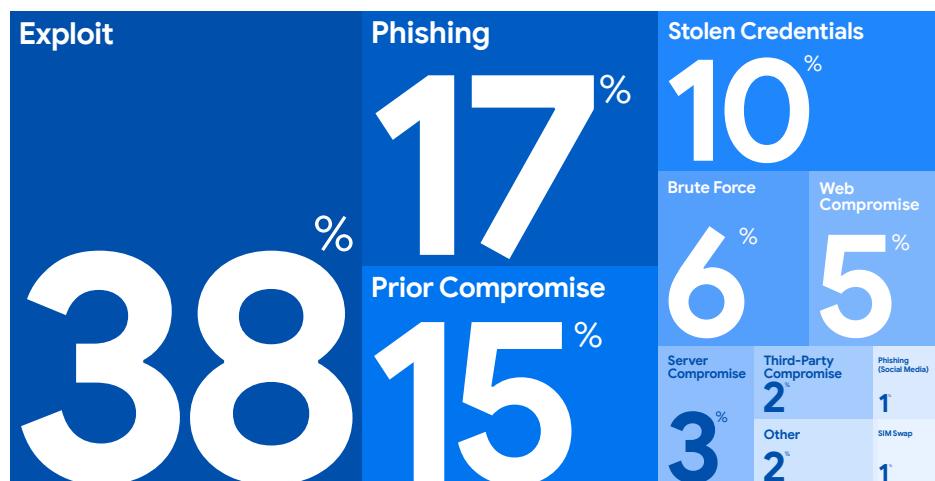
Initial Infection Vector

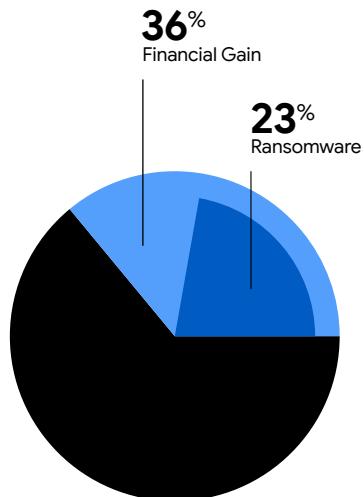
In 2023, Mandiant experts once again saw exploits used as the most prevalent adversary initial infection vector. In intrusions where the initial intrusion vector was identified, 38% of intrusions started with an exploit. This is a six percentage point increase from 2022, consistent with what defenders faced in 2021. For more information, please see “Attacker Operations Involving Zero-Days Vary Depending on Motivation”.

Phishing remained the second most common intrusion vector. However it declined in 2023, with 17% of intrusions, compared to 22% in 2022. Phishing remains an effective method to establish an initial foothold and a popular threat vector for adversaries. Full analysis can be found in “Evolution of Phishing Among Shifting Security Controls”.

Prior compromises were the third most significant intrusion vector used by attackers in 2023. Mandiant investigators noted a three percentage point increase in 2023 compared to what was observed in 2022 with 15% of intrusions beginning with access provided by a prior compromise. This increase is likely related to the ransomware ecosystem and the continued partnership between ransomware affiliates and various malware operators selling initial access.

Initial Infection Vector (When Identified)





Post-Compromise Activity

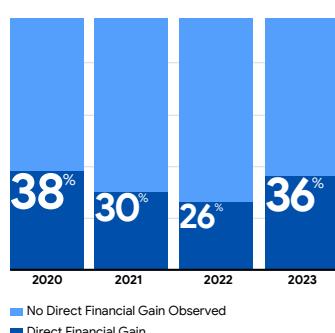
Financial Gain

The proportion of intrusions Mandiant responded to that served financially motivated objectives increased from more than a quarter of all investigations, 26%, in 2022 to more than a third, 36%, in 2023. Ransomware-related intrusions represented almost two thirds of financially motivated intrusions and 23% of all 2023 intrusions.

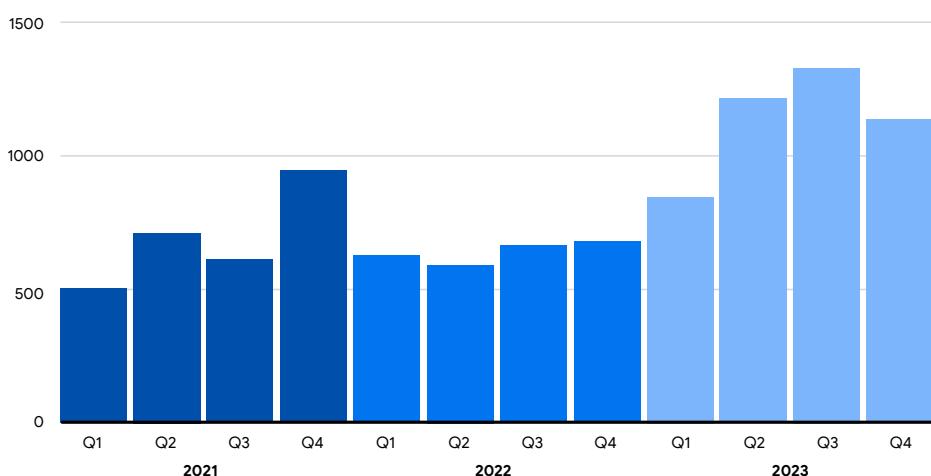
The remaining financially motivated intrusions included data theft extortion without ransomware encryption, attackers establishing initial access to facilitate other operations, business email compromise (BEC) fraud, and cryptocurrency theft events. Mandiant attributed several financially motivated intrusions to likely North Korean⁶ state-sponsored attackers, including cryptocurrency theft and IT worker wage theft. Mandiant continues to track North Korean threat groups that conduct financially motivated activity to cover both operational costs as well as larger scale activity intended to generate revenue for the state.⁷

The upward trend in ransomware and other extortion-related investigations in 2023 is consistent with Mandiant and open-source observations of a marked increase in listings on data leak sites (DLS) and extortion revenue estimates.⁸ DLS are websites where the illicitly retrieved data of companies that refuse to pay a ransom are published. While this data is skewed toward targets who refused to pay attackers' ransom demands, it is still useful for understanding broad trends in extortion operations. The FIN11 MOVEit exploitation campaign and UNC3944⁹ activity described in the Evolution of Phishing section showcase the prevalence of extortion intrusions without ransomware encryption.

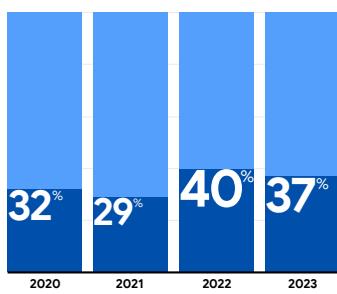
Financial Gain, 2020-2023



Count of DLS Listings per Quarter, 2021-2023

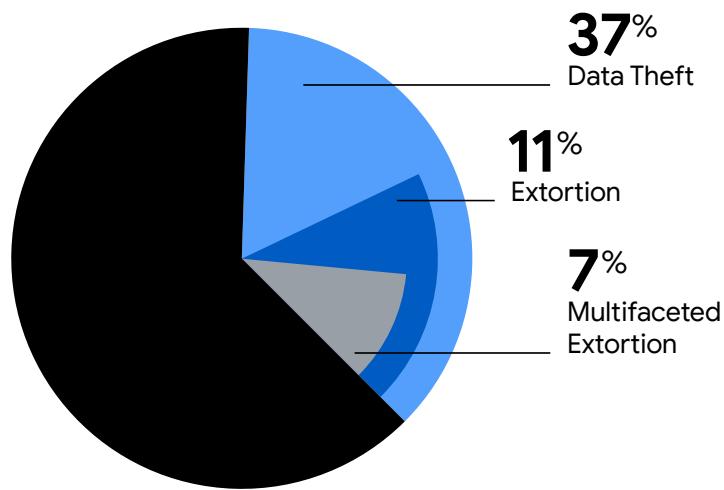


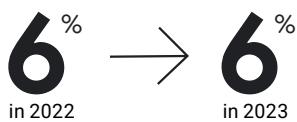
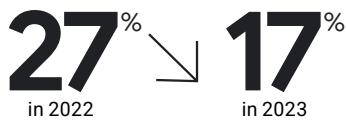
Data Theft, 2020-2023



Data Theft

Mandiant identified data theft in 37% of 2023 intrusions, which is slightly lower than the 40% of intrusions reported in 2022. In 11% of intrusions, attackers directly monetized stolen data through extortion. In an additional 7%, they used a combination of data theft, ransomware, and extortion, also known as multifaceted extortion. Mandiant also observed attackers steal credentials and other data likely to facilitate reconnaissance of target networks. Several cases involved large-scale data theft that included intellectual property. Mandiant also identified instances of targeted or selective data theft by groups such as the Russian cyber espionage group APT29¹⁰ and the suspected Chinese cyber espionage cluster UNC4841.¹¹



Compromised Architecture**Multiple Threat Groups Identified (per environment)****Environment**

In 2023, Mandiant experts continued to observe attackers use compromised architecture to conduct email spam, distribute botnets, and perform some types of cryptomining activity. During the past three years, intrusions related to compromised architecture have been heavily automated following the mass exploitation of vulnerabilities. Publicly released proof-of-concept (PoC) code for new exploits increases the ease of automating attacks, accelerating the attack cycle for adversaries abusing compromised infrastructure. Publicly available PoC code for vulnerabilities makes it simple for attackers to automate their exploits using scanning tools.

In 2023, Mandiant noted a decrease in the number of investigations that identified multiple threat groups in a single environment. In 17% of investigations, Mandiant experts uncovered more than one threat group operating in the target environment. This likely is related to the volume of targeted zero-days that Mandiant investigated. The 10 percentage point decrease from 2022 (27%) suggests a positive trend, potentially resulting from defenders' efforts to limit the ability of additional attackers to infiltrate environments.

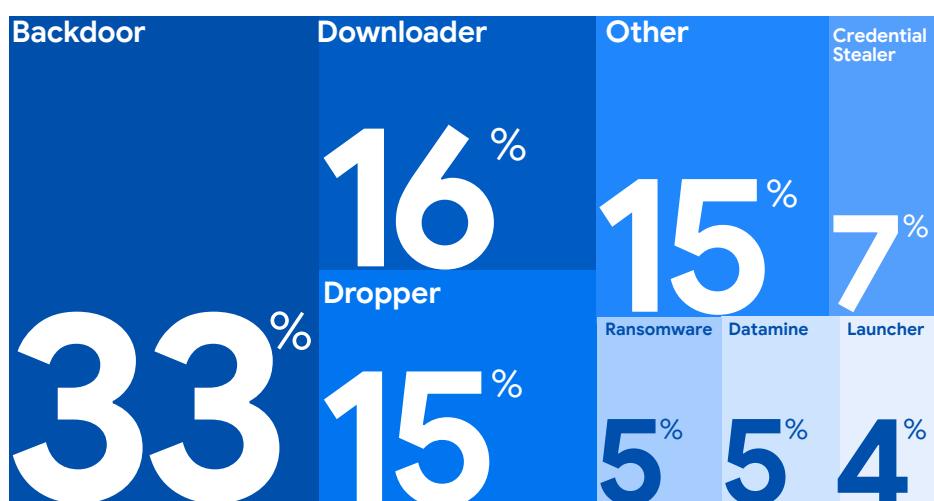
A malware category

describes a malware family's primary purpose. Each malware family is assigned only one category that best describes its primary purpose, regardless of functionality for more than one category.

New Malware Families by Category

The top five malware categories have remained relatively consistent year over year. Of the 626 newly tracked malware families, the top five categories include backdoors (33%), downloaders (16%), droppers (15%), credential stealers (7%), and ransomware (5%). Newly tracked credential stealers return to the top five categories in 2023 after a brief hiatus observed in 2022. Another notable change in rankings is the decrease in newly tracked ransomware families, from 7% of malware families to 5% of newly tracked families in 2023. Although Mandiant responded to a similar proportion of ransomware intrusions in 2023 as in 2021, the decline in net new ransomware families may reflect the prevalence of ransomware strains that existed prior to 2023, such as LOCKBIT, ALPHV, BASTA, and ROYALLOCKER.

Newly Tracked Malware Families by Category, 2023



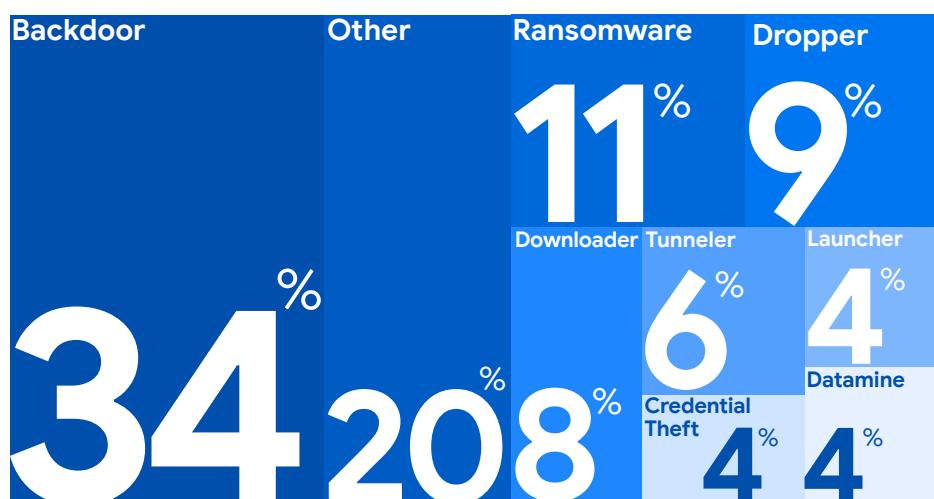
An observed malware family is a malware family identified during an investigation by Mandiant experts.

Observed Malware Families by Category

Observed malware family categories were also relatively consistent with the findings from previous years. Mandiant experts observed 277 malware families during investigations conducted in 2023. Backdoors remain the favorite among attackers, making up 34% of the observed malware dataset. This is up one percentage point from 2022. The remaining observed malware family categories show ransomware (11%), droppers (9%), downloaders (9%), and tunnelers (6%) rounding out the top five.

Mandiant continues to see a rise in attacker use of remote administration tools and other utilities to conduct their operations, noted in the continued increase in the “Other” category year over year. Of the 20% of malware families in this category, 8% represent legitimate utilities or remote administration tools. While not inherently malicious, attackers often leverage these tools in intrusions to evade detection, demonstrating their continued resourcefulness. To remain undetected and carry out further operations, attackers use living-off-the-land (LotL) techniques by employing system tools that are already in the environment or they abuse remote administrator tools that are less likely to be flagged by default in security technologies like Endpoint Detection and Response tooling.

Observed Malware Families by Category, 2023



**Observed Malware Families
2022 to 2023**

Backdoor

33% ↗ **34%**

Downloader

10% ↓ **8%**

Dropper

9% → **9%**

Launcher

5% ↓ **4%**

Tunneler

5% ↗ **6%**

Ransomware

10% ↗ **11%**

Other

28% ↓ **20%**

Malware Category	Primary Purpose
Backdoor	A program whose primary purpose is to allow an attacker to issue interactive commands to the system on which it is installed.
Credential Stealer	A utility whose primary purpose is to access, copy, or steal authentication credentials.
Datamine	A utility whose primary purpose is to gather data, typically for theft. Excludes utilities that gather data such as credentials used for the purpose of escalating privileges or information used for system or network reconnaissance.
Downloader	A program whose sole purpose is to download (and perhaps launch) a file from a specified address and which does not provide any additional functionality or support any other interactive commands.
Dropper	A program whose primary purpose is to extract, install, and potentially launch or execute one or more files.
Launcher	A program whose primary purpose is to launch one or more files. Differs from a dropper or an installer in that it does not contain or configure the file, but merely executes or loads it.
Ransomware	A program whose primary purpose is to perform some malicious action (such as encrypting data) with the goal of extracting payment from the target in order to avoid or undo the malicious action.
Tunneler	A program that proxies or tunnels network traffic.
Other	Includes other categories, such as utilities, remote admin technologies, keyloggers, and point of sale.

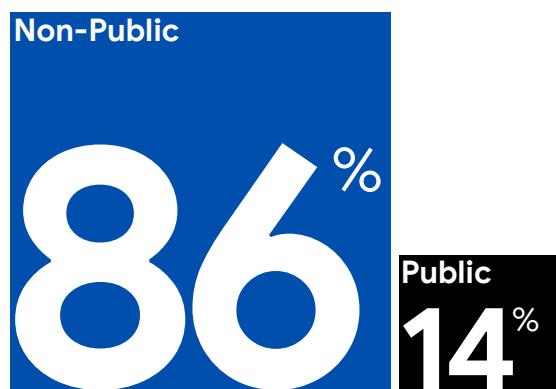
A publicly available tool or malware family is readily obtainable without restriction. This includes tools that are freely available on the internet as well as tools that are sold or purchased, as long as they can be purchased by any buyer.

A non-public tool or malware family is, to the best of our knowledge, not publicly available (either for free or for sale). They may include tools that are privately developed, held or used, as well as tools that are shared among or sold to a restricted set of customers.

Malware by Availability

Malware family availability for both newly tracked and observed malware families remains more heavily weighted toward non-public in 2023, similar to previous M-Trends reporting. In both categories, malware families are more often privately developed or have restricted availability. Adversaries traditionally use a variety of non-public malware to conduct their operations. However, the share of publicly available malware families observed in investigations has increased by one percentage point from 2021 to 2022 and again from 2022 to 2023 to arrive at 30%. The increased use of publicly available malware likely reflects the rise in financially motivated attackers who prioritize speed and efficiency over long-term stealth.

Newly Tracked Malware Families by Availability, 2023



Observed Malware Families by Availability, 2023

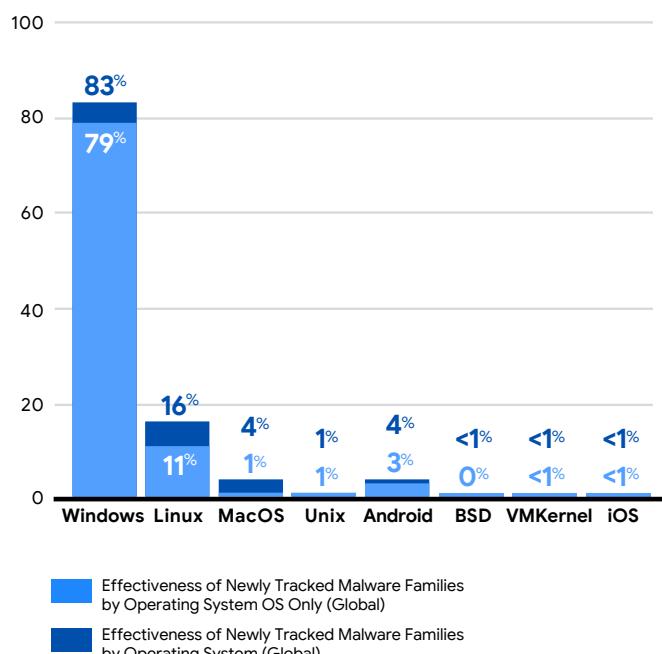


The operating system effectiveness of a malware family is the operating system(s) that the malware can be used against.

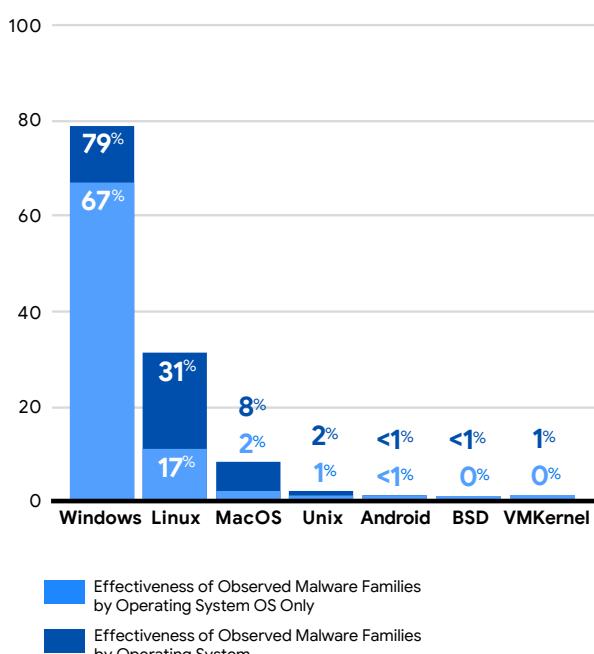
Operating System Effectiveness

In 2023, Mandiant noted a slight increase in newly tracked malware effective on Linux systems at 16%, compared to 12% in 2022. Notably, observed malware effective on Linux has increased to 31% of all malware observed in 2023, compared to 15% in 2022. Similar to previous M-Trends reporting periods, most newly tracked and observed malware families still remain effective on Windows. The apparent decline in the percentage of Windows-related malware from 2022 to 2023 likely reflects the greater share of Linux-related malware rather than a true decline in malware effective on Windows.

Operating System Effectiveness of Newly Tracked Malware Families, 2023



Operating System Effectiveness of Observed Malware Families, 2023



Regional Trends

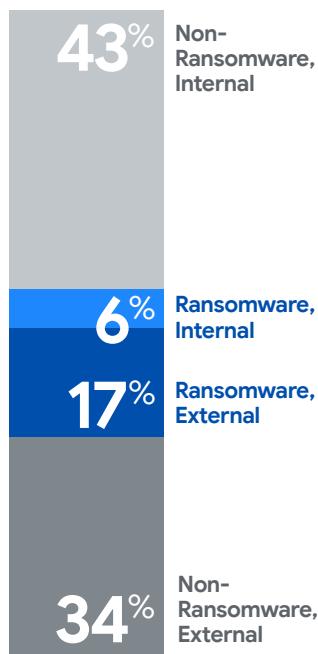
Special Report: Mandiant M-Trends 2024

34

Americas

The metrics reported in this section are based on Mandiant Consulting investigations affecting organizations that are located in North, Central, or South America.

Detection by Source—Americas, 2023

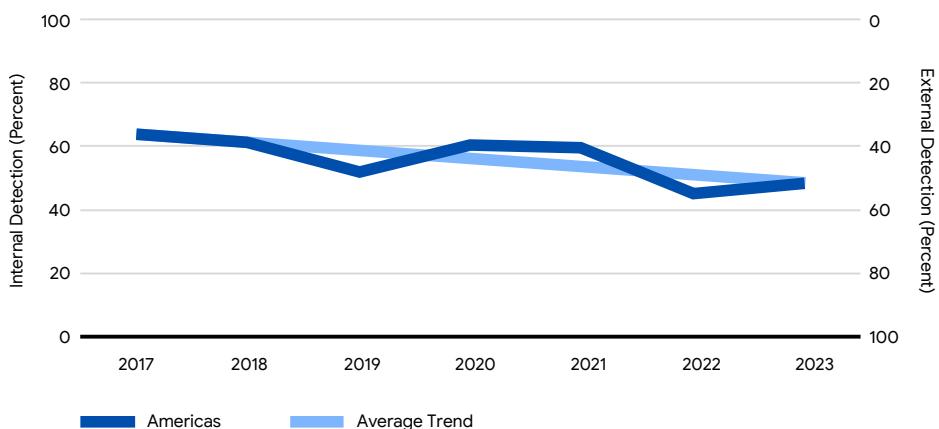


Detection by Source

In the Americas in 2023, 51% of organizations first learned of a compromise from an external source, while 49% identified evidence of a compromise internally. This split appears to be consistent with a long-term global trend toward a balance of internal versus external discovery. This is also consistent with observations in the Americas from 2022, continuing a trend toward higher rates of external notifications overall compared to 2017–2021. Growth in ransomware-related intrusions over the last four years has likely contributed to this shift in notification source.

Isolating ransomware-related intrusions from all other compromises exposes a strong divergence in notification sources in ransomware versus non-ransomware-related intrusions. Approximately two thirds of ransomware-related intrusions in the Americas were externally notified—most frequently by the attackers themselves in the form of a ransom note. In contrast, organizations in the region first discovered evidence of a compromise internally in slightly more than half of cases that were not related to ransomware encryption events.

Detection by Source—Americas, 2017–2023



Dwell time is calculated as the number of days an attacker is present in a target environment before they are detected. The median represents a value at the midpoint of a dataset sorted by magnitude.

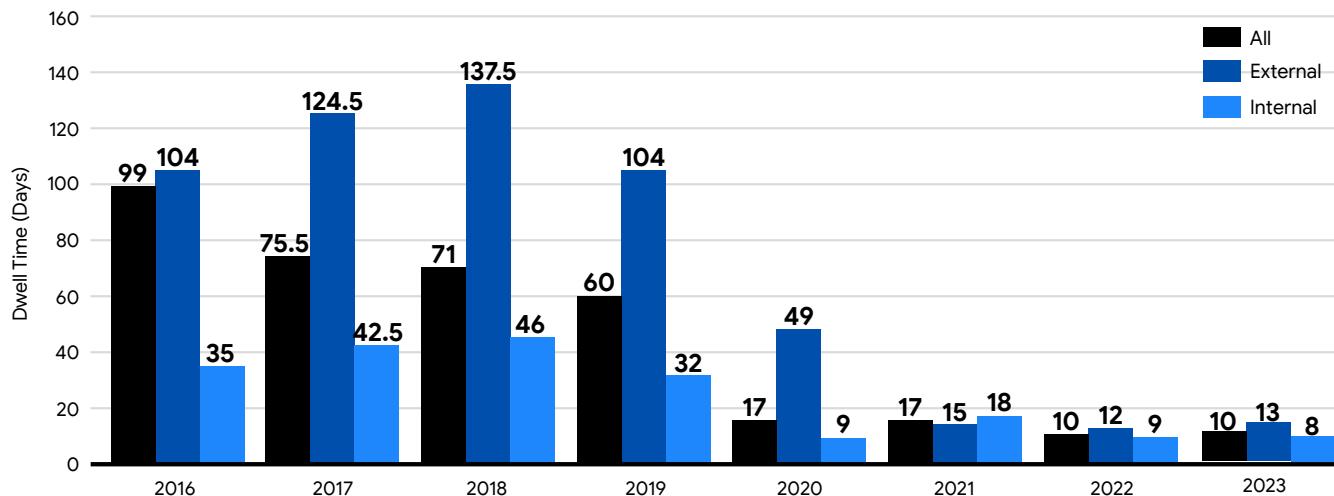
Americas Median Dwell Time

In 2023, organizations located in the Americas detected intrusions at the same pace as in 2022. Median dwell time in the Americas was 10 days. External parties notified these organizations of intrusions in 13 days, compared to 12 days in 2022. However, when intrusions were detected internally, organizations uncovered malicious activity in eight days in 2023 compared to nine days in the previous year.

Change in Americas Median Dwell Time

10 → 10
days in 2022 days in 2023

Americas Median Dwell Time, 2016-2023



Dwell Time Distribution

Organizations in the Americas region continue to improve their detection capabilities. Organizations detected 45% of intrusions in one week or less, a rate that is similar to that seen in 2022. In 68.5% of investigations conducted by Mandiant, defenders were made aware of intrusions in 30 days or less, a four percentage-point increase in investigations compared to 2022.

Consistent with trends seen globally, organizations continue to identify intrusions that had remained undetected for longer periods of time. Organizations located in the Americas region saw a small increase in intrusions detected in five years or less and a decrease in intrusions that were undetected for more than five years.

Americas Dwell Time Distribution, 2021-2023

	1 week or less	30 days or less	6 months or less	1 year or less	5 years or less	5 years or more
2021	38.8%	18.0%	28.2%	11.1%	3.6%	0.4%
2022	44.5%	19.4%	26.2%	4.5%	2.6%	2.8%
2023	45.0%	23.5%	22.3%	4.8%	4.2%	0.3%

Change in Americas Investigations Involving Ransomware

22% → **23%**
in 2022 in 2023

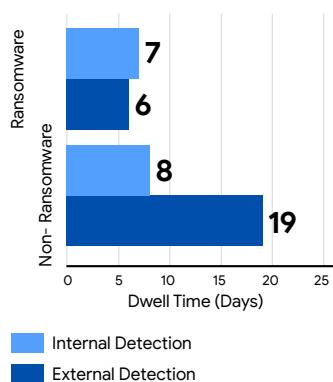
Change in Americas Median Dwell Time—Ransomware

5 days in 2022 → **6** days in 2023

Change in Americas Median Dwell Time—Non-Ransomware

12 days in 2022 → **12** days in 2023

Americas Median Dwell Time by Detection Source

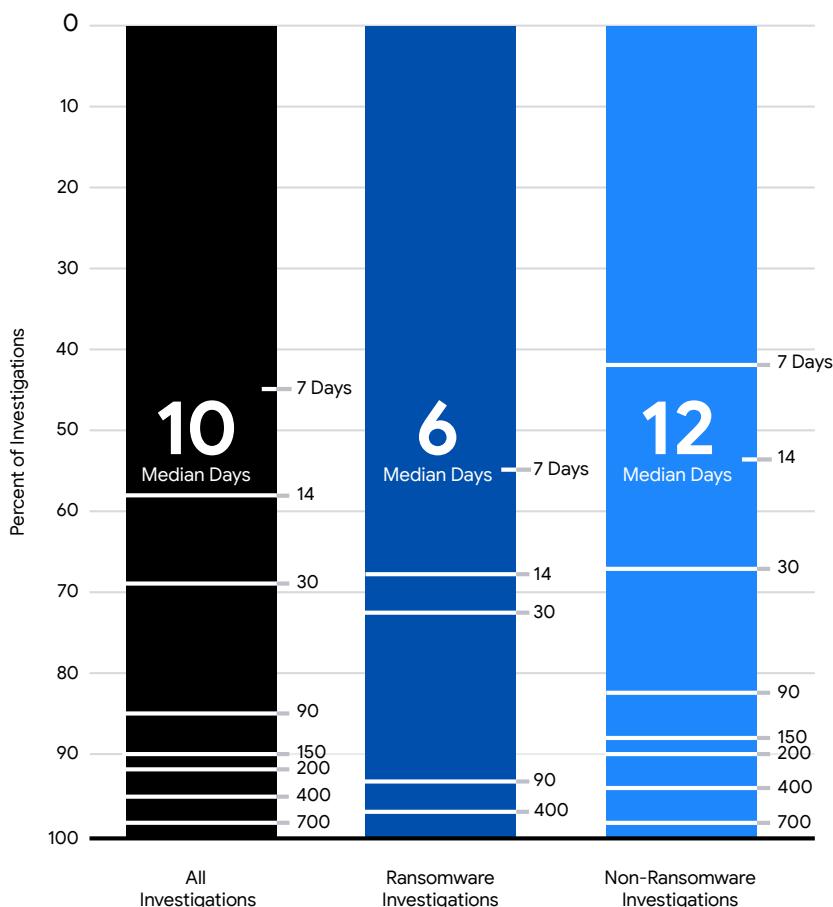


Investigations Involving Ransomware

Organizations located in the Americas detected overall intrusions related to ransomware in six days compared to five days seen in the previous M-Trends reporting period. This could be explained by the slight increase in investigations involving ransomware, or it could be a slight variation in the ransomware attackers' ability to conduct operations. In intrusions related to ransomware, targeted organizations detected malicious activity internally in seven days, compared to six days when an external party made organizations aware of an intrusion.

In intrusions that did not involve ransomware, internal detection remained the fastest way for organizations to be notified of an intrusion, with a dwell time of eight days. When they did not detect an intrusion internally, organizations in the Americas were notified of intrusions within a median of 19 days by an external party.

Americas Dwell Time by Investigation Type, 2023





Targeted Attacks

Initial Infection Vector

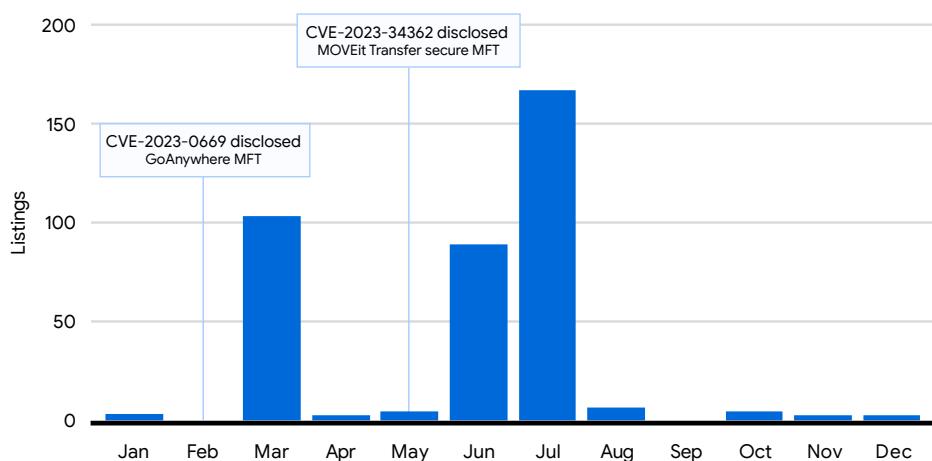
Organizations in the Americas faced threats similar to those experienced by organizations across the globe. In 41% of intrusions that had an initial infection vector identified, an exploit was the source of attacker activity in the region. Phishing was used as an initial vector in 18% of intrusions. Rounding out the top three, attackers leveraged prior compromised access gained from another threat group or malware in 14% of intrusions.

Threat Groups

Prevalent Threat Group Targeting Americas

The most frequently observed attacker in the Americas in 2023 was FIN11, a financially motivated threat group. The majority of FIN11 intrusions Mandiant investigated were related to the widespread campaign exploiting CVE-2023-34362 in the MOVEit Transfer secure managed file transfer (MFT) software.²¹ Mandiant also investigated intrusions in which FIN11 exploited CVE-2023-0669 in GoAnywhere MFT. Although FIN11 has deployed the CLOP ransomware in the past, in these campaigns the attacker focused on data theft extortion with no ransomware encryption. Counts of listings from the CLOP^_- LEAKS DLS corroborate Mandiant's investigative findings and demonstrate the scale FIN11 was able to achieve through these focused vulnerability exploitation campaigns.

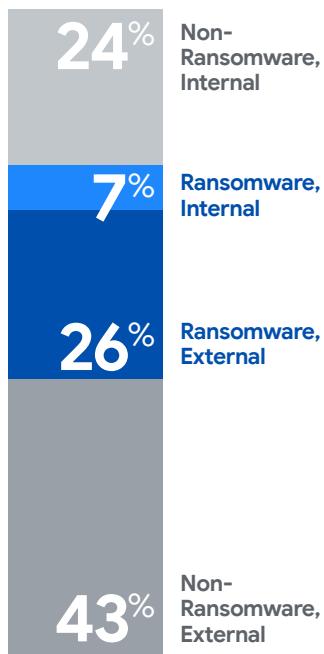
Listings Posted to CLOP^_- LEAKS DLS, 2023



JAPAC

The metrics reported in this section are based on Mandiant Consulting investigations affecting organizations in Japan and Asia Pacific (JAPAC).

Detection by Source— JAPAC, 2023

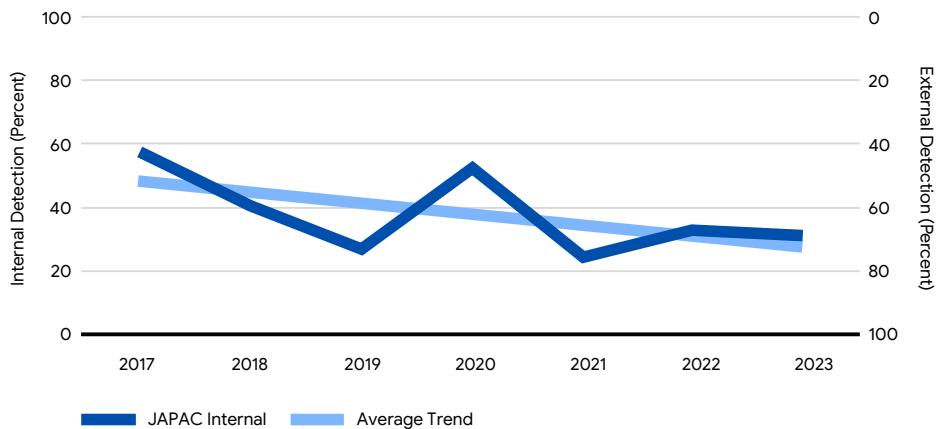


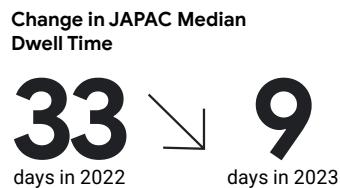
Detection by Source

For intrusions in the JAPAC region in 2023, organizations were notified of compromises from external sources in 69% of cases, while 31% of intrusions were discovered internally. This continues a long-term trend in JAPAC of internal detections representing a declining proportion of overall notification sources.

In line with global numbers, organizations located in JAPAC were notified more often of intrusions via external notifications. In 2023 in JAPAC, organizations learned of ransomware-related infections from external sources in three fourths of cases.

Detection by Source—JAPAC, 2017-2023

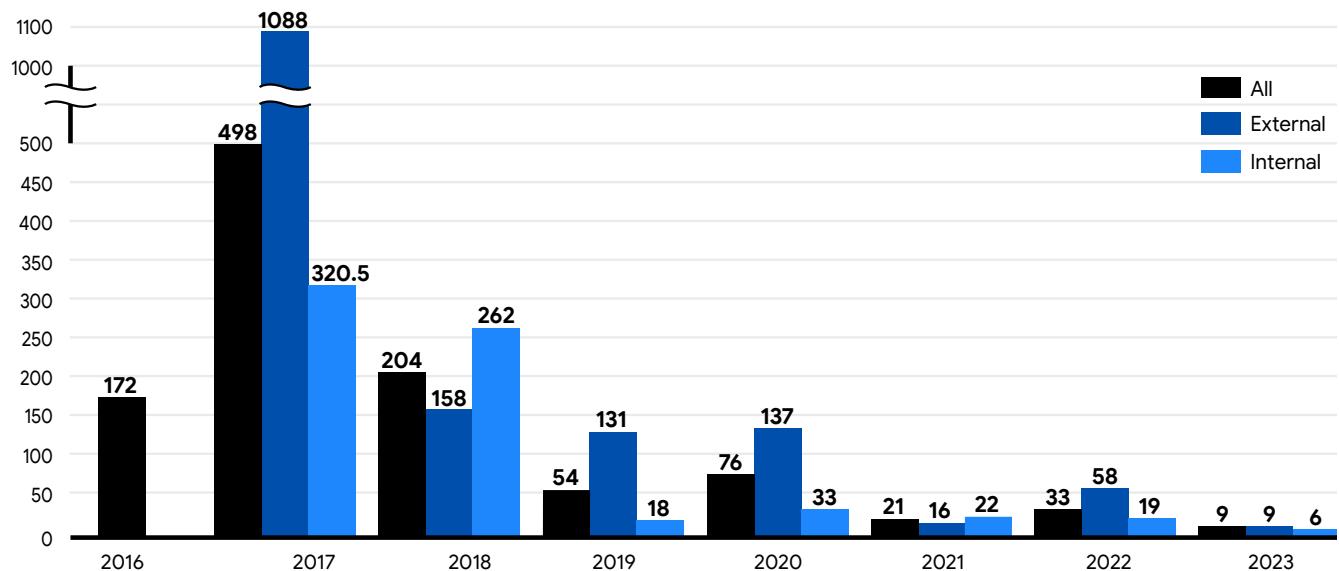




JAPAC Median Dwell Time

Organizations in the JAPAC region continued to detect intrusions more quickly year over year. This was true for both notification sources. Median dwell time in JAPAC achieved its quickest time of nine days from initial infection to detection, compared to 33 days in 2022. Organizations identified an intrusion internally in six days in JAPAC, compared to 19 days seen in 2022. Organizations received external notifications of malicious activity in nine days, just over one week, compared to nearly two months in 2022.

JAPAC Median Dwell Time, 2016-2023



Dwell Time Distribution

In 2023, targeted attacker activity was detected in 48% of intrusions in JAPAC in one week or less. Continuing with observations both globally and year over year in the region, the number of intrusions detected sooner continues to increase, showing the resilience of defenders. Over the past three years, Mandiant has seen fewer intrusions remain undetected for longer periods of time in the JAPAC region.

JAPAC Dwell Time Distribution, 2021-2023

	1 week or less	30 days or less	6 months or less	1 year or less	5 years or less	5 years or more
2021	36.4%	23.6%	20.0%	3.6%	3.6%	12.7%
2022	37.7%	11.7%	21.6%	8.4%	16.7%	5.0%
2023	48.1%	18.5%	20.4%	7.4%	5.6%	0.0%

Change in JAPAC Investigations Involving Ransomware

32% ↗ **33%**
in 2022 in 2023

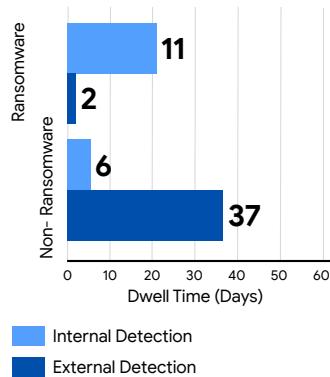
Change in JAPAC Median Dwell Time—Ransomware

19 days in 2022 ↘ **3** days in 2023

Change in JAPAC Dwell Time—Non-Ransomware

60 days in 2022 ↘ **26** days in 2023

JAPAC Median Dwell Time by Detection Source

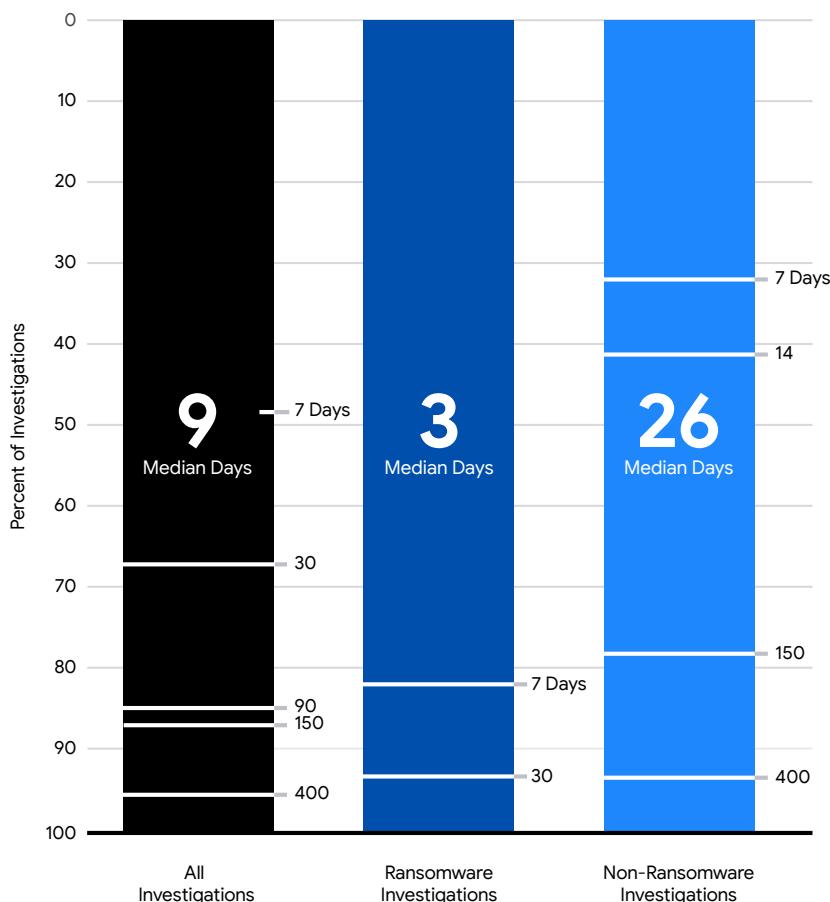


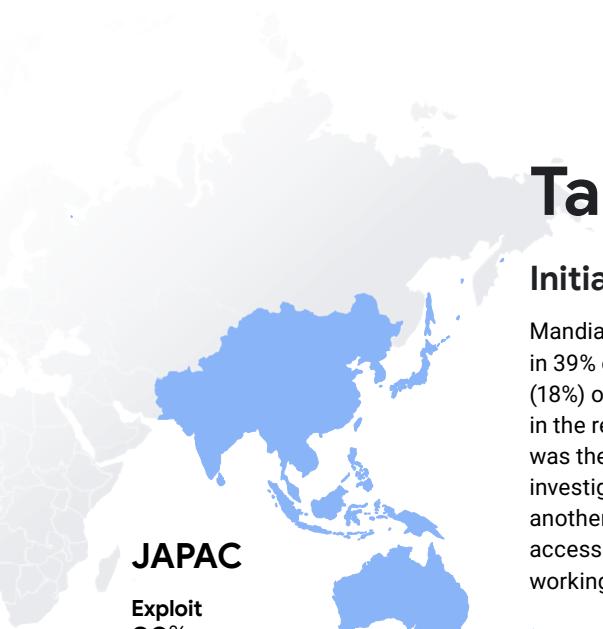
Investigations Involving Ransomware

JAPAC saw little movement in the volume of ransomware-related intrusions, with a small increase to 33% of investigations conducted in the region in 2023. However, dwell time for ransomware-related intrusions declined to three days compared to 19 days in 2022. This sharp decrease is likely a cause of the quick moving ransomware families used in intrusions over the years. Mandiant has observed ransomware-related intrusions balance speed and thoroughness of compromise. Attackers who deploy ransomware want to move fast enough to reduce the chance of detection, but also be meticulous enough to ensure potential damage that is sufficient to increase the likelihood of maximum ransom payment.

Organizations detected non-ransomware-related intrusions quicker in 2023 in slightly more than half the time observed in 2022. The median dwell time in the JAPAC region for non-ransomware-related intrusions was 26 days in 2023. Organizations were notified of an intrusion in six days by an internal security product or team member. Externally, however, organizations were notified of an intrusion 37 days after the malicious activity initially began.

JAPAC Dwell Time by Investigation Type, 2023





Targeted Attacks

Initial Infection Vector

Mandiant investigators identified that organizations in JAPAC were impacted by exploits in 39% of investigations when an initial infection vector was identified. In nearly a fifth (18%) of investigations, attackers leveraged brute-force techniques to gain initial access in the region. Rounding out the top three most seen initial infection vectors in the region was the use of access obtained by a prior compromise. In 15% of intrusions, Mandiant investigators identified evidence that an attacker leveraged access originally obtained by another attacker through either purchased access or by leveraging unsecured backdoor access. The increase in prior compromise usage is likely representative of the inner workings of the criminal ransomware ecosystem.

Threat Groups

Prevalent Threat Group Targeting JAPAC

In the Japan and Asia Pacific region in 2023, Mandiant investigators most often encountered suspected Chinese cyber espionage cluster UNC4841.

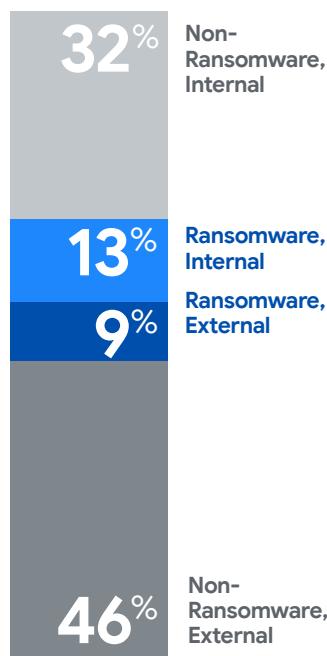
Beginning in at least October 2022, UNC4841 exploited a zero-day vulnerability, CVE-2023-2868, in Barracuda Email Security Gateway (ESG) appliances in a campaign targeting public and private organizations worldwide.²² In several cases, Mandiant observed evidence of UNC4841 searching for and exfiltrating data relevant to Chinese political or strategic interests. In the set of entities that UNC4841 selected for focused data theft, Mandiant uncovered shell scripts that targeted email domains and users from Ministries of Foreign Affairs of ASEAN member nations as well as individuals within foreign trade offices and academic research organizations in Taiwan and Hong Kong.

In this campaign, UNC4841 took a number of steps to disguise its activity. For example, it inserted malware in or used the names of legitimate Barracuda modules and phishing messages that were designed to be intercepted by spam filters and avoid further investigation by security teams. Notably, after the initial vulnerability disclosure and remediation efforts, UNC4841 responded aggressively, rapidly altering its malware, deploying additional persistence mechanisms, and moving laterally to maintain access to target environments. Further analysis on this can be found in Attacker Operations Involving Zero-Days Vary Depending on Motivation.

EMEA

The metrics reported in this section are based on Mandiant Consulting investigations affecting organizations in Europe, the Middle East, and Africa (EMEA).

Detection by Source—EMEA, 2023

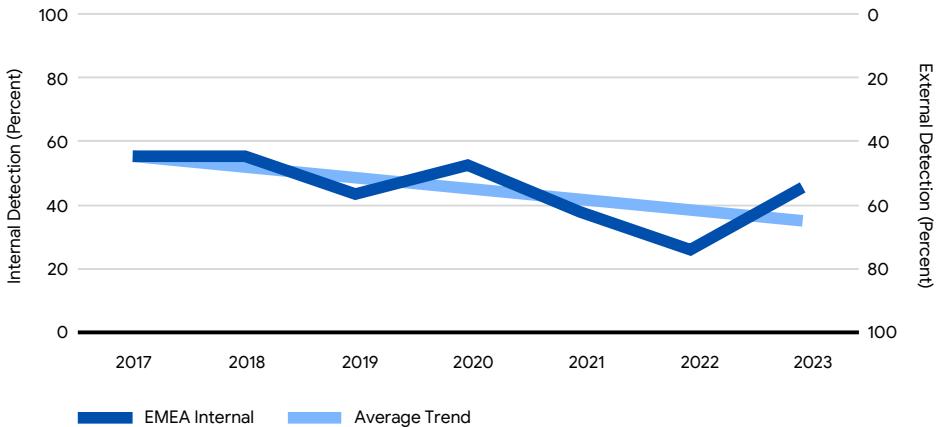


Detection by Source

In cases Mandiant investigated in 2023 in EMEA, organizations first discovered evidence of a compromise internally 46% of the time, while organizations were externally notified of compromises in 54% of intrusions. This split matches global numbers for 2023 and reverses a long-term trend toward declining rates of internal notifications for the region.

Organizations in EMEA identified ransomware-related intrusions internally slightly more frequently than through external notifications such as a ransom note. The majority of non-ransomware-related intrusions were identified by external security partners.

Detection by Source—EMEA, 2017–2023



Change in EMEA Median Dwell Time

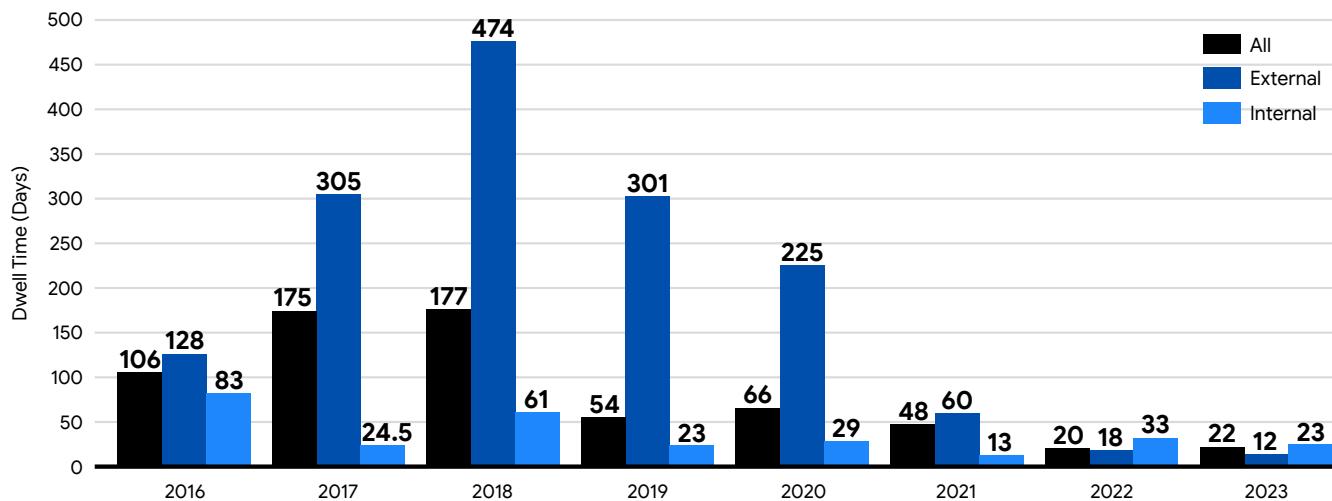
20 ↗ **22**
days in 2022 days in 2023

EMEA Median Dwell Time

Organizations in EMEA detected intrusions in 22 days in 2023 compared to 20 days in 2022. Dwell time for intrusions detected externally decreased to just under two weeks, at 12 days in 2023 compared to 18 seen in 2022. Organizations detected intrusions internally in 23 days in 2023 compared to 33 days in 2022.

Over the years, dwell time has varied across detection sources in EMEA. The general trend shows that median dwell time continues to decrease year over year, with median dwell time in 2022 resulting in the shortest time period seen in the region. The small variation seen in 2023 could be the result of regional data normalizing, following the notable portion of Mandiant's work in Ukraine in 2022.

EMEA Median Dwell Time, 2016-2023



Dwell Time Distribution

This year in EMEA, organizations saw intrusions go undetected for longer periods of time compared to previous years, with 14% of investigations conducted in the region remaining undetected for up to five years. However, in 2023, organizations saw less than 1% of investigations go undetected for more than five years.

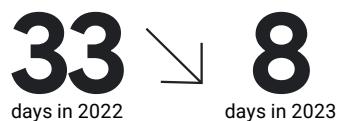
EMEA Dwell Time Distribution, 2021-2023

	1 week or less	30 days or less	6 months or less	1 year or less	5 years or less	5 years or more
2021	33.0%	14.0%	22.0%	12.0%	14.0%	6.0%
2022	41.6%	12.2%	17.7%	10.2%	11.5%	7.0%
2023	35.9%	20.5%	23.1%	6.4%	14.1%	0.0%

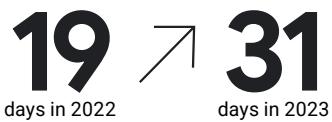
Change in EMEA Investigations Involving Ransomware



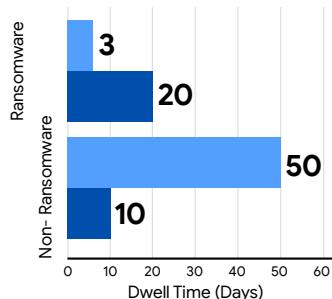
Change in EMEA Median Dwell Time—Ransomware



Change in EMEA Dwell Time—Non-Ransomware



EMEA Median Dwell Time by Detection Source



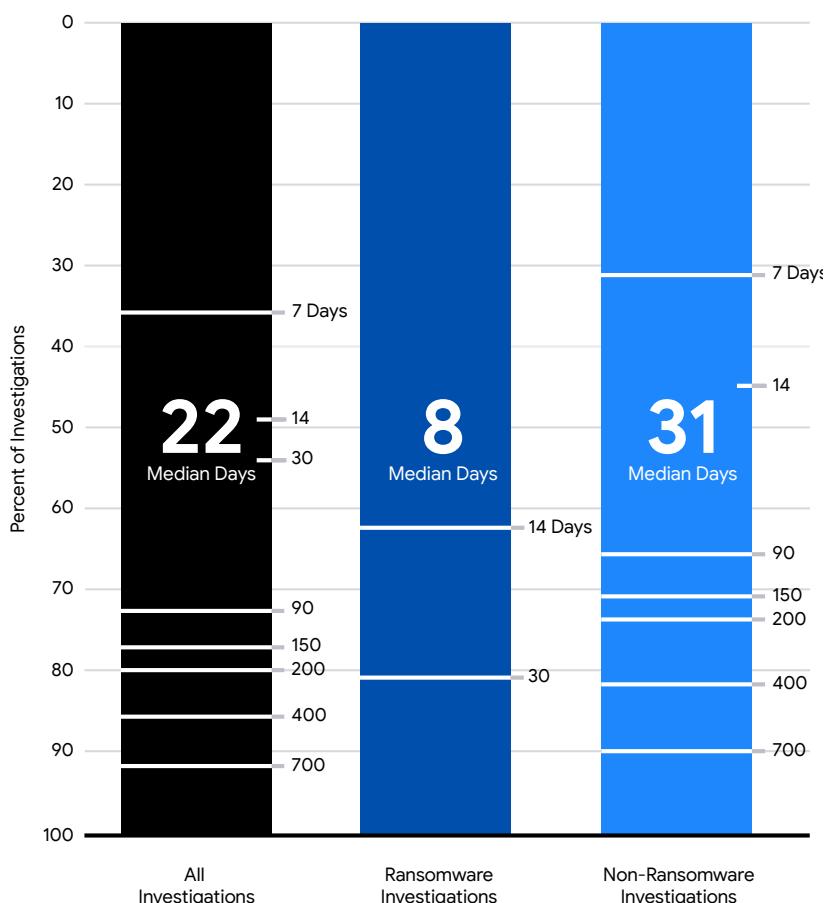
Investigations Involving Ransomware

Organizations working with Mandiant in EMEA saw ransomware-related intrusions return to a volume previously seen in 2021. Nearly a quarter of the investigations conducted in the region were ransomware-related, 22% in 2023 compared to 7% in 2022.

The median dwell time for ransomware-related intrusions decreased in the region. Ransomware intrusions were detected in little more than one week, with eight days compared to 33 days in 2022. Internal detection of ransomware intrusions in EMEA took 3 days, compared to 20 days for external notifications.

Intrusions not related to ransomware were detected in 31 days in 2023, compared to 19 days in 2022. Non-ransomware-related intrusions remain undetected for longer periods of time if they are detected by an internal source.

EMEA Dwell Time by Investigation Type, 2023





Targeted Attacks

Initial Infection Vector

In EMEA, Mandiant investigators noted intrusions began with an exploit in 36% of intrusions when an initial infection vector was identified. Organizations in EMEA also faced attackers abusing prior access in 21% of intrusions and phishing in 16% of intrusions.

Threat Groups

Prevalent Threat Group Targeting EMEA

Mandiant investigated a variety of intrusions in EMEA in 2023, including compromises attributed to UNC4393. UNC4393 is a financially motivated threat cluster that has monetized access by deploying BASTA ransomware. This cluster does not work alone but rather relies on other attackers to obtain initial access into target environments. Throughout most of 2023, Mandiant found that UNC2500 and UNC2633 QAKBOT infections consistently preceded UNC4393 activity in target environments. In August 2023, an international law enforcement effort disrupted the QAKBOT botnet,²³ which forced UNC2500 to shift to alternative malware payloads to continue operations. Starting in mid-September 2023, Mandiant observed UNC2500 begin distributing DARKGATE payloads, which UNC4393 leveraged to ultimately deploy BASTA ransomware.

Mandiant regularly observes evidence that multiple attackers were involved in different stages of a compromise, and prior compromise was the third most common initial access vector for 2023 Mandiant incident responses. The complexity of multi-attacker intrusions and the speed with which attacker tactics, techniques, and procedures (TTPs) evolve underscores the importance of implementing defense-in-depth strategies to minimize the impact of an attacker gaining a foothold in an environment.

MITRE ATT&CK

Special Report: Mandiant M-Trends 2024

49

Mandiant's Targeted Attack Lifecycle is the predictable sequence of events cyber attackers use to carry out their attacks.

Techniques Related to Mandiant Targeted Attack Lifecycle, 2023

Initial Reconnaissance

Reconnaissance

T1595: Active Scanning	1.1%	T1595.001: Scanning IP Blocks	0.6%
		T1595.002: Vulnerability Scanning	0.6%

Resource Development

T1608: Stage Capabilities	12.8%	T1608.003: Install Digital Certificate	6.6%
		T1608.005: Link Target	2.6%
		T1608.001: Upload Malware	2.1%
		T1608.002: Upload Tool	0.9%
		T1608.006: SEO Poisoning	0.9%
T1583: Acquire Infrastructure	5.4%	T1583.003: Virtual Private Server	5.4%
T1584: Compromise Infrastructure	3.2%		
T1587: Develop Capabilities	2.3%	T1587.002: Code Signing Certificates	1.3%
		T1587.003: Digital Certificates	0.9%
T1588: Obtain Capabilities	1.5%	T1588.004: Digital Certificates	1.1%
		T1588.003: Code Signing Certificates	0.4%
T1585: Establish Accounts	0.2%	T1585.002: Email Accounts	0.2%

Initial Compromise

Initial Access

T1190: Exploit Public-Facing Application	28.7%		
T1133: External Remote Services	20.3%		
T1566: Phishing	16.3%	T1566.001: Spearphishing Attachment	5.1%
		T1566.002: Spearphishing Link	3.2%
		T1566.004: Spearphishing Voice	1.9%
		T1566.003: Spearphishing via Service	0.8%
T1078: Valid Accounts	11.3%	T1078.004: Cloud Accounts	2.1%
		T1078.001: Default Accounts	0.2%
T1189: Drive-by Compromise	3.4%		
T1195: Supply Chain Compromise	0.8%	T1195.002: Compromise Software Supply Chain	0.6%
T1199: Trusted Relationship	0.8%		
T1091: Replication Through Removable Media	0.6%		
T1200: Hardware Additions	0.2%		

Establish Foothold

Persistence

T1543: Create or Modify System Process	28.3%	T1543.003: Windows Service	16.7%
		T1543.002: Systemd Service	0.9%
		T1543.004: Launch Daemon	0.4%
		T1543.001: Launch Agent	0.2%
T1098: Account Manipulation	18.6%	T1098.005: Device Registration	2.1%
		T1098.004: SSH Authorized Keys	1.7%
		T1098.001: Additional Cloud Credentials	0.4%
T1053: Scheduled Task/Job	18.0%	T1053.005: Scheduled Task	14.8%
		T1053.003: Cron	1.7%
T1003: OS Credential Dumping	16.9%	T1003.003: NTDS	7.1%
		T1003.001: LSASS Memory	5.4%
		T1003.002: Security Account Manager	3.0%
		T1003.008: /etc/passwd and /etc/shadow	2.4%
		T1003.006: DCSync	0.4%
		T1003.004: LSA Secrets	0.2%
T1505: Server Software Component	14.4%	T1505.003: Web Shell	14.3%
		T1505.001: SQL Stored Procedures	0.2%
		T1505.004: IIS Components	0.2%
T1136: Create Account	11.8%	T1136.001: Local Account	5.4%
		T1136.002: Domain Account	1.1%
		T1136.003: Cloud Account	0.6%
T1574: Hijack Execution Flow	10.3%	T1574.011: Services Registry Permissions Weakness	8.6%
		T1574.002: DLL Side-Loading	1.1%
		T1574.001: DLL Search Order Hijacking	0.4%
		T1574.008: Path Interception by Search Order Hijacking	0.4%
		T1574.006: Dynamic Linker Hijacking	0.2%
T1547: Boot or Logon Autostart Execution	9.6%	T1547.001: Registry Run Keys / Startup Folder	7.1%
		T1547.009: Shortcut Modification	2.6%
		T1547.004: Winlogon Helper DLL	0.4%
		T1547.011: Plist Modification	0.2%
T1552: Unsecured Credentials	8.8%	T1552.002: Credentials in Registry	2.4%
		T1552.004: Private Keys	1.7%
		T1552.001: Credentials In Files	1.3%
		T1552.003: Bash History	0.9%
		T1552.006: Group Policy Preferences	0.8%
		T1555.005: Password Managers	0.8%
T1056: Input Capture	8.1%	T1056.001: Keylogging	7.5%
		T1056.002: GUI Input Capture	0.6%
		T1056.003: Web Portal Capture	0.2%

T1110: Brute Force	7.3%	T1110.001: Password Guessing	2.8%
		T1110.003: Password Spraying	1.1%
		T1110.004: Credential Stuffing	0.8%
T1555: Credentials from Password Stores	5.4%	T1555.003: Credentials from Web Browsers	3.2%
		T1555.004: Windows Credential Manager	2.8%
		T1555.006: Cloud Secrets Management Stores	0.9%
		T1555.005: Password Managers	0.8%
		T1555.001: Keychain	0.2%
T1546: Event Triggered Execution	3.4%	T1546.003: Windows Management Instrumentation Event Subscription	2.8%
		T1546.008: Accessibility Features	0.4%
		T1546.010: Appinit DLLs	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
T1111: Multi-Factor Authentication Interception	3.2%		
T1558: Steal or Forge Kerberos Tickets	3.2%	T1558.003: Kerberoasting	1.7%
T1556: Modify Authentication Process	1.7%	T1556.006: Multi-Factor Authentication	1.1%
		T1556.002: Password Filter DLL	0.2%
		T1556.003: Pluggable Authentication Modules	0.2%
T1037: Boot or Logon Initialization Scripts	0.9%	T1037.004: RC Scripts	0.6%
T1187: Forced Authentication	0.8%		
T1539: Steal Web Session Cookie	0.8%		
T1649: Steal or Forge Authentication Certificates	0.4%		
T1557: Adversary-in-the-Middle	0.2%	T1557.00: LLMNR/NBT-NS Poisoning and SMB Relay	0.2%
T1621: Multi-Factor Authentication Request Generation	0.2%		

Escalate Privileges

Privilege Escalation

T1543: Create or Modify System Process	28.3%	T1543.003: Windows Service	16.7%
		T1543.005: Scheduled Task	14.8%
		T1543.002: Systemd Service	0.9%
		T1543.004: Launch Daemon	0.4%
		T1543.001: Launch Agent	0.2%
T1055: Process Injection	25.1%	T1055.003: Thread Execution Hijacking	1.3%
		T1055.004: Asynchronous Procedure Call	0.9%
		T1055.001: Dynamic-link Library Injection	0.8%
		T1055.002: Portable Executable Injection	0.4%
		T1055.012: Process Hollowing	0.4%
T1053 Scheduled Task/Job	18%	T1053.003: Cron	1.7%
T1134: Access Token Manipulation	13.7%	T1134.001: Token Impersonation/Theft	4.9%
		T1134.004: Parent PID Spoofing	0.6%
T1547: Boot or Logon Autostart Execution	9.6%	T1547.001: Registry Run Keys/Startup Folder	7.1%
		T1547.009: Shortcut Modification	2.6%
		T1547.004: Winlogon Helper DLL	0.4%
		T1547.011: Plist Modification	0.2%
T1546: Event Triggered Execution	3.4%	T1546.003: Windows Management Instrumentation Event Subscription	2.8%
		T1546.008: Accessibility Features	0.4%
		T1546.010: ApnlInit DLLs	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
T1484: Domain Policy Modification	1.5%	T1484.001: Group Policy Modification	1.5%
T1037: Boot or Logon Initialization Scripts	0.9%	T1037.004: RC Scripts	0.6%
T1548: Abuse Elevation Control Mechanism	0.8%	T1548.002: Bypass User Account Control	0.8%
T1068: Exploitation for Privilege Escalation	0.6%		

Internal Reconnaissance

Discovery

T1083: File and Directory Discovery	38.6%		
T1082: System Information Discovery	37.1%		
T1033: System Owner/User Discovery	31.7%		
T1087: Account Discovery	28.1%	T1087.002: Domain Account	15.0%
		T1087.001: Local Account	10.5%
		T1087.004: Cloud Account	0.8%
T1012: Query Registry	24.8%		
T1016: System Network Configuration Discovery	23.5%	T1016.001: Internet Connection Discovery	5.3%
T1622: Debugger Evasion	21.8%		
T1057: Process Discovery	18.9%		
T1003: OS Credential Dumping	16.9%	T1003.003: NTDS	7.1%
		T1003.001: LSASS Memory	5.4%
		T1003.002: Security Account Manager	3.0%
		T1003.008: /etc/passwd and /etc/shadow	2.4%
		T1003.006: DCSync	0.4%
		T1003.004: LSA Secrets	0.2%
T1518: Software Discovery	16.3%	T1518.001: Security Software Discovery	1.3%
T1614: System Location Discovery	15.9%	T1614.001: System Language Discovery	9.6%
T1069: Permission Groups Discovery	14.8%	T1069.002: Domain Groups	11.1%
		T1069.001: Local Groups	1.3%
		T1069.003: Cloud Groups	1.1%
T1482: Domain Trust Discovery	12.6%		
T1497: Virtualization/Sandbox Evasion	12.2%	T1497.001: System Checks	10.1%
T1007: System Service Discovery	11.4%		
T1552: Unsecured Credentials	8.8%	T1552.002: Credentials in Registry	2.4%
		T1552.004: Private Keys	1.7%
		T1552.001: Credentials In Files	1.3%
		T1552.003: Bash History	0.9%
		T1552.006: Group Policy Preferences	0.8%
T1049: System Network Connections Discovery	8.1%		
T1056: Input Capture	8.1%	T1056.001: Keylogging	7.5%
		T1056.002: GUI Input Capture	0.6%
		T1056.003: Web Portal Capture	0.2%
T1110: Brute Force	7.3%	T1110.001: Password Guessing	2.8%
		T1110.003: Password Spraying	1.1%
		T1110.004: Credential Stuffing	0.8%
T1010: Application Window Discovery	7.1%		

T1135: Network Share Discovery	6.8%			
T1555: Credentials from Password Stores	5.4%	T1555.003: Credentials from Web Browsers	3.2%	
		T1555.004: Windows Credential Manager	2.8%	
		T1555.006: Cloud Secrets Management Stores	0.9%	
		T1555.005: Password Managers	0.8%	
		T1555.001: Keychain	0.2%	
T1046: Network Service Discovery	3.4%			
T1111: Multi-Factor Authentication Interception	3.2%			
T1558: Steal or Forge Kerberos Tickets	3.2%	T1558.003: Kerberoasting	1.7%	
T1018: Remote System Discovery	2.8%			
T1556: Modify Authentication Process	1.7%	T1556.006: Multi-Factor Authentication	1.1%	
		T1556.002: Password Filter DLL	0.2%	
		T1556.003: Pluggable Authentication Modules	0.2%	
T1580: Cloud Infrastructure Discovery	1.5%			
T1124: System Time Discovery	1.3%			
T1619: Cloud Storage Object Discovery	1.3%			
T1040: Network Sniffing	0.8%			
T1615: Group Policy Discovery	0.8%			
T1187: Forced Authentication	0.8%			
T1539: Steal Web Session Cookie	0.8%			
T1526: Cloud Service Discovery	0.6%			
T1120: Peripheral Device Discovery	0.4%			
T1201: Password Policy Discovery	0.4%			
T1538: Cloud Service Dashboard	0.4%			
T1649: Steal or Forge Authentication Certificates	0.4%			
T1217: Browser Bookmark Discovery	0.2%			
T1557: Adversary-in-the-Middle	0.2%	T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay	0.2%	
T1621: Multi-Factor Authentication Request Generation	0.2%			

Lateral Movement

Lateral Movement

T1021: Remote Services	37.3%	T1021.001: Remote Desktop Protocol	28.3%
		T1021.004: SSH	10.3%
		T1021.002: SMB/Windows Admin Shares	10.1%
		T1021.006: Windows Remote Management	1.3%
		T1021.005: VNC	0.8%
T1570: Lateral Tool Transfer	2.3%		
T1563: Remote Service Session Hijacking	2.1%	T1563.002: RDP Hijacking	0.4%
T1550: Use Alternate Authentication Material	1.7%	T1550.001: Application Access Token	1.1%
		T1550.002: Pass the Hash	0.6%
		T1550.004: Web Session Cookie	0.2%
T1534: Internal Spearphishing	0.6%		
T1091: Replication Through Removable Media	0.6%		
T1072: Software Deployment Tools	0.2%		
T1080: Taint Shared Content	0.2%		

Maintain Presence

Persistence

T1027: Obfuscated Files or Information	46.5%	T1027.009: Embedded Payloads	9.6%
		T1027.002: Software Packing	8.6%
		T1027.010: Command Obfuscation	3.9%
		T1027.004: Compile After Delivery	1.3%
		T1027.005: Indicator Removal from Tools	0.4%
		T1027.001: Binary Padding	0.2%
		T1027.003: Steganography	0.2%
		T1027.008: Stripped Payloads	0.2%
T1070: Indicator Removal	35.1%	T1070.004: File Deletion	26.6%
		T1070.009: Clear Persistence	9.0%
		T1070.006: Timestamp	7.1%
		T1070.001: Clear Windows Event Logs	5.6%
		T1070.007: Clear Network Connection History and Configurations	3.4%
		T1070.005: Network Share Connection Removal	1.1%
		T1070.003: Clear Command History	0.6%
		T1070.002: Clear Linux or Mac System Logs	0.4%
		T1070.008: Clear Mailbox Data	0.2%
T1140: Deobfuscate/Decode Files or Information	31.5%		
T1543: Create or Modify System Process	28.3%	T1543.003: Windows Service	16.7%
		T1543.002: Systemd Service	0.9%
		T1543.004: Launch Daemon	0.4%
		T1543.001: Launch Agent	0.2%
T1112: Modify Registry	26.5%		
T1564: Hide Artifacts	19.5%	T1564.003: Hidden Window	14.8%
		T1564.001: Hidden Files and Directories	4.7%
		T1564.008: Email Hiding Rules	2.1%
		T1564.006: Accessibility Features	0.4%
		T1564.011: Ignore Process Interrupts	0.2%
T1562: Impair Defenses	18.6%	T1562.001: Disable or Modify Tools	13.3%
		T1562.004: Disable or Modify System Firewall	7.9%
		T1562.002: Disable Windows Event Logging	4.3%
		T1562.010: Downgrade Attack	0.9%
		T1562.003: Impair Command History Logging	0.9%
		T1562.009: Safe Mode Boot	0.2%
T1053: Scheduled Task/Job	18.0%		

T1218: System Binary Proxy Execution	16.1%	T1218.011: Rundll32	12.9%
		T1218.010: Regsvr32	1.7%
		T1218.005: Mshta	1.3%
		T1218.007: Msieexec	0.9%
		T1218.014: MMC	0.4%
		T1218.001: Compiled HTML File	0.2%
T1036: Masquerading	11.8%	T1036.001: Invalid Code Signature	6.8%
		T1036.008: Masquerade File Type	0.8%
		T1036.005: Match Legitimate Name or Location	0.8%
		T1036.003: Rename System Utilities	0.2%
T1547: Boot or Logon Autostart Execution	9.6%	T1547.001: Registry Run Keys / Startup Folder	7.1%
		T1547.009: Shortcut Modification	2.6%
		T1547.004: Winlogon Helper DLL	0.4%
		T1547.011: Plist Modification	0.2%
T1202: Indirect Command Execution	8.6%		
T1620: Reflective Code Loading	8.6%		
T1222: File and Directory Permissions Modification	7.9%	T1222.002: Linux and Mac File and Directory Permissions Modification	4.1%
		T1222.001: Windows File and Directory Permissions Modification	1.1%
T1546: Event Triggered Execution	3.4%	T1546.003: Windows Management Instrumentation Event Subscription	2.8%
		T1546.010: Process Argument Spoofing	0.2%
		T1546.010: AppInit DLLs	0.2%
		T1546.015: Component Object Model Hijacking	0.2%
T1556: Modify Authentication Process	1.7%	T1556.006: Multi-Factor Authentication	1.1%
		T1556.002: Password Filter DLL	0.2%
		T1556.003: Pluggable Authentication Modules	0.2%
T1037: Boot or Logon Initialization Scripts	0.9%	T1037.004: RC Scripts	0.6%
T1006: Direct Volume Access	0.8%		
T1553: Subvert Trust Controls	0.8%	T1553.002: Code Signing	0.6%
		T1553.005: Mark-of-the-Web Bypass	0.2%
T1578: Modify Cloud Compute Infrastructure	0.6%	T1578.002: Create Cloud Instance	0.6%
		T1578.005: Modify Cloud Compute Configurations	0.2%
T1207: Rogue Domain Controller	0.4%		
T1014: Rootkit	0.4%		
T1480: Execution Guardrails	0.2%		
T1601: Modify System Image	0.2%	T1601.001: Patch System Image	0.2%
T1647: Plist File Modification	0.2%		
T1127: Trusted Developer Utilities Proxy Execution	0.2%	T1127.001: MSBuild	0.2%
T1220: XSL Script Processing	0.2%		

Mission Completion

Collection

T1213: Data from Information Repositories	16.7%	T1213.002: Sharepoint	8.4%
		T1213.001: Confluence	0.4%
		T1213.003: Code Repositories	0.2%
T1560: Archive Collected Data	14.6%	T1560.001: Archive via Utility	7.5%
		T1560.002: Archive via Library	0.8%
T1056: Input Capture	8.1%	T1056.001: Keylogging	7.5%
		T1056.002: GUI Input Capture	0.6%
		T1056.003: Web Portal Capture	0.2%
T1074: Data Staged	5.4%	T1074.001: Local Data Staging	4.7%
		T1074.002: Remote Data Staging	0.4%
T1115: Clipboard Data	5.3%		
T1113: Screen Capture	4.7%		
T1125: Video Capture	3.9%		
T1114: Email Collection	2.4%	T1114.002: Remote Email Collection	0.6%
		T1114.001: Local Email Collection	0.2%
T1039: Data from Network Shared Device	1.7%		
T1005: Data from Local System	0.8%		
T1530: Data from Cloud Storage	0.6%		
T1602: Data from Configuration Repository	0.4%	T1602.002: Network Device Configuration Dump	0.4%
T1119: Automated Collection	0.2%		
T1123: Audio Capture	0.2%		
T1557: Adversary-in-the-Middle	0.2%	T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay	0.2%

Exfiltration

T1567: Exfiltration Over Web service	5.6%	T1567.002: Exfiltration to Cloud Storage	2.4%
		T1567.003: Exfiltration to Text Storage Sites	0.2%
T1041: Exfiltration Over C2 Channel	3.6%		
T1020: Automated Exfiltration	1.1%		
T1052: Exfiltration Over Physical Medium	0.2%	T1052.001: Exfiltration over USB	0.2%

Impact

T1486: Data Encrypted for Impact	25.5%			
T1489: Service Stop	15.9%			
T1657: Financial Theft	7.9%			
T1529: System Shutdown/Reboot	6.9%			
T1490: Inhibit System Recovery	5.8%			
T1485: Data Destruction	2.8%			
T1496: Resource Hijacking	2.3%			
T1565: Data Manipulation	2.3%	T1565.001: Stored Data Manipulation		2.3%
T1531: Account Access Removal	1.7%			
T1491: Defacement	1.1%	T1491.002: External Defacement		0.2%
T1561: Disk Wipe	0.6%	T1561.001: Disk Content Wipe		0.4%
T1498: Network Denial of Service	0.2%	T1498.001: Direct Network Flood		0.2%
T1499: Endpoint Denial of Service	0.2%			

CYBER INSECURITY IN HEALTHCARE: THE COST AND IMPACT ON PATIENT SAFETY AND CARE

Independently conducted by:



Sponsored by:



KEY FINDINGS

BY THE NUMBERS



of organizations had at least one cyber attack over the past 12 months



The average number of cyber attacks in this group



The average total cost for the single most expensive cyber attack over the past 12 months



The average cost of disruption to normal healthcare operations was the most expensive financial consequence from a cyber attack—a 30% increase from 2022.

ORGANIZATIONS ARE UNPREPARED TO STOP ATTACKS, WHICH IMPACTS PATIENT SAFETY AND CARE



of organizations experienced on average **four ransomware attacks** in the past two years.



of this group say ransomware attacks negatively impacted patient safety and care.



of organizations experienced an average of **five BEC attacks** in the past two years.

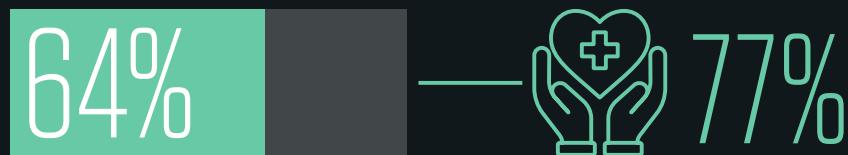


of this group say BEC attacks disrupted patient care.

RANSOMWARE

BEC

(CONT) ORGANIZATIONS ARE UNPREPARED TO STOP ATTACKS, WHICH IMPACTS PATIENT SAFETY AND CARE



of organizations experienced an average of **four supply chain attacks** in the last two years.



of this group say those attacks impacted patient care.



ONLY 45% of organizations say they have a strategy to stop BEC and supply chain attacks.

MOVING TO THE CLOUD INCREASES RISKS AND VULNERABILITIES



63% of organizations had an average of **21 cloud compromises** during the past two years.

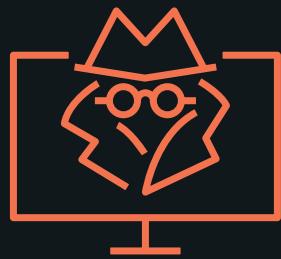
53% of respondents say project management and video conferencing tools were most attacked.

Despite these risks, the use of CASB and encryption tools to protect sensitive information in the cloud decreased significantly.

DATA LOSS AND EXFILTRATION IS ON THE RISE

100%

of organizations had at least one incident where sensitive healthcare data was lost or stolen.



Malicious insiders are the No. 1 cause of data loss and exfiltration.

19  The average number of data loss incidents was 19.

 43%

say these incidents impacted patient care.

47% are very concerned that employees don't understand the sensitivity and confidentiality of data they share via email.

EXECUTIVE SUMMARY

A STRONG CYBERSECURITY POSTURE IN HEALTHCARE ORGANIZATIONS IS IMPORTANT TO NOT ONLY SAFEGUARD SENSITIVE PATIENT INFORMATION BUT TO DELIVER THE BEST POSSIBLE MEDICAL CARE.

This second annual report was conducted to determine if the healthcare industry is making progress in achieving these two objectives.

With sponsorship from Proofpoint, Ponemon Institute surveyed 653 IT and IT security practitioners in U.S. healthcare organizations who are responsible for participating in such cybersecurity strategies as setting IT cybersecurity priorities, managing budgets and selecting vendors and contractors.

According to the research, 88 percent of organizations surveyed experienced at least one cyberattack in the past 12 months. For organizations in that group, the average number of cyberattacks was 40. We asked respondents to estimate the single most expensive cyberattack experienced in the past 12 months from a range of less than \$10,000 to more than \$25 million. Based on the responses, the average total cost for the most expensive cyberattack was \$4,991,500, a 13 percent increase over last year. This included all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

At an average cost of \$1.3 million, disruption to normal healthcare operations because of system availability problems was the most expensive consequence from the cyberattack, an increase from an average \$1 million in 2022. Users' idle time and lost productivity because of downtime or system performance delays cost an average of \$1.1 million, the same as in 2022. The cost of the time required to ensure the impact on patient care was corrected increased over 50 percent from an average of \$664,350 in 2022 to \$1 million in 2023.



of organizations in this research had at least one cyberattack over the past 12 months



The average total cost for the single most expensive cyberattack experienced over the past 12 months



in disruption to normal healthcare operations was on average the most significant financial consequence from the cyberattack

The report analyzes four types of cyberattacks and their impact on healthcare organizations, patient safety and patient care delivery:



CLOUD COMPROMISE

The most frequent attacks in healthcare are against the cloud, making it the top cybersecurity threat, according to respondents. Seventy-four percent of respondents say their organizations are vulnerable to a cloud compromise. Sixty-three percent say their organizations have experienced at least one cloud compromise. In the past two years, organizations in this group experienced 21 cloud compromises. Sixty-three percent say they are concerned about the threat of a cloud compromise, an increase from 57 percent.



BUSINESS EMAIL COMPROMISE (BEC)/SPOOFING PHISHING.

Concerns about BEC attacks have increased significantly. Sixty-two percent of respondents say their organizations are most concerned about a BEC/spoofing phishing incident, an increase from 46 percent in 2022. In the past two years, the frequency of such attacks increased as well from an average of four attacks to five attacks.



RANSOMWARE

Ransomware has declined as a top cybersecurity threat. Sixty-four percent of respondents believe their organizations are vulnerable to a ransomware attack. However, as a concern ransomware has decreased from 60 percent in 2022 to 48 percent in 2023. In the past two years, organizations that had ransomware attacks (54 percent of respondents) experienced an average of four such attacks, an increase from three attacks. While fewer organizations paid the ransom (40 percent in 2023 vs. 51 percent in 2022), the ransom paid increased nearly 30 percent from an average of \$771,905 to \$995,450.



SUPPLY CHAIN ATTACKS

Organizations are vulnerable to a supply chain attack, according to 63 percent of respondents. However, only 40 percent say this cyber threat is of concern to their organizations. On average, organizations experienced four supply chain attacks in the past two years.

As in the previous report, an important part of the research is the connection between cyberattacks and patient safety. Following are trends in how cyberattacks have affected patient safety and patient care delivery.

- **It is more likely that a supply chain attack will affect patient care.** Sixty-four percent of respondents say their organizations had an attack against their supply chains. Seventy-seven percent of those respondents say it disrupted patient care, an increase from 70 percent in 2022. Patients were primarily impacted by delays in procedures and tests that resulted in poor outcomes such as an increase in the severity of an illness (50 percent) and a longer length of stay (48 percent). Twenty-one percent say there was an increase in mortality rate.
- **A BEC/spoofing attack can disrupt patient care.** Fifty-four percent of respondents say their organizations experienced a BEC/spoofing incident. Of these respondents, 69 percent say a BEC/spoofing attack against their organizations disrupted patient care, a slight increase from 67 percent in 2022. And of these 69 percent, 71 percent say the consequences caused delays in procedures and tests that have resulted in poor outcomes while 56 percent say it increased complications from medical procedures.
- **Ransomware attacks can cause delays in patient care.** Fifty-four percent of respondents say their organizations experienced a ransomware attack. Sixty-eight percent of respondents say ransomware attacks have a negative impact on patient care. Fifty-nine percent of these respondents say patient care was affected by delays in procedures and tests that resulted in poor outcomes and 48 percent say it resulted in longer lengths of stay, which affects organizations' ability to care for patients.
- **Cloud compromises are least likely to disrupt patient care.** Sixty-three percent of respondents say their organizations experienced a cloud compromise, but less than half (49 percent) say cloud compromises disrupted patient care. Of these respondents, 53 percent say these attacks increased complications from medical procedures and 29 percent say they increased mortality rate.
- **Data loss or exfiltration disrupts patient care and can increase mortality rates.** All organizations in this research had at least one data loss or exfiltration incident involving sensitive and confidential healthcare data in the past two years. On average, organizations experienced 19 such incidents in the past two years and 43 percent of respondents say they impacted patient care. Of these respondents, 46 percent say it increased the mortality rate and 38 percent say it increased complications from medical procedures.

OTHER KEY TRENDS IN CYBER INSECURITY

CONCERN
ABOUT EMPLOYEE
BEHAVIOR-RELATED
THREATS INCREASED
SIGNIFICANTLY

61%

of organizations are now worried about the security risks created by BYOD, an increase from 34% in 2022.

62%

are concerned about BEC/spoof phishing, an increase from 46% in 2022.

THE TOTAL COST OF A CYBERSECURITY COMPROMISE

\$1.3M

Disruption to normal healthcare operations because of system availability problems increased to \$1.3 million from \$1 million in 2022.

\$1M

The cost of the time taken to ensure impact on patient care was corrected increased to \$1 million in 2023 from \$664,350 in 2022.

\$1.1M

Users' idle time and lost productivity because of downtime or system performance delays averaged \$1.1 million.

MALICIOUS INSIDERS AND ACCIDENTAL DATA LOSS ARE THE TOP TWO CAUSES OF DATA LOSS AND EXFILTRATION

Malicious insiders are **the number one cause** of data loss and infiltration.

32%

Yet only 32% say they are prepared to prevent and respond to this threat.



Accidental data loss is **the second highest cause** of data loss and exfiltration.

47%

say their organizations are very concerned that employees do not understand the sensitivity and confidentiality of data they share by email.

MORE PROGRESS IS NEEDED TO REDUCE THE RISK OF DATA LOSS OR EXFILTRATION

19

All organizations in this research have experienced at least one data loss or exfiltration incident involving sensitive and confidential healthcare data.

The average number of such incidents is 19.

43%

say data loss or exfiltration impacted patient care.

Of this group:

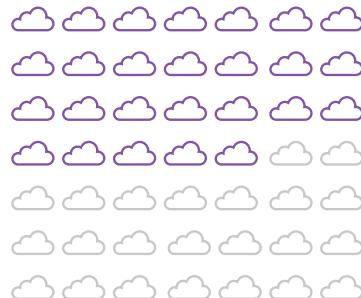
46%

say it increased mortality rates.

38%

say it increased complications from medical procedures.

CLOUD-BASED USER ACCOUNTS/ COLLABORATION TOOLS ARE MOST OFTEN ATTACKED



53%

say project management tools and Zoom/Skype/video-conferencing tools were attacked.

THE LACK OF PREPAREDNESS TO STOP BEC/SPOOF PHISHING AND SUPPLY CHAIN ATTACKS PUTS ORGANIZATIONS AND PATIENTS AT RISK

45%

While BEC/spoof phishing is considered a top cybersecurity threat, only 45% say their organizations include steps to prevent and respond to such an attack as part of their cybersecurity strategy.

45%

Similarly, only 45% say their organizations have documented the steps to prevent and respond to attacks in the supply chain.

TOP THREE CHALLENGES TO HAVING AN EFFECTIVE CYBERSECURITY POSTURE



EXPERTISE

58%

say they lack
in-house expertise,
up from 53% in 2022.



STAFFING

50%

say insufficient
staffing is a problem,
up from 46%.



BUDGET

47%

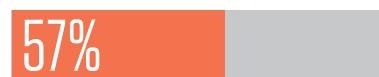
say they don't have
enough budget, up
from 41%.

SECURITY AWARENESS TRAINING PROGRAMS CONTINUE TO BE THE PRIMARY STEP TAKEN TO REDUCE INSIDER RISK

More organizations say they are taking steps to address the risk of employees' lack of awareness about cybersecurity threats.



Of this group:



say they conduct regular training and awareness programs.



say they monitor the actions of employees.

USE OF CASB AND ENCRYPTION TOOLS TO PROTECT SENSITIVE INFORMATION IN THE CLOUD DECREASED SIGNIFICANTLY



KEY FINDINGS

ANALYSIS

The complete audited findings are presented in the Appendix of this report. Whenever possible, we compare the 2022 findings to this year's report. The report is organized according to the following topics:

- Cloud compromise, ransomware, supply chain and BEC in healthcare
- The impact of cyberattacks on patient care
- The cost of cyber insecurity
- Vulnerabilities in the cloud and risk to patient data
- Solutions and responses to healthcare cyber insecurity

CLOUD COMPROMISE, RANSOMWARE, SUPPLY CHAIN AND BEC IN HEALTHCARE

FIGURE 1.

Healthcare organizations are vulnerable to cyberattacks

Healthcare organizations recognize how vulnerable they are to the four cyberattacks featured in this research. Respondents were asked to rate their organizations' vulnerability to specific types of cyberattacks on a scale from 1 = not vulnerable to 10 = highly vulnerable.

Figure 1 presents the very vulnerable to highly vulnerable responses (7+ on the 10-point scale are presented). As shown, almost all respondents recognize the threat of cloud compromises (74 percent). Concerns about ransomware attacks (64 percent) and supply chain attacks (63 percent) have declined from 72 percent and 71 percent, respectively.

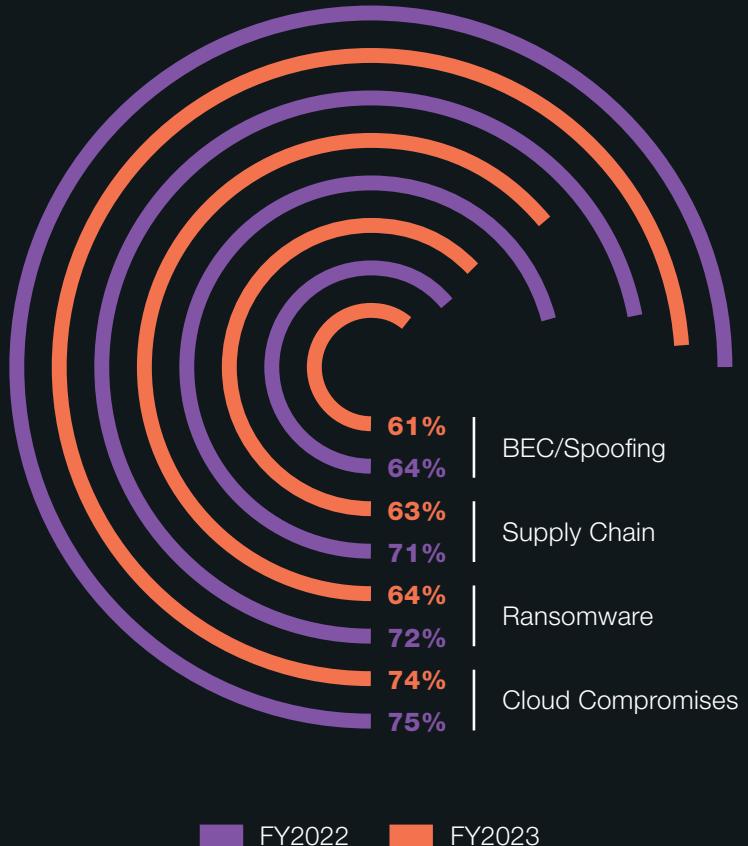
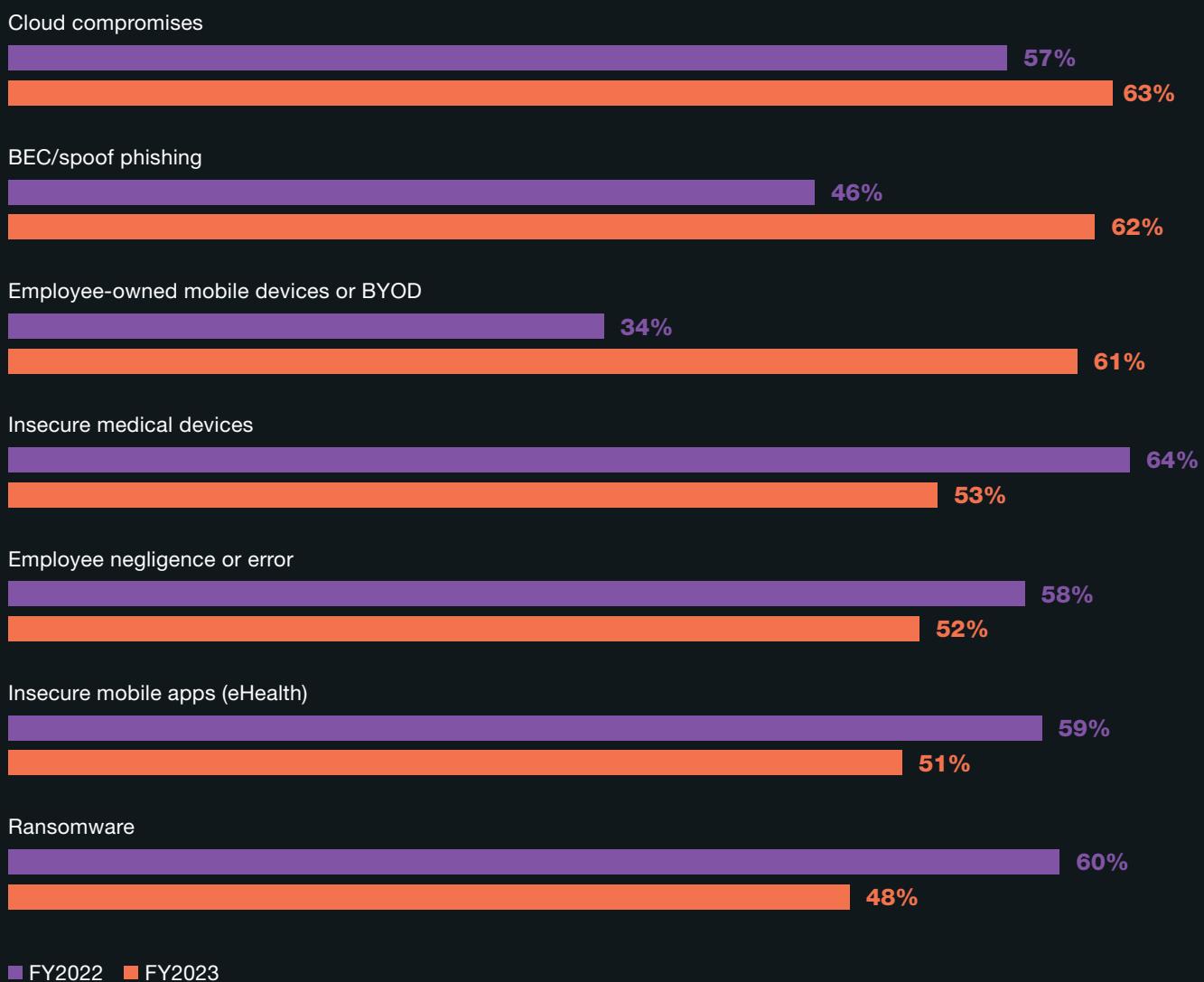


FIGURE 2.

The top cybersecurity threats of greatest concern

In this year's research, cloud compromises and BEC/spoof phishing attacks replace insecure medical devices and ransomware as the top cybersecurity threats in healthcare. As shown in Figure 2, last year's two top concerns were insecure medical devices and ransomware (64 percent and 60 percent of respondents, respectively). Today, cloud compromises and BEC/spoof phishing (63 percent and 62 percent, respectively) are the top threats to prepare for. Since 2022, threats created by employee-owned mobile devices or BYOD have increased significantly from 34 percent to 61 percent, respectively.

More than one response permitted



■ FY2022 ■ FY2023

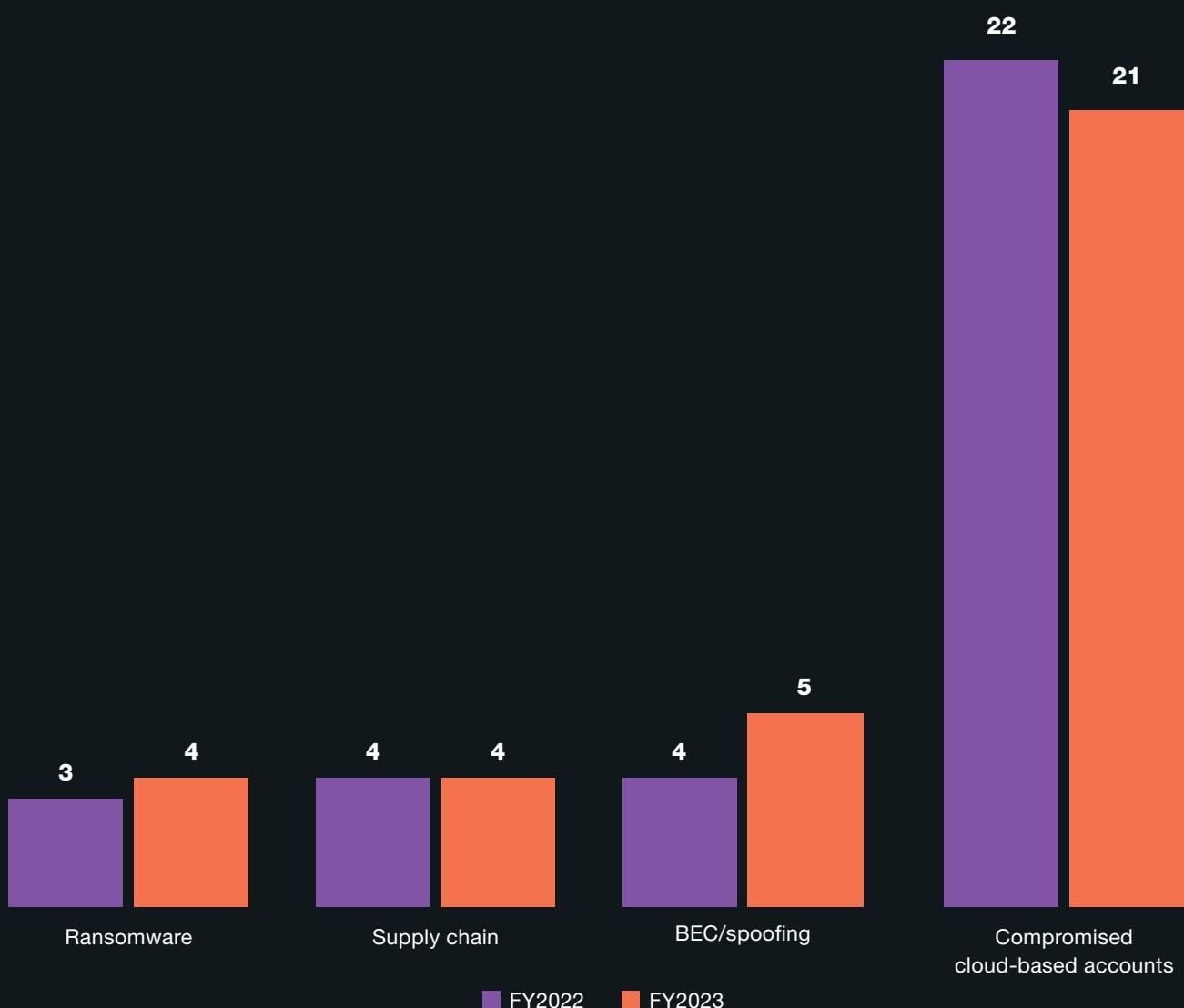
Cloud compromises continue to be the most frequent type of attack against healthcare organizations.

Figure 3A shows the average frequency for each type of cyberattack. Cloud compromise results from criminals obtaining access to credentials (e.g., user ID and passwords). The consequence is typically an account takeover where criminals then use those validated credentials to commit fraud and transfer sensitive data to systems under their control. Sixty-three percent of respondents say their organizations experienced a cloud compromise. The average number of cloud compromises for these healthcare organizations was 21 in the past two years.

FIGURE 3A.

Average number of attacks for the four types of cyberattacks in the past two years

Extrapolated value



Organizations that had a ransomware attack (54 percent of respondents) experienced an average of four ransomware attacks in the past two years. Ransomware is a sophisticated piece of malware that blocks the victim's access to files. While there are many strains of ransomware, they generally fall into two categories. Crypto ransomware encrypts files on a computer or mobile device making them unstable. It takes the files hostage, demanding a ransom in exchange for the decryption key needed to restore the files. Locker ransomware is a virus that blocks basic computer functions, essentially locking the victim out of their data and files located on the infected devices. Instead of targeting files with encryption, cybercriminals demand a ransom to unlock the device.

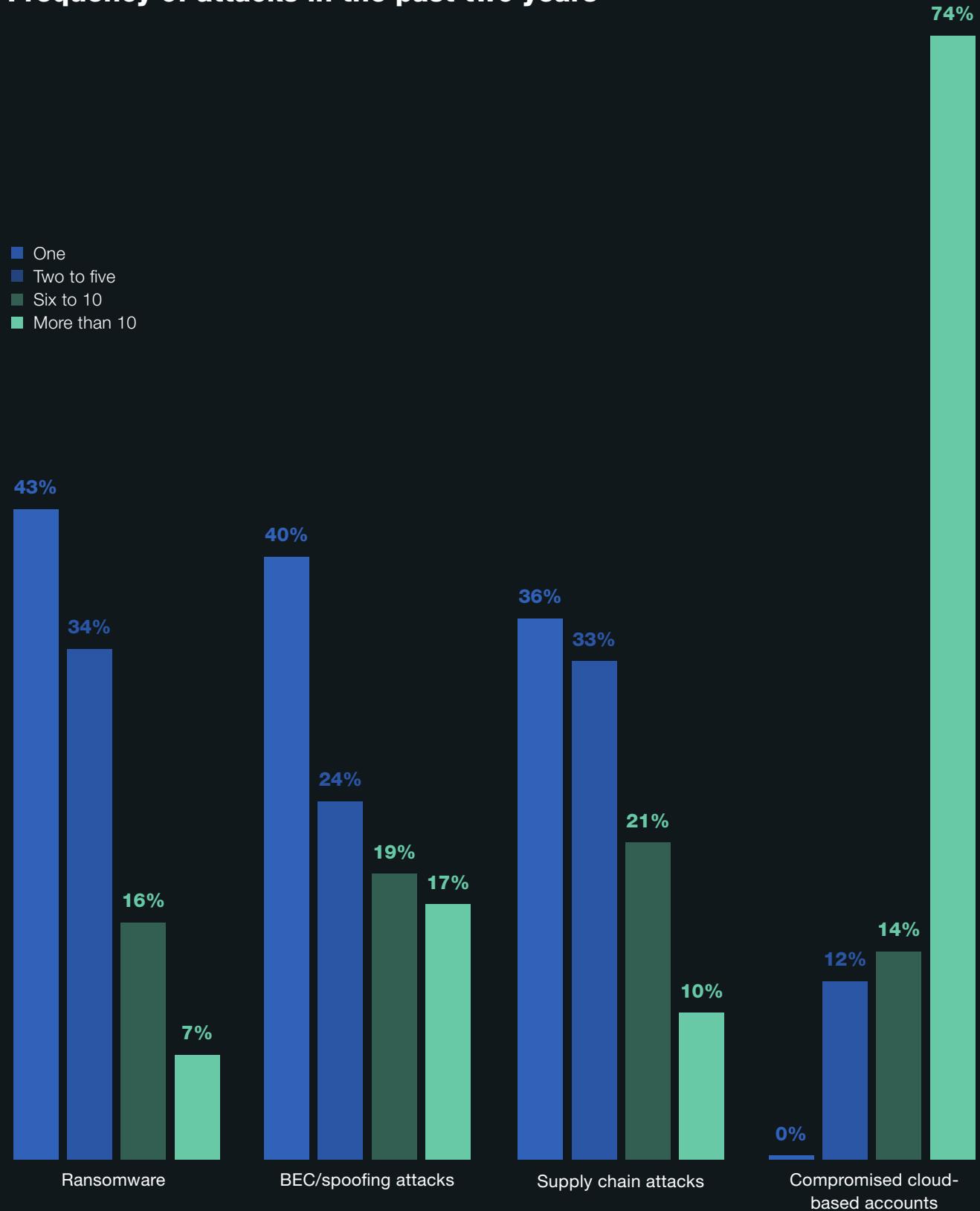
In the past two years, 64 percent of respondents say their organizations' supply chains were attacked an average of 4 times. Supplier impersonation and compromise attacks occur when a malicious actor impersonates or successfully compromises an email account in the supply chain. The attacker then observes, mimics and uses historical information to craft scenarios to spoof employees in the supply chain.

In the past two years, 54 percent of healthcare organizations experienced an average of 5 BEC/spoofing phishing attacks. BEC attacks are a form of cybercrime that uses email fraud to attack healthcare organizations to achieve a specific outcome. Examples include invoice scams, spear phishing that are designed to gather data for other criminal activities, attorney impersonation and CEO fraud.

Figure 3A presents the extrapolated average number of attacks. Figure 3B shows how many attacks for the four types of cyberattacks they experienced on a scale from 1 to more than 10. Seventy-four percent of respondents say cloud-based user accounts were compromised more than 10 times. Most organizations represented in this research had one incident involving the following: ransomware (43 percent of respondents), BEC/spoofing attacks (40 percent) and supply chain attacks (36 percent).

FIGURE 3B.

Frequency of attacks in the past two years



THE IMPACT OF CYBERATTACKS ON PATIENT CARE

ACCORDING TO THE RESEARCH, CYBERATTACKS HAVE DISRUPTED CARE, INCREASING THE RISK TO PATIENTS.

FIGURE 4.

Did cyberattacks disrupt patient care?

Figure 4 shows the four types of cyberattacks featured in this research and if they had a negative impact on patient safety and delivery of care. Such disruptions include delays in procedures and tests that have resulted in poor outcomes, longer lengths of stay, increases in patients transferred or diverted to other facilities, increases in complications from medical procedures and increases in mortality rate.

Of those organizations that experienced these attacks, more respondents this year (77 percent vs. 70 percent in 2022) believe the supply chain attacks disrupted patient care followed by the BEC/spoofing and ransomware attacks (69 percent and 68 percent, respectively). Cloud compromises are having less impact on patient care, a decrease from 64 percent to 49 percent.

Yes responses presented

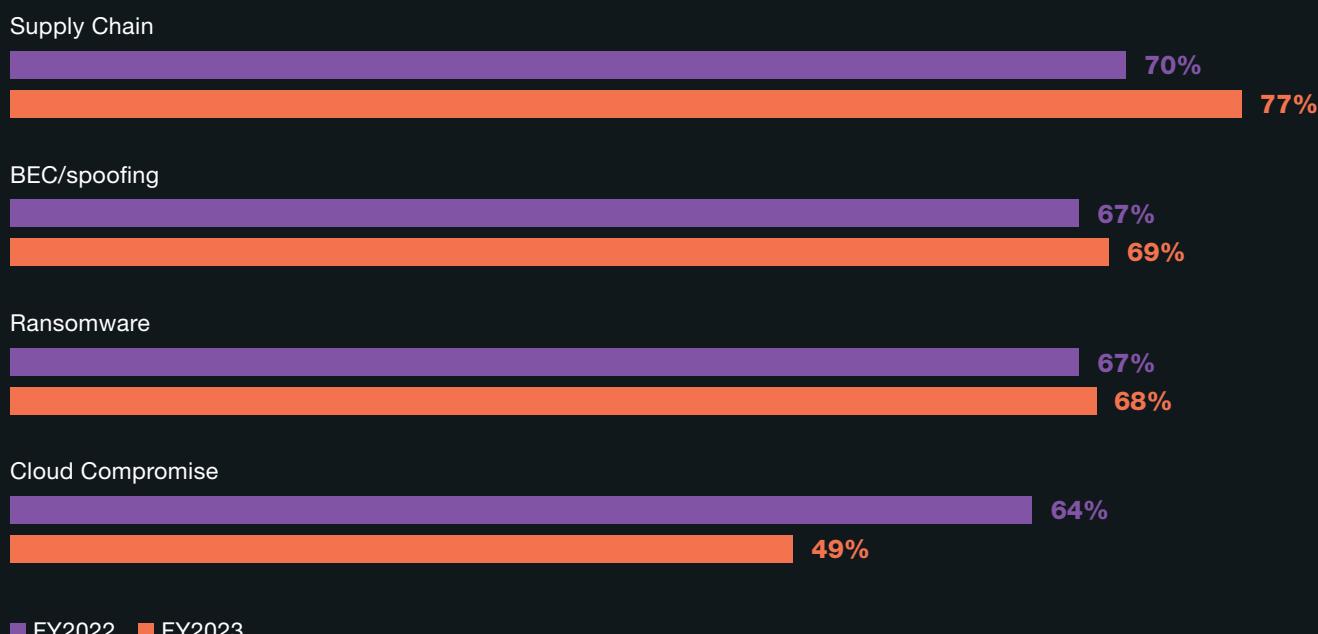
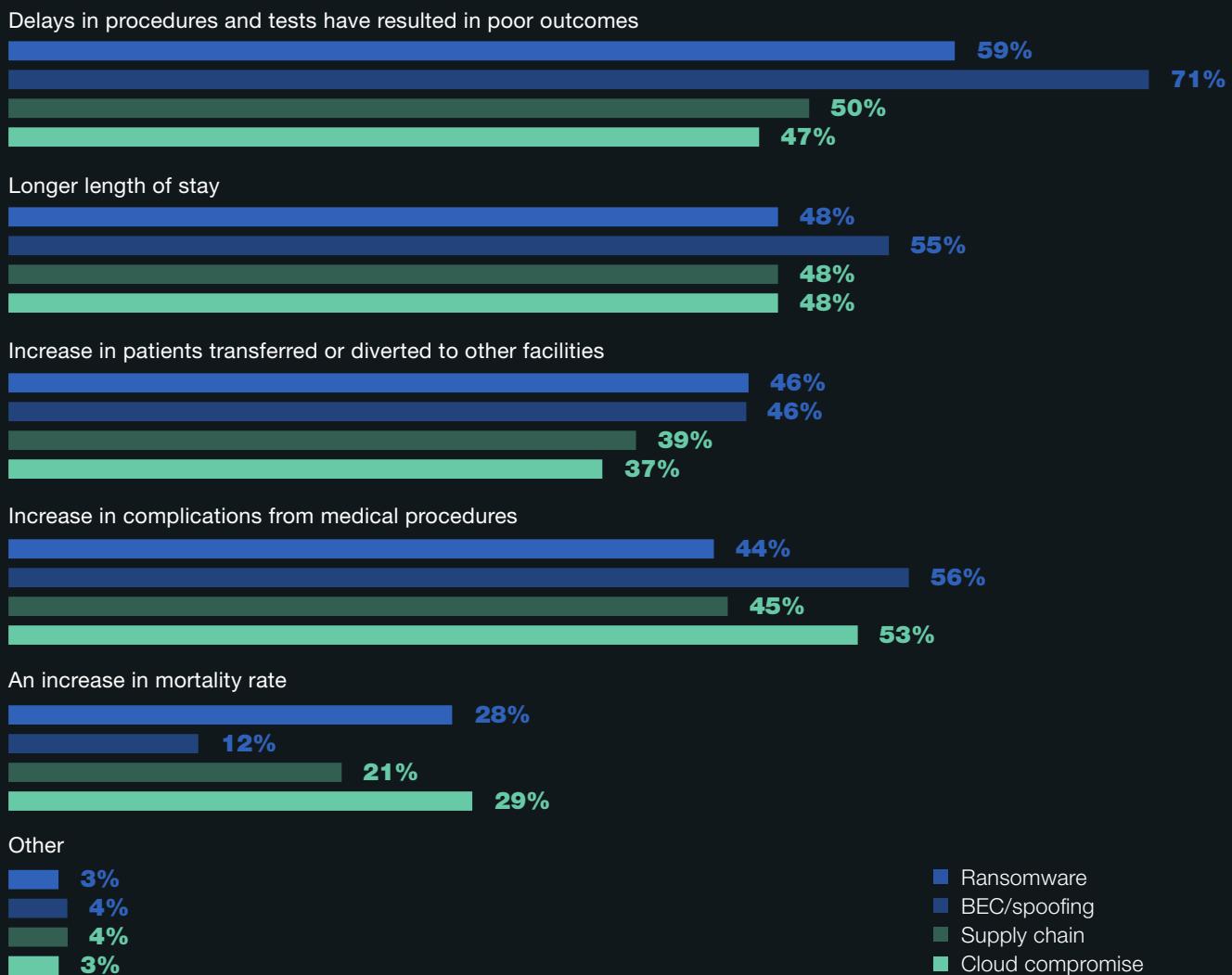


FIGURE 5.

If your organization experienced these cyberattacks, what impact did they have on patient care?

To protect patients, organizations need to reduce BEC/spoofing attacks. As shown in Figure 5, 71 percent of respondents in organizations that had a BEC/spoofing attack say it caused delays in procedures and tests that resulted in poor outcomes such as the increase in the severity of the illness. These attacks also were more likely to cause longer lengths of stay (55 percent) and increases in complications from medical procedures (56 percent). Cloud compromises and ransomware were more likely to increase mortality rates (29 percent and 28 percent, respectively).

More than one response permitted



THE COST OF CYBER INSECURITY

SYSTEM AVAILABILITY PROBLEMS AND DOWNTIME ARE THE MOST SIGNIFICANT FINANCIAL CONSEQUENCES FROM A CYBERSECURITY COMPROMISE.

Organizations also are spending more to ensure the impact on patient care is corrected.

TABLE 1.

Five average costs of a healthcare cybersecurity compromise

According to the research, 88 percent of organizations in this research experienced at least one cyberattack. In the past year, organizations experienced an average of 40 cyberattacks. As shown in Table 1, the average total cost for the single most expensive cyberattack was \$4,991,500 million, an increase from \$4,429,000. This includes all direct cash outlays, direct labor expenditures, indirect labor costs, overheard costs and lost business opportunities.

Respondents estimated that the highest cost (\$1.3 million) was caused by disruption to normal healthcare operations because of system availability problems, an increase from \$1 million in 2022. The cost due to users' idle time and lost productivity because of downtime or system performance delays was \$1.1 million, the same as in 2022. The cost caused by the time required to ensure the impact on patient care was corrected increased from an average of \$664,350 to \$1 million in this year's report.

Other changes were a decrease in damage or theft of IT assets and infrastructure from \$930,090 in 2022 to \$748,725 in 2023 and an increase in remediation and technical support activities from \$708,640 in 2022 to \$748,725 in 2023.

HEALTHCARE CYBERSECURITY COMPROMISE	2023 AVERAGE COST	2022 AVERAGE COST
Disruption to normal healthcare operations because of system availability problems	\$1,297,790	\$1,018,670
Users' idle time and lost productivity because of downtime or system performance delays	\$1,148,045	\$1,107,250
Time required to ensure impact on patient care is corrected	\$1,048,215	\$664,350
Damage or theft of IT assets and infrastructure	\$748,725	\$930,090
Remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients	\$748,725	\$708,640
Total	\$4,991,500	\$4,429,000

VULNERABILITIES IN THE CLOUD AND RISK TO PATIENT DATA

AS HEALTHCARE ORGANIZATIONS MOVE SENSITIVE PATIENT DATA TO THE CLOUD, RESPONDENTS RECOGNIZE THE RISKS.

FIGURE 6.

Which cloud-based user accounts/collaboration tools were most attacked in your organization?

Sixty-three percent of respondents say their organizations' cloud accounts were successfully compromised at some point. As shown in Figure 6, productivity tools, such as project management and videoconferencing tools, were the hardest hit (both 53 percent of respondents).

More than one choice permitted

Project management tools



Zoom/Skype/Video conferencing



Application/system-generated email



OneDrive/DropBox/Document/File-sharing tools



Teams/Slack/Office collaboration tools



Email



Text messaging



FIGURE 7.

How does your organization protect confidential or sensitive information in the cloud?

More organizations concerned about protecting sensitive data in the cloud are shifting to the use of premium security services from the cloud provider. As shown in Figure 7, the use of premium security service increased from 56 percent of respondents in 2022 to 60 percent in this year's research. The use of a CASB and encryption, tokenization or other cryptographic tools decreased significantly from 53 percent to 43 percent in 2023 and 65 percent to 59 percent in 2023, respectively.

More than one response permitted



FIGURE 8.

What best describes your organization's approach to user access and identity management in the cloud?

Organizations are likely to use a combination of several approaches to user access and identity management in the cloud. To secure access to patient data in the cloud there are specific methods to pursue. As in last year's research, a hybrid combination is still the most often used. Fifty-six percent in 2023 vs. 60 percent of respondents in 2022 say their organizations use a combination of approaches, according to Figure 8.

This is followed by separate identity management interfaces for the cloud and on-premises environments (50 percent in 2023 vs. 53 percent in 2022) and unified identity management interface for both the cloud and on-premises environments (43 percent in 2023 vs. 48 percent in 2022). The deployment of SSO has declined from 37 percent in 2022 to 30 percent in 2023.

More than one response permitted



FIGURE 9.

How would you characterize the data loss or exfiltration?

More progress is needed to achieve a healthier security posture. All healthcare organizations in this research have experienced at least one data loss or exfiltration incident involving sensitive and confidential healthcare data. The average number of such incidents is 19. As shown here, malicious insiders (32 percent of respondents) most often caused data loss and infiltration followed by accidental data loss (27 percent).

A common example of accidental data loss is mistakes made when employees are emailing documents. Almost half of respondents (47 percent) in this survey say their organizations are very concerned that employees do not understand the sensitivity and confidentiality of data they share by email.

Only one choice permitted

Malicious insiders



Accidental data loss



Employee negligence because of not following policies



Uncertain



FIGURE 10.

What impact did the data loss protection or exfiltration incident have on patient care?

Data loss or exfiltration can disrupt patient care and increase mortality rates. Forty-three percent of respondents say the data loss or exfiltration incident had an impact on patient care. Of these respondents, 46 percent of respondents say it increased mortality rates and 38 percent say it increased complications from medical procedures, as shown in Figure 10.

More than one response permitted

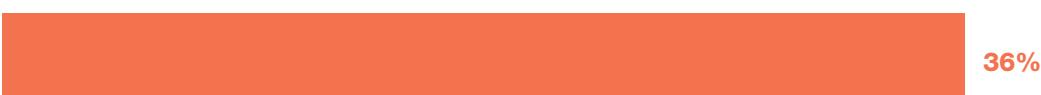
An increase in mortality rate



Increase in complications from medical procedures



Increase in patients transferred or diverted to other facilities



Delays in procedures and tests have resulted in



Longer length of stay



Other



FIGURE 11.

What security methods and technologies does your organization use to reduce the consequences of a data loss or exfiltration incident?

According to Figure 11, the top security methods and technologies used to reduce the consequences are a cloud access security broker (CASB) (67 percent of respondents). CASBs can be used to prevent unauthorized sharing of sensitive data that limit or allow access based on employee status or location. Fifty-four percent say their organizations deploy user and entity behavior analytics (UEBA). Fifty-one percent say their organizations have an enterprise data loss prevention platform that covers multiple channels, including email, web, network endpoint and cloud.

More than one response permitted

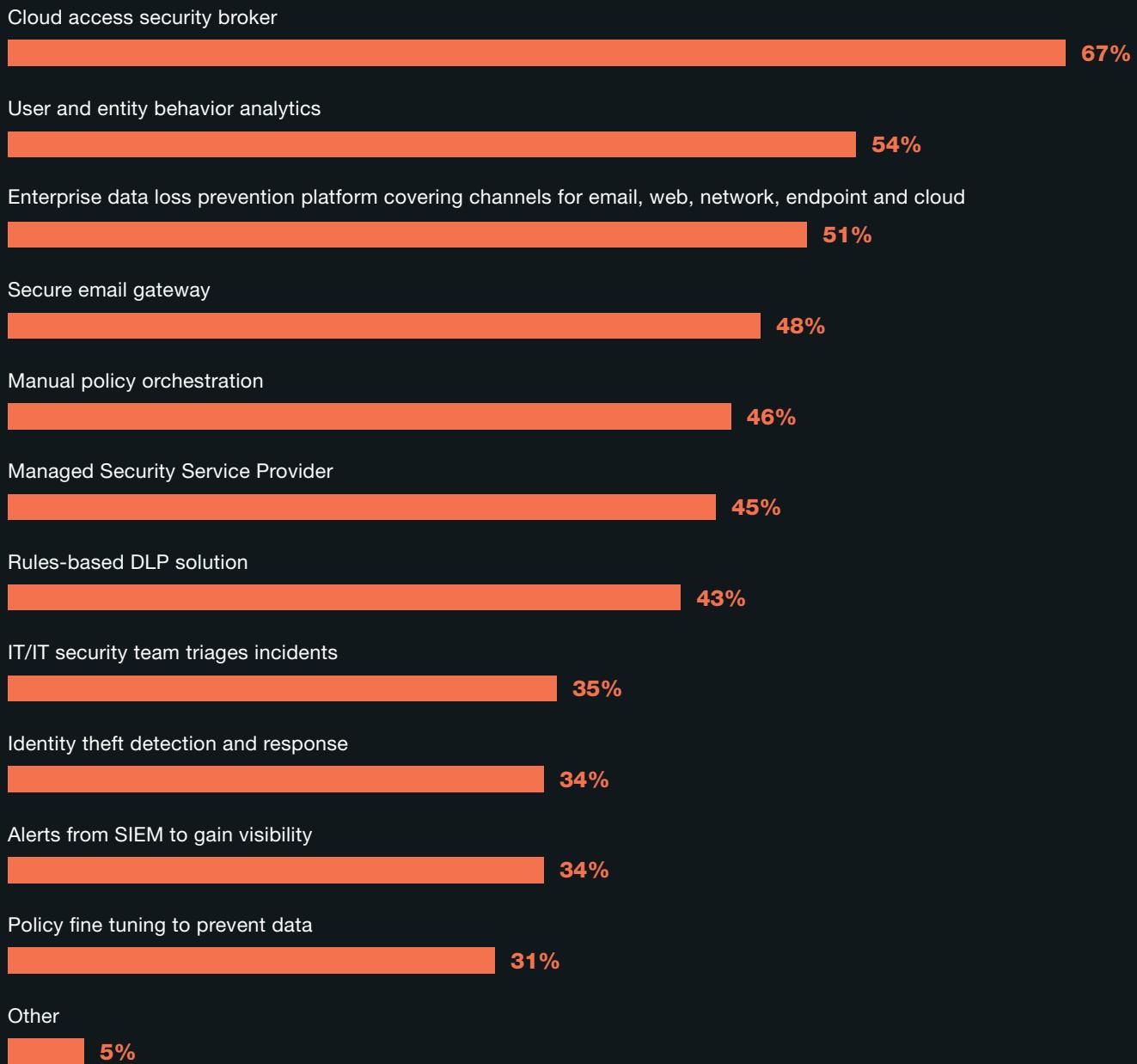
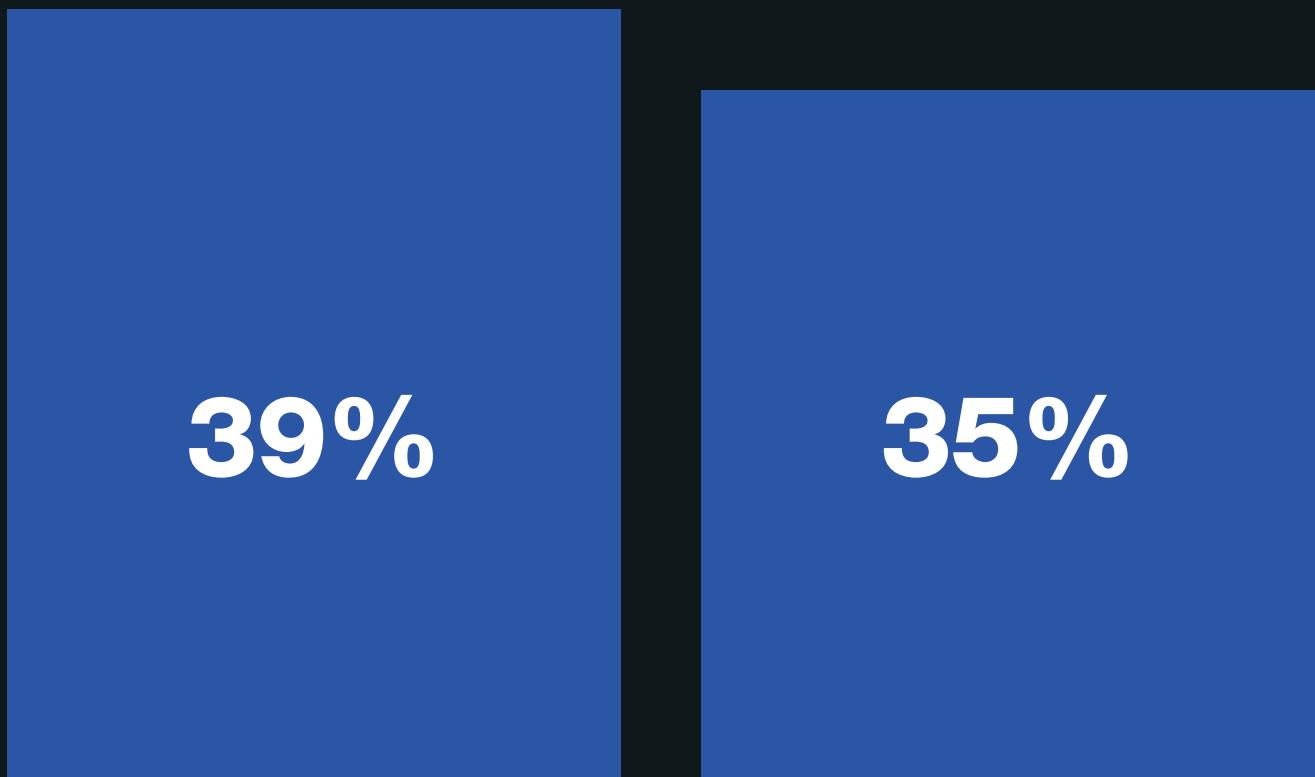


FIGURE 12.

How effective are your data loss prevention solutions in preventing data loss incidents by employees and malicious insiders?

New data loss prevention tools are needed. Respondents were asked to rate the effectiveness of their current solutions in preventing data loss incidents caused by malicious insiders and employees on a scale from 1 = not effective to 10 = very effective. Figure 12 presents the very effective responses (7+ on the 10-point scale). As shown, only 35 percent of respondents say their data loss prevention solutions are very effective in preventing data loss incidents caused by employees. Only 39 percent say these solutions are very effective in preventing data loss incidents caused by malicious insiders.

On a scale from 1 = not effective to 10 = very effective, 7+ responses presented



Effectiveness of current DLP solutions in preventing data loss incidents caused by malicious insiders

Effectiveness of current DLP solutions in preventing data loss incidents caused by employees

SOLUTIONS AND RESPONSES TO CYBER INSECURITY

THE LACK OF PREPAREDNESS TO STOP BEC/ SPOOF PHISHING AND SUPPLY CHAIN ATTACKS PUTS PATIENTS AT RISK.

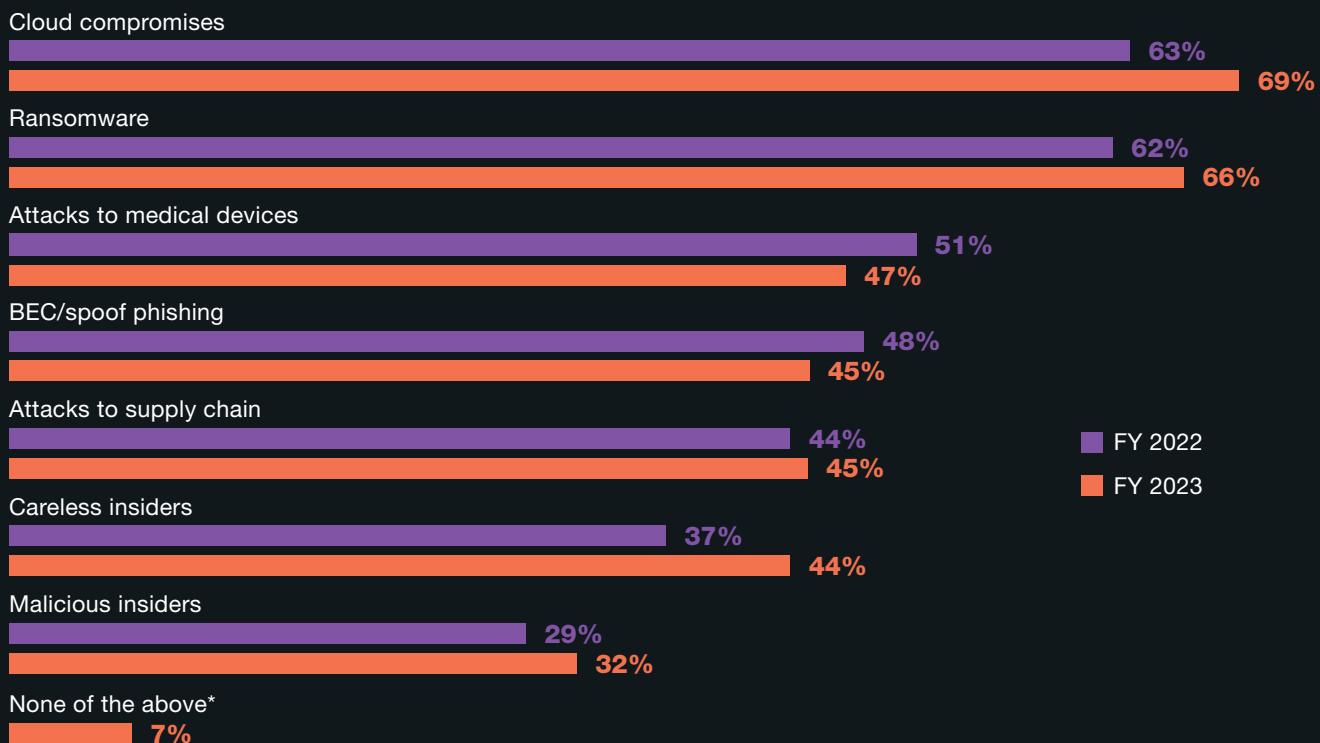
FIGURE 13.

Does your organization include the prevention and response to the following threats as part of its cybersecurity strategy?

According to Figure 13, most organizations focus on steps to prevent and respond to cloud compromises (69 percent of respondents) and ransomware attacks (66 percent).

While BEC/spoof phishing is considered a top cybersecurity threat to healthcare organizations only 45 percent of respondents say their organizations include prevention and response practices to such an attack as part of their cybersecurity strategy. Forty-five percent say they have documented the steps which prevent and respond to attacks to the supply chain. Only 32 percent say they are improving their ability to respond to attacks caused by malicious insiders, which is the primary cause of data loss and infiltration incidents.

More than one response permitted



*Not a response in FY 2022

FIGURE 14.

What challenges keep your organization's cybersecurity posture from being fully effective?

As the sophistication and frequency of cyberattacks increase, in-house expertise is more important than ever. However, as shown in Figure 14, 58 percent of respondents say their organizations lack in-house expertise (an increase from 53 percent in last year's research) and 50 percent say insufficient staff is a challenge. Lack of budget is also a factor (47 percent).

Three responses permitted

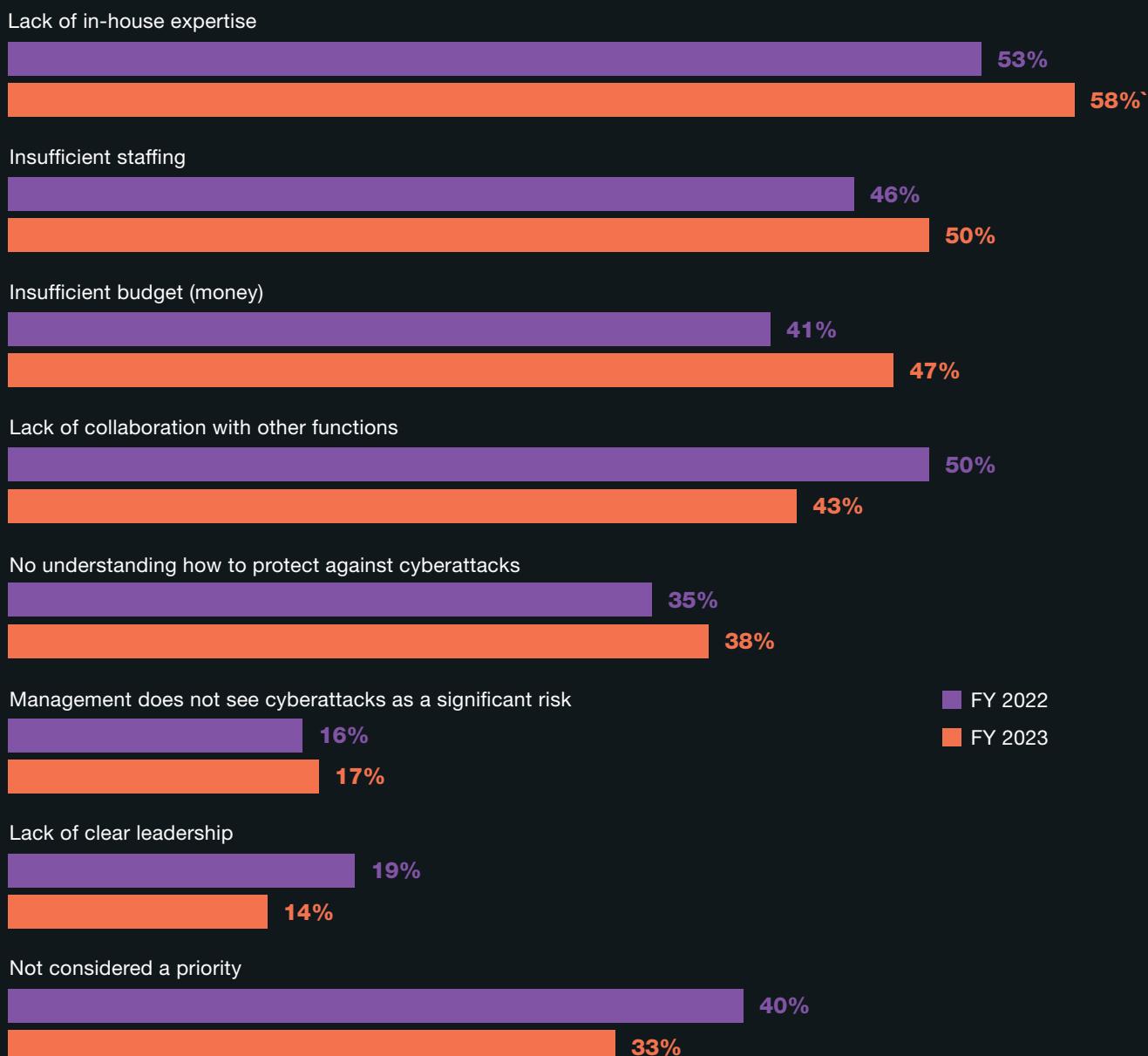


FIGURE 15.

Steps taken to reduce the risk of employees' lack of awareness

Security awareness training programs and employee monitoring are the top two steps taken to reduce the insider risk. More organizations (65 percent in 2023 vs. 59 percent in 2022) are taking steps to address the risk of employees' lack of awareness about cybersecurity threats.

As shown in Figure 15, of these respondents, 57 percent vs. 63 percent of respondents in 2022 say their organizations conduct a regular training and awareness program. Fifty-four percent vs. 59 percent in 2022 say their organizations monitor the actions of employees.

More than one response permitted

Regular training and awareness programs



Monitoring of employees



Audits and assessments of areas most vulnerable to employees' lack awareness



Simulations of phishing attacks



Include user's compliance with privacy and security policies in performance evaluations



Other



FIGURE 16.

Technologies used to reduce phishing and email-based attacks

The use of identity and access management to reduce phishing and email-based attacks increased significantly from 56 percent to 65 percent of respondents.

As shown in Figure 16, multi-factor authentication continues to be a primary solution to reducing phishing and email-based attacks (58 percent). Domain-based message authentication increased from 38 percent to 43 percent.

More than one response permitted

Identity and access management



Multi-factor authentication



Email data loss prevention



Domain-based Message Authentication



CASB



Web-isolation technology

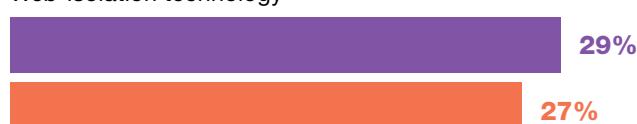
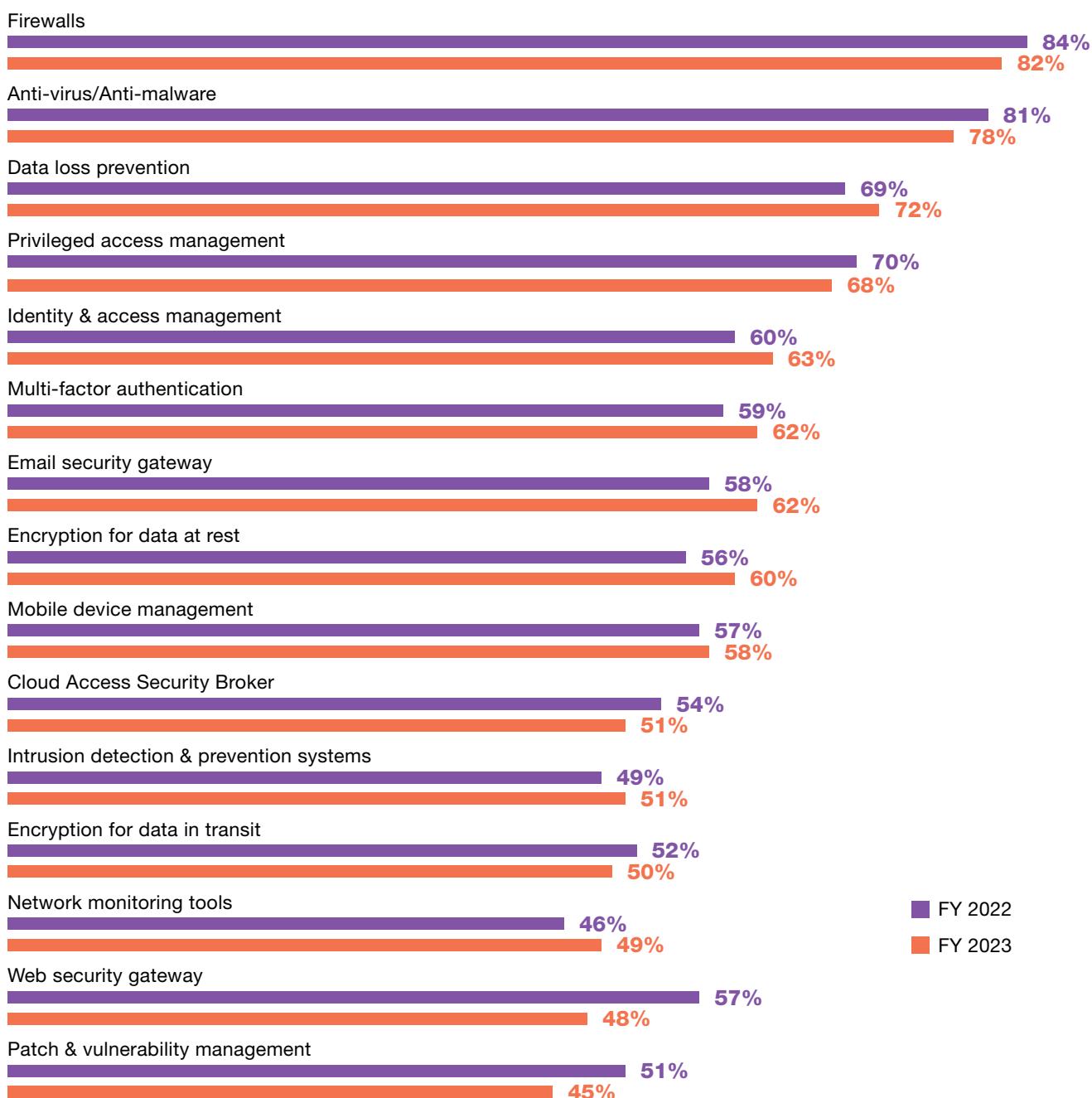


FIGURE 17.

The top technologies fully deployed to stop cyberattacks

The top technologies that organizations have fully implemented are shown in Figure 17. Since 2022, technologies fully deployed to stop cyberattacks have not changed significantly. As part of their cybersecurity strategy, the technologies most fully deployed are firewalls (82 percent of respondents), anti-virus/anti-malware (78 percent) and data loss prevention (72 percent). The use of web security gateways and patch & vulnerability management declined to 48 percent and 45 percent, respectively.

More than one response permitted



APPENDIX WITH THE DETAILED AUDITED FINDINGS

THE FOLLOWING TABLES PROVIDE THE FREQUENCY OR PERCENTAGE FREQUENCY OF RESPONSES TO ALL SURVEY QUESTIONS CONTAINED IN THIS REPORT.

All survey responses were captured in March 2023.

SURVEY RESPONSE	FY2023	FY2022
Total sampling frame	17,085	16,451
Total returns	715	698
Rejected returns	62	57
Total sample	653	641
Response rate	3.8%	3.9%

S1	WHICH OF THE FOLLOWING BEST DESCRIBES YOUR ROLE IN IT OR IT SECURITY WITHIN YOUR ORGANIZATION? (Check all that apply)	FY2023	FY2022
	Setting IT cybersecurity priorities	51%	46%
	Managing IT security budgets	45%	42%
	Selecting vendors and contractors	49%	47%
	Participating in IT cybersecurity strategies	51%	51%
	Evaluating and measuring effectiveness of cybersecurity strategies	36%	34%
	Managing cybersecurity risk	34%	36%
	Overseeing governance and compliance	27%	29%
	None of the above [Stop]	0%	0%

PART 1. CYBERSECURITY THREATS TO HEALTHCARE ORGANIZATIONS

Q1	WHAT CYBERSECURITY THREATS IS YOUR ORGANIZATION MOST CONCERNED ABOUT? (Please select the top six)	FY2023	FY2022
BEC/spoof phishing	62%	46%	
Cloud compromises	63%	57%	
Employee negligence or error	52%	58%	
Employee-owned mobile devices or BYOD	61%	34%	
Insecure medical devices	53%	64%	
Insecure mobile apps (eHealth)	51%	59%	
Malicious insiders	45%	37%	
Nation state attacks	19%	17%	
Process failures	31%	36%	
Ransomware	48%	60%	
Supply chain risks	40%	43%	
System failures	35%	36%	
Third-party misuse of patient data	26%	33%	
Use of public cloud services	11%	18%	
Other (please specify)	3%	2%	
Total	600%	600%	

Q2	DOES YOUR ORGANIZATION INCLUDE THE PREVENTION AND RESPONSE TO THE FOLLOWING THREATS AS PART OF ITS CYBERSECURITY STRATEGY? (Please check all that apply)	FY2023	FY2022
Attacks to medical devices	47%	51%	
Attacks to the supply chain	45%	44%	
BEC/spoof phishing	45%	48%	
Cloud compromises	69%	63%	
Malicious insiders	32%	29%	
Careless insiders	44%	37%	
Ransomware	66%	62%	
None of the above	7%		
Total	355%	334%	

Q3 WHAT CHALLENGES KEEP YOUR ORGANIZATION'S CYBERSECURITY POSTURE FROM BEING FULLY EFFECTIVE? (Please select the top three challenges)		FY2023	FY2022
Insufficient budget (money)		47%	41%
Insufficient staffing		50%	46%
Lack of in-house expertise		58%	53%
Lack of clear leadership		14%	19%
No understanding how to protect against cyberattacks		38%	35%
Management does not see cyberattacks as a significant risk		17%	16%
Lack of collaboration with other functions		43%	50%
Not considered a priority		33%	40%
Total		300%	300%
Extrapolated value		6.8	6.9
Q4 USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO BEC/SPOOFING PHISHING (From 1 = not vulnerable to 10 = highly vulnerable)		FY2023	FY2022
1 or 2		8%	11%
3 or 4		16%	13%
5 or 6		15%	12%
7 or 8		25%	24%
9 or 10		36%	40%
Total		100%	100%
Extrapolated value		6.8	6.9
Q5 USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO SUPPLY CHAIN ATTACKS (From 1 = not vulnerable to 10 = highly vulnerable)		FY2023	FY2022
1 or 2		2%	5%
3 or 4		11%	8%
5 or 6		24%	16%
7 or 8		23%	23%
9 or 10		40%	48%
Total		100%	100%
Extrapolated value		7.3	7.5

Q6 USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO RANSOMWARE ATTACKS (From 1 = not vulnerable to 10 = highly vulnerable)		FY2023	FY2022
1 or 2		5%	6%
3 or 4		10%	9%
5 or 6		21%	13%
7 or 8		26%	25%
9 or 10		38%	47%
Total		100%	100%
Extrapolated value		7.1	7.5
Q7 USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO CLOUD COMPROMISES (From 1 = not vulnerable to 10 = highly vulnerable)		FY2023	FY2022
1 or 2		5%	0%
3 or 4		6%	9%
5 or 6		15%	16%
7 or 8		40%	30%
9 or 10		34%	45%
Total		100%	100%
Extrapolated value		7.3	7.7
Q8 DID YOUR ORGANIZATION EVER EXPERIENCE A RANSOMWARE ATTACK?		FY2023	FY2022
Yes		54%	41%
No (please skip to Q16a)		44%	52%
Unsure (please skip to Q16a)		2%	7%
Total		100%	100%

Q9	HOW MANY RANSOMWARE INCIDENTS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	FY2023	FY2022
One		43%	53%
Two to five		34%	33%
Six to 10		16%	9%
More than 10		7%	5%
Total		100%	100%
Extrapolated value		3.7	3.0

Q10A	DID YOUR ORGANIZATION PAY THE RANSOM?	FY2023	FY2022
Yes		40%	51%
No		60%	49%
Total		100%	100%

Q10B	IF YES, HOW MUCH WAS THE RANSOM? (If your organization has had more than one ransomware attack, please select the costliest ransom paid)	FY2023	FY2022
Less than \$10,000		0%	2%
\$10,000 to \$25,000		13%	9%
\$25,001 to \$50,000		9%	7%
\$50,001 to \$75,000		14%	10%
\$75,001 to \$100,000		18%	17%
\$100,001 to \$250,000		11%	19%
\$250,001 to \$500,000		12%	18%
\$500,001 to \$1,00,000		9%	8%
\$1,00,001 to \$5,000,000		7%	5%
\$5,00,001 to \$10,000,000		4%	3%
More than \$10,000,000		3%	2%
Total		100%	100%
Extrapolated value		\$995,450	\$771,905

Question	Response	FY2023	FY2022
Q11A	DID THE RANSOMWARE ATTACK RESULT IN A DISRUPTION IN PATIENT CARE?		
Yes	68%	67%	
No	26%	30%	
Unsure	6%	3%	
Total	100%	100%	
Q11B	IF YES, WHAT IMPACT DID THE RANSOMWARE ATTACK HAVE ON PATIENT CARE?	FY2023	FY2022
An increase in mortality rate	28%	24%	
Delays in procedures and tests have resulted in poor outcomes	59%	64%	
Increase in complications from medical procedures	44%	48%	
Increase in patients transferred or diverted to other facilities	46%	50%	
Longer length of stay	48%	59%	
Other (please specify)	3%	3%	
Total	228%	248%	
Q12A	DID YOUR ORGANIZATION EVER EXPERIENCE A BEC/SPOOFING PHISHING ATTACK?	FY2023	FY2022
Yes	54%	51%	
No (please skip to Q14a)	41%	40%	
Unsure (please skip to Q14a)	5%	9%	
Total	100%	100%	
Q12B	IF YES, HOW MANY BEC/SPOOFING ATTACKS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	FY2023	FY2022
One	40%	49%	
Two to five	24%	31%	
Six to 10	19%	12%	
More than 10	17%	8%	
Total	100%	100%	
Extrapolated value	4.8	3.5	

Q13A DID THE BEC/SPOOFING ATTACK RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?		FY2023	FY2022
Yes		69%	67%
No		26%	30%
Unsure		5%	3%
Total		100%	100%
Q13B IF YES, WHAT IMPACT DID THE BEC/SPOOFING ATTACK HAVE ON PATIENT CARE? (Please select all that apply)		FY2023	FY2022
An increase in mortality rate		12%	21%
Delays in procedures and tests have resulted in poor outcomes		71%	60%
Increase in complications from medical procedures		56%	51%
Increase in patients transferred or diverted to other facilities		46%	45%
Longer length of stay		55%	48%
Other (please specify)		4%	2%
Total		244%	227%
Q14A DID YOUR ORGANIZATION EVER EXPERIENCE ATTACKS AGAINST ITS SUPPLY CHAIN?		FY2023	FY2022
Yes		64%	50%
No (please skip to Q16a)		30%	44%
Unsure (please skip to Q16a)		6%	6%
Total		100%	100%
Q14B IF YES, HOW MANY SUPPLY CHAIN ATTACKS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?		FY2023	FY2022
One		36%	44%
Two to five		33%	29%
Six to 10		21%	19%
More than 10		10%	8%
Total		100%	100%
Extrapolated value		4.2	3.9

Q15A	DID THE SUPPLY CHAIN ATTACKS RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	FY2023	FY2022
Yes		77%	70%
No		18%	24%
Unsure		5%	6%
Total		100%	100%

Q15B	IF YES, WHAT IMPACT DID THE SUPPLY CHAIN ATTACKS HAVE ON PATIENT CARE? (Please select all that apply)	FY2023	FY2022
An increase in mortality rate		21%	23%
Delays in procedures and tests have resulted in poor outcomes		50%	54%
Increase in complications from medical procedures		45%	48%
Increase in patients transferred or diverted to other facilities		39%	40%
Longer length of stay		48%	51%
Other (please specify)		4%	3%
Total		207%	219%

PART 2. PROTECTING THE CLOUD

Q16A	DID YOUR ORGANIZATION EVER EXPERIENCE A SUCCESSFUL CLOUD/ACCOUNT COMPROMISE?	FY2023	FY2022
Yes		63%	54%
No (Please skip to Q18)		33%	41%
Unsure (Please skip to Q18)		4%	5%
Total		100%	100%

Q16B	HOW MANY TIMES HAVE ATTACKERS COMPROMISED CLOUD-BASED USER ACCOUNTS WITHIN YOUR ORGANIZATION OVER THE PAST TWO YEARS?	FY2023	FY2022
	Once	0%	5%
	2 to 5	12%	9%
	6 to 10	14%	6%
	11 to 15	10%	9%
	16 to 20	21%	22%
	21 to 25	19%	22%
	26 to 50	16%	18%
	More than 50	8%	9%
	Total	100%	100%
	Extrapolated value	21.4	21.7
Q16C	WHICH CLOUD-BASED USER ACCOUNTS/COLLABORATION TOOLS WERE MOST ATTACKED IN YOUR ORGANIZATION? (Please select all that apply)	FY2023	
	Email	49%	
	Text messaging	45%	
	Zoom/Skype/Videoconferencing	53%	
	Teams/Slack/Office collaboration tools	49%	
	Project management tools	53%	
	OneDrive/DropBox/Document/file-sharing tools	49%	
	Application/system-generated email	51%	
	Total	349%	
Q17A	DID THE CLOUD COMPROMISES RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	FY2023	FY2022
	Yes	49%	64%
	No	40%	32%
	Unsure	11%	4%
	Total	100%	100%

Q17B	IF YES, WHAT IMPACT DID THE CLOUD COMPROMISES HAVE ON PATIENT CARE? (Please select all that apply)	FY2023	FY2022
An increase in mortality rate	29%	18%	
Delays in procedures and tests have resulted in poor outcomes	47%	49%	
Increase in complications from medical procedures	53%	51%	
Increase in patients transferred or diverted to other facilities	37%	37%	
Longer length of stay	48%	50%	
Other (please specify)	3%	2%	
Total	217%	207%	
Q18	HOW DOES YOUR ORGANIZATION PROTECT CONFIDENTIAL OR SENSITIVE INFORMATION IN THE CLOUD? (Please select all that apply)	FY2023	FY2022
We use private data network connectivity	40%	43%	
We use premium security services provided by the cloud provider	60%	56%	
We use encryption, tokenization or other cryptographic tools to protect data in the cloud	59%	65%	
We use a Cloud Access Security Broker (CASB)	43%	53%	
Don't know	18%	6%	
Other (Please specify)	5%	3%	
Total	225%	226%	
Q19	WHAT BEST DESCRIBES YOUR ORGANIZATION'S APPROACH TO USER ACCESS AND IDENTITY MANAGEMENT IN THE CLOUD ENVIRONMENT? (Please select all that apply)	FY2023	FY2022
Separate identity management interfaces for the cloud and on-premise environments	50%	53%	
Unified identity management interface for both the cloud and on-premise environments	43%	48%	
Deployment of single sign-on (SSO)	30%	37%	
Hybrid combination of the above choices	56%	60%	
Don't know	6%	5%	
Total	185%	198%	

PART 3. DATA LOSS PROTECTION SOLUTIONS TO REDUCE THE LOSS OR THEFT OF SENSITIVE HEALTHCARE DATA

Q20 HOW MANY DATA LOSS AND EXFILTRATION INCIDENTS INVOLVING SENSITIVE AND CONFIDENTIAL HEALTHCARE DATA OCCURRED WITHIN YOUR ORGANIZATION OVER THE PAST TWO YEARS? FY2023

Once	8%
2 to 5	5%
6 to 10	12%
11 to 15	24%
16 to 20	10%
21 to 25	23%
26 to 50	13%
More than 50	5%
Total	100%
Extrapolated value	19

Q21 HOW WOULD YOU CHARACTERIZE THE DATA LOSS OR EXFILTRATION? FY2023

Accidental data loss	27%
Employee negligence because of not following policies	25%
Malicious insiders	32%
Uncertain	16%
Total	100%

Q22A DID THE DATA LOSS OR EXFILTRATION RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS? FY2023

Yes	43%
No	51%
Unsure	6%
Total	100%

Q22B IF YES, WHAT IMPACT DID THE DATA LOSS PROTECTION OR EXFILTRATION INCIDENT HAVE ON PATIENT CARE?		FY2023
(Please select all that apply)		
An increase in mortality rate		46%
Delays in procedures and tests have resulted in poor outcomes		34%
Increase in complications from medical procedures		38%
Increase in patients transferred or diverted to other facilities		36%
Longer length of stay		24%
Other (please specify)		6%
Total		184%

Q23 WHAT SECURITY METHODS AND TECHNOLOGIES DOES YOUR ORGANIZATION USE TO REDUCE THE CONSEQUENCES OF A DATA LOSS OR EXFILTRATION INCIDENT? (Please select all that apply)		FY2023
(Please select all that apply)		
Rules-based DLP solution		43%
IT/IT security team triages incidents		35%
Policy fine tuning to prevent data loss		31%
Manual policy orchestration		46%
Alerts from SIEM to gain visibility		34%
Managed Security Service Provider (MSSP)		45%
Enterprise data loss prevention platform covering multiple channels for email, web, network, endpoint and cloud		51%
Cloud access security broker (CASB)		67%
User and entity behavior analytics (UEBA)		54%
Secure email gateway (SEG)		48%
Identity theft detection and response (IDTR)		34%
Other (please specify)		5%
Total		493%

Q24	HOW EFFECTIVE ARE YOUR CURRENT DATA LOSS PREVENTION SOLUTIONS IN PREVENTING DATA LOSS INCIDENTS CAUSED BY EMPLOYEES? (From 1 = not effective to 10 = very effective)	FY2023
1 or 2	18%	
3 or 4	33%	
5 or 6	14%	
7 or 8	16%	
9 or 10	19%	
Total	100%	
Extrapolated value	5.2	
Q25	HOW EFFECTIVE ARE YOUR CURRENT DATA LOSS PREVENTION SOLUTIONS IN PREVENTING DATA LOSS INCIDENTS CAUSED BY MALICIOUS INSIDERS? (From 1 = not effective to 10 = very effective)	FY2023
1 or 2	15%	
3 or 4	20%	
5 or 6	26%	
7 or 8	25%	
9 or 10	14%	
Total	100%	
Extrapolated value	5.56	
Q26	HOW CONCERNED IS YOUR ORGANIZATION THAT ITS EMPLOYEES DO NOT UNDERSTAND THE SENSITIVITY AND CONFIDENTIALITY OF DATA THAT THEY SHARE THROUGH EMAIL? (From 1 = not concerned to 10 = very concerned)	FY2023
1 or 2	15%	
3 or 4	17%	
5 or 6	21%	
7 or 8	25%	
9 or 10	22%	
Total	100%	
Extrapolated value	5.94	

PART 4. STEPS AND SOLUTIONS TO REDUCING CYBERSECURITY THREATS

Q27A	DOES YOUR ORGANIZATION TAKE STEPS TO ADDRESS THE RISK OF EMPLOYEES' LACK OF AWARENESS ABOUT CYBERSECURITY THREATS, ESPECIALLY BEC/SPOOFING PHISHING?	FY2023	FY2022
Yes		65%	59%
No		30%	35%
Unsure		5%	6%
Total		100%	100%

Q27B	IF YES, WHAT STEPS DOES IT TAKE? (Please select all that apply)	FY2023	FY2022
Regular training and awareness programs		57%	63%
Simulations of phishing attacks		40%	41%
Monitoring of employees		54%	59%
Audits and assessments of areas most vulnerable to employees' lack of awareness		43%	39%
Include user's compliance with privacy and security policies in performance evaluations		36%	35%
Other (please specify)		4%	3%
Total		234%	240%

Q28	WHAT TECHNOLOGIES DOES YOUR ORGANIZATION USE TO REDUCE PHISHING AND EMAIL-BASED ATTACKS? (Please select all that apply)	FY2023	FY2022
Domain-based Message Authentication (DMARC)		43%	38%
Web-isolation technology		27%	29%
Multi-factor authentication		58%	56%
Email data loss prevention		49%	52%
CASB		35%	41%
Identity and access management (IAM)		65%	56%
Total		277%	272%

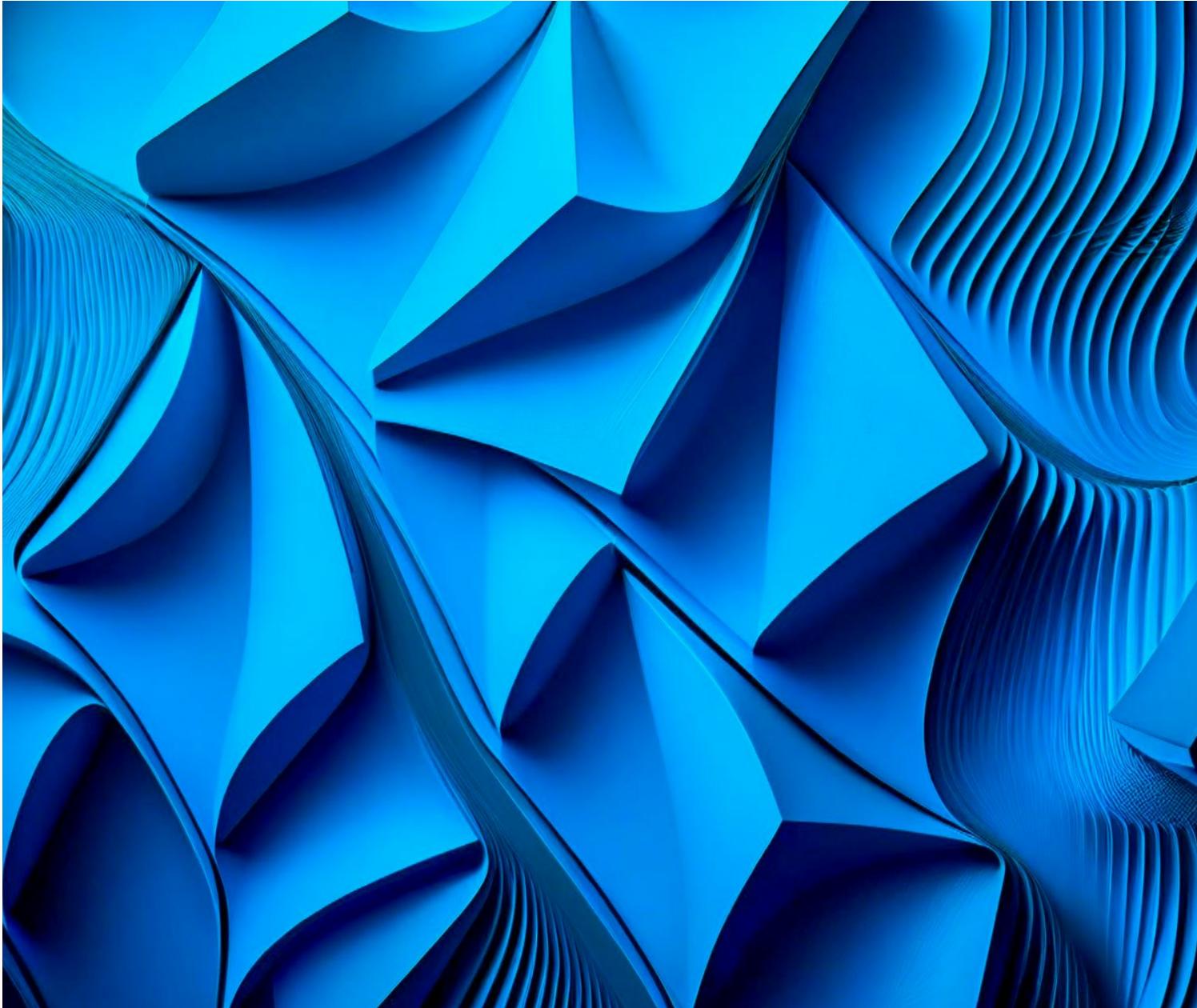
Q29	TO WHAT EXTENT HAS YOUR ORGANIZATION FULLY IMPLEMENTED THE FOLLOWING SECURITY TECHNOLOGIES? (Please select all that apply)	FY2023	FY2022
Anti-virus/anti-malware	78%	81%	
Firewalls	82%	84%	
Email security gateway	62%	58%	
Encryption for data in transit	50%	52%	
Network monitoring tools	49%	46%	
Web security gateway	48%	57%	
Intrusion detection & prevention systems (IDPS)	51%	49%	
Encryption for data at rest	60%	56%	
Patch & vulnerability management	45%	51%	
Multi-factor authentication	62%	59%	
Identity & access management	63%	60%	
Privileged access management	68%	70%	
Data loss prevention	72%	69%	
Mobile device management (MDM)	58%	57%	
Cloud Access Security Broker (CASB)	51%	54%	
Total	899%	903%	



Microsoft Digital Defense Report

Building and improving
cyber resilience

October 2023
Microsoft Threat Intelligence



Chapter 2

The State of Cybercrime

What we know about
cybercrime today

Key developments	13
Introduction	14
How the threat landscape is evolving	15
Ransomware and extortion	17
Phishing	27
Business email compromise	32
Identity attacks	34
Distributed denial of service attacks (DDoS)	38
Return on mitigation: Targeting investment to increase resilience	41



What we can learn from attack notifications

Managed extended detection and response (XDR) services, such as Microsoft Defender Experts, are invaluable resources for security operations centers to effectively detect and respond to critical incidents.

When we observe novel tactics, techniques, and procedures, human-directed attacks, or attack progression, notifications are sent to our customers to provide specific information regarding the scope, method of entry, and instructions for remediation.

Cybersecurity Tech Accord principles mapping index on page 124

Based on the notifications shared with customers, these are the top threats identified by Microsoft Defender Experts this year:

1 Successful identity attacks: Attacks across identity included traditional brute-force attempts, sophisticated password spray attempts across multiple countries and IP addresses, and adversary-in-the middle (AiTM) attacks.

➤ [For more about identity attacks, see page 34.](#)

2 Ransomware encounters: These are defined in this report as any instance of ransomware activity or attempted attacks that we have detected and prevented or alerted on, throughout the various stages of a ransomware attack.

In addition to several ransomware variants this year, we observed a unique large-scale ransomware campaign targeting both endpoints and cloud architecture of an organization. This was driven by the threat actor we named Mango Sandstorm. This campaign included both on-premises and cloud environments, and involved privilege escalation and destruction activities, including deletion of victim user resources, and persistence using OAuth applications. Attackers added a secret or certificate to an application in order to connect to Azure Active Directory (Azure

AD) as the application, and perform operations (such as reading confidential data and emails, exfiltrating information through emails) leveraging the application permissions that are assigned to it.

➤ [For more about ransomware see page 17.](#)

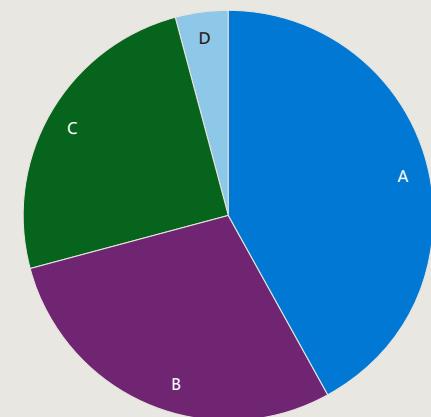
3 Targeted phishing attempts leading to device or user compromise: We have observed both malware phishing with intent to compromise devices, and AiTM phishing attempting to steal identities. Defense evasion techniques included phishing from compromised vendors and abuse of legitimate services.

➤ [For more about phishing and AiTM, see page 27.](#)

4 Business email compromise (BEC): Attackers used various methods including email conversation hijacking and mass spamming with malicious applications to commit financial fraud. They also sent phishing emails with harmful links and attachments from the victim's email address to other users within the victim's organization. Since these phishing emails were sent internally, multiple users fell victim to the attack by clicking on the links within a short period of time.

➤ [For more about BEC, see page 32.](#)

Distribution of top four attack progression notifications



(A) 42% Successful identity attacks (C) 25% Successful targeted phishing attempts
 (B) 29% Ransomware encounters (D) 4% Business email compromise (BEC)

Telemetry sources: Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Azure AD Identity Protection, Microsoft Defender Threat Intelligence

Additional information

Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft

Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity | Microsoft

Insights on ransomware and extortion

New tactics and trends

Microsoft's telemetry indicates that organizations faced an increased rate of ransomware attacks compared to last year, with the number of human-operated ransomware attacks up more than 200 percent since September 2022.

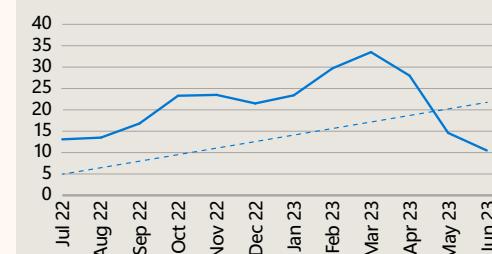
The good news is, for organizations with a strong security posture, the likelihood of an attack succeeding is very low. Typically, an attack is stopped in the pre-ransom phase, with on average 2 percent of attacks progressing to a successful ransomware deployment.

Approximately 40 percent of the ransomware encounters we detected in June were human-driven. Most of these attacks can be attributed

to 123 tracked ransomware-as-a-service affiliates. The number of affiliates grew by 12 percent in the last year, setting up conditions for human-operated ransomware attacks to continue to grow in 2024.

Ransomware breaches per month per 100,000 organizations

We observed an overall increase in successful ransomware attacks with a sharp decrease in March-April.



Telemetry sources: Microsoft Security Graph, Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Azure AD Identity Protection, Microsoft Defender Threat Intelligence

Remote encryption

In a notable change from last year, we observed a sharp increase in the use of remote encryption during human-operated ransomware attacks. Instead of deploying malicious files on the victim device, encryption is done remotely, with the system process performing the encryption, which renders process-based remediation ineffective. On average, 60 percent of human-operated ransomware attacks used remote encryption over the past year. This is a sign of attackers evolving to further minimize their footprint.

Initial attack vectors

The Microsoft Incident Response team responds to incidents and helps customers secure their most sensitive, critical environments. Based on findings during these engagements, the top three initial access vectors were fairly evenly split, showing criminals are consistently exploiting the same vectors: external remote services, valid accounts, and public facing applications.

We found that among external remote services, adversaries primarily leveraged unsecured remote desktop protocol (RDP) and virtual private networks (VPN). Threat actors attacking valid accounts, where the attacker somehow gained legitimate account credentials, were most often able to log in via Citrix.

Among vulnerable external facing applications, cybercriminals exploited vulnerabilities ranging from zero-day vulnerabilities to those that were two to three years old, with Zoho Java ManageEngine, Exchange, MOVEit, and PaperCut print management software among the top applications exploited.

Actionable insights

To safeguard against these attacks:

- 1 It is crucial to implement Zero Trust and least privilege principles.
- 2 The most efficient solutions are those that can instantly identify attackers by utilizing signals from devices, users, and the entire organization, and take automatic remedial measures across both managed and unmanaged devices.
- 3 It is essential to have a seamless method to restore encrypted files at the organizational level.

Additional information

[How automatic attack disruption works in Microsoft 365 Defender | Microsoft](#)

[Automatically disrupt adversary-in-the-middle attacks with XDR | Microsoft](#)

Insights on phishing

Adversary-in-the-middle phishing attacks

Adversary-in-the-middle (AiTM) is a longstanding technique used by threat actors to obtain credentials, session cookies or personal data, or to distribute malware.

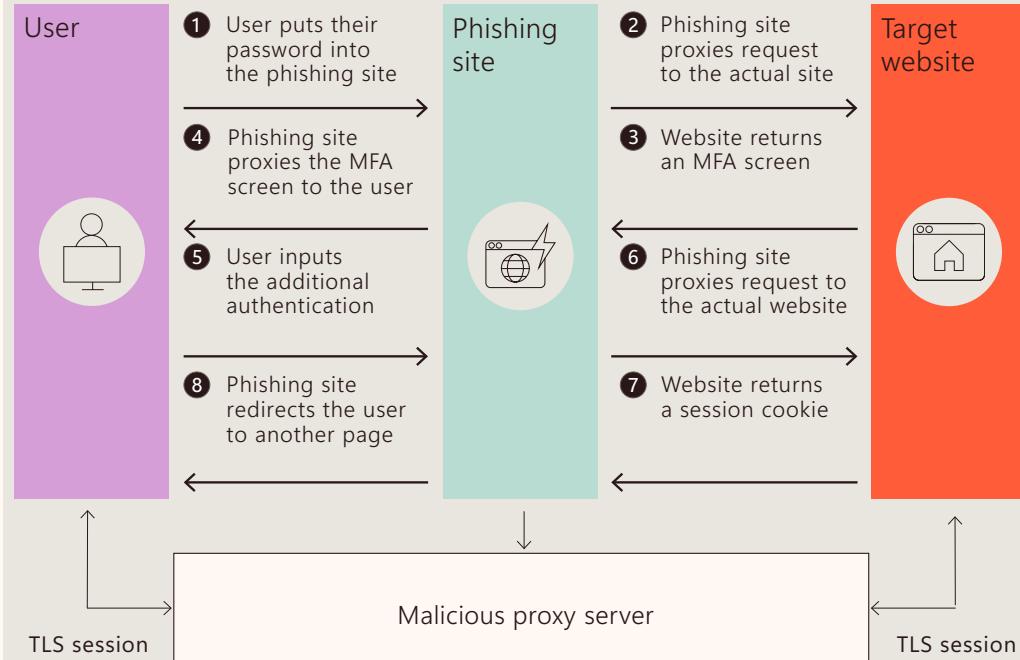
We have consistently observed a daily influx of high-volume AiTM phishing campaigns, with some instances involving millions of phishing emails sent within a 24-hour period. This trend of high-volume campaigns first appeared in September 2021 and we saw a significant surge in mid-July 2022, indicating an effort to bypass MFA on a massive scale.

Unlike traditional phishing attacks, revoking and

resetting user account credentials is not enough to address AiTM phishing incidents. The stolen session cookies also need to be revoked because session cookies, which are data stored in browsers, grant privileged access without repeated authentication.

During an AiTM phishing attack, a reverse proxy server is set up between the target and a legitimate login page. Reverse proxy servers sit between a client, such as a web browser, and a web server, forwarding information and requests between the client and the server. Reverse proxies are used legitimately for increasing security and performance but can also be used for malicious purposes such as AiTM attacks. The target unwittingly submits their credentials through the proxy, which triggers an MFA prompt on their mobile device. After the user inputs the authentication code, the proxy continues to deceive them by presenting subsequent MFA screens, relaying the user's input and allowing the attacker to access the account without the user's knowledge.

Anatomy of an AiTM phishing attack



The importance of MFA enablement on virtual private networks

For many years, VPNs have been used to enable secure remote access to company resources through encrypted tunnels. However, like any technology, ensuring compliance with an organization's security strategy requires proper configuration and alignment with a modern secure architecture, such as Zero Trust. Due to VPNs' widespread use in corporate networks and their accessibility from the internet, they have become common targets for attacks, often due to misconfigurations, such as insufficient monitoring of user accounts and devices. In a typical corporate setup, users are assigned separate VPN accounts with restricted access to the internal network.



Through our compromise recovery engagements, we found that almost half of VPN accounts lacked adequate MFA. Enabling MFA for these individual accounts is a crucial part of any VPN risk mitigation strategy. Other essential steps to secure these accounts include implementing conditional access, monitoring, and integrating security automation, if abuse of these accounts is detected.

Almost half of VPN accounts lacked adequate MFA.

In the month of June 2023 alone, we detected 158 million instances of password reuse across sites.

Source: Enhanced Phishing Protection with Microsoft Defender SmartScreen

Actionable insights

- 1 Use a unique password for each site.
- 2 Secure your devices and accounts with multifactor authentication.

Additional information

[Create and use strong passwords | Microsoft](#)

Insights on distributed denial of service attacks (DDoS)

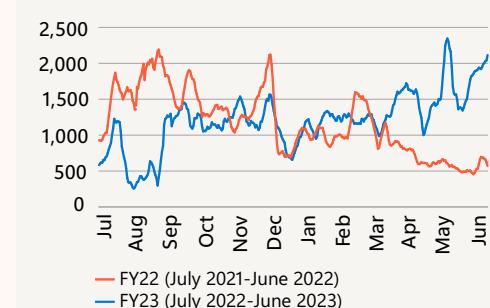
Battling a growing threat

Not only are DDoS attacks continuing to grow, they may be poised to have an even greater impact in the future. Our global DDoS mitigation operations combatted an average of 1,700 DDoS attacks per day in the past year.

In the previous year, we amplified our globally distributed mitigation capacity to handle and neutralize DDoS attacks at rates of up to 90 Terabits of data per second (Tbps). To put this into perspective, some of the largest attacks covered by the press in last years were in the range of several Tbps.

With a mitigation scale of 90 Tbps, we can mitigate the largest recorded attacks known, as well as multiple such attacks in parallel, to protect our cloud platform, reinforcing our commitment to maintaining a secure environment for our customers.

Comparison of DDoS attack patterns by average number of attacks



Source: Microsoft Global DDoS Mitigation Operations

DDoS for hire

DDoS-for-hire services—also known as booters, stressers, or ddosers—offer subscriptions to botnets for varying lengths of time, allowing users to flood target internet resources with large amounts of data.

This results in a denial of service. Since the attacks are launched from multiple networks, they are referred to as distributed denial of service attacks, or "DDoS". These services can be purchased for as little as \$5 USD and are increasingly being used as a cyberweapon in human operated ransomware attacks to exploit vulnerabilities in internet resources.

These services pose a significant risk to cybersecurity, serving as a powerful tool for cybercriminals. In today's world, where we rely heavily on online services, DDoS attacks can render platforms such as business productivity and gaming inaccessible. Additionally, these attacks can be used in triple-extortion human operated ransomware attacks to force victims to make payments,

potentially leading to the destruction of confidential and proprietary business data hosted on servers.

A notable achievement is the disruption by law enforcement of 48 DDoS-for-hire service platforms and legal action against six individuals involved.⁶ Such intervention plays a vital role in mitigating the impact of DDoS attacks by targeting the infrastructure and individuals supporting these illicit services.

The magnitude of the struggle is reflected in the fact that despite these achievements, the number of DDoS-for-hire platforms continues to rise, with 20 percent having emerged in the past year alone. This alarming trend emphasizes the necessity for continuous monitoring, tracking, and decisive action against these platforms. The DCU has taken a proactive stance by actively tracking and monitoring 14 DDoS-for-hire sites, including one situated in the dark web, as part of its commitment to identifying potential threats and remaining ahead of cybercriminals.

The number of DDoS-for-hire platforms continues to rise, with 20 percent having emerged in the past year alone.

A new era of cyberattacks: the rise of the botnets at scale

Last year marked a significant shift in cybercriminal tactics, with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks.

To minimize costs, they targeted discounted Azure subscriptions across various regions, establishing and commandeering subscription accounts at every opportunity. From January 2023 onwards, we noted that compromised subscriptions were generating resources in up to 40 Azure regions monthly, demonstrating the global reach for malicious botnets holding potential for targeting assets and organizations. Among these, the US regions were the most exploited, constituting around 70 percent of the falsely spawned resources, while Europe followed at 15 percent.

As the size of DDoS attacks increases, more and more cloud computing power is needed to absorb the leading wave of the attack until patterns can be identified, spurious traffic diverted, and legitimate traffic preserved. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks. In addition, due to the global distribution of the cloud, closer proximity helps to block attacks closest to the sources.



Microsoft Digital Crimes Unit

The healthcare sector as a target

This year, we observed an increase in daily DDoS attacks on the healthcare sector, particularly starting in January 2023. While the overall attack throughput is not very high, at around 100,000 packets per second 99 percent of the time, there was a significant spike of 14 million packets per second at its peak, with the attack intensity reaching a peak of almost 100 attacks per day in June. KillNet, a group that the US Department of Health and Human Services has assessed to be pro-Russia hacktivists, has been launching waves of DDoS

attacks against western countries, including with a focus on the healthcare sector.

The US Cybersecurity and Infrastructure Security Agency has collaborated with the FBI to develop guidance for DDoS response strategies to guide government agencies in protecting themselves against DDoS attacks.

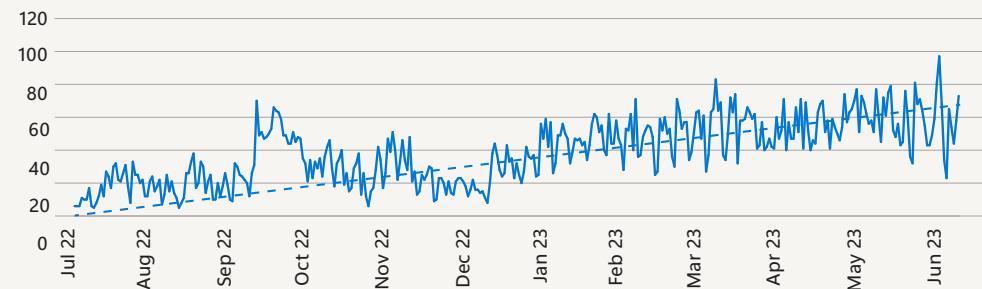
Additional information

[KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks | Microsoft](#)

[Understanding and responding to distributed denial of service attacks | CISA](#)

[HC3 provides tips for maintaining IoT security in healthcare | Health IT Security](#)

Daily DDoS attack volumes on healthcare applications



Source: Microsoft Global DDoS Mitigation Operations tracking healthcare applications in Azure

TCP attacks as the preferred vector

Transmission Control Protocol (TCP) has become the dominant attack vector, encompassing 59 percent of all DDoS attacks.

This shift toward TCP stems from the escalated activities of some hacktivist groups, who are increasingly turning their sights on web applications, bolstered by the rising adoption of DDoS-for-hire tools. In comparison, last year User Datagram Protocol (UDP) amplification and UDP flood attacks occupied most of the attack spectrum, comprising 51 percent of attacks while TCP was only 45 percent.

The predominance of UDP-led attacks in previous years, particularly targeting gaming applications, can be linked to the ripple effects of the COVID-19 pandemic. The enforced quarantines and lockdowns led to a surge in gaming's popularity, rendering these services a lucrative target for attackers.

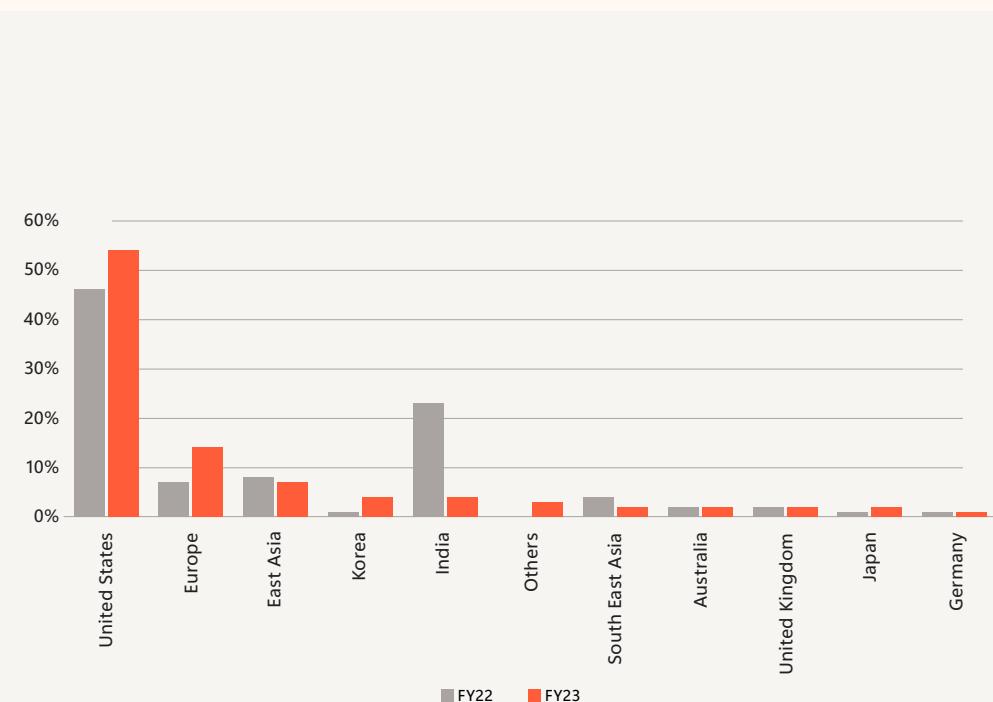
Attacks increase in the United States and Europe, shifting away from India

US entities have continued to be primary targets for DDoS attacks, bearing the brunt of 54 percent of all attacks. However, the past year has seen Europe climb to the second highest with 14 percent of attacks, overtaking East Asia. The change is tied to geopolitical conflicts, with pro-Russian hacktivist groups intensifying their onslaught against Europe and the United States. India, the second most attacked country last year, is now fifth.

Additional information

[What is a DDoS attack? | Microsoft Security](#)

Two-year comparison of top 10 most attacked regions



Source: Microsoft Global DDoS Mitigation Operations

Return on mitigation: Targeting investment to increase resilience

During Microsoft Incident Response engagements, customer environments have been found to lack mitigations that range from the simple to the more complex.

While the goal of all mitigations is to make environments more resilient to cyberattacks, customers may not always have the resources to implement all of them, and a return on mitigation framework is helpful for prioritization. Generally speaking, the lower the resources and effort involved, the higher the return on mitigation (ROM). As an example of a high return, consider a simple solution to implement context-based MFA protection. This solution is highly effective in preventing initial access (high security value) but very simple to implement (low effort). When implemented, this solution effectively prevents initial access by providing more context around the authentication attempt, such as geographic location and the application used. The additional context can be combined with requiring the user to enter a number (number matching) to complete MFA to further improve sign-in security.

Return on Mitigation scoring methodology

Return on Mitigation score = $(3x \text{ security value} + 2x \text{ potential user impact}) / \text{Potential ease of implementation}$

Return on Mitigation score	Type	Percentage of users potentially impacted	Score
10 – 15	Higher	Lower impact (<20% of users impacted)	3
6 – 9	Medium	Medium impact (Up to 50% users impacted)	2
2 – 5	Lower	Higher impact (>50% users impacted)	1

Engagement distribution (%) by major tactic	Score
50 – 100	3
25 – 49	2
0 – 24	1

Potential ease of implementation	Score
Easy to implement (20 hours or less)	1
Medium (20 – 40 hours)	2
Harder (40+ hours)	3

We have calculated ROM values using a formula multiplying the weighted impact of the solution or mitigation by a weighted value of the solution in terms of effectiveness (security value), and factored in the effort involved in implementing the solution. The higher the ROM score, the lower the resources and effort involved in implementing the solution for the impact and value provided.

The percentage of environments missing each of the mitigations across all the environments reviewed during incident response engagements is also included.

Return on mitigation: Targeting investment to increase resilience continued

**An example of a high ROM**

A customer used the same local administrator password for all Windows endpoints. When an attacker gained access to one endpoint, they were able to move laterally and gain administrative privileges on all endpoints because of the shared password. This led to privilege escalation within the Active Directory Domain Services (ADDS) domain and a total domain compromise. To prevent this type of lateral movement, the customer could have used a solution called Local Administrator Password Solution (LAPS) to randomize local administrator passwords across all endpoints. By doing so, the impact could have been contained to just one endpoint, and with other mitigations for privilege escalation, a total domain compromise could have been averted.

The most prevalent gaps we found during reactive incident response engagements were:

- Lack of adequate protection for local administrative accounts.
- A broken security barrier between on-premises and cloud administration.
- Lack of adherence to the least privilege model.
- Legacy authentication protocols.
- Insecure Active Directory configurations.

These gaps enable attacker tactics ranging from Initial Access to Lateral Movement and Persistence. To mitigate and protect against these tactics, we recommend randomizing local administrative account passwords, not synchronizing on-premises administrative accounts to the cloud, and having separate accounts and purpose-built hardened workstations for on-premises and cloud administration.

➤ **For more information about return on mitigation by techniques observed, please see page 43.**

We also recommend using just-in-time and just-enough administration in the cloud and on premises, separating daily use and administrative accounts, making an inventory of all applications using legacy authentication protocols, and modernizing those applications where possible and phasing out those that cannot be modernized.

Recommendations

Navigating evolving threats continued

Espionage operations increase and destructive operations decline

Nation-state and state-affiliated threat actor activities in the past year pivoted away from high-volume destructive attacks in favor of espionage campaigns. While the impact of destructive attacks is felt more immediately, persistent and stealthy espionage operations pose a long-term threat to the integrity of government, private industry, and critical sector networks.

Russian and Iranian state-sponsored actors that employed destructive attacks most frequently, changed the frequency of their destructive operations over the past year. At the same time, threat actors globally acted to increase their collection capacity against foreign and defense policy organizations, technology firms, and critical infrastructure organizations.

The high-volume of destructive attacks that dominated the early stages of Russia's invasion of Ukraine tapered off. Nearly 50 percent of destructive Russian attacks we observed against Ukrainian networks occurred in the first six weeks of the war.

➤ Please see 'About this Report' on page 9 for relevant definitions used in this chapter.

50%

of destructive Russian attacks we observed against Ukrainian networks occurred in the first six weeks of the war.

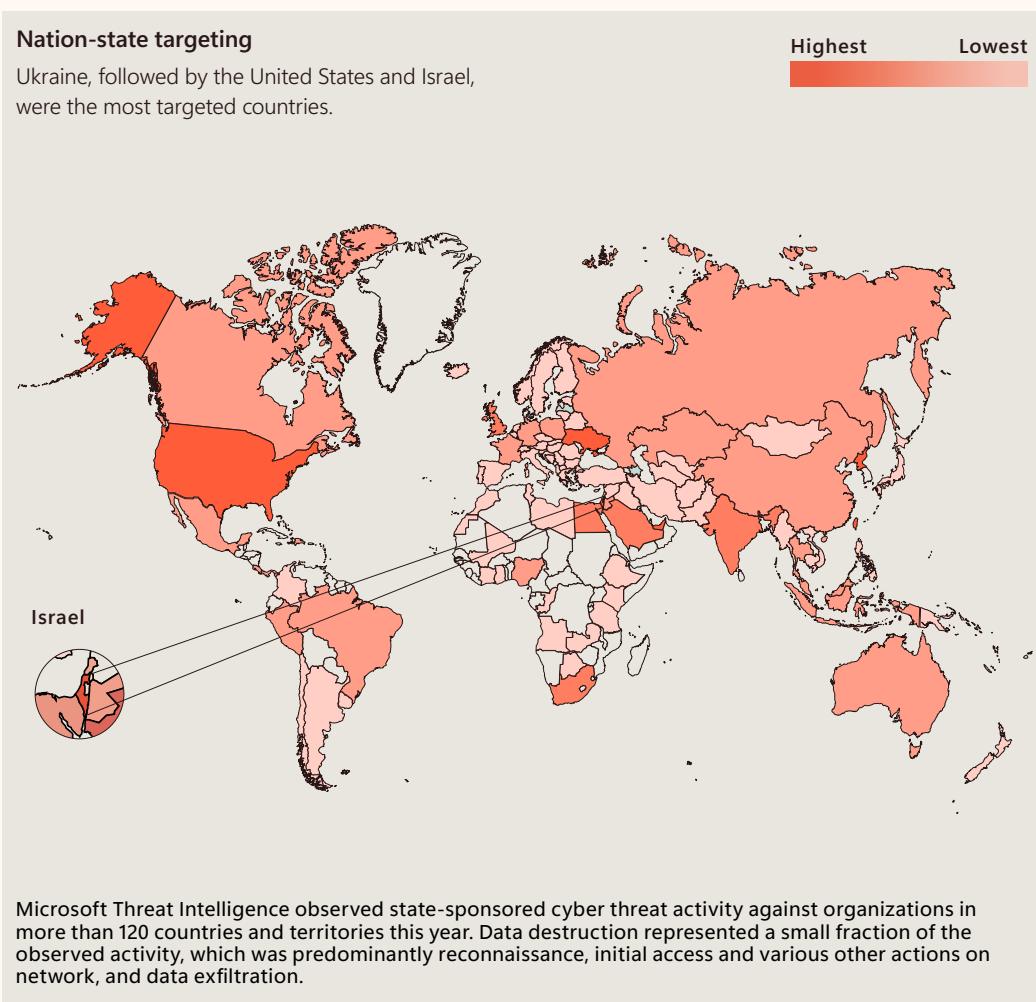
Later, in October and November 2022, Russian state actor Seashell Blizzard added destructive ransomware to its toolkit, deploying Prestige ransomware against a Polish entity, and Prestige and Sullivan ransomware against Ukrainian organizations.¹ The actor demonstrated consistent testing and development of the Sullivan payload, but Microsoft has not observed subsequent ransomware-style attacks from this threat actor.²

What Microsoft observed most often from Seashell Blizzard and other Russia-affiliate threat actors were phishing and password spray campaigns, credential theft, lateral movement through networks, data exfiltration, and other actions associated with gaining and retaining access to targets for intelligence collection.

➤ For more about Russian state actors' activity, see page 54.⁵

Nation-state targeting

Ukraine, followed by the United States and Israel, were the most targeted countries.



Microsoft Threat Intelligence observed state-sponsored cyber threat activity against organizations in more than 120 countries and territories this year. Data destruction represented a small fraction of the observed activity, which was predominantly reconnaissance, initial access and various other actions on network, and data exfiltration.

Navigating evolving threats continued

Increased sophistication enhances threat actors' capabilities

Iranian and North Korean state actors are demonstrating increased sophistication in their cyber operations, in some cases starting to close the gap with nation-state cyber actors such as Russia and China.

- **Iran:** Iranian state actors have increasingly migrated their cyber targeting and operations to focus on attacks that allow them to move from on-premises into cloud environments, representing a tangible increase in the maturity of their capabilities. In March, one group conducted a GoldenSAML attack, a technique only previously seen used by the highly sophisticated Russian group Midnight Blizzard, enabling Iranian operators to move from an on-premises site to a cloud environment. In February, another Iranian state actor moved laterally from an on-premises location to a cloud environment where it later conducted a destructive attack.

➤ **For more about Iranian state actor activity, see page 65.**

- **North Korea:** In early 2023, Ruby Sleet showed increasing sophistication by utilizing a stolen legitimate certificate of an IT security solutions provider to sign malicious files used to target organizations. In March, Citrine Sleet conducted a supply chain compromise leveraging a prior supply chain compromise, marking the first time Microsoft observed such an attack.⁶

➤ **For more about North Korean cyber operations, see page 70.**

- **Other adversarial cyber advancements:** Iranian partners and proxies also demonstrated consistent improvements in cyber operations since 2022, as highlighted in our 2022 report's disclosure of Plaid Rain's (POLONIUM) abuse of cloud services for command and control (C2) across most of its victims. In 2023, a Palestinian group delivered backdoors configured to enable rotation of C2 domains likely to evade detections.

➤ **For more about Palestinian threat actor activity, see page 73.**

Additional information

Please see our mitigation and protection guidance in this article published in May 2023:

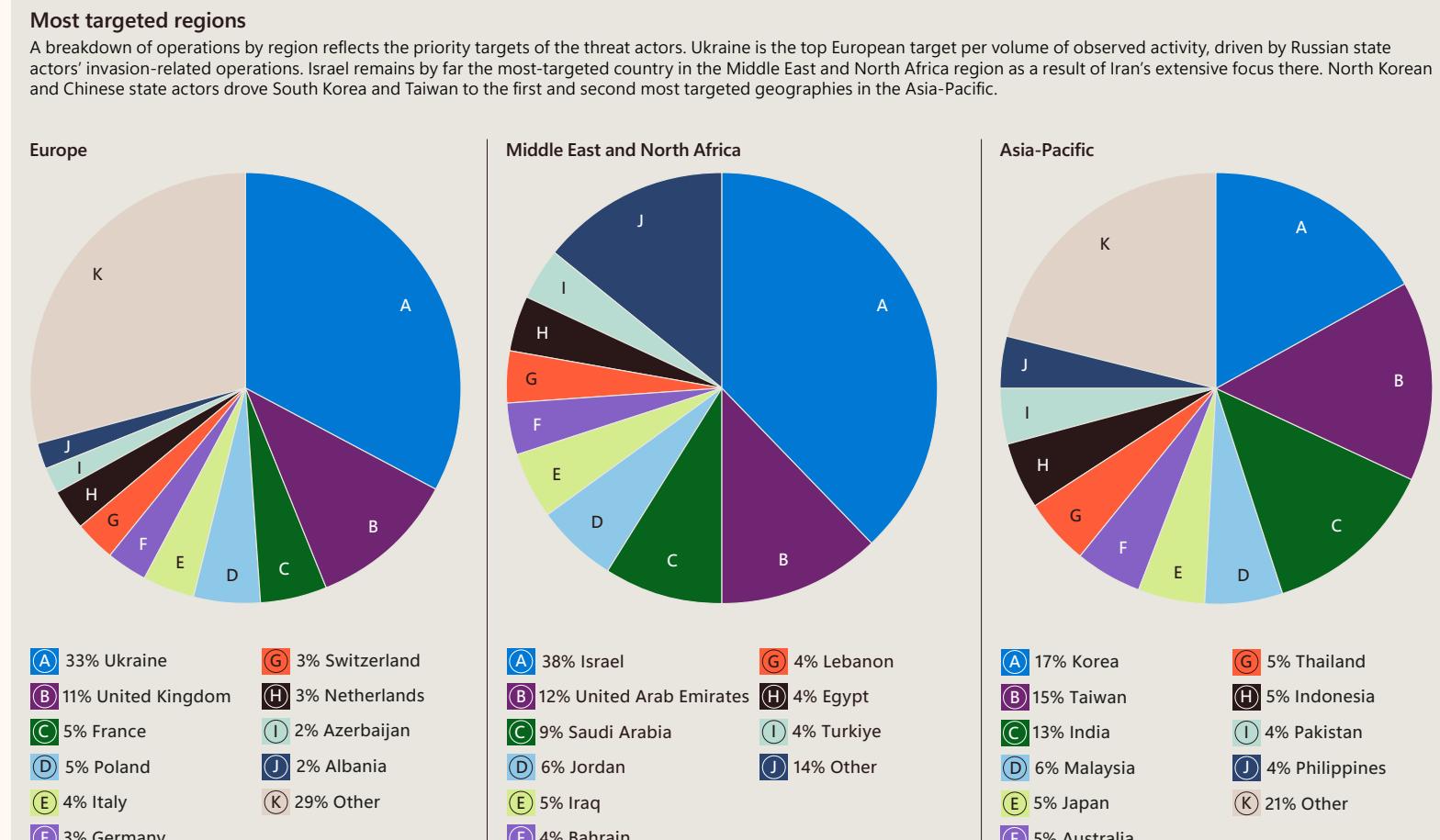
Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Security Blog

CSA Living off the Land.PDF | defense.gov

Navigating evolving threats continued

Threat actors are
expanding their
global target set

Nation-state actors' cyber operations grew increasingly global in scope this past year, particularly expanding in the Global South to more parts of Latin America and sub-Saharan Africa. While cyber operations remained most pronounced against the US, Ukraine, and Israel, and pervasive throughout Europe, operations increased in the Middle East owing to Iranian actors. Organizations involved in the policymaking and implementation ecosystem were among the most targeted, in line with many groups' espionage-focused remits.

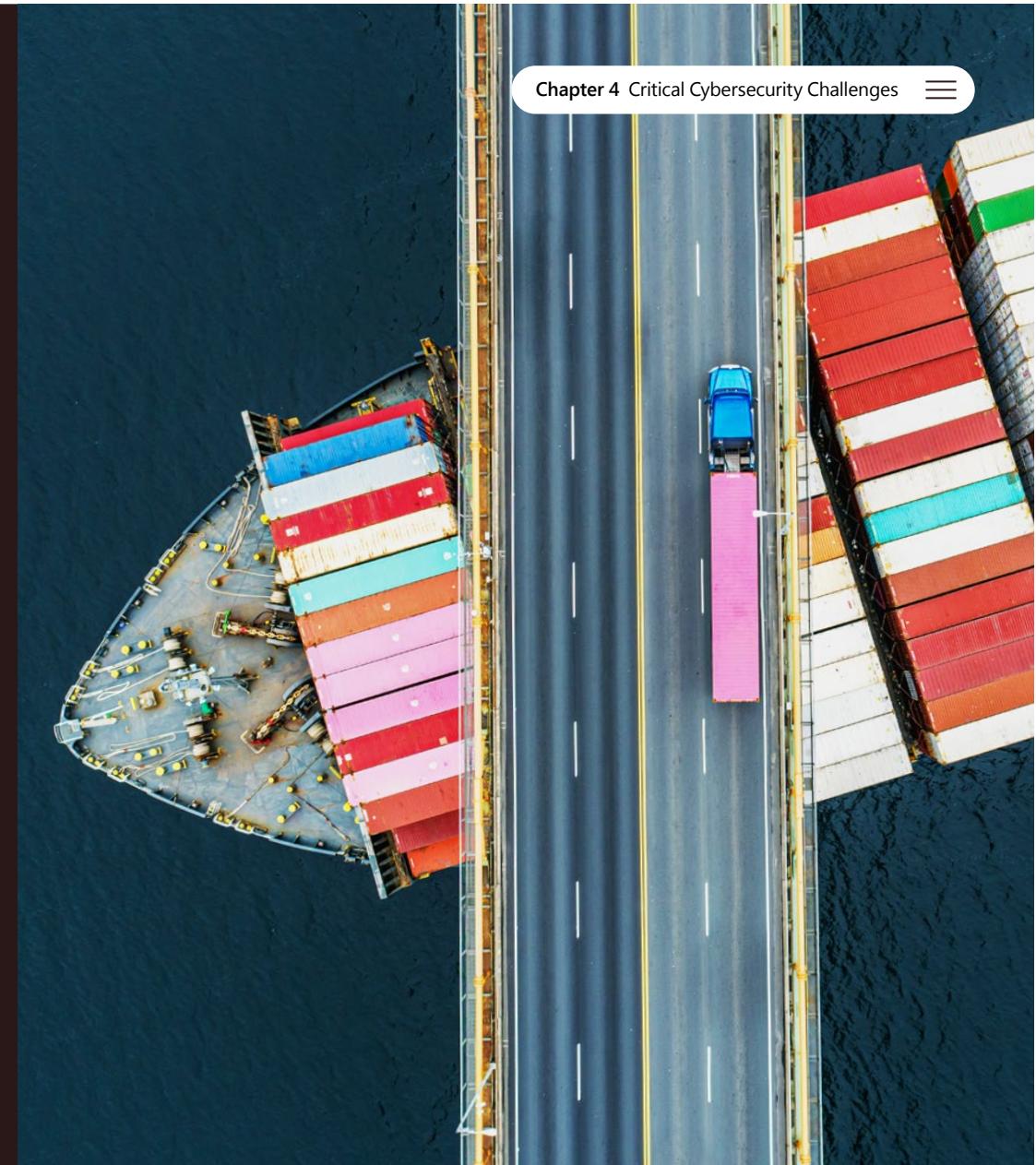


Source: Microsoft Threat Intelligence events data

Chapter 4 Critical Cybersecurity Challenges

Charting a path forward

Key developments	76
Introduction	77
The state of IoT and OT security	78
Improving global critical infrastructure resilience	86
Innovating for supply chain resilience	90



The state of IoT and OT security

IoT/OT security has undergone significant changes. Initially, systems were air-gapped, specialized, and isolated, which made them less attractive targets for attacks. However, as industrial systems started to connect with enterprise IT systems, the approach shifted towards greater network connectivity.

This transformation brought about new security guidelines, heavily influenced by the Purdue model aimed at mitigating the risks associated with increased interconnectedness.¹

In recent years, there has been a notable move towards centralized security in response to the growing complexity and diversity of assets within organizations.

This shift in approach acknowledges that OT is just one component of a broader ecosystem of unmanaged devices, encompassing IoT, OT, building management systems, and internet of medical things device technologies.

This recognition has paved the way for the development of new categories of IoT/OT security solutions such as deception, supply chain security, firmware analysis, and managed security services.

These emerging solutions aim to address the evolving challenges and threats posed by the interconnected nature of these devices, ensuring comprehensive protection across the entire ecosystem.

The expanding role of Chief Information Security Officer

The role of Chief Information Security Officer (CISO) has undergone a remarkable transformation as it expands beyond the traditional focus on securing information and users. Today, CISOs are entrusted with protecting all aspects of the connected business, including digital assets and cyber-physical and operational domains. The CISO's responsibility extends to safeguarding critical infrastructure, IoT/OT systems, and ensuring the continuity of operational processes. This expanded role reflects the growing recognition that cybersecurity must address the holistic protection of the entire business. In an era where the convergence of the digital and physical realms demands comprehensive security strategies and a deep understanding of the cyber-physical landscape, the CISO plays a pivotal role in the organization's resilience and success.



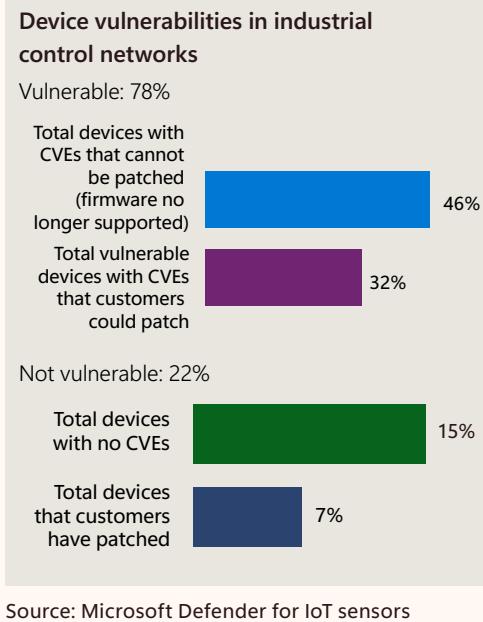
The state of IoT and OT security continued

Vulnerable devices susceptible to compromise

OT and industrial control system devices are frequently left unpatched and exposed, making them easy targets for hackers. Patching these systems can be challenging for organizations, as updates may need to be postponed to avoid disrupting operations.

Additionally, some OT devices lack patches for vulnerabilities, often due to discontinued support. Hackers can exploit vulnerable OT devices by using internet search tools to find ports used for remote management and gain unauthorized access, often using default credentials.

It is vitally important to know the status of your devices and to take steps to protect them from potential attacks.



25%

of OT devices on customer networks use unsupported operating systems, making them more susceptible to cyberattacks due to a lack of essential updates and protection against evolving threats.



Microsoft Defender for IoT actively monitors critical infrastructure device security to stay ahead of emerging threats. However, recent data reveals that 78% of devices on customer networks have known vulnerabilities that threat actors can exploit, and 46% of these devices cannot be patched.

Some OT devices still use unsupported operating systems, such as Windows 2000, which are no longer receiving security patches from Microsoft. Twenty-five percent of OT devices on customer networks use unsupported systems, making them more susceptible to cyberattacks due to a lack of essential updates and protection against evolving threats. This allows threat actors to exploit known vulnerabilities in unsupported OT devices, posing significant risks to critical infrastructure and industrial processes.

Pr Cybersecurity Tech Accord principles mapping index page 124

Actionable insights

- 1 Gain deeper visibility into IoT/OT devices and prioritize them based on their risk to the enterprise if compromised.
- 2 Reduce the attack surface by eliminating unnecessary internet connections, open ports, and restricting remote access using VPN services.
- 3 Ensure devices are robust by applying patches, changing default passwords, and modifying default SSH ports.

The state of IoT and OT security continued

Missing security patch deployment leaves systems vulnerable

Balancing robust cyber hygiene with uninterrupted operations in industrial and critical infrastructure environments is complex. One of the key challenges lies in effectively managing timely patch updates while maintaining peak system performance. This delicate equilibrium demands careful consideration, as overlooking the importance of cyber hygiene can leave vital systems vulnerable to malicious actors seeking to exploit weaknesses.

To examine how this balance is managed across a variety of programmable logic controllers (PLCs), we started by using Defender for IoT's on-premises network sensors to identify OT assets on a network, including vendor, model, and firmware version. Our focus was on a collection of widely used PLCs within the Defender for IoT customer base to determine the distribution of firmware versions deployed on the devices. To investigate device

vulnerabilities, we partnered aDolus Technology, a supply chain security company that uses machine learning algorithms to analyze manufacturer and industry disclosures and identify CVEs (publicly disclosed cybersecurity vulnerabilities) present in firmware.²

We found a significant lag between the availability of security fixes in firmware and their deployment onto the OT network. Although many of the PLC models showed a marked reduction in high confidence exploitable CVEs from older versions to the newest versions, over 60 percent of devices were still running older versions of the firmware with eight or more exploitable CVEs. If the latest version of the firmware available for these PLC models were to be deployed, the number of devices with no known exploitable CVEs would increase from four to 40 percent.

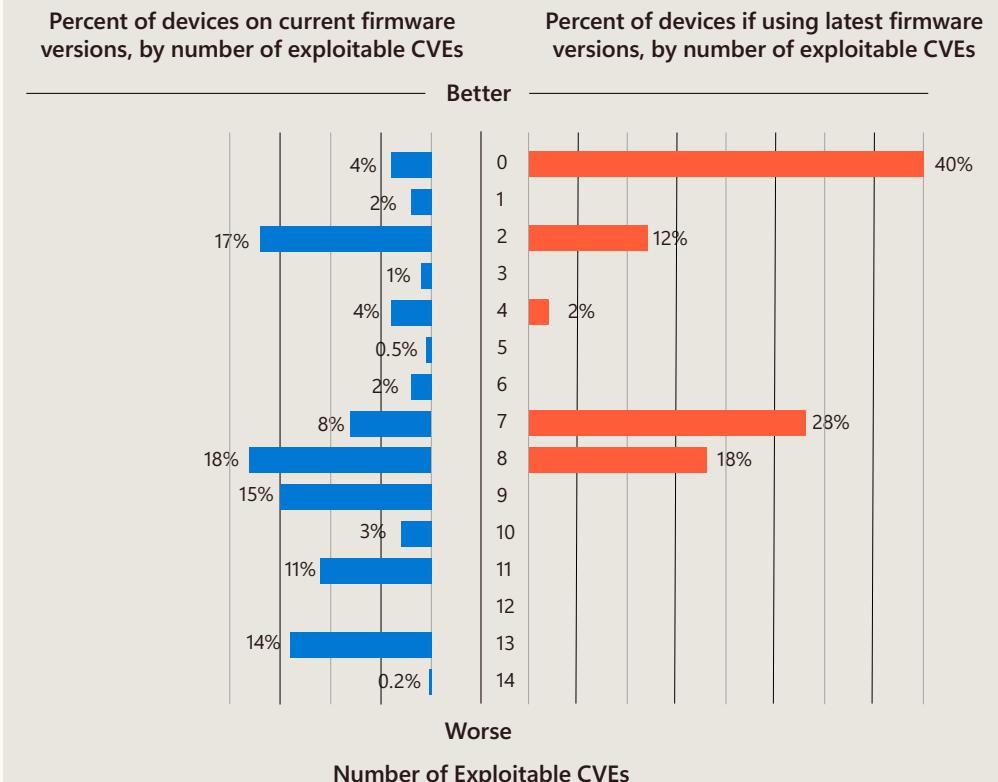
There are valid reasons for the delay in some devices receiving patches. Unlike traditional IT devices with regular "patch Tuesday" updates, OT devices have years-long patch cycles. It is not as simple as rebooting a PLC on the spot, especially when it manages a process that requires high availability. However, most facilities typically have annual or bi-annual maintenance outage windows that will allow for patching.

Deploying the latest firmware versions available for these PLC models could increase the percentage of devices with no known exploitable CVEs from

4-40%

OT common vulnerabilities and exposures (CVEs)

More than 60 percent of devices are on firmware versions that expose the devices to eight or more exploitable CVEs, even when some patches have been available for over five years.



Source: Microsoft Defender for IoT and aDolus Technology



The 2021 Cost of Phishing Study

Sponsored by Proofpoint

Independently conducted by Ponemon Institute LLC

Publication Date: June 2021

The 2021 Cost of Phishing Study

Presented by Ponemon Institute: June 2021

Part 1. Introduction

Ponemon Institute is pleased to present the results of *The 2021 Cost of Phishing Study* sponsored by Proofpoint. Initially conducted in 2015, the purpose of this research is to understand the risk and financial consequences of phishing. For the first time in this year's study we look at the threats and costs created by business email compromise (BEC), identity credentialing and ransomware in the workplace.

The key takeaway from this research is that the costs have increased significantly since 2015. Moreover, with the difficulty many organizations have in securing a growing remote workforce due to COVID-19, successful phishing attacks are expected to increase.

We surveyed 591 IT and IT security practitioners in organizations in the United States. Forty-four percent of respondents are from organizations with 1,000 or more employees who have access to corporate email systems.

The following findings reveal that phishing attacks are having a significant impact on organizations not only because of the financial consequences but also because these attacks increase the likelihood of a data breach, decrease employee productivity and increase the likelihood of a business disruption.

The cost of phishing more than tripled since 2015. The average annual cost of phishing has increased from \$3.8 million in 2015 to \$14.8 million in 2021. The most time-consuming tasks to resolve attacks are the cleaning and fixing of infected systems and conducting forensic investigations. Documentation and planning represent the least time-consuming tasks.

Loss of employee productivity represents a significant component of the cost of phishing. Employee productivity losses are among the costliest to organizations and have increased significantly from an average of \$1.8 million in 2015 to \$3.2 million in 2021. Employees are spending more time dealing with the consequences of phishing scams. We estimate the productivity losses based on hours spent each year by employees/users viewing and possibly responding to phishing emails averages 7 hours annually, an increase from 4 hours in 2015.

The cost of resolving malware infections has doubled total cost of phishing. The average total cost to resolve malware attacks is \$807,506 in 2021, an increase from \$338,098. Costs due to the inability to contain malware have more than doubled from an average of \$3.1 million to \$5.3 million.

Credential compromises increased dramatically. As a result, organizations are spending more to respond to these attacks. The average cost to contain phishing-based credential compromises increased from \$381,920 in 2015 to \$692,531 in 2021. Organizations are experiencing an average of 5.3 compromises over the past 12-month period.

Credential compromises not contained have more than doubled. The average total cost of credential compromised not contained is \$2.1 million and has increased significantly from \$1 million in 2015.

BEC is a security exploit in which the attacker targets employees who have access to an organization's funds or data. The average total cost of BEC's exploits was \$5.96 million (see Table 1a). Based on the findings, the extrapolated average maximum loss resulting from a BEC attack is \$8.12 million. The average total amount paid to BEC attackers was \$1.17 million.

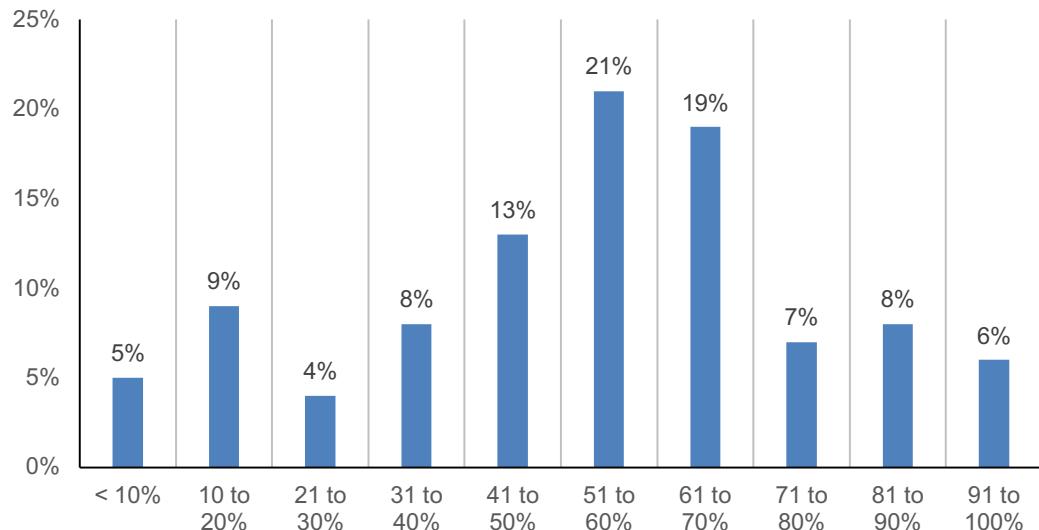
What is the cost of business disruption due to ransomware? Ransomware is a sophisticated piece of malware that blocks the victim's access to his/her files. The average total cost of ransomware last year was \$5.66 million (see Table 1a), and the average percentage rate of ransomware attacks from phishing was 17.6 percent.

Employee training and awareness programs on the prevention of phishing attacks can reduce costs. Phishing attacks are costing organizations millions of dollars. According to the research, the average annual cost of phishing scams is \$14.8 million, an increase from \$3.8 million in 2015.

Respondents were asked to estimate what percentage of phishing costs that could be reduced through training and awareness programs that specifically address the risks of phishing attacks targeting the workforce. As shown in Figure 1, the cost can be reduced by an average of more than half (53 percent) if training is conducted.

Figure 1. Percentage decrease in the cost of phishing attacks as a result of employee training interventions

Extrapolated value = 53%



Part 2. Key findings

In this section, we provide an analysis of the research findings. The complete audited findings are presented in the Appendix of this report. The report is organized according to the following topics.

- The cost of phishing scams and impact on employee productivity
- The cost of malware contained and not contained
- The cost of business disruption due to phishing
- The cost to contain and not contain credential compromises
- The cost of business email compromise (BEC)
- The cost of ransomware

The cost of phishing scams and impact on employee productivity

Loss of employee productivity represents a significant component of the cost of phishing. Table 1a presents the costs related to different types of phishing attacks.

The average annual cost of phishing has increased from \$3.8 million in FY2015 to \$14.83 million in 2021. As shown, productivity losses have increased significantly from \$1.8 million in 2015 to \$3.2 million in FY2021. Please note that information about BEC and ransomware was not available in FY2015. In the current study, we estimate an annual cost of phishing for BEC at \$5.97 million and ransomware at \$996 thousand.

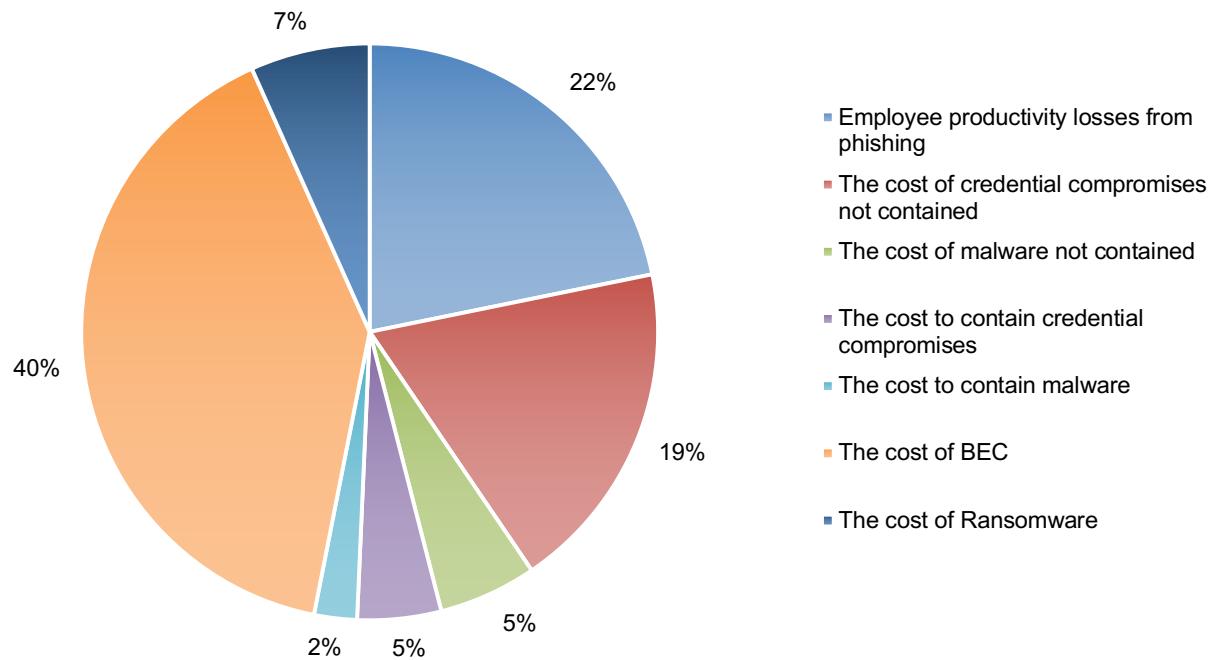
Table 1a. Phishing cost components	Estimated cost FY2015	Estimated cost FY2021
The cost to contain malware	\$208,174	\$353,582
The cost of malware not contained	\$338,098	\$807,506
Productivity losses from phishing	\$1,819,923	\$3,234,459
The cost to contain credential compromises	\$381,920	\$692,531
The cost of credential compromises not contained	\$1,020,705	\$2,776,340
Total original phishing cost components	\$3,768,820	\$7,864,418
Total cost of BEC		\$5,965,534
Total cost of ransomware from phishing		\$ 996,265
Extrapolated total cost of phishing		\$14,826,217

Table 2 summarizes the annual hours incurred for six tasks by the average-sized organization on an annual basis. The most time-consuming tasks to resolve phishing scams are the cleaning and fixing of infected systems and conducting forensic investigations. Documentation and planning represent the least time-consuming tasks.

Table 2. Six tasks to resolve attacks	Malware infections	Business email compromise	Ransomware	Credential theft
Planning	1,248	1,019	967	885
Capturing intelligence	4,892	4,450	3,889	3,630
Evaluating intelligence	4,282	5,001	4,200	5,411
Investigating	12,045	12,336	11,901	12,884
Cleaning & fixing	13,215	14,395	13,415	11,950
Documenting	951	1,075	913	1,002
Total hours	36,633	38,276	35,285	35,762

Pie Chart 1 shows the distribution of organizational costs caused by phishing scams (excluding BEC and ransomware). The top two cost categories are

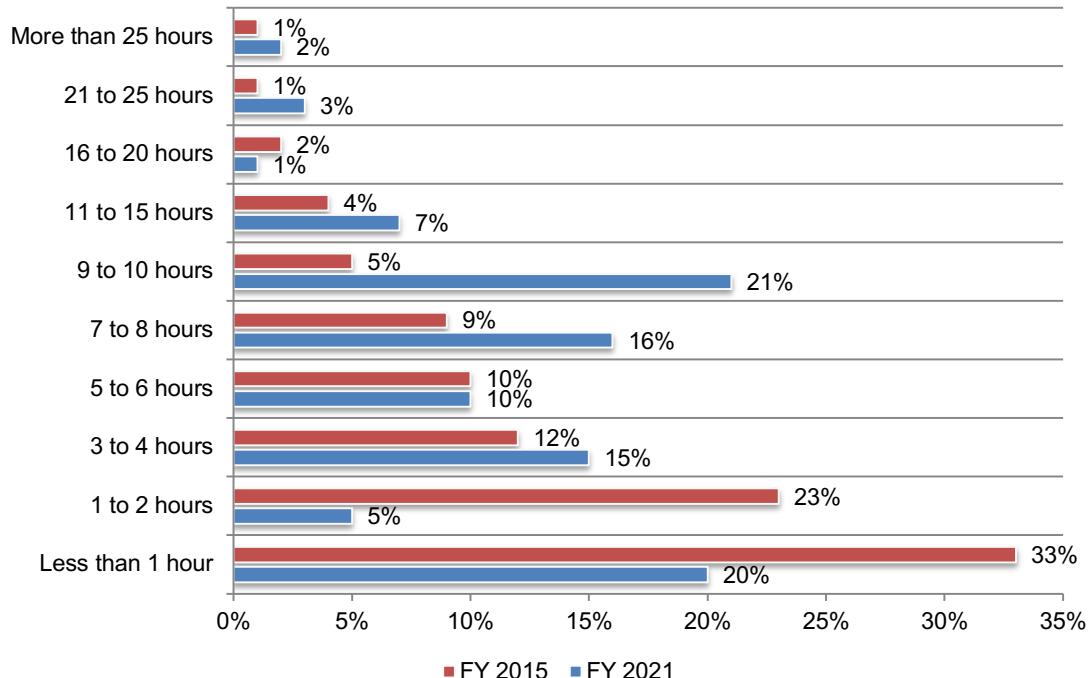
Pie Chart 1. Percentage distribution of phishing cost categories (as shown in Table 1)



Employees are spending more time dealing with the consequences of phishing scams. Figure 2 reports the distribution of time wasted for the average employee (office worker) due to phishing scams. The range of hours is less than 1 to more than 25 hours per employee each year. We estimate the productivity losses based on hours spent each year by employees/users viewing and possibly responding to phishing emails. As shown, each employee wastes an average of 7 hours annually due to phishing scams, an increase from 4 hours in 2015.

Figure 2. Estimated hours per employee each year spent dealing with phishing scams

Extrapolated hours per year in FY 2021 = 6.83
 Extrapolated hours per year in FY 2015 = 4.16



As discussed, the costliest consequence of a successful phishing attack is employees' diminished productivity. Table 3 reports the calculus used to estimate the productivity losses. Here we assume an average-sized organization with a headcount of 9,567 individuals with user access to corporate email systems. Based on an average of 7 hours per employee we calculate 65,343 hours wasted because of phishing. Assuming an average labor rate of \$49.5 for non-IT employees (users) we calculate a total productivity loss of \$3.2 million annually, an increase from \$1.8 million in 2015.

Table 3. Employee/user productivity losses	Calculus FY 2015	Calculus FY 2021
Extrapolated hours per employee each year	4.16	6.83
Average organization headcount (see Part 3)	9,552	9,567
Extrapolated hours per organization each year	39,736	65,343
Fully loaded average hourly rate for non-IT users*	\$45.80	\$49.50
Total productivity loss per year for the average-sized organization	\$1,819,923	\$3,234,459

*Source: Annual IT Security Benchmark Tracking Study, Ponemon Institute, March 2015

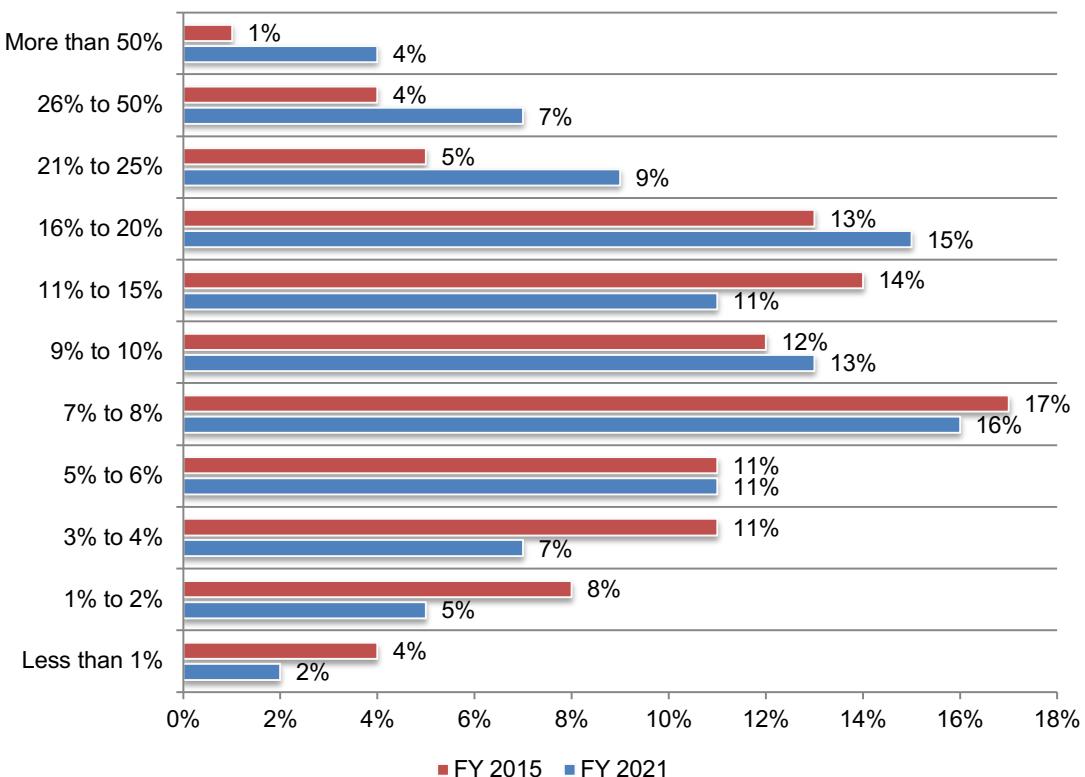
The cost of malware and malware not contained

An average of 15 percent of an organization's malware infections are caused by phishing scams. Respondents were asked to estimate the percentage of malware infections caused by phishing scams. As shown in Figure 3, the estimated range is less than 1 percent to more than 50 percent. The extrapolated average rate is 15 percent. As discussed above, the cost to contain malware is estimated to be \$353,582 (see Table 1).

Figure 3. Percentage rate of malware infections caused by phishing scams

Extrapolated rate FY 2021 = 15%

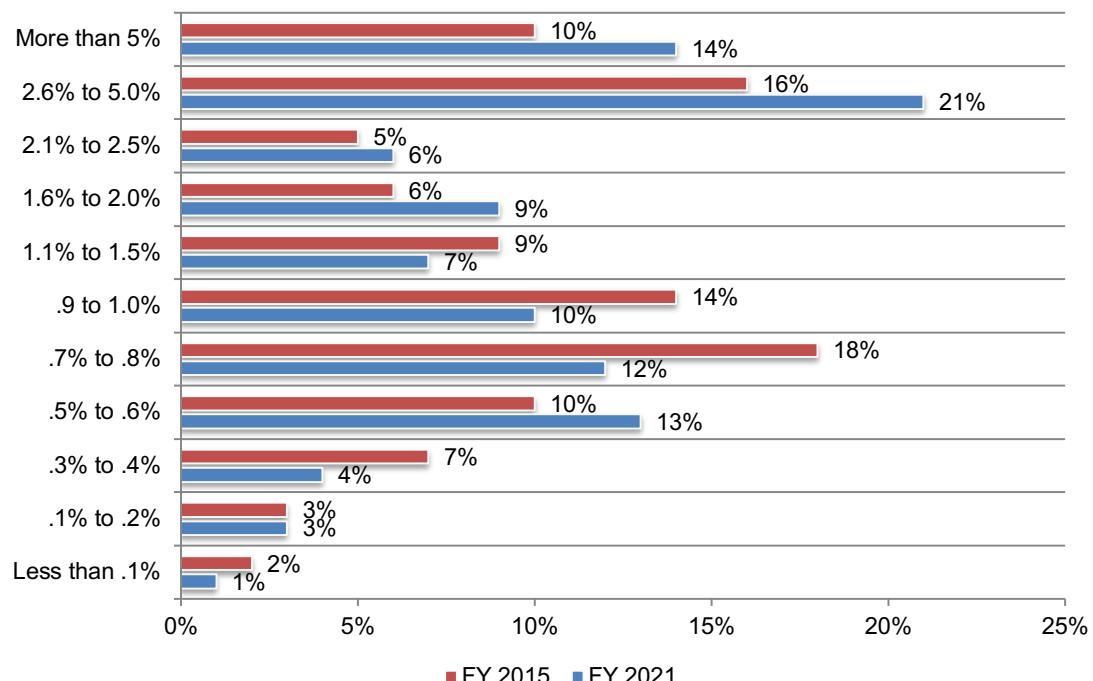
Extrapolated rate FY 2015 = 11%



The likelihood of a malware attack causing a material data breach due to data exfiltration has increased since 2015. In the context of this research, a material data breach involves the loss or theft of more than 1,000 records. Respondents were asked to estimate the likelihood of this occurring. According to Figure 4, the probability distribution ranged from less than .1 percent to more than 5 percent. The extrapolated average likelihood of occurrence is 2.3 percent over a 12-month period, an increase from 1.9 percent.

Figure 4. Likelihood of data exfiltration caused by a malware attack (over 12 months)

Extrapolated likelihood of occurrence in FY 2021 = 2.3%
 Extrapolated likelihood of occurrence in FY 2015 = 1.9%



The total cost attributable to malware attacks caused by phishing scams more than doubles. Table 3 reports the expected cost of malware attacks relating to data exfiltration at \$3.2 million and disruptions to IT and business processes at \$2.2 million. The total cost to resolve malware attacks is \$807,506 in 2021, an increase from \$338,098 in 2015.

Table 3. The expected cost of malware attacks	Calculus FY 2015	Calculus FY 2021
Probable maximum loss resulting from data exfiltration	\$105,900,000	\$137,170,000
Likelihood of occurrence over the next 12 months	1.9%	2.3%
Expected value	\$2,012,100	\$3,154,910
Probable maximum loss resulting from business disruptions (including denial of services, damage to IT infrastructure and revenue losses)	\$66,345,000	\$117,300,000
Likelihood of occurrence over the next 12 months	1.6%	2.1%
Expected value	\$1,061,520	\$2,157,630
Percentage rate of malware infections caused by phishing scams (see Figure 3)	11.0%	15.2%
Average cost of malware attacks	\$338,098	\$807,506

Phishing costs due to the inability to contain malware have more than doubled (see Table 1) and represents 11 percent of the total cost of phishing. Malware not contained is malware at the device level that has evaded traditional defenses such as firewalls, anti-malware software and intrusion prevention systems. Following are two attacks caused by an active malware attack that are difficult to contain: (1) data exfiltration (a.k.a. material data breach) and (2) business disruptions. The total cost of malware not contained has increased from \$3.1 million to \$5.3 million.

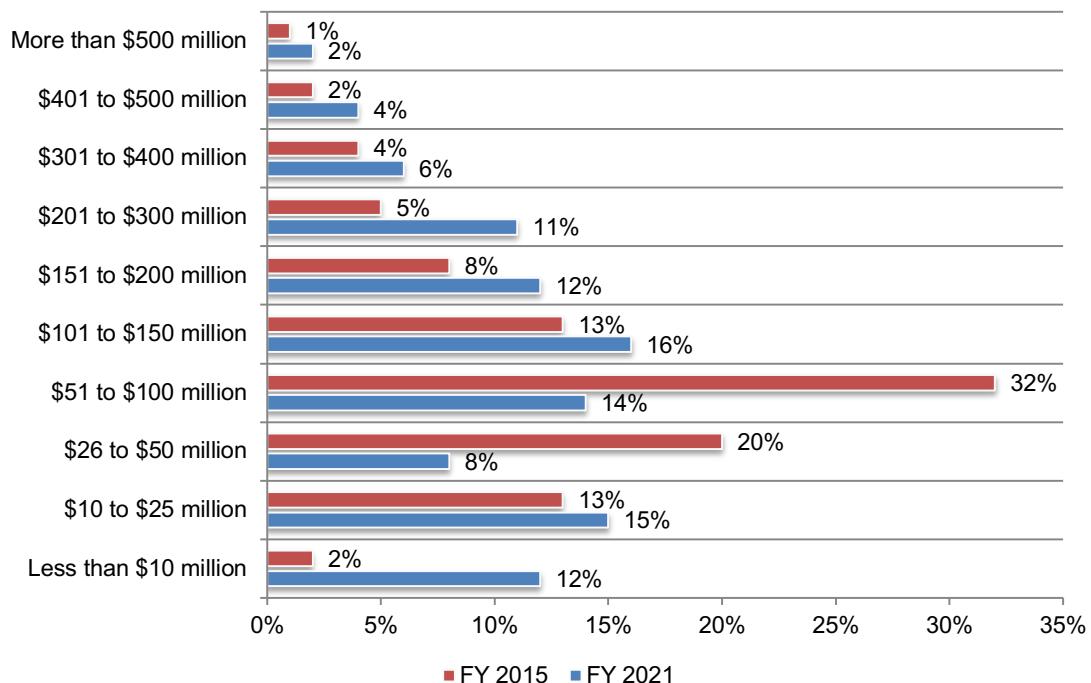
A malware attack resulting in a data breach due to data exfiltration could cost an organization an average of \$137.2 million. The following formula is used to determine the probable maximum loss (PML) and the likelihood of such an attack:

Expected cost = Probable maximum loss (PML) x Likelihood of occurrence [over a 12-month period].

Respondents in our survey were asked to estimate the probable maximum loss (PML) resulting from a material data breach (i.e., exfiltration) caused by an active malware attack.¹ Figure 5 shows the distribution of maximum losses ranging from less than \$10 million to more than \$500 million. The extrapolated average PML resulting from data exfiltration is \$137.2 million, an increase from \$105.9 million in 2015.

Figure 5. Maximum loss resulting from data exfiltration caused by a malware attack

Extrapolated PML FY 2021 = \$137.2 million
 Extrapolated PML FY 2015 = \$105.9 million



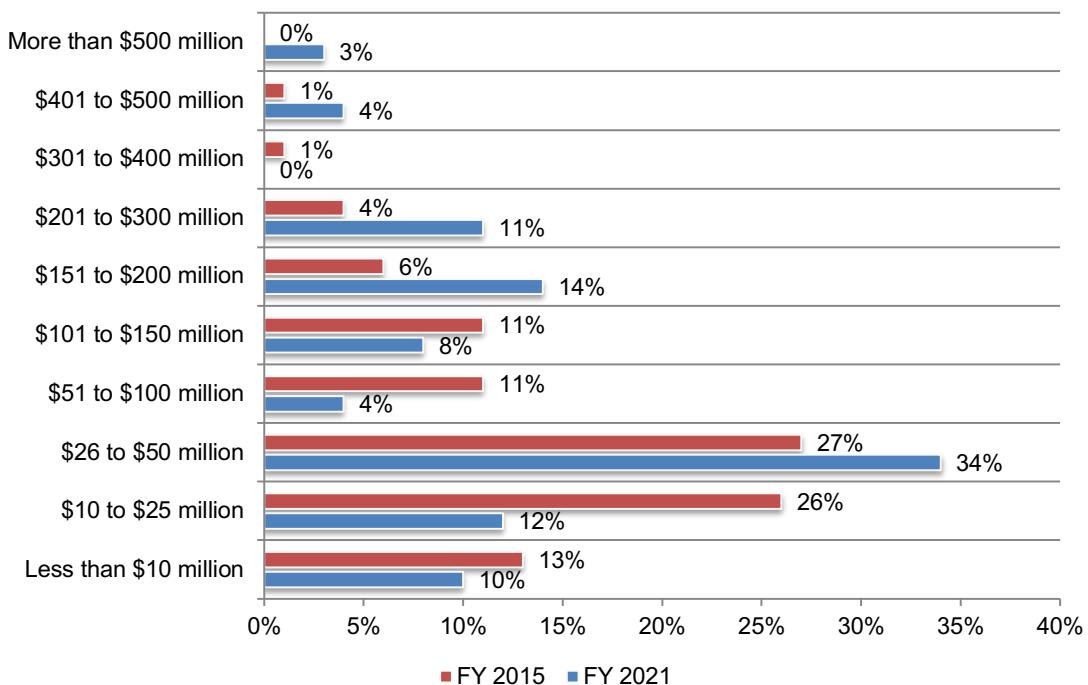
¹Probable Maximum Loss (PML) is defined as the value of the largest loss that could result from cyber attacks, assuming the normal functioning of perimeter controls and other commonly deployed security technologies. Insurance companies frequently use PML to determine risk exposures.

What is the cost of business disruption due to a malware attack? Respondents were asked to estimate the PML resulting from business disruptions caused by a malware attack. Business disruptions include denial of services, damage to IT infrastructure and revenue losses. Figure 6 shows the distribution of maximum losses ranging from less than \$10 million to \$500 million. The extrapolated average PML resulting from data exfiltration is \$117.3 million, an increase from \$66.3 million.

Figure 6. Maximum loss resulting from business disruptions caused by a malware attack

Extrapolated PML in FY 2021 = \$117.3 million

Extrapolated PML in FY 2015 = \$ 66.3 million

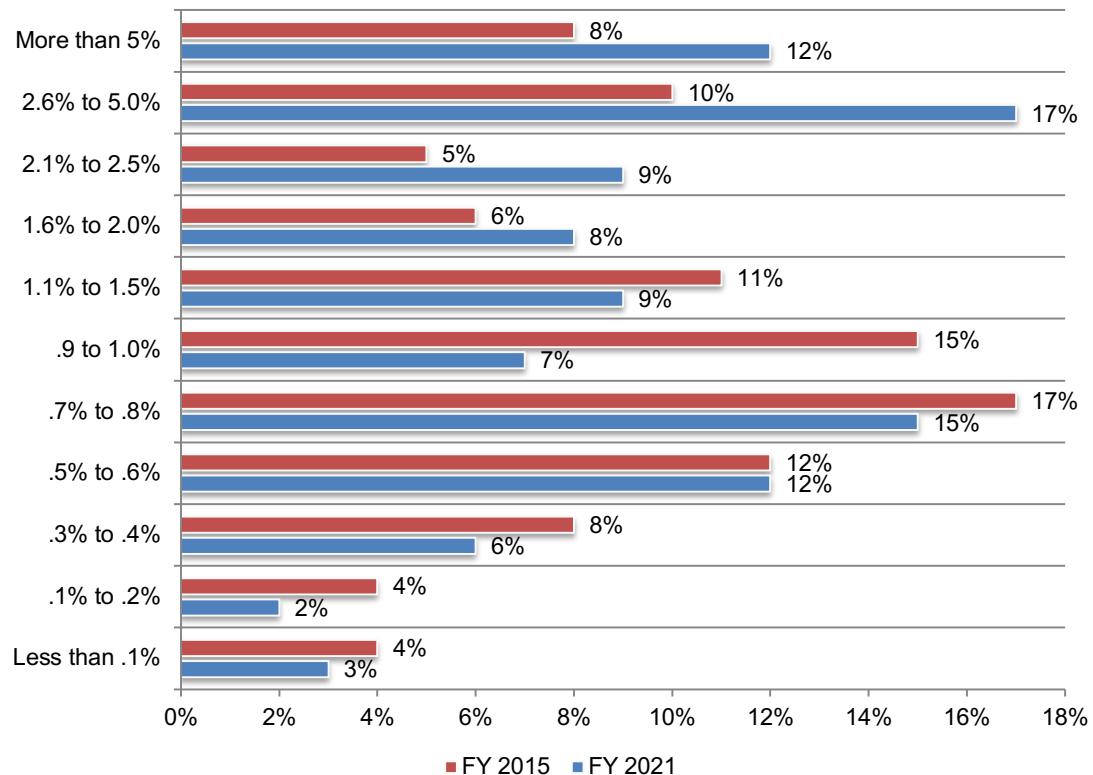


How likely are business disruptions caused by a malware attack will affect your organization? Respondents were asked to estimate the likelihood of material business disruptions caused by malware. Figure 7 shows the probability distribution ranging from less than .1 percent to more than 5 percent. The extrapolated average likelihood of occurrence is 2.1 percent over a 12-month period, an increase from 1.6 percent in 2015.

Figure 7. Likelihood of business disruption caused by a malware attack (over 12 months)

Extrapolated likelihood of occurrence in FY 2021 = 2.1%

Extrapolated likelihood of occurrence in FY 2015 = 1.6%



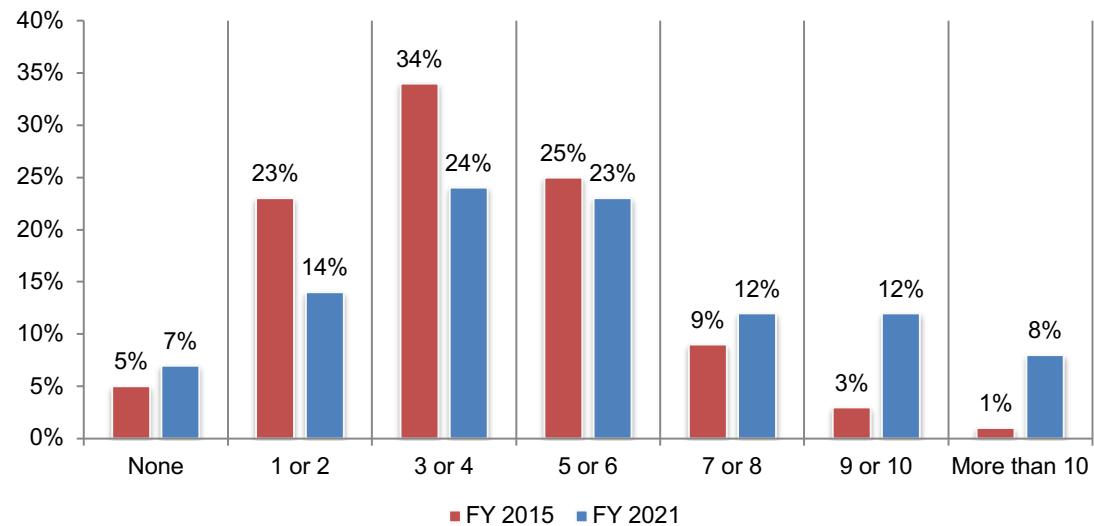
Cost to contain credential compromises

Credential compromises increase (see Table 1) and represent 10 percent of the total cost of phishing. As a result, organizations are spending more to respond to these attacks. The cost to contain credential compromises increased from \$381,920 in 2015 to \$692,531 in 2021. The costs are based on what organizations incurred to contain credential compromises that originated from a successful phishing attack, including the theft of cryptographic keys and certificates. The first step in this analysis is to estimate the total number of compromises expected to occur over the next 12 months.

Figure 8 shows the distribution of credential compromises caused by phishing scams estimated over the past 12-month period. The range of responses includes zero to more than 10 incidents. The extrapolated average is 5.3 compromises that originated from phishing.

Figure 8. Distribution of credential compromises caused by phishing scams

Extrapolated compromises per year in FY 2021 = 5.32
 Extrapolated compromises per year in FY 2015 = 4.00



Based on an earlier study on the cost of key or credential compromise, we estimate a total of 2,050 hours of tech time investigating and responding to one compromise or 10,906 hours estimated over the next 12 months.² Assuming an average annual rate of \$63.50 for tech support, we estimate a total annual cost of \$692,531, an increase from \$381,920 in 2015 (\$62).

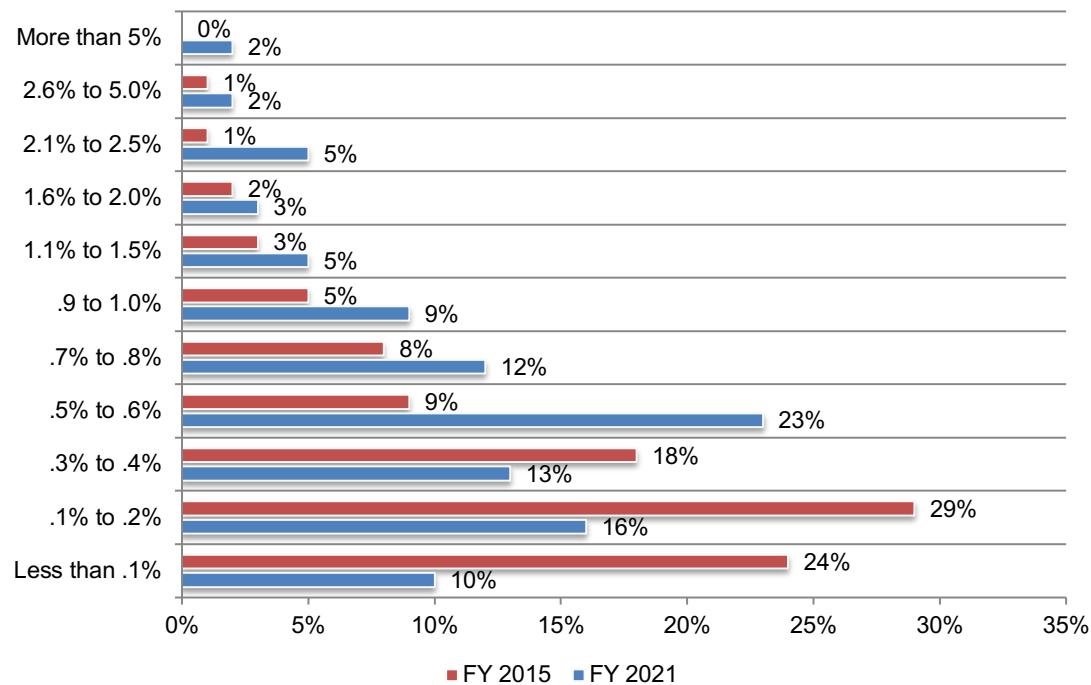
Table 5. Cost of credential compromises caused by phishing	Calculus FY 2015	Calculus FY 2021
Estimated number of credential compromises over the next 12 months	4.0	5.32
Tech time investigating and responding to one compromise	1,540	2,050
Tech time investigating and responding to all compromise per year	6,160	10,906
Fully loaded average hourly rate (\$) for IT security ops*	\$62	\$63.50
Total cost of tech time	\$381,920	\$692,531

Organizations are more likely in 2021 than in 2015 to have a data breach due to credential compromises. Respondents were asked to estimate the likelihood of a material data breach caused by credential compromise. Figure 10 shows the probability distribution ranging from less than .1 percent to 5 percent. The extrapolated average likelihood of occurrence is .81 percent over a 12-month period, an increase from .40 percent in 2015.

Figure 10. Likelihood of data exfiltration caused by credential compromises (over 12 months)

Extrapolated likelihood of occurrence in FY 2021 = .81%

Extrapolated likelihood of occurrence in FY 2015 = .40%



²See: Annual Cost of Failed Trust Report: Threats and Attacks (sponsored by Venafi), Ponemon Institute February 2013.

Respondents were asked to estimate the likelihood of material business disruption caused by credential compromises not contained. Figure 11 shows the probability distribution ranging from less than .1 percent to 5 percent. The extrapolated average likelihood of occurrence is 1.42 percent over a 12-month period, an increase from .9 percent.

Figure 11. Likelihood of business disruptions caused by credential compromises not contained (12 months)

Extrapolated likelihood of occurrence in FY 2021 = 1.42%
 Extrapolated likelihood of occurrence in FY 2015 = 0.9%

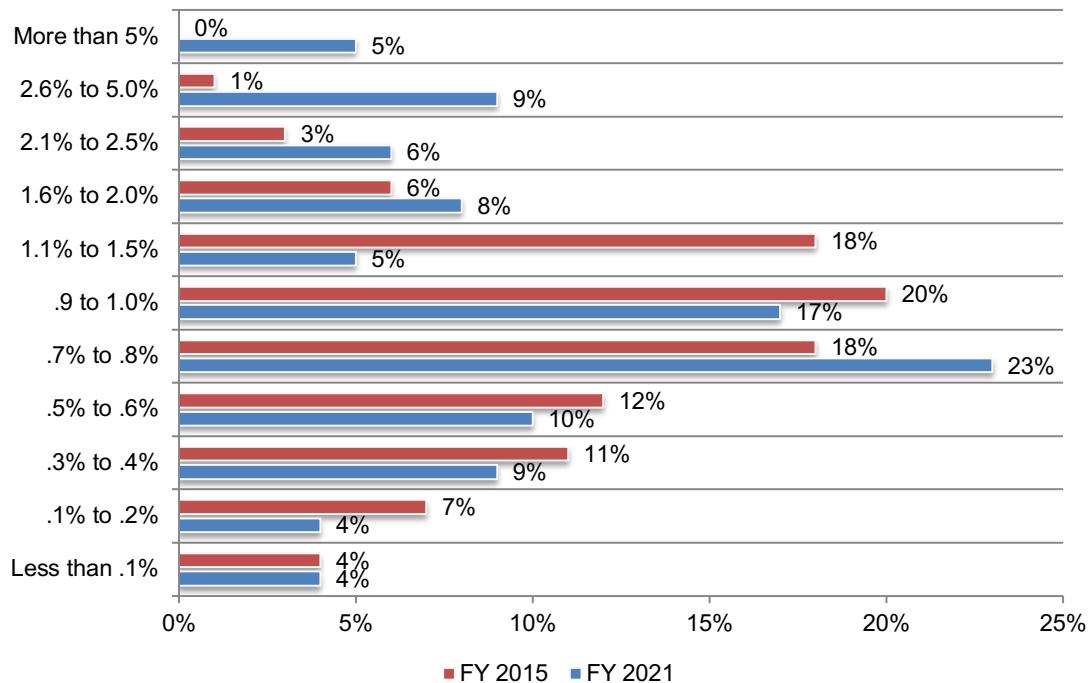


Table 6 reports the expected cost relating to data exfiltration is \$1,111,077 and disruptions to IT and business processes is \$1,665,660, which originated from credential compromises not contained. The total cost of credential compromised not contained is \$2,076,737 and has increased significantly since 2015.

Table 6. The cost of credential compromises not contained	Calculus FY 2015	Calculus FY 2021
Probable maximum loss resulting from data exfiltration	\$105,900,000	\$137,170,000
Likelihood of occurrence over the next 12 months	.4%	0.81%
Expected value	\$423,600	\$1,111,077
Probable maximum loss resulting from business disruptions (including denial of services, damage to IT infrastructure and revenue losses)	\$66,345,000	\$117,300,000
Likelihood of occurrence over the next 12 months	.9%	1.42%
Expected value	\$597,105	\$1,665,660
Total cost of credential compromises not contained	\$1,020,705	\$2,776,737

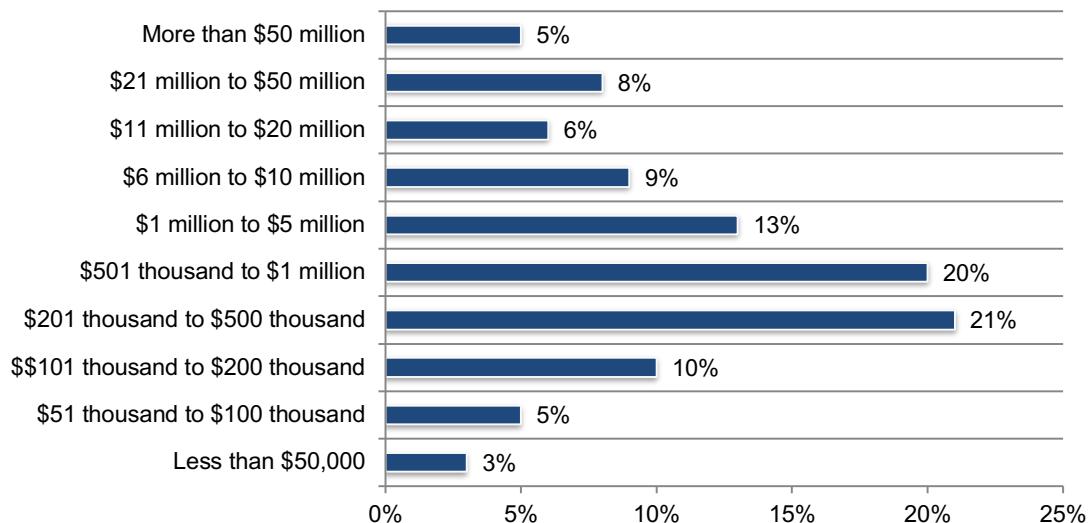
Business email compromises (BEC) and ransomware

BEC is a security exploit in which the attacker targets an employee who has access to company funds or data. The attacker convinces the victim to transfer data or money to the attacker. For the first time in this research, we study the cost consequences of such attacks.

Respondents in our survey were asked to estimate the maximum loss resulting from a successful BEC attack. Figure 12 shows the distribution of maximum losses ranging from less than \$50,000 to more than \$50 million. The extrapolated average maximum loss resulting from a BEC attack is \$8.12 million.

Figure 12. Maximum loss resulting from a successful BEC attack

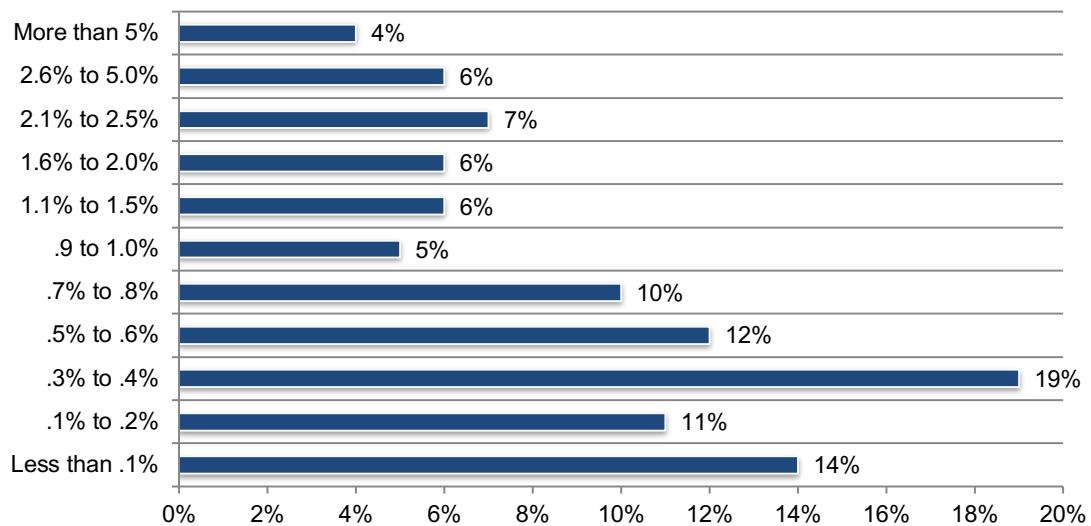
Extrapolated PML in FY 2021 = \$8.12 million



What is the likelihood of a catastrophic BEC attack within the next 12 months? In the context of this research a catastrophic BEC attack is so severe that it impacts the ability to operate as a growing concern even though, as shown in Figure 14, the likelihood of such an attack is low.

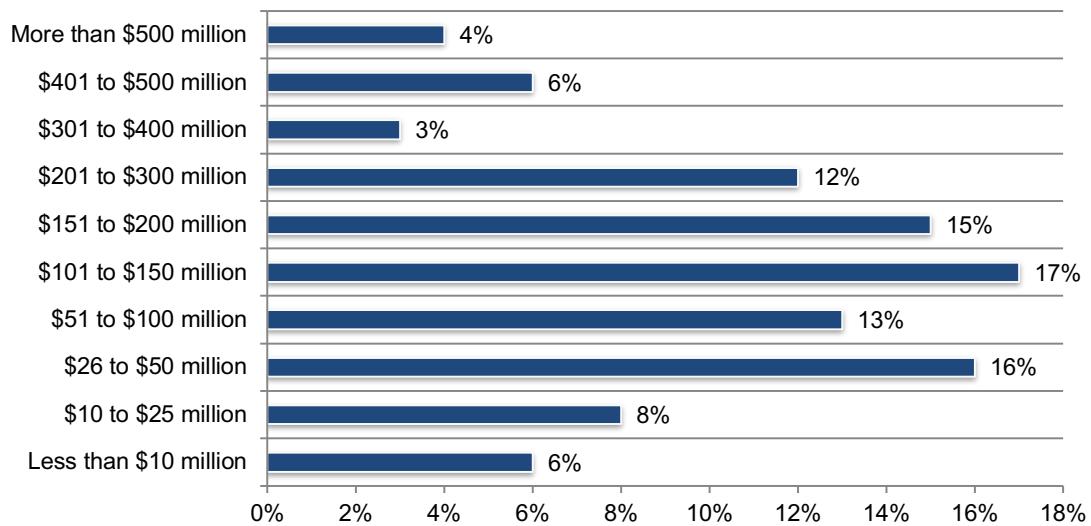
Respondents were asked to estimate the likelihood of such an attack occurring. According to Figure 13, the probability distribution ranging from less than .1 percent to more than 5 percent. The extrapolated average likelihood of occurrence is 1.09 percent over a 12-month period.

Figure 13. Likelihood of a catastrophic BEC attack within the next 12 months
Extrapolated likelihood of occurrence in FY 2021 = 1.09%



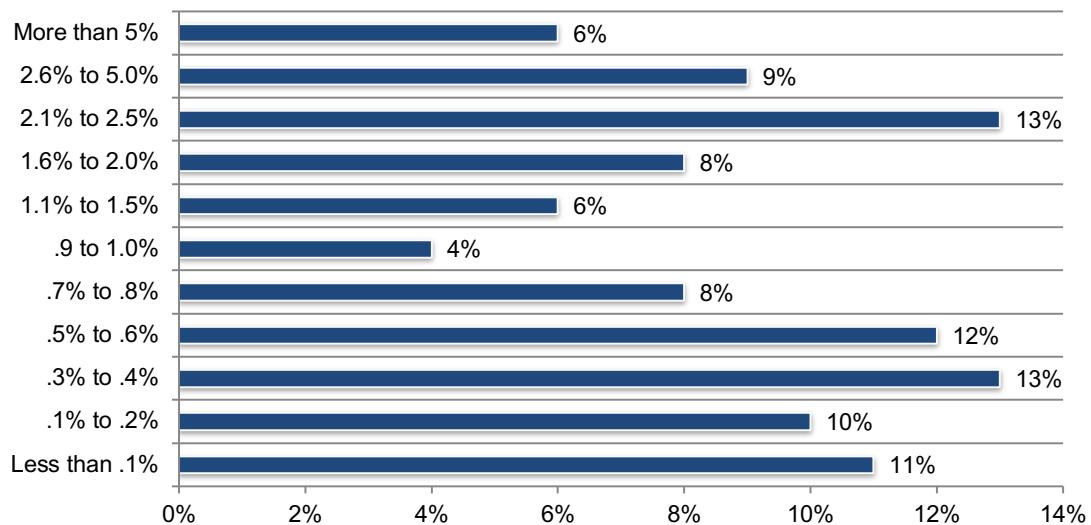
What is the cost of business disruption caused by a BEC attack? Respondents were asked to estimate the PML resulting from business disruptions caused by a BEC attack. Business disruptions include denial of services, damage to IT infrastructure and revenue losses. Figure 14 shows the distribution of maximum losses ranging from less than \$10 million to more than \$500 million. The extrapolated average PML resulting from business disruptions is \$157 million.

Figure 14. Maximum loss resulting from material disruptions caused by BEC
Extrapolated PML in FY 2021 = \$157 million



How likely are business disruptions caused by BEC? Respondents were asked to estimate the likelihood of material business disruptions caused by BEC. As shown in Figure 15, shows the probability distribution ranging from less than .1 percent to more than 5 percent. The extrapolated average likelihood of occurrence in 2021 is 1.45 percent.

Figure 15. Likelihood of a business disruption caused by BEC
Extrapolated likelihood of occurrence in FY 2021 = 1.45%



Organizations transferred an average of \$1.17 million to BEC attackers in the past 12 months. Figure 16 shows the distribution of funds transferred to attackers from less than \$50,000 to more than \$5 million. An average of \$1.17 million was transferred in the past year.

Figure 16. Funds transferred to attackers due to BEC in the past year

Extrapolated funds transferred = \$1.17 million

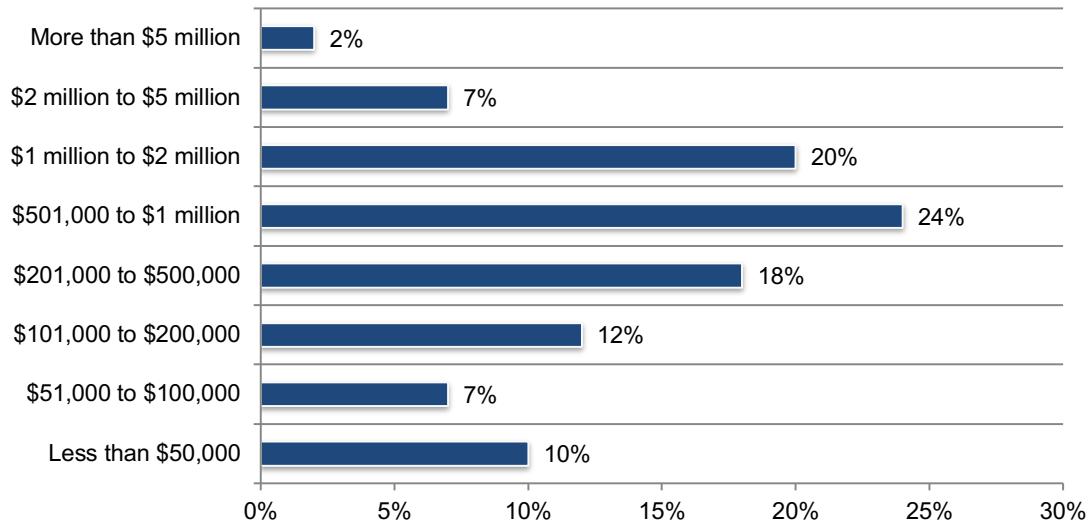


Table 7 presents the factors that determine the total cost of business email compromise.

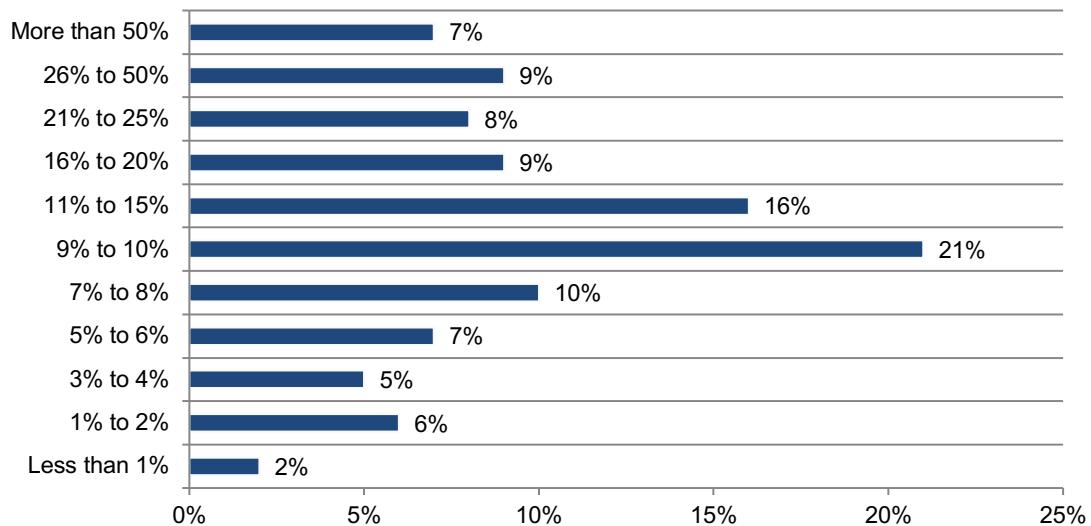
Table 7. The total cost of BEC	Calculus FY2021
Probable maximum loss resulting from data exfiltration	\$8,120,000
Likelihood of occurrence over the next 12 months	1.09%
Expected value	\$88,508
Probable maximum loss resulting from business disruptions caused by business email compromise	\$157,000,000
Likelihood of occurrence over the next 12 months	1.45%
Expected value	\$2,276,500
Costs to contain BEC (38,276 hours x \$63.5 IT hourly wage)	\$2,430,526
Cost of funds transferred in BEC attacks (Figure 17)	\$1,170,000
Total cost of business email compromise from phishing	\$5,965,534

Ransomware

Ransomware is a sophisticated piece of malware that blocks the victim's access to his/her files. As shown in Figure 17, the average percentage rate of ransomware experienced from phishing by organizations is 17.6 percent.

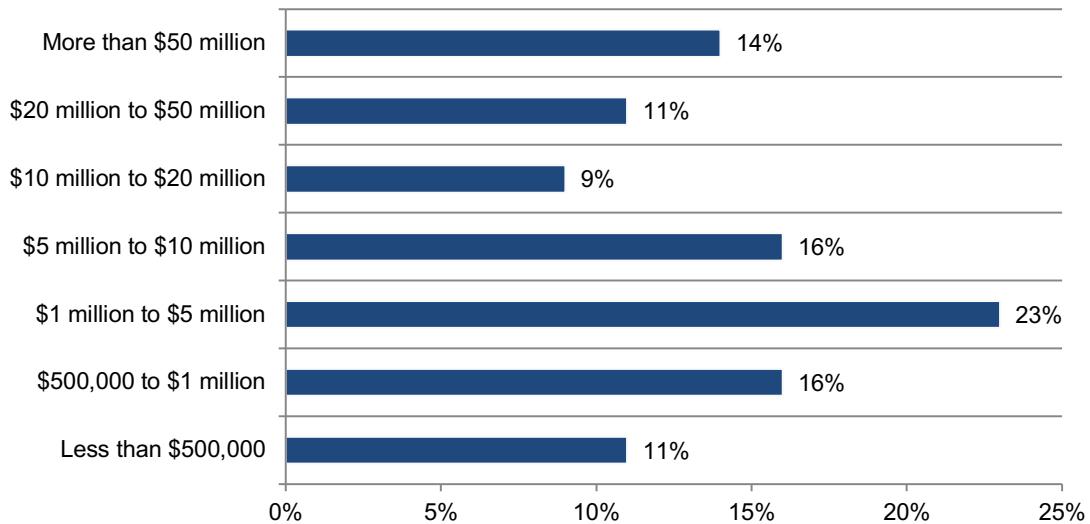
Figure 17. Percentage rate of ransomware from phishing

Extrapolated value = 17.6%



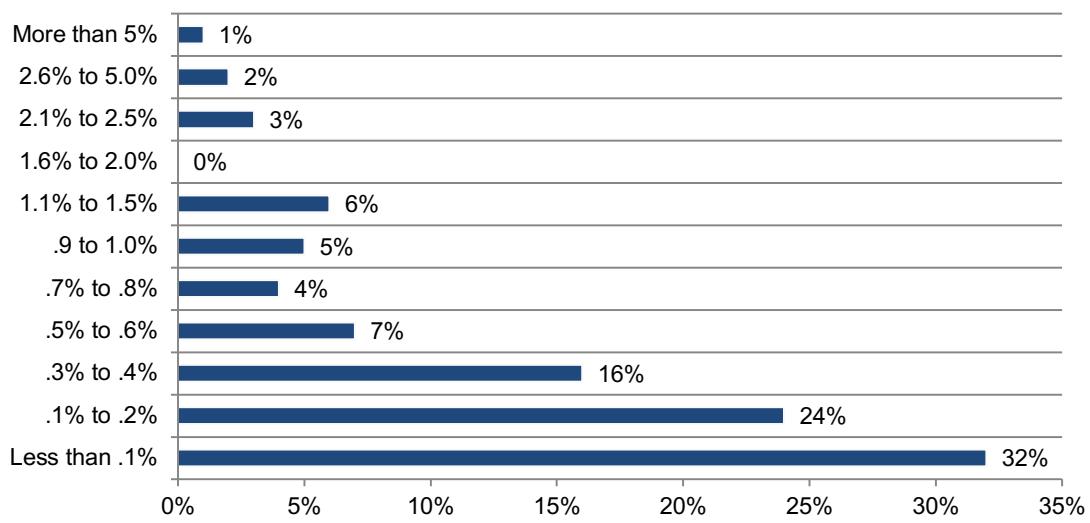
Respondents in our survey were asked to estimate the PML resulting from a successful ransomware attack. Figure 18 shows the distribution of maximum losses ranging from less than \$500,000 to more than \$50 million. The extrapolated average PML resulting from ransomware is \$15.64 million.

Figure 18. Maximum loss resulting from a material and successful ransomware attack
Extrapolated PML in FY 2021 = \$15.64 million



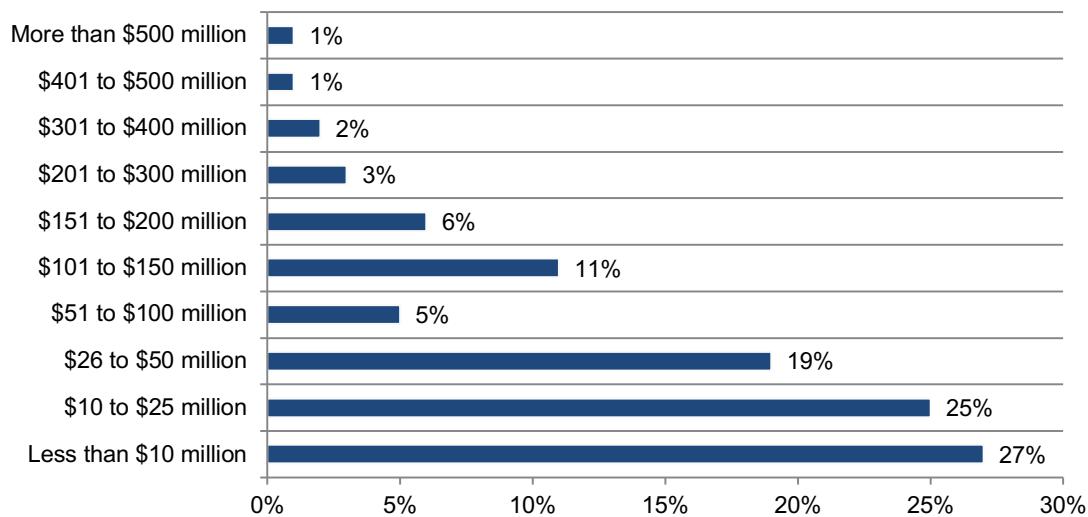
What is the likelihood of a ransomware attack in the next 12 months? Respondents were asked to estimate the likelihood of this occurring. According to Figure 19, the probability distribution ranges from less than 1 percent to more than 5 percent. The average likelihood of such an attack is 3 percent.

Figure 19. Likelihood of a catastrophic ransomware attack in the next 12 months
Extrapolated likelihood of occurrence in FY 2021 = 3.0%



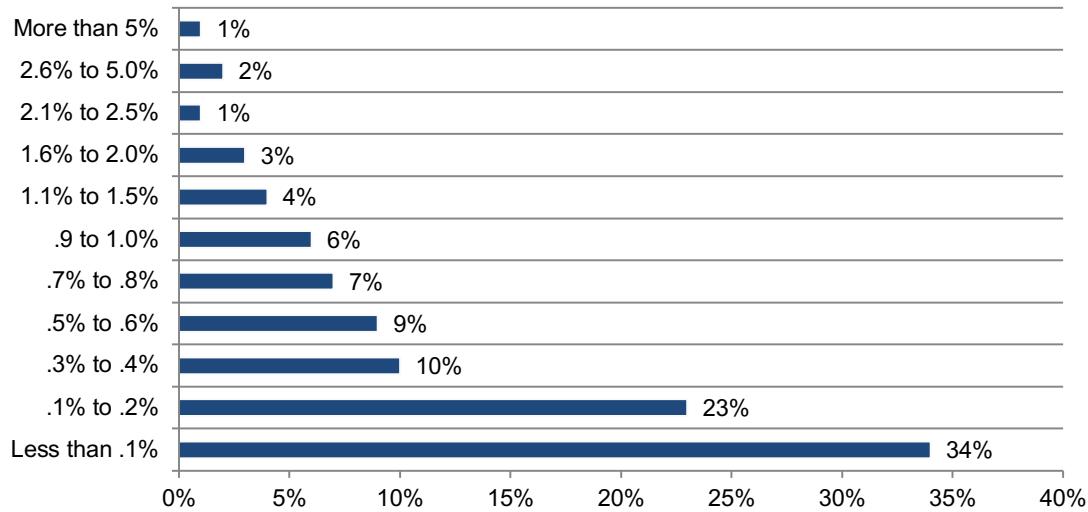
What is the cost of business disruption due to ransomware? Respondents were asked to estimate the PML resulting from business disruptions caused by ransomware. Business disruptions include denial of services, damage to IT infrastructure and revenue losses. Figure 20 shows the distribution of maximum losses ranging from less than \$10 million to more than \$500 million. The average PML resulting from ransomware is \$67.5 million.

Figure 20. Maximum loss resulting from business disruptions caused by ransomware
Extrapolated PML in FY 2021 = \$67.5 million



How likely are business disruptions due to ransomware? Respondents were asked to estimate the likelihood of material disruptions caused by ransomware. Figure 21 shows the probability distribution ranging from less than 1 percent to more than 5 percent. The average likelihood of occurrence in the next 12 months is 3.2 percent.

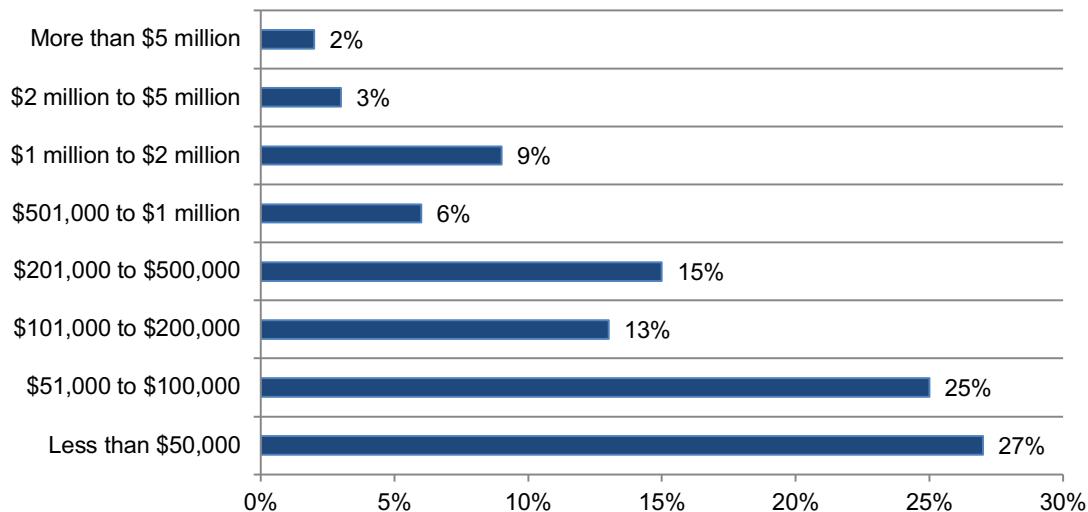
Figure 21. Likelihood of material business disruptions caused by ransomware in the next 12 months
Extrapolated likelihood of occurrence in FY 2021 = 3.2%



Ransomware cost organizations \$790,000 in the past year. As shown in Figure 23, organizations paid an average of \$790,000 in funds transferred directly to attackers in ransomware attacks.

Figure 22. Cost of funds transferred in ransomware attacks

Extrapolated funds transferred in FY 2021 = \$790,000



The total cost of ransomware can be as high as \$5.66 million. As shown in Table 8, the expected value of the PML resulting from business disruptions caused by ransomware is \$67.5 million. The average total cost of ransomware caused by phishing is \$996 thousand for the current year.

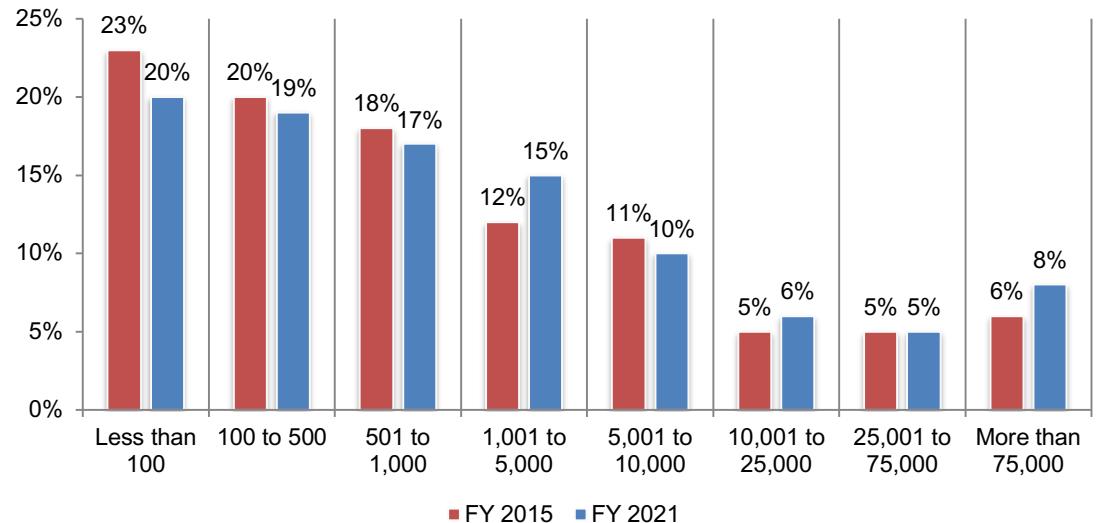
Table 8. The cost of ransomware	Calculus FY2021
Probable maximum loss resulting from ransomware (US \$millions)	\$15.64
Likelihood of occurrence over the next 12 months	3.00%
Expected value (US\$ millions)	\$470,000
Probable maximum loss resulting from business disruptions caused by ransomware (US\$ millions)	\$67.50
Likelihood of occurrence over the next 12 months	3.20%
Expected value (US\$ millions)	\$2.16
Costs to contain Ransomware (35,285 hours x \$63.5 IT hourly wage)	\$2,240,598
Cost of funds transferred in ransomware attacks (\$US)	\$790,000
Total cost of ransomware (US\$ millions)	\$5.66
Percentage rate of ransomware caused by phishing scams (Figure 18)	17.6%
Total cost of ransomware (US\$ millions)	\$996,265

Part 4. Demographics and methods

Headcount in organizations represented in this study ranges from less than 100 to more employees with access to corporate email systems. In this study, headcount is used as a surrogate for organizational size. The extrapolated average headcount in 2021 is 9,567 users with email access, as shown in Figure 23.

Figure 23. Average headcount of employees with access to corporate email

Extrapolated headcount in FY 2021 = 9,567
 Extrapolated headcount in FY 2015 = 9,552

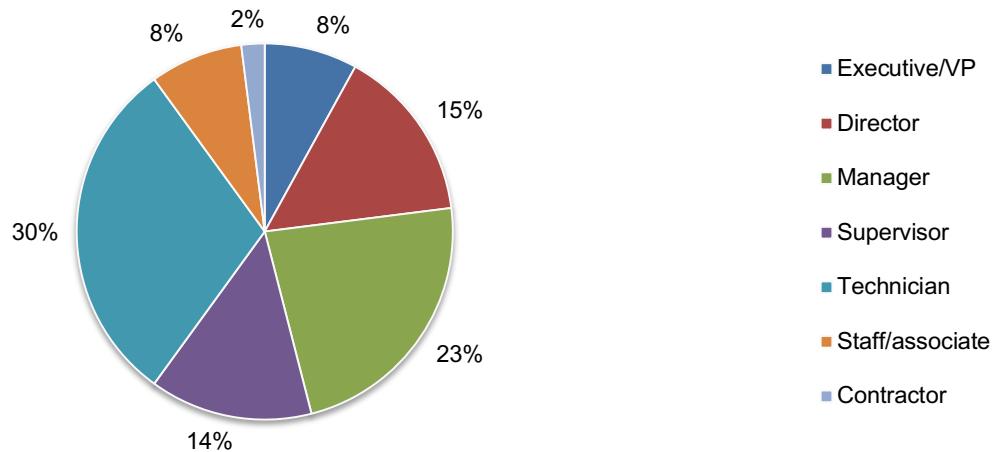


Our sampling frame is composed of 14,550 IT and IT security practitioners located in the United States, whose job involves the protection of sensitive or confidential information. As shown in Table 9, 641 respondents completed the survey. Screening removed 50 surveys. The final sample was 591 surveys (or a 4.1 percent response rate).

Table 9. Sample response	FY 2015	FY 2021
Total sampling frame	12,442	14,550
Total survey returns	415	641
Rejected surveys	38	50
Final sample	377	591
Response rate	3.0%	4.1%

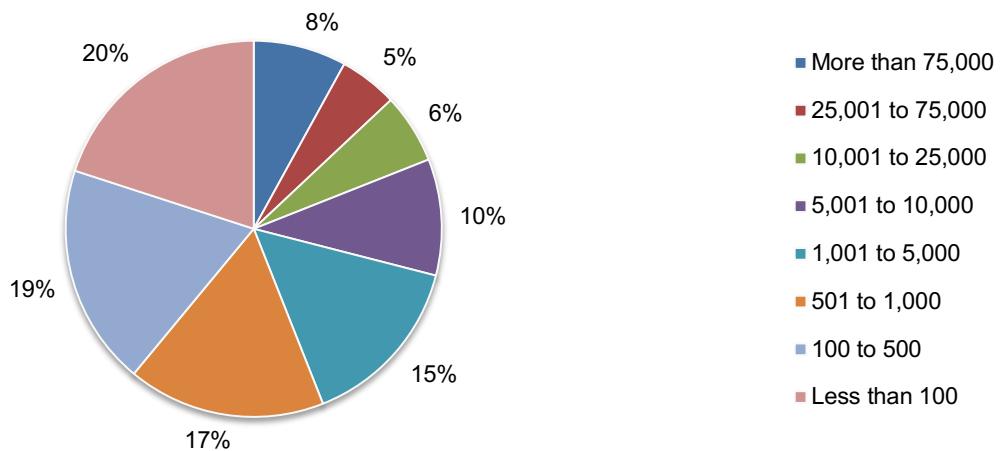
Pie Chart 2 reports the current position or organizational level of the respondents. Half of the respondents reported their current position as supervisory or above. The largest segment at 30 percent of respondents is the technician position.

Pie Chart 2. Current position within the organization



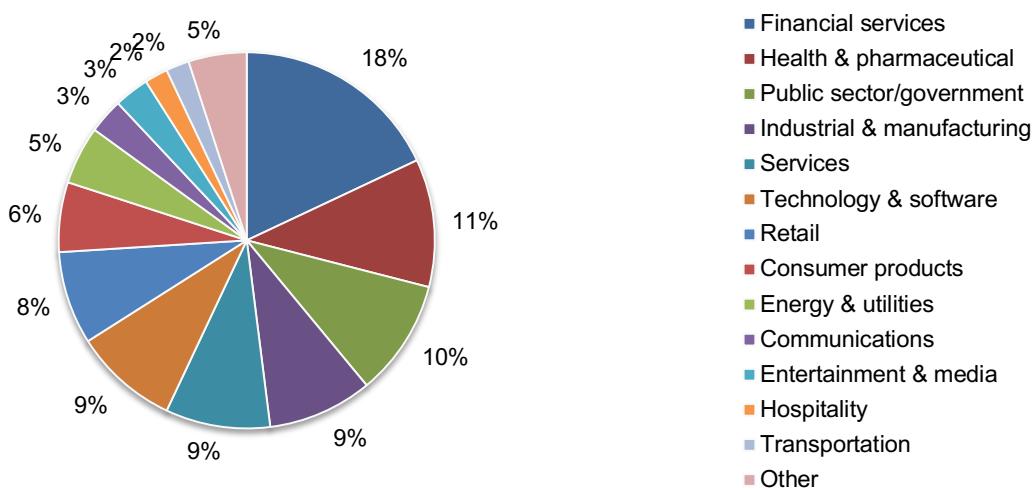
According to Pie Chart 3, 1,000 or more employees have access to corporate email systems according to 44 percent of the respondents. Fifty-six percent of respondents indicated up to 1,000 employees have access to corporate email systems.

Pie Chart 3. Full time employees with access to corporate email systems



Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceutical (11 percent of respondents), and public sector/government (10 percent of respondents). Industrial/manufacturer, services, and technology and software are each at 9 percent of respondents.

Pie Chart 4. Primary industry classification



Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Appendix: Detailed Survey Results

Survey response	Freq
Total sampling frame	14,550
Total survey returns	641
Rejected surveys	50
Final sample	591

Part 1. Background

Q1. What best describes your current position level within the organization?	Pct%
Executive/VP	8%
Director	15%
Manager	23%
Supervisor	14%
Technician	30%
Staff/associate	8%
Contractor	2%
Other (please specify)	0%
Total	100%

Q2. How many full-time employees have access to corporate email systems within your organization? Your best estimate is welcome.	Pct%
Less than 100	20%
100 to 500	19%
501 to 1,000	17%
1,001 to 5,000	15%
5,001 to 10,000	10%
10,001 to 25,000	6%
25,001 to 75,000	5%
More than 75,000	8%
Total	100%

Q3. What best describes your organization's primary industry sector? Please select only one best choice.	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	6%
Defense & aerospace	1%
Energy & utilities	5%
Entertainment & media	3%
Financial services	18%
Health & pharmaceutical	11%
Hospitality	2%
Industrial & manufacturing	9%
Public sector/government	10%
Retail	8%
Services	9%
Technology & software	9%
Transportation	2%
Other (please specify)	3%
Total	100%

Part 2. Cost of phishing and email-based threats

Q4. The following table provides seven (7) cost categories of phishing and other email-based threats such as malware and ransomware. Please allocate all 100 points to provide the relative distribution of each cost category. Please keep in mind that the total points must equal 100.

Distribution of phishing-related cost categories	Points
Productivity losses from phishing	24
Cost of credential compromises not contained	20
Cost of ransomware	15
Cost to contain credential compromise from phishing	13
Cost of business email compromise (a.k.a. email fraud)	11
Cost of malware not contained	9
Cost of malware containment	8
Total points (100 points)	100

Q5. Following are six tasks to contain malware infections caused by email-based threats over a 12-month period. Please select the total hours the cybersecurity team spent dealing with each activity.

Q5a. Planning	Pct%
Less than 10 hours	4%
10 to 50 hours	8%
51 to 100 hours	15%
101 to 250 hours	27%
251 to 500 hours	17%
501 to 1,000 hours	13%
1,001 to 2,500 hours	5%
2,501 to 5,000 hours	3%
5,001 to 10,000 hours	5%
More than 10,000 hours	3%
Total	100%

Q5b. Capturing intelligence	Pct%
Less than 10 hours	0%
10 to 50 hours	6%
51 to 100 hours	5%
101 to 250 hours	4%
251 to 500 hours	9%
501 to 1,000 hours	6%
1,001 to 2,500 hours	15%
2,501 to 5,000 hours	19%
5,001 to 10,000 hours	21%
More than 10,000 hours	15%
Total	100%

Q5c. Evaluating intelligence	Pct%
Less than 10 hours	0%
10 to 50 hours	0%
51 to 100 hours	3%
101 to 250 hours	7%
251 to 500 hours	8%
501 to 1,000 hours	15%
1,001 to 2,500 hours	15%
2,501 to 5,000 hours	21%
5,001 to 10,000 hours	21%
More than 10,000 hours	10%
Total	100%

Q5d. Investigating	Pct%
Less than 10 hours	0%
10 to 50 hours	0%
51 to 100 hours	0%
101 to 250 hours	0%
251 to 500 hours	6%
501 to 1,000 hours	6%
1,001 to 2,500 hours	3%
2,501 to 5,000 hours	0%
5,001 to 10,000 hours	11%
More than 10,000 hours	74%
Total	100%

Q5e. Cleaning & fixing	Pct%
Less than 10 hours	0%
10 to 50 hours	1%
51 to 100 hours	0%
101 to 250 hours	0%
251 to 500 hours	0%
501 to 1,000 hours	0%
1,001 to 2,500 hours	3%
2,501 to 5,000 hours	3%
5,001 to 10,000 hours	12%
More than 10,000 hours	81%
Total	100%

Q5f. Documenting	Pct%
Less than 10 hours	9%
10 to 50 hours	6%
51 to 100 hours	9%
101 to 250 hours	10%
251 to 500 hours	13%
501 to 1,000 hours	18%
1,001 to 2,500 hours	23%
2,501 to 5,000 hours	9%
5,001 to 10,000 hours	0%
More than 10,000 hours	0%
Total	97%

Q6. What is the percentage rate of malware infections caused by phishing or email-based threats? Your best estimate is welcome.	Pct%
More than 50%	4%
26% to 50%	7%
21% to 25%	9%
16% to 20%	15%
11% to 15%	11%
9% to 10%	13%
7% to 8%	16%
5% to 6%	11%
3% to 4%	7%
1% to 2%	5%
Less than 1%	2%
Total	100%

Q7. What best describes the maximum loss that could be realized by your organization as a result of a catastrophic data exfiltration event caused by malware? Your best estimate is welcome.	Pct%
More than \$500 million	2%
\$401 to \$500 million	4%
\$301 to \$400 million	6%
\$201 to \$300 million	11%
\$151 to \$200 million	12%
\$101 to \$150 million	16%
\$51 to \$100 million	14%
\$26 to \$50 million	8%
\$10 to \$25 million	15%
Less than \$10 million	12%
Total	100%

Q8. What best describes the Likelihood of a catastrophic data exfiltration event caused by malware within the next 12 months? Your best estimate is welcome.	Pct%
More than 5%	14%
2.6% to 5.0%	21%
2.1% to 2.5%	6%
1.6% to 2.0%	9%
1.1% to 1.5%	7%
.9 to 1.0%	10%
.7% to .8%	12%
.5% to .6%	13%
.3% to .4%	4%
.1% to .2%	3%
Less than .1%	1%
Total	100%
Q9. What best describes the maximum loss that could be realized by your organization resulting from material business disruptions caused by malware? Your best estimate is welcome.	Pct%
More than \$500 million	3%
\$401 to \$500 million	4%
\$301 to \$400 million	0%
\$201 to \$300 million	11%
\$151 to \$200 million	14%
\$101 to \$150 million	8%
\$51 to \$100 million	4%
\$26 to \$50 million	34%
\$10 to \$25 million	12%
Less than \$10 million	10%
Total	100%
Q10. What best describes the Likelihood of material business disruptions caused by malware within the next 12 months? Your best estimate is welcome.	Pct%
More than 5%	12%
2.6% to 5.0%	17%
2.1% to 2.5%	9%
1.6% to 2.0%	8%
1.1% to 1.5%	9%
.9 to 1.0%	7%
.7% to .8%	15%
.5% to .6%	12%
.3% to .4%	6%
.1% to .2%	2%
Less than .1%	3%
Total	100%

Q11. How many hours per employee each year are spent dealing with phishing or any email-based threat/fraud? Your best estimate is welcome.		Pct%
More than 25 hours		2%
21 to 25 hours		3%
16 to 20 hours		1%
11 to 15 hours		7%
9 to 10 hours		21%
7 to 8 hours		16%
5 to 6 hours		10%
3 to 4 hours		15%
1 to 2 hours		5%
Less than 1 hour		20%
Total		100%
Extrapolated value		-

Q12. What best describes the number of credential compromises caused by phishing or other email-based threats over the past 12 months? Your best estimate is welcome.		Pct%
More than 10		8%
9 or 10		12%
7 or 8		12%
5 or 6		23%
3 or 4		24%
1 or 2		14%
None		7%
Total		100%

Q13. What best describes the Likelihood of data exfiltration caused by credential compromises over the next 12 months? Your best estimate is welcome.		Pct%
More than 5%		2%
2.6% to 5.0%		2%
2.1% to 2.5%		5%
1.6% to 2.0%		3%
1.1% to 1.5%		5%
.9 to 1.0%		9%
.7% to .8%		12%
.5% to .6%		23%
.3% to .4%		13%
.1% to .2%		16%
Less than .1%		10%
Total		100%

Q14. What best describes the Likelihood of material business disruptions caused by credential compromises over the next 12 months? Your best estimate is welcome.	Pct%
More than 5%	5%
2.6% to 5.0%	9%
2.1% to 2.5%	6%
1.6% to 2.0%	8%
1.1% to 1.5%	5%
.9 to 1.0%	17%
.7% to .8%	23%
.5% to .6%	10%
.3% to .4%	9%
.1% to .2%	4%
Less than .1%	4%
Total	100%

Part 3. Business email compromise: Business email compromise (BEC) is a security exploit in which the attacker targets an employee who has access to company funds or data. They convince the victim to transfer data or money to the attacker.

Recap: Six tasks to contain business email compromise (hours)	Hours
Planning	1,019
Capturing intelligence	4,450
Evaluating intelligence	5,001
Investigating	12,336
Cleaning & fixing	14,395
Documenting	1,075
Total	38,276

Recap: Six tasks to contain business email compromise (cost)*	Amount
Planning	\$ 64,707
Capturing intelligence	\$ 282,575
Evaluating intelligence	\$ 317,564
Investigating	\$ 783,336
Cleaning & fixing	\$ 914,083
Documenting	\$ 68,263
Total	\$ 2,430,526

*Fully loaded average hourly rate for IT security practitioners = \$63.5.

Q15. Likelihood of a business disruption caused by BEC	Pct%
Less than .1%	11%
.1 to .2%	10%
.3 to .4%	13%
.5% to .6%	12%
.7% to .8%	8%
.9 to 1.0%	4%
1.1% to 1.5%	6%
1.6% to 2.0%	8%
2.1% to 2.5%	13%
2.6% to 5.0%	9%
More than 5%	6%
Total	100%
Extrapolated value	1.45%
Q16. What best describes the actual funds transferred to an attacker by your organization due to business email compromise in the past year? Your best estimate is welcome.	Pct%
Less than \$50,000	10%
\$51,000 to \$100,000	7%
\$101,000 to \$200,000	12%
\$201,000 to \$500,000	18%
\$501,000 to \$1 million	24%
\$1 million to \$2 million	20%
\$2 million to \$5 million	7%
More than \$5 million	2%
Total	100%
Extrapolated value (US\$ millions)	\$ 1.17

Q17. Percentage decrease in the cost of phishing as a result of employee training interventions	Pct%
< 10%	5%
10 to 20%	9%
21 to 30%	4%
31 to 40%	8%
41 to 50%	13%
51 to 60%	21%
61 to 70%	19%
71 to 80%	7%
81 to 90%	8%
91 to 100%	6%
Expected value	53%

Part 4. Ransomware

Q18. What is the percentage rate of ransomware caused by email-based attacks? Your best estimate is welcome.	Pct%
Less than 1%	2%
1% to 2%	6%
3% to 4%	5%
5% to 6%	7%
7% to 8%	10%
9% to 10%	21%
11% to 15%	16%
16% to 20%	9%
21% to 25%	8%
26% to 50%	9%
More than 50%	7%
Total	100%
Extrapolated value	17.6%

Q19. What best describes the maximum loss that could be realized by your organization as a result of a successful ransomware attack. Your best estimate is welcome.	Pct%
Less than \$500,000	11%
\$500,000 to \$1 million	16%
\$1 million to \$5 million	23%
\$5 million to \$10 million	16%
\$10 million to \$20 million	9%
\$20 million to \$50 million	11%
More than \$50 million	14%
Total	100%

Q20. What best describes the Likelihood of a catastrophic ransomware attack within the next 12 months? Your best estimate is welcome	Pct%
Less than .1%	32%
.1% to .2%	24%
.3% to .4%	16%
.5% to .6%	7%
.7% to .8%	4%
.9 to 1.0%	5%
1.1% to 1.5%	6%
1.6% to 2.0%	0%
2.1% to 2.5%	3%
2.6% to 5.0%	2%
More than 5%	1%
Total	100%
Extrapolated value	3.2%

Q21. What best describes the maximum loss that could be realized by your organization resulting from material business disruptions caused by ransomware? Your best estimate is welcome.	Pct%
Less than \$10 million	27%
\$10 to \$25 million	25%
\$26 to \$50 million	19%
\$51 to \$100 million	5%
\$101 to \$150 million	11%
\$151 to \$200 million	6%
\$201 to \$300 million	3%
\$301 to \$400 million	2%
\$401 to \$500 million	1%
More than \$500 million	1%
Total	100%
Extrapolated value (US\$ millions)	\$ 67.50

Q22. What best describes the Likelihood of material business disruptions caused by ransomware within the next 12 months? Your best estimate is welcome	Pct%
Less than .1%	34%
.1% to .2%	23%
.3% to .4%	10%
.5% to .6%	9%
.7% to .8%	7%
.9 to 1.0%	6%
1.1% to 1.5%	4%
1.6% to 2.0%	3%
2.1% to 2.5%	1%
2.6% to 5.0%	2%
More than 5%	1%
Total	100%
Extrapolated value	3.2%

Q23. What best describes the actual cost of ransom by your organization due to ransomware in the past year. Your best estimate is welcome.	Pct%
Less than \$50,000	27%
\$51,000 to \$100,000	25%
\$101,000 to \$200,000	13%
\$201,000 to \$500,000	15%
\$501,000 to \$1 million	6%
\$1 million to \$2 million	9%
\$2 million to \$5 million	3%
More than \$5 million	2%
Total	100%
Extrapolated value (US\$ millions)	\$ 0.79

Table 8. The cost of ransomware	Calculus FY2021
Probable maximum loss resulting from ransomware (US \$millions)	\$15.64
Likelihood of occurrence over the next 12 months	3.00%
Expected value (US\$ millions)	\$470,000
Probable maximum loss resulting from business disruptions caused by ransomware (US\$ millions)	\$67.50
Likelihood of occurrence over the next 12 months	3.20%
Expected value (US\$ millions)	\$2.16
Costs to contain Ransomware (35,285 hours x \$63.5 IT hourly wage)	\$2,240,598
Cost of funds transferred in ransomware attacks (\$US)	\$790,000
Total cost of ransomware (US\$ millions)	\$5.66
Percentage rate of ransomware caused by phishing scams (Figure 18)	17.6%
Total cost of ransomware from phishing (US\$ millions)	\$996,265

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **October 2022**
Commissioned by **IRONSCALES**

The Business Cost of Phishing

Executive Summary

Phishing is a type of cybersecurity attack experienced by all organizations. Successful attacks result in lost account credentials, fraud, and data theft. Preventing successful attacks is proving costly for organizations, with phishing-related activities consuming one third of the total time available to IT and security teams. On average, organizations spend almost 30 minutes dealing with each phishing email identified in their email infrastructure.

The purpose of this research was to quantify the direct costs borne by organizations in mitigating the phishing threat, and to explore expectations about how phishing will change over the next 12 months.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Phishing has been, is currently, and is expected to continue to represent a significant threat to organizations**
Current and expected levels of phishing represent a “threat” or “extreme threat” to one third of organizations due to the consequences of successful phishing incidents, such as loss of account credentials, business email compromise, and data theft.
- **Phishing represents a huge time burden for IT and security teams**
IT and security teams spend one third of their total available time handling the phishing threat every week. At most organizations, phishing is expected to get worse over the coming 12 months.
- **Phishing is an expensive issue for organizations to address**
On average, dealing with the threat of a single phishing email takes 27.5 minutes at a cost of \$31.32 per phishing message. Some organizations are taking much longer and paying more per phishing message, and no organization sees only a single phishing attack in any given time period.
- **Phishing is expected to get more sophisticated and better able to evade detection over time**
IT and security professionals expect the volume of phishing attacks to increase over the next 12 months, as well as getting more sophisticated and pernicious. The time and cost currently expended on mitigating phishing will increase unless organizations start relying on better phishing protections.
- **Phishing is spreading beyond email**
Organizations are already seeing phishing attacks in new communication and collaboration tools beyond email, with phishing in messaging apps and cloud-based file sharing platforms the most common new attack vectors.

***Phishing:
dangerous,
costly, risky, and
increasingly
pernicious.***

ABOUT THIS WHITE PAPER

The survey and white paper were commissioned by IRONSCALES. Information about IRONSCALES and details on the survey methodology are provided at the end of the paper.

The Threat of Phishing

Phishing is a threat to organizational data, finances, and reputation. In this section, we look at how the survey respondents rate the threat of phishing.

THE THREAT OF PHISHING

Current and expected levels of phishing represent a “threat” or “extreme threat” to one third of organizations. The current level of threat has declined over the past 12 months—perhaps reflective of the shift at many organizations towards office-based work again, where phishing risks are lower than for remote workers—but is expected to increase again over the coming 12 months. See Figure 1. Threats from phishing include:

- **Loss of account credentials**

Phishing emails commonly impersonate well-known brands (e.g., Microsoft, Amazon, Apple, and banks) and ask the target victim to check their account for abnormal behavior. The link included in the phishing email instead takes the victim to a fake website that captures their account credentials, providing the phisher with full access to the victim’s account and associated privileges. Sophisticated phishing attacks that circumvent multi-factor authentication (MFA) protections are becoming more commonplace.

- **Trickery of users into paying fake invoices or diverting payroll**

Business email compromise (BEC) attacks frequently start with targeted phishing emails intended to trick a manager or finance employee into authorizing fake invoices or changing employee payroll details.

- **Compromise of corporate data**

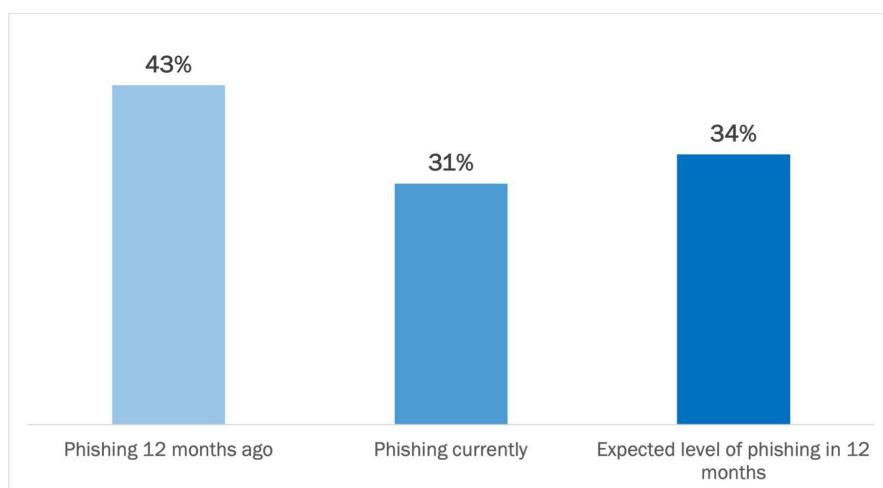
Phishing emails that install malware can result in data exfiltration, as can messages that compromise account credentials. Phishers gain corporate data, triggering data breach notification procedures, the risk of identity theft for customers, loss of customer trust, and reputational damage.

Phishing is seen as a significant threat at one third of organizations.

Figure 1

Evaluating the Threat of Phishing

Percentage of respondents indicating “threat” or “extreme threat”

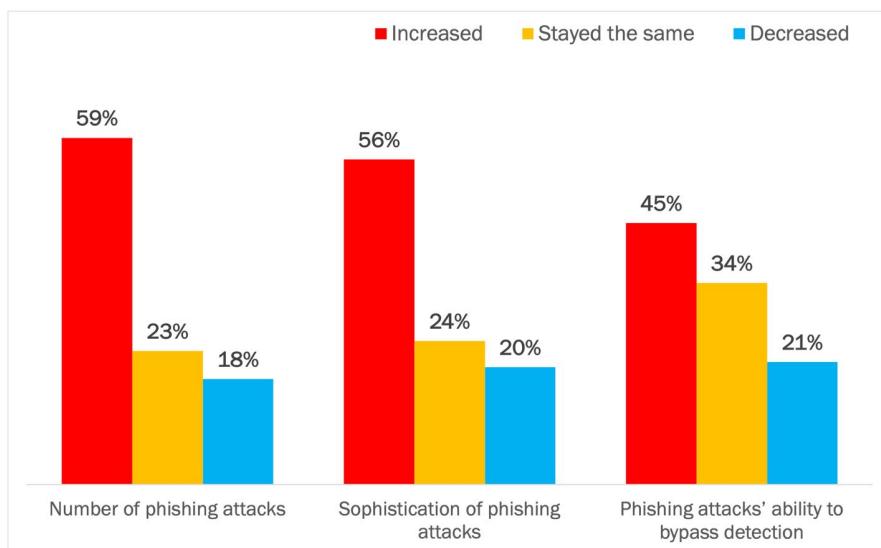


Source: Osterman Research (2022)

HOW PHISHING ATTACKS ARE CHANGING OVER TIME

Four out of five respondents reported that various dynamics of phishing attacks had gotten worse or stayed the same over the past 12 months. These dynamics were the number of phishing attacks (82% increased or stayed the same), the sophistication of phishing attacks (80%), and the ability of phishing attacks to bypass current detection mechanisms (79%). See Figure 2.

Figure 2
Dynamics of Phishing Attacks Over the Past 12 Months
 Percentage of respondents



Source: Osterman Research (2022)

The increase and continuity of these various dynamics is seen in the characteristics of phishing threats rated as concerning by respondents (see Figure 3 on the next page). Half of respondents rated three characteristics as highly concerning:

- **Use of adaptive techniques by threat actors to create unique attributes for each phishing message**

Adaptive techniques, also known as polymorphic attacks, vary each phishing message slightly as a method of increasing sophistication and decreasing the likelihood of being detected as a phishing message. Polymorphic attacks create unique messages that must be evaluated one by one, rather than being able to match using signatures or other known or trained identifiers. The use of polymorphic attack methods is ranked as the issue of highest concern.

- **Use of compromised account credentials by threat actors to hijack current email threads to send phishing threats**

Account credentials obtained from an earlier phishing message—or purchased on the dark web—are then used to spread subsequent phishing messages on current email threads. This is a sophisticated attack, since social dynamics in the thread are already established, assuring a level of interpersonal trust and rapport that is more difficult to create between unknown parties. It is also likely to bypass detection since the messages are sent from the organization's own email infrastructure, removing many threat signals that can be evaluated when messages originate externally.

80% of organizations indicate that various dynamics of phishing have worsened or remained the same over the past 12 months.

- **Use of advanced obfuscation techniques by threat actors to hide phishing threats**

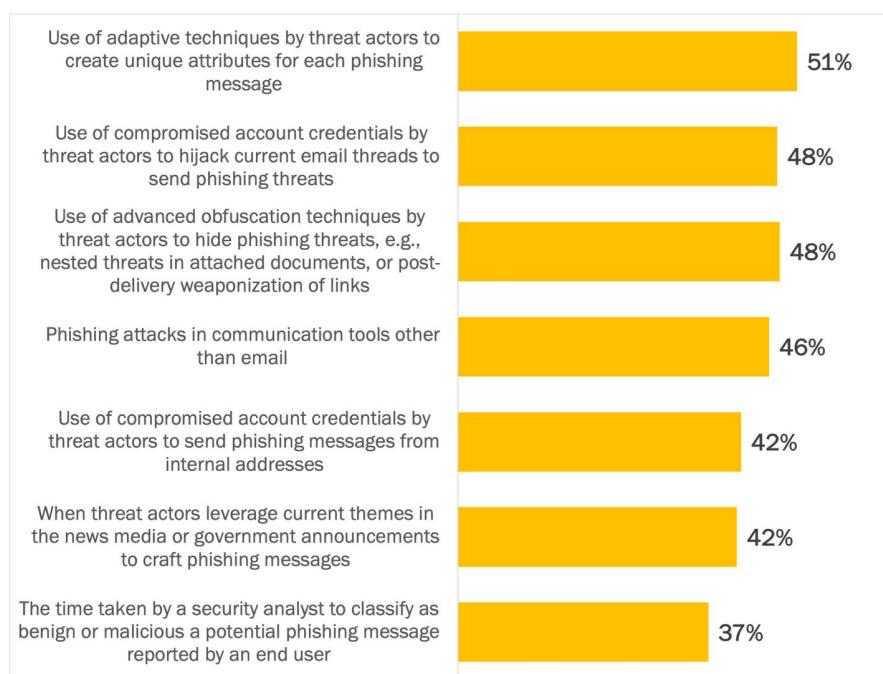
A related method of increasing sophistication and decreasing the likelihood of being detected is advanced obfuscation, where payload and link threats are nested, initially presented as benign, or subsequently downloaded. Phishing defenses must then evaluate messages for threat signals at multiple points in the lifecycle of the message.

Several additional issues evidencing growing sophistication and bypass capabilities of phishing messages are shown in Figure 3. These include:

- Phishing in tools other than email—rendering detection capabilities focused solely on the email channel as ineffective.
- Internal phishing using compromised accounts—which decreases the detection likelihood since messages do not originate externally.
- Leveraging current themes in news media and government announcements—thereby increasing sophistication and the temptation for a targeted victim to open the message, attachments, and any links.

Figure 3
Concerns with Characteristics of Phishing Threats

Percentage of respondents indicating “concern” or “extreme concern”



A diverse set of increasingly sophisticated phishing threats are slipping through protections and causing havoc for organizations.

Source: Osterman Research (2022)

The Cost of Phishing

In this section, we investigate the direct cost of phishing to organizations.

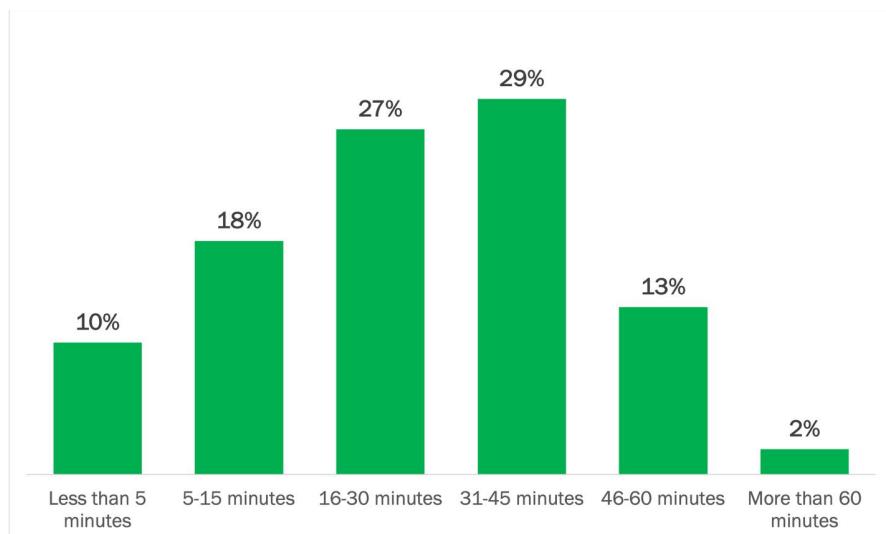
TIME TO DEAL WITH A SINGLE PHISHING EMAIL

Organizations spend a significant amount of time dealing with phishing emails, with 70% of organizations spending 16 to 60 minutes for each phishing email. This covers the phishing lifecycle from initial discovery of a potential phishing email to its complete removal from the environment. It is most common for organizations to spend 31-45 minutes per phishing email (29% of respondents indicate it takes this long at their organization).

See Figure 4.

Figure 4

Total Time for IT and Security Teams to Deal with a Single Phishing Email
Percentage of respondents



70% of organizations spend 16-60 minutes dealing with a single phishing email message.

Source: Osterman Research (2022)

Clearly, no organization has to deal with only a single phishing email. With several billion phishing messages sent globally every day, phishing is a significant proportion of overall email volumes.

CALCULATING WHAT IT COSTS TO DEAL WITH PHISHING

To calculate the cost of dealing with phishing in IT and security teams, we need to determine the average salary and benefits of an IT and security professional. To do so, we created a composite based on the roles reflected in this survey who spend time each week dealing with phishing at their organization. See Figure 5, where:

- **Column 1: Roles**
The seven roles in the survey that personally spend time each week dealing with phishing threats are listed in the first column.
- **Column 2: Percentage of survey respondents**
The percentage of respondents in each role who completed the survey is shown in column 2.
- **Column 3: Median annual salary and benefits**
The median annual salary and benefits reported for each role in the United States on salary.com in July 2022 is shown in column 3.
- **Column 4: Contribution to the composite IT and security professional**
Column 4 calculates the contribution of each role to the composite fully burdened annual salary and benefits. This totals to \$136,528 per year or based on an annual work year of 2,000 hours, \$68.26 per hour.

Figure 5
Calculating the Cost of a Composite IT and Security Professional

Role of respondent completing the survey	Percentage of respondents	Annual salary and benefits	Contribution to composite
IT security manager or IT security team lead	40%	\$ 138,504	\$ 55,512
IT manager or IT team lead	29%	\$ 151,150	\$ 44,385
Email security manager or email security team lead	16%	\$ 141,000	\$ 22,381
Security manager	8%	\$ 101,329	\$ 8,042
Email security administrator	5%	\$ 82,781	\$ 4,270
SOC manager or SOC team lead	1%	\$ 134,330	\$ 1,599
SOC analyst	0.4%	\$ 85,324	\$ 339
			\$ 136,528

Source: Osterman Research (2022)

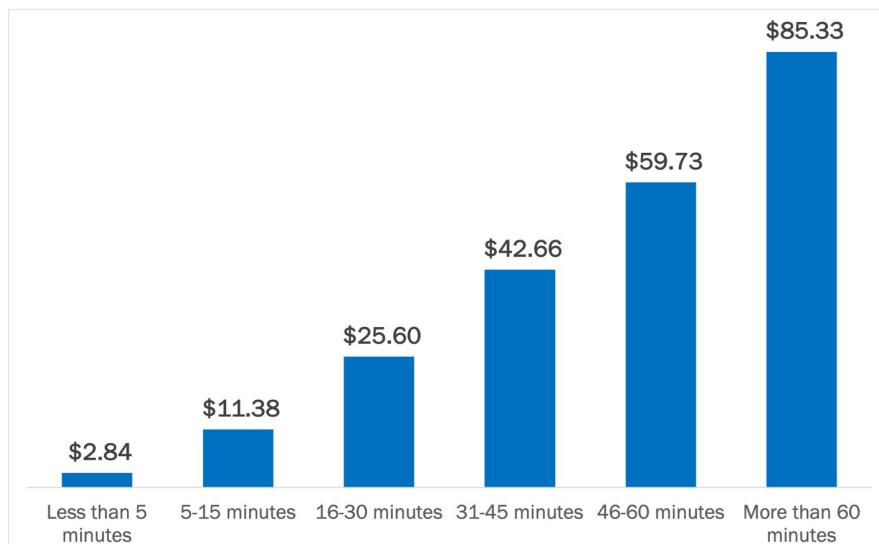
A composite IT and security professional costs \$136,528 per year in salary and benefits, or \$68.26 per hour.

COST OF DEALING WITH A SINGLE PHISHING EMAIL

Dealing with phishing costs time for IT and security teams, and the professionals spending their time on phishing in these teams represent cost to the organization in salary and benefits. The fully burdened labor cost per phishing email for the professionals represented in this study is shown in Figure 6—ranging from teams spending five minutes or less per phishing email, costing \$2.84 per phishing email, to teams spending more than 60 minutes, costing \$85.33 per phishing email.

On average, time spent per phishing email is 27.5 minutes, at a cost of \$31.32 per phishing email. This is calculated by combining the distribution of time spent with the fully burdened labor cost of the specific roles of IT and security professionals reflected in this study (as calculated in Figure 5 above).

Figure 6
Cost of Dealing with a Single Phishing Email
Fully burdened labor cost per phishing email



Source: Osterman Research (2022)

IT and security teams spend an average of 27.5 minutes to deal with a single phishing email, at a fully burdened labor cost of \$31.32 per message.

The above figures are per phishing email. All organizations see many more than a single phishing email (remember, billions are sent every day), hence the costs increase as an organization receives more phishing messages. See Figure 7.

Figure 7
The More Phish, the Higher the Cost

Phishing messages	Less than 5 minutes	5-15 minutes	16-30 minutes	31-45 minutes	46-60 minutes	More than 60 minutes
250	\$710	\$2,845	\$6,400	\$10,665	\$14,933	\$21,333
1,000	\$2,840	\$11,380	\$25,600	\$42,660	\$59,730	\$85,330
7,500	\$21,300	\$85,350	\$192,000	\$319,950	\$447,975	\$639,975
15,000	\$42,600	\$170,700	\$384,000	\$639,900	\$895,950	\$1,279,950
20,000	\$56,800	\$227,600	\$512,000	\$853,200	\$1,194,600	\$1,706,600

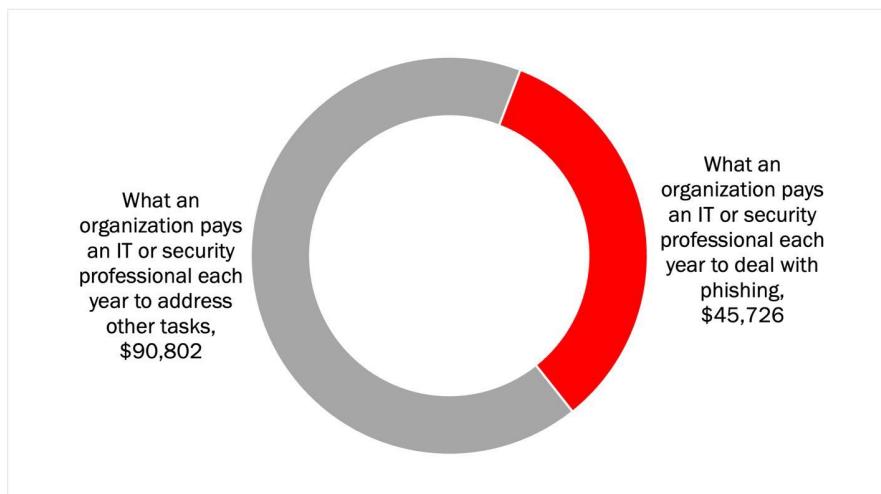
Source: Osterman Research (2022)

TIME SPENT PER WEEK ON PHISHING-RELATED ACTIVITIES

Respondents indicated that handling phishing-related activities consumes an average of one third of the working hours available each week for the IT and security teams at their organization. On an annual basis, for the composite IT and security professional created above, this equates to \$45,726 in salary and benefits paid per IT and security professional to handle phishing. See Figure 8.

Figure 8

Annual Salary Paid Per IT or Security Professional to Handle Phishing and Other Tasks
Fully burdened labor cost per year



Source: Osterman Research (2022)

The salary amounts shown in Figure 8 are per IT or security professional in an organization, so for organizations with multiple professionals, the annual cost currently incurred for dealing with phishing only increases. For example:

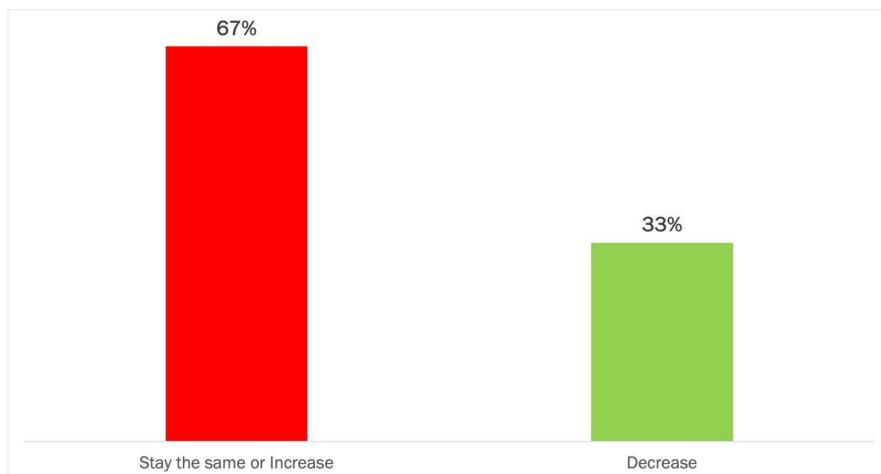
- An organization with five IT and security professionals is currently paying \$228,630 of the annual salary and benefits paid to handle phishing.
- An organization with 10 IT and security professionals is paying \$457,260 per year to handle phishing.
- An organization with 25 IT and security professionals is currently paying \$1,143,150 per year to handle phishing.

Dealing with phishing consumes one third of the total available work hours available to IT and security teams.

EXPECTED CHANGE IN TIME SPENT PER WEEK

Most respondents expect the impact of phishing on their IT and security teams to get worse over the coming 12 months, with 67% expecting the time spent on phishing per week for IT and security teams to stay the same or increase. See Figure 9. This will drive up the proportion of annual salary paid to each IT and security professional for handling phishing.

Figure 9
Expected 12-Month Change in Time Spent Per Week on Phishing
Percentage of respondents



Source: Osterman Research (2022)

COSTS WE HAVE IGNORED

We have focused exclusively on the direct, quantifiable cost of phishing within an organization as incurred for staff time by IT and security professionals. We have not included opportunity costs of IT and security staffers, nor indirect but consequential costs. These represent the costs of successful phishing attacks that compromise account credentials, corporate data, and lead to stolen and misdirected funds. In combination, the following incur costs that are orders of magnitude greater than the direct costs profiled above:

- **Data breach notification costs**
Email, postage, and phone call notifications to customers affected by a data breach.
- **Loss of customer trust**
Lost sales as affected customers and disgruntled prospects shop elsewhere to avoid doing business with a tarnished organization.
- **Loss of corporate reputation and market value**
Market value decreases on market exchanges in response to news about poor defenses and resultant breaches.
- **Regulatory fines**
In a growing set of jurisdictions, regulatory fines are levied on organizations with insufficient technology and organizational protections against common security threats.

Indirect but consequential costs of successful phishing attacks incur costs orders of magnitude higher than only considering the direct costs.

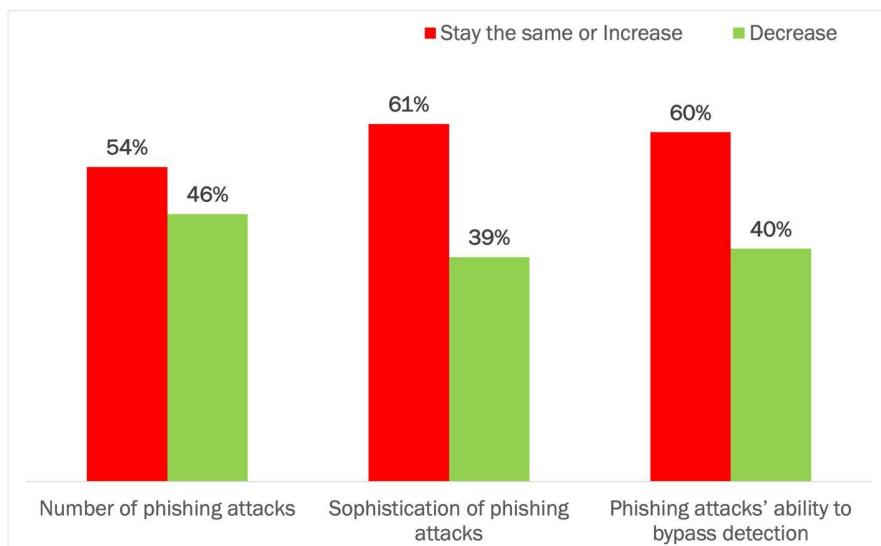
The Outlook for Phishing

Phishing is expected to remain a problem over the coming 12 months, with one worrying development the spread of phishing to new communication and collaboration tools.

PHISHING ATTACKS REMAIN A PROBLEM

We asked respondents to indicate their expectation about what will happen with three characteristics of phishing attacks over the next 12 months: the number, the sophistication, and the ability to bypass traditional email security detection technologies. In a significant departure from how respondents scored these changes over the past 12 months (see Figure 2 on page 4), twice as many expect all three to decrease over the next 12 months (see Figure 10).

Figure 10
Expected Dynamics of Phishing Attacks Over the Next 12 Months
Percentage of respondents



Source: Osterman Research (2022)

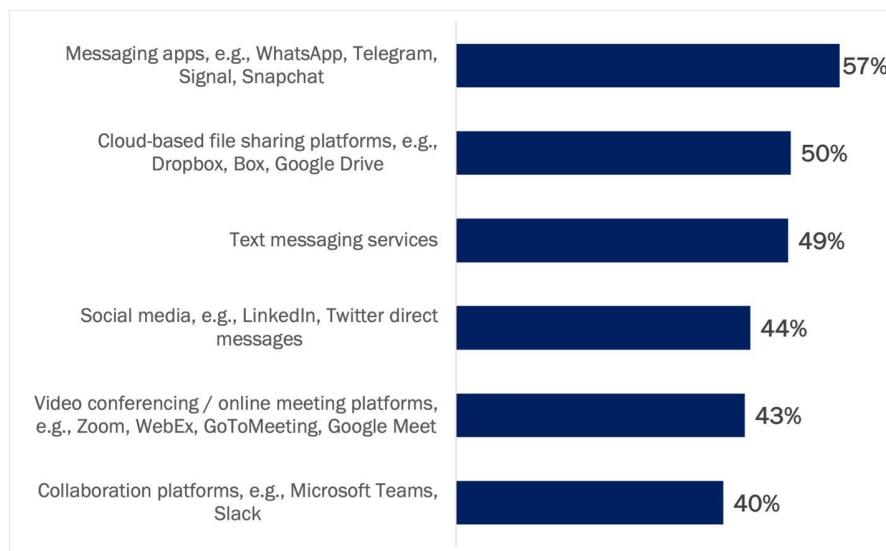
Given the question is about characteristics that are independent of the defenses employed by organizations, this expectation feels misplaced. Because phishing attacks will almost certainly become more numerous, more sophisticated, and better able to bypass traditional email security detection, a better interpretation of the data presented in this figure is that it indicates the desire of how respondents' organizations want to respond to the phishing threat and not the nature of phishing attacks themselves.

Most organizations anticipate that the phishing threat will get worse, and many would like to be better equipped to deal with it.

PHISHING IS ALREADY SPREADING TO OTHER TOOLS

A worrying development is the spread of phishing messages to tools beyond email, such as messaging apps, cloud-based file sharing platforms, and text messaging services. At least half of respondents indicated they are already seeing phishing attacks in these three communication and collaboration tools beyond email, and two in five respondents are seeing phishing attacks in social media, video conferencing/online meeting platforms, and collaboration platforms such as Microsoft Teams and Slack. As phishing spreads to these new tools—often driven by account credential compromise—IT and security professionals will have to spend even more time addressing threats and seeking to eradicate threat actors from their other services. See Figure 11.

Figure 11
Phishing Attacks Reaching End Users in Communication and Collaboration Tools
Percentage of respondents



Source: Osterman Research (2022)

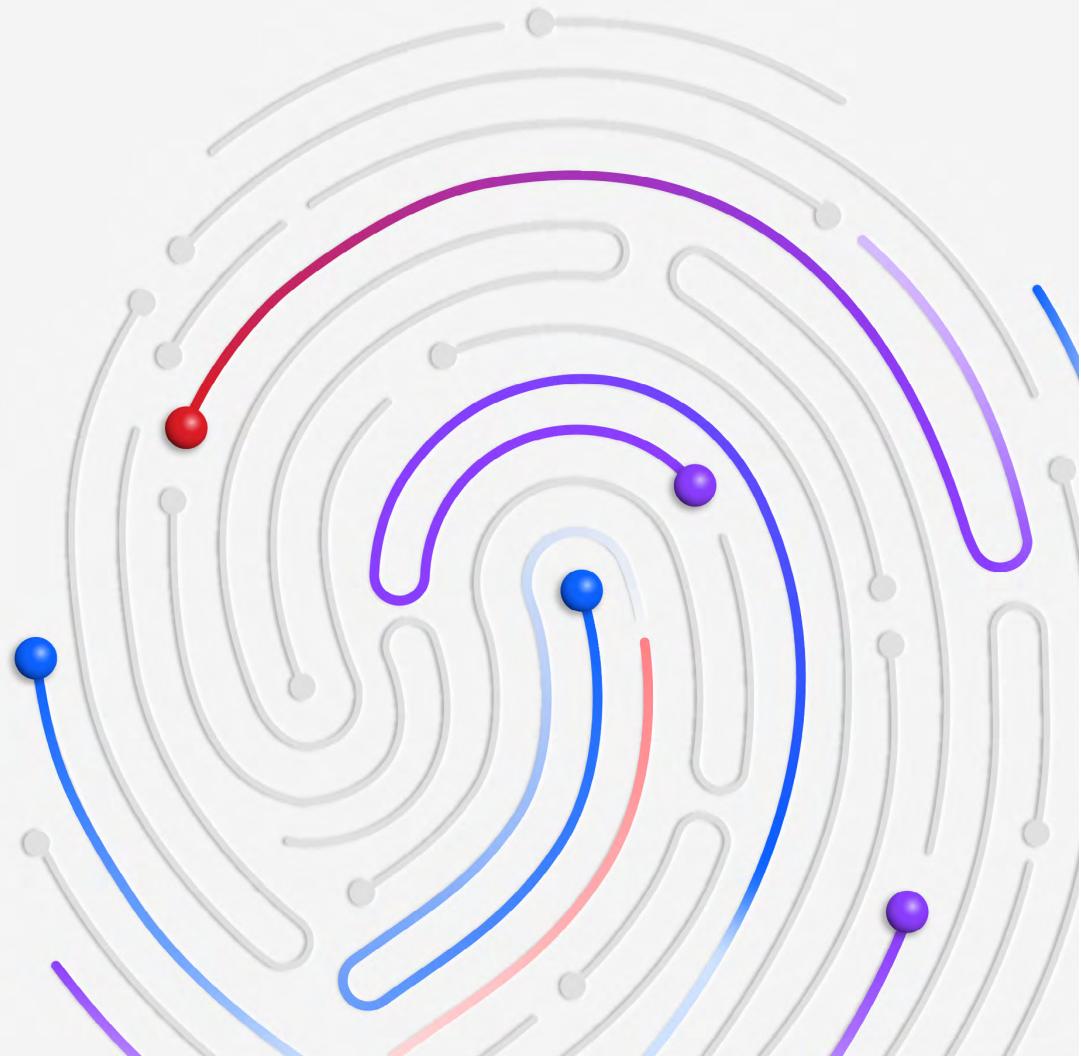
Organizations are already seeing phishing spread to tools beyond email—increasing the number and sophistication of phishing threats.

Conclusion

Phishing continues to represent a time-intensive and costly problem for organizations. The number of phishing attacks is expected to increase over the next 12 months, along with attack sophistication and continued detection bypass capabilities. Organizations are also seeing phishing attacks spread to new tools beyond email. Organizations wanting to free up cybersecurity staff time for more strategic initiatives and reduce their expenditure on addressing phishing attacks should be looking for more capable solutions that detect and stop more phishing attacks, offer detection of advanced polymorphic and nested threats, and protect communication and collaboration tools via a holistic solution rather than being limited to protecting email only.

X-Force Threat Intelligence Index

2024



IBM®

Report highlights

71%

Increase year over year in volume of attacks using valid credentials

For the first time ever, abusing valid accounts became cybercriminals' most common entry point into victim environments. It represented 30% of all incidents X-Force responded to in 2023.

11.5%

Drop in enterprise ransomware incidents

Despite remaining the most common action on objective (20%), X-Force observed a drop in enterprise ransomware incidents. This drop is likely to impact adversaries' revenue expectations from encryption-based extortion as larger organizations are stopping attacks before ransomware is deployed and opting against paying and decrypting in favor of rebuilding if ransomware takes hold.

32%

Percentage of data theft and leak incidents

Data theft and leak rose to the most common impact for organizations, indicating more groups are favoring this method to obtain financial gains.

266%

Upsurge in use of info stealers

X-Force has observed threat groups who have previously specialized in ransomware showing increasing interest in info stealers. And a number of prominent new info stealers recently debuted and demonstrated increased activity in 2023, such as Rhadamanthys, LummaC2 and StrelaStealer.

30%

Share of security misconfigurations among web application vulnerabilities identified

X-Force penetration testing engagements revealed that the most observed web application risk across client environments globally was security misconfigurations. Of these misconfigurations, the top offenses included allowing concurrent user sessions in the application, which could weaken multifactor authentication (MFA) through session hijacking.

32%

Percentage of incidents that involved malicious use of legitimate tools

Nearly one-third of incidents that X-Force responded to were cases where legitimate tools were used for malicious purposes, such as credential theft, reconnaissance, remote access or data exfiltration.

50%

Market share threshold likely to trigger attacks against AI platforms

X-Force analysis indicates that the establishment of AI market dominance will signal AI attack surface maturity. This analysis suggests that once a single AI technology approaches 50% market share, or when the market consolidates to three or less technologies, the cybercriminal ecosystem will be incentivized to invest in developing tools and attack paths targeting AI technologies.

84%

Percentage of critical infrastructure incidents where initial access vector could have been mitigated

For a majority of incidents on critical infrastructure that X-Force responded to, the initial access vector could have been mitigated with best practices and security fundamentals, such as asset and patch management, credential hardening and the principle of least privilege.

25.7%

Share of manufacturing attack incidents within the top 10 attacked industries

Manufacturing was once again the top attacked industry in 2023 for the third year in a row, representing 25.7% of incidents within the top 10 attacked industries. Malware was the top action on objective observed at 45%. Ransomware accounted for 17% of incidents.

31%

Increase in attacks year over year in Europe

Europe also experienced the highest percentage of incidents (32%) out of the five geographic regions. Malware was the most observed action on objective accounting for 44% of incidents.

Top initial access vectors

One of the top initial access vectors in 2023—jumping from third to first place—was the abuse of valid accounts identified in 30% of the observed incidents X-Force responded to. As defenders increase their detection and prevention capabilities, attackers are finding that obtaining valid credentials is an easier route to achieving their goals, considering the alarming volume of compromised yet valid credentials available—and easily accessible—on the dark web. X-Force found that cloud account credentials alone make up 90% of for sale cloud assets on the dark web, making it easy for threat actors to take over legitimate user identities to establish access into victim environments. Attacker use of valid accounts as an initial access vector appears to have a significant impact on the required response efforts, as well.

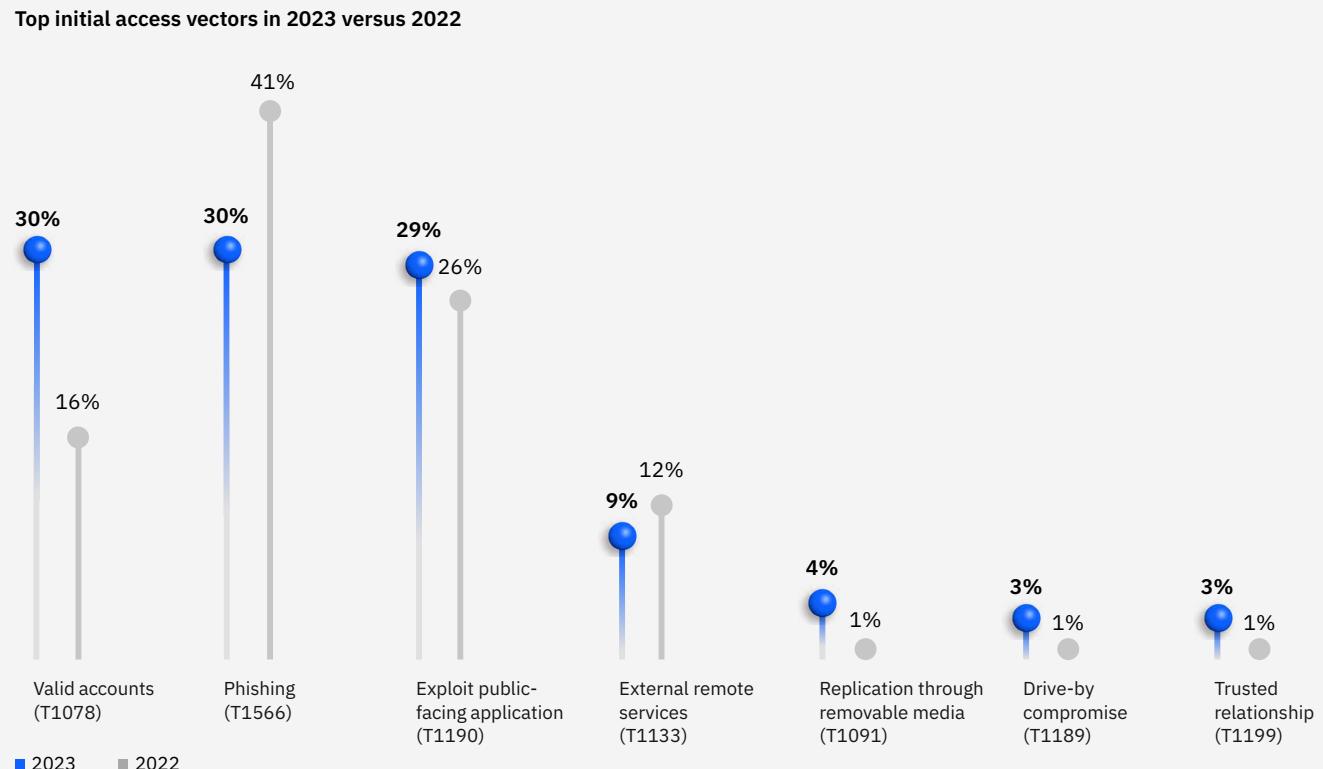


Figure 1: Top initial access vectors X-Force observed in 2022 and 2023.
Sources: X-Force and MITRE ATT&CK Matrix⁴ for Enterprise framework

Top initial access vectors

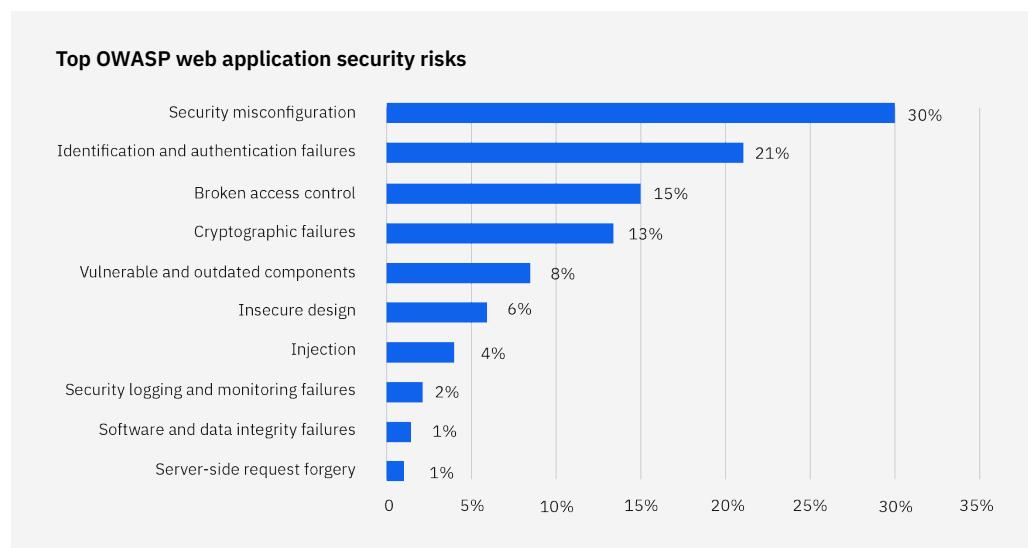


Figure 2. Top OWASP web application security risks based on penetration testing data. Source: X-Force

In second place, identification and authentication failures made up 21% of the most observed web application security risks. Of these findings, the top offenses were weak password policies that included Active Directory password policies (19%), usernames verifiable through errors (17%), Server Message Block (SMB) signing not required and URLs containing sensitive information at 8% each.

Zero-day decline

Every year there are a few vulnerabilities that catch enterprises by surprise and cause widespread damage. In 2023, the CL0P ransomware group exploited a vulnerability in the file transfer application MOVEit, common vulnerabilities and exposures (CVE)-2023-34362, to expose information on millions of individuals.

Top actions on objectives

According to IBM X-Force Incident Response data, deployment of malware was the most common action threat actors took on victim networks, occurring in 43% of all reported incidents. Of the total incidents, 20% were ransomware cases. Backdoors and crypto miners were discovered in 6% and 5% of cases, respectively. The remaining malware incidents included info stealers, loaders, bots, worms, web shells and downloaders.

Top actions on objectives 2023

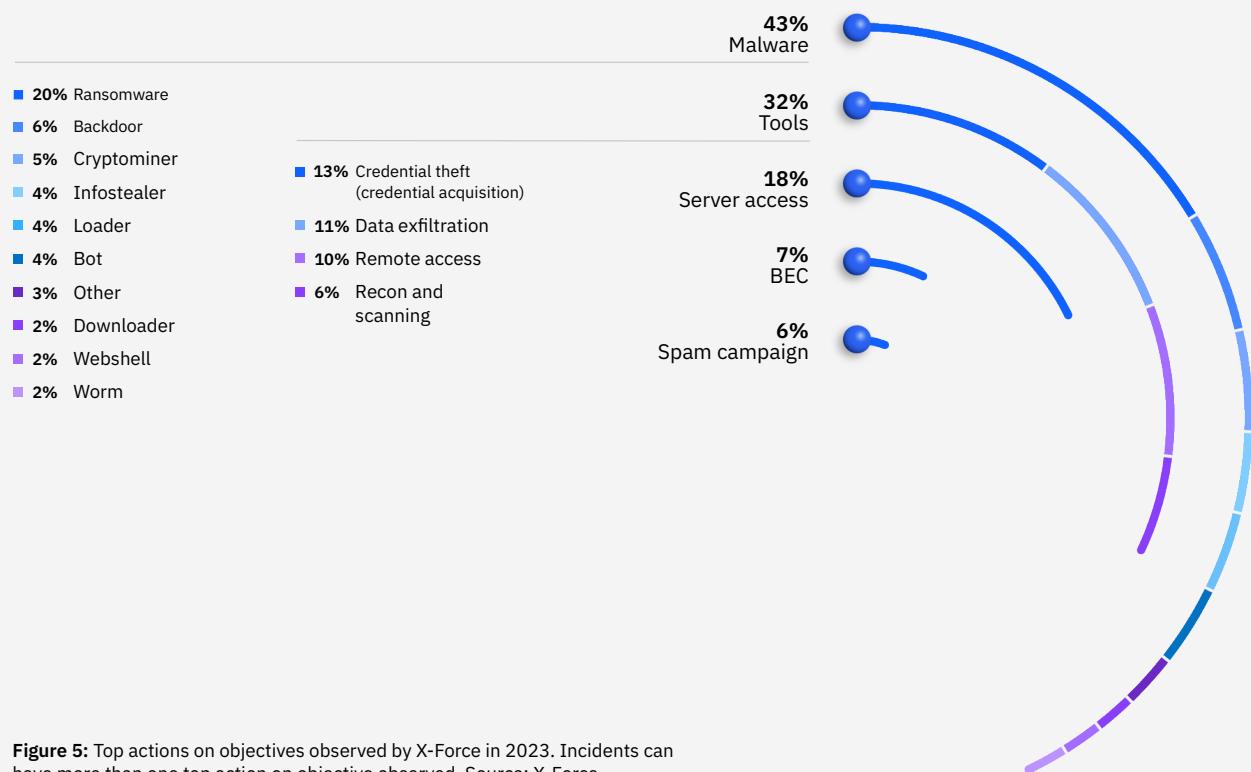


Figure 5: Top actions on objectives observed by X-Force in 2023. Incidents can have more than one top action on objective observed. Source: X-Force

Top impacts

The top impact to organizations was data theft and leak, making up 32% of the incidents X-Force responded to—accounting for 19% of the incidents in 2022. This increase aligns with the rise in observed infostealer activity and use of legitimate tools to exfiltrate data. Furthermore, extortion incidents more than doubled in 2023, and the share of all incidents that were extortion increased from 21% in 2022 to 24% in 2023.

As mentioned, extortion-based attacks remained one of the driving forces of cybercrime in 2023 with threat actors leveraging various attack types to deliver on their extortion objectives.

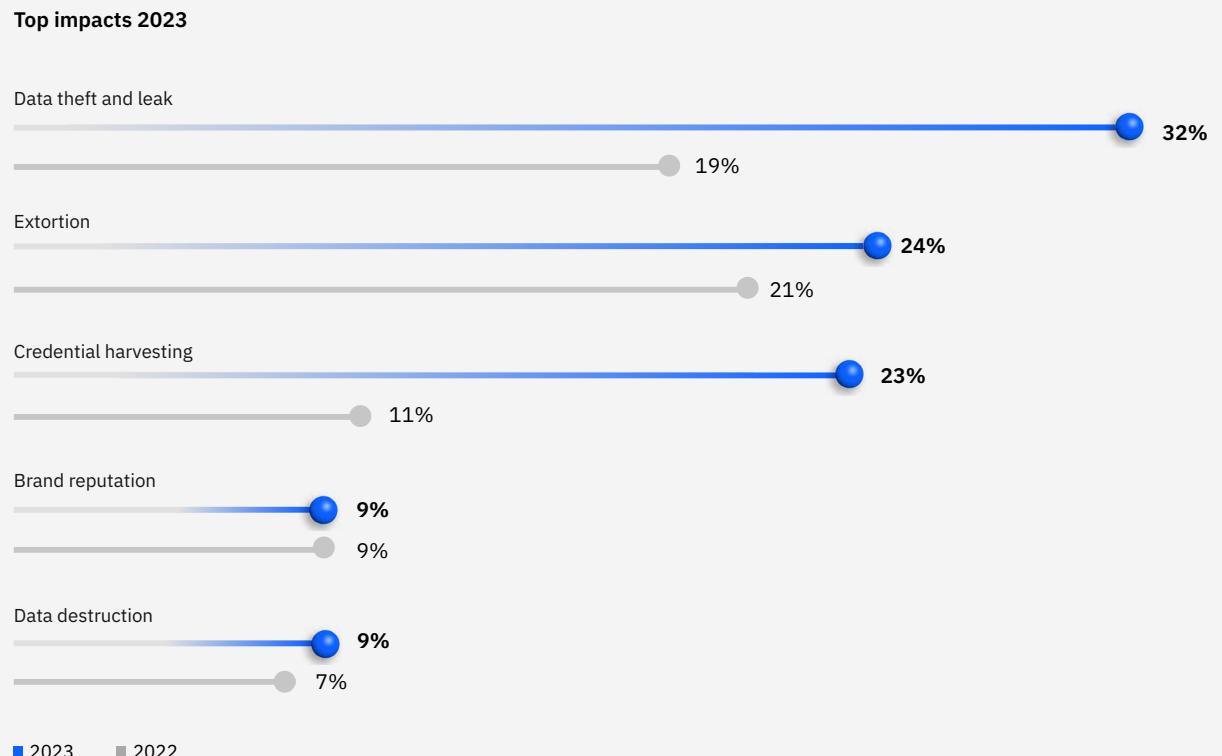


Figure 7: Top impacts X-Force observed in incident response engagements in 2023. Incidents can have more than one impact observed. Source: X-Force

Geographic trends

In 2021 and 2022, the Asia-Pacific region held the top spot as most impacted region, with Europe trailing behind as the second-most impacted. In 2023, Europe earned the number one spot as the most-impacted region, accounting for 32% of incidents to which X-Force responded. North America represented 26% of incidents, while Asia-Pacific saw 23%, Latin America 12% and the Middle East and Africa 7%.

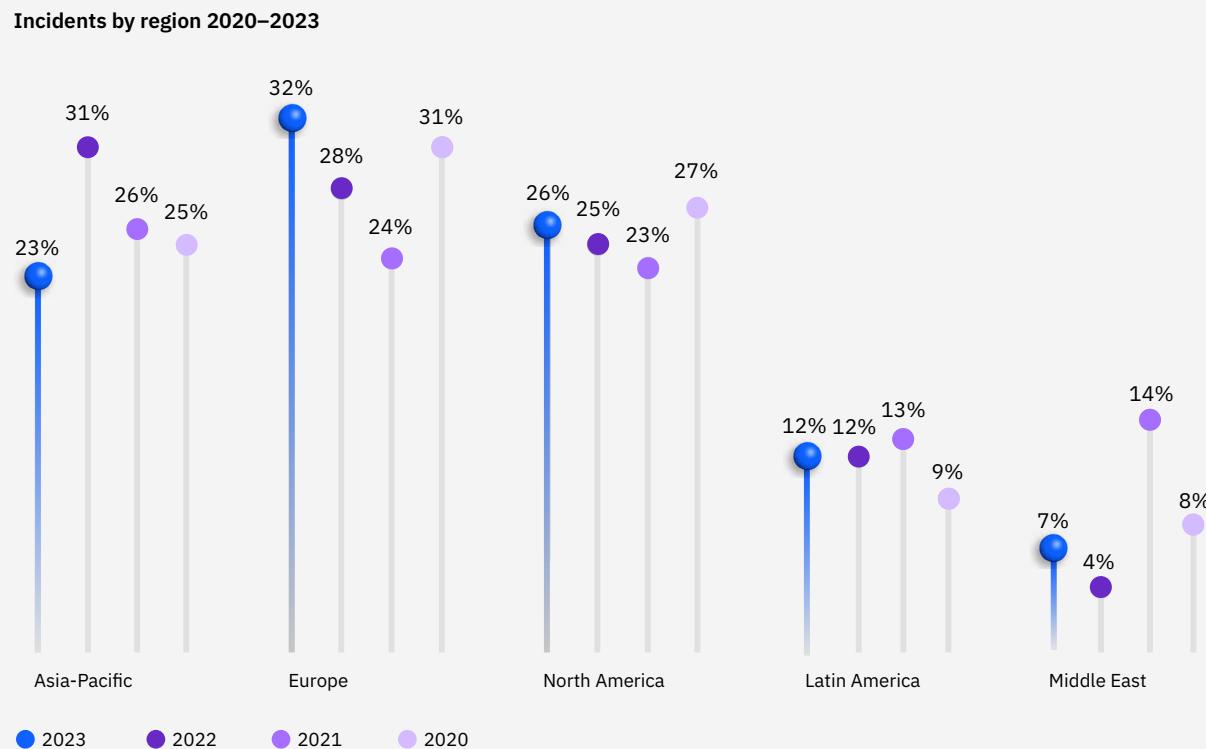


Figure 13: Proportion of incident response cases by region to which X-Force responded from 2021 through 2023. Source: X-Force

Share of attacks by industry 2019–2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

45%

of manufacturing attacks
employed malware

#1 | Manufacturing

Manufacturing was once again the top attacked industry in 2023 for the third year in a row, representing 25.7% of incidents within the top 10 industries. Malware was the top action on objective observed at 45%. Ransomware accounted for 17% of incidents, which is what was observed in 2022. The use of legitimate tools for malicious purposes was observed in 31% of incidents, with the use of tools to steal credentials the top offender at 17%. Server access incidents accounted for 21% of the cases, which is an increase from 2022 where these cases accounted for 17%.

Credential harvesting and data theft and leak were both the top impacts on manufacturing organizations, involved in

36% of incidents each, followed by data destruction and extortion at 16% of cases each. Phishing was the top initial infection vector, representing 39% of incidents, impacting the manufacturing industry, followed by exploitation of public-facing applications at 33%, and abuse of external remote services at 22% of cases.

Once again, the Asia-Pacific region saw the most incidents in manufacturing in approximately 54% of cases. Europe saw the second most at 26%, followed by North America at 12% and Latin American at 5%.



38%

of finance and insurance incidents involved malware

#2 | Finance and insurance

Finance and insurance trailed behind manufacturing as the second most attacked industry in 2023 for the third year in a row, representing 18.2% of incidents to which X-Force responded. Malware was the most common action on objective observed, accounting for 38% of incidents within the finance and insurance industry, with ransomware accounting for 25% of cases. Server access cases came in second at 25% of attacks, while the use of legitimate tools for malicious purposes was the third most observed action on objective, accounting for 19% of incidents.

Extortion was the top impact observed on finance and insurance organizations in 2023 at 35%, followed by botnet at 28%

and credential harvesting at 19%. The use of phishing was the most common initial infection vector at 28%, followed closely by the use of valid accounts in 27% of cases remediated by X-Force. The third most observed initial access vector was the abuse of external remote services at 27%.

Europe once again experienced the highest percentage of incidents in the finance and insurance industry at 37%, while Latin America saw the second most at 17% with North America, the Middle East and Africa, and the Asian-Pacific each experiencing 15% of attacks.



22%

of professional, business and consumer services malware cases involved crypto miners

Industry trends

#3 | Professional, business and consumer services

The professional, business and consumer services sector was the third most attacked industry, accounting for 15% of cases. The professional services industry includes consultancies, management companies and law firms. These services make up 34% of victims in this segment. Business services include firms such as IT and technology services, public relations, advertising and communications. These services represent 42% of victims. Consumer services, encompassing home builders, real estate, arts, entertainment and recreation, accounted for 24% of cases.

Malware cases represent half of observed incidents in the professional, business and consumer services sector. Notably, crypto

miners were the most observed malware, accounting for 22% of all cases. The use of legitimate tools for malicious purposes was the second most observed action on objective, accounting for 21% of incidents and spam campaigns and server access cases tied for third representing 14% of attacks each.

The top infection vector was the use of valid accounts observed in 46% of incidents. In second place was phishing at 31% and exploitation of public-facing applications came in third at 24% of attacks. Digital currency mining and credential harvesting tied as the most common impact, representing 27% of cases each, followed by extortion at 18% of cases.



X-Force responded to 49% of cases in Europe, 36% in North America, 7% in the Asia-Pacific, 5% in the Middle East and Africa, and 3% in Latin America.

43%

of energy cases involved malware

#4 | Energy

Energy organizations, including electric utilities and oil and gas companies, were the fourth most attacked industry, representing 11.1% of attacks. Malware was the most common action on objective observed, representing 43% of cases, with ransomware cases accounting for 22% of attacks. The use of legitimate tools for malicious purposes was the second most observed action on objective, accounting for 36% of incidents and server access incidents followed at 21%.

Data theft and leak accounted for the top impact on energy organizations at 33% of observed cases, followed by digital

currency mining and extortion tying for 22% of incidents each. The exploitation of public-facing applications was the top initial infection vector, representing half of the cases, followed by the use of valid local accounts at 38% and replication through removable media in 13% of cases.

Europe experienced the highest percentage of incidents within the energy sector at 43%, followed by North America at 22%, Latin America at 14% and the Middle East and Africa and Asia-Pacific at 11% each.



50%

of incidents in the retail and wholesale industry involved malware

Industry trends

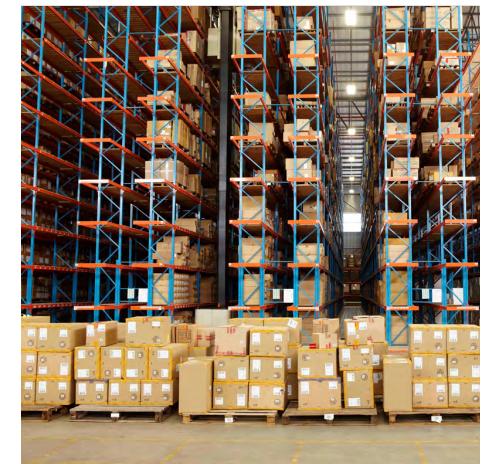
#5 | Retail and wholesale

In 2023, the retail and wholesale industry accounted for 10.7% of all incidents to which X-Force responded. Retailers are responsible for the sale of goods to consumers and wholesalers. Wholesalers are typically responsible for the transportation and distribution of these goods directly from manufacturers to retailers or directly to consumers.

Malware was the most common action on objective observed, accounting for 50% of incidents within the retail and wholesale industry, with ransomware accounting for 26% of total cases. BEC cases came in second at 38% of attacks, while the use of legitimate tools for malicious purposes, server access and spam campaigns tied as the third most observed action on objective, accounting for 13% of incidents each.

The top impacts observed on retail and wholesale organizations in 2023 at 25% each were illicit financial gain, reconnaissance and extortion. The use of valid accounts was the most common initial infection vector at 43%, followed by phishing and the exploitation of public-facing applications, each representing 29% of the cases. Leveraging drive-by compromise was observed in 14% of cases.

North America experienced the highest percentage of incidents in this industry at 56%, while Latin America saw the second most at 32% and Europe experienced 11% of attacks.



59%

of healthcare incidents involved valid account abuse

#6 | Healthcare

Moving up one spot from the seventh most attacked in 2022 to sixth most attacked in 2023 and accounting for 6.3% of total attacks is healthcare. The use of legitimate tools for malicious purposes was the most observed action on objective, accounting for 43% of incidents, and spam campaigns and malware cases tied for second, representing 29% of attacks each. Email thread hijacking and server access cases each represented 14%.

The top infection vectors observed in the healthcare industry was the use of valid accounts at 59% of incidents. The exploitation of public-facing applications

at 21% and the use of phishing at 20% rounded out the top three. The top impact observed was credential harvesting, accounting for half of the cases, followed by reconnaissance, data leak and extortion, each representing 25% of the cases.

X-Force responded to 50% of cases in North America, 38% in Europe, 6% in the Asia-Pacific and 6% in Latin America.



40%

of government incidents involved phishing incidents

#7 | Government

Accounting for 4.3% of incidents—and moving up one spot from 2022—government was the seventh most attacked industry in 2023. The use of legitimate tools for malicious purposes and DDoS attacks were the most observed actions on objective, each accounting for 33% of incidents. Server access, adware and malware each accounted for 17% of cases.

The top infection vector observed in government was phishing at 40% of incidents. The exploitation of public-facing applications, replication through removable media and drive-by compromises were each observed in 20% of cases. The top impacts observed were credential harvesting, data leak, extortion and botnet activity, each representing 33% of the cases.

In 2023, government entities, though representing a small fraction of reported incidents, witnessed an uptick in cybersecurity threats, according to X-Force, compared to 2022. Despite being the least likely to meet ransom demands, governments remain attractive targets for criminal threat actors.

The persistence of cybercriminals in targeting government networks is fueled by the vast amount of sensitive data these entities possess, obtained through the wide range of services provided to companies and people. Successful breaches could result in the leakage of state-level intelligence, classified assets and personal identifiable information (PII). Such leakage poses risks, such as identity theft, creation of forged documents, unauthorized access



to organizations and the takeover of privileged accounts through the sale of stolen data in dark marketplaces.

X-Force responded to 64% of cases in North America, 26% in the Asia-Pacific and 9% in the Middle East and Africa.

67%

of transportation incidents involved data leak and extortion

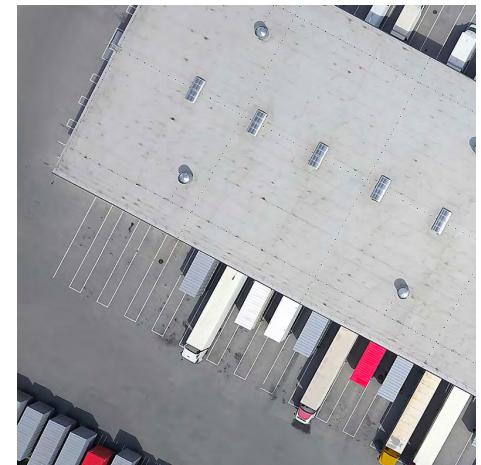
#8 | Transportation

Up from ninth place in 2022, transportation accounted for 4.3% of incidents and ranked eighth in 2023. Malware and the use of legitimate tools for malicious purposes were the top actions on objective observed, both representing 38% of attacks. Server access attacks were observed in 13% of incidents.

Data leak and extortion were both the top impacts on transportation organizations, involved in 67% of incidents each, followed by data destruction at 33%. The exploitation of public-facing applications

and use of phishing were the top initial infection vectors, each representing 50% of incidents impacting the transportation industry, followed by use of valid local accounts, used in 25% of attacks.

Unlike 2022, where European transportation entities were the most targeted group, in 2023, the Asia-Pacific experienced the most attacks at 63%. The Middle East and Africa accounted for 27% of attacks in this industry, while Europe accounted for 10%.



2.8%

of incidents remediated by X-Force were in the education sector

#9 | Education

Dropping from sixth place in 2022 to ninth place in 2023, education accounted for 2.8% of incidents remediated by X-Force. Notably, malware was the most commonly observed action on objective, while X-Force also observed the use of legitimate tools for malicious purposes in a larger portion of incidents.

Data theft, data destruction and extortion were the top impacts on education organizations. Top initial infection vectors included phishing and the use of valid accounts. Most commonly, X-Force responded to incidents across education in North America and the Asia Pacific.



1.2%

of incidents X-Force responded to involved media and telecommunications

#10 | Media and telecommunications

Media and telecommunications accounted for only 1.2% of incidents to which X-Force responded, coming in last place for the third year running. The use of legitimate tools for malicious purposes and server access were commonly observed actions on objective. Media organizations were predominantly targeted in the Middle East, the Asia Pacific and Europe regions.



Ransomware: the **true cost**

to business 2024



Our Annual Global Study on Ransomware Business Impact
Attackers are evolving. Paying isn't the solution. **It's time to reject the ransom.**

 **cybereason**[®]

The results at a glance

This year's results paint an interesting picture. Despite being breached before, many defenders don't believe their organizations have the right people and plans in place to manage the next attack.

Attackers are evolving

More complex, low-and-slow attacks are designed to compromise as much of the targeted network as possible to exact the highest ransom in 'RansomOps' attacks.

59%

said their organization didn't detect a breach for **3-12 months**.

What were they after?



Intellectual Property (IP)/ Trade secrets



Personally Identifiable Information (PII)



Protected Health Information (PHI)



Customer data



Account credentials

How did they get in?

41%

got in via a **supply chain partner**.

24%

got in **directly**.

22%

got in with the help of **an insider**.

Paying the ransom isn't the solution

Despite most victims agreeing to pay the ransom, **less than half who did got their systems and data back uncorrupted**. And **most were breached again** within a year.



Why did they pay the ransom?



Attackers threatened to disclose sensitive information



We feared loss of business



It seemed to be the fastest solution



It was a holiday/weekend and we were short-staffed



It was a matter of life and death



We didn't have backup files

78%

were then breached again.

And

63%

of these were asked to **pay more** the second time.

82% were breached again within a year.
36% by the same actor.

42% by a different actor.

The true impact is staggering

Ransom fees remain high, and they're just the tip of the iceberg when it comes to the true cost to a business.

40%

estimate business losses of \$1-10 million.

16%

estimate losses of over \$10 million.

Average ransom payments over the last 24 months:

USA: \$1.4 million

France: \$1 million

Germany: \$762k

UK: \$423k

The true **cost** is much **higher** and includes:

- Brand damage
- Lost revenue
- Temporary closure
- C-level resignations
- Layoffs

Businesses need to do more

Most organizations **increased their investment** in cybersecurity after a breach, but the **risk remains**.

Less than half of defenders say they're adequately prepared for the next attack.



37%

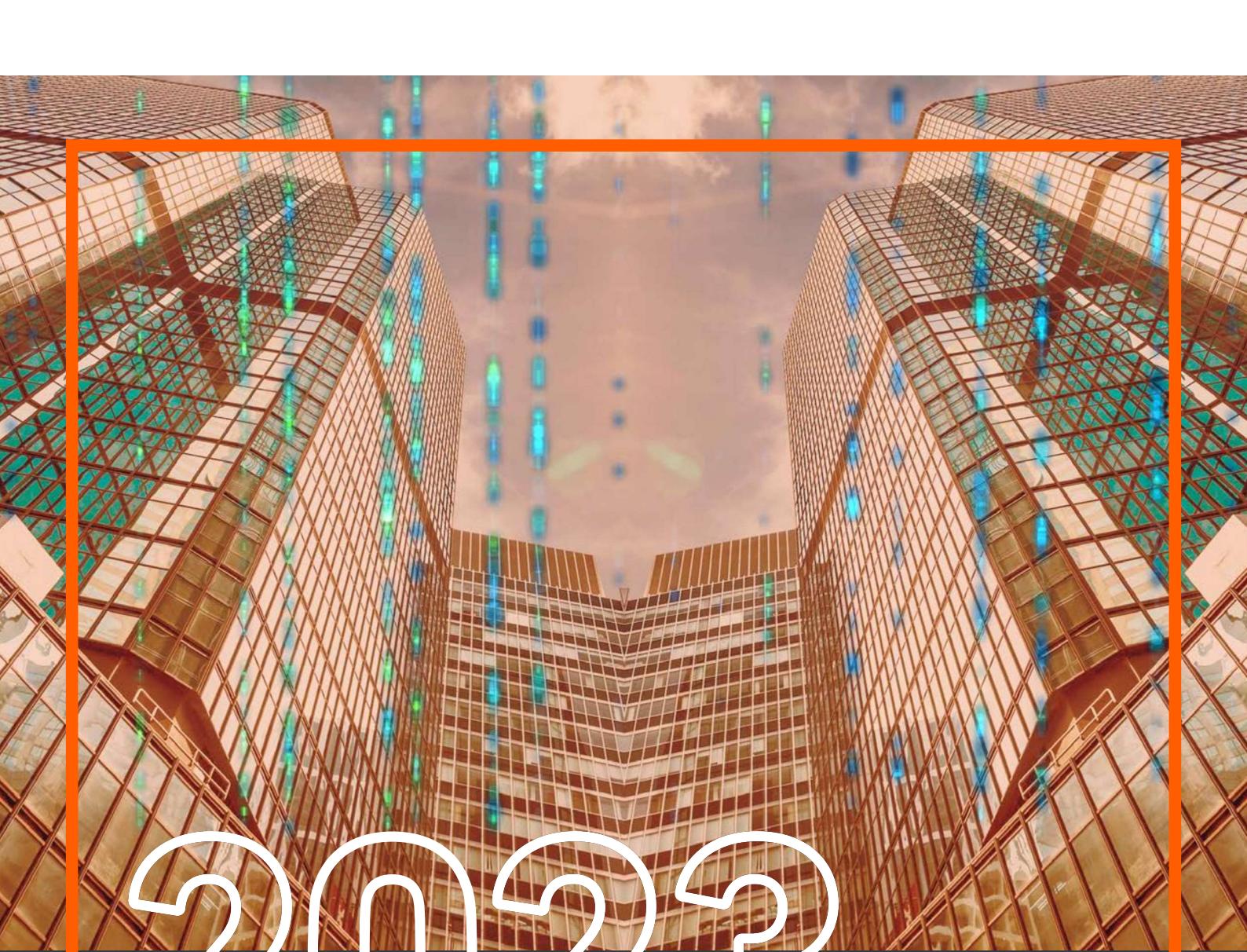
have the **right people**
but not the plan.

18%

have the **right plan**
but not the people.

They're investing in:

1. Cybersecurity talent
2. Awareness training
3. New tech (e.g. endpoint tech & identity services)
4. Increased internal/supply chain compliance
5. Cyber insurance
6. Cryptocurrency wallets

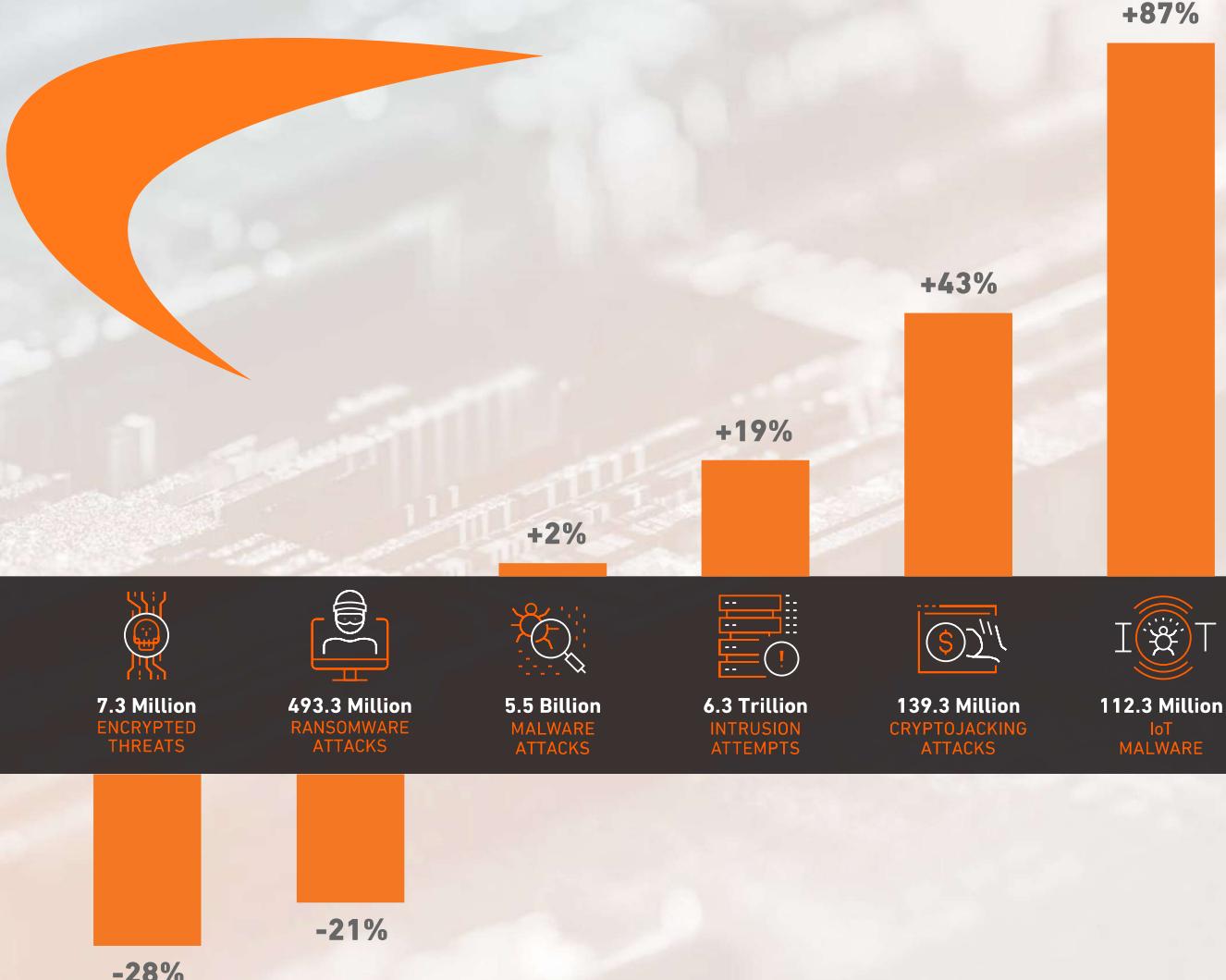


2023

SONICWALL CYBER THREAT REPORT

CHARTING CYBERCRIME'S
SHIFTING FRONTLINES

2022 GLOBAL ATTACK TRENDS



As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries.

While the past several years have given the cybersecurity world plenty to worry about, there have nonetheless been a few things we could count on. Malware was falling. Ransomware was rising. And attackers continued to prioritize targets in the U.S.

But from start to finish, 2022 was characterized by change. Ushered in by the announcement of the historic Log4j vulnerabilities just weeks before, the year brought a seismic shift in cybercriminal behavior that sent ripples across every region and every industry.

Ransomware Remains Top of Mind in 2022

While ransomware was on the decline in 2022, it was still ranked as the top threat in [SonicWall's inaugural Threat Mindset survey](#), released in August.

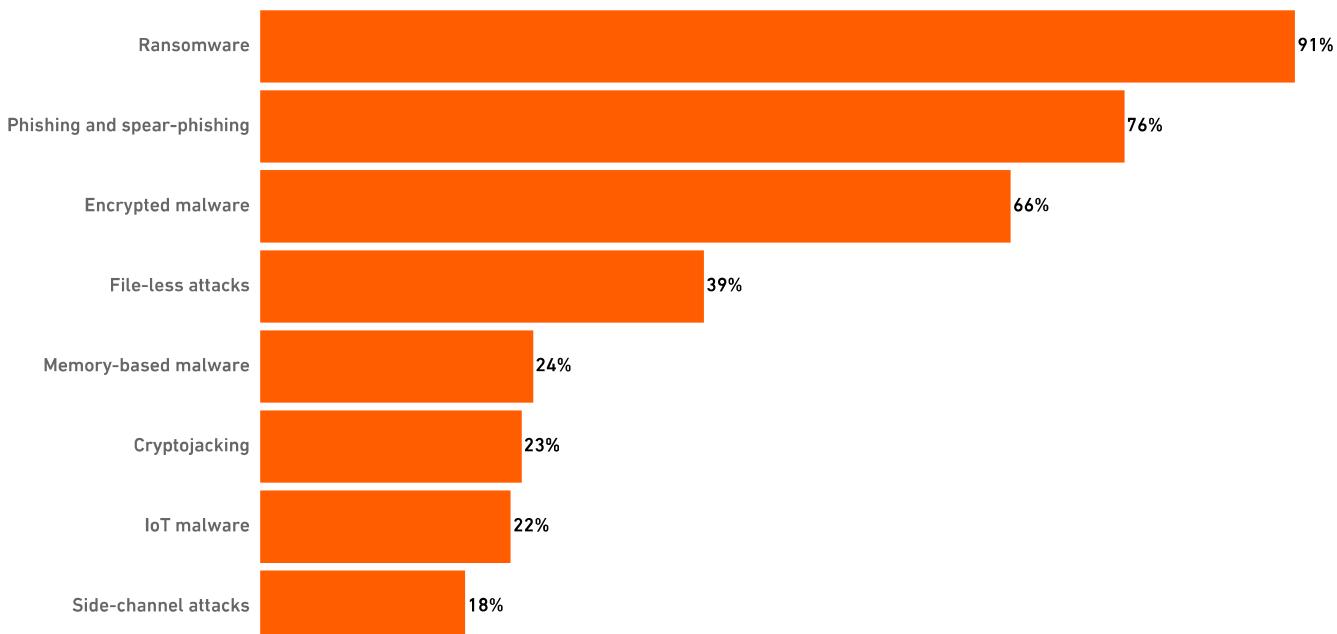
For this survey, SonicWall surveyed customers across a variety of industries located around the globe, asking a series of questions to evaluate the sentiments of those "on the ground" in the war on cybercrime.

When asked what types of cyberattack they're most concerned about, 91% of respondents answered ransomware. Phishing and spear-phishing, which are often used as vectors for ransomware, were ranked second, with roughly three-quarters of respondents rating them as a concern.

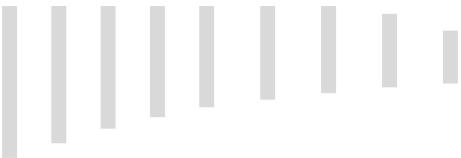


WHEN ASKED WHAT TYPES OF CYBERATTACK THEY'RE MOST CONCERNED ABOUT, 91% OF RESPONDENTS ANSWERED RANSOMWARE.

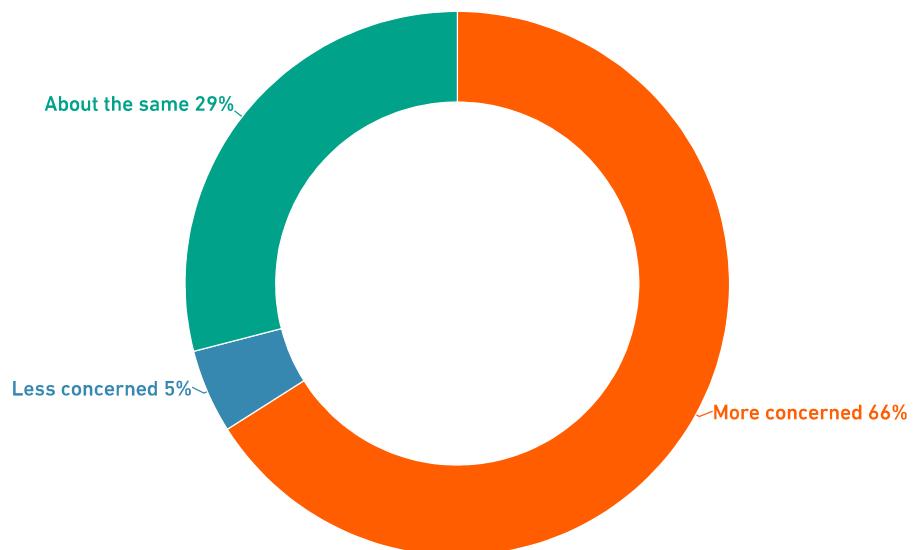
Which types of cyberattacks are you most concerned about?



Source: 2022 SonicWall Threat Mindset Survey.



Are you more or less concerned about cyberattacks in your organization in 2022 than in previous years?



Source: 2022 SonicWall Threat Mindset Survey.

What's more, 66% of respondents reported being more concerned about attacks this year than last year, with another 29% reporting that they have roughly the same amount of concern about attacks as they did in 2021. Only 5% reported being less concerned.

The survey's open-ended questions provided a more in-depth look at how respondents were perceiving their risk, along with what they planned to do about it.

"Frankly, I live in terror of a ransomware attack and state-sponsored intrusions. On my logs, I have seen massive increases in probes from Russia, China and a handful of other (what I would call) enemy nations," a business professional employed at a small business healthcare company said.

Another respondent, an IT director for a financial services business, said that they were doubling down on training in response to the recent increase in attacks.

"The evolving cyber landscape has made us train users a lot more," they said. "It's made us spend more on cybersecurity. It scares the hell out of me that an end user can click on something and bring our systems down — even though we're well protected."

For more on how SonicWall customers perceive the current state of cybersecurity — and their place in it — download the [2022 SonicWall Threat Mindset Survey](#).



CVEs

Published CVEs Break 25,000 for First Time

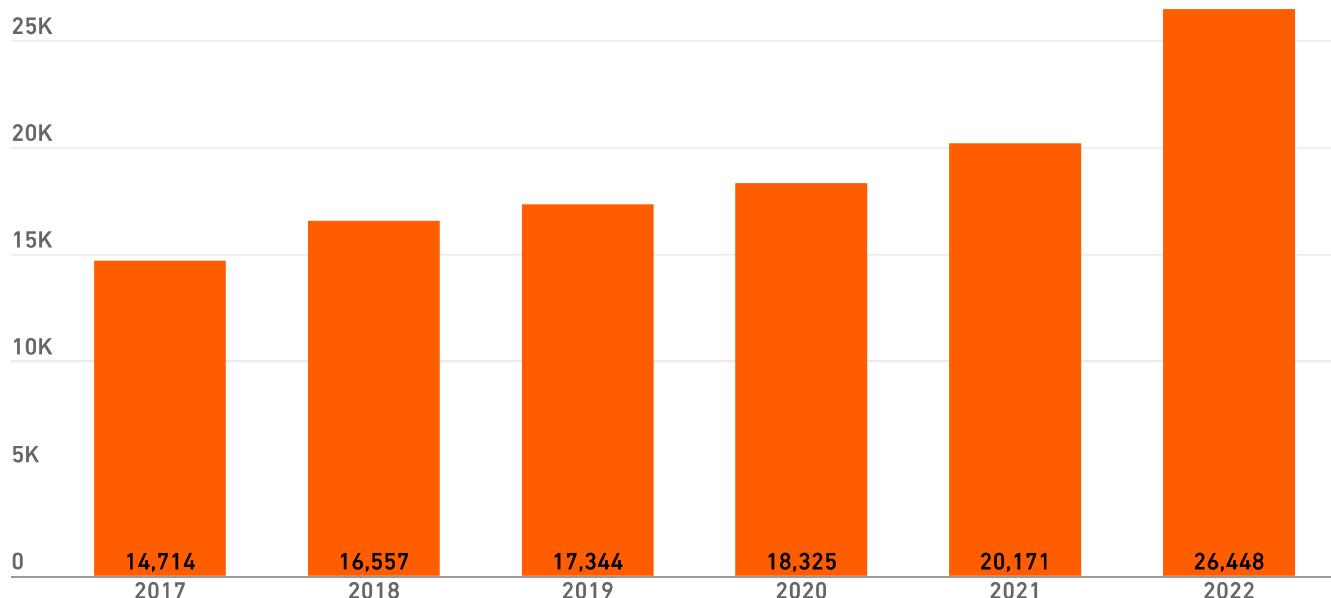
A total of 26,448 Common Vulnerabilities and Exposures (CVEs) were published in 2022, according to NIST. This marks the sixth year in a row that a record number of vulnerabilities has been discovered, and the first time in history that the number of CVEs has passed 25,000.

While this milestone represents the hard work those in the cybersecurity industry are doing to identify vulnerabilities more quickly and efficiently, it isn't necessarily cause for celebration. It also reflects the pernicious trends that make quicker and more efficient work necessary in the first place.

As organizations deploy more software and tools, the attack surface continues to grow. And the more products a company utilizes, the more likely it is that one will be vulnerable. (A good example of this is the Apache Log4j vulnerabilities; see [page 13](#))

The most severe vulnerabilities, the ones rated a nine or above on the 10-point scale, become entry points for cybercriminals, and attackers are increasingly utilizing this means of entry to deploy ransomware and other malware and to exfiltrate data.

CVEs by Year



UKRAINE

Ukraine Sees Unprecedented Attack Volume in 2022

While the Russia-Ukraine conflict may have resulted in suppressed ransomware attack volume in the rest of the world, it had a dark side: It sent attack levels through the roof in Ukraine, as cyber warfare zeroed in on both military targets and critical civilian and communication infrastructure.

Because SonicWall requires a minimum of 1,000 active sensors in a region for public reporting, and our footprint in Ukraine falls far short of that threshold, we don't generally report on cybercrime in Ukraine. But amid the ongoing conflict, the sensors we do have there recorded an enormous amount of malicious activity.

Despite Ukraine's relatively small number of sensors, the country appears high in the rankings when compared with other nations. With 7.1 million attacks in 2022, Ukraine ranks No. 13 in total ransomware volume, and also had the third-highest ransomware spread percentage at 2.23%.

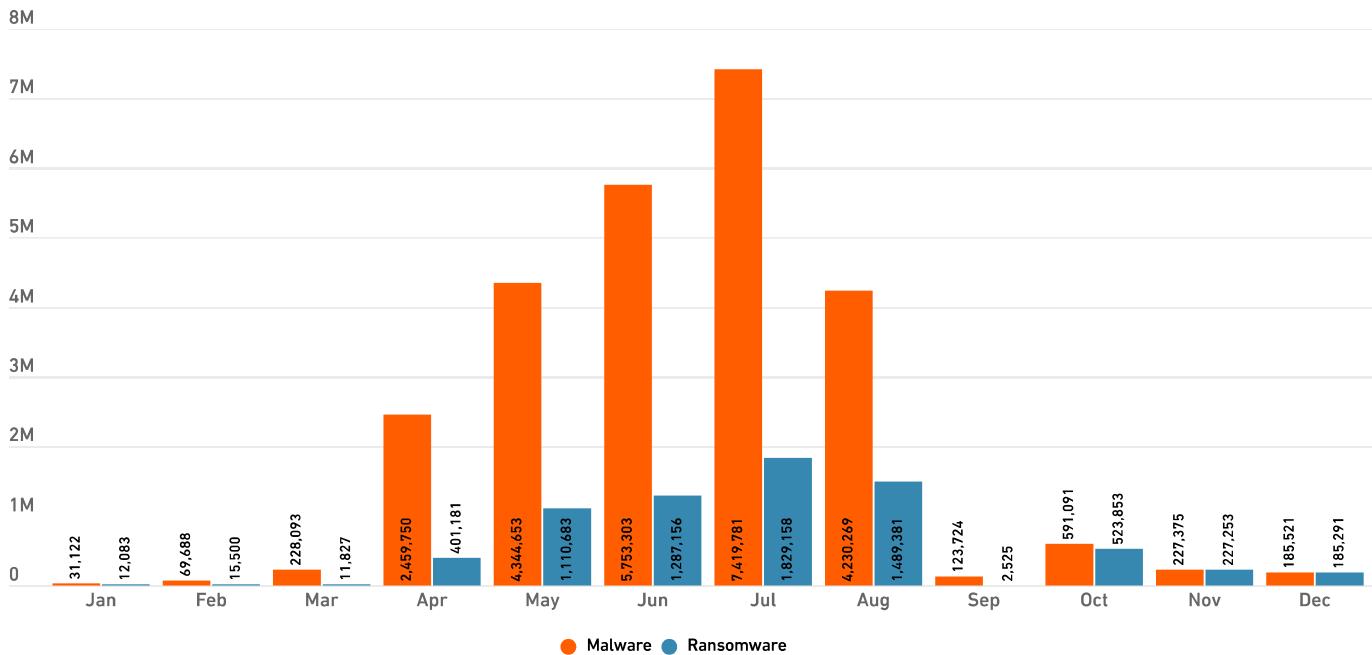
These numbers were fueled by a massive 8,105% increase in total malware and a 5,835% increase in ransomware.

Along with other Eastern European countries, Ukraine was once given preferential treatment among certain threat actors, [with a number of examples](#) specifically sparing [those living in the region](#).

The opposite seemed to be true in 2022, however, as SonicWall observed several attacks targeting Ukraine directly:

- [Caddywiper Hits Ukrainian Networks, Wipes Data and Renders Machines Unbootable](#)
- [A Look at PartyTicket Ransomware Targeting Ukrainian Systems](#)
- [HermeticWiper Data Wiping Malware Targeting Ukrainian Organizations](#)

2022 Attack Volume | Ukraine



Note: Threshold for statistical relevancy not met. SonicWall typically requires minimum of 1,000 active sensors for public reporting.

Key Findings from 2022



▲ 2%



▼ 21%



465K



139M



Malware

Malware rose for the first time since 2018, reaching 5.5 billion attacks—a 2% increase year over year. Skyrocketing cryptojacking and IoT malware rates fueled much of this jump.

[READ MORE ON PAGE 21. >>](#)

Ransomware

On the heels of 2021's meteoric highs, ransomware fell in 2022, with volumes dipping to 493.3 million. While this represents a 21% year-over-year decrease, it's still far above the levels seen in 2017, 2018, 2019 or 2020.

[READ MORE ON PAGE 33. >>](#)

RTDMI Discoveries

SonicWall's patented Real-Time Deep Memory Inspection™ discovered 465,501 never-before-seen malware variants in 2022. This new high-water mark pushed the all-time detection total past the 1 million mark.

[READ MORE ON PAGE 42. >>](#)

Cryptojacking

As cybercriminals shifted to lower-profile revenue sources in 2022, the number of cryptojacking attempts rose to a record high of 139.3 million.

[READ MORE ON PAGE 44. >>](#)

Key Findings from 2022



△ 87%



IoT Malware

With the number of connected devices continuing to rise, IoT malware jumped 87% year over year to a new high of 112.3 million.

[READ MORE ON PAGE 59. »](#)

△ 19%



Intrusions

The number of overall intrusion attempts in 2022 hit 6.3 trillion, a 19% increase over 2021's total. Fortunately, however, the number of *malicious* intrusions fell 10%.

[READ MORE ON PAGE 52. »](#)

△ 35%



Malicious PDF and Office Files

SonicWall Capture Advanced Threat Protection (ATP) sandbox recorded a 35% increase in the number of new PDF-based attacks in 2022. These attacks now make up 19% of total malicious files identified by Capture ATP.

[READ MORE ON PAGE 56. »](#)

▽ 17%



Phishing

Phishing decreased 17% globally in 2022, with Financial/Mortgage, Cryptocurrency, Healthcare and Pandemic the top themes for malicious emails.

[READ MORE ON PAGE 66. »](#)

▽ 28%



Encrypted Attacks

Encrypted attacks fell 28% year-over-year to 7.3 million, down from 10.1 million in 2021.

[READ MORE ON PAGE 50. »](#)

MALWARE

Malware Up for the First Time Since 2018

After three straight years of decline, malware reversed course in 2022, rising to 5.5 billion hits — a 2% increase year over year.

While the increase is small, it's being fueled by massive growth in two areas. In 2022, cryptojacking rose 43% and IoT malware jumped 87%. Together, these increases were more than enough to offset a 21% drop in global ransomware volume, pushing overall malware trends into positive territory for the first time since 2018.

But unlike the seismic shifts underpinning it, a quick look at the 2022 malware trend line reveals an unusual degree of stability. This is both good news and bad news: No massive jumps or upward trajectory means that, at least for the moment, malware growth isn't accelerating. But sustained levels of malware indicate that this uptick likely isn't just temporary — at least for the time being, elevated levels of malware are here to stay.

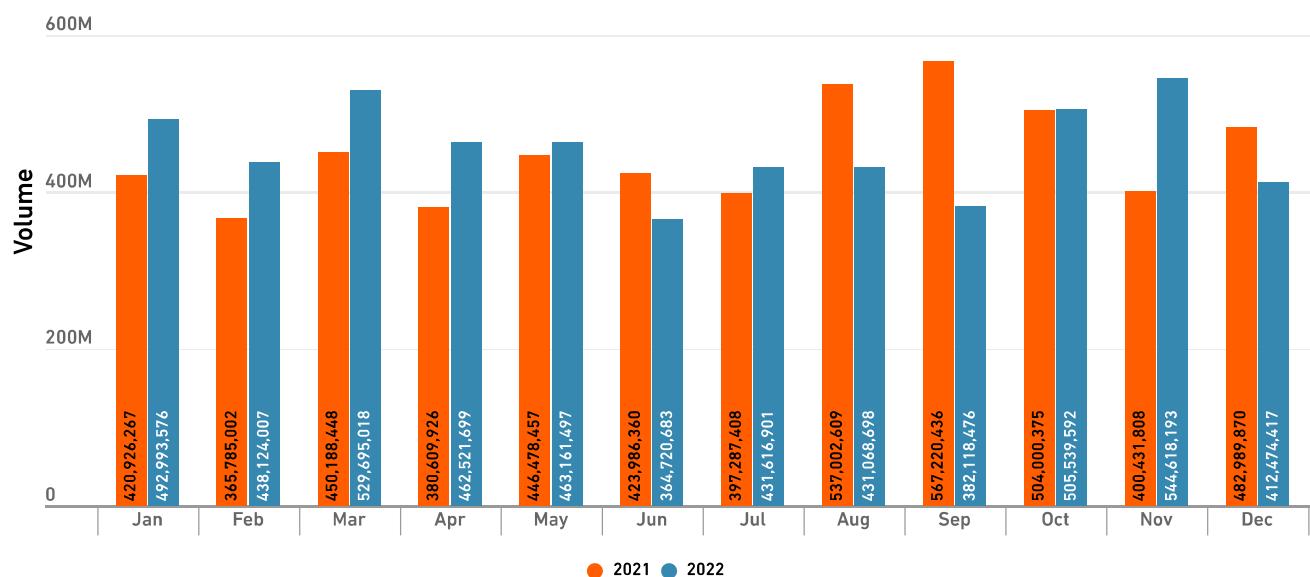
Malware by Region

In 2022, Europe, LATAM and Asia recorded double-digit increases of 10%, 17% and 38%, respectively.

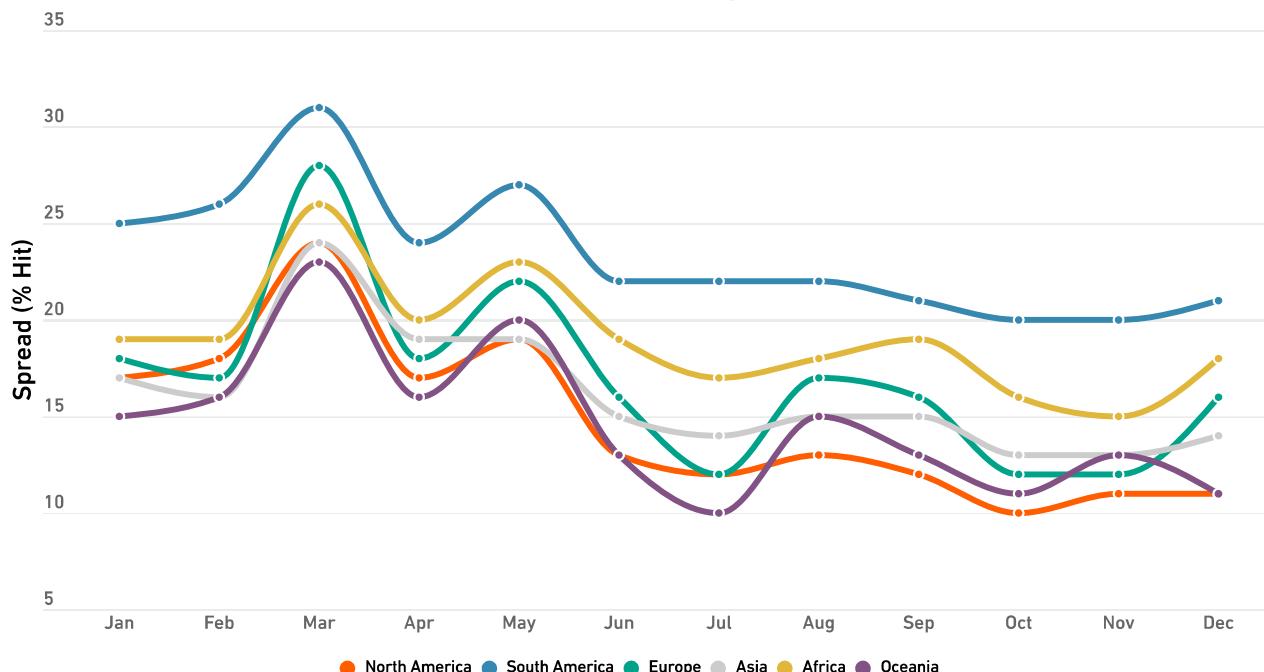
But North America, which has experienced the highest malware volume for four years running, showed a double-digit decrease, falling 10% year-over-year to 2.75 billion — its lowest volume since 2017.

And it's still trending downward: In December, malware attempts in North America fell to 158.9 million, the lowest monthly volume since 2018. Taken together, these trends suggest we're likely to see cybercriminals continue to shift from targets in North America and other cybercrime hotspots to elsewhere in the world.

Global Malware Volume



2022 Global Malware Spread Trend



What is Malware Spread?

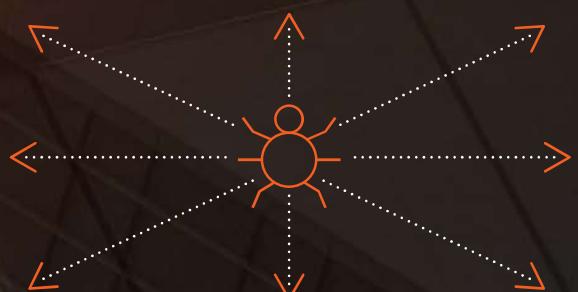
The data on the following pages offers a look at some of the countries with the highest malware volume. But just because a country sees a higher number of attacks doesn't mean that you're more likely to be targeted there.

Malware totals are useful in calculating trends, but they're of limited utility when determining relative risk: They ignore factors such as size, population, number of sensors and more.

To figure out the odds of a given organization in a particular area seeing an attack, we use the malware spread percentage — a calculation of what percentage of sensors recorded a malware attack.

If we think of malware volume as being similar to the total amount of rainfall in a region, then malware spread percentage could be compared to the probability or precipitation, or "chance of rain."

In other words, while annual precipitation numbers can be useful in determining whether your area saw more rainfall than it did last year, it says nothing about whether your umbrella will see heavier use than your sunglasses. As with "chance of rain," malware spread percentage considers a variety of additional factors to provide a more meaningful risk assessment.



Malware Volume By Country

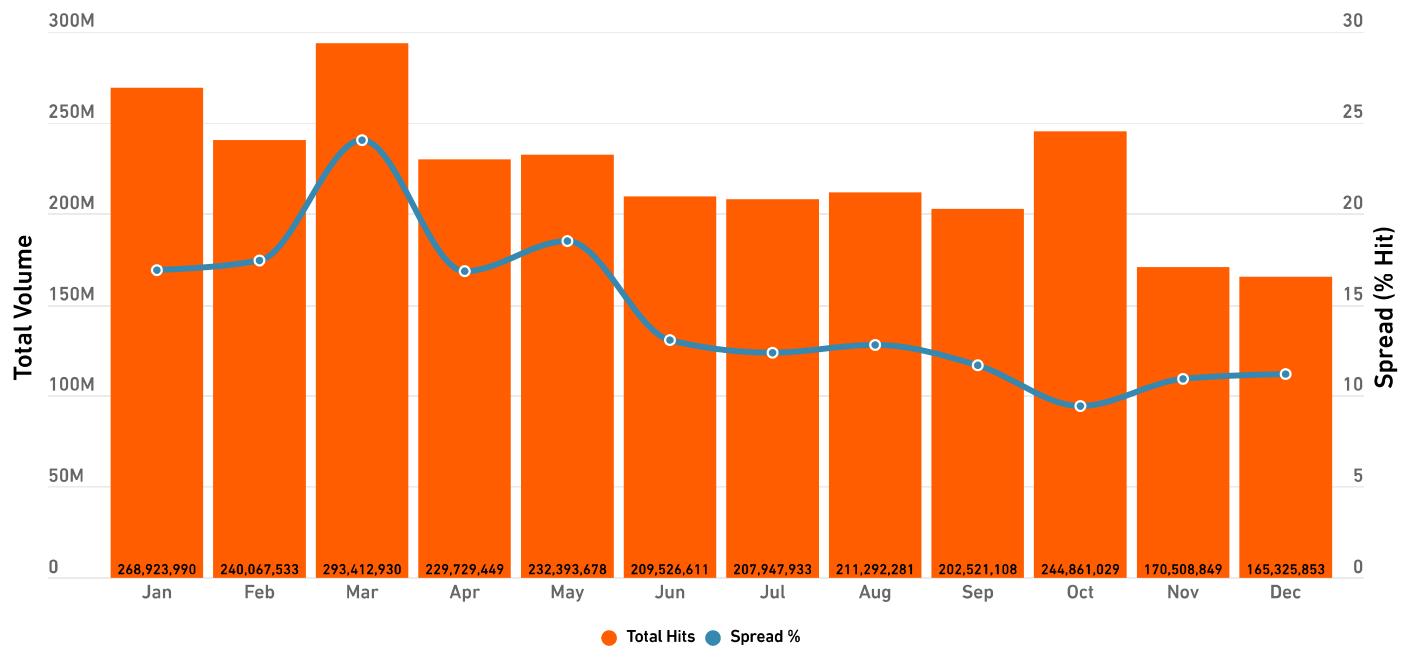
As in most years, 2022's country-level data showed a huge variety in outcomes, each of which contributes to the overall shifts we're seeing at the regional and global level.

To help illustrate the variety of ways that malware trends evolved over the past year, we looked at a sample of eight countries in a variety of regions, some near the top of the list in terms of malware volume, and some further down.

Despite their differences, these countries all happen to share two things in common. In each one, malware spread peaked in March, and each one had a lower average malware spread percentage in the second half than in the first half — which, considering there is no corresponding drop in volume, suggests that these attacks are becoming more targeted over time.



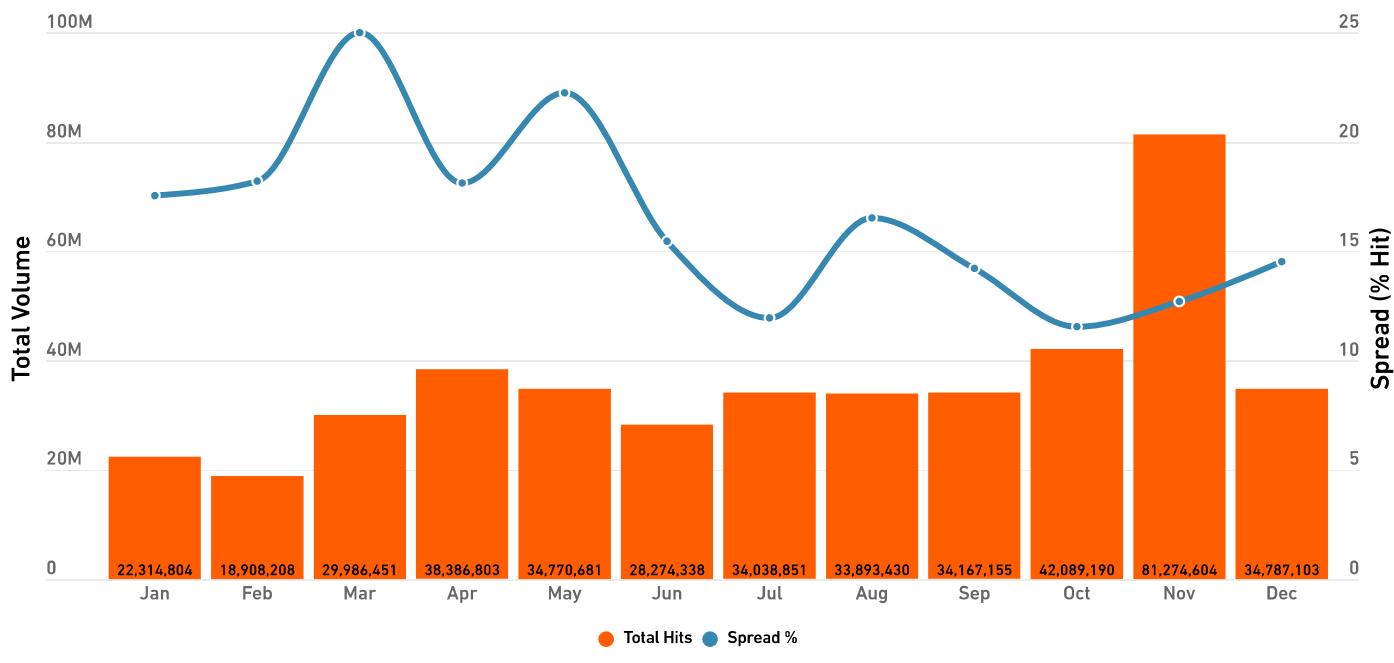
2022 Malware Attacks | United States



MALWARE RANK 2022 ATTACK VOLUME YoY CHANGE
1 **2.68 BILLION** -9%

After averaging more than 250 million in the first quarter, malware in the U.S. trended downward as cybercriminals began targeting other areas.

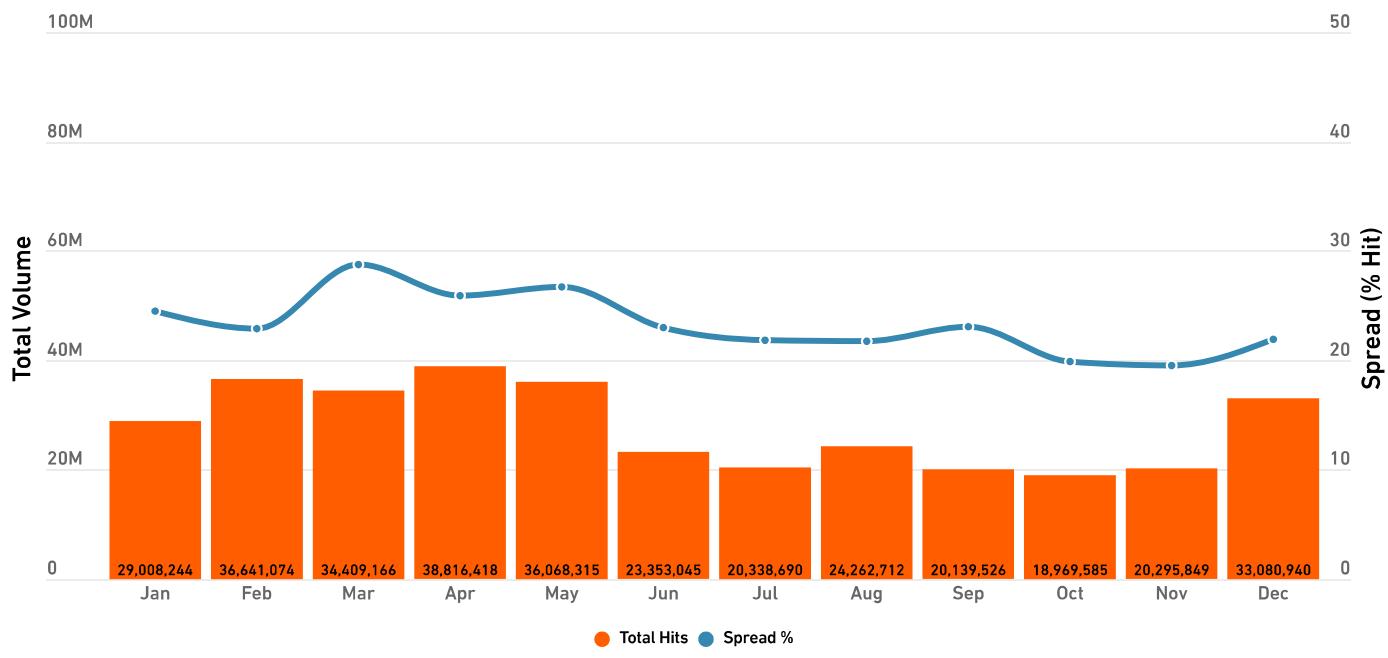
2022 Malware Attacks | United Kingdom



MALWARE RANK 2022 ATTACK VOLUME YoY CHANGE
2 432.9 MILLION -13%

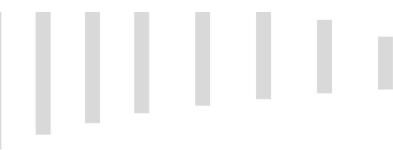
Malware in U.K. trended upward as 2022 went on, with Q4's totals up 122% from Q1's. But low volume in the first half contributed to an overall year-over-year decrease.

2022 Malware Attacks | India

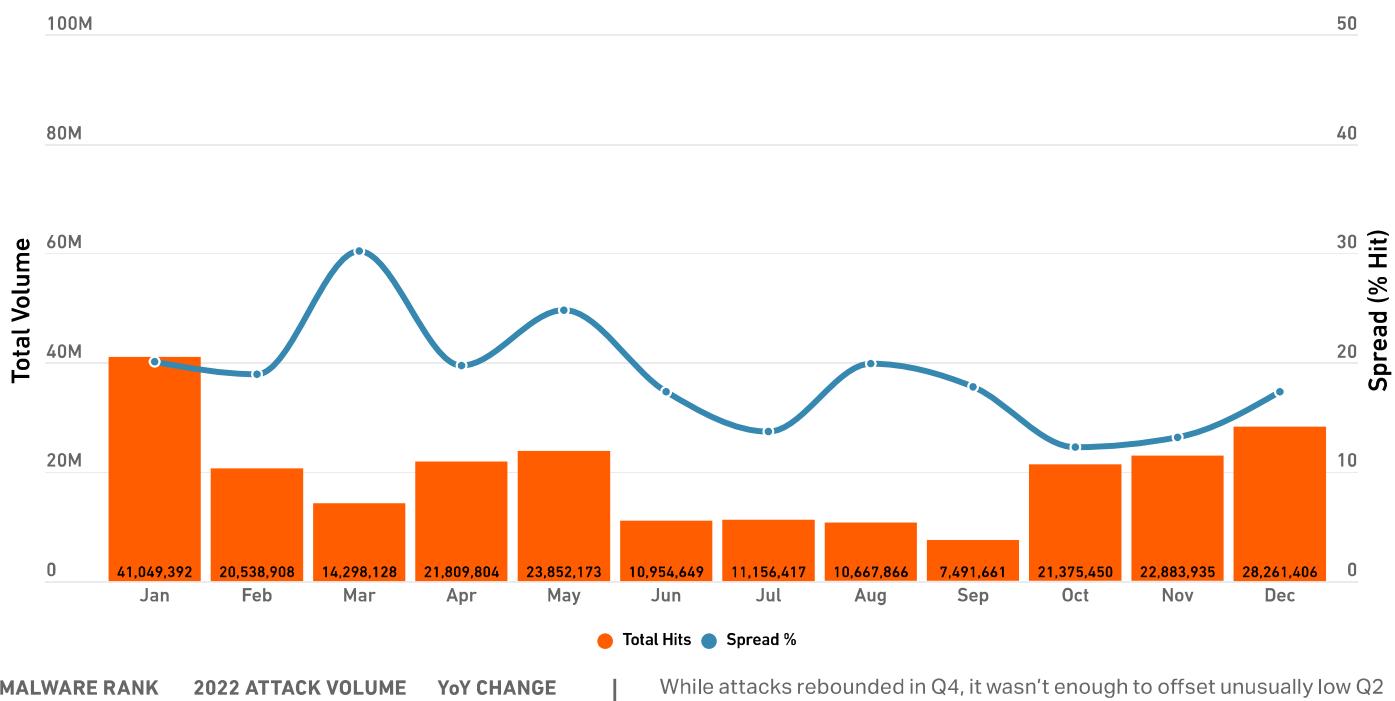


MALWARE RANK 2022 ATTACK VOLUME YoY CHANGE
3 335.4 MILLION +31%

Despite attack volumes mostly trending downward in 2022, India experienced the largest attack volume increase of any country we studied.



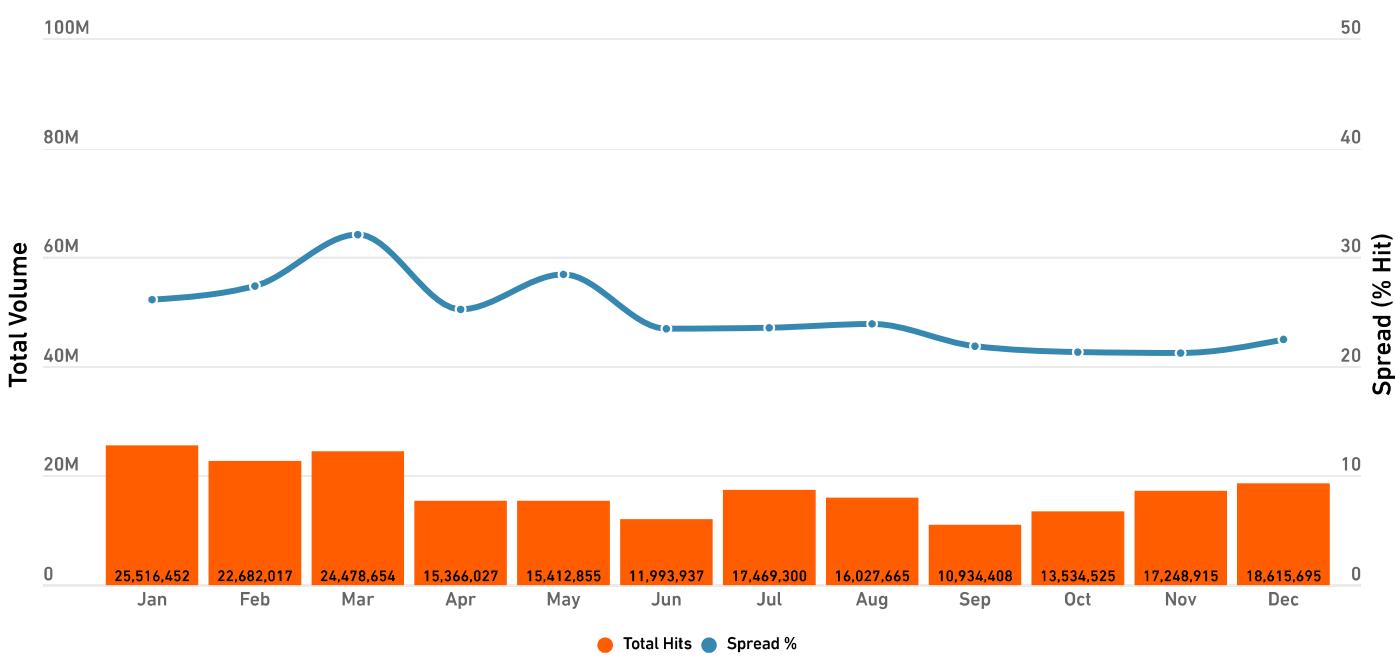
2022 Malware Attacks | Germany



MALWARE RANK 2022 ATTACK VOLUME YoY CHANGE
4 234.3 MILLION -28%

While attacks rebounded in Q4, it wasn't enough to offset unusually low Q2 and Q3 volumes. The resulting 28% drop was the biggest decrease of any country we studied.

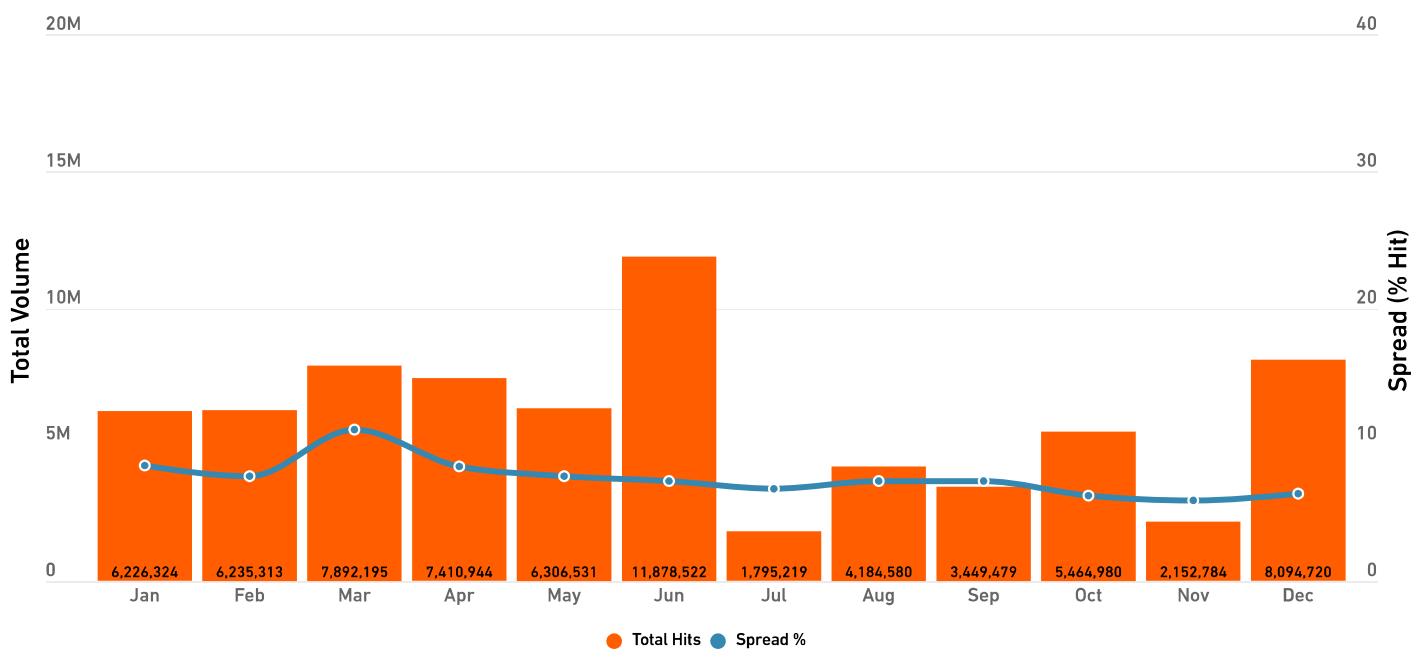
2022 Malware Attacks | Brazil



MALWARE RANK 2022 ATTACK VOLUME YoY CHANGE
6 209.3 MILLION -1%

With a difference of just 1.4 million between 2021's malware total and 2022's, yearly attack volume was essentially flat.

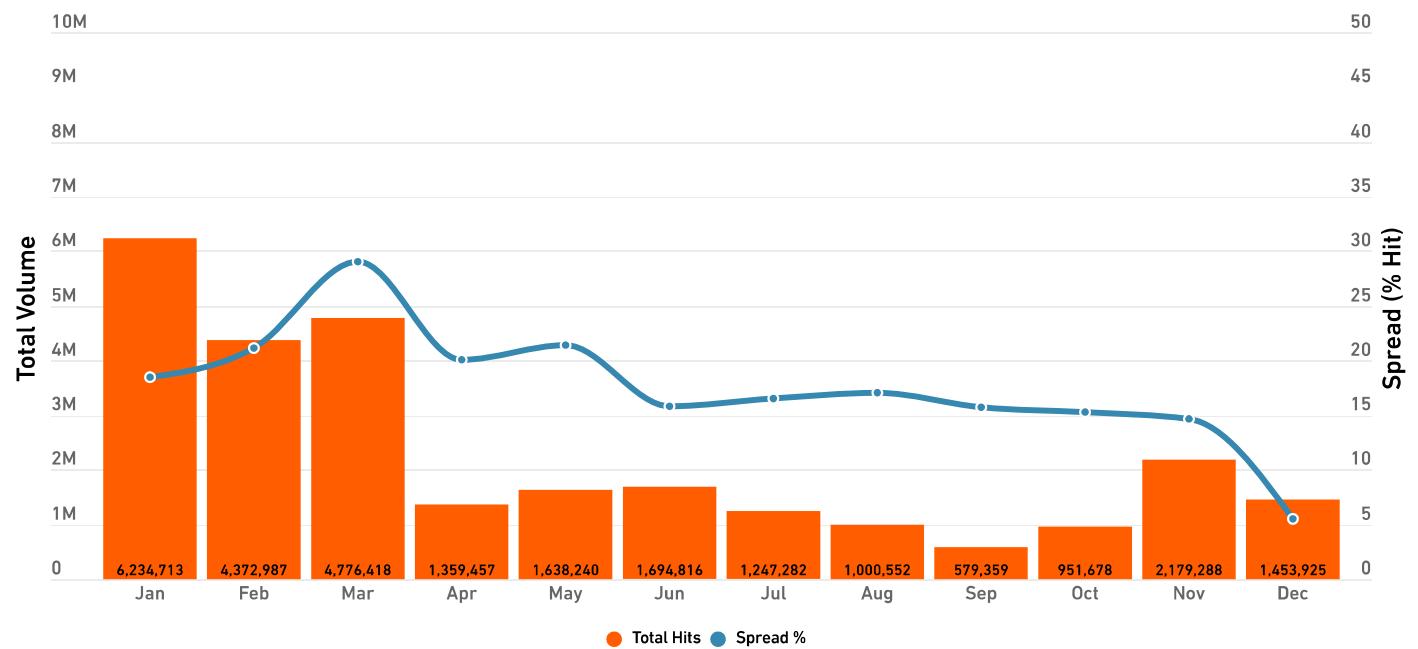
2022 Malware Attacks | United Arab Emirates



MALWARE RANK 2022 ATTACK VOLUME YoY CHANGE
12 71.1 MILLION -14%

While malware in UAE dropped in 2022, this comes on the heels of a 33% increase in 2021 — meaning the region is still seeing dramatically higher malware.

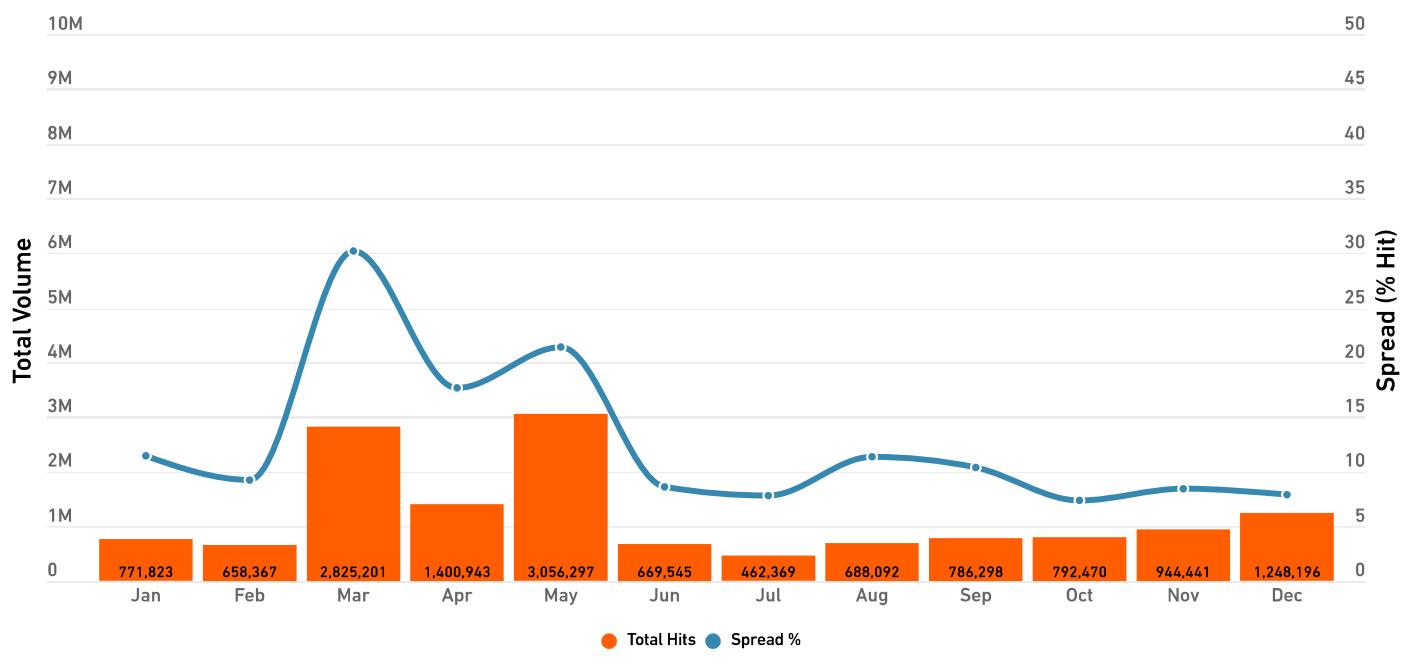
2022 Malware Attacks | Mexico



MALWARE RANK 2022 ATTACK VOLUME YoY CHANGE
21 27.5 MILLION -14%

Malware in Mexico has recently reversed course: After increasing 73% in 2020, it increased just 3% in 2021, then dropped in 2022.

2022 Malware Attacks | Japan

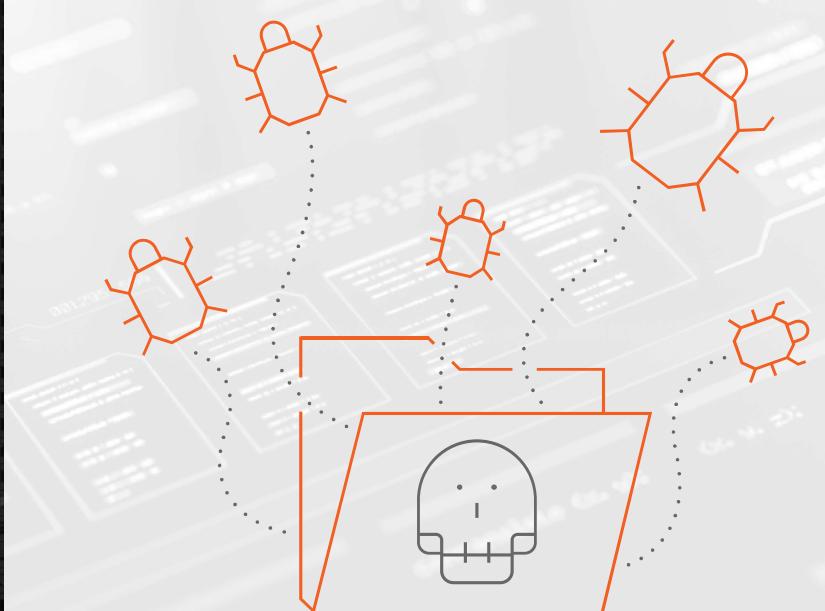


MALWARE RANK 2022 ATTACK VOLUME YoY CHANGE
32 **14.3 MILLION** **+2%**

In March, malware spread in Japan spiked to just over 30% — though the yearly average was just under 13%.

Top 10 Malware File Names

1. purchase order.exe
2. soa.exe
3. invoice.exe
4. swift copy.exe
5. quotation.exe
6. img-order-confirmation-pdf.exe
7. payment copy.exe
8. ziraat bankasi swift mesaji.exe
9. shipping documents.exe
10. new order.exe



Malware Spread by Country

Despite seeing a decrease in malware volume in 2022, the U.S. and U.K. are still the countries with the highest malware volume. But based on our malware spread data, an organization is most likely to see a malware attempt in Vietnam: 30.2% of customers there were targeted in 2022.

But while the same three countries — Vietnam, Sri Lanka and Slovenia — topped the malware spread list in 2022 as they did in 2021, there's a lot of variation further down the rankings. Most notably, the rise of Europe as a new cybercrime hotspot is showing up in SonicWall's malware spread data as well. Between 2021 and 2022, the number of European countries on the list doubled, and European countries now make up a majority of the top 10.

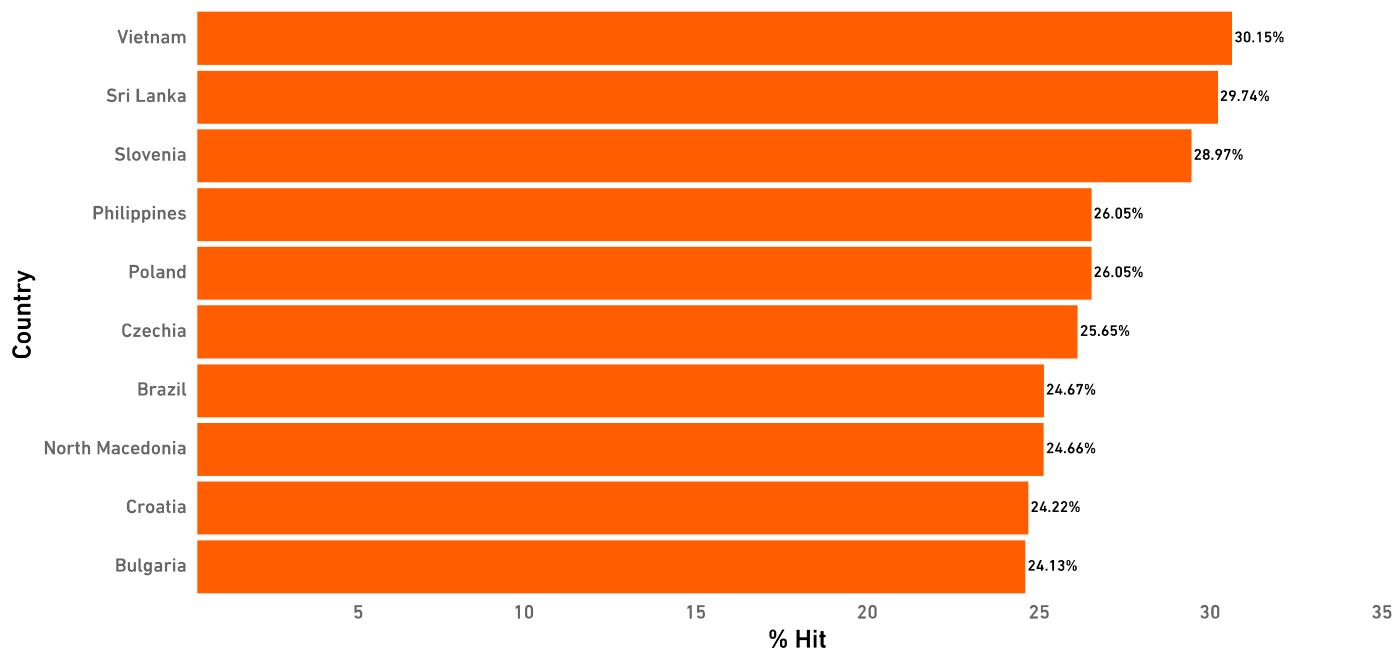
We're also continuing to see malware spread drop overall: Last year, the highest-ranked country had a malware spread of 36.5%. This year, it's fallen to 30.2%.

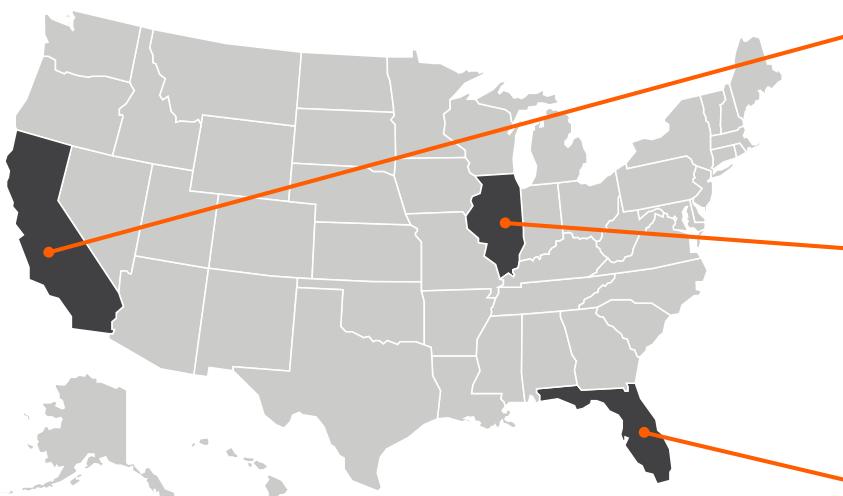
One thing remained unchanged from 2021, however: The country where you're least likely to be targeted by malware is still Luxembourg, where just 6.3% of SonicWall sensors recorded malware hits (down from 6.6% in 2021.)



BETWEEN 2021 AND 2022,
THE NUMBER OF EUROPEAN
COUNTRIES ON THE LIST
DOUBLED, AND EUROPEAN
COUNTRIES NOW MAKE UP A
MAJORITY OF THE TOP 10.

2022 Malware Spread | Top 10 Countries





321M
Malware attacks in California

315M
Malware attacks in Illinois

191M
Malware attacks in Florida

Malware by State

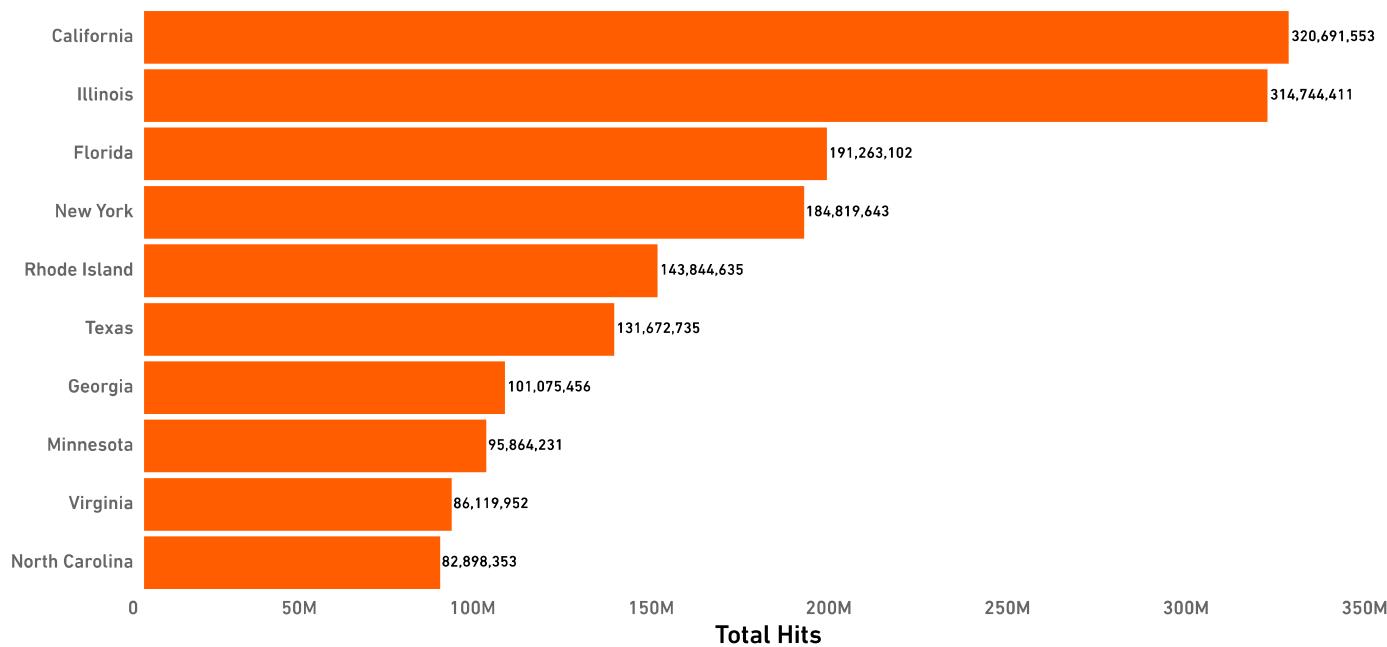
In 2021, Florida recorded 625.4 malware hits — compared with second-ranked New York, which had less than half that total. Louisiana, which rounded out the top 10, had roughly a tenth of that at 69.9 million.

In 2022, we've seen this range narrow considerably. This year, California had the worst malware attack volume, but with 320.7 million hits, it's less than half what Florida saw in 2021 — and Illinois was right behind it.

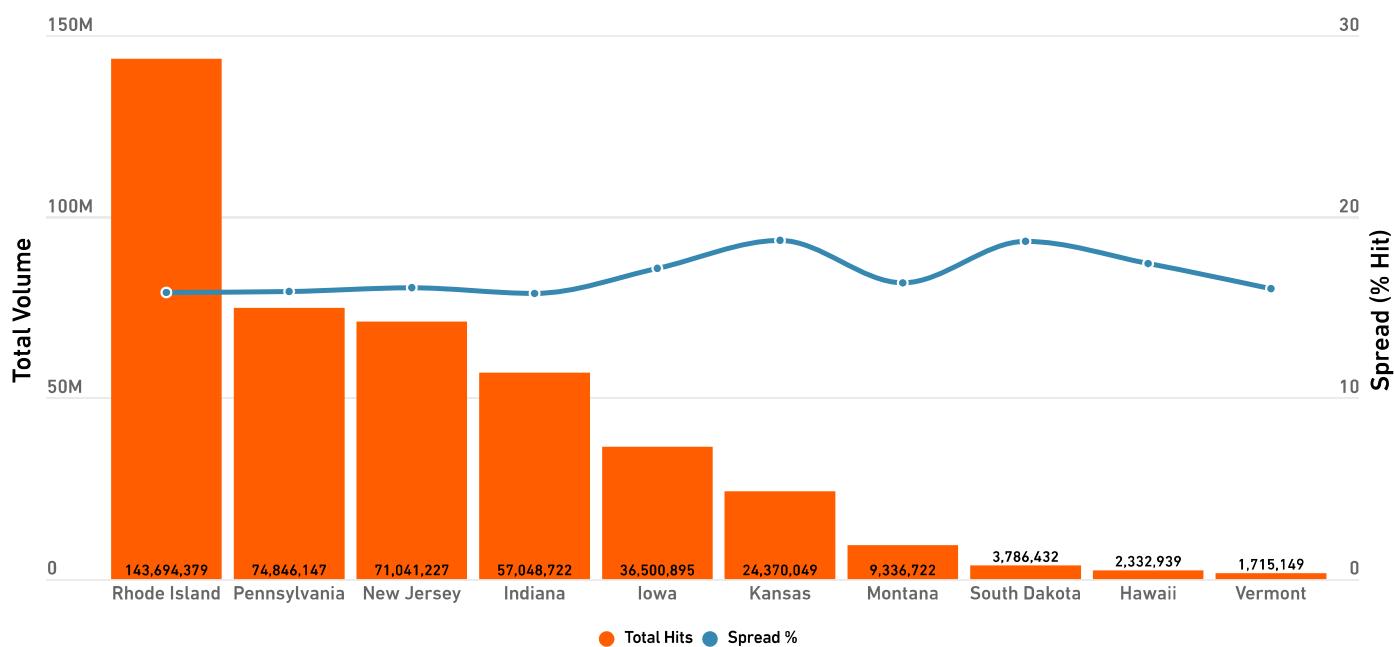
The attack volume for No. 10, however, grew: North Carolina had 82.9 million malware attacks.

This trend echoes what we're seeing at the regional and country level. States that typically experience more malware are seeing less, and states that may have once considered themselves "safe" are seeing an uptick.

2022 Malware Volume | Top 10 U.S. States



2022 Malware Spread | Top 10 Riskiest U.S. States



But once again, these states weren't actually the riskiest for malware. In fact, four of the top 10 states for malware volume appeared in the bottom 10 for malware spread, including California. (Only one state on the top-10 list for worst malware volume appears in the top-10 list for worst malware spread: Rhode Island.)

So which state is the riskiest? For the third year in a row, it's Kansas, where approximately 18.7% of SonicWall sensors logged a malware hit. Fortunately for those in the Sunflower State, however, this continues to fall: from 26.7% in 2020, to 21.4% in 2021, to 18.7% in 2022.

Conversely, Texas was the lowest: only 12.7% of sensors there logged a malware attempt.

2022 Brings Surge in Wiper Malware

SonicWall in 2022 observed an uptick in so-called wiper malware. In contrast with ransomware, intended to render files unusable until a ransom is paid, wiper malware is designed to "wipe" or render data unusable permanently.

In February, SonicWall Capture Labs threat research team analyzed a sample believed to be targeting Ukrainian organizations. Known as HermeticWiper, the malware prevents Windows from recording any information in the memory dump file and disables the VSS (Volume Shadow Copy Service, which is used to back up application data). Finally, it corrupts the first 512 bytes, the Master Boot Record (MBR) for every physical drive. It then initiates a reboot and, once completed, the missing OS prompt is displayed, leaving the system unusable.

Another wiper targeting Ukrainian networks, CaddyWiper, was analyzed by SonicWall in March. This malware iterates through files, including critical system files, and replaces their contents with null bytes. Once the data is overwritten, the physical drive is also overwritten with null bytes, rendering the machine unbootable.

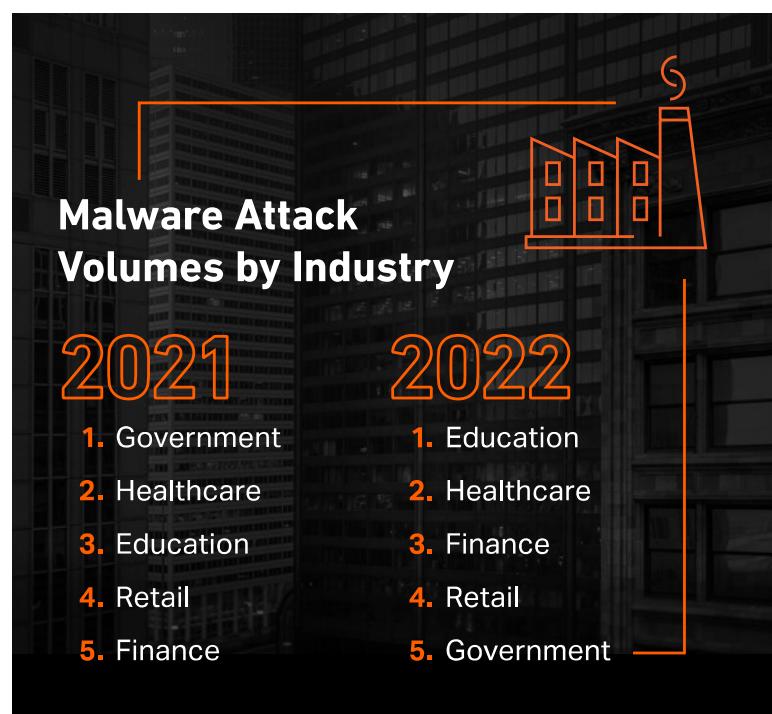
In October, SonicWall analyzed yet another wiper, this one a multicomponent infection purporting to be a picture. It arrives as a file titled "SexyPhotos.jpg," but is actually a self-extracting archive. While a ransom note is displayed, the malware only gives the appearance of encrypting files — instead, it's intended to delete all data on a given drive.

Malware by Industry

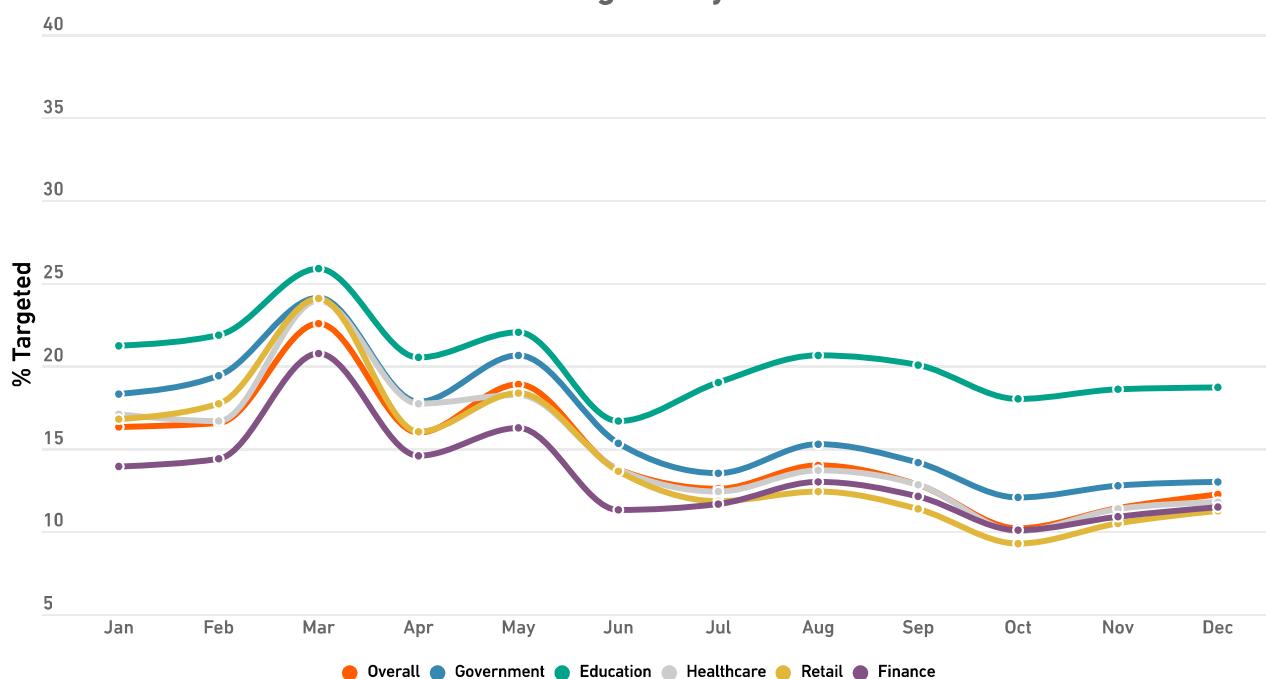
Malware targeting those in the healthcare industry fell 15% year over year, while government customers saw an even larger drop of 58%. Retail and finance, on the other hand, experienced double-digit increases, with overall malware attack volume rising 50% and 86%, respectively.

The largest increase, however, was in education, where malware volume jumped 157%. But this is actually the average of two outcomes: Attacks targeting higher education customers rose a (relatively) modest 26%, while attacks targeting K-12 institutions skyrocketed 323%.

When it comes to the average percentage of customers targeted by malware in 2022, every industry we studied showed a decrease from 2021's average. The percentage of healthcare customers targeted in 2022 slightly edged out the percentage of retail customers targeted, but the rankings remained otherwise unchanged.



% of Customers Targeted by Malware in 2022



RANSOMWARE



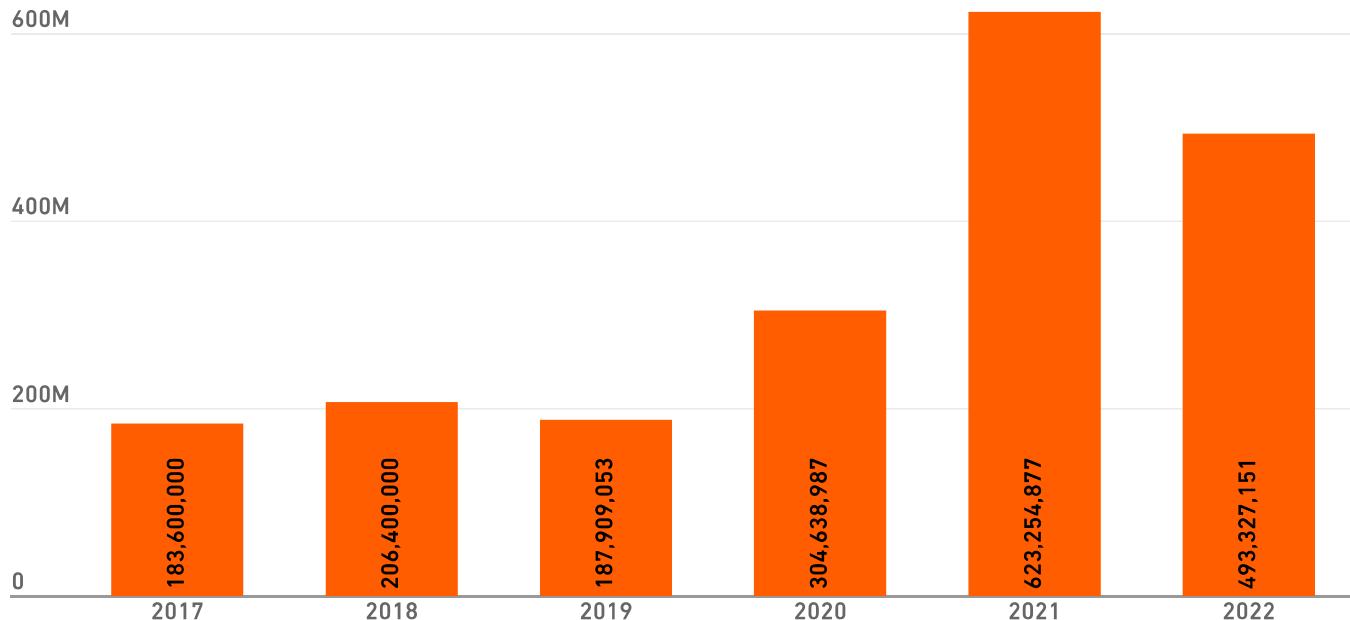
Ransomware Reverses Course

2022 brought a bit of a reprieve from 2021's sky-high ransomware volumes. In 2022, SonicWall Capture Labs threat researchers recorded 493.3 million ransomware attempts, down 21% year-over-year.

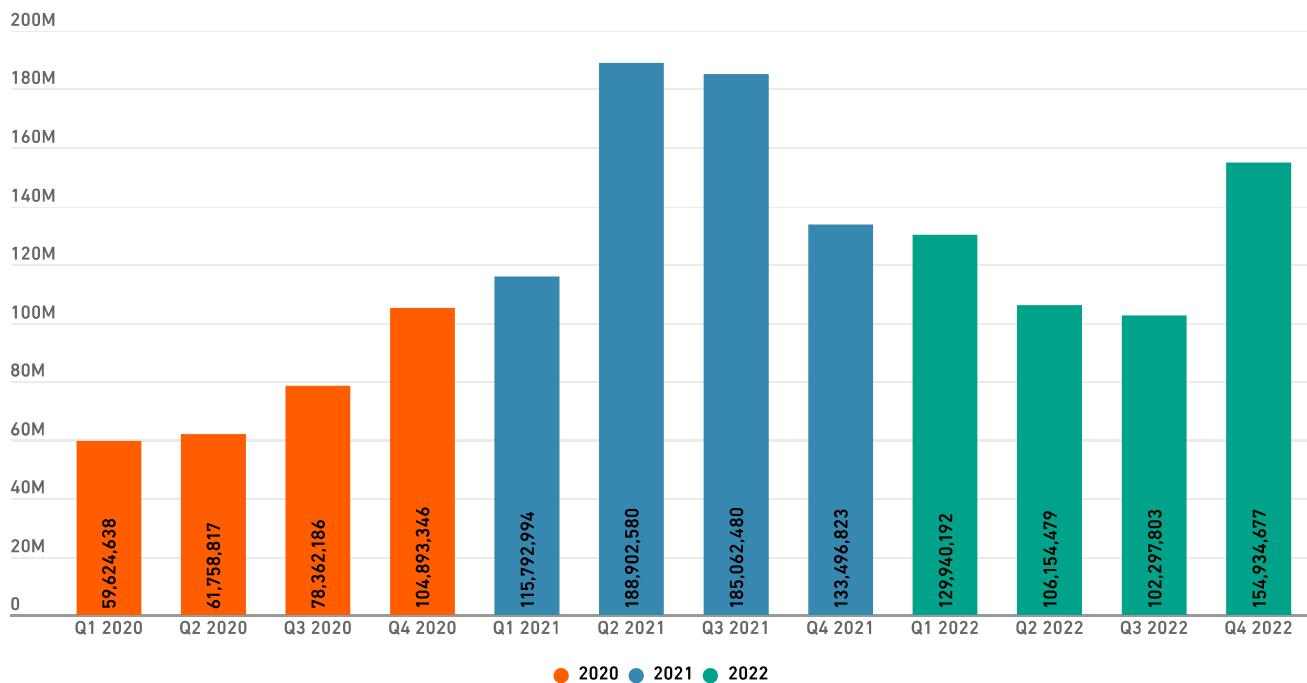
Unfortunately, however, we're already seeing signs of a potential reversal. After ransomware bottomed out in June, bringing the lowest attack volume we'd seen since July 2020, the trend line began reversing. When attacks doubled between September and October, it pushed Q4 ransomware totals to 154.9 million — the highest quarter we've seen since Q3 2021.

This is especially concerning because ransomware in 2022 wasn't that low to begin with. Despite dropping by a little more than a fifth, 2022 was still the second-highest year on record for ransomware attacks globally. And it's far closer to the stratospheric volumes we saw in 2021 than it is to prior years, outpacing 2017 (+155%), 2018 (+127%), 2019 (+150%), and 2020 (+54%) by significant margins.

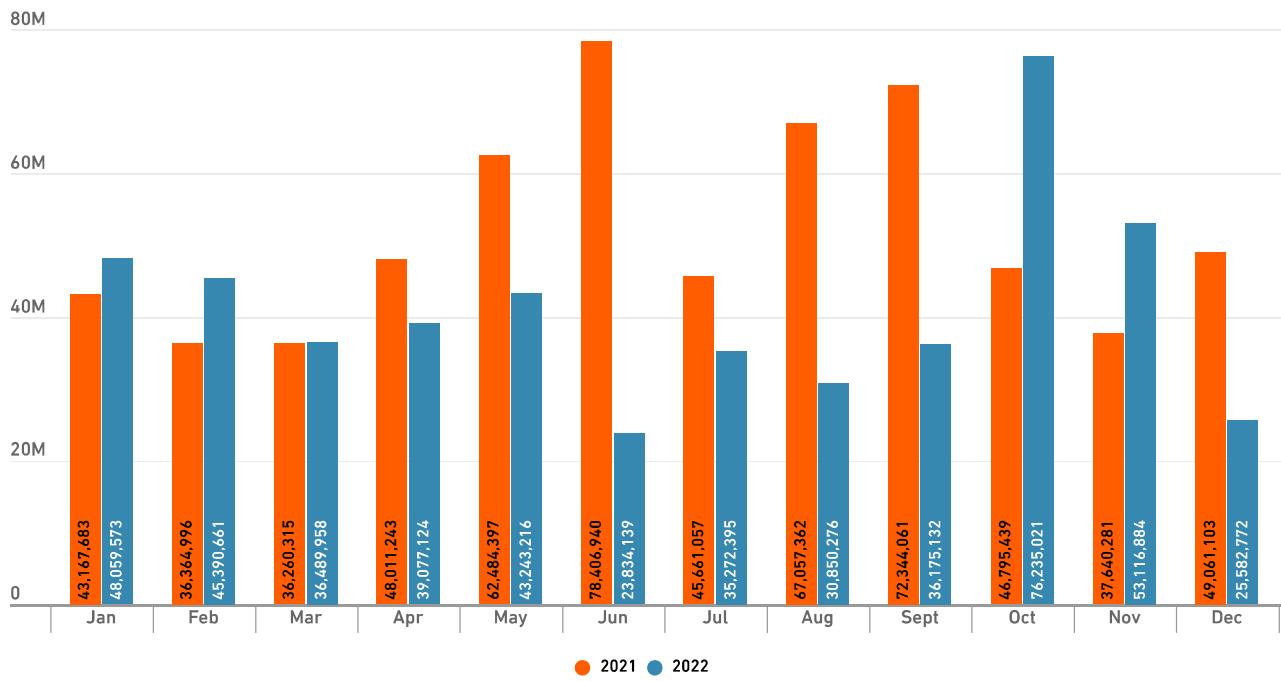
Global Ransomware Volume by Year



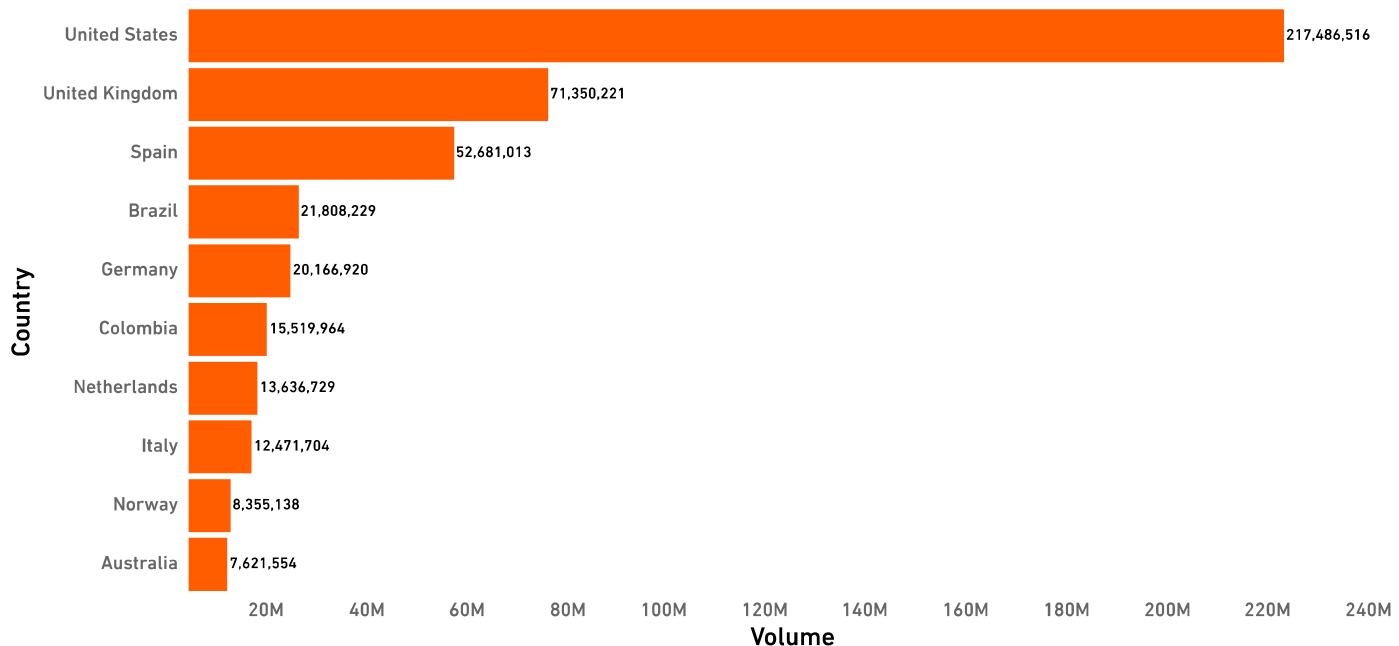
Global Ransomware by Quarter



Global Ransomware Volume



2022 Ransomware Volume | Top 10 Countries



Ransomware by Country

Despite a 48% year-over-year drop, the United States once again saw the highest ransomware attack volume of any country in 2022 — but with a 112% jump, the U.K. is beginning to catch up. In contrast, ransomware attacks in Germany fell 42%, moving it from the second-highest attack volume to fifth.

One newcomer to this list was Spain: Last year, the country wasn't even in the top 10 for ransomware volume, but 2022 brought a massive spike that propelled the country all the way up to No. 3 on the list. And while India's ransomware volumes still fall short of making the top 10, it also saw a large jump in 2022, with ransomware volumes up 51% year over year.



Ransomware by Industry

As with the regional and country data, the industry-specific data also showed a huge variety in outcomes. Customers in government and the retail industry saw double-digit decreases in ransomware, with attack volumes falling 82% and 50%, respectively.

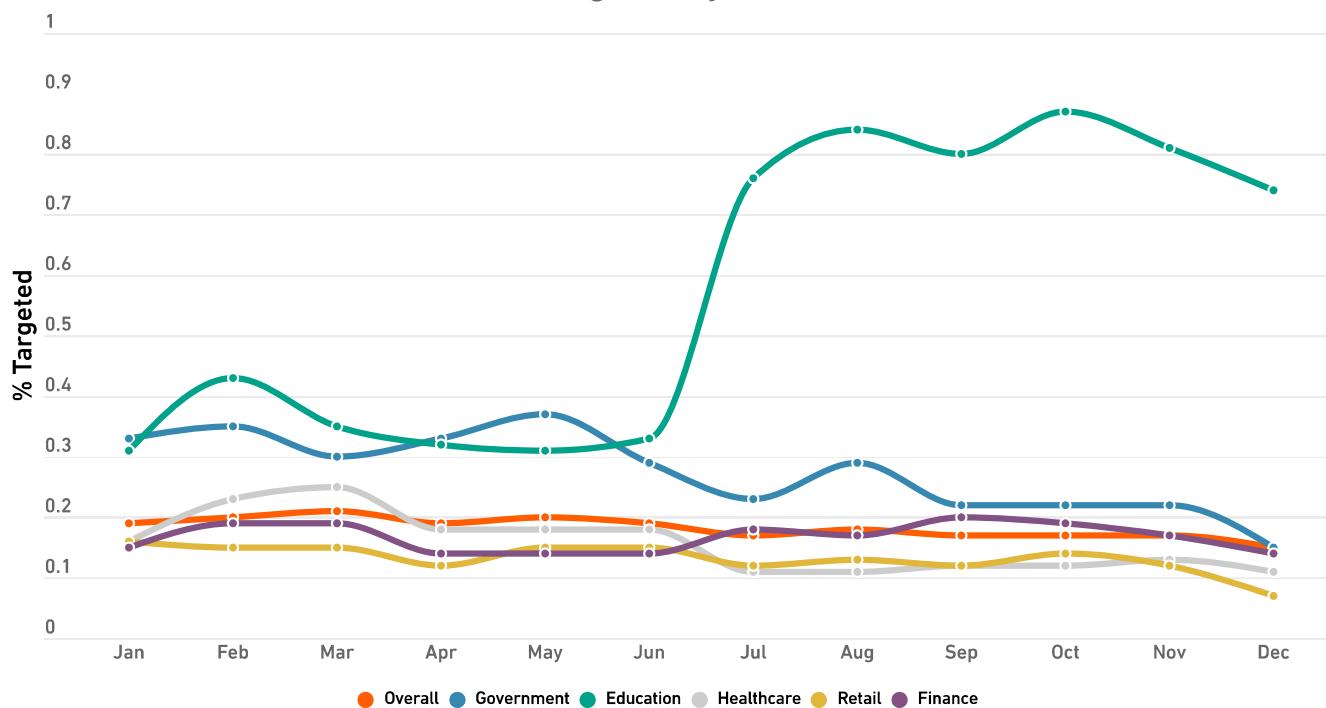
But the other industries studied saw the opposite. With an 8% year-over-year increase, healthcare saw the smallest jump, but customers in finance (+41%) and education (+275%) weren't so lucky.

A 275% jump is bad enough on its own — but as we saw in the malware data (see [page 32](#)), this number is actually the confluence of disparate trends. Higher education customers experienced a 29% decrease in ransomware, putting it roughly in the middle on the list of industries we studied when taken on its own.

But this double-digit drop serves as a counterbalance to an absolutely massive increase in attacks on K-12 institutions and primary schools. *Attacks on these schools rose 827%*, disproportionately impacting the world's children and educators.

The per-customer data showed education customers once again inordinately affected by ransomware. In addition to being the only industry studied to have a higher average percentage of customers targeted this year than last year, ransomware attacks spiked in the second half — pushing education to a distant first in terms of how many education customers saw a ransomware attempt.

% of Customers Targeted by Ransomware in 2022



CRYPTOJACKING

Cryptojacking Continues Record-Breaking Run

As cybercriminals complemented ransomware with more low-profile revenue streams in 2022, cryptojacking rates began to accelerate significantly. By year's end, SonicWall Capture Labs threat researchers recorded 139.3 million cryptojacking attempts, a 43% year-over-year increase.

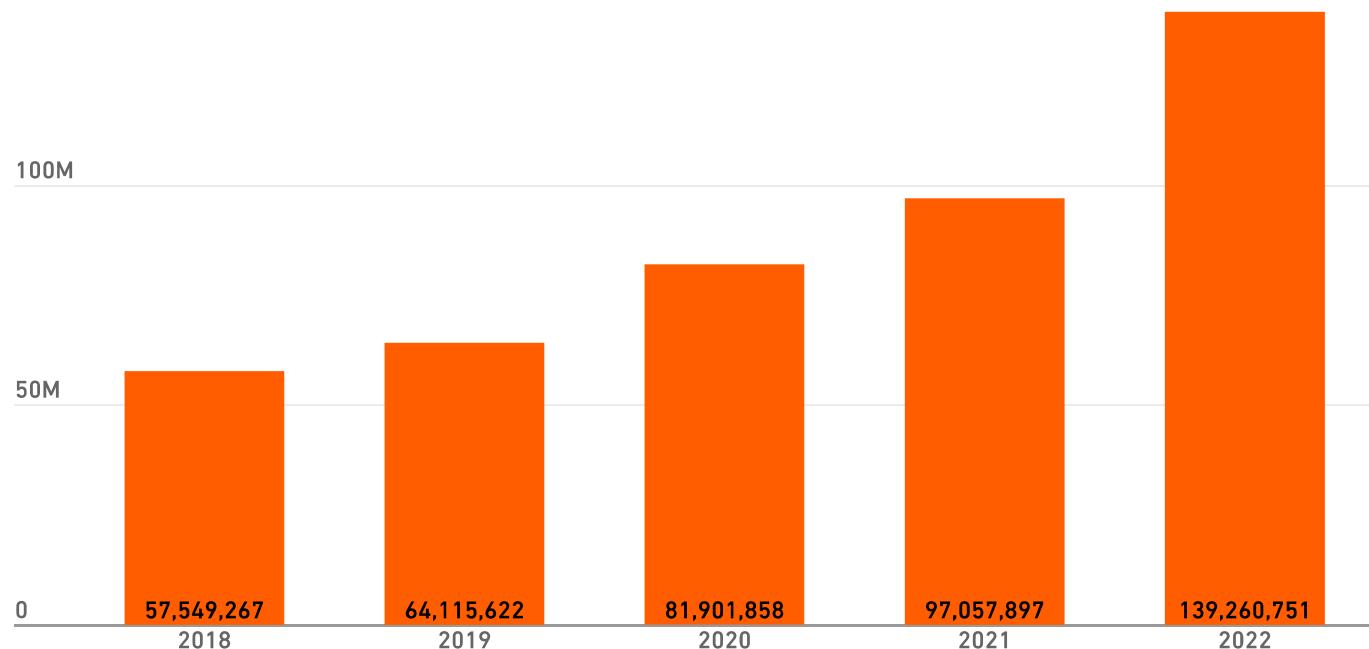
Not only did 2022 mark the first time that yearly attack volume surpassed 100 million, it was also more cryptojacking than SonicWall had ever observed in a single year.

Monthly record totals were set as well: In January, cryptojacking attempts rose to 18.4 million, surpassing the previous monthly record (set in March 2020) by nearly 3 million.

After attack volume dropped dramatically in November, December came with a vengeance, bringing with it 30.4 million cryptojacking attempts. This unprecedented total not only exceeded the previous monthly record by roughly 12 million, it also surpassed the total for all but three quarters on record.

Even so, highly suppressed volume in November, combined with sustained high rates of cryptojacking at the beginning of 2022, meant that Q1, not Q4, ended the year with the highest volume on record.

Global Cryptojacking Volume by Year



Cryptojacking by Region

While LATAM recorded a 66% drop in cryptojacking volume year over year, it was the only region to see a drop.

In North America, which typically sees by far the most attacks, volume rose from 78.0 million in 2021 to 105.9 million in 2022 — a 36% increase, and more than the *entire world* saw the year before.

Asia saw an even larger year-over-year increase of 129%, jumping from 3 million to 6.9 million. But it was Europe where cryptojacking grew the fastest: Volume there soared from 3.4 million in 2021 to 22.0 million in 2022, an increase of 548%.

Despite skyrocketing attack volumes in Europe, the United States remained the country with the highest volume. Cryptojacking attempts there rose 41% year over year.

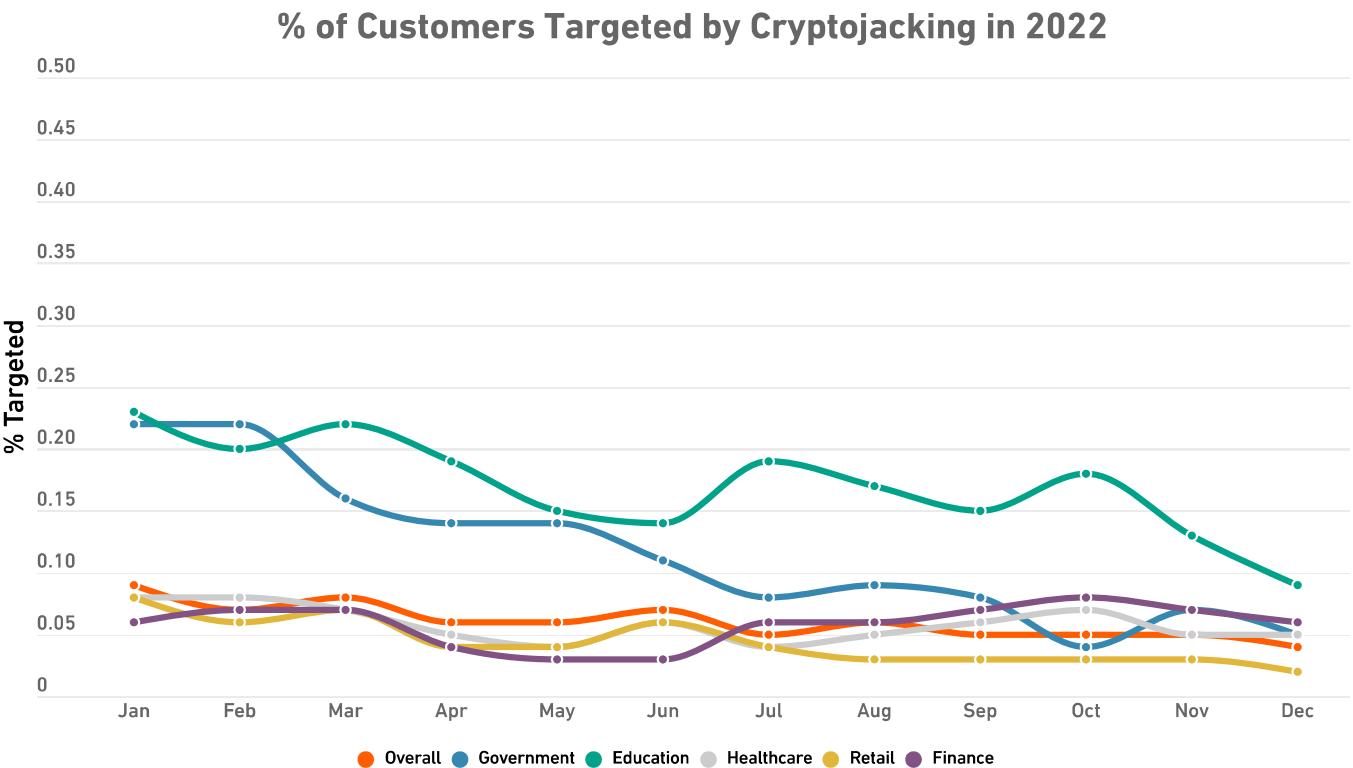
XMRig Now Used in Nearly 90% of Cryptojacking Attempts

Due to its high availability and ease of use, XMRig was once again the cryptominer of choice. In 2022, 89.4% of all cryptojacking attempts recorded by SonicWall were based on XMRig, up from 67.4% in 2021.

XMRig is an open-source, cross-platform miner that, while not malicious on its own, is frequently abused by cybercriminals to illegally mine the privacy coin Monero on victims' computers.

The miner can be dropped on a victim's machine through a variety of means, such as the modular [Glupteba malware](#) and, increasingly, [malware targeting Linux](#).





Cryptojacking by Industry

Among the most volatile of our data sets, 2022's data on cryptojacking by industry highlights the rapid evolution of cybercriminal behavior. The least movement was seen in education, where total attack volume increased 20% over 2021's totals. Government and healthcare also saw double-digit movement, with attack volumes falling 83% and 76% respectively.

Attacks on finance customers increased 352% in 2022, enough to move it from No. 4 to No. 3 for attack volume. But even this triple-digit spike wasn't the worst observed: **those in retail saw year-over-year attack volume jump a staggering 2,810%**. But despite retail having the highest total attack volume, these customers were the least likely to see an attack: it was education customers that had the highest percentage of customers targeted.

Cryptojacking Attack Volumes by Industry

2021

1. Healthcare
2. Education
3. Government
4. Finance
5. Retail

2022

1. Retail
2. Education
3. Finance
4. Healthcare
5. Government



ENCRYPTED ATTACKS

Encrypted Attacks Fall 28%

In 2022, SonicWall Capture Labs threat researchers recorded 7.3 million encrypted attacks, down from 10.1 million in 2021. But in 2022, the total was closer to last year's record high than to the volumes seen in 2019 (3.7 million) and 2020 (3.8 million).

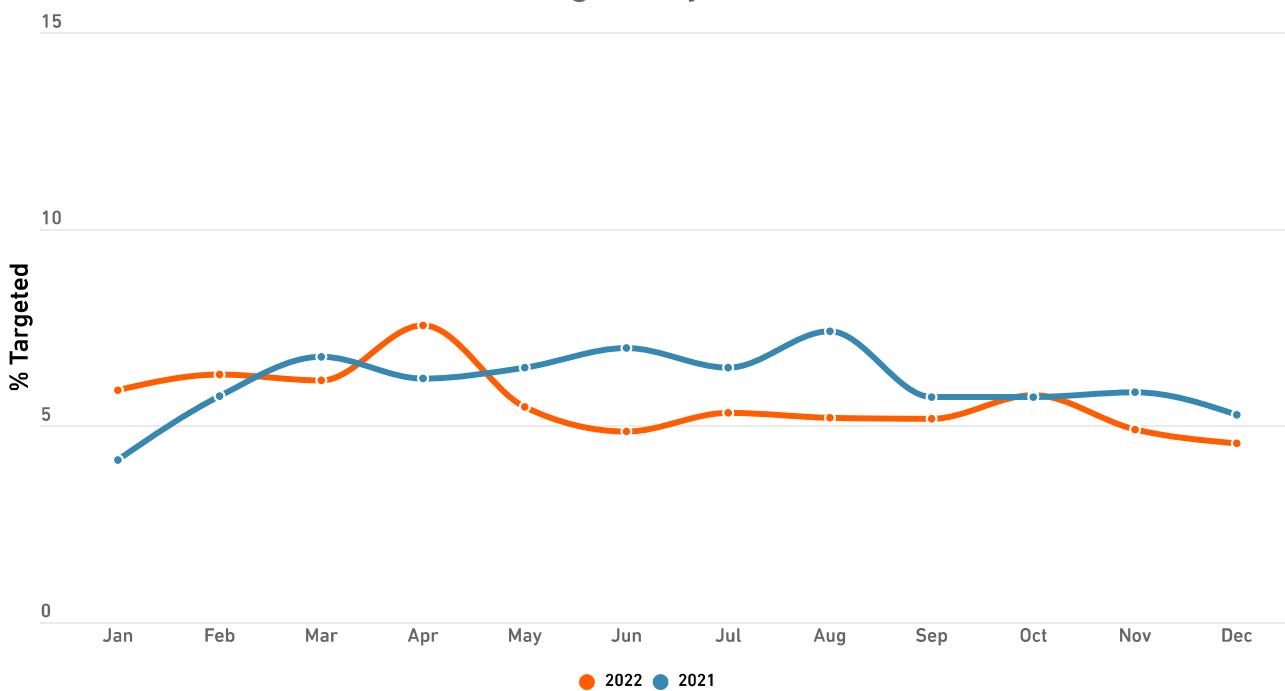
But while a 28% decrease is somewhat modest compared with some of the movement we've seen elsewhere, it hides a great deal of regional variation.

In Asia, attack volumes fell dramatically in 2022, dropping 85% year over year. For most of the year, LATAM appeared to be going the same direction. By November, attack volumes for 2022 were less than half that seen in 2021.

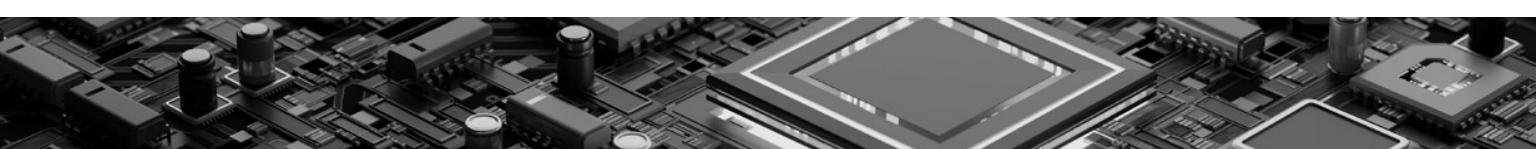
But then December came, bringing with it more than twice the number of attacks that LATAM recorded in the other 11 months combined. This late-year blitz was enough to singlehandedly push encrypted attacks in the region from a 62% year-over-year decrease to a 29% increase.

While it lacked the volatility seen in other regions, double-digit movement was also seen in North America and Europe, which experienced a drop of 39% and an increase of 22%, respectively.

% of Customers Targeted by Malware Over HTTPs



* Organization must have a SonicWall firewall with DPI-SSL activated.



Encrypted Attacks by Industry

For the industries studied, the news ranged from good, to bad, to worse. Retail and finance received a welcome reprieve from encrypted attacks, with attack volumes for these industries falling 79% and 45%, respectively.

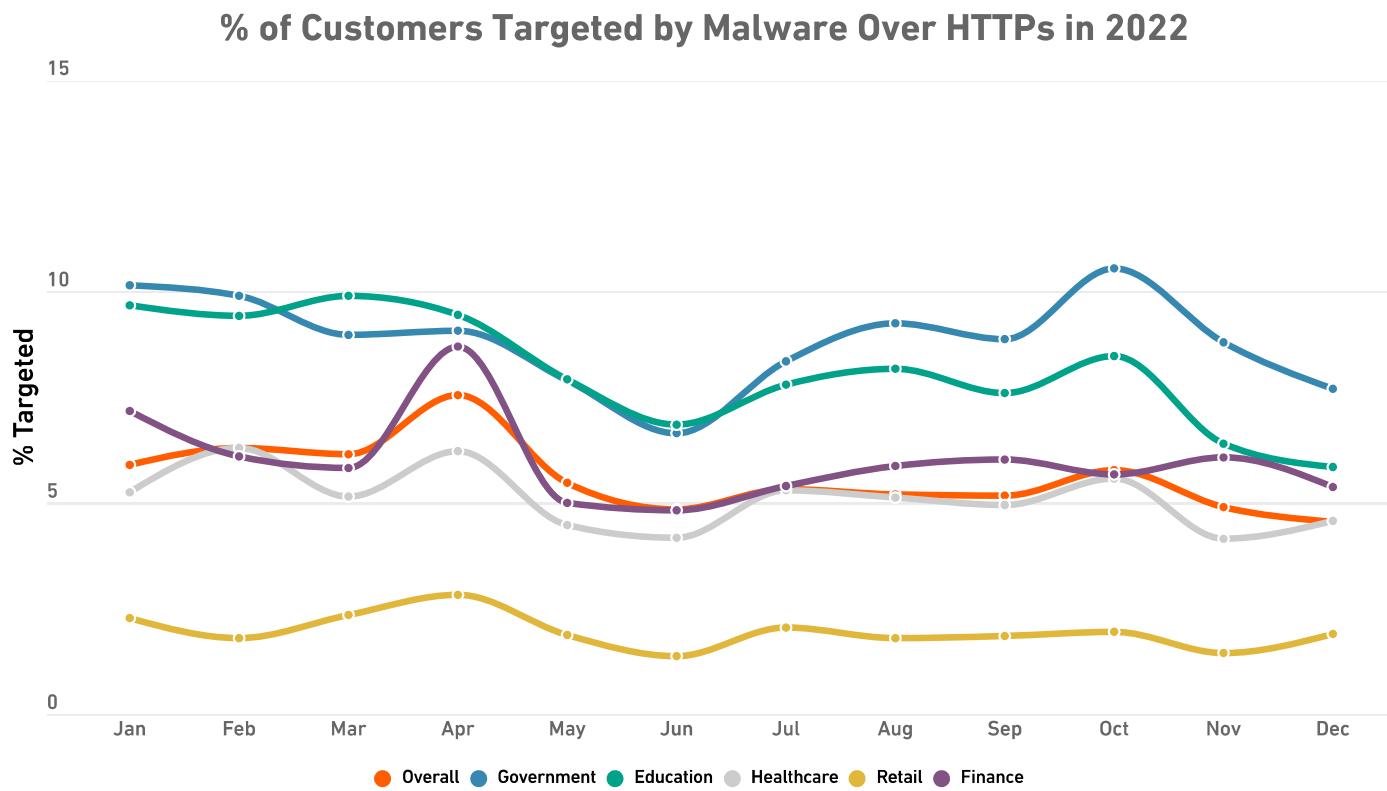
In contrast, healthcare saw a 35% jump in malware attacks over HTTPs—but this was small compared with what was experienced by customers in education and healthcare. Both of these industries experienced triple-digit attack volume increases, with attacks on education rising 411% and attacks on government spiking 887%.

The huge increase in attacks on government organizations can also be observed in the per-customer data. Government was the only industry studied to see a year-over-year increase in the average percentage of customers targeted. This increase pushed it above education, the industry that saw the most attacks per customer in 2021.

What Are Encrypted Threats?

Put simply, TLS (Transport Layer Security) is used to create an encrypted tunnel for securing data over an internet connection. While TLS provides security benefits for web sessions and internet communication, this encryption protocol is also increasingly used by cybercriminals who want to hide malware, ransomware, zero-day attacks and more.

Legacy firewalls and other traditional security controls lack the capability or processing power required to detect, inspect and mitigate cyberattacks sent via HTTPs traffic, making this a highly successful avenue for skilled threat actors to deploy and execute malware.



INTRUSION ATTEMPTS

Overall Intrusion Attempts Up

Intrusion attempts continued to climb in 2022, hitting a new high of 6.3 trillion. This represents a 19% increase over 2021's total, and is roughly six times the number of overall attempts observed in 2013, the first year SonicWall recorded this data.

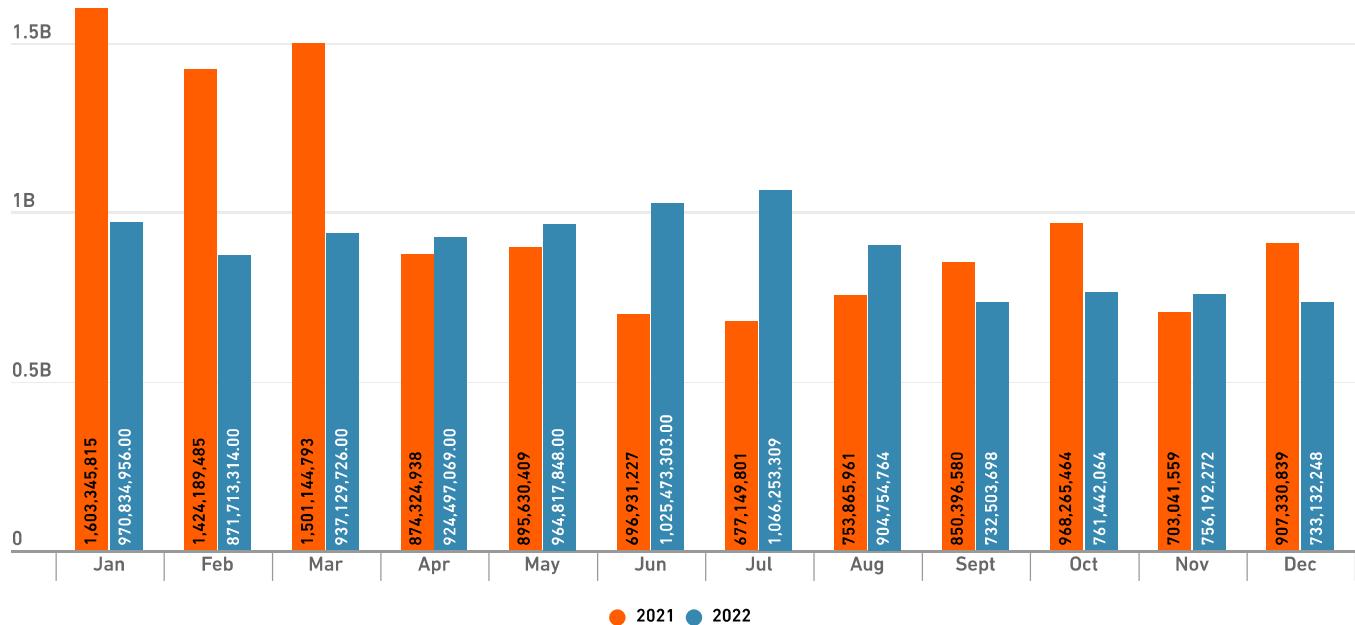
But while there may be more overall intrusions, a majority of this increase is due to low-severity hits associated with pings and other actions that are typically benign. The number of moderate- or high-severity intrusion attempts, also known as malicious intrusion attempts, observed in 2022 actually fell, dipping to 10.6 billion — a 10% year-over-year drop.

Even larger decreases were recorded in Europe and Asia, where malicious intrusions fell 28% and 17%, respectively. In North America, malicious intrusion attempts remained essentially unchanged from 2021 levels. Only LATAM saw a statistically significant increase: Malicious intrusion attempts there rose 8%.

But while there was no reshuffling of the regions with regards to who was hardest hit, the gap between North America and Europe, which had the second-highest attack volume, is continuing to grow — making it likely that malicious intrusion attempts will continue to disproportionately affect this region for the foreseeable future.



Global Intrusion Attempts



Note: Only includes malicious medium- and high-risk intrusion attempts.

What is an Intrusion Attempt?

A malicious intrusion attempt is a security event in which a cybercriminal, hacker, threat actor or intruder tries to gain access to a system or resource by exploiting a vulnerability without authorization. Such vulnerabilities are generally public and published as CVEs (see [page 10](#)). While these vulnerabilities are public, not everyone patches at the same rate, giving attackers an opportunity to take advantage of unpatched software or appliances that can be used as an entry point into a network.

Malicious intrusions also include the exploitation of vulnerabilities that are not yet well publicized or haven't been published—the dreaded zero-day vulnerabilities.

Vulnerability exploitation doesn't stop once attackers get inside the network. In fact, it usually accelerates. Attackers attempt to gain network persistence and lateral movement by exploiting other, internal vulnerabilities in unpatched systems and software inside the network.

What SonicWall records is detection and prevention of vulnerabilities coming from both external and internal sources. When a piece of code that constitutes a vulnerability passes a firewall with Intrusion Prevention enabled, and the firewall detects and neutralizes that code, an intrusion attempt is counted.

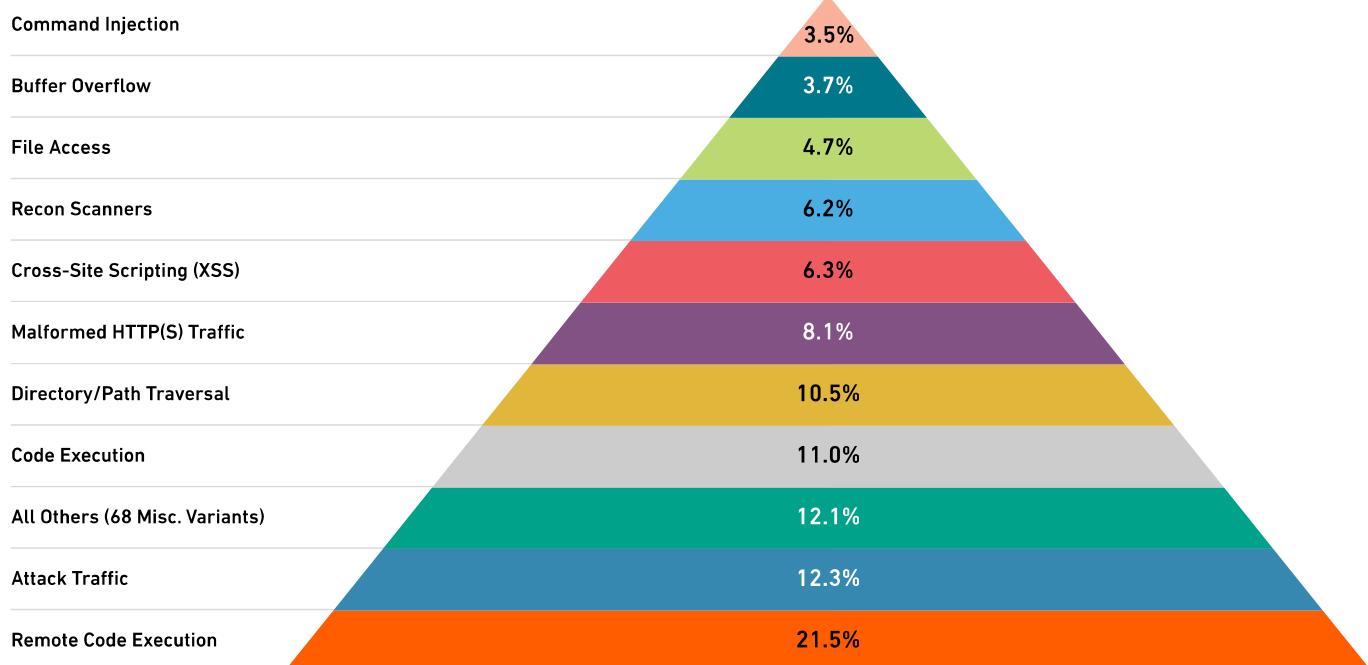
As noted, malicious intrusions consist of moderate- and high-severity intrusion attempts—low-severity intrusion attempts are typically harmless.

The Rise of RCEs

While very little in the cybersecurity world has returned to its 2019 state, malicious intrusion types are one exception: Just like we saw four years ago, Remote Code Executions (RCEs) are once again the most common form of malicious intrusion we observed.

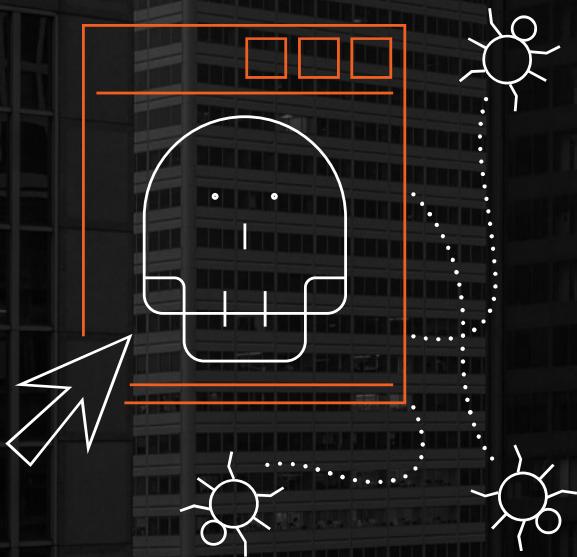
While this type of intrusion attempt made up less than 10% of total malicious intrusions in 2021, their numbers grew tremendously in 2022, and they now make up 21.5% of malicious intrusion attempts globally.

2022 Malicious Intrusion Attempts



What is an RCE?

An RCE attack takes place when a threat actor uses a vulnerability to remotely run malicious programming code, usually in an unexpected path and with system-level privileges. (The infamous Bluekeep vulnerability is one example of this.) These vulnerabilities are among the most dangerous on software systems and are frequently used to spread ransomware.



Here are some of the RCEs SonicWall Capture Labs threat researchers reported in 2022:

EmbedThis Goahead Web Server CGI RCE	2/4/22
Samba vfs_fruit Module RCE Vulnerability	3/4/22
Java Spring Framework Spring4Shell RCE Vulnerability	4/1/22
VMware Workspace One Access & Identity Manager RCE Vulnerability	4/22/22
WSO2 API Manager RCE Vulnerability	4/29/22
Parse Server Databasecontroller RCE Vulnerability	5/6/22
Follina MS-MSDT RCE Vulnerability	6/1/22
Atlassian Confluence OGNL Vulnerability	6/10/22
Oracle MySQL NDB Cluster RCE	7/22/22
Ivanti Avalanche RCE Vulnerability	8/5/22
Zimbra Collaboration RCE Vulnerability	9/2/22
Microsoft Exchange Server Zero-Day Vulnerabilities	9/30/22
Zimbra Collaboration Suite TAR RCE	10/20/22
Follina Vulnerability Is Being Used to Deliver Redline Info Stealer	11/2/22

Malicious Intrusions by Industry

The industry-specific intrusion data for 2022 showed less volatility than some other threat types, but that doesn't mean there weren't still some significant upticks.

Government organizations saw the worst of it: malicious intrusion attempts on these customers spiked 74% year over year. With a 55% increase, the finance industry didn't fare much better. Healthcare and retail saw significantly more modest increases of 5% and 3%, respectively.

Only education saw a decrease — total malicious intrusions targeting these organizations dropped 17% from 2021's levels.

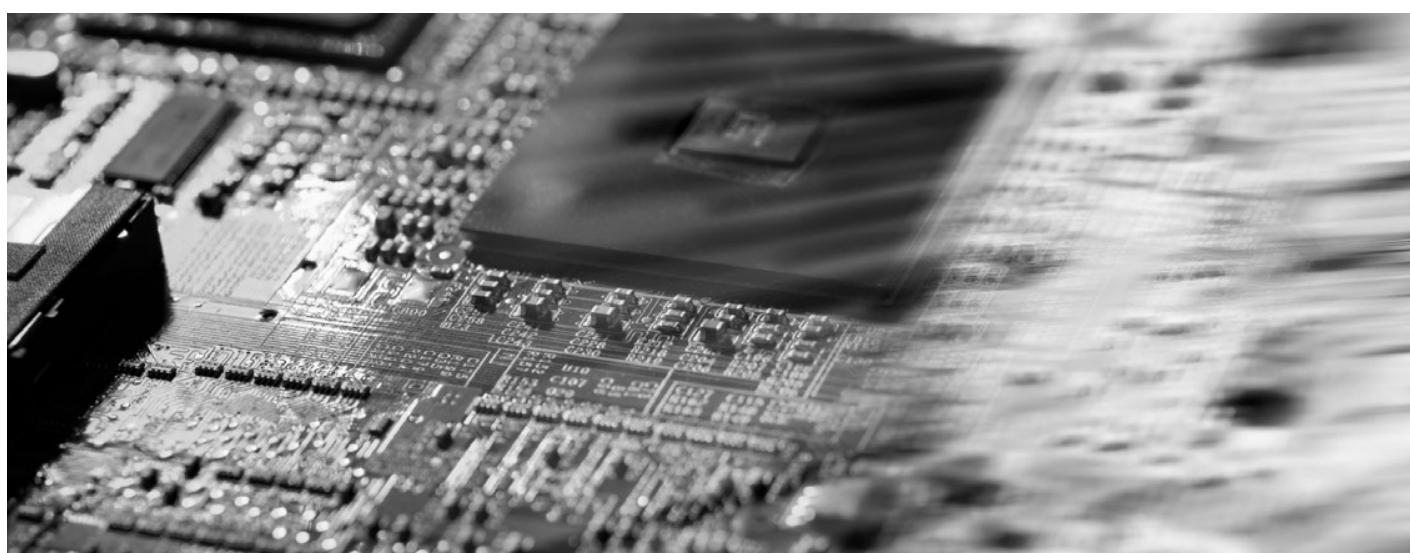
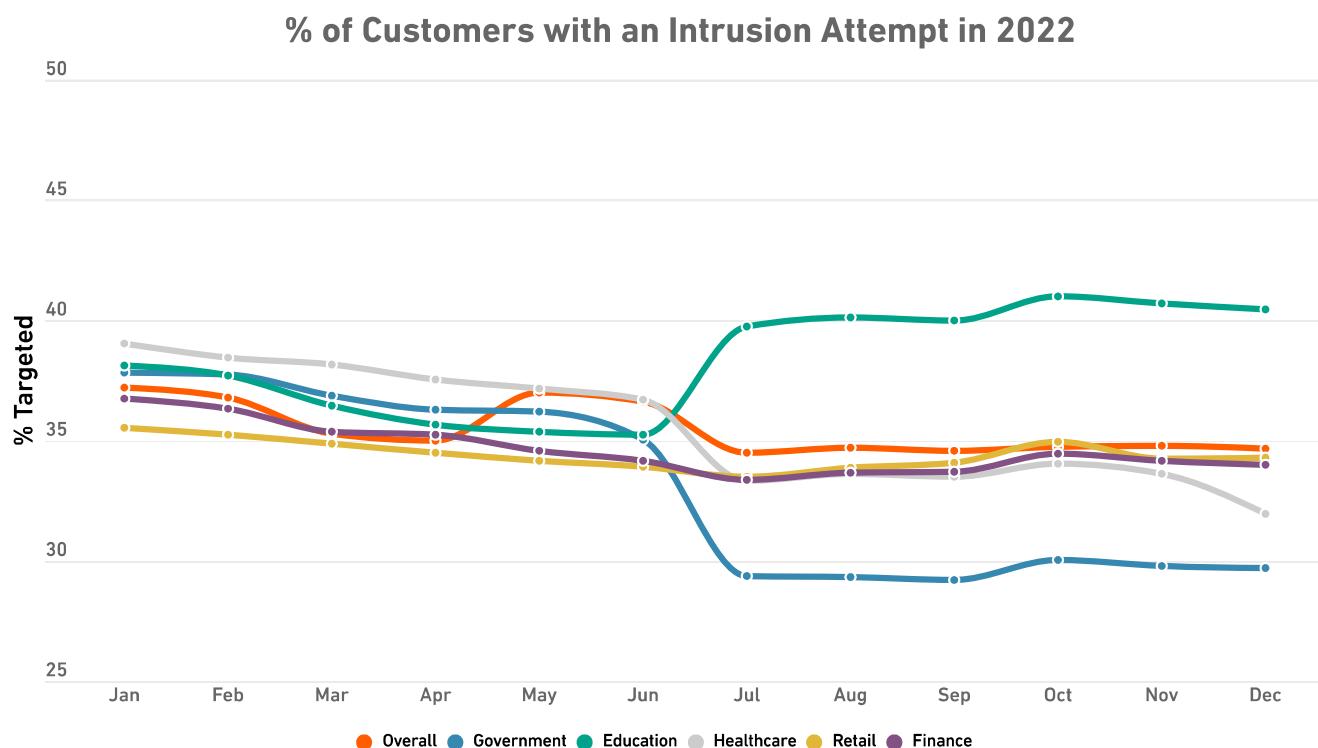
But a look at the per-customer data shows that while most of the industries studied saw an increase, that doesn't necessarily mean more of these customers are seeing an attack. In fact, we observed the opposite.

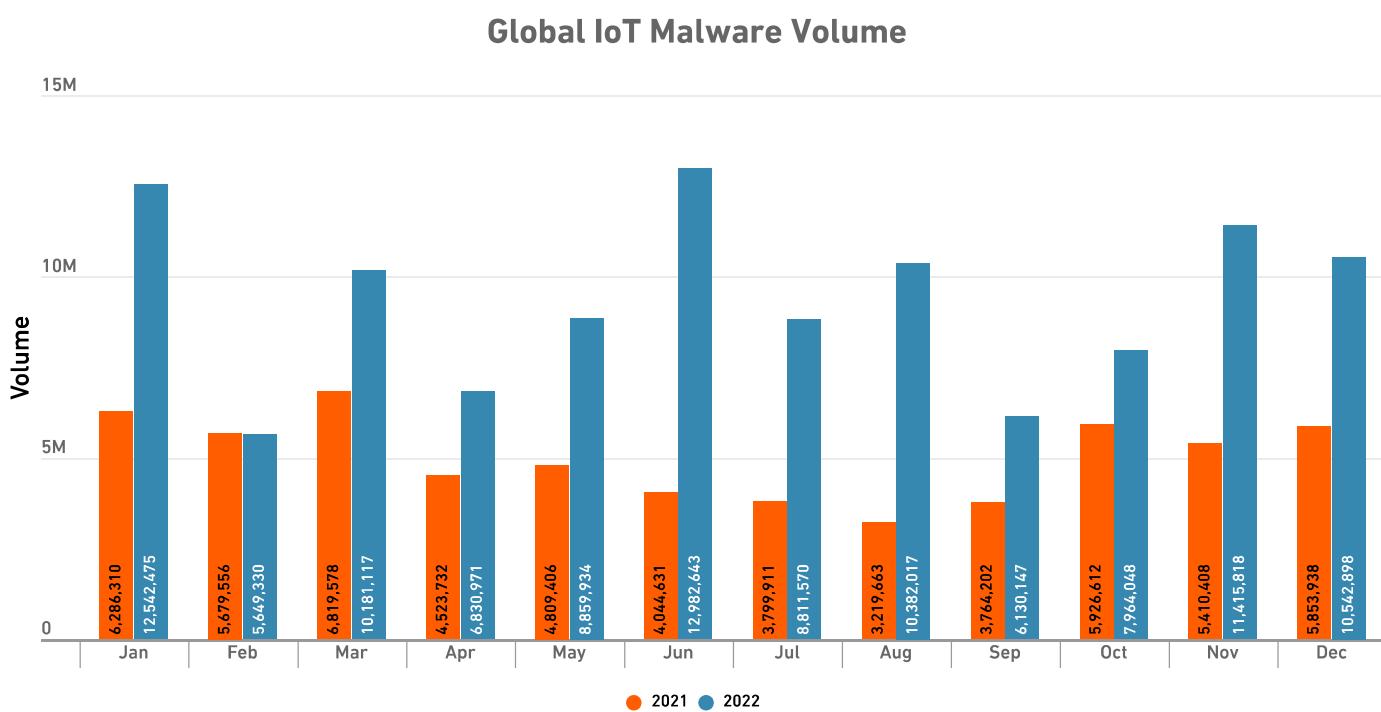
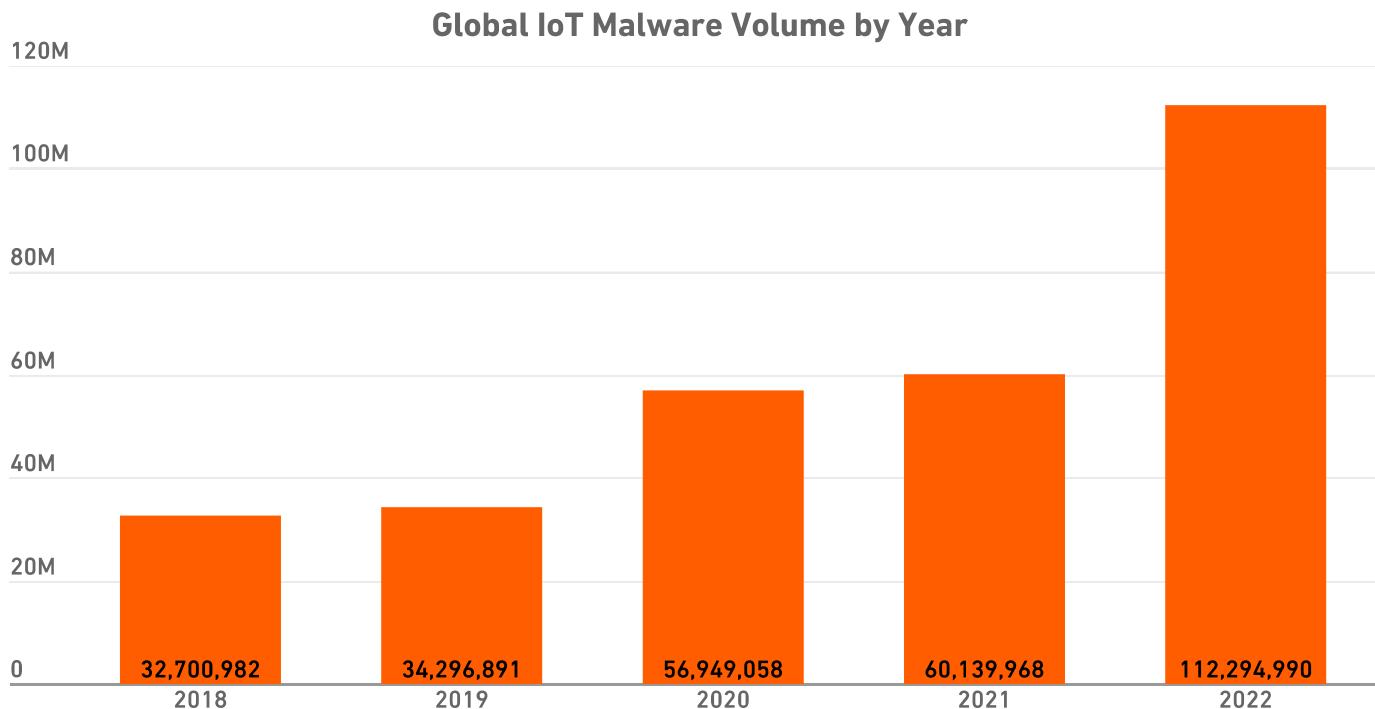
The biggest decrease in percentage of customers targeted by malicious intrusion attempts was for government: In 2021, 40.7% of these customers saw an attack, but in 2022, only 33.1% did.

Combined with the 74% increase in attacks on government overall, this suggests that malicious intrusion attempts on government are becoming much more targeted.

The opposite held true for education customers. While education saw a sizeable drop in overall attacks, per-customer data showed the least-favorable trend, with the percentage of customers targeted falling only 3.2% year-over-year. These averages (and their accompanying rankings) are largely courtesy of an odd divergence that began in Q3.

After remaining in the middle of the pack for the first half of the year, in July the percentage of education customers targeted rose several percentage points — and the percentage of attacks on government customers fell by nearly the same amount. Both trends persisted through the end of the year, suggesting a sustained change in cybercriminal behavior.





IoT Malware by Region

Given the global IoT malware increase, it's unsurprising that there were significant, across-the board increases at the regional level. IoT malware volume in Europe increased 21%, followed by the LATAM (65%) and Asia (73%) regions.

And while overall malware, ransomware and other threat types saw attacks fall in the hardest-hit regions, IoT malware did not follow this pattern. North America, which experienced the biggest increase at 145% year-over-year, already led the pack in IoT malware attacks — and it has for three years running.

As cybercriminals doubled down on attacking targets in North America last year, the gulf between it and the second-highest region widened from just a few million to roughly 40 million: By the end of 2022, North America had recorded 62.9 million attacks, versus 23.2 million in Europe.

On a country-by-country level, the two countries that typically see the highest IoT malware attack volume also saw triple-digit increases. The U.K., which has the second-highest attack volume, saw IoT malware increase 163%. And in the U.S., which typically sees the most attacks, attack volume rose 169%.

IoT Malware by Industry

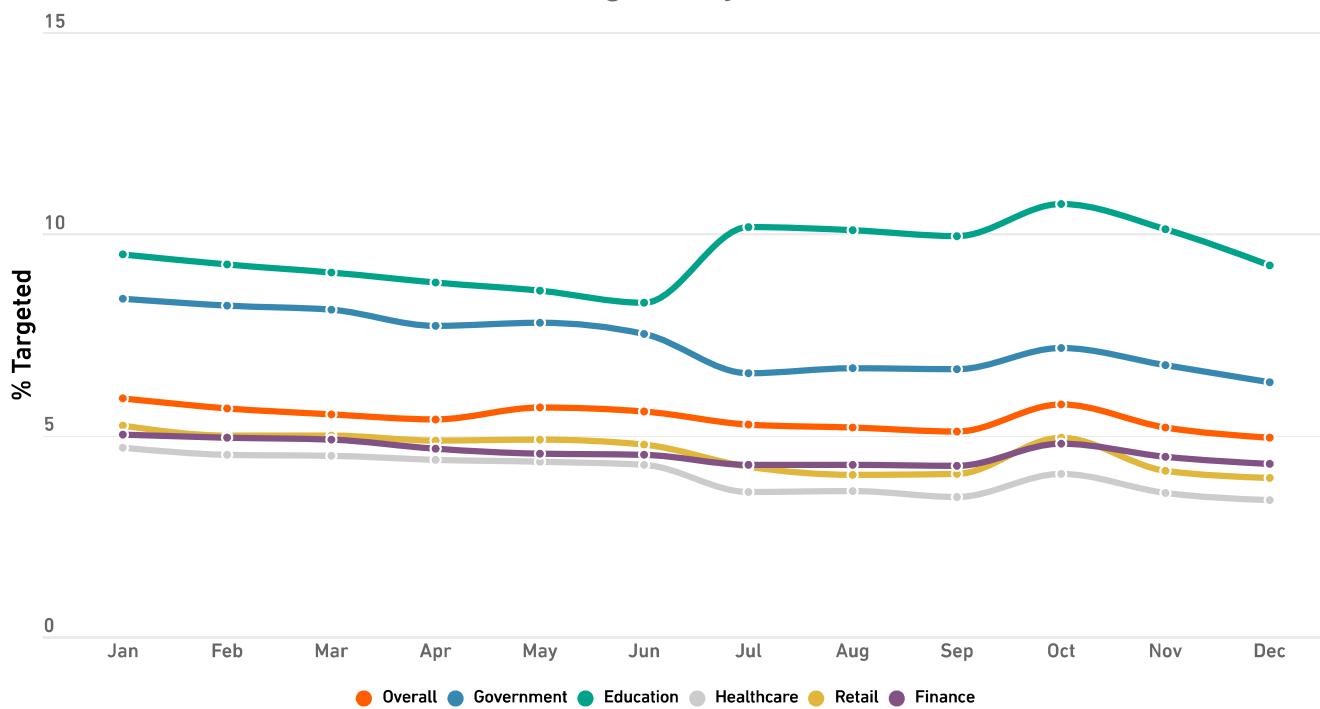
For the second year in a row, SonicWall Capture Labs threat researchers observed increases in IoT malware volume across every industry studied — and this year, the increases were even bigger.

Healthcare customers saw the least change, with a 33% year-over-year increase in attacks. Government, which saw a jump of 40%, wasn't far behind.

The news gets considerably worse from here, however: Retail experienced a 159% increase in attack volume, and education wasn't much better off at 146%. But it was finance that saw the brunt of the increase: attacks on finance customers skyrocketed 252% year over year.

On a per-customer basis, the rankings remained mostly the same in 2022 as they were in 2021, with the only exceptions being retail and finance. Always close in terms of the percentage of customers targeted, this year retail surpassed finance, but only by the tiniest margin.

% of Customers Targeted by IoT Malware in 2022



The State of Ransomware in Retail 2021

Based on an independent survey of 435 IT decision makers, this report shares new insights into the current state of ransomware in the retail sector. It provides a deep dive into the prevalence of ransomware in retail, the impact of those attacks, the cost of ransomware remediation, and the proportion of data that retail organizations could recover after an attack. The survey also reveals how retail stacks up with other sectors, as well as the future expectations and readiness of retail organizations in the face of these attacks.

Key findings in Retail

- › 44% of retail organizations **were hit by ransomware in the last year**
- › 54% of organizations hit by ransomware said the **cybercriminals succeeded in encrypting their data** in the most significant attack
- › 32% of those whose data was encrypted **paid the ransom to get their data back** in the most significant ransomware attack
- › The **average ransom payment** was **US\$147,811**
- › However, **those who paid the ransom got back just 67% of their data** on average, leaving almost a third of the data inaccessible
- › The **average bill for rectifying a ransomware attack in the retail sector**, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more, was **US\$1.97 million**
- › 56% of those whose data was encrypted **used backups to restore data**
- › 91% of retail organizations have a **malware incident recovery plan**

Retail, together with education, was the sector most hit by ransomware in 2020. Cybercriminals were quick to exploit opportunities presented by the pandemic, which in the retail sector was primarily the rapid growth in online shopping. Some retail organizations started trading online for the first time, while others saw a huge increase in their web traffic and the percentage of transactions that happened online.

Enabling and managing this change introduced new challenges for IT teams while also consuming significant capacity: nearly three quarters (72%) of respondents said their cybersecurity workload increased over 2020. The good news is that, in light of this increase in workload, 77% of IT teams in retail said their ability to develop cybersecurity knowledge and skills increased over the course of 2020, *the highest among all industries*.

The growth in online retail also exacerbated existing security challenges facing the retail sector, including the extensive use of legacy systems that are harder to maintain and update, and frequent mergers and acquisitions that require IT teams to integrate disparate systems. Add to this the need to protect a wide range of valuable information, including customers' personal and financial data, and the challenge of securing complex, distributed environments, and it is easy to see why retail is an attractive target for cybercriminals.

In the face of these challenges, almost a third (32%) of retail organizations whose data was encrypted paid the ransom to get their data back, which is in line with the cross-sector average. However, those who did pay only got back, on average, 67% of their data, leaving almost a third inaccessible, and just 9% got all their encrypted data back. While this is slightly higher than the global average (65%/8%), it's clear that paying the ransom doesn't really pay off.

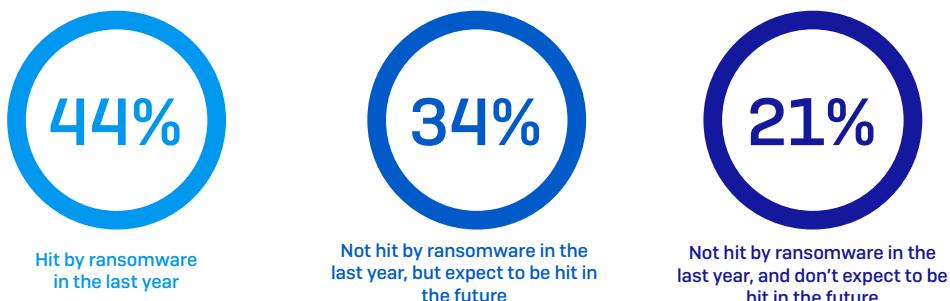
While the average ransom paid by retail organizations (US\$147,811) is considerably below the cross-sector average (US\$170,404), the overall average ransomware recovery cost comes in higher than the global average (US\$1.97 million vs. US\$1.85 million). This is likely due to high costs of notifying individuals whose data has been breached, as well as the considerable impact of reputational damage in this sector – it's generally much easier to switch to a different retailer than to a different school or hospital.

Retail organizations should prioritize strengthening their defenses against ransomware. Investing in modern infrastructure, together with cybersecurity technology and skills, will considerably reduce both the overall cost and impact of ransomware.

The prevalence of ransomware in retail

Retail's experience with ransomware last year

Of the 435 retail sector respondents that were surveyed, 44% were hit by ransomware in the last year, defined as *multiple computers being impacted by a ransomware attack, but not necessarily encrypted*.



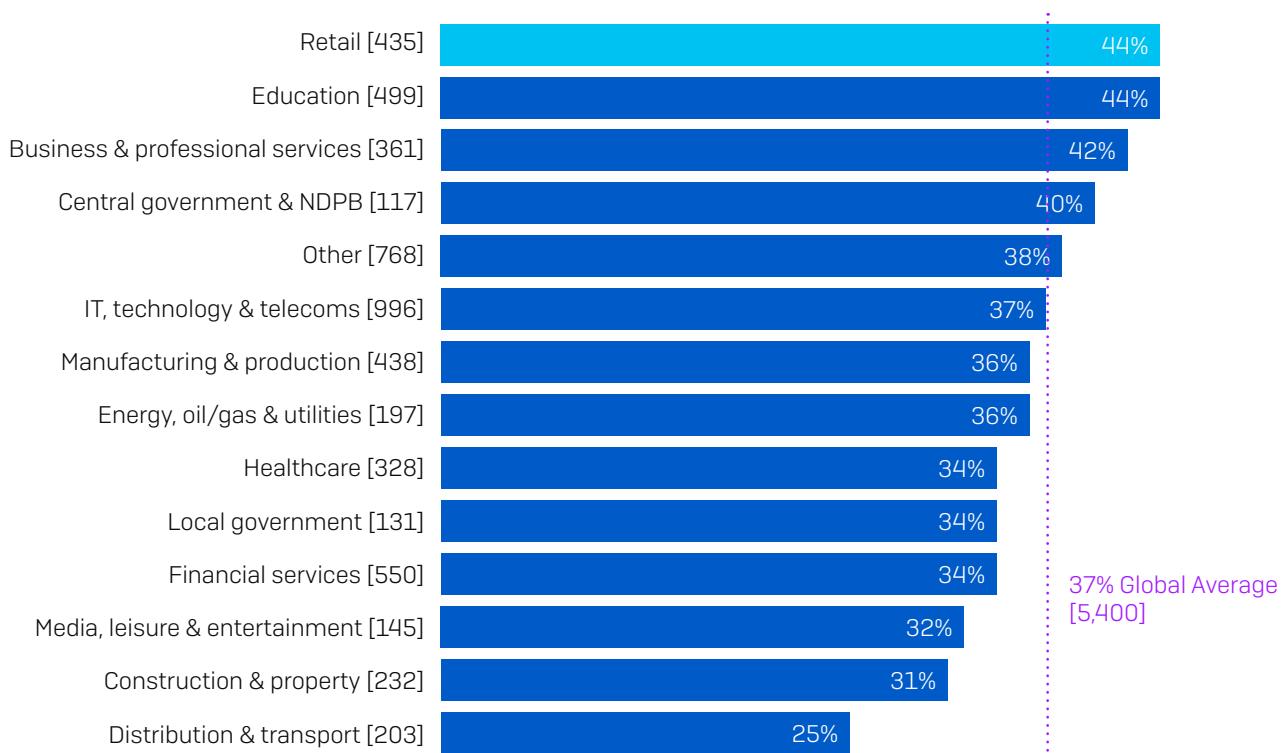
In the last year, has your organization been hit by ransomware? [435 retail respondents]

Among the organizations not hit last year, 34% said they expected to be hit by ransomware in the future, while 21% were confident that they are safe from future attacks. We'll dive deeper into the reasons behind the expectation to be hit in the future, as well as what gives others confidence in the face of future attacks, later in the report.

Retail saw the highest level of ransomware attack

Looking at the prevalence of ransomware across all the sectors surveyed, retail, along with education, experienced the highest level of ransomware attacks: 44% of respondents in these sectors reported being hit compared to the global average of 37%.

% respondents hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? Yes [base numbers in chart] omitting some answer options, split by sector

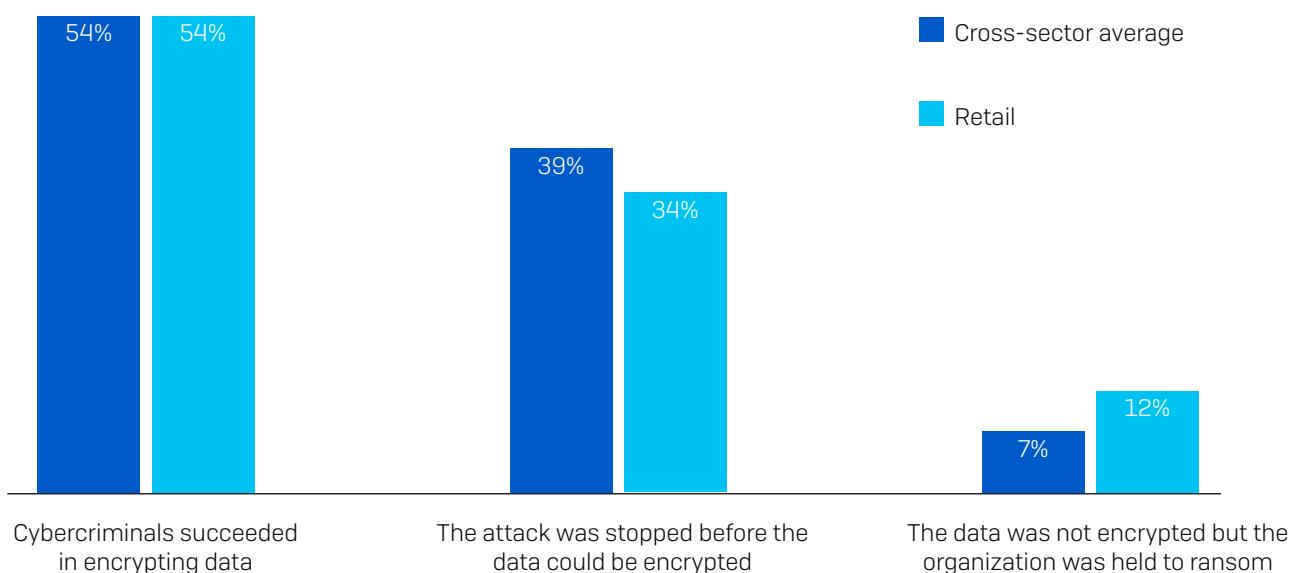
The State of Ransomware in Retail 2021

Globally across all sectors, the percentage of organizations hit by ransomware in the last year has dropped considerably from last year, when 51% admitted being hit. While the drop is welcome news, it's likely due in part to evolving attacker behaviors observed by SophosLabs and the Sophos Managed Threat Response team. For instance, many attackers have moved from larger scale, generic, automated attacks to more targeted attacks that include human-operated, hands-on-keyboard hacking. While the overall number of attacks is lower, our experience shows that the potential for damage from these targeted attacks is much higher.

The impact of ransomware

Ability of retail to stop data encryption

We asked those organizations that were hit with ransomware whether the cybercriminals succeeded in encrypting their data. 54% of retail respondents said their data was encrypted, which is the same as the global average.



Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? [2006 cross-sector; 193 retail establishments that have been hit by ransomware in the last year]

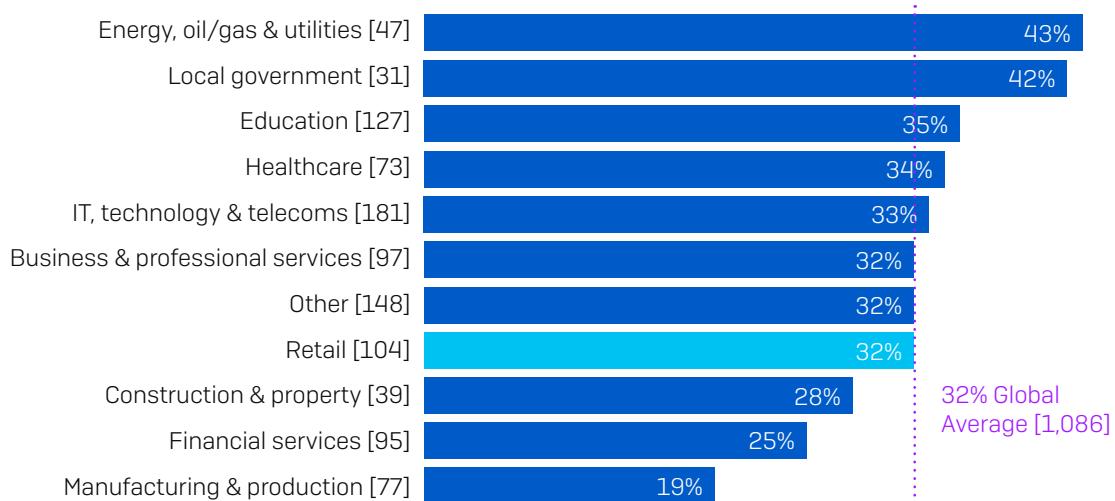
Retail organizations are less successful at stopping encryption than the global average: 34% vs. 39%. This sector also saw the second highest number of attacks across all industries (12% vs 7% of global average) where the data was not encrypted but they were held to ransom based on the threat of exposing the data.

SophosLabs has seen an increase in extortion-style attacks over the last year where, instead of encrypting files, adversaries steal data and threaten to publish it unless the ransom demand is paid. This requires less effort on the part of the attackers as no encryption or decryption is needed. Adversaries often leverage the punitive fines for data breaches in their demands in a further effort to make victims pay up.

Propensity to pay the ransom

Retail organizations (32%) are on par with the global industry average (32%) when it comes to propensity to pay the ransom to get their data back. This is encouraging to note given that retail sector is, along with education, the most hit by ransomware.

% that paid the ransom to get their data back



Did your organization get the data back in the most significant ransomware attack? Yes, we paid the ransom [base numbers in chart] organizations where the cybercriminals succeeded in encrypting their data in the most significant ransomware attack, omitting some answer options, split by sector

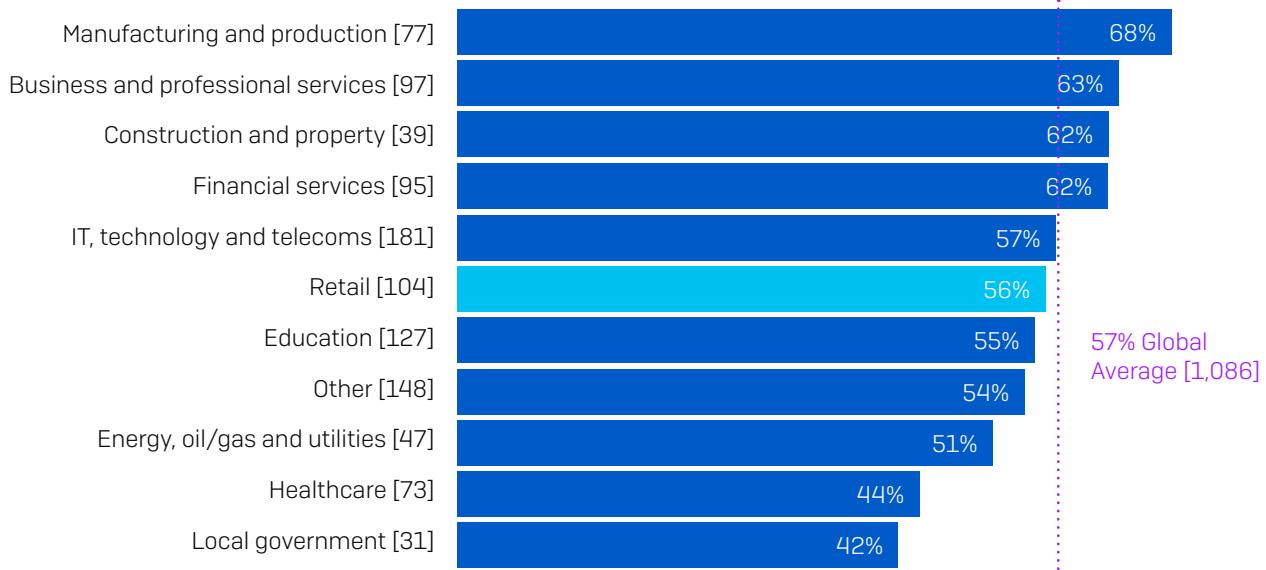
Across sectors, the **energy, oil/gas, and utilities sector** is most likely to pay the ransom, with 43% submitting to the ransom demand. This sector typically has a lot of legacy infrastructure that cannot easily be updated, so victims may feel compelled to pay the ransom to enable continuation of services.

Local government reports the second-highest level of ransom payments (42%). This is also the sector most likely to have its data encrypted. It may well be that the propensity of local government organizations to pay up is driving attackers to focus their more complex and effective attacks on this audience.

Ability to restore data using backups

There is a correlation between ability to restore data from backups and propensity to pay the ransom, with those organizations most able to use backups also least likely to pay up.

% that used backups to restore encrypted data

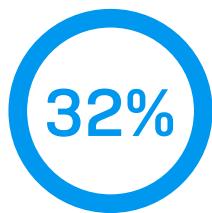


Did your organization get the data back in the most significant ransomware attack?

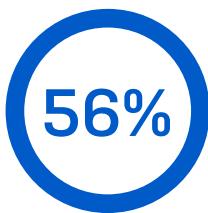
Yes, we used backups to restore the data [base numbers in chart] organizations where the cybercriminals succeeded in encrypting their data in the most significant ransomware attack, omitting some answer options, split by sector

In the previous chart we saw that retail's likeliness to pay the ransom was in line with the global average. Similarly, 56% of retail organizations were able to restore their data from backups – a notch lower than the global average of 57%.

97% got encrypted data back



Paid ransom to get the data back



Used backups to restore their data

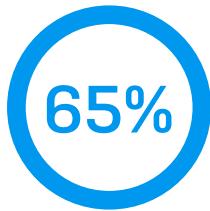


Used other means to get their data back

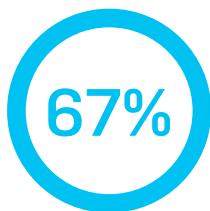
Did your organization get the data back in the most significant ransomware attack? [104] retail organizations responded.

The good news for retail organizations is that 97% of those whose data was encrypted got it back. As we've seen, 32% paid the ransom, 56% used backups, and 9% used other means to get their data back.

Paying the ransom only gets you some of your data



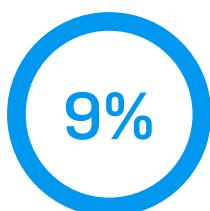
Percentage of data restored
after paying the ransom
CROSS-SECTOR AVERAGE



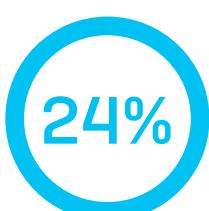
Percentage of data restored
after paying the ransom
RETAIL AVERAGE

Average amount of data organizations got back in the most significant ransomware attack. [344/33] organizations that paid the ransom to get their data back

The bad news, however, is that retail organizations that paid the ransom rarely got *all* their data back. On average, those that paid out got back just 67% of their data, leaving almost a third inaccessible. This is slightly better than the global average (65%) but still leaves a considerable proportion of the data inaccessible.



Got ALL their data back



Got half or less of their data back

Average amount of data Retail organizations got back in the most significant ransomware attack. [33] organizations that paid the ransom to get their data back

In fact, just 9% of retail organizations that paid the ransom got back all their data, and 24% got back **half or less** of their data. Clearly paying up doesn't pay off.

The cost of ransomware

Revealed: the ransom payments

Of the 357 respondents across all sectors who reported that their organization paid the ransom, 282 also shared the exact amount paid, including 36 in the retail sector.

\$ 170,404

Average GLOBAL ransom payment

\$ 147,811

Average RETAIL ransom payment

How much was the ransom payment your organization paid in the most significant ransomware attack? [282/36]

organizations that paid the ransom to get their data back

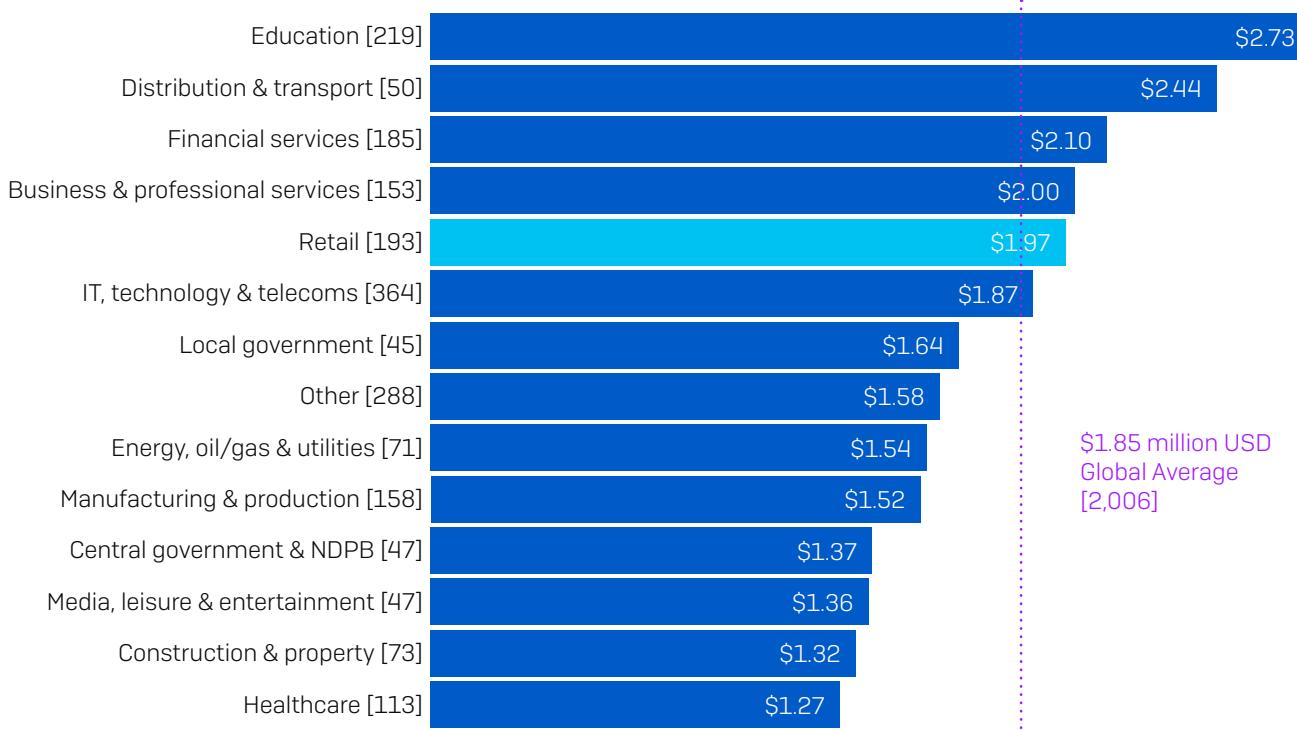
Globally across all sectors, the average ransom payment was US\$170,404. However, in retail, the average ransom payment was almost US\$23,000 lower, coming in at US\$147,811.

These numbers vary greatly from the eight-figure dollar payments that dominate the headlines for multiple reasons.

1. **Organization size.** Our respondents are from mid-sized organizations between 100 and 5,000 users who, in general, have fewer financial resources than larger organizations. Ransomware actors adjust their ransom demand to reflect their victim's ability to pay, typically accepting lower payments from smaller companies. The data backs this up, with the average ransom payment for 100-1,000 employee organizations coming in at US\$107,694, while the average ransom paid by 1,001 to 5,000 employee organizations is US\$225,588.
2. **The nature of the attack.** There are many ransomware actors, and many types of ransomware attacks, ranging from highly skilled attackers who use sophisticated tactics, techniques, and procedures (TTPs) focused on individual targets, to lower skilled operators who use 'off the shelf' ransomware and a general 'spray and pray' approach. Attackers who invest heavily in a targeted attack will be looking for high ransom payments in return for their effort, while operators behind generic attacks often accept lower return on investment (ROI).
3. **Location.** As we saw at the start, this survey covers 30 countries across the globe, with varying levels of GDP. Attackers target their highest ransom demands on developed Western economies, motivated by their perceived ability to pay larger sums. The two highest ransom payments were both reported by respondents in Italy. Conversely, in India, the average ransom payment was US\$76,619, less than half the global number (base: 86 respondents).

Ransomware recovery cost in retail

The ransom is just a small part of the overall cost of recovering from a ransomware attack. Victims face a wide range of additional expenses including the cost to rebuild and secure their IT systems, PR, and forensic analysis.



Average approximate cost to organizations to rectify the impacts of the most recent ransomware attack [considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.] [base numbers in chart] respondents whose organization had been hit by ransomware in the last year, split by sector, Millions of US\$

The survey revealed that the retail sector experiences an average remediation cost of US\$1.97 million (considering downtime, hours lost, device cost, network cost, lost opportunity, ransom paid, and so on), which is above the global average (US\$1.85 million).

There are several likely factors behind this. Firstly, due to the nature of their business, retail organizations typically hold a lot of sensitive data, including their customers' personal as well as financial information. As a result, they are disproportionately affected by the high costs of dealing with a data breach, which include notifying affected individuals and putting in place credit monitoring services. Secondly, retail is far more impacted by reputational damage than many other sectors – it's generally much easier to switch to a different retailer than to a different school or hospital. Another factor contributing to high recovery costs in this sector is the need to often rebuild legacy systems from the ground up in the wake of an attack.

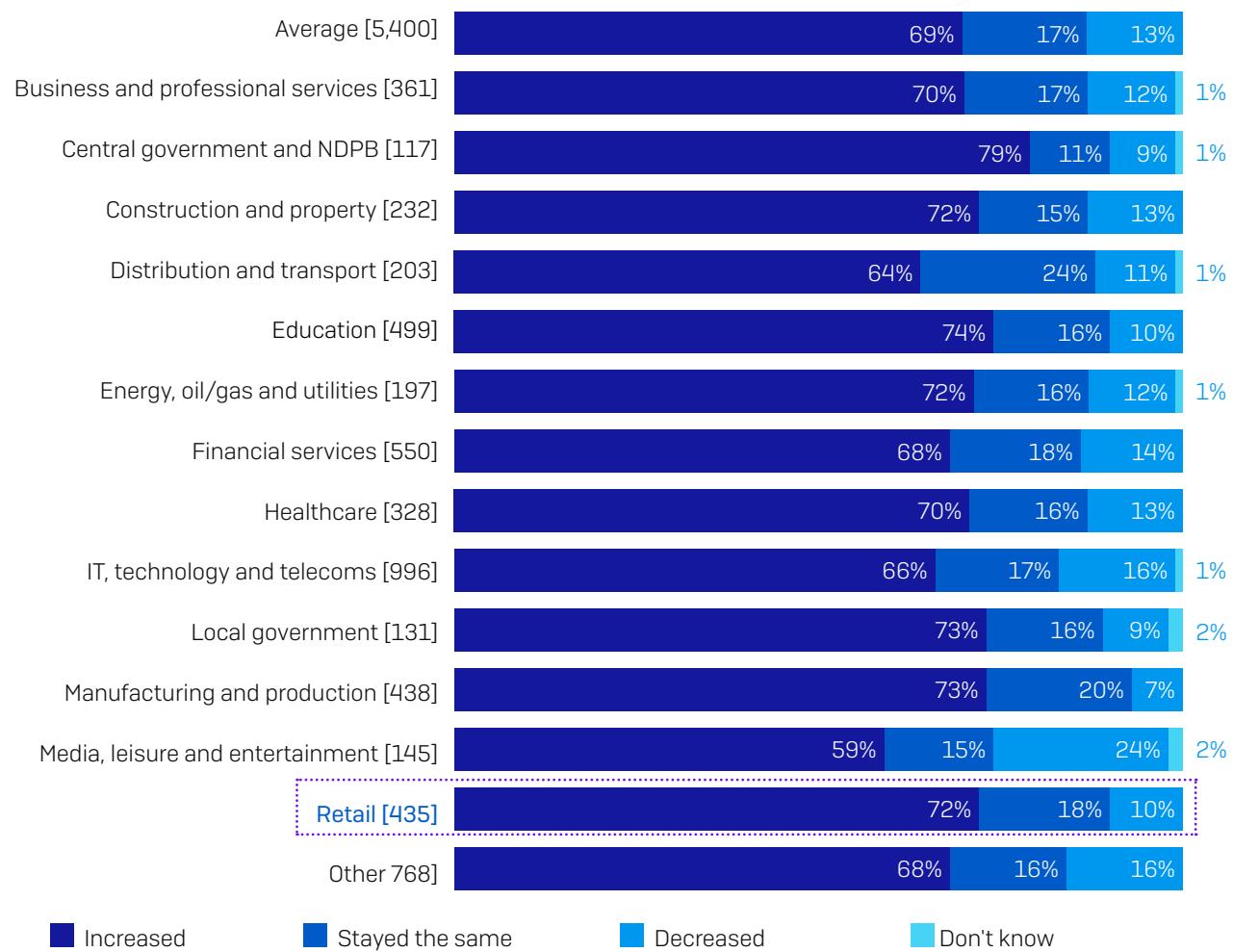
Ransomware is just a part of the cybersecurity challenge

Ransomware is a major cybersecurity issue for retail organizations, but not the only one. IT teams are juggling multiple cybersecurity demands, and their challenge has been exacerbated by the pandemic.

Cybersecurity workload increased in 2020

We asked the survey respondents how their cybersecurity workload had changed over the course of 2020.

How cybersecurity workload changed over the course of 2020



■ Increased

■ Stayed the same

■ Decreased

■ Don't know

Over the course of 2020, our cybersecurity workload has decreased/increased/stayed the same [base sizes in chart], split by sector.

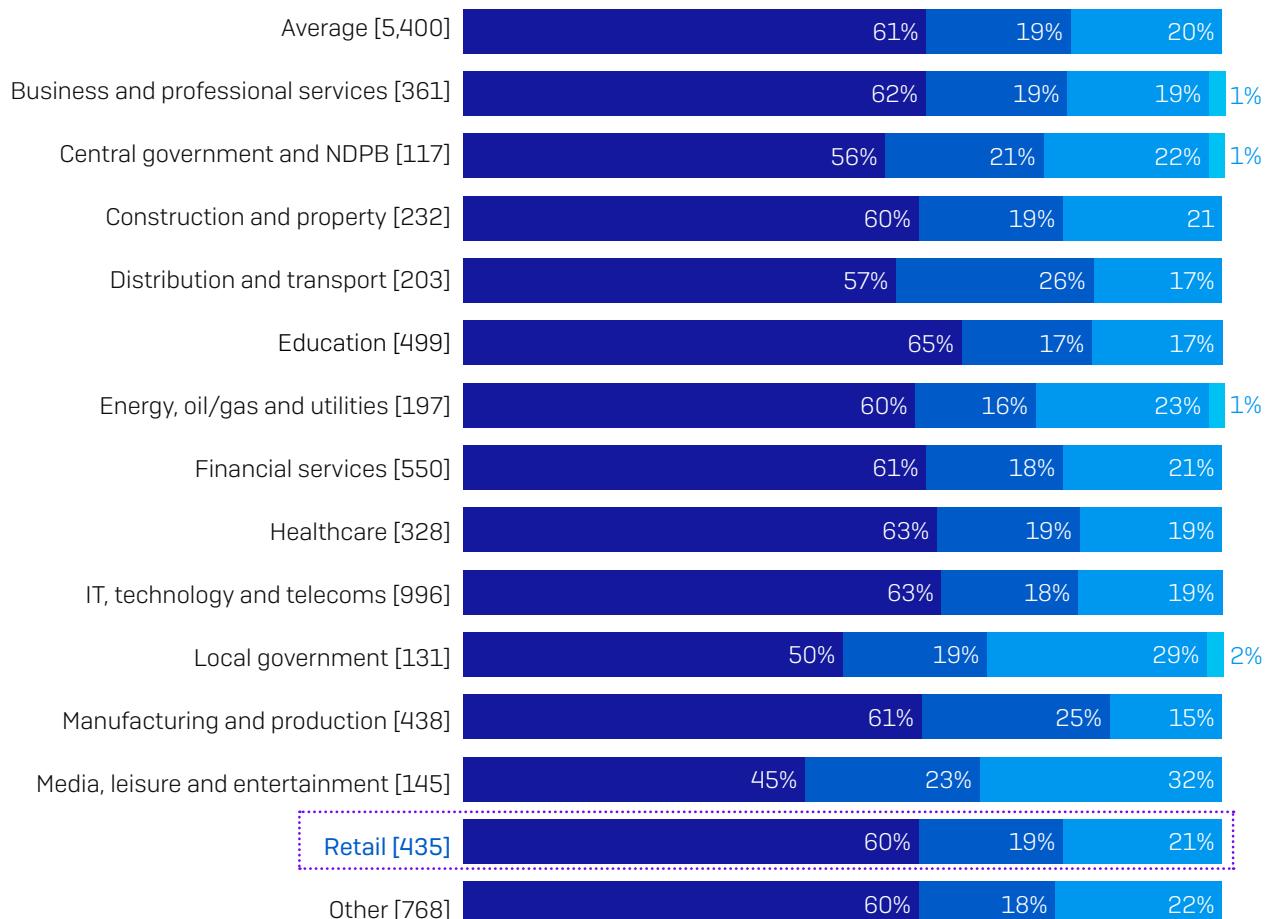
IT teams in the retail sector were impacted by the pandemic, with 72% experiencing an increase in cybersecurity workload over the course of 2020. While the majority of respondents in all sectors reported an increase, central government saw the most increase in growth in workload.

The switch to online shopping was likely a major factor behind the increased workload with IT teams needing to secure new online platforms as well as the increased traffic to their online sites. The heavy focus on securing online platforms would have likely reduced IT teams' capacity to monitor for and respond to ransomware threats.

Increased workload slowed response times

One of the consequences of the increase in cybersecurity workload over 2020 was a slowdown in response time to IT cases.

Changes in response time to IT cases over the course of 2020



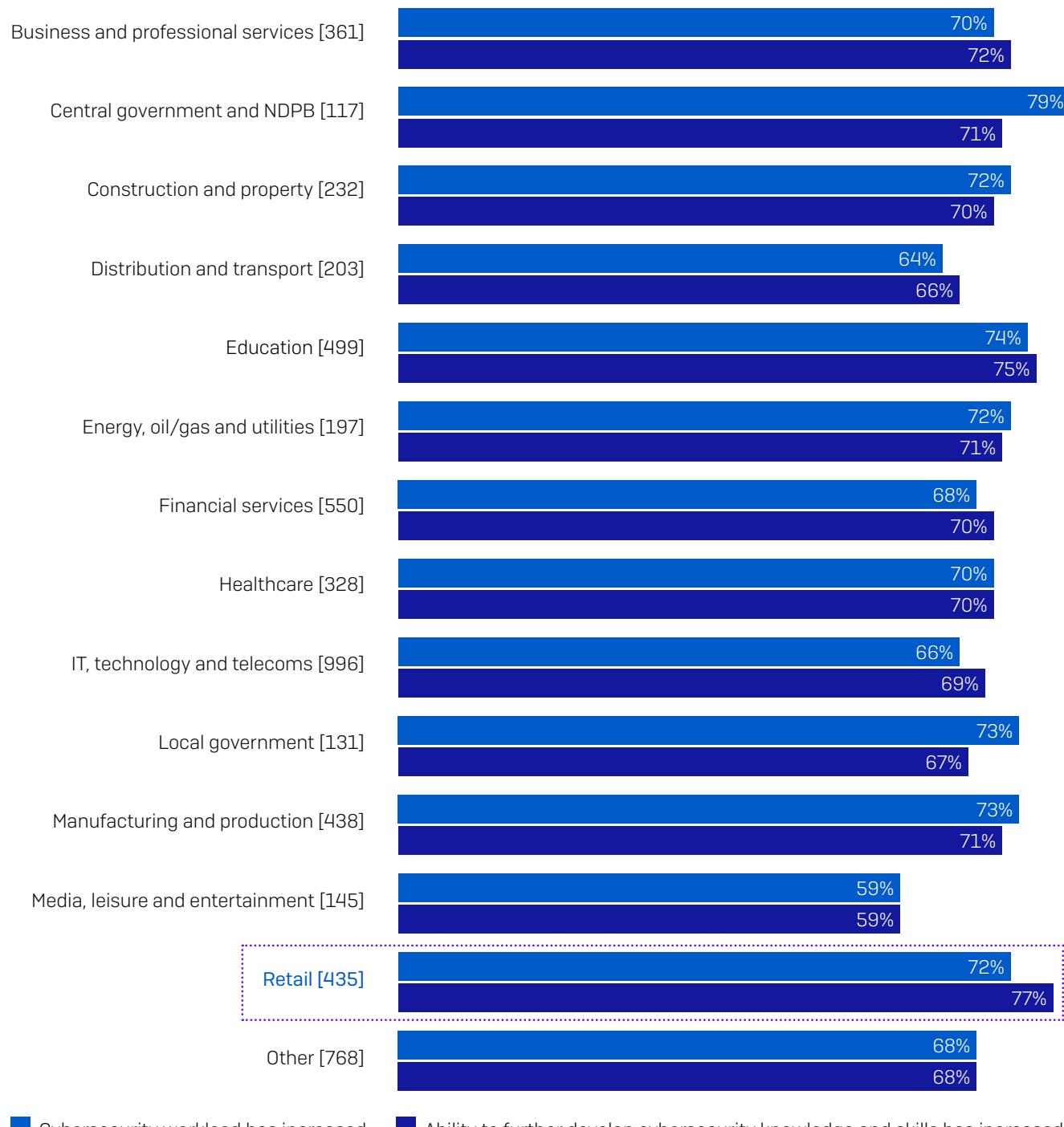
Over the course of 2020, our response time to IT cases has decreased/increased/stayed the same. [base sizes in chart], split by sector. N.B. Due to rounding, some totals are greater than 100%

The retail sector was significantly affected, with 60% respondents reporting that response time increased over last year. When an adversary is in your environment, it's imperative to stop them as early as possible. The longer they are allowed to explore your network and access your data, the greater the financial and operational impact of the attack. The slowdown in response time is therefore a cause for alarm.

Increased workload increased knowledge and skills

Every cloud has a silver lining, and there is also a clear correlation between increase in cybersecurity workload and increased ability to develop cybersecurity knowledge and skills.

Increase in cybersecurity workload and increase in ability to develop cybersecurity knowledge and skills



█ Cybersecurity workload has increased █ Ability to further develop cybersecurity knowledge and skills has increased

Over the course of 2020, our cybersecurity workload/our ability to further develop our cybersecurity knowledge and skills has increased [base sizes in chart], split by sector

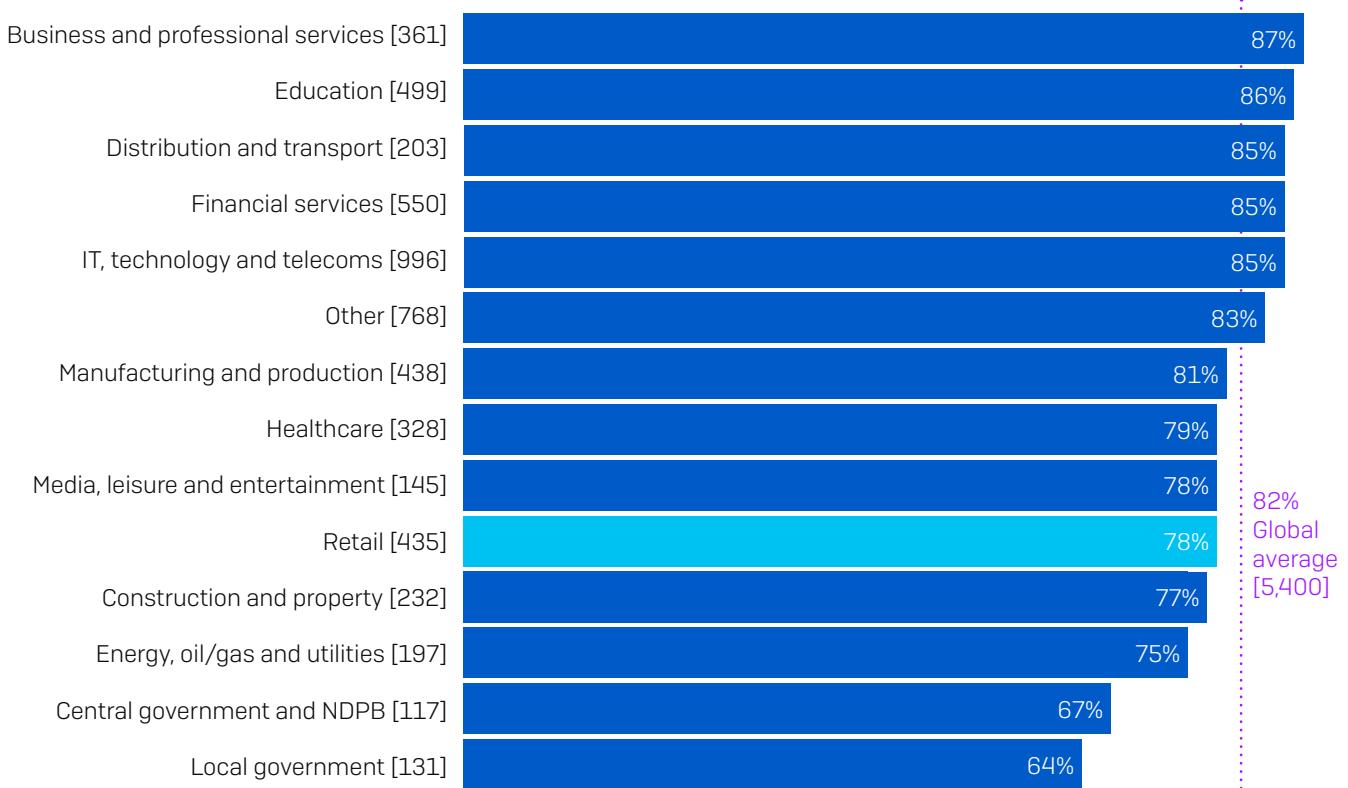
The State of Ransomware in Retail 2021

77% of IT teams in retail said their ability to develop cybersecurity knowledge and skills increased over the course of 2020, the highest of all industries. While increased workload adds pressure, it also provides more opportunities to learn new things. It's also likely that the unique circumstances of the pandemic also required IT teams to deliver outputs that they had never been asked for before.

Readiness to take on future challenges

Even though the IT teams in retail reported to have the highest ability to develop cybersecurity knowledge and skills over 2020, this confidence was not reflected proportionally when asked if they had the tools and knowledge needed to investigate suspicious activities in their organization.

Have the tools and knowledge to investigate suspicious activity



If I detect suspicious activities in my organization, I have the tools and knowledge I need to investigate fully: Strongly agree, Agree. Omitting some answer options [base sizes in chart], split by sector

Only 78% of retail respondents said they have the tools and knowledge needed – lower than the global average [82%]. This is a cause for worry given the high level of ransomware attacks experienced by the retail sector and the increased cybersecurity workload. Having the right tools and knowledge is key to being able to investigate and address cyberthreats.



The State of Ransomware 2024

**Findings from an independent, vendor-agnostic survey
of 5,000 leaders responsible for IT/cybersecurity across
14 countries, conducted in January–February 2024.**

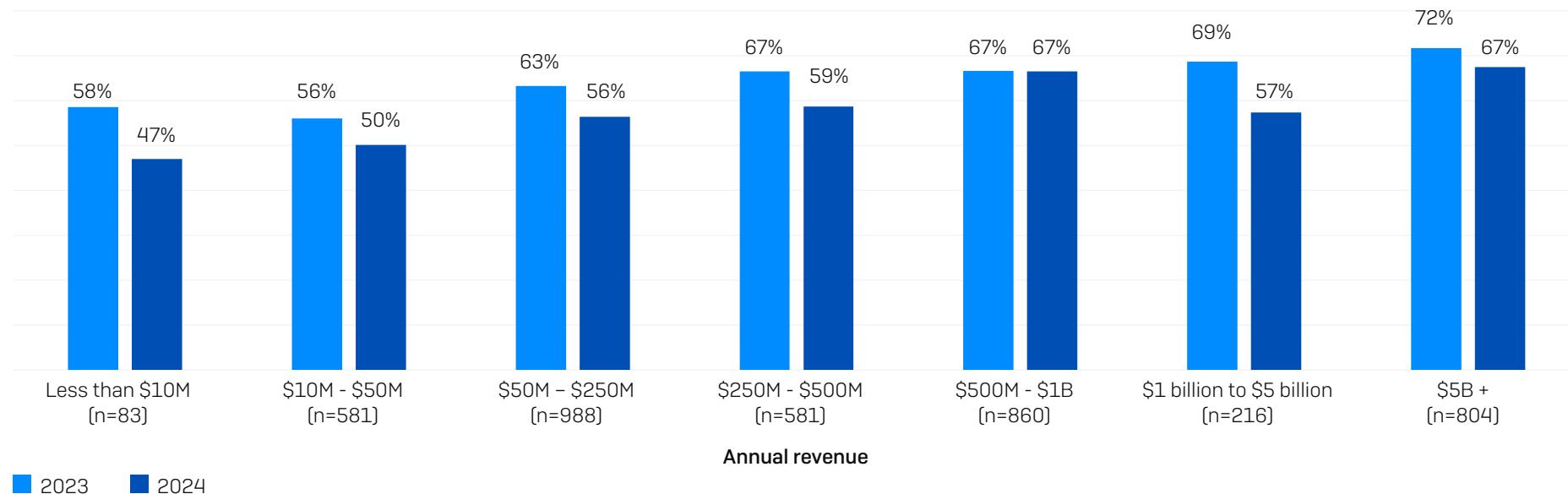
Rate of Ransomware Attacks

59% of organizations were hit by ransomware last year, a small but welcome drop from the 66% reported in both the previous two years. While any reduction is encouraging, with more than half of organizations experiencing an attack, this is no time to lower your guard.



In the last year, has your organization been hit by ransomware?
Yes. n=5,000 [2024], 3,000 [2023], 5,600 [2022], 5,400 [2021], 5,000 [2020].

Percentage of organizations hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? Yes. n=5,000 [2024], 3,000 [2023]. 2024 segment base numbers in chart.

Attacks by Revenue

Encouragingly, all revenue segments reported a reduction in ransomware attack rate in the last year (although for \$500M - \$1B it was less than one percentage point).

The propensity to be hit by ransomware generally increases with revenue, with \$5B+ organizations reporting the joint highest rate of attack (67%). However, even the smallest organizations (less than \$10M revenue) are still regularly targeted, with just under half (47%) hit by ransomware in the last year. While many ransomware attacks are executed by sophisticated, well-funded gangs, the use of crude, cheap ransomware by lower-skilled threat actors is on the rise.

Attacks by Industry

With a few exceptions, ransomware attack rates were broadly consistent across the different sectors, with between 60% and 68% of organizations hit in 11 of the 15 industries covered. The notable winners in this year's study are *state/local government* [34%] and *retail* [45%] where fewer than half of respondents reported being hit in the last year.

Interestingly, the two government sectors occupy opposing positions, with *central/federal government* reporting the highest attack rate across all industries [68%], double the rate reported by *state/local government* [34%]. At the same time, reflecting the general downward trend in attacks, the *central/federal government* rate is lower than the sector's 2023 figure of 70%.

There are several possible reasons behind this government variance. In a year of widespread unrest, it may be that central governments have experienced an increase in politically motivated attacks. The results could also reflect efforts over the last year by state/local government organizations to strengthen their resilience to attack – or a shift in approach by adversaries in response to the state/local government sector's limited ability to pay ransoms.

Other notable industry changes over the last year include:

- Reduction in the highest individual rate of attack reported, down from 80% [*lower education*] to 69% [*central/federal government*]
- The education sector no longer reports the two highest rates of attack, coming in at 66% [*higher education*] and 63% [*lower education*] this year vs. 79% and 80% respectively last year
- *Healthcare* was one of five sectors that reported an increase in attack rate over the last year, up from 60% to 67%
- *IT, telecoms, and technology* no longer has the lowest attack rate with 55% of organizations hit in the last year, an increase from the 50% reported in 2023

See the appendix for a detailed breakdown of rate of ransomware attacks by industry.

Attacks by Country

France reported the highest rate of ransomware attacks in 2024 with 74% of respondents saying they had been hit in the last year, followed by South Africa [69%] and Italy [68%]. Conversely, the lowest reported attack rates were by respondents in Brazil [44%], Japan [51%], and Australia [54%].

Overall, nine countries reported a lower attack rate than in 2023. The five countries that reported a higher rate of attack than in 2023 are all in Europe: Austria, France, Germany, Italy, and the UK [Germany's increase was less than 1%]. This may reflect an increase in targeting of European organizations or that European defenses have been less able to keep pace with the evolving attacker behaviors than in other geographies.

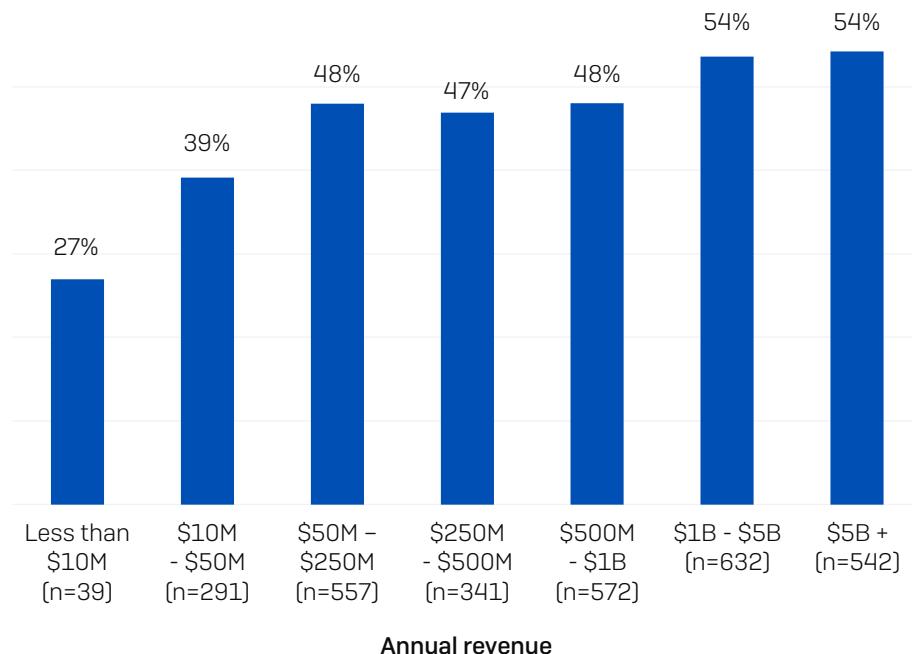
See the appendix for a detailed breakdown of rate of ransomware attacks by country.

Percentage of Computers Impacted by Revenue

While globally, across all respondents, the distribution was broad, we see considerable variation in devices impacted both by organization size and industry.

As revenue increases, so does the proportion of the computer estate that was impacted in the ransomware attack, with the smallest organizations (less than \$10M) reporting half the percentage of devices impacted compared to those with revenue of \$1B or more (27% vs. 54%).

There are several factors that may contribute to this finding. Smaller organizations are less likely to centrally manage all their devices, reducing the opportunity for attacks to spread across the estate. Additionally, most small businesses and startups are heavy users of SaaS platforms, reducing the risk of business outage from threats like ransomware.



What percentage of your organization's computers were impacted by ransomware in the last year? n=2,974 organizations hit by ransomware.

Percentage of Computers Impacted by Industry

IT, technology and telecoms reported the smallest percentage of devices impacted (33%), reflecting the strong cyber posture that is often seen in this sector.

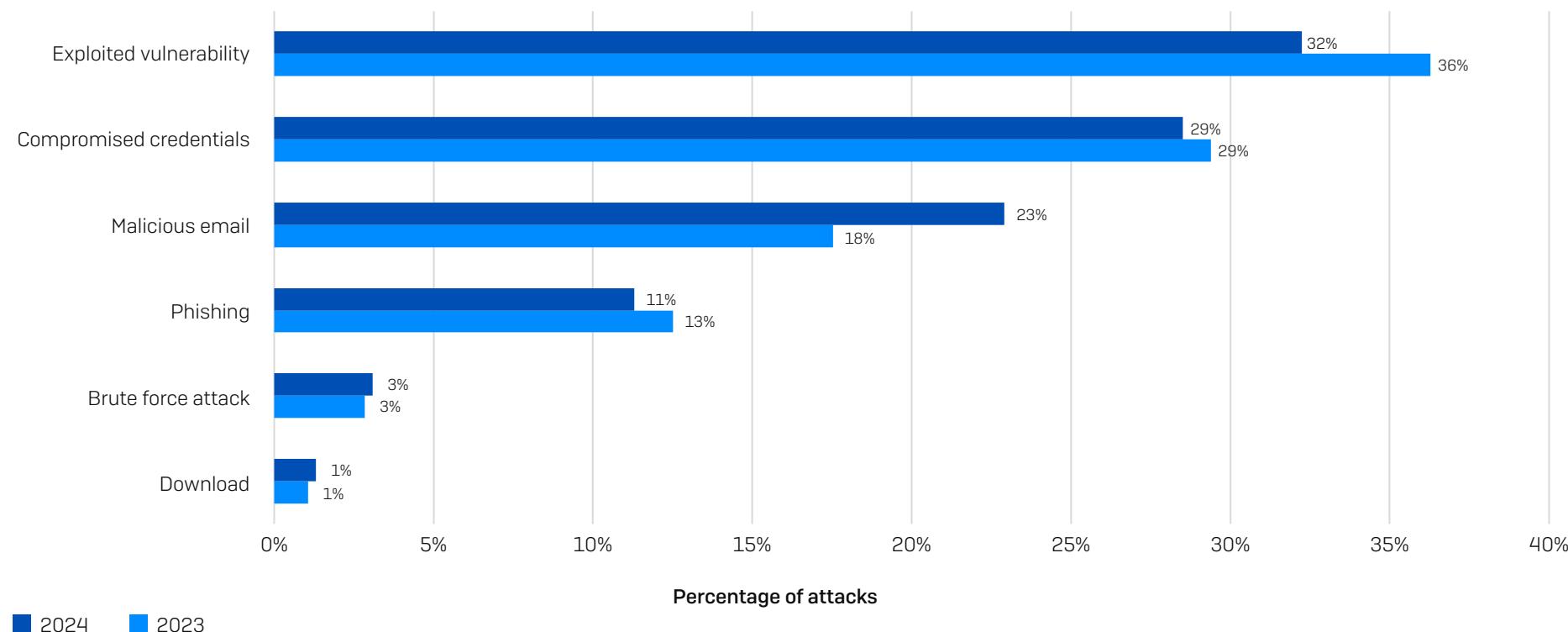
Conversely, *energy, oil/gas and utilities* is the sector where the effects of an attack are most broadly experienced, with 62% of devices impacted, on average, followed by *healthcare* (58%). Both industries are challenged by higher levels of legacy technology and infrastructure controls than most other sectors, which likely makes it harder to secure devices, limit lateral movement, and prevent attacks from spreading.

See the appendix for a detailed breakdown of percentage of computers impacted by industry.

Root Causes of Ransomware Attacks

99% of organizations hit by ransomware were able to identify the root cause of the attack, with exploited vulnerabilities the most commonly identified starting point for the second year running. Overall, the running order remained consistent with our 2023 study.

Email-based approaches were identified as the root cause of attack by 34% of respondents, with around twice as many starting with a malicious email [i.e., a message with a malicious link or attachment that downloads malware] as phishing [i.e., a message designed to trick readers into revealing information]. It's worth noting that phishing is typically used to steal log-in details and as such can be considered the first step in a compromised credentials attack.



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=2,974 organizations hit by ransomware.

Exploited Vulnerability Attacks

While all ransomware attacks have negative outcomes, some are more devastating than others. Organizations whose attacks began with exploitation of an unpatched vulnerability report considerably more severe outcomes than those where the attack started with compromised credentials, including a higher propensity to:

- Have backups compromised
(75% success rate vs. 54% for compromised credentials)
- Have data encrypted
(67% encryption rate vs. 43% for compromised credentials)
- Pay the ransom
(71% payment rate vs. 45% for compromised credentials)
- Cover the full cost of the ransom in-house (31% funded the full ransom in-house vs. 2% for compromised credentials)

They also reported:

- 4X higher overall attack recovery costs
(\$3M vs. \$750K for compromised credentials)
- Slower recovery time (45% took more than a month vs. 37% for compromised credentials)

For a deeper dive, read [Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector](#).

Root Cause by Industry

Certain weaknesses in cyber defenses are more prevalent in some sectors than others, and adversaries are quick to take advantage. As a result, the root cause of ransomware attacks varies considerably by industry:

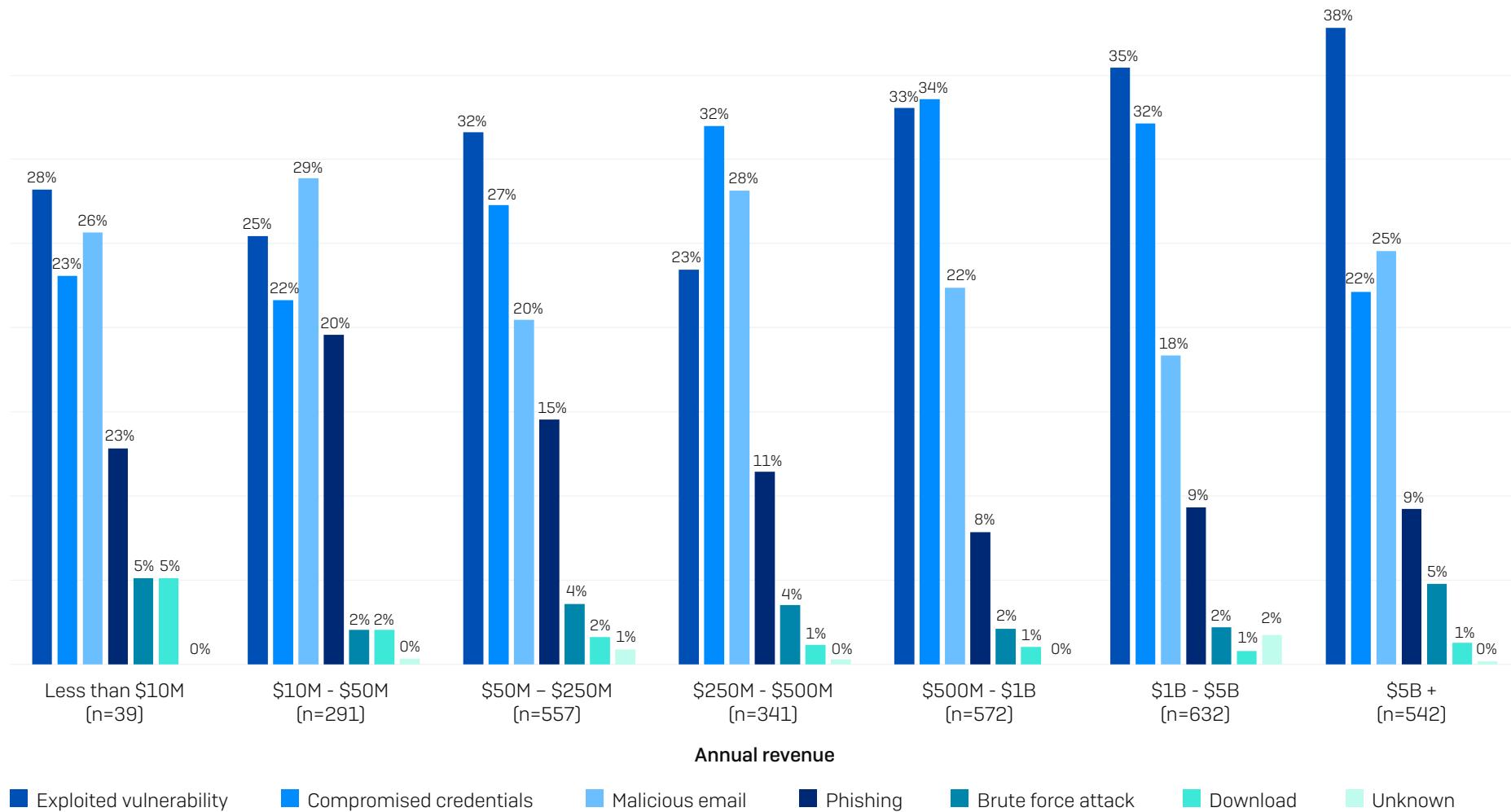
- *Energy, oil/gas and utilities* is the sector most likely to fall victim to the exploitation of unpatched vulnerabilities, with almost half (49%) of attacks beginning in this way. This industry typically uses a higher proportion of older technologies more prone to security gaps than many other sectors, and patches may not be available for legacy and end-of-life solutions
- Government organizations are particularly vulnerable to attacks that start with abuse of compromised credentials: 49% [*state/local*] and 47% [*central/federal*] of attacks began with the use of stolen login data
- *IT, technology and telecoms* and *retail* both reported that 7% of ransomware incidents began with a brute force attack – it may be that their reduced exposure to unpatched vulnerabilities and compromised credentials forces adversaries to focus, in part, on other approaches

See the appendix for a detailed breakdown of rate of the root cause of attack by industry.

Root Cause by Revenue

Generally speaking, larger organizations are more likely to experience an attack that starts with an unpatched vulnerability, with the \$5B+ segment reporting the highest percentage of attacks that started in this way (38%). It is likely that IT infrastructures increase in both size and complexity as organizations grow, making it harder for IT teams to see all their exposures and patch before they are exploited.

Compromised credentials as a ransomware attack vector peaks in the mid/high revenue cohorts and is the top cause of attack in both the \$250M-\$500M and \$500M-\$1B segments. While vulnerabilities and compromised credentials rightly get a lot of focus, malicious email is the top reported root cause in \$10M-\$50M organizations. Overall, email-based threats account for just under half (49%) of attacks in this space.



Do you know the root cause of the ransomware attack your organization experienced in the last year? n=2,974 organizations hit by ransomware.

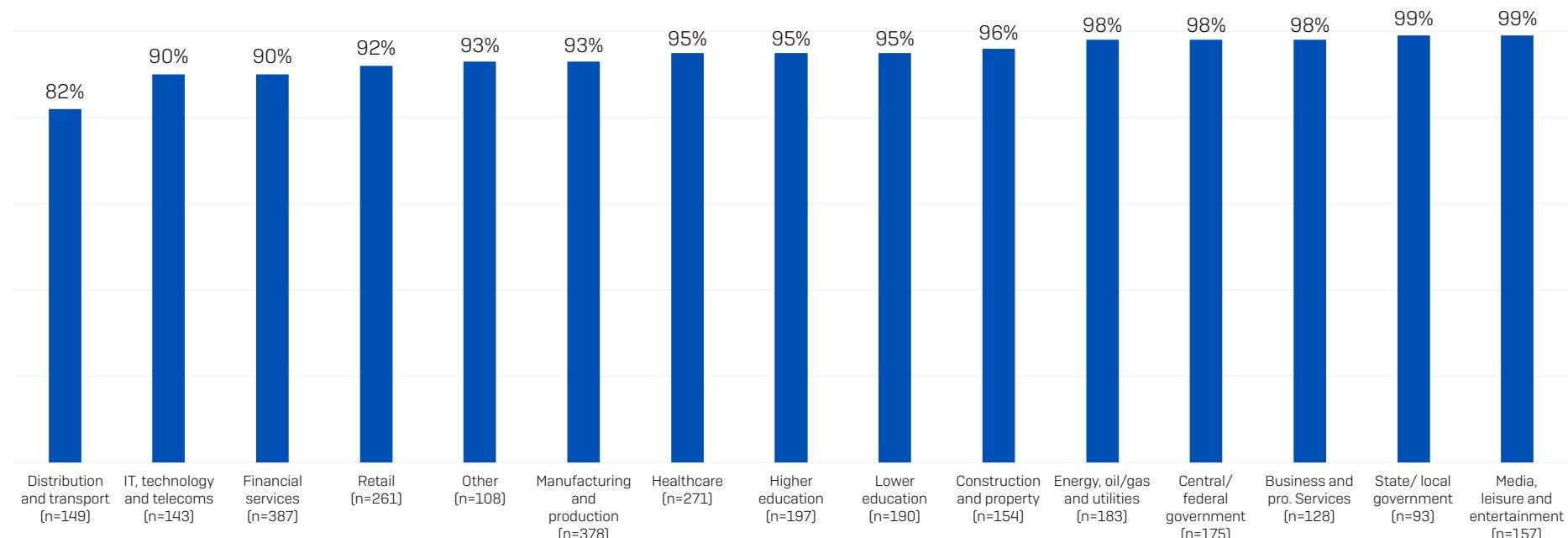
Backup Compromise

There are two main ways to recover encrypted data in a ransomware attack: restoring from backups and paying the ransom. Compromising an organization's backups enables adversaries to restrict their victim's ability to recover encrypted data and dials up the pressure to pay the ransom.

Attempted Backup Compromise

94% of organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack. This rose to 99% in both *state/local government*, and the *media, leisure and entertainment* sector. The lowest rate of attempted compromise was reported by *distribution and transport*, however even here more than eight in ten (82%) organizations hit by ransomware said the attackers tried to access their backups.

Percentage of attacks where adversaries attempted to compromise backups



Did the cybercriminals try to compromise your organization's backups? Yes. Base number in chart.

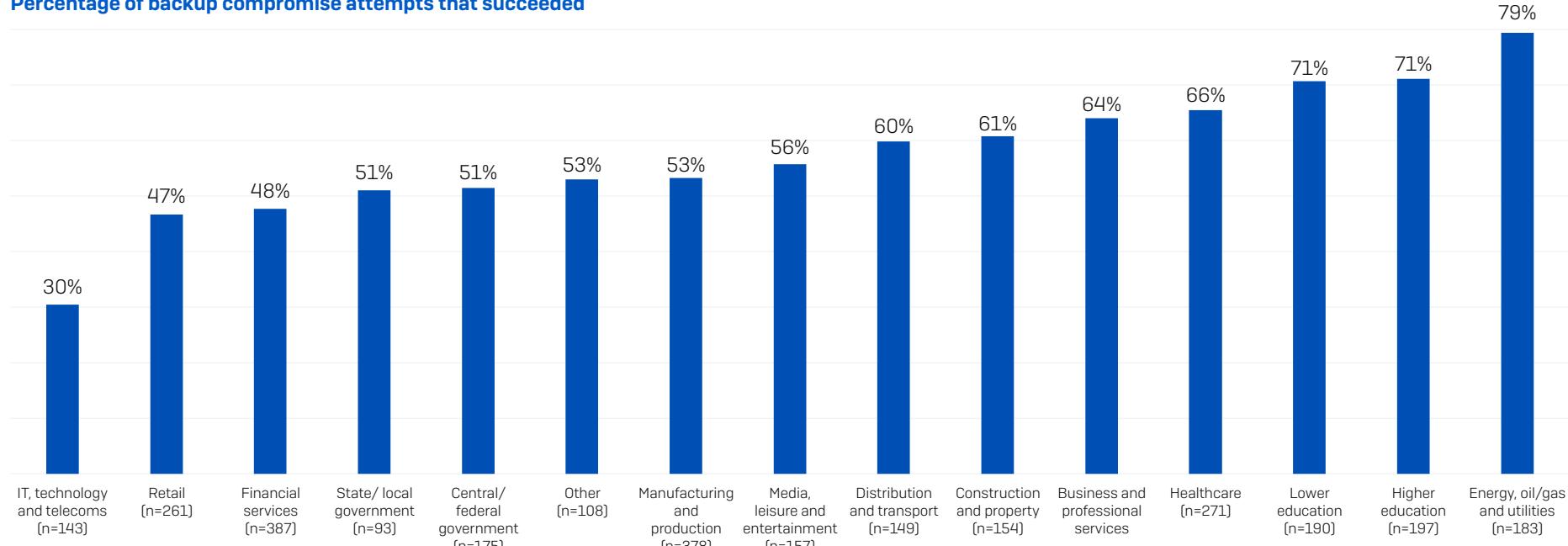
Success Rate of Backup Compromise Attempts

Across all sectors, 57% of backup compromise attempts were successful, meaning that adversaries were able to impact the ransomware recovery operations of over half of their victims. The analysis revealed considerable variation in adversary success rate by sector:

- Attackers were most likely to successfully compromise their victims' backups in the *energy, oil/gas and utilities* [79% success rate] and *education* [71% success rate] sectors
- IT, technology and telecoms* [30% success rate] and *retail* [47% success rate] reported the lowest rates of successful backup compromise

There are several possible reasons behind the differing success rates. It may be that *IT, telecoms and technology* had stronger backup protection in place to start with so was more resilient to attack than other sectors. They may also be more effective at detecting and stopping attempted compromise before the attackers could succeed.

Percentage of backup compromise attempts that succeeded



Did the cybercriminals try to compromise your organization's backups? Yes, Base number in chart.

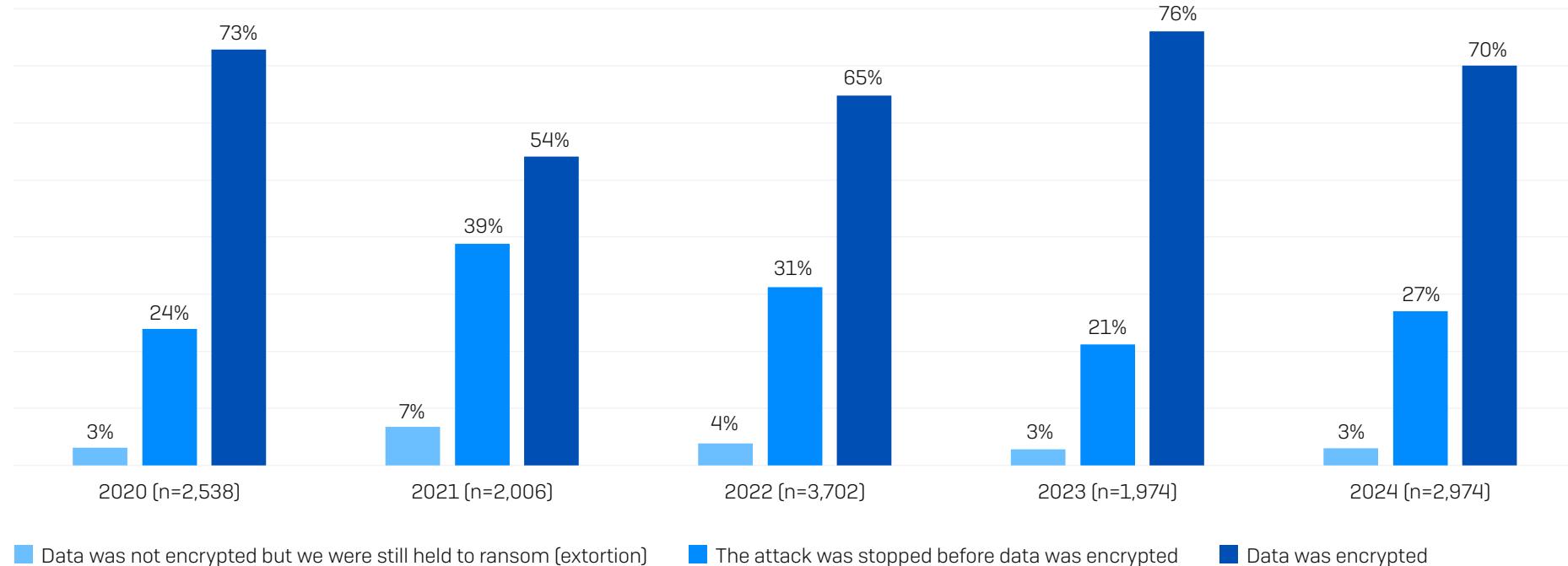
Whatever the cause, organizations that had backups compromised reported considerably worse outcomes than those whose backups were not breached:

- Ransom demands were, on average, more than double that of those whose backups weren't impacted (\$2.3M vs. \$1M median initial ransom demand)
- Organizations whose backups were compromised were almost twice as likely to pay the ransom to recover encrypted data [67% vs. 36%]
- Median overall recovery costs came in eight times higher [\$3M vs. \$375K] for those that had backups compromised

For a deeper dive, read [The Impact of Compromised Backups on Ransomware Outcomes](#).

Rate of Data Encryption

Seven in ten (70%) ransomware attacks in the last year resulted in data encryption. While high, this rate represents a small drop from the 76% of attacks where adversaries succeeded in encrypting data that was reported in 2023.



Data Encryption Rate by Industry

The 2024 survey reveals considerable variation in encryption rate across industries.

- While state/local government reported the lowest frequency of attack this year (34% hit by ransomware), it also reported the **highest rate of data encryption**, with 98% of attacks resulting in data being encrypted
- Financial services (49%) followed by retail (56%) reported the **lowest rates of data encryption**
- Distribution and transport* is the sector most likely to have experienced an **extortion-based attack** with 17% saying that data was not encrypted but they were held to ransom anyway – almost three times the rate of any other sector

See the appendix for a detailed breakdown of data encryption rates by industry.

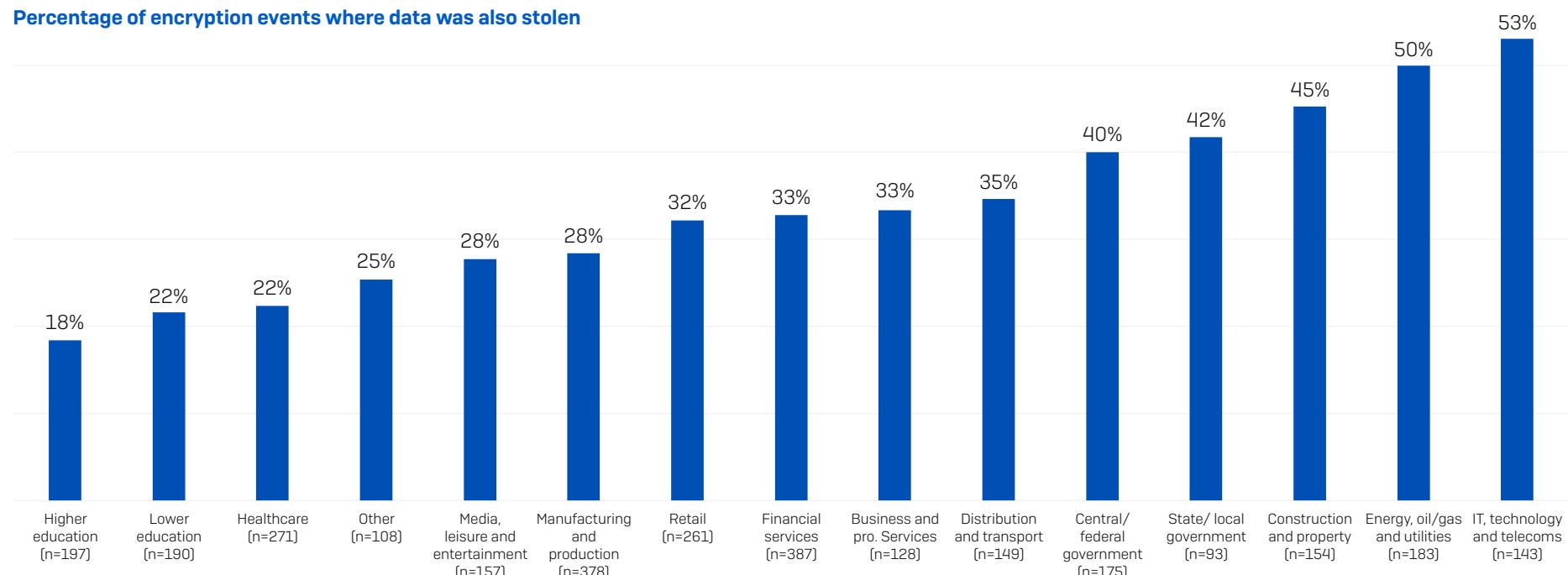
Data Theft

Adversaries don't just encrypt data; they also steal it. In 32% of incidents where data was encrypted, data was also stolen – slightly above last year's rate of 30%. Data theft increases attackers' ability to extort money from their victims, while also enabling them to further monetize the attack by selling the stolen data on the dark web.

Again, there is considerable variation by industry. On the surface *IT, technology and telecoms* fares worst, with 53% of attacks where data was encrypted reporting that it was also stolen. *Energy, oil/gas and utilities* is in second position, with data stolen in 50% of encryption events. Conversely, the education sector is least likely to report data theft in an attack, with *higher education* reporting the lowest overall propensity to have data encrypted and stolen [18%], followed by *lower education*, which shares second spot with healthcare (both 22%).

The findings may reflect differing levels of investigation capabilities across the sectors, and differing priorities. Determining whether data has been exfiltrated requires higher levels of forensic capabilities and often relies on logs from EDR/XDR tools. It may be that the *IT, technology and telecoms* sector is simply better able to identify data theft than other industries. The simplicity of many *energy, oil/gas and utilities* environments may also make theft easier to detect in this sector. Conversely, schools often lack the skills and tools to determine whether data has been stolen. At the same time, some organizations may prefer not to know if data has been exfiltrated as a data breach would require them to undertake expensive disclosures.

Percentage of encryption events where data was also stolen



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Yes. Yes, and the data was also stolen. Base number in chart.

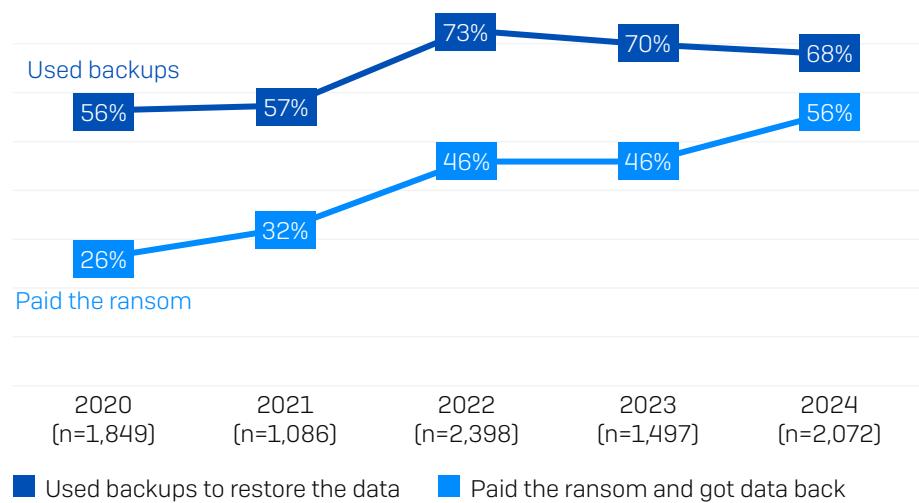
Data Recovery

98% of organizations that had data encrypted got data back. The two primary ways of recovering data were restoring from backups (68%) and paying the ransom to get the decryption key (56%). 26% of those that had data encrypted indicated that they used "other means" to get data back – while the survey did not explore this area further, this could include working with law enforcement or using decryption keys that had already been made public.



A notable change over the last year is the increase in propensity for victims to use multiple approaches to recover encrypted data [e.g., paying the ransom and using backups]. Almost half of organizations that had data encrypted reported using more than one method (47%) this time around, more than double the rate reported in 2023 (21%).

The five-year view reveals that the gap between use of backups and payment of the ransom continues to shrink. Backup use has fallen, albeit slightly, for the second consecutive year. At the same time, there has been a 10-percentage point increase in ransom payments since the 2023 study. Propensity to pay the ransom depends on many factors, including availability of backups. However, this is a worrying trend and it is concerning that over half of victims are resorting to paying for the decryption key.



Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. Base numbers in chart.

Data Recovery by Revenue

Propensity to pay the ransom to recover data generally increases with revenue. The smallest revenue organizations [less than \$10M] report by far the lowest ransom payment rate (25%) while the largest revenue organizations (\$5B+) have the highest payment rate (61%). The fundamental availability of funds to cover the ransom is likely a major factor at play here – many very small businesses are simply unable to find the money to pay a ransom.

However, as we've seen, data recovery is not a case of either backups or ransom. The nuances behind data recovery methods become apparent when we dive deeper into the data and compare the 2024 figures with last year's results.

Outside the sub \$10M group, all revenue segments reported an increased ransom payment rate compared to last year, and three of them also reported an increase in the use of backups to restore the data. While the lowest revenue group reported the highest rate of backup use (88%), the \$250M-\$500M was close behind (85%).

Data Recovery by Industry

Perhaps unsurprisingly, *central/federal government* is the sector least likely to pay the ransom to get data back – no doubt it is highly limited in the ability to pay by regulations – and also reported the highest use of backups to restore data (39% and 81% respectively).

Overall, there is no smooth correlation between backup use and ransom payments:

- *Media, leisure and entertainment* reported the highest rate of ransom payment to recover data (69%) and also one of the higher rates of backup use (74%)
- *Energy, oil/gas and utilities* has the lowest level of backup use (51%) and has a ransom payment rate of 61%, lower than four other sectors

See the appendix for a detailed breakdown of data recovery method by industry.

	ANNUAL REVENUE													
	Less than \$10M (n=39)		\$10M - \$50M (n=291)		\$50M - \$250M (n=557)		\$250M - \$500M (n=341)		\$500M - \$1B (n=572)		\$1B - \$5B (n=632)		\$5B + (n=542)	
Data recovery method used	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024
Used backups to restore the data	80%	88% ▲	72%	68% ▼	77%	60% ▼	75%	85% ▲	68%	70% ▲	66%	65% ▼	63%	66% ▲
Paid the ransom and got data back	36%	25% ▼	41%	49% ▲	42%	57% ▲	33%	50% ▲	51%	59% ▲	52%	56% ▲	55%	61% ▲

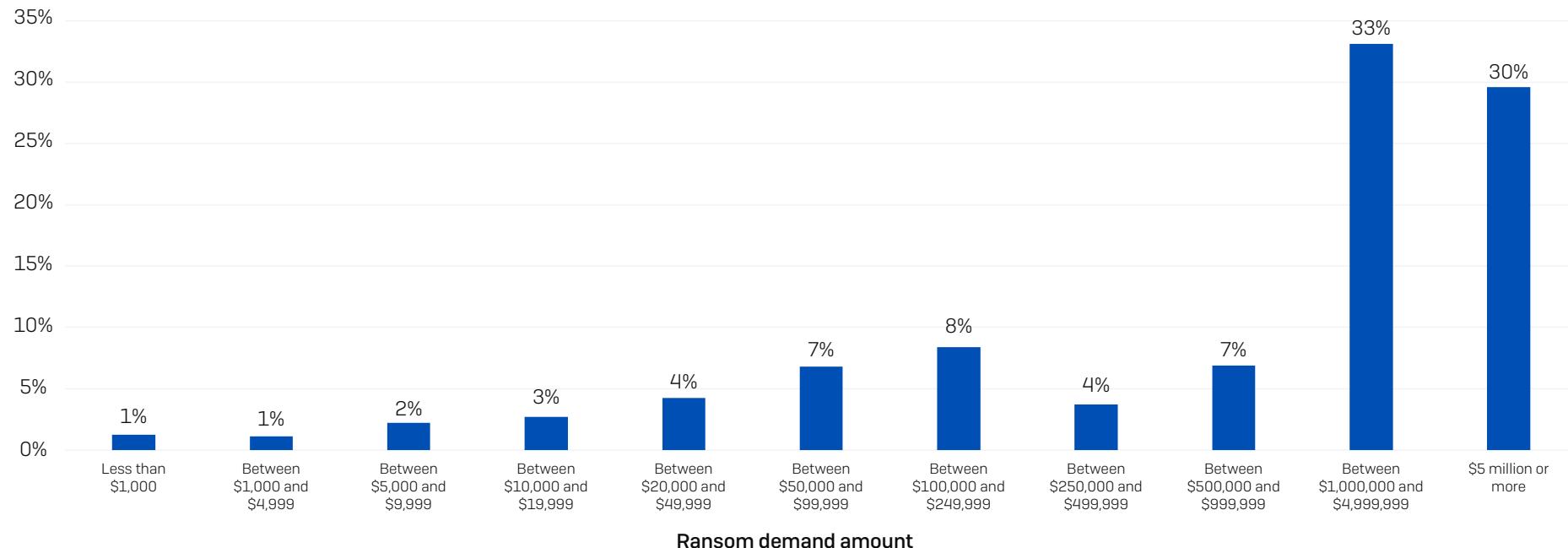
Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. 2024 base numbers in chart. Arrow indicates increase/decrease vs. 2023.

Ransom Demands

This year, for the first time, we included both ransom demands and payments in this report. Across the 1,701 organizations that had their data encrypted and were able to share the initial ransom demand from the attackers, the average ask was \$4,321,880 (mean) and \$2M (median).

One of the most notable findings in this year's study is that 63% of ransom demands are for \$1M or more, with 30% of demands for \$5M or more. While a small number of respondents reported four-figure ransom demands, these are very much in the minority.

Percentage of demands for the ransom amount



How much was the ransom demand from the attacker(s)? n=1,701

Ransom Demand by Revenue

Looking at both mean and median data, the ransom demand trends upward with revenue, indicating that adversaries adjust their ransom demand based – in part, at least – on likely ability to pay.

Huge ransom demands are no longer the preserve of the highest-revenue organizations, and \$1M or more asks are now commonplace across the board: 47% of organizations with revenue of \$10M-\$50M received a seven-figure ransom demand in the last year.

Ransom Demand by Industry

There are no winners here, with all named sectors (excluding "other") reporting median ransom demands of \$1M or higher.

- *Retail and IT, technology and telecoms* received the lowest median demands [\$1M], followed by *construction* [\$1.1M]
- *Central/federal government* is the sector with the biggest target on its head, reporting the highest median [\$7.7M] and mean [9.9M] demands

See the appendix for a detailed breakdown of ransom demand by industry.

Ransom Demand	ANNUAL REVENUE					
	\$10M - \$50M [n=207]	\$50M - \$250M [n=288]	\$250M - \$500M [n=158]	\$500M - \$1B [n=268]	\$1B - \$5B [n=366]	\$5B + [n=398]
Mean average	\$1,774,941	\$1,704,853	\$3,407,796	\$5,184,024	\$4,281,258	\$7,467,294
Median average	\$330,000	\$220,000	\$840,000	\$2,000,000	\$3,000,000	\$6,600,000

How much was the ransom demand from the attacker(s)? Base numbers in chart. N.B. "Less than \$10M" has been excluded from this table due to the low number of respondents in this revenue segment.

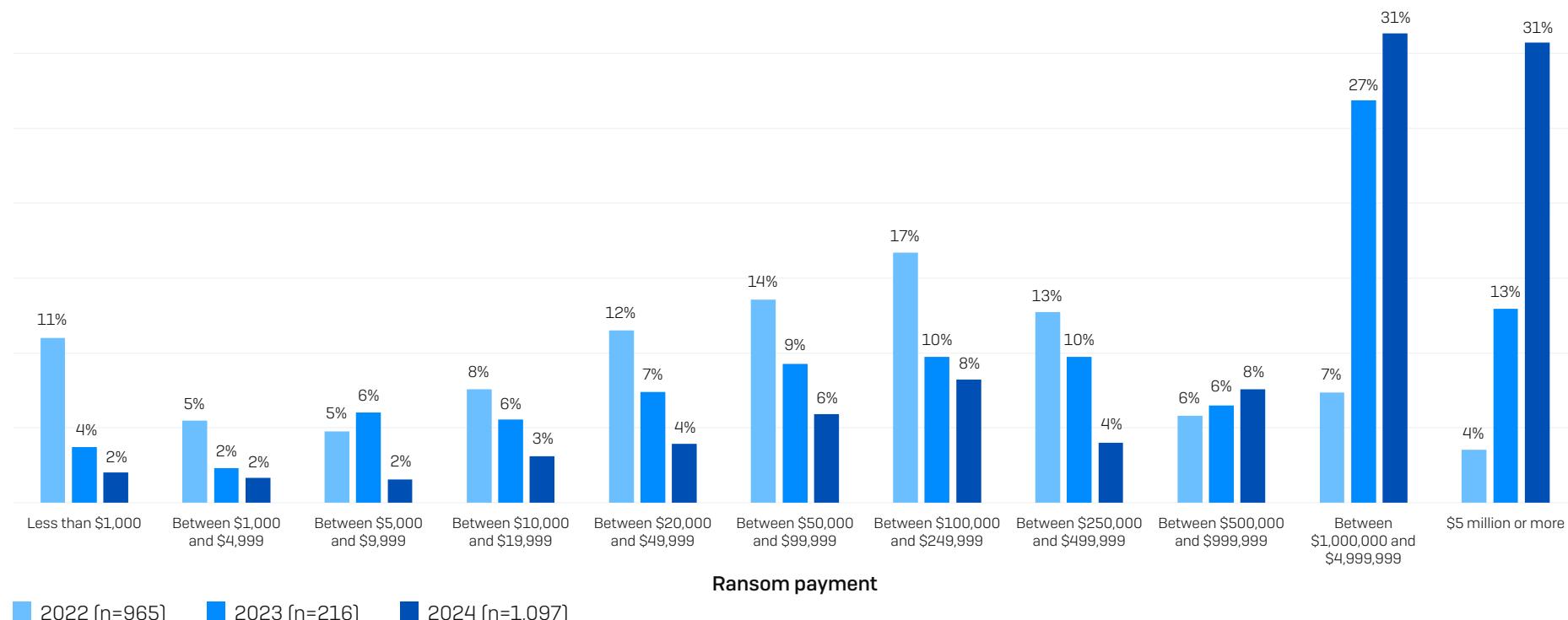
Ransom Payments

1,097 respondents whose organization paid the ransom shared the actual sum paid. Looking at both median and mean averages, we see that ransom payments have increased considerably in the last year:

- Median payment: \$2,000,000 [a 5X increase on the \$400,000 reported in 2023]
- Mean payment: \$3,960,917 [a 2.6X increase on the \$1,542,330 reported in 2023]

The chart below makes clear how the proportion of lower ransom payments has steadily decreased over the last three years, while the proportion of very high payments has soared. Paying a seven-figure or more ransom sum is now the norm.

Distribution of ransom payments 2022-24



How much was the ransom payment that was paid to the attackers? Base numbers in chart.

Ransom Payments by Industry

Just as average ransom demands vary considerably by industry, so too do the ransom payments. *IT, technology and telecoms* reported the lowest median ransom payment (\$300,000), followed by *distribution and transport* (\$440,000). At the other end of the scale, both *lower education* and *central/federal government* paid median ransoms of \$6.6M.

While there is a broad correlation between lower demands and lower payments (and vice versa), there are exceptions – notably *distribution and transport*, whose median ransom demand was north of \$2.8M but paid, on average, \$440,000.

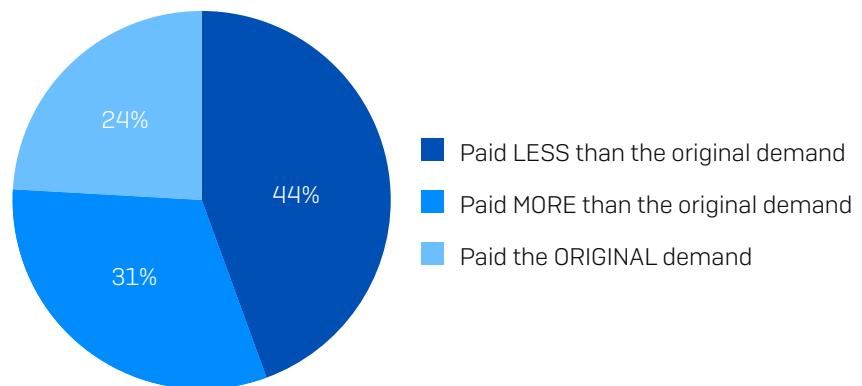
See the appendix for a detailed breakdown of average ransom payment by industry.

Ransom Demand vs. Ransom Payment

When data has been encrypted, it is an incredibly high-pressure time for everyone involved, with both sides trying to optimize their outcomes. Organizations whose data has been encrypted look to minimize the financial impact, while adversaries attempt to secure as much money as possible in the shortest possible timeframe, often using the threat that the ransom will increase if payment is not made by a certain time to pile on further pressure.

Propensity to Negotiate Ransom Amounts

The study has revealed that victims rarely pay the initial sum demanded by the attackers, with only 24% of respondents saying that their payment matched the original request. 44% paid less than the original demand, while 31% paid more.



How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? n=1,097.

Looking at the data by industry, we see that the two services sectors – *business and professional services* and *financial services* – are most likely to negotiate down the ransom payment, with 67% saying that they paid less than the original demand. *Manufacturing and production* is close behind with 65% of organizations paying less than the initial ask.

Conversely, the sectors most likely to pay more than the original demand are those with a high proportion of public sector organizations:

- *Higher education* is most likely to pay more than the original demand [67% paid more], and least likely to pay less than the original demand [20% paid less]
- *Healthcare* was second most likely to pay more than the original demand [57% paid more], followed by *lower education* [55% paid more]

It may be that these industries are less able to access professional ransom negotiators to help reduce their costs. They may also have a greater need to recover the data "at any cost" due to their public remit. Either way, it's clear that there is room for movement between the original demand and the eventual payment.

See the appendix for a detailed breakdown of ransom demand vs. ransom payment by industry.

Proportion of Ransom Demand Paid

While negotiation on the ransom amount occurs in the majority of cases, the eventual movement is relatively small with respondents reporting that 94% of the original demand was paid, on average, across the full cohort.

Diving deeper, we see that all revenue groups except the very largest were able to reduce the size of the ransom payment. The \$50M-\$250M segment paid the lowest proportion of the initial demand (84%). The only group to pay more than the initial ask is the \$5B+ segment which covered, on average, 115% of the ransom demand.

	ANNUAL REVENUE					
Cohort	\$10M - \$50M (n=100)	\$50M - \$250M (n=206)	\$250M - \$500M (n=104)	\$500M - \$1B (n=175)	\$1B - \$5B (n=233)	\$5B + (n=275)
Proportion of ransom demand paid	93%	84%	90%	88%	85%	115%

How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? n=1,097. Note: the 'less than \$10M' cohort is excluded from the annual revenue breakdown due to very low response base.

Proportion of Ransom Demand Paid by Industry

At an industry level, we see that the sectors most likely to negotiate down the ransom amount also pay the lowest percentage of the initial ask – and vice versa.

LESS THAN 100%	MORE THAN 100%
Manufacturing and production (70%)	Higher education (122%)
Business and professional services (74%)	Lower education (115%)
Financial services (75%)	Healthcare (111%)
Other (79%)	State/local government (104%)
IT, telecoms and technology (82%)	Central/federal government (103%)
Retail (84%)	Energy, oil/gas and utilities (101%)
Construction and property (95%)	
Distribution and transport (95%)	
Media, leisure and entertainment (95%)	

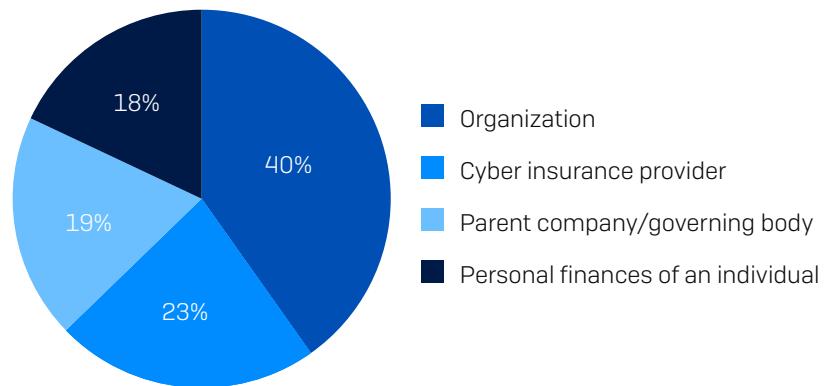
How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? n=1,097.

Source of Ransom Funding

Who provides the money for the ransom is an area of considerable interest, and the study has revealed a number of insights in this area:

- Funding the ransom is a collaborative effort, with respondents reporting multiple sources of monies in more than four-fifths [82%] of cases
- The primary source of ransom funding is the organization itself, covering 40% of the payment on average; the organization's parent company and/or governing body typically provides 19%
- Insurance providers are heavily involved in ransom payments
 - 23% of all ransom payment funding comes from insurance providers
 - Insurance providers contribute toward the ransom in 83% of attacks
 - However, providers very rarely [1%] cover the full amount and in 79% of cases, the insurer funded less than half of the total payment

Source of ransom payment funding



From which of the following source(s) was the money to fund the ransom payment obtained? n=1,168.

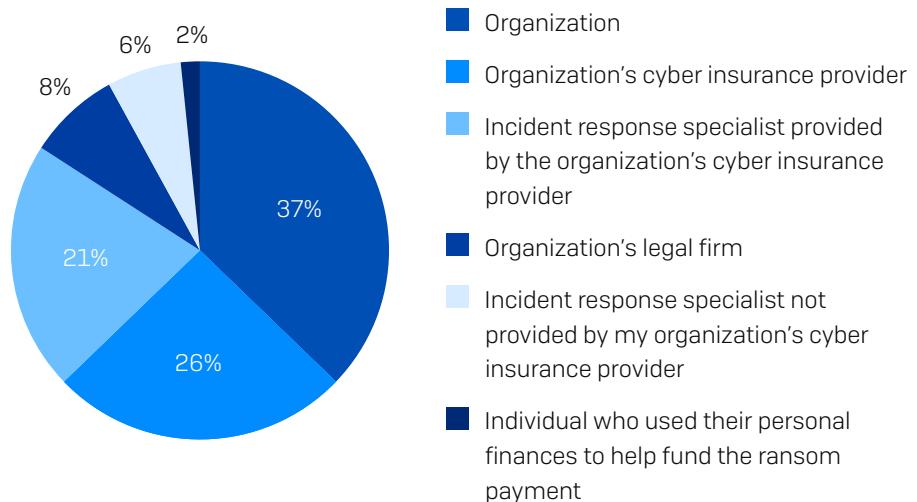
Ransom Transaction Execution

While multiple bodies can contribute to the ransom, funds are typically transferred in a single payment by one party.

Globally, insurance providers transferred the funds for almost half of ransom payments, either directly [26%] or through their appointed incident response specialist [21%]. The victim organization made 37% of payments, while 8% were executed by the victim's legal firm.

Overall, 28% (with rounding) of transfers were made by incident response specialists, whether appointed by the insurance provider [21%] or another party, typically the victim [6%].

Executor of ransom payment transfer



Who made the ransom payment transaction i.e., who transferred the money to the attacker's account? n=1,168.

Recovery Costs

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024, organizations reported a mean cost to recover from a ransomware attack of \$2.73M, an increase of almost \$1M from the \$1.82M reported in 2023.

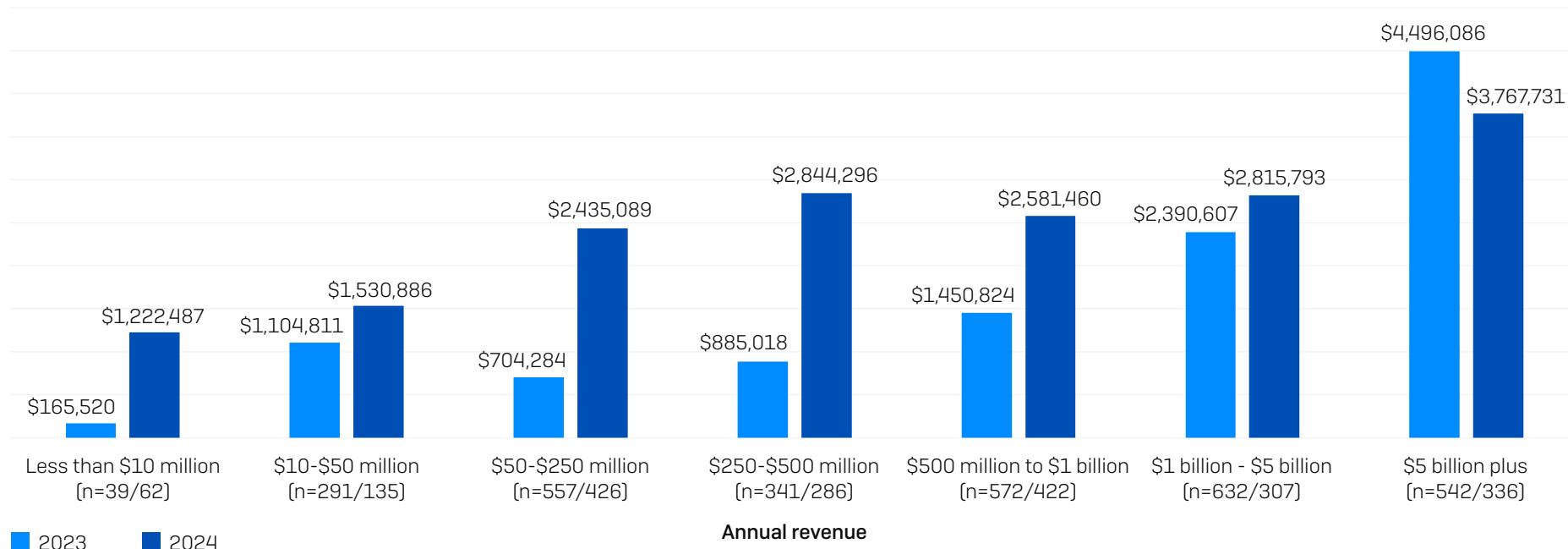
2021	2022	2023	2024
\$1.85M	\$1.4M	\$1.82M	\$2.73M

What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack [considering downtime, people time, device cost, network cost, lost opportunity etc.]? n=2,974 [2024]/ 1,974 [2023]/ 3,702 [2022]/ 2,006 [2021]. N.B. 2022 and 2021 question wording also included "ransom payment".

The greatest increase in overall recovery costs was experienced by the lower and mid-revenue segments, with the \$250M-\$500M cohort reporting the biggest individual increase of \$2M (from \$885,018 to \$2,885,296).

Organizations with \$1B-\$5B revenue reported a (relatively) small increase of just over \$400,000, while the largest organizations with \$5B+ annual revenue were the only cohort to experience a reduction in recovery cost, down from \$4,496,096 to \$3,767,731.

Looking at the median recovery cost data confirms the trends. Globally, median recovery costs doubled from \$375,000 to \$750,000 over the last year. Increases were mostly concentrated in the five lower revenue cohorts who all reported a considerable increase in costs, while remaining relatively flat for the two larger.



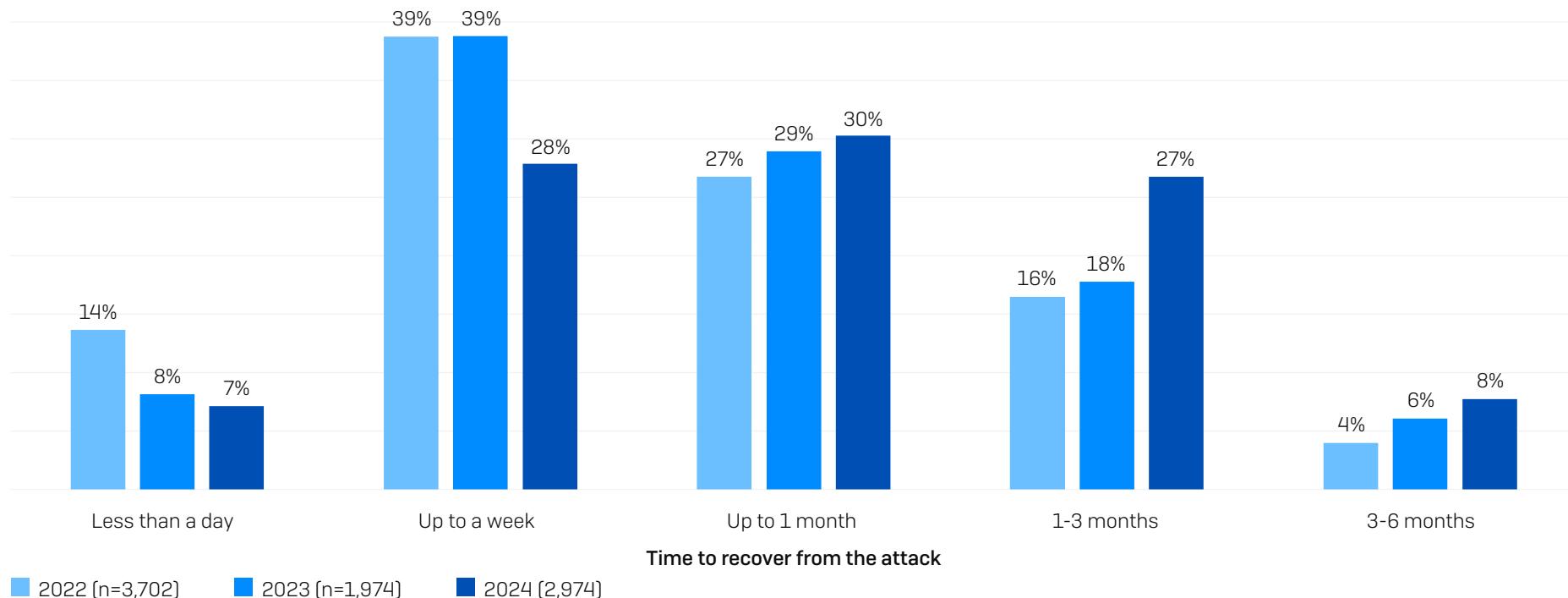
What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack [considering downtime, people time, device cost, network cost, lost opportunity etc.]? n=2,974 [2024], 1,974 [2023]. 2024/2023 base numbers by revenue in chart.

Recovery Time

The time taken to recover from a ransomware attack is getting steadily longer. Our 2024 research revealed:

- 35% of ransomware victims are fully recovered in a week or less, down from 47% in 2023 and 52% in 2022
- One third [34%] now take more than a month to recover, up from 24% in 2023 and 20% in 2022

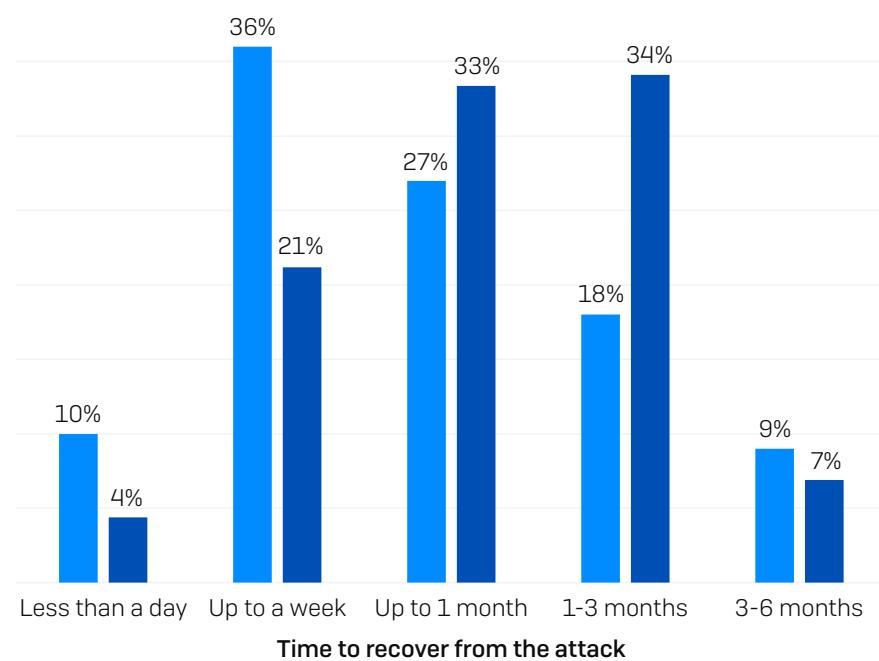
This slowdown may reflect the increased complexity and severity of attacks, necessitating greater recovery work. It may also indicate a growing lack of recovery preparation.



How long did it take your organization to fully recover from the ransomware attack? Base number in chart.

Recovery Time: Impact of Backup Compromise

Having your backups compromised has a major impact on overall recovery time. Almost half of organizations whose backups are not compromised recover in a week or less (46%), compared to a quarter (25%) of those whose backups are affected. Having your backups compromised both increases the complexity of recovering encrypted data while adding the overhead of creating and securing new, untainted backups.



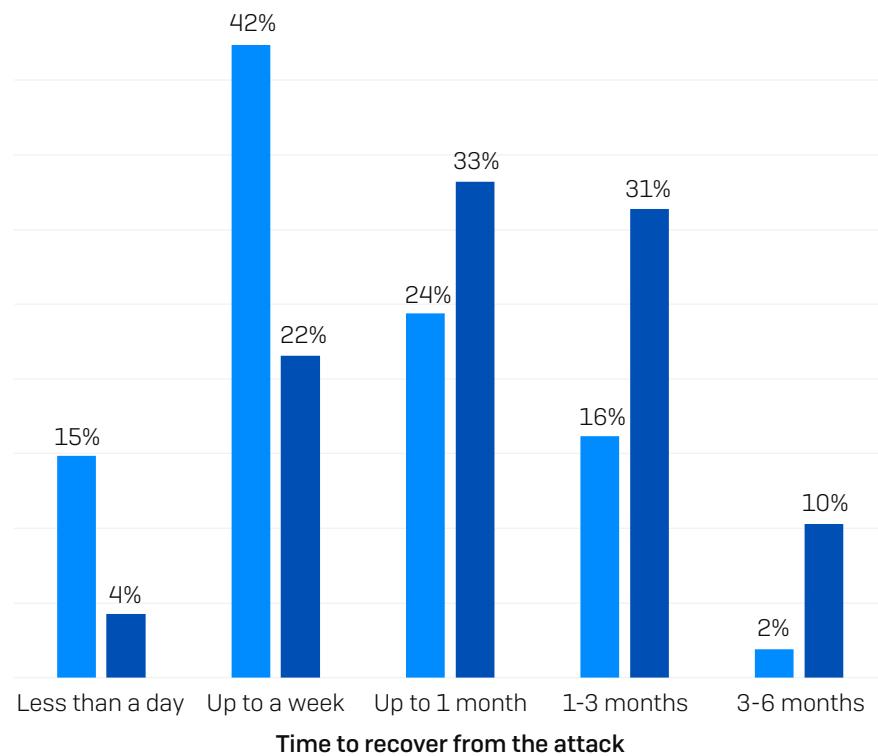
■ Backups not compromised [n=1,379]

■ Backups compromised [n=1,595]

How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart.

Recovery Time: Impact of Data Encryption

It is likely no surprise that having data encrypted in an attack significantly increases recovery time. 57% of those who didn't have data encrypted were fully recovered within a week, compared to 25% of those whose data was encrypted.



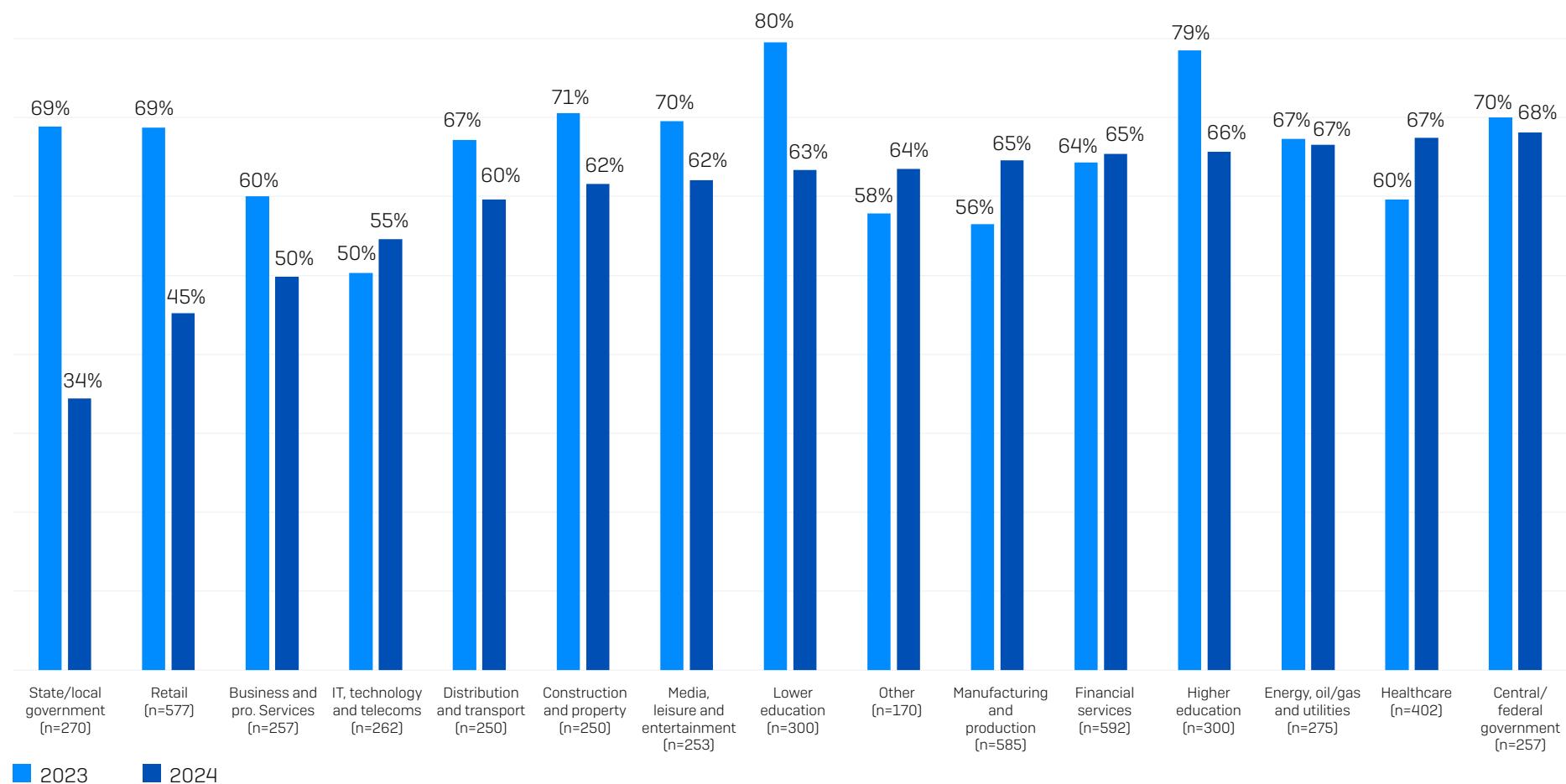
■ Data not encrypted [n=902]

■ Data encrypted [n=2,072]

How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart.

Rate of Ransomware Attacks by Industry

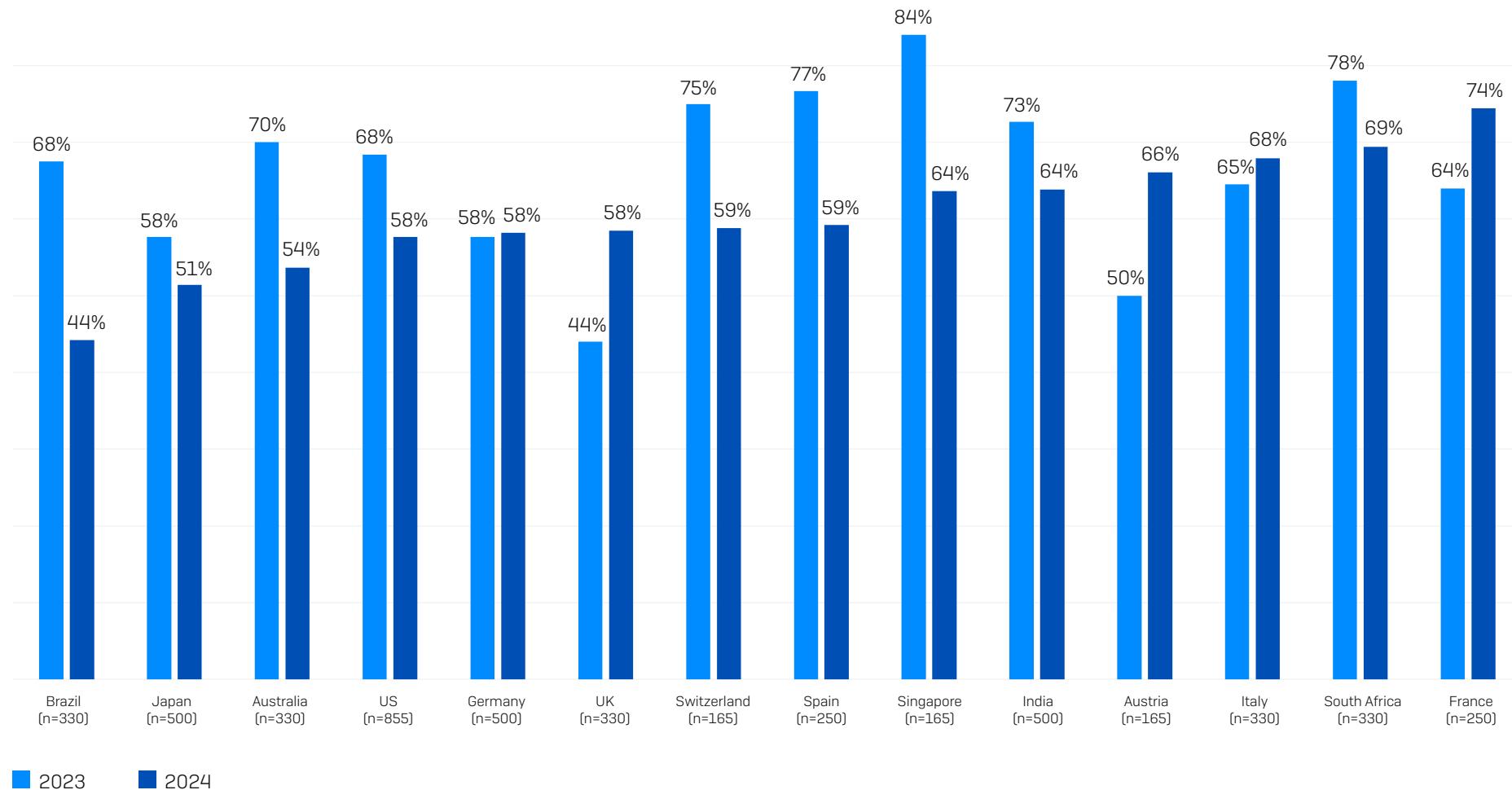
Percentage of organizations hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? Yes. n=5,000 (2004) n=3,000 (2023), 5,600 (2022). 2024 industry base numbers in chart.

Rate of Ransomwares Attack by Country

Percentage of organizations hit by ransomware in the last year

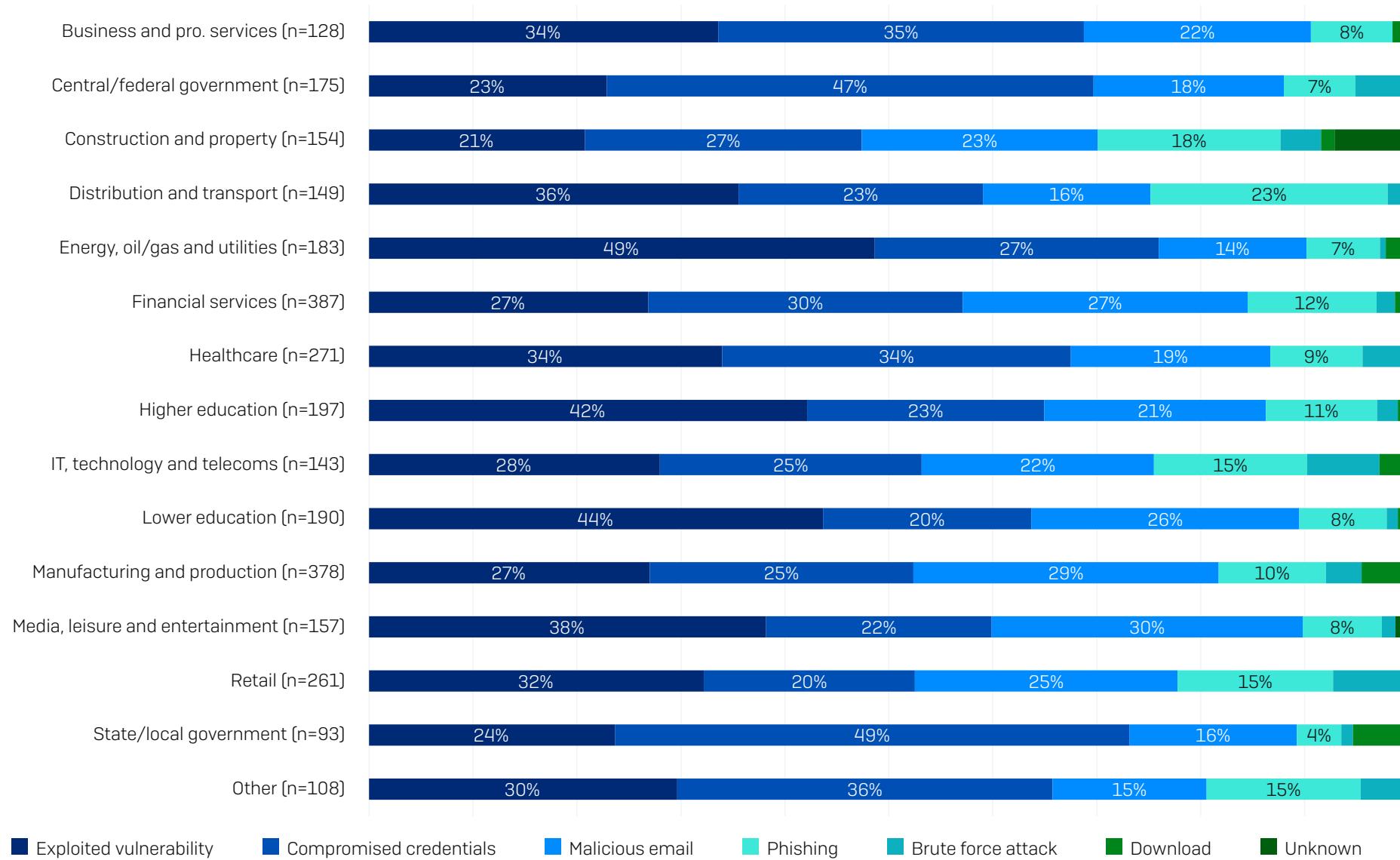


2023

2024

In the last year, has your organization been hit by ransomware? Yes. n=5,000 (2004) n=3,000 (2023). 2024 country base numbers in chart.

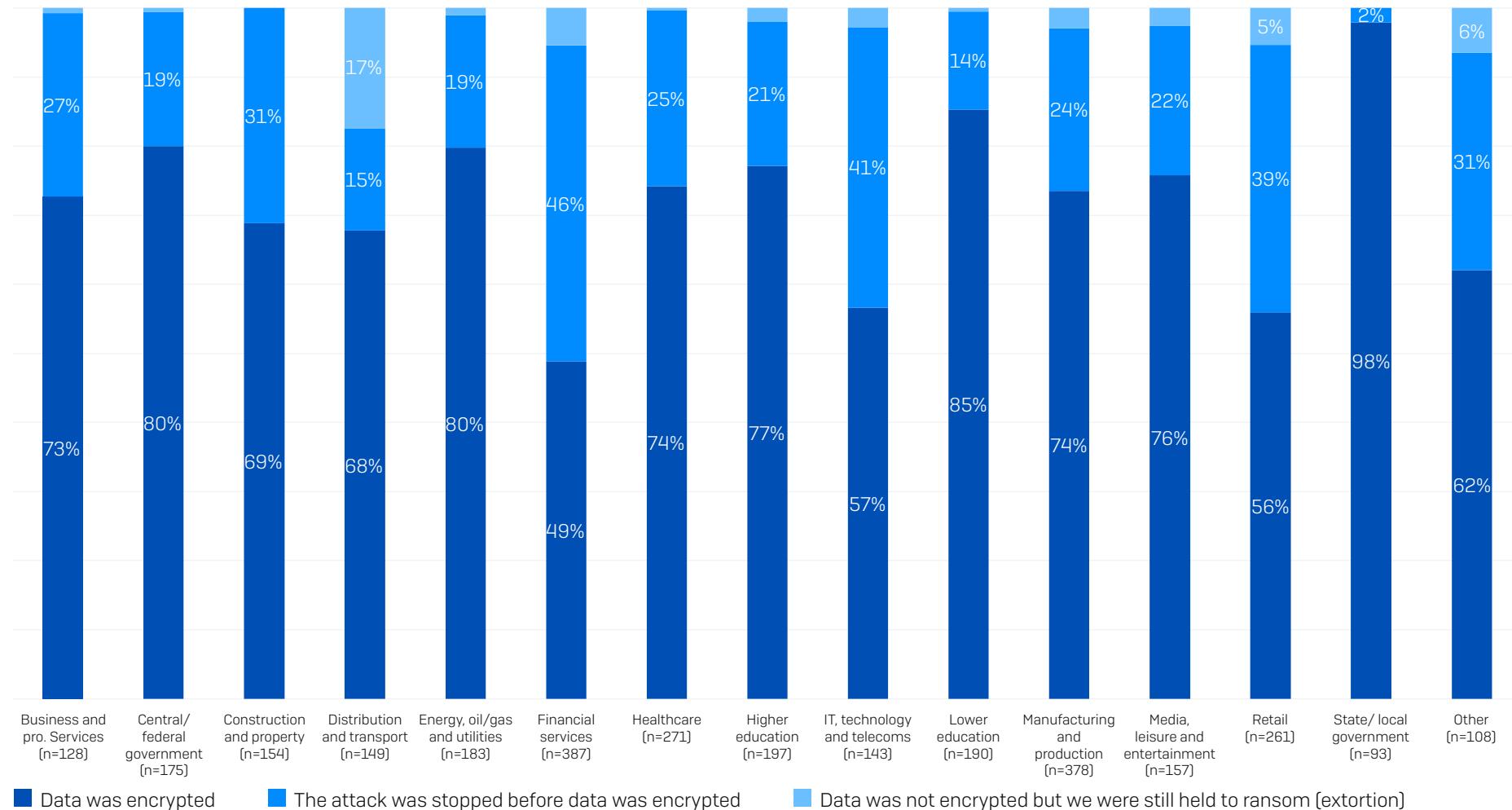
Root Cause of Attack by Industry



Do you know the root cause of the ransomware attack your organization experienced in the last year? n=2,974 organizations hit by ransomware.

Data Encryption Rate by Industry

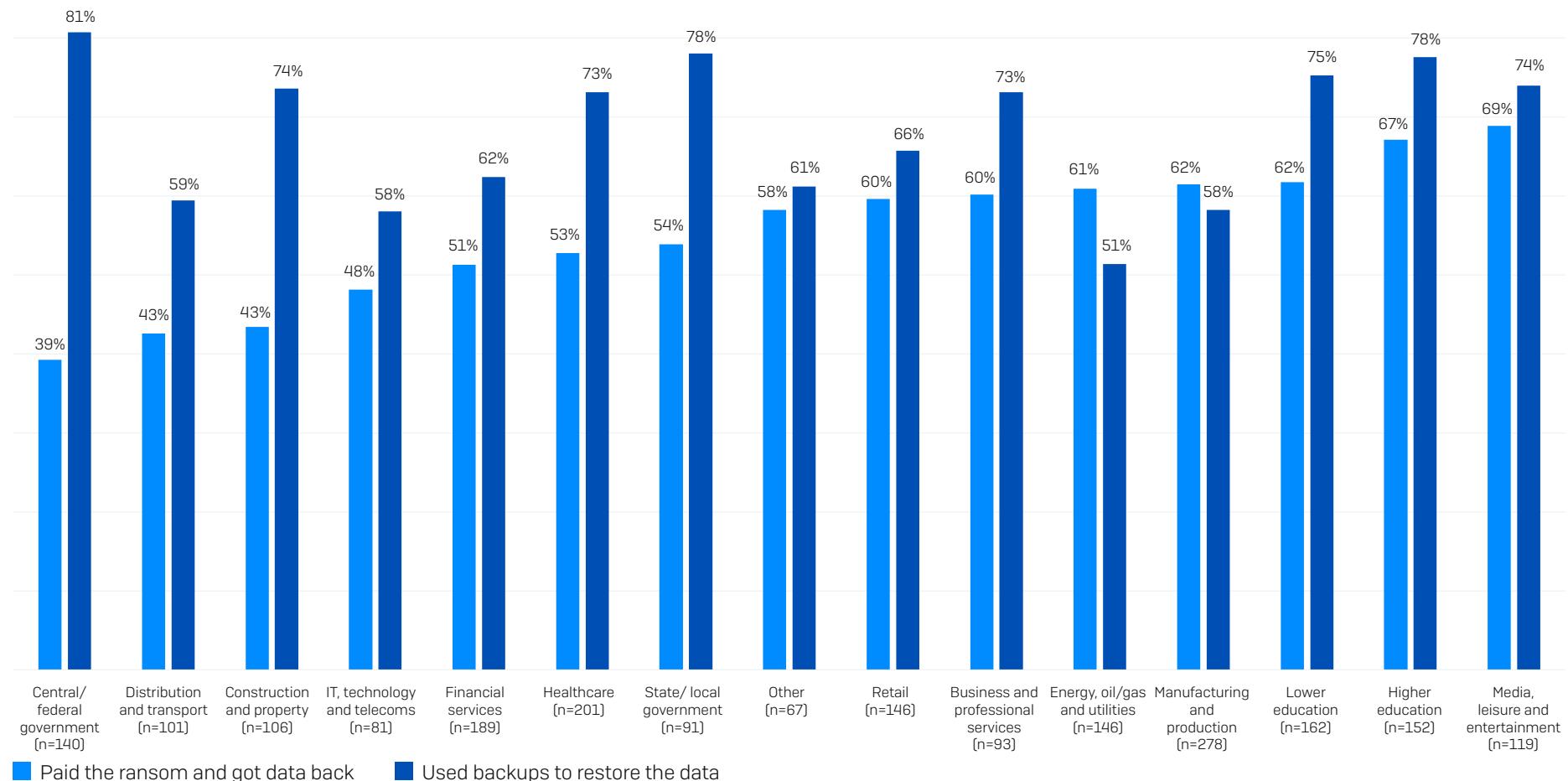
Propensity to have data encrypted in an attack



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base number in chart.

Data Recovery Method by Industry

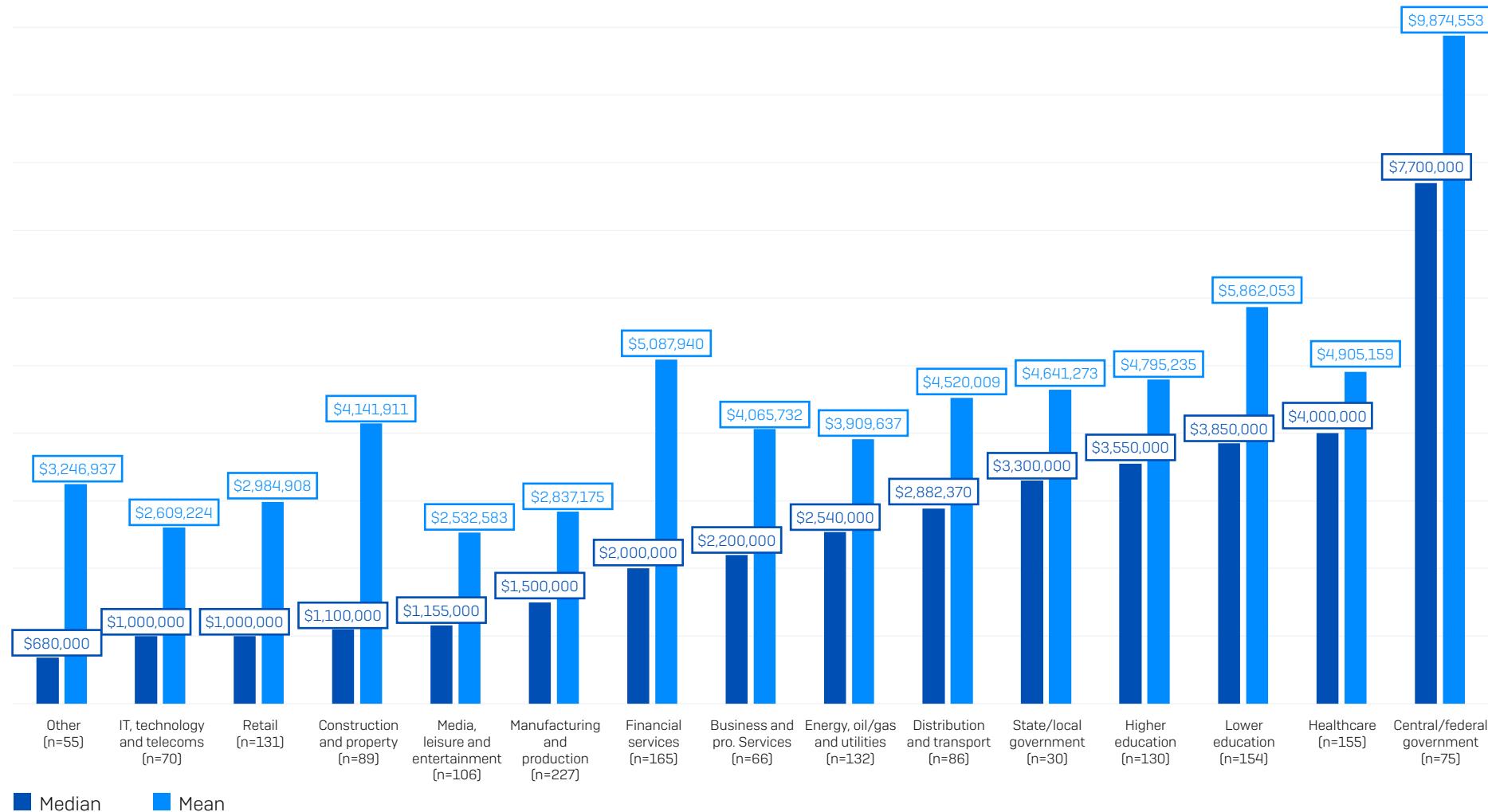
How often data is recovered by using backups and paying the ransom



Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. Base numbers in chart. Ordered by propensity to pay the ransom.

Ransom Demand by Industry

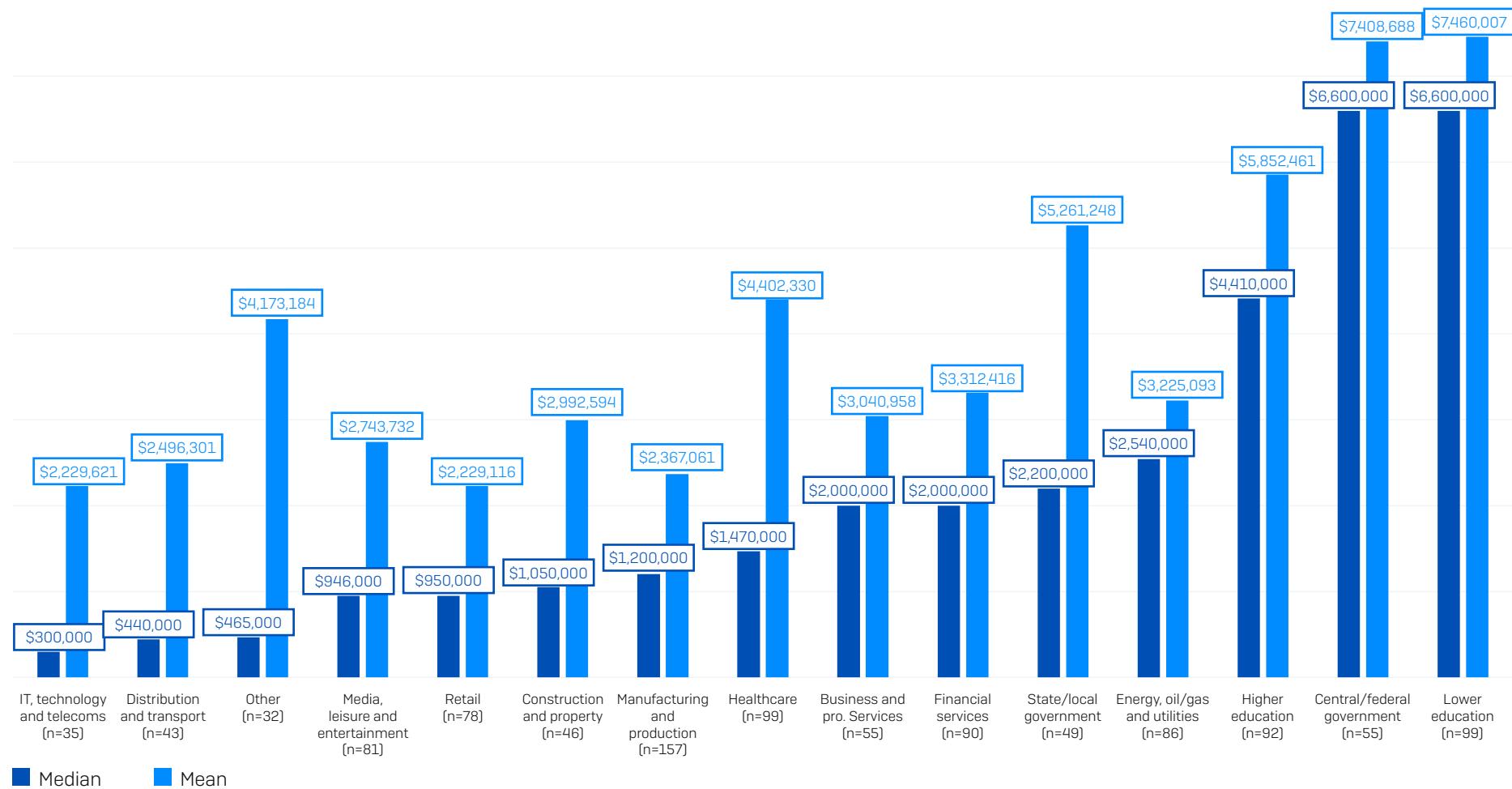
Ransom demand



How much was the ransom demand from the attacker(s)? Base numbers in chart. Ordered by median demand.

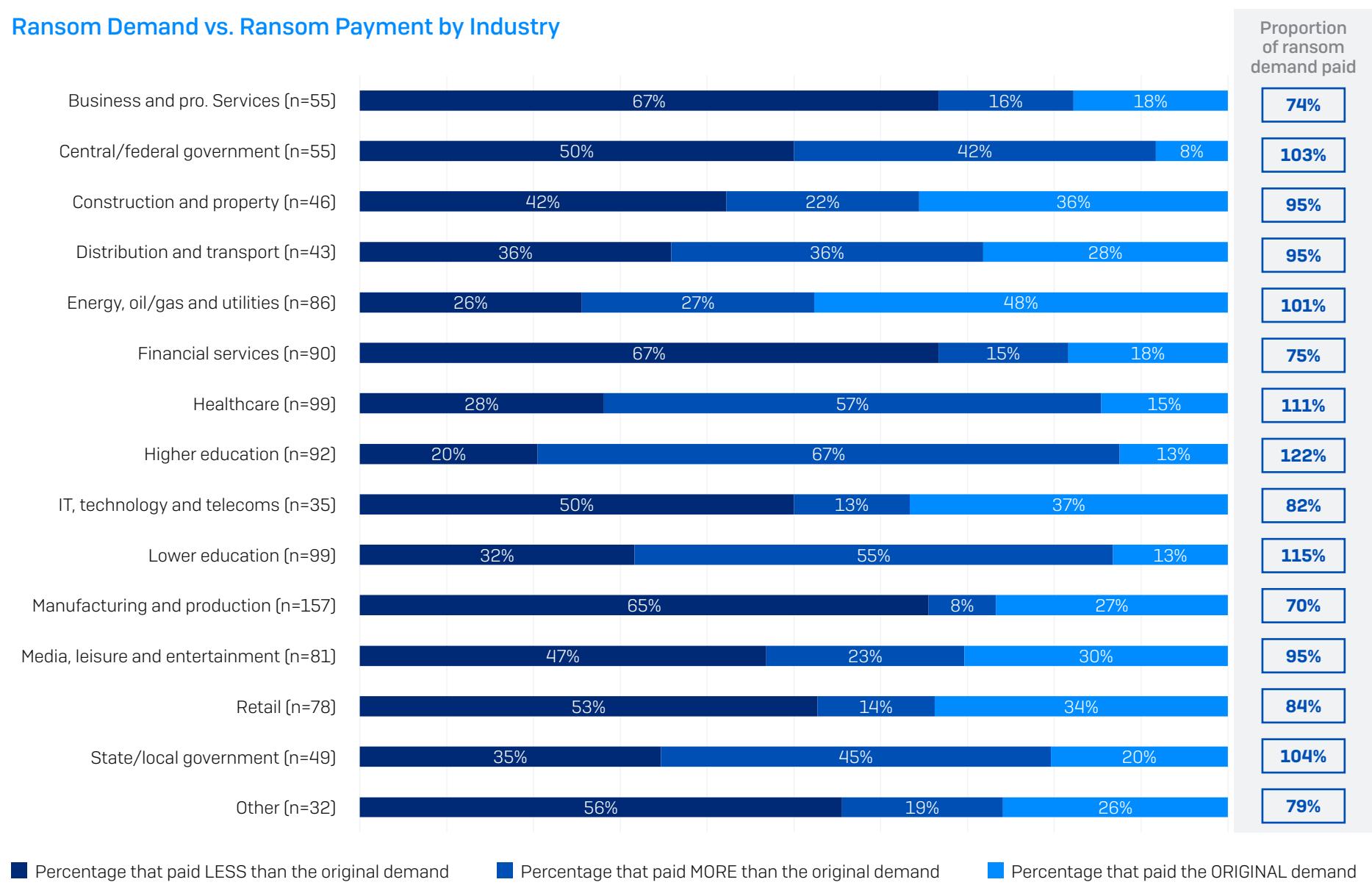
Ransom Payment by Industry

Ransom payment



How much was the ransom payment that was paid to the attackers? Base numbers in chart. Data ordered by median payment.

Ransom Demand vs. Ransom Payment by Industry



■ Percentage that paid LESS than the original demand

■ Percentage that paid MORE than the original demand

■ Percentage that paid the ORIGINAL demand

How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? Base numbers in chart.



BRAZIL THREAT LANDSCAPE REPORT

“Unmasking Stealer Malware Dominance
in Brazil”



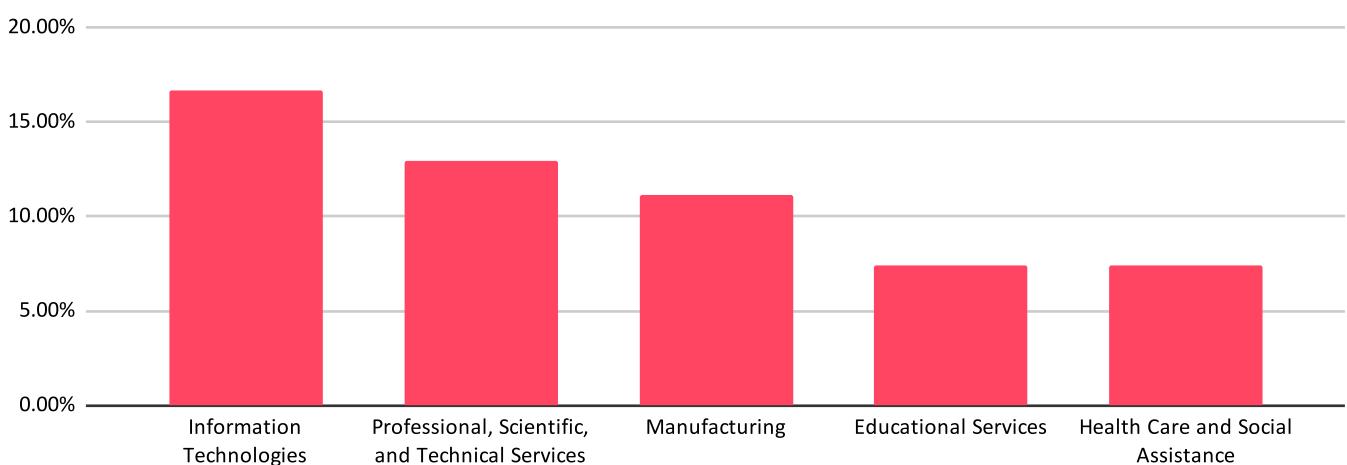
socradar.io

Analyzing Ransomware Threat Landscape of Brazilian Organizations

Industries Under Siege

Turning our attention to the most recent year from June 2022 to May 2023, we highlight the industries most often mentioned in these ransomware posts. Information Technologies was most frequently targeted, making up 16.7% of all posts. The Professional, Scientific, and Technical Services followed closely at 13.0%, with Manufacturing at 11.1%. Educational Services and Health Care and Social Assistance were not spared either, each constituting 7.4% of the posts.

Top Industries Targeted by Ransomware

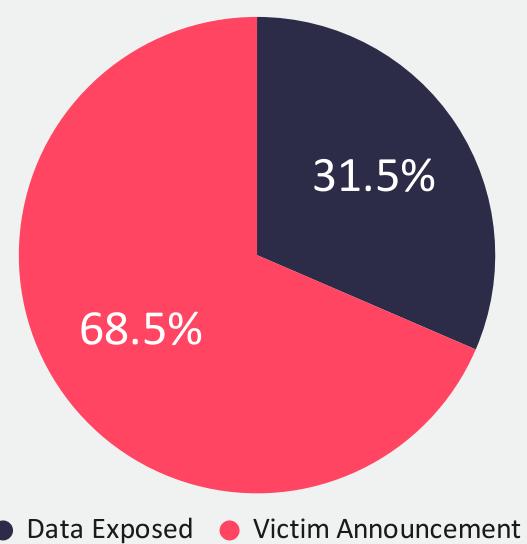


Categorizing Ransomware Posts

Last, we categorize the ransomware posts from the past year by their type. The majority of the posts, 68.5%, were Victim Announcements, while Data Exposed posts constituted 31.5%. This suggests a focus on broadcasting attacks and identifying victims over sharing sensitive compromised data.

This analysis gives a thorough understanding of the ransomware threat landscape in Brazilian organizations, helping them design robust defense strategies against such attacks.

Share Types of Ransomware Blogs



Osterman Research

WHITE PAPER

White Paper by Osterman Research

Published **March 2021**

Sponsored by **Trend Micro**

How to Reduce the Risk of Phishing and Ransomware

Executive Summary

Cybersecurity challenges abound for organizations across the world. The tsunami of phishing attacks that threaten account compromise, data breaches and malware infection remains a critical threat to neutralize. Ransomware is a second critical threat, with a well-played ransomware attack capable of bringing an organization to a complete halt, and in some cases putting it out of business permanently (e.g., Travelex¹ and Vastaamo²). Both phishing and ransomware were critical threats before the health pandemic of 2020 forced a sudden shift to remote working, and such a move has only served to intensify the threat levels. The Global Risks Report 2021, a recently released publication from the World Economic Forum, ranks information security as the top technology objective that has become a greater priority due to COVID, noting that it is complex, there is a skills shortage, and cybercriminals are difficult to track, among others.³

This white paper and the survey commissioned for this research looks specifically at the threats of phishing and ransomware, and how the risks of both can be reduced.

KEY TAKEAWAYS

Osterman Research conducted an in-depth survey of security-focused professionals specifically for this white paper. Here are the key takeaways from the research:

- Half of organizations believe they are effective at counteracting various phishing and ransomware threats. Of the 17 threat types we asked about in the survey, 37% of organizations believed they were highly effective at counteracting 11 or more of the threat types.
- Only 16% of organizations reported no security incident types related to phishing and ransomware in the past 12 months. In other words, it is a widespread problem for most organizations.
- Respondents indicated only mid-range confidence in the ability of various groups of employees to recognize phishing attempts through email and other channels. Confidence levels in the ability to recognize ransomware attacks were lower still.
- The most effective mitigations against phishing attacks, from our research, are multi-factor authentication, security awareness training, and the ability to remove phishing messages from employees' mailboxes. For ransomware, it is multi-factor authentication, rapid patching of vulnerabilities, and security awareness training.
- Best practices to reduce the risk of phishing and ransomware include focusing on significant root causes, not waiting to start, and making it harder for yourself.

Phishing and ransomware were already critical threats before the health pandemic forced a sudden shift to remote working.

ABOUT THIS WHITE PAPER

This white paper is sponsored by Trend Micro. Information about Trend Micro is provided at the end of the paper. This paper references data from an in-depth survey of 130 cybersecurity professionals in mid-sized and large organizations that was conducted specifically for this paper.

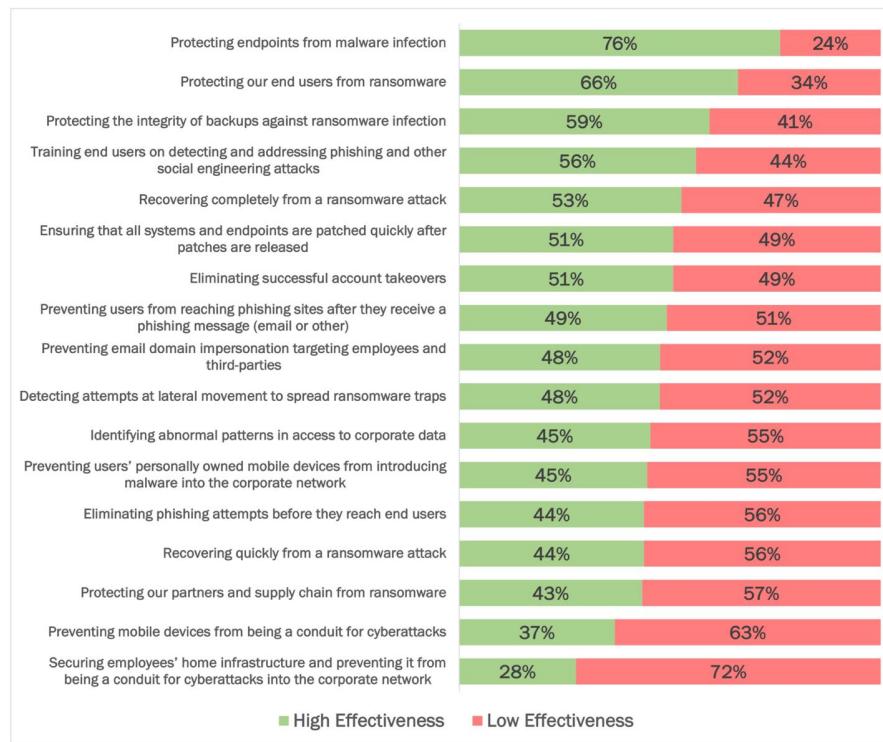
Current Threat Landscape

This section looks at the threats facing organizations today. It reports the data from the organizations surveyed for this report, along with the wider threat context.

HIGH AND LOW EFFECTIVENESS AGAINST THREATS

Whatever the threat type, low effectiveness at counteracting the potential effects makes an organization more susceptible to being hit hard. For the organizations we surveyed for this report, many believe they are highly effective at counteracting some threats related to phishing and ransomware, but not very effective at counteracting others. As a general conclusion, half of all organizations are not effective at counteracting phishing and ransomware threats. See Figure 1.

Figure 1
Organizational Effectiveness Against Various Phishing and Ransomware Threats
 Percentage of Respondents



Only 37% of organizations believed they were highly effective at counteracting 11 or more of the phishing and ransomware threats.

Source: Osterman Research (2021)

Another way of looking at the data, however, is to look for a pattern of effectiveness against the 17 threat types at individual organizations. The question becomes whether an organization effective against one type of threat is more likely to be effective against the others as well. The survey data showed that:

- 37% of organizations believed they were highly effective at counteracting 11 or more of the phishing and ransomware threats.
- 63% of organizations believed they were highly effective at counteracting 10 or fewer of the threats.

INCIDENTS FROM THE PAST 12 MONTHS

Almost 85% of the organizations surveyed have experienced one or more of 17 types of security incidents in the past 12 months. Just over half of the organizations surveyed have experienced between one and three types of incidents. Just under a third have experienced four or more types. Only 16% of organizations have reported no security incident types related to phishing and ransomware in the past 12 months. The three most commonly occurring type of security incidents are business email compromise (BEC) attacks that successfully tricked lower-level employees (53%), phishing messages that result in a malware infection (49%), and phishing messages that result in an account compromise (47%). See Figure 2.

Figure 2

Types of Security Incidents That Have Occurred During the Previous 12 Months
Percentage of Respondents

Type of Security Incident	%
A business email compromise attack was successful in tricking at least one lower-level employee within our company	53%
A phishing message has resulted in a malware infection	49%
A phishing message has resulted in an account compromise	47%
Your domain has been “spoofed” to perpetrate phishing campaigns	38%
Ransomware was detected in our systems before it activated	34%
A business email compromise attack was successful in tricking at least one senior executive within our company	28%
A phishing message impersonating your domain compromised a third-party	16%
A phishing message has resulted in a ransomware infection	14%
A ransomware attack was successfully launched	10%
A ransomware attack resulted in internal IT systems becoming non-operational	10%
A ransomware attack resulted in unrecoverable data loss	6%
A department or business unit at our organization had to cease operations, at least temporarily, due to a ransomware attack resulting in unrecoverable system and data loss	6%
A ransomware attack resulted in operational technology systems becoming non-operational	4%
Our entire organization had to cease operations, at least temporarily, due to a ransomware attack resulting in unrecoverable systems and data loss	3%
Data was exfiltrated as part of a ransomware attack	2%
Data exfiltrated in a ransomware attack was offered for public sale or auction	1%
Our infrastructure was compromised to host malicious content that threat actors used against other companies and individuals	0%

Source: Osterman Research (2021)

While Figure 2 accurately reports the results from survey respondents, the results are likely to be understated. First, security incidents are embarrassing to an organization generally and IT security professionals personally, hence some incidents may remain unreported. Second, awareness of each type of security incident requires the capability to detect (and mitigate) such incidents, and not all

Only 16% of organizations have reported no security incident types related to phishing and ransomware in the past 12 months.

organizations have the optics to do so. On balance, we believe the rate of security incident types is higher than what is reported in Figure 2.

ISSUES OF HIGH CONCERN TO SECURITY TEAMS

Of the 14 security issues we asked respondents to rate, ten were rated of high concern by more than half of the respondents. Phishing attempts making their way to end users was the top-rated issue of concern (by 65% of respondents), followed closely by employees being unable to spot phishing or social engineering attacks before clicking a link or attachment (by 64% of respondents). The issues in third and fourth place were related to ransomware attacks.

Figure 3

Issues of High Concern to Security Teams

Percentage Responding “Concerned” or “Extremely Concerned”

Security Issue	%
Phishing attempts making their way to end users	65%
Employees failing to spot phishing and social engineering attacks before clicking on a link or attachment	64%
Breaching of corporate data by a ransomware attack	61%
Ransomware attacks successfully infecting endpoints	59%
Our ability to prevent zero-day threats from infecting our systems and applications	56%
Negative effects on our brand reputation after a security incident	54%
Our ability to prevent lower-level employees from falling victim to a business email compromise attack	53%
Our ability to prevent senior executives from falling victim to a business email compromise attack	53%
Our ability to keep all systems and applications patched against current threats	52%
Our ability to recover corporate data and system integrity after a ransomware attack	50%
Our ability to prevent data exfiltration as part of a ransomware attempt	47%
Domain impersonation to perpetrate phishing and BEC campaigns	46%
Our ability to restore normal business operations after a ransomware attack	46%
Our ability to learn from phishing and ransomware attacks to mitigate future attempts	42%

Source: Osterman Research (2021)

In our 2019 report on phishing, business email compromise, account takeovers and other security threats, the same two issues above also rated at the top of the list but were of higher concern in 2019. The level of concern about ransomware, by contrast, has increased over the same time period, reflecting the growing occurrence and threat of ransomware incidents to organizations everywhere.⁴

Phishing attempts making their way to end users was the top-rated issue of concern (by 65% of respondents).

SECURITY SPENDING IN 2020 VS. 2021

There is no perfect way to draw a comparison of security spending across a population of organizations because of differences in industry, business model, organization size, and even the data protection regulations in play in various geographies. However, despite the lack of perfection available, our research showed that security budgets are set to increase in 2021 compared to 2020 at both organizations with less than 1,000 employees and those with more than 1,000 employees. See Figure 8.

Figure 8
Security Budgets per Employee
Average of Respondents



Source: Osterman Research (2021)

Security budgets are increasing in 2021 compared to 2020.

Increased spending is likely to—or should—focus on:

- **Greater Use of Cloud Security Services**

Respondents indicated a preference for higher usage of cloud security services (see Figure 9). Cloud services offer a rapid pathway to elevated security, along with negating the need for many of the administration and maintenance tasks that go with on-premises infrastructure.

- **Improved Security Awareness Training**

With respondents only indicating mid-range confidence in current security awareness training outcomes, elevating the competence of all employee groups to recognize and neutralize phishing and ransomware threats is essential. Refer to Figure 5 and Figure 7.

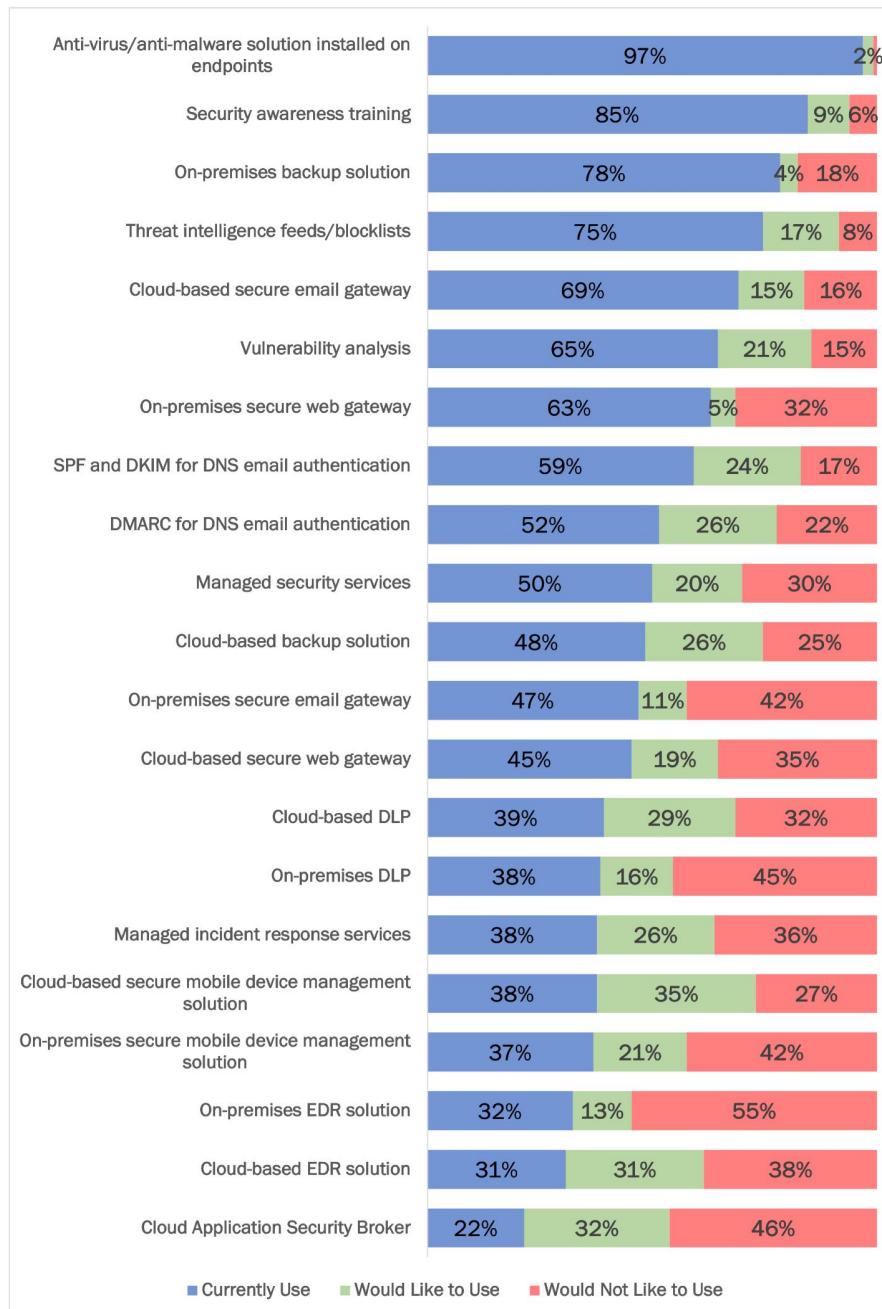
- **General Elevation of Security Solutions**

Improved capabilities for rapidly patching vulnerabilities, and for faster detection of internal phishing threats and external spoofing attacks should be considered, as well as increased adoption of AI (artificial intelligence) and ML (machine learning) in the fight against phishing and ransomware. These are current areas where organizations show weaknesses.

CURRENT AND PREFERRED USAGE OF SECURITY TOOLS

Organizations make use of a variety of security tools to counteract, respond to, and mitigate security threats, and others would like to do so. See Figure 9. Please note that the third value in the chart—"would not like to use"—is a calculated value that attempts to map changing preferences for different types of security tools.

Figure 9
Current and Preferred Usage of Security Tools
 Percentage of Respondents Currently Using or Wishing They Could



*Organizations
make use of a
variety of
security tools to
counteract,
respond to, and
mitigate security
threats, and
others would
like to do so.*

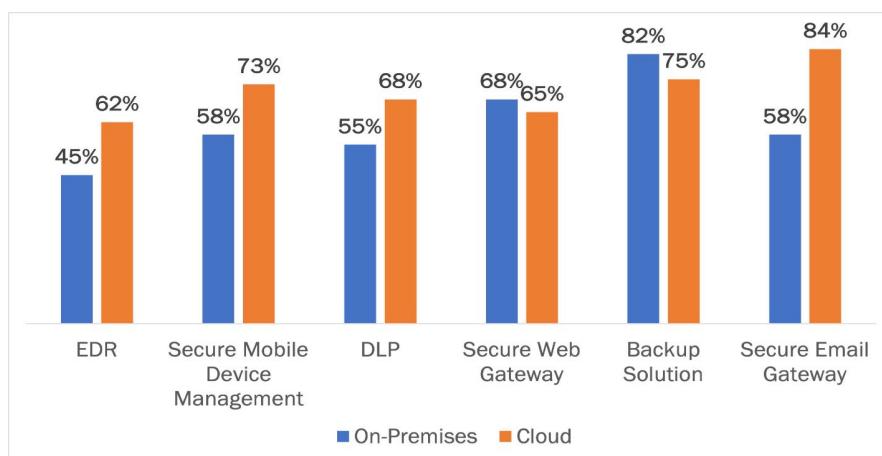
Source: Osterman Research (2021)

In reviewing the current and preferred usage profiles, we note the following:

- Endpoints Both Are and Are Not Protected**
Endpoint protection through anti-virus and anti-malware solutions shows high usage (currently by 97% of respondents), but the use of Endpoint Detection and Response (EDR) is currently at the other end of the spectrum at slightly less than one third for both on-premises and cloud-based approaches. While one can stop and block active threats, the other can seek out threats and vulnerabilities across the entire endpoint estate, irrespective of whether a particular threat has broached a given endpoint.
- Sender Policy Framework (SPF)/DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC) Are Almost Equivalent**
The current and preferred usage of SPF/DKIM and DMARC for email authentication are almost the same, although DMARC trails slightly. Usage of the three is moving closer together, at it should, since the three work in lockstep. Clearly there is a difference between using DMARC with a policy of none and a policy of reject, a nuance we did not query in this research.
- Growing Appetite for Managed Services**
One half of respondents currently use managed security services, and two fifths use managed incident response services. Once the preference to use both is added to this base score, the variation between the two is negligible, at 70% for managed security and 63% for managed incident response services.
- Growing Preference for Cloud Security Services**
Respondents have a greater preference for using cloud security services than on-premises security tools for four of the six tools (see Figure 10). EDR, secure mobile device management, Data Loss Prevention (DLP) and secure email gateway all received a higher aggregate score for cloud-based usage for both current and preferred usage than on-premises versions of the same. Respondents currently have a higher preference for on-premises secure web gateway compared to cloud-based (although there is not much difference), and for on-premises backup.

Respondents have a greater preference for using cloud security services than on-premises security tools for four of the six tools.

Figure 10
On-Premises vs. Cloud-Based Security Tools
Percentage of Respondents Currently Using and Wishing They Could



Source: Osterman Research (2021)

EFFECTIVE PHISHING MITIGATIONS

Respondents indicated the phishing mitigations they found most effective, with four mitigations ranked as mostly or highly effective by more than half of the respondents. See Figure 16. The three mitigations with the highest ratings were:

- **Multi-Factor Authentication (74%)**

Multi-factor authentication (MFA) to reduce the ease of stealing usable credentials was ranked as the most effective mitigation by 74% of respondents in our research. When MFA is in use, even if a victim enters their credentials for the cybercriminal to harvest, the presence of the MFA demand renders usage of the compromised credentials much more difficult. While phishing may still result in compromised credentials, MFA reduces the consequential impact.

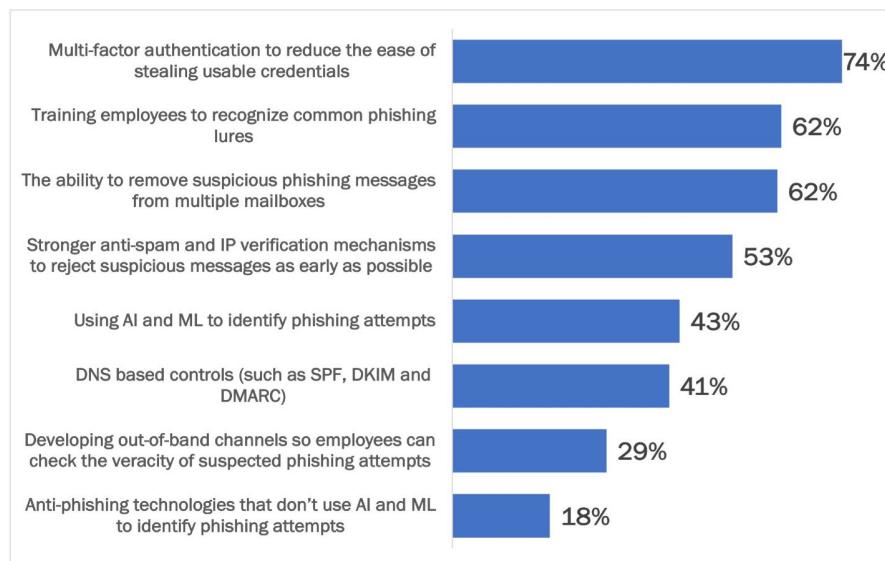
- **Security Awareness Training (62%)**

Training employees to recognize common phishing lures was the mitigation with the second highest effectiveness rating, by just over 62% of respondents. When people have the ability to discern when something about a message doesn't seem quite right, or to recognize common phishing attack patterns, a successful phishing attack is harder to execute.

- **Removal of Phishing Messages from Mailboxes (62%)**

The ability to remove suspicious phishing messages from multiple mailboxes was the third highest ranked mitigation, by just under 62% of respondents. When the first few instances of a phishing message are activated or questioned—which happens within minutes of the message being delivered—the ability to remove every other copy of the message decreases the available threat space.

Figure 16
Effectiveness of Phishing Mitigations
Percentage Responding "Mostly Effective" or "Highly Effective"



Source: Osterman Research (2021)

The ranking of the two options for AI and ML in identifying phishing attempts is interesting. Anti-phishing technologies that do use AI/ML were ranked as being almost two-and-a-half times more effective than technologies not using AI/ML.

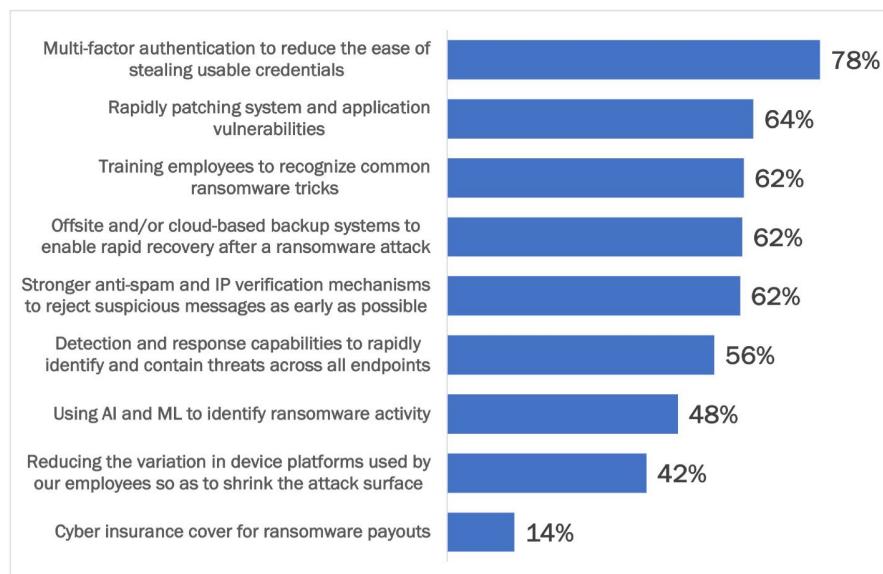
Multi-factor authentication (MFA) to reduce the ease of stealing usable credentials was ranked as the most effective mitigation by 74% of respondents in our research.

EFFECTIVE RANSOMWARE MITIGATIONS

Respondents found a range of mitigations to be more effective than others in addressing the risks of ransomware (Figure 17). The top-ranked mitigations were:

- **Multi-Factor Authentication (78%) and Security Awareness Training (62%)**
MFA and security awareness training ranked in first and third place respectively. These were also ranked highly for phishing mitigations.
- **Rapid Patching of Vulnerabilities (64%)**
Software and application vulnerabilities are often targeted by ransomware operators, as they offer a foothold into a device or network. Rapid patching reduces the undefended areas, decreasing the likelihood of attack susceptibility. Respondents ranked rapid patching as the second most effective mitigation in decreasing the risks of ransomware.
- **Offsite or Cloud Backup (62%)**
Offsite or cloud backup services provide the ability to recover data encrypted by a ransomware attack and thus assure operational continuity. Backups must be protected from ransomware infection. While backups can restore data, they can do nothing about the extortion element of modern ransomware attacks.
- **Stronger Anti-Spam and IP Verification Mechanisms (62%)**
Anti-spam and IP verification mechanisms aim to eliminate suspicious messages from reaching end users, by sanitizing the inbound message flow.

Figure 17
Effectiveness of Ransomware Mitigations
Percentage Responding “Mostly Effective” or “Highly Effective”



Source: Osterman Research (2021)

Cyber insurance cover was ranked effective by the fewest number of respondents (14%). Such cover can provide an immediate resolution to an incident, but the money spent on cyber insurance doesn't directly elevate the security posture of an organization. Other mitigations in addressing ransomware present their own form of insurance (risk reduction), which can greatly reduce the likelihood of an impactful incident, and thus the extent of cyber insurance coverage required.

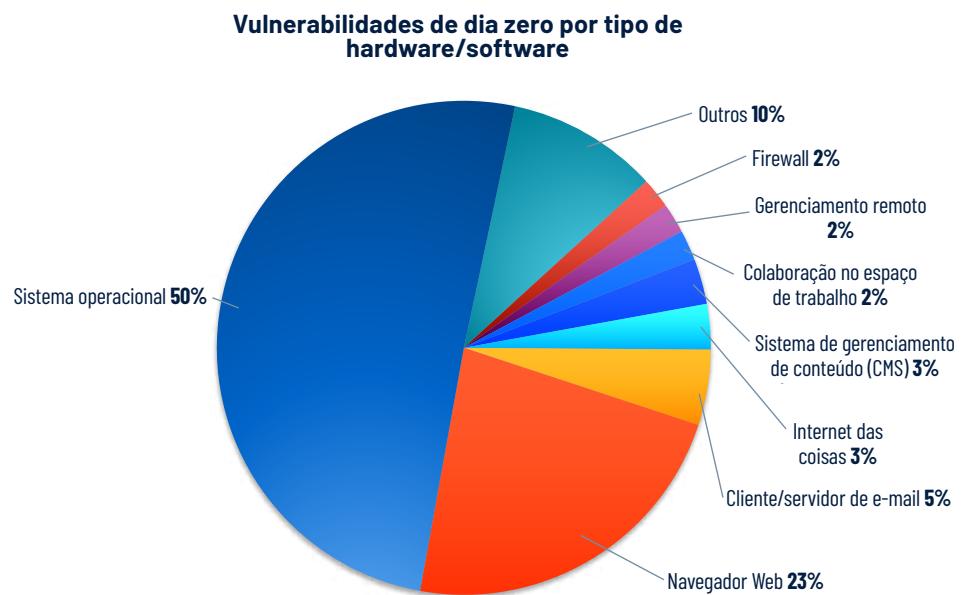
Rapid patching reduces the undefended areas of devices and networks, decreasing the likelihood of attack susceptibility.



RELATÓRIO DO CENÁRIO DE AMEAÇAS DE 2022 DA TENABLE

Um guia de navegação pela superfície de ataque
moderna para profissionais de segurança



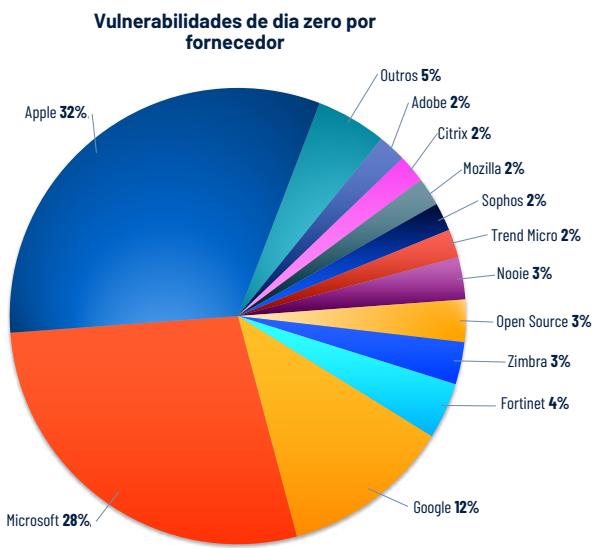


Em 2022, observamos mudanças gritantes nas tendências de vulnerabilidades de dia zero. Ao contrário dos dois anos anteriores, em que as vulnerabilidades de navegador estavam à frente, este ano as vulnerabilidades de sistema operacional subiram para o topo das paradas, representando mais da metade de todas as vulnerabilidades de dia zero.

Principais vulnerabilidades por tipo de software/hardware

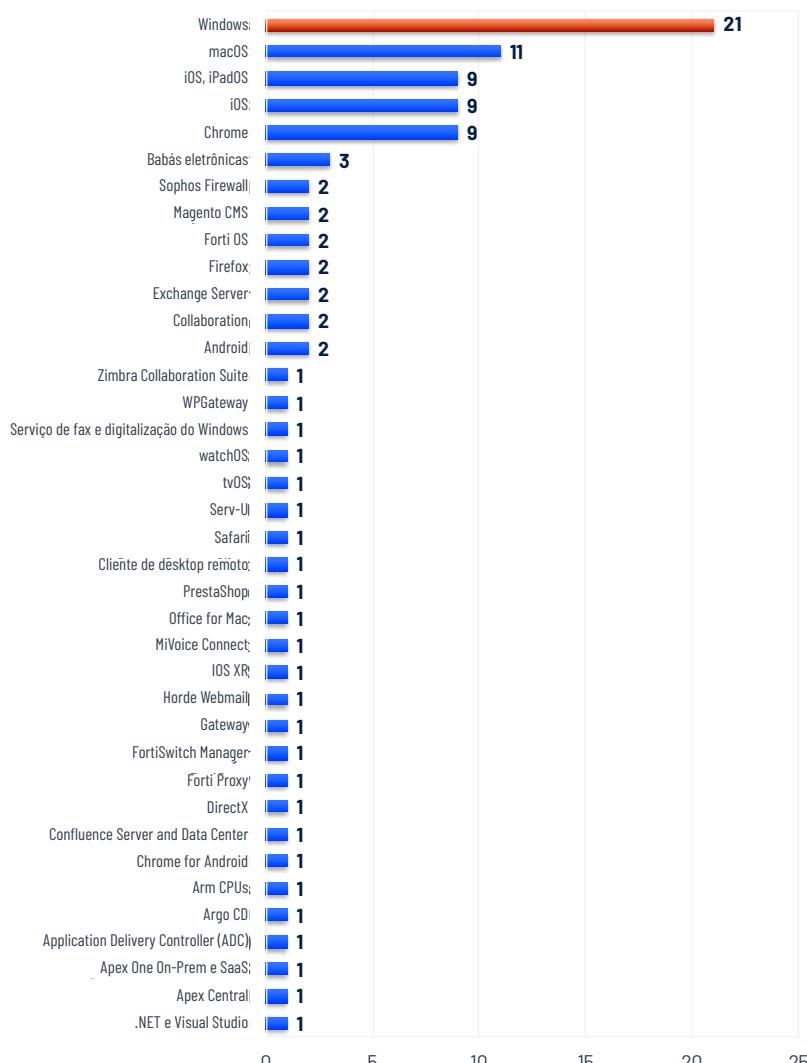
2020	2021	2022
35,7%	30,5%	50,5%
Vulnerabilidades de navegador	Vulnerabilidades de navegador	Vulnerabilidades de sistema operacional

A categoria de vulnerabilidades de sistema operacional inclui vulnerabilidades nativas em sistemas operacionais, além de ferramentas e serviços originários do sistema operacional em si. Essa categoria inclui falhas como as encontradas no Windows Print Spooler e no Windows COM+ Event System Service, entre outras.



Como nos anos anteriores, plataformas com maior base de usuários tiveram a maior quantidade de vulnerabilidades em 2022. Entre todas as vulnerabilidades de dia zero, as presentes nos produtos da Apple representaram 31,7%, seguidas pelas da Microsoft, com 27,7%. Os produtos da Apple e da Microsoft representaram um total combinado de 59,4% de todas as vulnerabilidades de dia zero divulgadas em 2022.

Vulnerabilidades de dia zero por produto



As vulnerabilidades do Microsoft Windows representaram 21% de todas as vulnerabilidades de dia zero divulgadas, seguidas por um trio de produtos da Apple: macOS (11%), iOS (9%) e iPadOS (9%). Em 2022, as vulnerabilidades do Google Chrome representaram apenas 9% de todas as vulnerabilidades de dia zero divulgadas.

Declínio nas vulnerabilidades de navegador

2021	2022
32	23
-	-28,1%

Em 2021, foram divulgadas 32 vulnerabilidades de dia zero em navegadores, e o navegador Google Chrome foi responsável por 17 delas. Em 2022, as vulnerabilidades de dia zero em navegadores diminuíram quase 30% (28,1%), totalizando 23, sendo que nove delas estavam associadas ao Google Chrome. Não está claro por que houve esse declínio acentuado nas vulnerabilidades de dia zero em navegadores, mas uma teoria é que os sandboxes baseados em navegadores dificultaram a exploração pelos invasores. Outra possibilidade é que os agentes de ameaças estejam desistindo das vulnerabilidades de dia zero e focando seus esforços em vulnerabilidades conhecidas que permanecem sem patches.

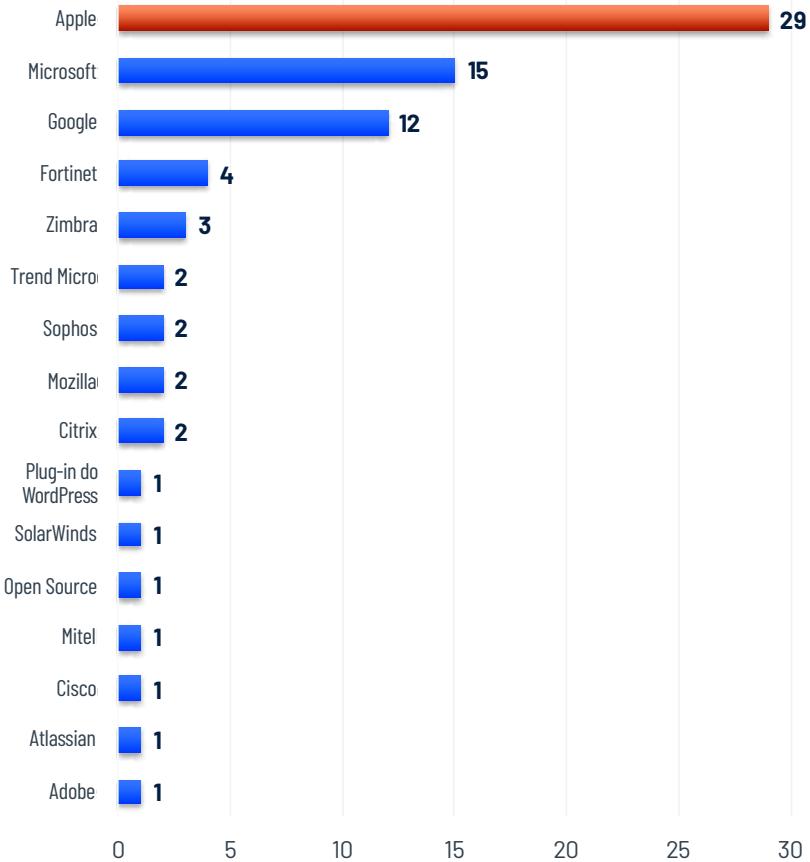
Vulnerabilidades de dia zero por status de exploração



A grande maioria (77,2%) das vulnerabilidades de dia zero divulgadas em 2022 foram exploradas no mundo real. Ainda assim, houve uma queda de 5,8% em relação a 2021, quando 83% das vulnerabilidades de dia zero divulgadas foram exploradas no mundo real.

Entre as 78 vulnerabilidades de dia zero exploradas no mundo real este ano, a maior parte está em produtos Apple, Microsoft e Google. A Apple foi responsável por 37,2% das vulnerabilidades de dia zero exploradas no mundo real em vários produtos, incluindo iOS, iPadOS e macOS, seguida pela Microsoft com 19,2%. O Google foi responsável por 15,4%, incluindo Chrome e Android.

Vulnerabilidades de dia exploradas no mundo real



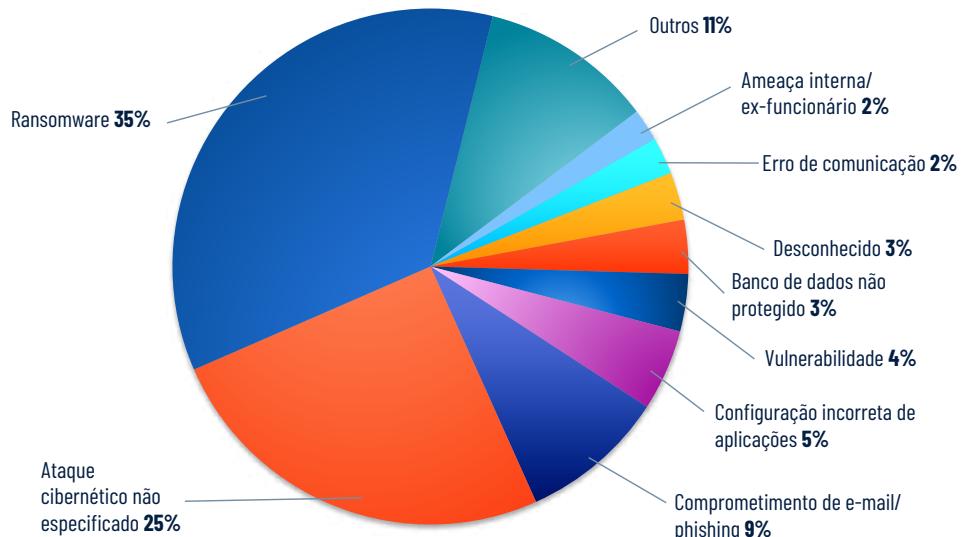
Sete fornecedores tiveram apenas uma única vulnerabilidade de dia zero que afetasse seus produtos. Entre estes quatro fornecedores – Citrix, Mozilla, Sophos e Trend Micro – cada um foi responsável por duas vulnerabilidades de dia zero exploradas no mundo real, enquanto a Zimbra foi responsável por três. No caso da Fortinet, duas vulnerabilidades de dia zero afetaram o FortiOS e um CVE afetou o FortiProxy e o FortiSwitchManager.



Região	Registros expostos no total	% do total
Ásia-Pacífico (APAC)	1.561.990.339	68,00%
América do Norte (NAM)	405.954.391	17,67%
Europa, Oriente Médio e África (EMEA)	305.994.856	13,32%
Desconhecido/Global	22.540.901	0,98%
América Latina (LATAM)	461.200	0,02%
Total	2.296.941.687	

Mais de dois terços (68%) dos registros expostos originaram-se em organizações localizadas na Ásia-Pacífico (APAC). Organizações da América do Norte (NAM) e da Europa, no Oriente Médio e na África (EMEA) representaram um total de 31% dos registros expostos. Em alguns casos, a região de uma organização não estava clara, então categorizamos esses eventos de violação como "Desconhecido/Global". Por fim, as ocorrências de violação na América Latina (LATAM) representaram apenas 0,02% dos registros expostos. Nós presumimos que essa grande diferença tenha mais a ver com os diferentes requisitos de comunicação de violações entre os países da LATAM e da NAM, da APAC e da EMEA, do que uma diferença considerável nas atividades de invasores nas diferentes regiões.

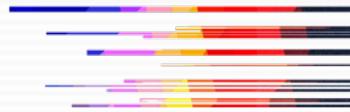
Violações de 2022 por causa raiz



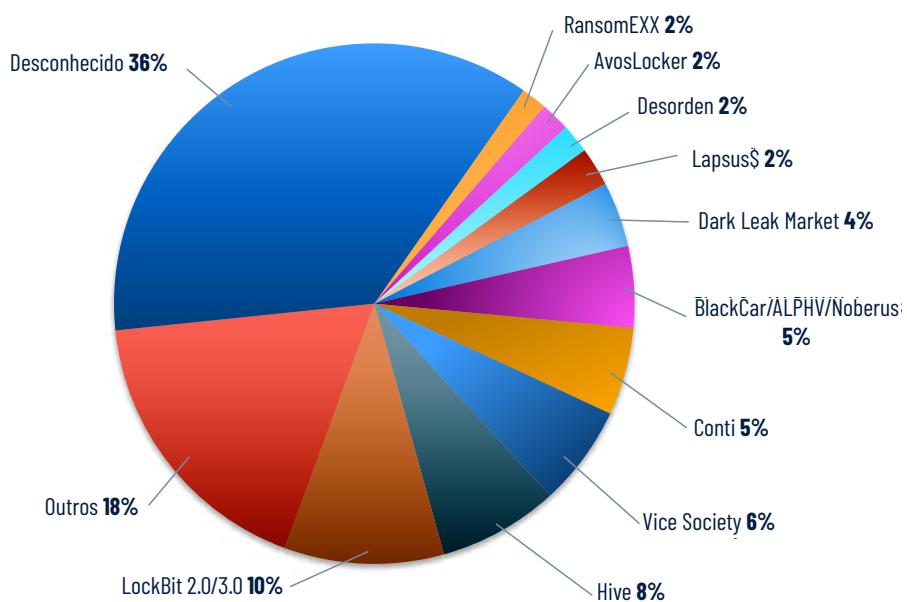
Em 2022, o ransomware continuou sendo a causa raiz mais comum de violações nas organizações, representando 35,4% de todas as ocorrências de violação. Houve uma pequena queda em relação a 2021, quando o ransomware representou 38% de todas as ocorrências de violação.

Ocorrências de ransomware como percentual de todas as ocorrências de violação

2022	2021	2020
35,4%	38%	35%



Ataques de ransomware/extorsão em 2022



Ao analisarmos todas as ocorrências de violação vinculadas a ataques de ransomware ou extorsão, classificamos quase metade (36,4%) como "Desconhecido", pois não conseguimos identificar nenhum detalhe específico sobre o grupo de ransomware ou extorsão responsável por esses ataques. Também tentamos fazer referência cruzada desses ataques com sites de vazamento de dados na dark web associados a grupos de ransomware e extorsão, mas não conseguimos vinculá-los a um grupo específico. Como não há requisitos de comunicação para ataques de ransomware, esses tipos de detalhe costumam ser desprezados.

Fora da categoria "Desconhecido", o grupo de ransomware LockBit dominou os ataques de ransomware em 2022, representando 9,9% das ocorrências de violação de ransomware analisadas. O LockBit foi autopromovido de 2.0 para 3.0, então esse número inclui ambas as iterações. Outros grupos da lista incluem o grupo de ransomware Hive (7,5%), Vice Society (6,3%) e BlackCat/ALPHV (5,1%). Outros, que compreendem 37 outros grupos, foram coletivamente responsáveis por 17,8% dos incidentes de ransomware/extorsão restantes em 2022.

Apesar de o notório grupo de ransomware Conti ter fechado as portas em maio de 2022, ele foi responsável por 5,5% das ocorrências de violação de ransomware analisadas. Para mais informações sobre o Conti, consulte a seção anterior sobre ransomware.

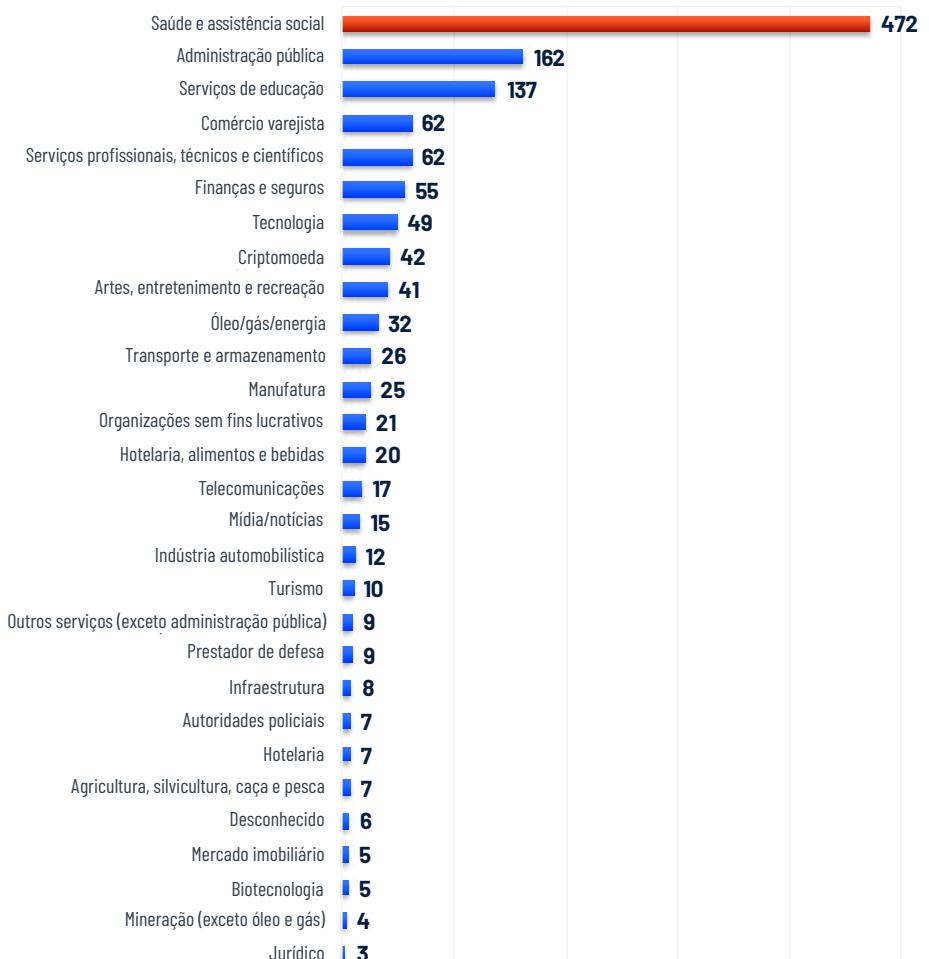
Ataques cibernéticos não especificados são a causa raiz de um quarto das ocorrências de violação

Em 2022, foi introduzida uma nova categoria chamada "ataque cibernético não especificado", como um termo geral para ocorrências de violação que não especificavam um tipo de causa raiz, mas se referiam globalmente à ocorrência de violação como um ataque cibernético ou incidente cibernético. Essa categoria representou 25,2% de todas as ocorrências em 2022. Na maioria das vezes, apesar de chamar essas ocorrências de ataque cibernético, muitas entidades afetadas não prestaram mais esclarecimentos sobre os incidentes.

**Em 2022,
o setor de
saúde foi
o principal
alvo de
ataques de
ransomware,
com 472
violações.**

O comprometimento de e-mail, que inclui ataques de phishing, representou 9,1% das ocorrências de violação em 2022, enquanto 5,1% foram decorrentes de configurações incorretas de aplicações, que muitas vezes incluem instâncias de armazenamento em nuvem mal configuradas, como Amazon Simple Storage Service (S3), Google Cloud Storage Buckets e Azure Blob Storage.

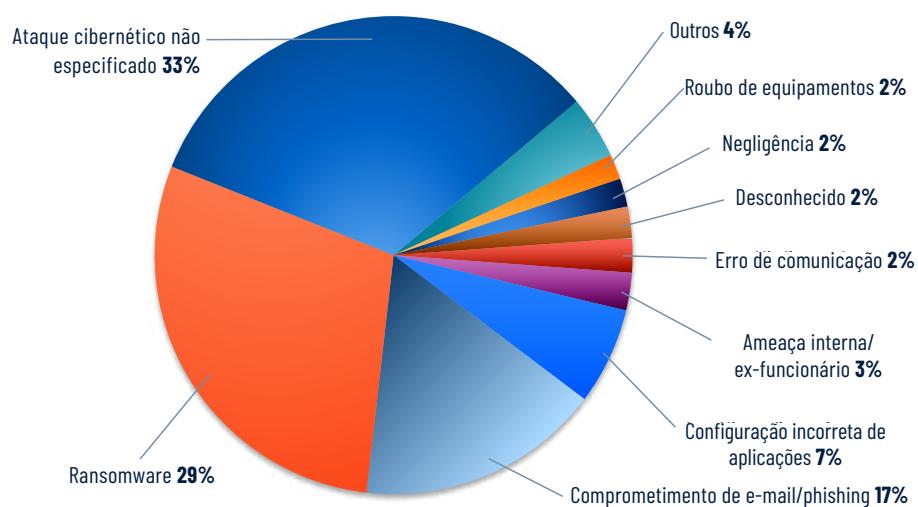
Violações de 2022 por setor



Sem nenhuma surpresa, as áreas de saúde e assistência social continuam tendo a maior quantidade de violações, representando 35,4% de todas as ocorrências analisadas – um aumento acentuado em relação a 2021, em que 24% das violações foram atribuídas à área da saúde.

A administração pública, que inclui governos e municípios, desbancou a educação para o segundo lugar em 2022, representando 12,1% das ocorrências de violação. A área de serviços educacionais ficou em terceiro lugar em 2022, representando 10,3% das ocorrências de violação.

Violações no setor de saúde em 2022 por causa raiz

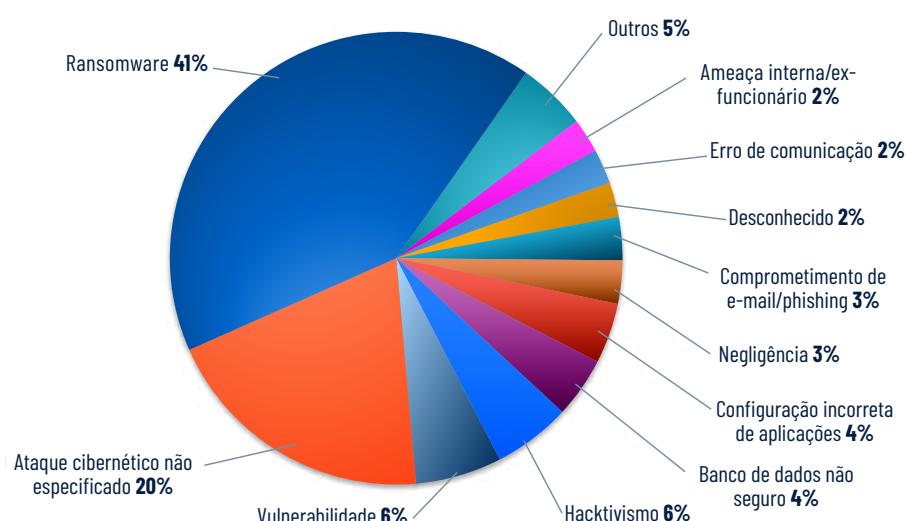


Quase um terço de todas as ocorrências de violação na área da saúde rastreadas em 2022 foram atribuídas a ataques cibernéticos não especificados, seguidos por ransomware em quase 29,2%. Isso representa uma redução de 7% em relação a 2021, quando o ransomware representou 36,2% das violações na área da saúde. Em 2022, 16,5% das violações na área de saúde resultaram de comprometimento de e-mail/phishing.

Por que a saúde é o setor mais afetado?

A área da saúde permanece no topo da nossa lista de ocorrências de violação a cada ano, em parte devido aos [requisitos de relatórios do Departamento de Saúde e Serviços Humanos dos EUA](#) e a regra de notificação de violação da Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) (45 CFR §§ 164.400-414). Além disso, as entidades americanas deverão fazer um comunicado à mídia se uma ocorrência de violação afetar mais de 500 pessoas. Se os padrões de comunicação de violação fossem adotados no mundo todo e fossem tão rigorosos quanto as regras da HIPAA, talvez tivéssemos muito mais informações sobre o nível de exposição das informações de identificação pessoal.

Violações na administração pública em 2022 por causa raiz

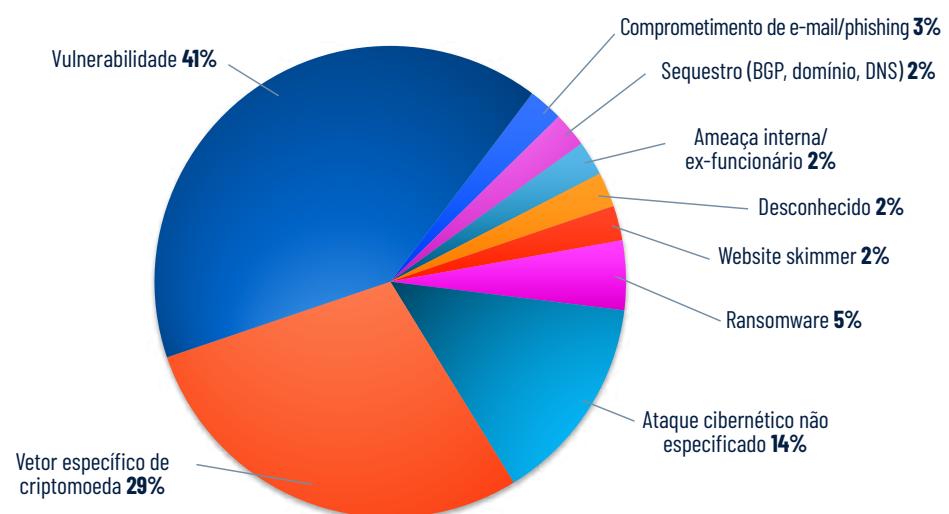


Os ataques de ransomware foram responsáveis por 41,4% de todas as ocorrências de violação na administração pública. Mais notavelmente, em 2022, observamos um esforço conjunto em direção a várias entidades de administração pública na LATAM, incluindo Costa Rica, Brasil e México. O hacktivismo também foi responsável por 5,6% das ocorrências de violação na administração pública, com impressionantes 89% afetando órgãos na LATAM.

Ataques de criptomoedas resultaram no roubo de US\$ 2,4 bilhões

Em 2022, houve pelo menos 42 ocorrências de violação vinculadas ao setor de criptomoedas, incluindo ataques contra entidades em finanças descentralizadas (DeFi), um setor em si que não é administrado por uma entidade ou corporação central e é regido por um código no blockchain conhecido como smart contracts.

Violações de criptomoedas em 2022 por causa raiz



Mais de dois terços (69,1%) das ocorrências de violação no espaço das criptomoedas resultaram de vulnerabilidades ou de uma causa raiz que chamamos de "vetor específico de criptomoeda", que inclui elementos exclusivos desse espaço, como **ataques de empréstimo instantâneo** e **manipulação de oráculo de preço**. Mais de US\$ 1,2 bilhão roubados em ocorrências de violação de criptomoedas foram atribuídos a essas duas causas raiz.

Violações de criptomoedas em 2022 por causa raiz	Fundos roubados
Vulnerabilidade	US\$ 766.460.000
Comprometimento de e-mail/phishing	US\$ 625.000.000
Vetor específico de criptomoeda	US\$ 531.530.000
Ataque cibernético não especificado	US\$ 204.400.000
Desconhecido	US\$ 160.000.000
Website skimmer	US\$ 120.000.000
Sequestro (BGP, domínio, DNS)	US\$ 235.000
Total	US\$ 2.407.625.000

Executive summary

Uptime Intelligence report: March 2024

Annual outage analysis 2024

Avoiding digital infrastructure failures remains paramount for data center owners and operators. This report analyzes recent Uptime Institute data on IT and data center outage trends: their causes, costs and consequences.

Uptime Intelligence: actionable insight for the digital infrastructure ecosystem.

To enquire about an annual subscription to Uptime Intelligence (intelligence.uptimeinstitute.com), which includes this report; or to purchase this report, please contact info@uptimeinstitute.com

Members of the Uptime Institute Membership Network can download the full report on Inside Track: insidetrack.uptimeinstitute.com

Uptime Intelligence is a research subscription service offered by Uptime Institute. It delivers in-depth, clear analysis and practical guidance focused on the present and future of data center and digital infrastructure strategies, technologies and operations. It serves enterprises that are operating their own digital infrastructure or contracting with third parties; providers of colocation, cloud and other infrastructure-as-a-service offerings; and suppliers of technology and services to all operators of digital infrastructure.

Uptime Institute serves all stakeholders that are responsible for IT service availability through industry-leading standards, education, membership, consulting and award programs delivered to enterprise organizations and third-party operators, manufacturers and providers.

This executive summary summarizes the key findings of Uptime Intelligence's *Annual outage analysis 2024* report, and includes sample pages from the full 29-page report, which is available to Uptime Institute members and Uptime Intelligence customers.

Key findings

- Despite increased media attention on outages, and a worrying increase in cyberattacks, our findings suggest that the overall frequency and severity of outages is actually decreasing.
- Uptime Institute has used multiple surveys of data center managers, and reports from our members, along with publicly available reports, to produce reliable conclusions about trends in data center outages. However, all data relating to outages should be treated skeptically. Outage information is commercially sensitive and subject to uncertainty.
- Outages are costly. More than half (54%) of the respondents to the 2023 Uptime Institute data center survey say their most recent significant, serious or severe outage cost more than \$100,000, with 16% saying that their most recent outage cost more than \$1 million.
- Power issues are consistently the most common cause of serious and severe data center outages. However, network-related issues are the largest single cause of IT service outages.
- Four in five respondents to the 2023 Uptime Institute data center survey say that their most recent serious outage could have been prevented with better management, processes and configuration. This suggests that, as in previous years, there is an opportunity to reduce outages through training and process review.
- Uptime data suggests that each year there are, on average, 10 to 20 high-profile IT outages or data center events globally that cause serious or severe financial loss, business and customer disruption, reputational loss and, in extreme cases, loss of life.

Outage frequency and severity

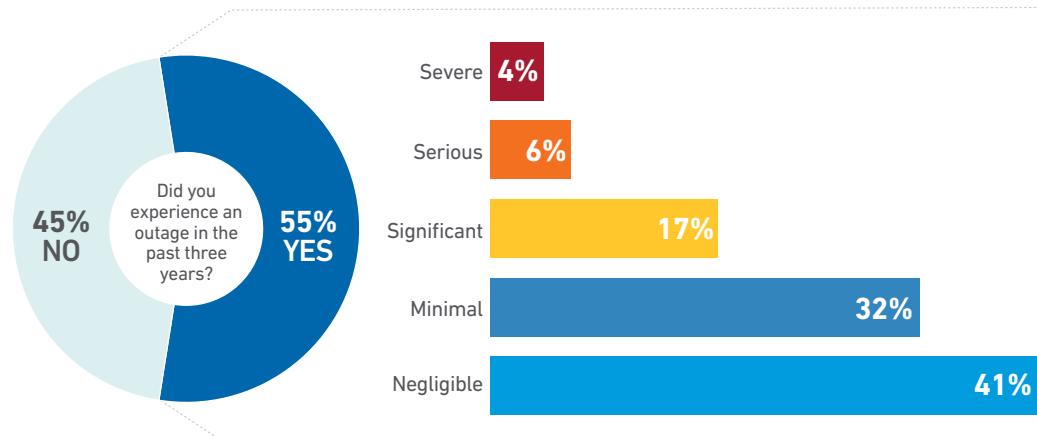
As the global data center footprint expands to meet new demand, the overall number of data center-related outages is expected to increase. However, Uptime data reveals a consistent, downward trend in the frequency and severity of outages relative to the overall growth in IT. This trend has been observed for several years.

More than half (55%) of operator respondents to the 2023 Uptime Institute data center survey report having an outage in the past three years — down from 60% in 2022 and 69% in 2021. At the same time, only one in 10 outages in 2023 was categorized as either serious or severe (see **Figure 1**). This is an improvement of four percentage points from the 2022 response and an improvement of 10 percentage points compared with 2021. When analyzing this data, Uptime focuses on data center outages and not all IT service outages. To collect more precise survey data and to improve accuracy, respondents to our annual survey are now asked about outages at the specific facility that they are most familiar with, rather than the largest site within the data center operator's organization. This may have led to some shifts in the data — however, our control questions suggest the effect on longitudinal comparisons has been minor.

Figure 1

While majority of operators experienced an outage, most had negligible impact

On a scale of 1 (negligible) to 5 (severe) how would you classify your data center's most impactful outage in the past three years, either in your own facility or because of a third-party service provider? (n=781)



(Responses for "Don't know" are not included.)

UPTIME INSTITUTE GLOBAL SURVEY OF IT AND DATA CENTER MANAGERS 2023

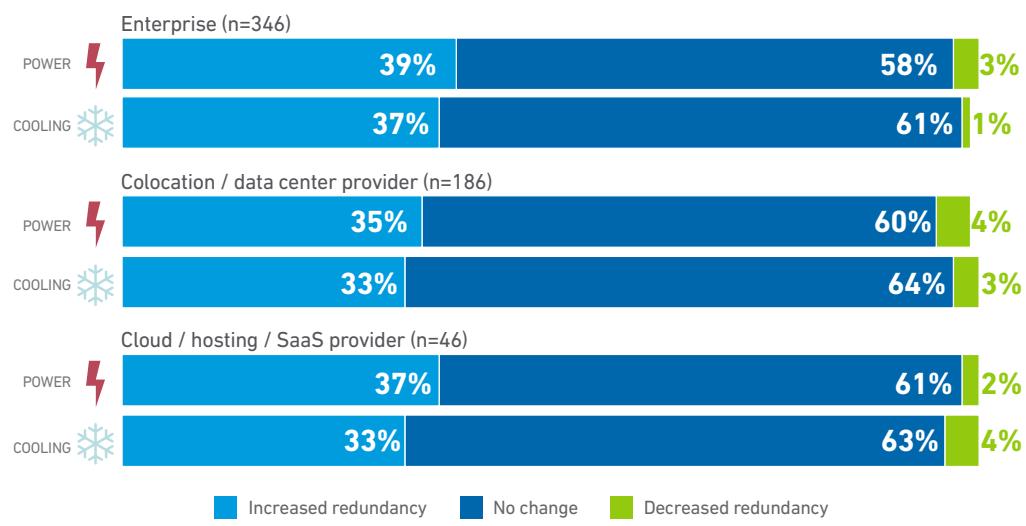
Despite the increase in risk factors, Uptime's annual survey data up to 2023 suggests that the rate of outages per facility is falling. What could be driving this trend? One factor stands out: Uptime research finds that, year-on-year, most organizations are investing more in physical infrastructure redundancy (see **Figure 2**).

This trend contradicts expectations that multisite approaches will undermine expensive, physical site redundancy strategies. While the industry may indeed move further toward distributed and software-based resiliency models, maintaining and increasing site-level redundancy remains a high priority for most operators.

Figure 2

Physical site redundancy still climbing

How have redundancy levels changed in the past three to five years in your data center?



(All figures rounded.)

UPTIME INSTITUTE GLOBAL SURVEY OF IT AND DATA CENTER MANAGERS 2023

Outage causes

Establishing the root cause of a data center outage is imperative for preventing repeat instances of disruption and for identifying areas that require greater investment to mitigate the risks. However, assessing outage data poses challenges due to the multifaceted nature of most incidents, which often stem from a combination of factors.

Uptime's annual surveys consistently show that disruptions to on-site power distribution are the most common cause behind impactful outages (see **Figure 4**). This is unsurprising given the intolerance of IT hardware to any significant power disturbances, such as voltage fluctuations or complete loss of power, that last more than fractions of a second.

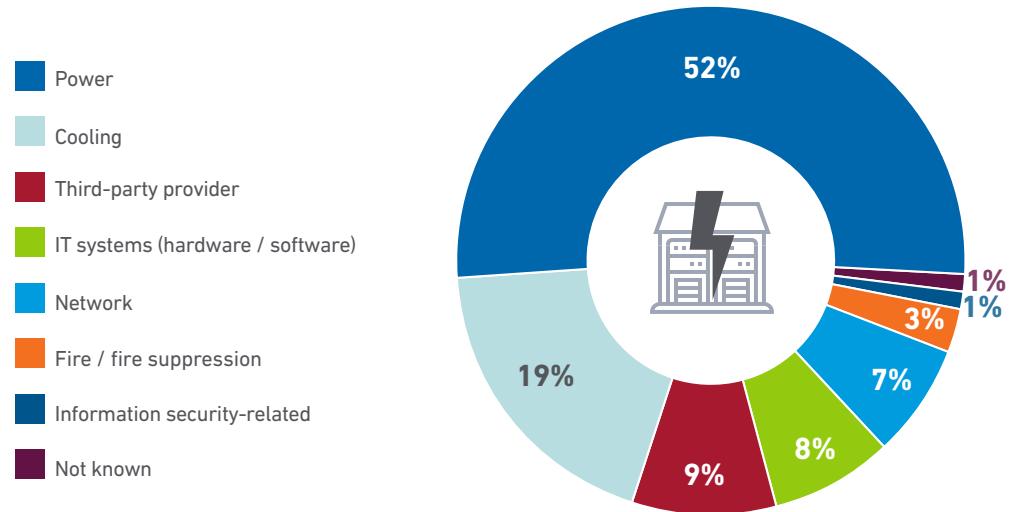
Conversely, failures or underperformance of cooling equipment are generally tolerated for longer durations, often measured in minutes, due to thermal ride-through mechanisms or network traffic redirection capabilities. While IT-originating failures may occur more frequently, they often have isolated, minor effects that go unrecorded and primarily impact specific applications or datasets.

Third-party provider issues have seen a marginal but consistent uptick since 2020, rising by five percentage points to account for nearly one in 10 outages in 2023. This steady increase reflects the growing reliance on cloud / hosting, software as a service (SaaS) and colocation providers.

Figure 4

Power remains the number one root cause of outages

What was the primary cause of your data center's most recent impactful incident or outage? (n=108)



UPTIME INSTITUTE GLOBAL SURVEY OF IT AND DATA CENTER MANAGERS 2023

PUBLICLY REPORTED OUTAGES

Commercial operators in the limelight

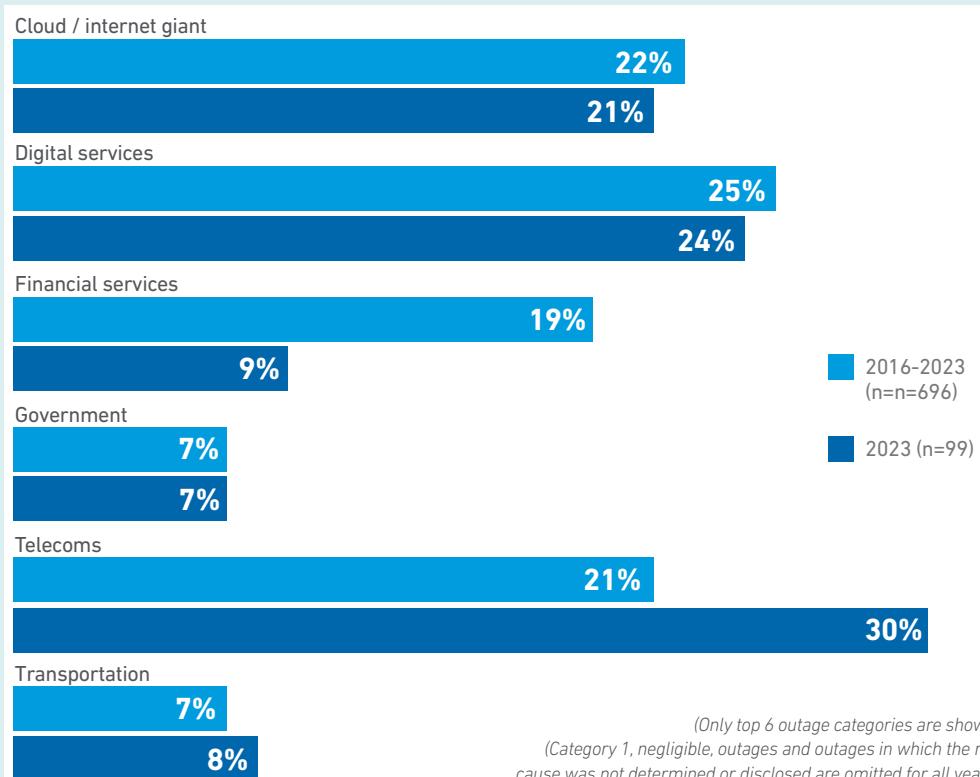
Over the past eight years, third-party commercial operators of IT and/or data centers combined (cloud / internet giants, digital services, telecommunications, etc.) have accounted for more than two-thirds (67%) of publicly reported outages recorded by Uptime (see **Figure 7**). This reflects the growth of professional, outsourced IT services, from colocation to cloud and hosting. Moving to third-party venues and services may reduce risks but failures still occur, and they can be very serious.

Compared with the average over this period, financial sector outages fell in both 2022 and 2023. This may be influenced by stricter regulations and oversight following a series of large, high-impact outages before 2021.

The telecommunications sector, on the other hand, has experienced an uptick in outages. This has been driven by various factors: rising demand for connectivity and capacity across all sectors has put a strain on networks and legacy infrastructure, while the criticality of mobile networks, in particular, means outages can have an outsized impact. The increasing use of standardized and less expensive data centers — compared with earlier, resilient but limited designs — may have increased some risks while lessening others. The adoption of technologies, such as software-defined networking, 5G and network function virtualization, adds complexity to these systems.

Figure 7

Publicly reported outages by sector, 2016 to 2023



The human factor

Data center operators face considerable challenges when it comes to preventing and mitigating downtime caused by human error. This is because failures can stem from various factors, such as the adequacy of training, the effectiveness of procedures in place, staff fatigue, resource availability and the complexity of equipment operation. There is also uncertainty around how such incidents should be defined; for instance, whether a machine failure caused by a software error at the factory constitutes human error.

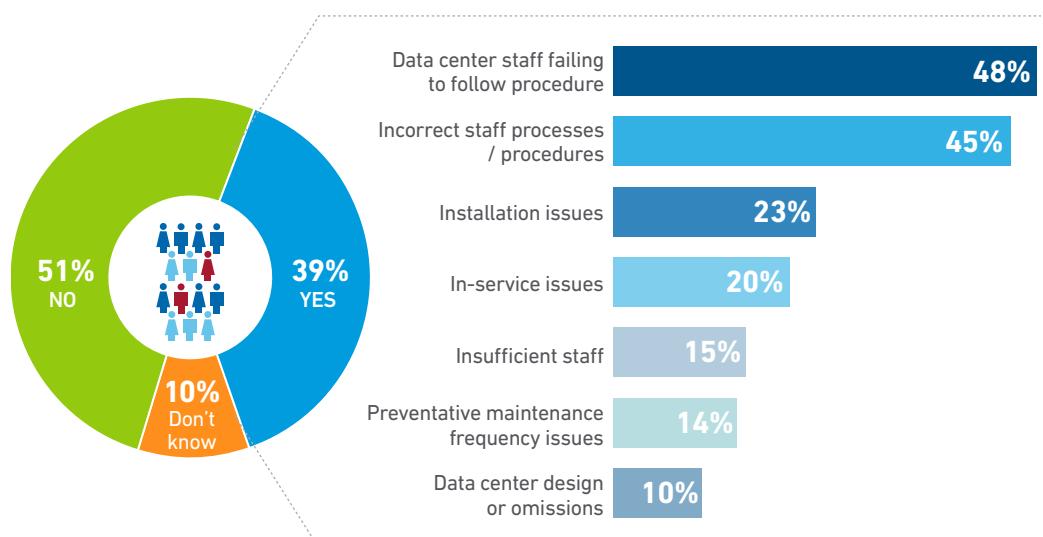
As a result, Uptime tends to analyze human error as a contributing factor rather than the sole or primary cause of outages. Drawing on 25 years of data, Uptime estimates that human error, whether directly or indirectly, contributes to a significant majority — ranging from two-thirds to four-fifths — of all downtime incidents.

In recent surveys on resiliency, Uptime has tried to understand how the makeup of some of these failures relates to human error. **Figure 13** shows that human error-related outages are mostly caused either by staff failing to follow procedures (even if they have been agreed upon and codified) or by the procedures themselves being inadequate.

Figure 13

Most common causes of major human error-related outages

Has your organization experienced a significant, serious, or severe IT service outage(s) that was caused by human error over the past three years? If so, what are their most common causes? Choose no more than three. (n=418)



(Responses for "Other" and "Don't know" are not included.)

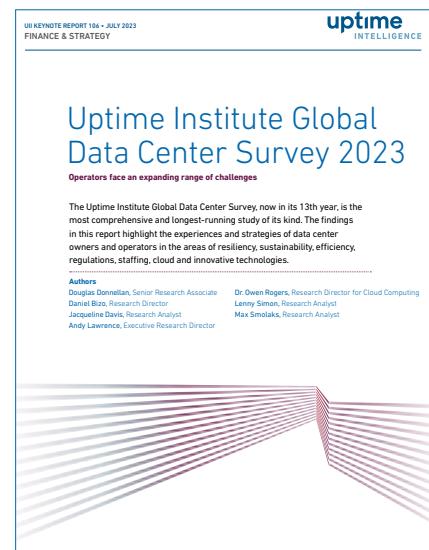
(The sum percentages for most common causes exceed 100% due to respondents being asked to choose up to three options.)

Executive summary

July 2023

Uptime Institute Global Data Center Survey 2023

The Uptime Institute Global Data Center Survey, now in its 13th year, is the most comprehensive and longest-running study of its kind. The findings in this report highlight the experiences and strategies of data center owners and operators in the areas of resiliency, sustainability, efficiency, regulations, staffing, cloud and innovative technologies.



Uptime Intelligence: actionable insight for the digital infrastructure ecosystem

This executive summary includes excerpts from a subscriber-only report published by Uptime Intelligence (a service of Uptime Institute).

To learn more, visit: uptimeinstitute.com/ui-intelligence

Members of the Uptime Institute Membership Network can download the full report on Inside Track: insidetrack.uptimeinstitute.com

Uptime Intelligence is a research subscription service offered by Uptime Institute. It delivers in-depth, clear analysis and practical guidance focused on the present and future of data center and digital infrastructure strategies, technologies and operations. It serves enterprises that are operating their own digital infrastructure or contracting with third parties; providers of colocation, cloud and other infrastructure-as-a-service offerings; and suppliers of technology and services to all operators of digital infrastructure.

Uptime Institute serves all stakeholders that are responsible for IT service availability through industry-leading standards, education, membership, consulting and award programs delivered to enterprise organizations and third-party operators, manufacturers and providers.

Introduction

The 13th annual Uptime Institute Global Data Center Survey is the most comprehensive and longest-running study of its kind. The survey tracks the state of the industry in terms of resiliency, sustainability, efficiency, regulations, staffing, cloud and the use of innovative technologies.

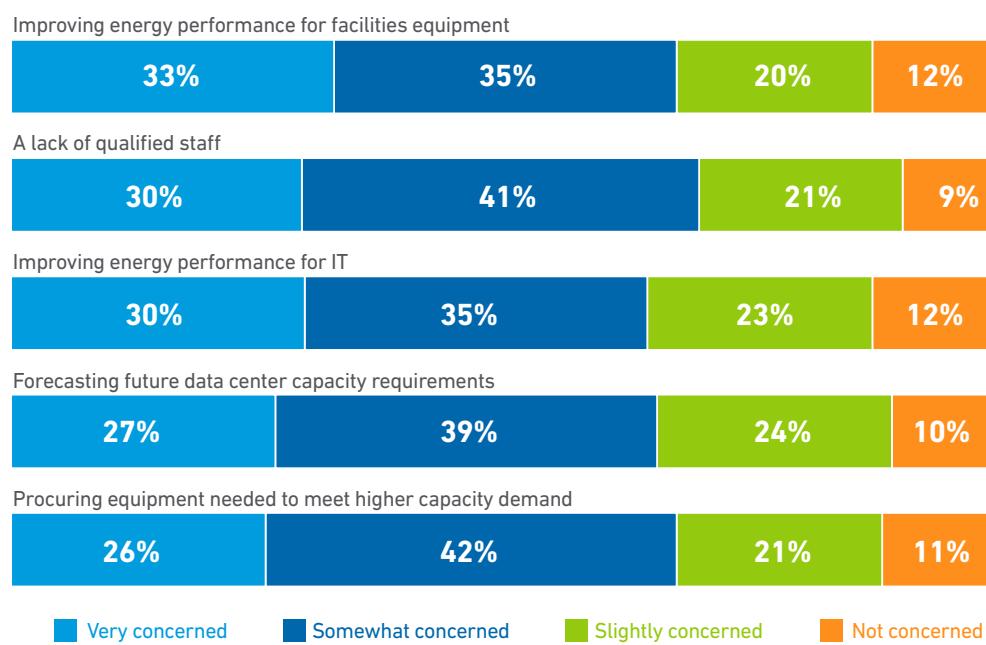
The survey was conducted online from February 2023 to April 2023 and collected responses from more than 850 data center owners and operators, as well as nearly 700 vendors and consultants. This report focuses on owners and operators of digital infrastructure (an analysis of the experiences and views of vendors and consultants will be published separately). For more details, including demographics, see the [Appendix](#).

For the first time, the survey asked operators to identify and weigh up some of their key management concerns. While the lingering effects of the COVID-19 pandemic have receded in 2023, new challenges have taken their place: digital infrastructure managers are now most concerned with improving energy performance and dealing with staffing shortfalls (see **Figure 1**). Government commitments to reduce carbon emissions are nearing their target deadlines and, as a result, regulations aimed at data center energy use require urgent attention, investment and action.

Figure 1

Staffing and energy efficiency are managers' top concerns

Looking at the next 12 months, how concerned is your digital infrastructure management regarding each of the following issues? (n=629)



(Only the top five response categories are shown.)
(All figures rounded.)

UPTIME INSTITUTE GLOBAL SURVEY OF IT AND DATA CENTER MANAGERS 2023

Cloud and provisioning

Many organizations remain wary of using the public cloud for mission critical applications. Their primary concern is data security, with concern about infrastructure performance and resiliency being less significant.

Data security, not infrastructure, blocks cloud adoption

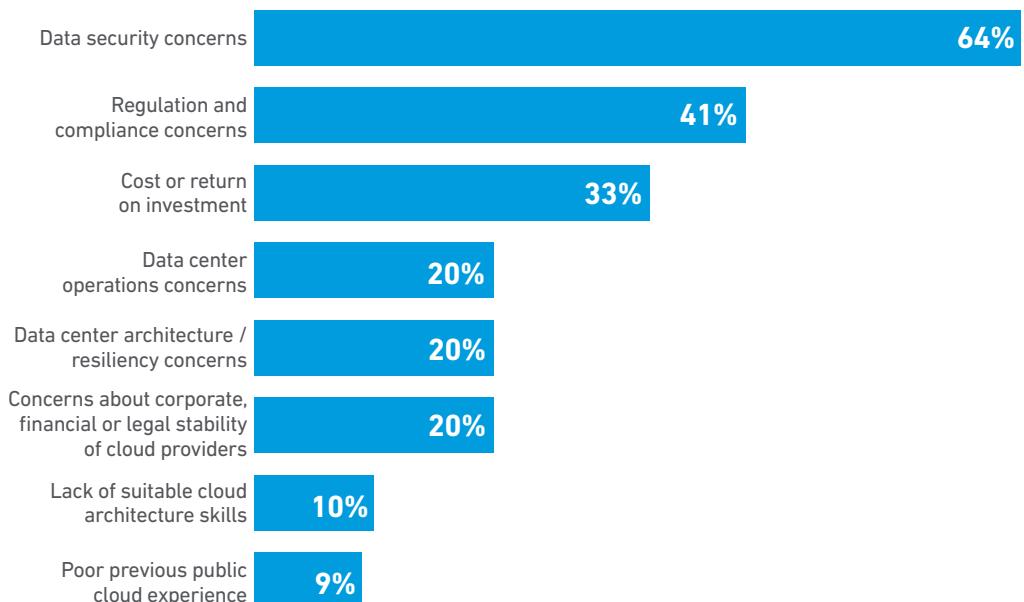
Two-thirds (65%) of respondents to the 2023 Uptime Institute data center survey are not hosting any mission-critical applications in the public cloud — a high proportion. In the past, many Uptime members have said that a lack of clarity in hyperscaler data centers' operations and resiliency had discouraged cloud adoption. Many said they preferred to operate their own data centers and have greater control. Respondents also believed that their data centers were less likely to experience outages than public cloud operators, which have suffered from some much-publicized failures across availability zones and regions.

However, Uptime's 2023 research suggests that visibility into public cloud operations and resiliency may not be the main reason for not using the public cloud — the challenge is data protection. Respondents who did not place mission-critical workloads in the cloud were asked to identify the reasons: almost two-thirds (64%) cited data security as a barrier to adoption; with 41% also expressing concerns over regulation and compliance (see **Figure 15**). Compared with other obstacles, concerns relating to data center operations and resiliency ranked relatively low — each was selected by 20% of respondents. Only 9% said a previous negative experience with the public cloud had deterred them from using it again.

Figure 15

Data security and compliance concerns impede adoption

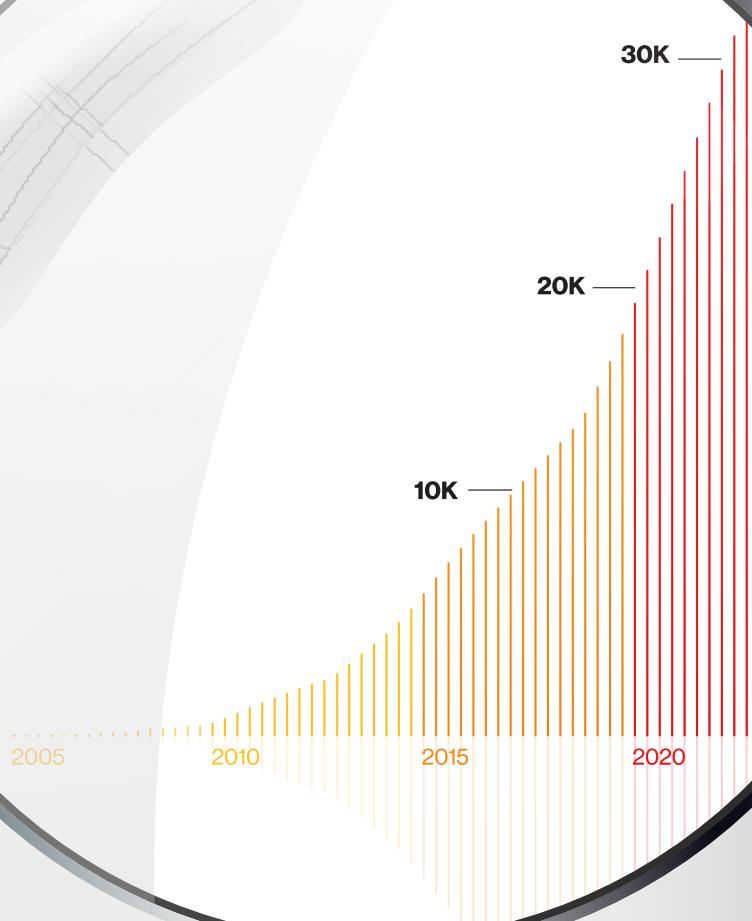
What are the main reasons you do not place mission-critical workloads into public clouds?
Choose no more than three. (n=240)



DBIR

2023 Data Breach Investigations Report

Small and Medium Business Snapshot



verizon ✓

Summary of findings

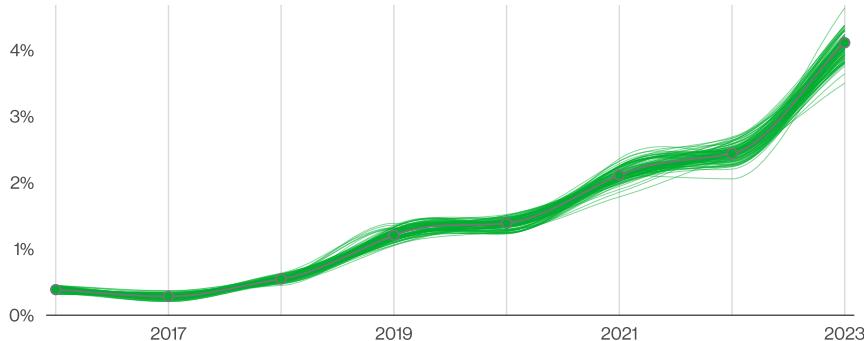


Figure 1. Pretexting incidents over time

Business Email Compromise is a key issue.

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is why Business Email Compromise (BEC) attacks (which are in essence pretexting attacks) have almost doubled across our entire incident dataset, as can be seen in Figure 1, and now represent more than 50% of incidents within the Social Engineering pattern.

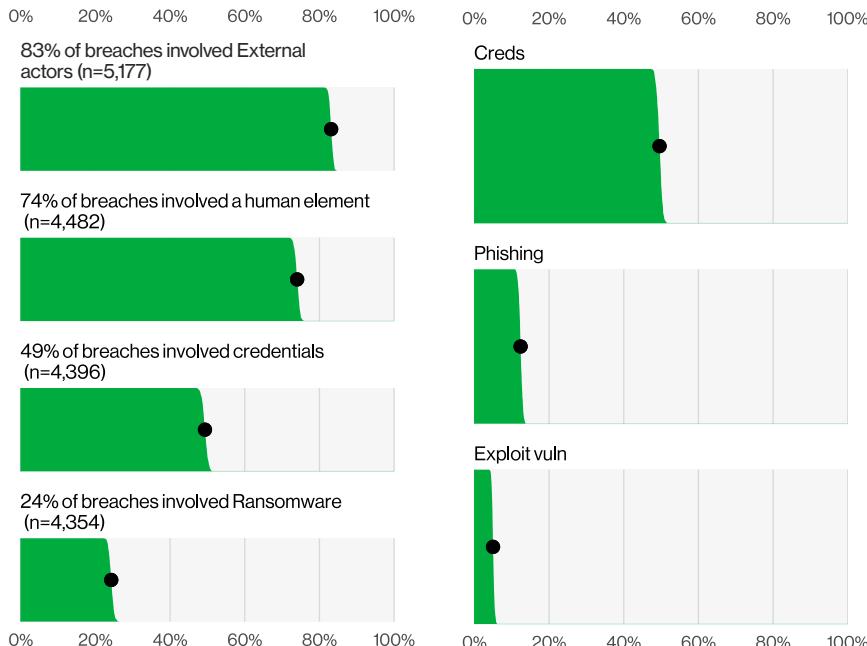


Figure 2. Select key enumerations

Figure 3. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

The human element risk cannot be understated.

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.

Looking for access on multiple fronts.

The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

Incident Classification Patterns

The DBIR first introduced the Incident Classification Patterns in 2014 as a useful shorthand for scenarios that occurred very frequently. Last year, due to changes in attack type and the threat landscape, we revamped and enhanced those patterns, moving from nine to eight—the seven you see in this report and the Everything Else “pattern,” which is a catch-all for incidents that don’t fit within the orderly confines of the other patterns.

These patterns are based on an elegant machine-learning clustering process, equipped to better capture complex interaction rules, and they are much more focused on what happens during the breach. That makes them better suited for control recommendations, too.

Here are our key findings for each pattern:

System Intrusion	<p>These are complex attacks that leverage malware and/or hacking to achieve the objectives. Frequently included in this pattern is the deployment of ransomware.</p>	<p>80% of System Intrusion incidents involved Ransomware as attackers continue to leverage a bevy of different techniques to compromise an organization and monetize their access.</p> <ul style="list-style-type: none">• 91% of industries have Ransomware as one of their top varieties of incidents.• 32% of Log4j vulnerability scanning occurred within 30 days of the vulnerability’s release.• 97% of breaches were Financially motivated, and 3% were motivated by Espionage.• While only 7% of Ransomware incidents reported losses to the FBI Internet Crime Complaint Center (IC3), the median loss more than doubled from last year to \$26,000, with 95% of incidents ranging between \$1 and \$2.25 million.
Social Engineering	<p>This attack involves the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.</p>	<p>Social Engineering incidents have increased from the previous year largely due to the use of Pretexting, which is commonly used in BEC, almost doubling since last year.</p> <ul style="list-style-type: none">• Based on IC3 data, the median amount stolen from these attacks has increased over the last couple of years to \$50,000.• Social Engineering accounts for 17% of Breaches and 10% of Incidents.

Basic Web Application Attacks	These attacks are against a web application (as the name implies), and after the initial compromise, they typically do not have a large number of additional Actions. This is the “get in, get the data and get out” pattern.	While representing approximately one-fourth of our dataset, Basic Web Application Attacks breaches and incidents tend to be largely driven by attacks against credentials and then leveraging those stolen credentials to access a variety of resources. <ul style="list-style-type: none"> • 86% of Basic Web Application Attacks breaches involve the Use of stolen credentials. • 10% of breaches in this pattern involve the Exploitation of a vulnerability.
Miscellaneous Errors	Incidents where unintentional actions directly compromised a security attribute of an information asset fall into this pattern. This does not include lost devices, which are grouped with theft in the Lost and Stolen Assets pattern.	Error-related breaches are down to 9% as opposed to 13% last year. However, this could be due to sample size (715 error incidents and 708 with confirmed data disclosure in last year's data as opposed to 602 incidents, with 513 confirmed breaches this year). <ul style="list-style-type: none"> • Data compromised included Personal (89%), Medical (19%), Other (10%) and Bank (10%). • Misdelivery (sending something to the wrong recipient) accounts for 43% of breach-related errors. • Publishing errors (showing something to the wrong audience) is in second place at 23%. • Misconfiguration comes in third and accounts for 21% of error-related breaches. • The majority of errors that lead to breaches are committed by Developers and System admins.
Denial of Service	These attacks are intended to compromise the availability of networks and systems, which includes both network and application layer attacks.	The median size of attacks grew 57% from 1.4 gigabits per second (Gbps) last year to 2.2 Gbps this year, and the top size of attacks, the 97.5 percentile, grew 25% from 99 Gbps to 124 Gbps. <ul style="list-style-type: none"> • A point of attention that some of our partners brought to us was the growth of distributed DNS Water Torture attacks in, you guessed it, shared DNS infrastructure.
Lost and Stolen Assets	Any incident where an information asset went missing, whether through misplacement or malice, is grouped into this pattern.	The loss and theft of mobile phones continues to be an issue across the board. While less data tends to be on these devices, the same cannot be said of laptops. While less data tends to be on these devices, the same cannot be said of laptops, the loss and theft of which increased last year.
Privilege Misuse	Incidents predominantly driven by unapproved or malicious use of legitimate privileges are grouped here.	We are increasingly seeing Privilege Misuse breaches paired with Fraudulent transactions, more so this year than in the past several.

Table 1. Incident Classification Patterns key findings

Insights for small and medium business

"Let's do some word problems!"—said no one ever (except math teachers)

In certain prior reports, we have compared and contrasted small and medium businesses (SMBs) against large organizations to determine whether the attack surface differed significantly between them. Increasingly, both SMBs and large companies are using similar services and infrastructure, and that means that their attack surfaces share more in common than ever before. This has led to a convergence of attack profiles regardless of the size of the organization. However, what is very different is the ability of organizations to respond to threats due to the number of resources they can deploy in the event that they are attacked.

The tables on the right illustrate the fact that SMBs and large organizations have increasingly become similar to each other. This phenomenon began several years ago, and by now there is so little difference based on organizational size that we were hard-pressed to make any distinctions whatsoever. Therefore, this year we decided to look at these a bit differently by looking at the implementation of security controls for various size SMBs (smaller, midsize and larger) and how they may overlap or differ.

In past reports we have discussed the research we conduct with regard to controls—in particular, the work we have done with MITRE to map VERIS to ATT&CK. This year, we would like to take this research a bit more into the real world and apply it to how you would use these mappings with the appropriate Center for Internet Security (CIS) Implementation Group protective controls.

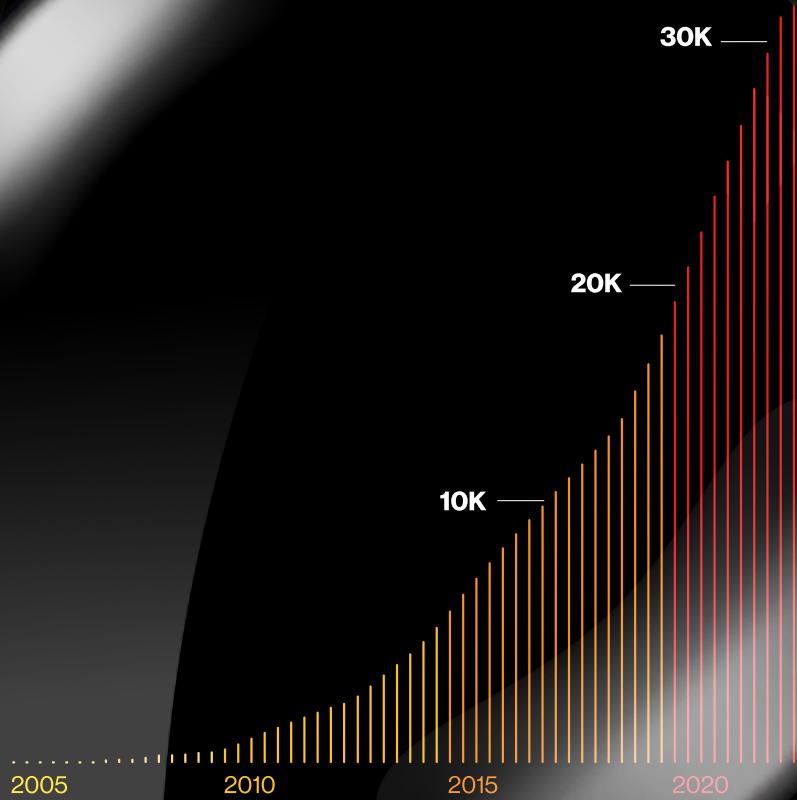
Small businesses (less than 1,000 employees)		Large businesses (more than 1,000 employees)	
Frequency	699 incidents, 381 with confirmed data disclosure	Frequency	496 incidents, 227 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches	Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches)	Threat actors	External (89%), Internal (13%), Multiple (2%), Partner (2%) (breaches)
Actor motives	Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches)	Actor motives	Financial (97%), Espionage (3%), Ideology (2%), Convenience (1%), Fun (1%) (breaches)
Data compromised	Credentials (54%), Internal (37%), Other (22%), System (11%) (breaches)	Data compromised	Internal (41%), Credentials (37%), Other (30%), System (22%) (breaches)

Table 2. At a glance for SMBs

Table 3. At a glance for large organizations

DBIR

2023 Data Breach
Investigations Report



verizon[✓]

Summary of findings

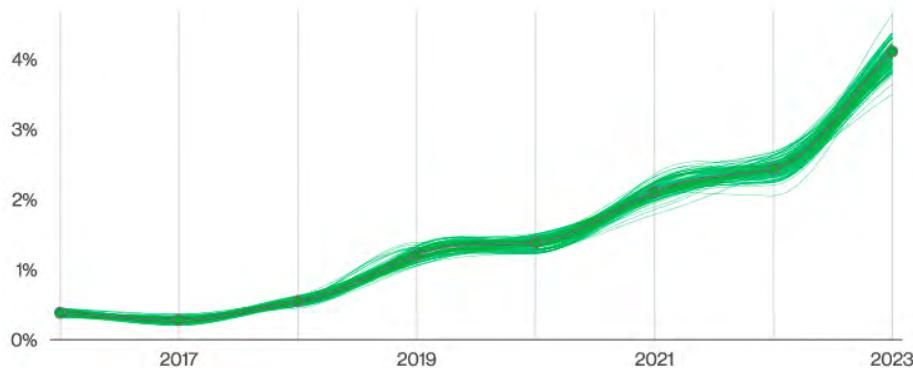


Figure 5. Pretexting incidents over time

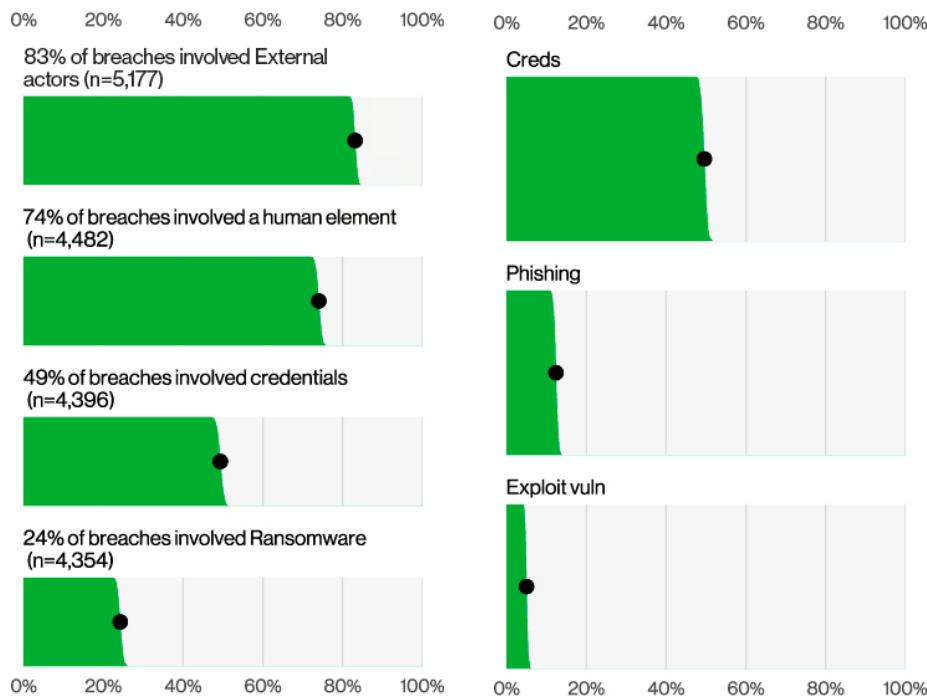


Figure 6. Select key enumerations

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is why Business Email Compromise (BEC) attacks (which are in essence pretexting attacks) have almost doubled across our entire incident dataset, as can be seen in Figure 5, and now represent more than 50% of incidents within the Social Engineering pattern.

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.

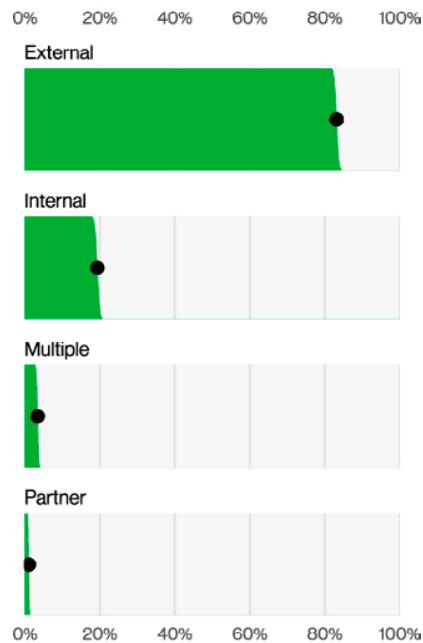
The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

Figure 7. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

Actors

Life can be scary and unpredictable, which is why we like to start our results discussion with the cozy and familiar Actor analysis. It really is true, as they say, that the only certainties in life are death, taxes and External actors.⁷

As Figure 11 demonstrates, External actors were responsible for 83% of breaches, while Internal ones account for 19%. It is worth reminding our readers that Internal actors are not only responsible for intentional harm in these cases, but they are also just as likely⁸ to be responsible for Error actions. Regardless, the clear frequency of External actors as instigators of breaches is a datapoint that has held steady ever since we started this gig.



Actor categories⁹

External: External threats originate from sources outside of the organization and its network of partners. Examples include criminal groups, lone hackers, former employees and government entities. This category also includes God (as in “acts of”), “Mother Nature” and random chance. Typically, no trust or privilege is implied for external entities.

Internal: Internal threats are those originating from within the organization. This encompasses company full-time employees, independent contractors, interns and other staff. Insiders are trusted and privileged (some more than others).

Partner: Partners include any third party sharing a business relationship with the organization. This includes suppliers, vendors, hosting providers and outsourced IT support. Some level of trust and privilege is usually implied between business partners. Note that an attacker could use a partner as a vector, but that does not make the partner the Actor in this case. The partner has to initiate the incident.

7 That's what they say, right?

8 OK, actually twice as likely.

9 <https://verisframework.org/actors.html>

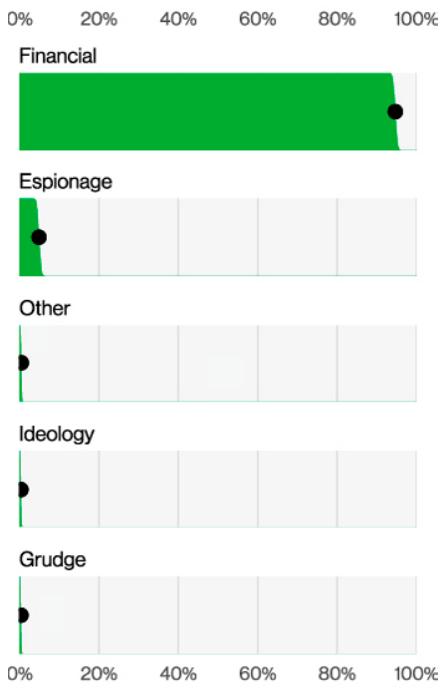


Figure 12. Threat actor Motives in breaches (n=2,328)

Long-time readers of the report will be similarly shocked to learn that Financial motives still drive the vast majority of breaches (Figure 12), showing growth in relation to last year with a whopping 94.6% representation in breaches. If we look inside to see which external actors are the hardest working, the top performer is Organized crime (Figure 13).

What is most interesting in Figure 13, however, is realizing that the internal variety of End-user shows up more often than the external variety State-sponsored attackers.¹⁰ Those organization employees are mostly involved in Misuse (read, internal malicious activity) and Errors (accidents), which suggests where we should be paying more attention on our day-to-day security management.

This is relevant because we were expecting some increased activity in State-sponsored attacks, be it Espionage-related or not, due to the ongoing conflict in Ukraine. Even with anecdotal evidence of increased ideology or hacktivism-related attacks stemming from the geopolitical discussion, it really isn't making a dent in larger statistical terms. It is also worth noting that this kind of activity would also be unlikely to disrupt our average reader's organization.¹¹

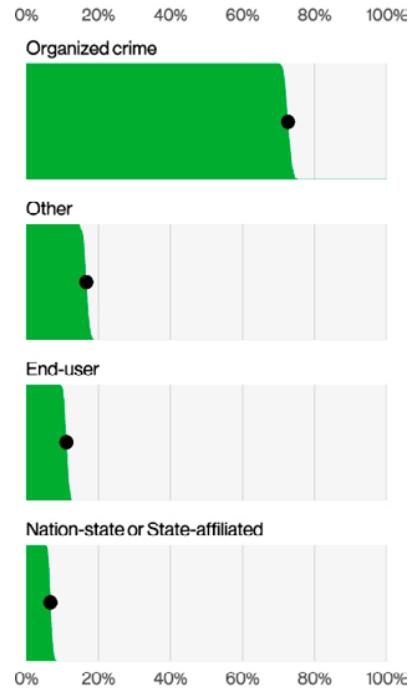


Figure 13. Threat actor Varieties in breaches (n=2,489)

¹⁰ Huge win for anarchists and other state-abolishing ideologies, if you ask us.

¹¹ No, Mr. Bond, MI6 does not represent our average reader.

Actions

Action, as the name would imply, is what brings dynamism to our report. What dastardly deeds have the threat actors been up to? If you replied “ransomware,” we’d say you have no imagination, but you would also be right. This pesky Malware variety has been holding our talking points hostage for years now, and we can’t scrounge up enough cryptocurrency to pay the ransom!

Figures 14, 15, 16 and 17 describe the top Action varieties (what happened in more detail) and vectors (how those actions came to pass).

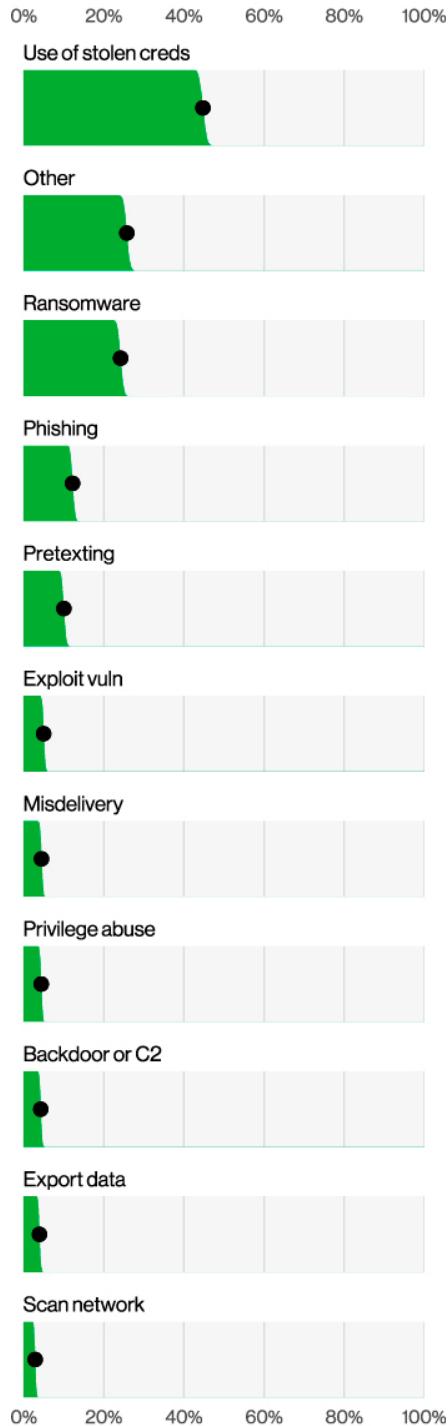


Figure 14. Top Action varieties in breaches (n=4,354)

Action categories¹²

Hacking (hak): attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms.

Malware (mal): any malicious software, script or code run on a device that alters its state or function without the owner's informed consent.

Error (err): anything done (or left undone) incorrectly or inadvertently.

Social (soc): employ deception, manipulation, intimidation, etc., to exploit the human element, or users, of information assets.

Misuse (mis): use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended.

Physical (phy): deliberate threats that involve proximity, possession or force.

Environmental (env): not only includes natural events such as earthquakes and floods but also hazards associated with the immediate environment or infrastructure in which assets are located.

12 <https://verisframework.org/actions.html>

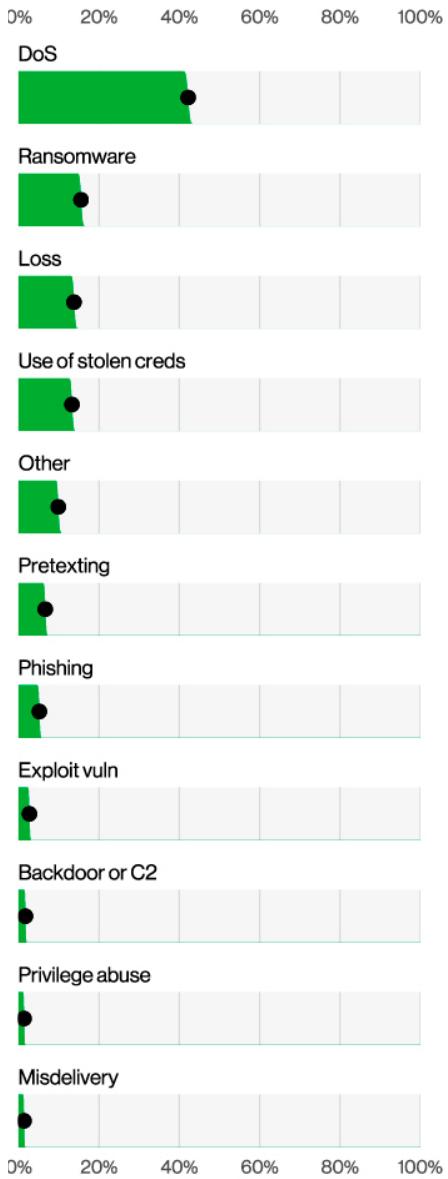


Figure 15. Top Action varieties in incidents (n=14,829)

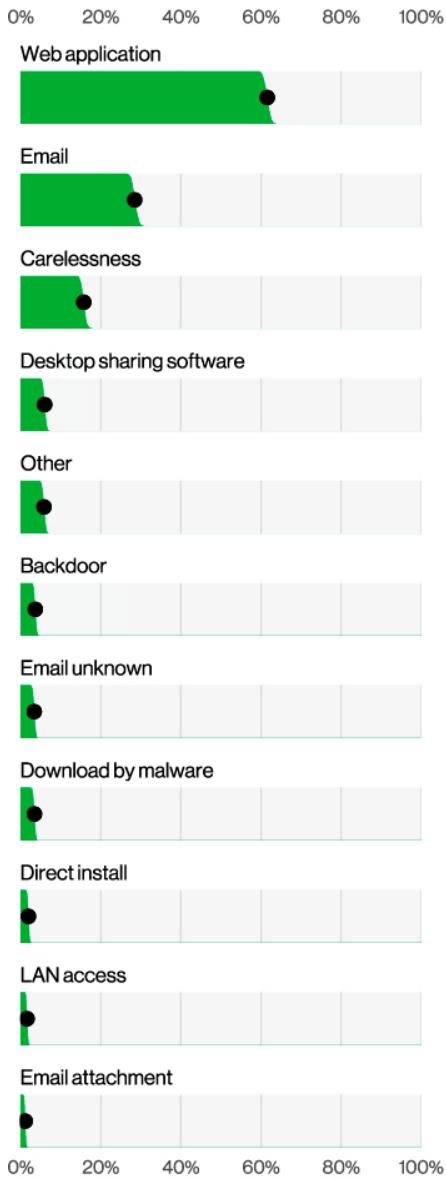


Figure 16. Top Action vectors in breaches (n=3,194)

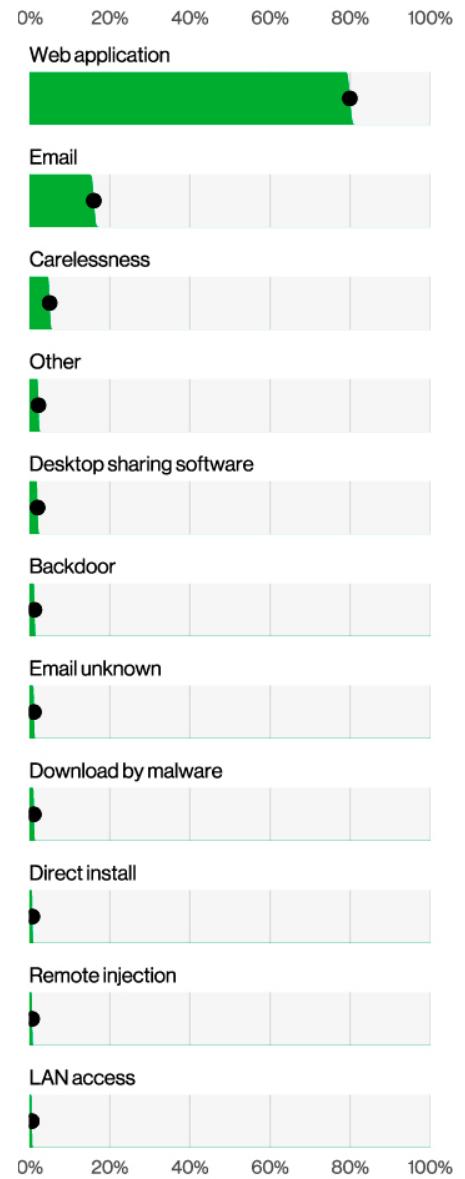


Figure 17. Top Action vectors in incidents (n=10,502)

Assets

In case you just wandered out of an Accounting 101 class, our Assets are more than the numbers that you list on the left side of your balance sheet.¹⁸ They encompass the entities that can be affected in an incident or breach and end up being manipulated by the threat actors for their nefarious goals. The callout box describes some of the most common top-level Assets in VERIS and some of the most common attack patterns that target them.

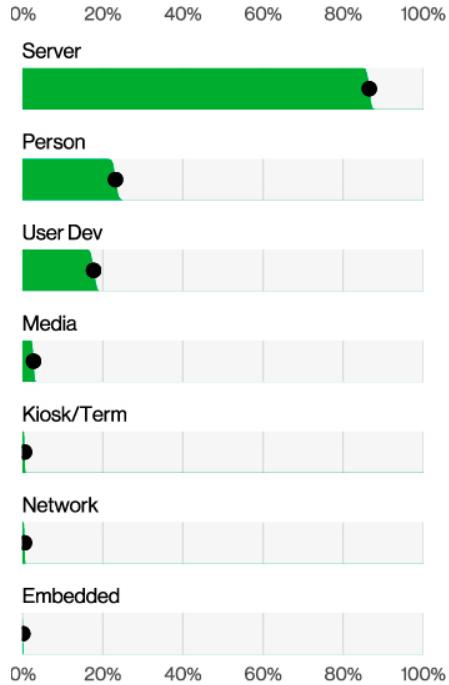


Figure 19. Assets in breaches
(n=4,433)

Figure 19 has the breakdown of varieties of Assets affected in breaches, and the results are pretty much what would be expected given the focus of System Intrusion, Basic Web Application Attacks and Social Engineering as the top attack patterns this year.

We can see a small fluctuation on the top three, as slightly less Servers were affected and slightly more User devices, but this order has held true for at least a couple of years, ever since Person overtook the second spot. Don't forget that in VERIS, people are assets too,¹⁹ and they are the "where" that is affected by social threat actions.

Asset categories²⁰

Server (srv): a device that performs functions of some sort supporting the organization, commonly without end-user interaction. Where all the web applications, mail services, file servers and all that magical layer of information is generated. If someone has ever told you "the system is down," rest assured that some Servers had their Availability impacted. Servers are common targets in almost all of the attack patterns, but especially in our System Intrusion, Basic Web Application Attacks, Miscellaneous Errors and Denial of Service patterns.

Person (per): the folks (hopefully) doing the work at the organization. No AI chat allowed. Different types of

Person will be members of different departments and will have associated permissions and access in the organization stemming from this role. At the very least they will have access to their very own User device and their own hopes and dreams for the future. Person is a common target in the Social Engineering pattern.

User device (usr): the devices used by Persons to perform their work duties in the organizations. Usually manifested in the form of laptops, desktops, mobile phones and tablets. Common target in the System Intrusion pattern but also in the Lost and Stolen Asset pattern. People do like to take their little computers everywhere.

Network (net): not the concept, but the actual network computing devices that make the bits go around the world, such as routers, telephone and broadband equipment, and some of the traditional in-line network security devices, such as firewalls and intrusion detection systems. Hey, Verizon is a Telecommunications company, OK?

Media (med): precious diluted data in its most pure and crystalline form. Just kidding, mostly thumb drives and actual printed documents. You will see the odd full disk drive and actual physical payment cards from time to time, but those are more rare. Common in the Lost and Stolen Assets pattern.

18 However, not caring for them properly could cause liabilities that would go on the right side.

19 Just ask your organization's HR department.

20 <https://verisframework.org/assets.html>

Breaking the Asset varieties down further in Figure 20 showcases Web application and Mail servers on top, as would be expected, but it is interesting to see Person - Finance trending up from last year as we see a related growth in Pretexting social actions. We will be discussing those, and more specifically BECs, in the “Social Engineering” section of this report.

As a parting note, we continue to see very small numbers of incidents involving Operational Technology (OT), where the computers interface with heavy machinery and critical infrastructure, as contrasted with incidents involving Information Technology (IT), where we keep our cat pictures and internet memes. Industries like Manufacturing and Mining, Quarrying and Oil & Gas Extraction + Utilities²¹ continue to be relatively well-represented in our dataset, but reports of actual impact on OT devices are still too few for us to meaningfully write about in this report.

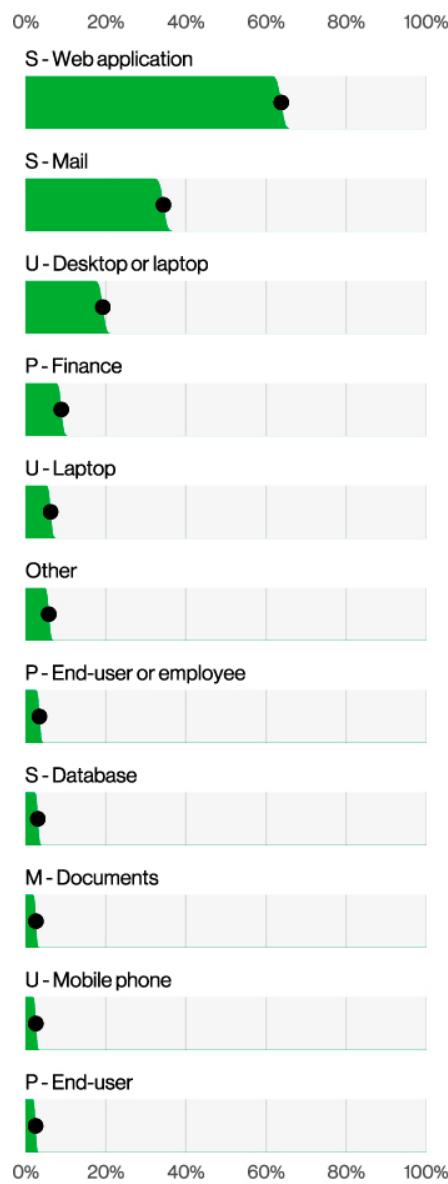


Figure 20. Top Asset varieties in breaches (n=3,207)

For those keeping track, we had a 3.4% showing of OT assets in breaches that declared their impact. In summary – keep your attention level high, given the potential impact when those systems are affected, but either those numbers are very low overall, or they just don’t make it to our contributors’ dataset due to national²² security concerns.

21 We know, it's a mouthful.

22 From any country really.

Attributes

When VERIS describes Attributes, it is directly referencing the CIA triad in information security (InfoSec): Confidentiality, Integrity and Availability. It's a tried-and-true method of understanding the potential impact of an incident by describing what properties of the asset were potentially affected.

Attribute categories²³

Confidentiality (cp): refers to limited observation and disclosure of an asset (or data). A loss of confidentiality implies that data were actually observed or disclosed to an unauthorized actor rather than endangered, at-risk or potentially exposed (the latter fall under the attribute of Possession and Control). Short definition: limited access, observation and disclosure.

Integrity (ia): refers to an asset (or data) being complete and unchanged from the original or authorized state, content and function. Losses to integrity include unauthorized insertion, modification and manipulation. Short definition: complete and unchanged from original.

Availability (au): refers to an asset (or data) being present, accessible and ready for use when needed. Losses to availability include destruction, deletion, movement, performance impact (delay or acceleration) and interruption. Short definition: accessible and ready for use when needed.

The next time you meet an incident responder in the wild, know that all that goes through their mind is, "Did the asset or a copy of the data get out the door" (Confidentiality), "was it changed from a known and trusted state" (Integrity) and "do we still have access to it ourselves?" (Availability). Please offer them a word of kindness and a beverage, because it is a very tortured existence. If you are feeling cold, they are cold too.

One of the most interesting Attribute varieties we track year over year is the Confidentiality data varieties (Figure 21), or what kinds of data got out in a breach. Personal data represents Personally Identifiable Information (PII) from your customers, partners or employees, and it is the one that usually gets companies the most in trouble with regulators, as more and more privacy-related laws are passed around the world (although Medical data is a whole other ball of earwax).

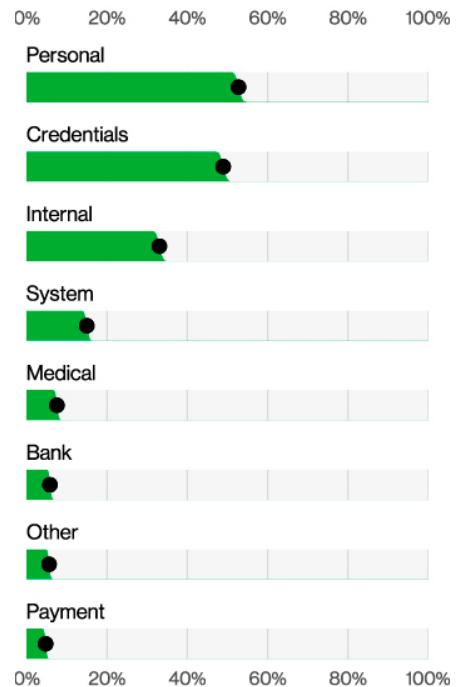


Figure 21. Top Confidentiality data varieties in breaches (n=5,010)

Virtual money, real problems

One data variety really caught the DBIR team's attention this year: Virtual currency. We saw a fourfold increase this year in the number of breaches involving cryptocurrency from last year. That is a far cry from the days of innocence in 2020 and earlier, when we got one or two cases maximum each year. If our cartoon animal NFTs had these kinds of returns, we can assure you we would be living large and writing this report from our Lambos, not from our parents' basements.²⁴

Figures 23 and 24 show the top action varieties and vectors in breaches involving virtual currency, and it is a fierce competition between Exploit vulnerabilities, Use of stolen creds and Phishing. These types of breaches

23 <https://verisframework.org/attributes.html>

24 Our Lambos might be parked in our parent's garage, though.

Internal data and System data are usually byproducts of an extensive breach with multiple steps, as information from emails and documents are vacuumed up by threat actors. Credentials have really gained ground over the past five years, as the Use of stolen credentials became the most popular entry point for breaches.

Of course, we still get specific data being beset, such as Medical, Bank account information and Payment card data. Those could be specific, targeted events or just be a part of the data that is acquired during a ransomware attack with data exfiltration. And just in case you are not tired of us moaning about ransomware,²⁵ please enjoy Figure 22, where we can see another impact of the ransomware growth as the Obscuration of data became the most common availability impact variety, handily overcoming plain old Loss of data.

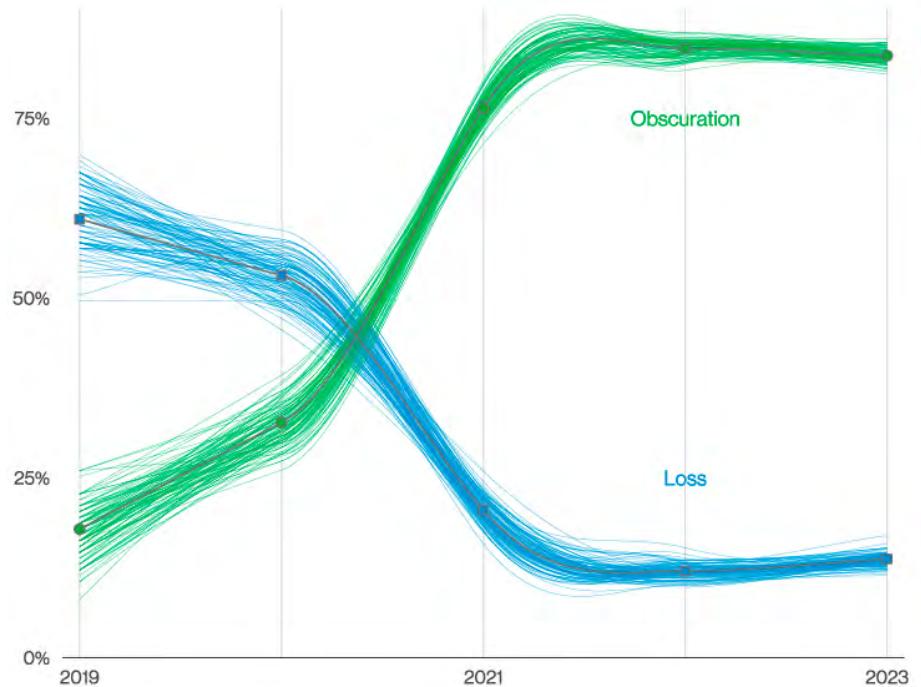


Figure 22. Availability variety over time

fall between the actual coin networks or exchanges being breached via their applications and application programming interfaces (APIs), or phishing and pretexting activity on chat platforms (like Discord) of the coin communities, where after a simple click on a link, suddenly your wallet is not yours anymore.

Having assets in virtual currency is a risky endeavor at best, even when there are no bad actors involved in rug-pulling.²⁶ The added focus of threat actors on these types of assets doesn't make the landscape any easier. Our parting message is that unless security is taken seriously in those cases, we, in fact, are not going to make it.

25 We're not bitter; you're bitter.

26 That rug really tied the room together, man!

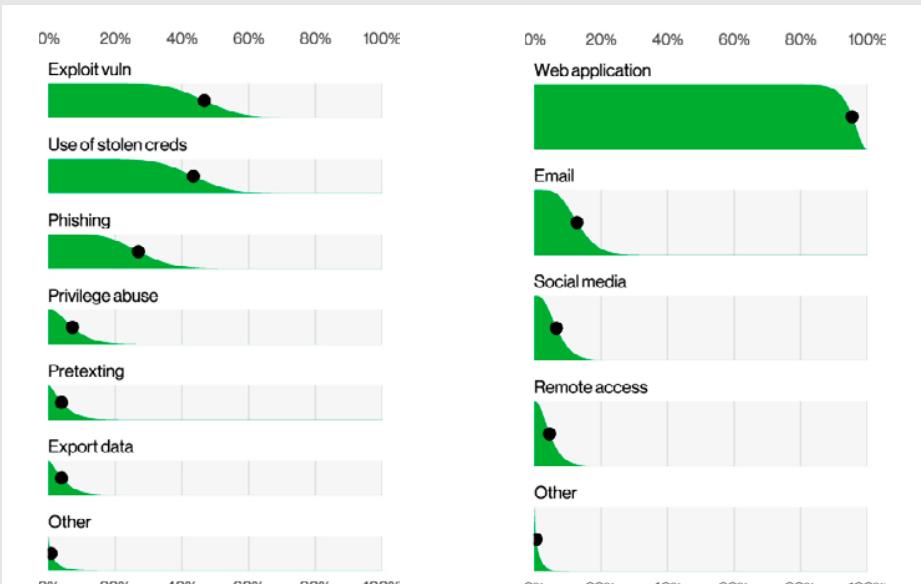


Figure 23. Top Action varieties in breaches where virtual currency was involved (n=30)

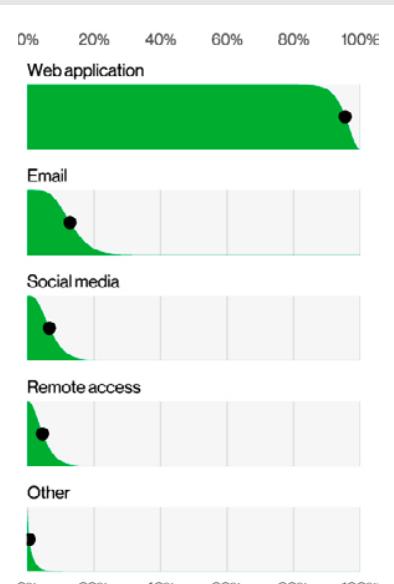


Figure 24. Top Action vectors in breaches where virtual currency was involved (n=48)

System Intrusion

Summary

This pattern largely pertains to attacks perpetrated by more dedicated criminals who utilize their expertise in hacking and ready access to malware to breach and/or impact organizations of different sizes, frequently leveraging Ransomware as their means of getting a payday.

What is the same?

Ransomware continues to dominate this pattern as attackers leverage a bevy of different techniques to compromise an organization.

Frequency	3,966 incidents, 1,944 with confirmed data disclosure
Threat actors	External (96%), Internal (4%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (97%), Espionage (3%) (breaches)
Data compromised	Other (42%), Personal (34%), System (31%), Internal (24%) (breaches)

This is mine, and this is mine ...

Imagine strolling into your office one morning only to discover an alarming desktop image from some criminal group with a cringeworthy name requesting Bitcoin (BTC) in exchange for the return of all your data. Hopefully, being the avid DBIR reader you are, you would have recent and well-tested backups to restore from. However, what if these criminals do not stop at only encrypting your data but also threaten to leak portions of your more sensitive information unless paid? Oftentimes it appears that no matter how fast our defenses and practices evolve, attackers adapt theirs just as quickly.

Relevant ATT&CK techniques

Exploit vuln (VERIS)

Exploitation for Privilege Escalation: T1068

Exploit Public-Facing Application: T1190

Exploitation for Defense Evasion: T1211

Exploitation for Credential Access: T1212

Exploitation of Remote Services: T1210

External Remote Services: T1133

Vulnerability Scanning: T1595.002

Use of stolen creds (VERIS)

Compromise Accounts: T1586
– Social Media Accounts:
T1586.001
– Email Accounts: T1586.002

External Remote Services: T1133

Remote Services: T1021
– Remote Desktop Protocol:
T1021.001

Use Alternate Authentication Material: T1550
– Web Session Cookie:
T1550.004

Valid Accounts: T1078
– Default Accounts: T1078.001
– Domain Accounts: T1078.002
– Local Accounts: T1078.003
– Cloud Accounts: T1078.004

Execution: TA0002

Persistence: TA0003

Privilege Escalation: TA0004

Defense Evasion: TA0005

Credential Access TA0006

This creates a perpetual arms race, and nowhere is it better represented than in the System Intrusion pattern.

We frequently think of the threat actors in this pattern as the “hands on keyboard” type of attackers. While they might leverage automation to gain a foothold, once they are inside the organization, they utilize finely honed skills to bypass controls and achieve their goals. As Figure 28 illustrates, this commonly includes Ransomware. They use a variety of tools to traverse your environment and then pivot, including using phishing and stolen credentials to obtain access and adding backdoors to maintain that access and leverage vulnerabilities to move laterally. We can see these attacks more clearly when we break them into three smaller, more consumable portions. Namely, the initial access phase, the breach escalation and the results. Figure 27 has a breakdown of the Action-Asset combinations that we see during different steps of the attack.

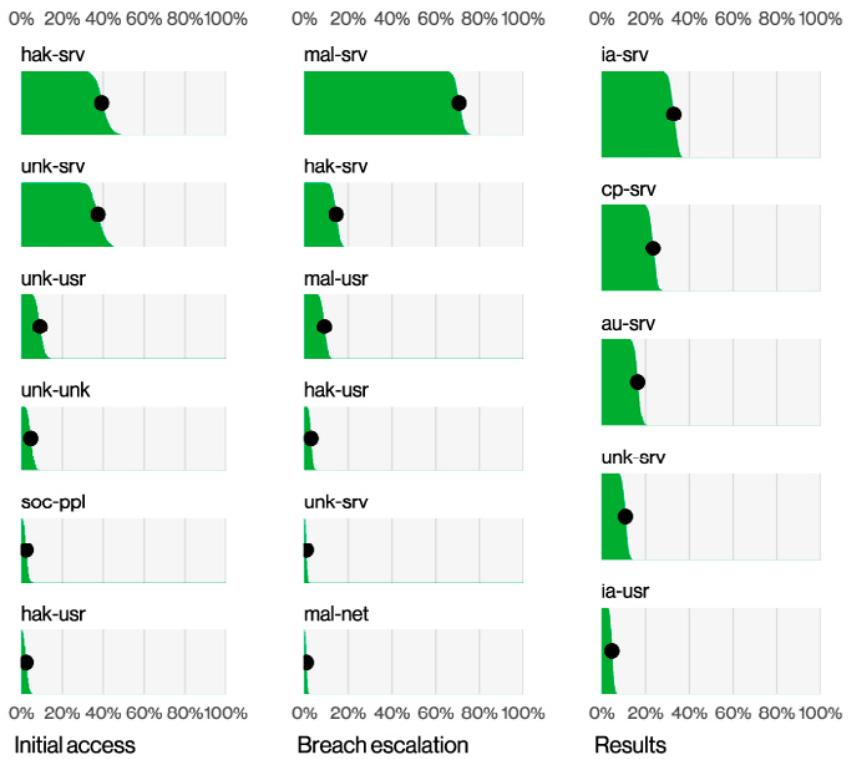


Figure 27. Steps in System Intrusion breaches

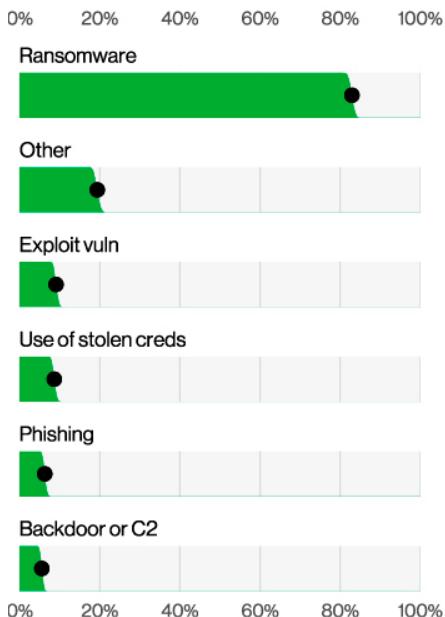


Figure 28. Action varieties in System Intrusion incidents (n=2,700)

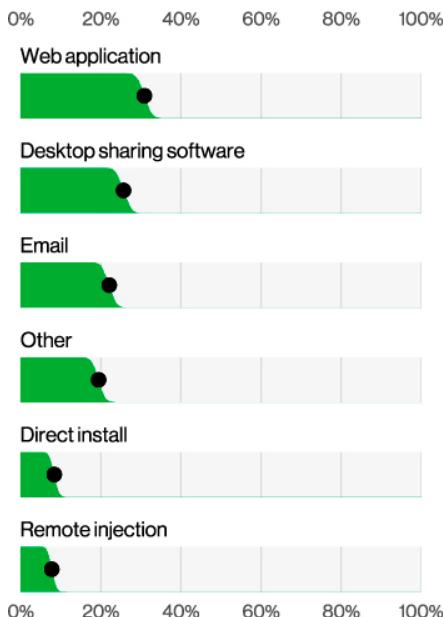


Figure 29. Action vectors in System Intrusion incidents (n=787)

Jiggling locks

When looking at Figure 27, we see the clear leaders for the initial access—a great deal of hacking servers and an almost equal amount of unknown actions. In terms of hacking, 9% of incidents involve Exploiting vulnerabilities and 8% involve the Use of stolen credentials. When we examine only our incidents that contain the exploitation of vulnerabilities, we find those vulnerabilities are largely exploited via Web applications (Figure 29).

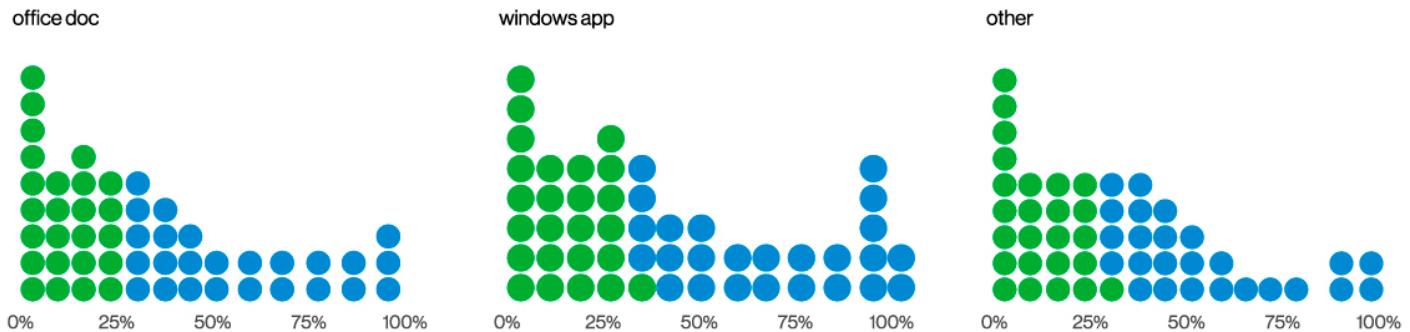
In addition, we see some User devices being directly targeted, and we also observe Phishing in roughly 6% of cases. Phishing provides just another means of ingress, either to get a set of usable credentials or to deploy a payload on a user system. Malware is largely distributed via email and often comes in the form of Microsoft Office documents (see Figure 30). This makes sense when you consider that most of these documents now have the ability to run code on the client system, which is extremely useful if you're an attacker.

Admittedly, there are many cases in which we do not know the exact means of entry the attacker used. However, these pathways of Exploiting vulnerabilities, Using stolen credentials and Phishing are very similar to previous years' findings, and let's face it, they are straight out of InfoSec 101. This again demonstrates the importance of the fundamentals.

Well, that escalated quickly.

Once attackers have access to your environment, they will typically look for ways to escalate privileges, maintain persistence and locate paths to move across the organization to achieve their ultimate goal, whatever that may be. For those ATT&CK aficionados out there, you may be thinking this

Malware file types (n=1,756)



Malware delivery methods (n=1,069)

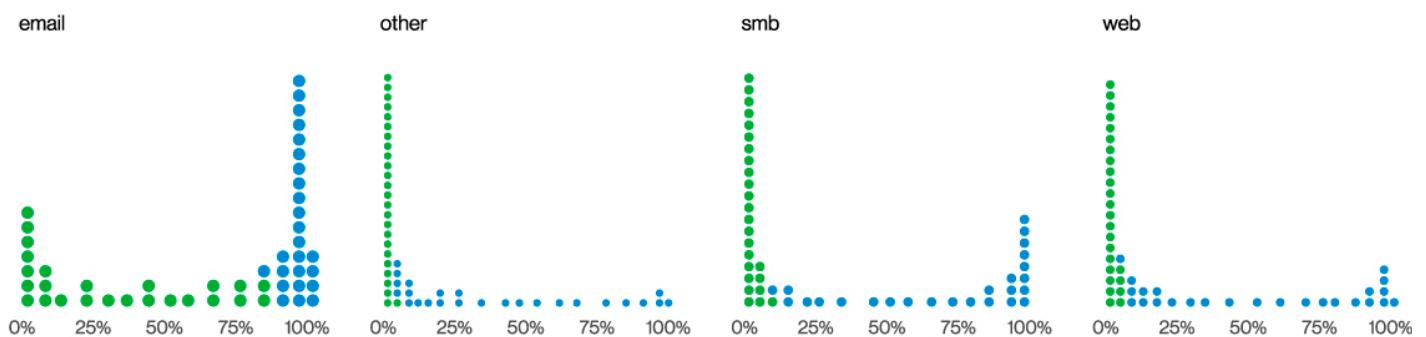


Figure 30. Malware delivery method proportion per organization

sounds like we're talking about a big chunk of that matrix. Well, we are. While we have a higher view of the incidents, we do not always have the telemetry required to find out exactly what techniques were used. However, below we discuss some of the additional hacking techniques and malware capabilities that we can track.

Malware that maintains command and control (C2) access to the system was witnessed in about 5% of incidents. Also present are the more typical types of malware that profile hosts, scan networks and (a local favorite) dump passwords. Lastly, just in case you thought the 2010s were behind us, we even found a handful of crypto miners in this dataset. There were not enough for us to confirm that they are back en vogue, but definitely enough to confirm that certain parties still consider compromised servers as free real estate from which to mine.

Results

With such a high reliance upon the installation of malware across this pattern (either in the form of Ransomware, backdoors or payment card skimming malware) we shouldn't be too surprised when we find servers that have illicit software installed as the most common combination of Attribute and Asset. The second most common is the exfiltration of data, and rounding out the trio is the loss of availability, aka rendering your data unreadable. These top three describe the final steps associated with many of these attacks quite well—attackers find a way to install their payload across the organization, steal data and then encrypt the systems on their way out.

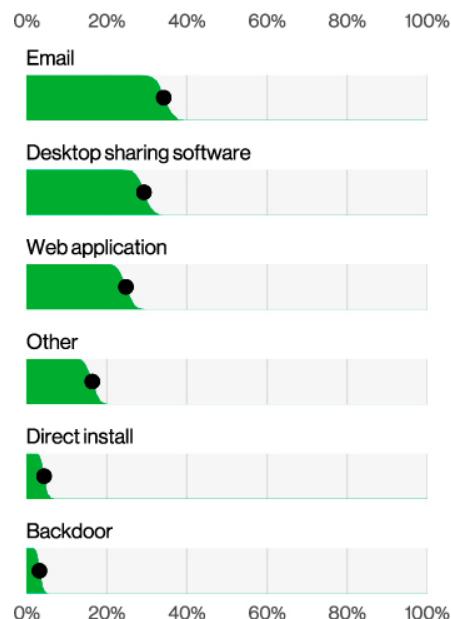


Figure 31. Action vectors for Ransomware (n=690)

Ransomware ... seriously, we're still doing this section?

Ransomware continues to be a major threat for organizations of all sizes and industries and is present in 24% of breaches. Of those cases, 94% fall within System Intrusion. While Ransomware has increased only slightly this year, it is so ubiquitous that it may simply be a threat that we will always have to protect against—91% of our industries have Ransomware as one of their top three actions.

To understand how these attacks occur, it is often useful to look at the top Vectors for the actions. In this case, the most common ways in are Email, Desktop sharing software and Web applications (Figure 31). Email as a vector isn't going away any time soon. The convenience of sending your malware and having the user run it for you makes this technique timeless. The next most common vector, Desktop sharing software, makes sense, since these breaches and incidents frequently leverage some means of accessing a system. What better way to do that than by using a built-in tool such as RDP or a third-party version to provide the criminal mastermind a nice GUI?

Social Engineering

Summary

Social Engineering incidents have increased from the previous year largely due to the use of Pretexting, which is commonly used in BEC, almost doubling since last year. Compounding the frequency of these attacks, the median amount stolen from these attacks has also increased over the last couple of years to \$50,000.

What is the same?

Phishing and Pretexting continue to dominate this pattern, thus ensuring that email remains one of the most common means of influencing individuals.

Professional engineers?

Engineering is a beautiful combination of math and physics applied to a practical and meaningful end—or so we're told. However, much to our parents' disappointment, most of us are not engineers, but only an infinite collection of monkeys tied to typewriters. (Legend has it we will compose "Hamlet" by pure chance any day now. Watch your back, GPT-4.)

Frequency	1,700 incidents, 928 with confirmed data disclosure
Threat actors	External (100%), Multiple (2%), Internal (1%), Partner (1%) (breaches)
Actor motives	Financial (89%), Espionage (11%) (breaches)
Data compromised	Credentials (76%), Internal (28%), Other (27%), Personal (26%) (breaches)

However, this section is about another, not-so-useful-to-society, form of engineer—the social engineer. This pattern focuses on tactics used by threat actors that leverage our innate helpful nature to manipulate and victimize us. These attackers use a combination of strategies to accomplish this: by creating a false sense of urgency for us to provide a reply or to perform an action, a fake petition from authority, or even hijacking existing communication threads to convince us to disclose sensitive data or take some other action on their behalf. Social engineering has come a long way from your basic Nigerian Prince scam to tactics that are much more difficult to detect. This increased sophistication explains why Social Engineering continues to rise and currently resides in our top three patterns (accounting for 17% of our Breaches and 10% of Incidents).

Relevant ATT&CK techniques

Compromise Accounts: T1586
– Email Accounts: T1586.002
Establish Accounts: T1585
– Email Accounts: T1585.002
External Remote Services: T1133
Internal Spearphishing: T1534
Phishing: T1566
– Spearphishing Attachment: T1566.001
– Spearphishing Link: T1566.002
– Spearphishing via Service: T1566.003
Phishing for Information: T1598
– Spearphishing Service: T1598.001
Use Alternate Authentication Material: T1550
– Application Access Token: T1550.001
Valid Accounts: T1078
– Domain Accounts: T1078.002

Please use this bank account number going forward.

There is a common misconception when it comes to distinguishing phishing from the more complex forms of social engineering. Raise your hand if you haven't received an email with a dubious attachment or a malicious link requesting that you update your password. Nobody? Yeah, that's what we thought. This is phishing, and it makes up 44% of Social Engineering incidents. Now, who has received an email or a direct message on social media from a friend or family member who desperately needs money? Probably fewer of you. This is social engineering (pretexting specifically) and it takes more skill. The most convincing social engineers can get into your head and convince you that someone you love is in danger. They use information they have learned about you and your loved ones to trick you into believing the message is truly from someone you know, and they use this invented scenario to play on your emotions and create a sense of urgency. Figure 35 shows that Pretexting is now more prevalent than Phishing in Social Engineering incidents. However, when we look at confirmed breaches, Phishing is still on top.

One of the more complex social attacks is the BEC. In these pretexting attacks, actors leverage existing email threads and context to request that the recipient conduct a relatively routine task, such as updating a vendor's bank account. However, the devil is in the details, and the new bank account belongs to the attacker, so all payments the victim makes to that account will make zero dents in what they owe that vendor. These types of attacks are often much harder to detect due to the groundwork laid by the threat

actors prior to the attack. For example, they might have spun up a look-alike domain that closely resembles that of the requesting party and possibly even updated the signature block to include their number instead of the vendor they're pretending to represent. These are just two of the numerous subtle changes that attackers can make in order to trick their marks—especially those who are constantly bombarded with similar legitimate requests. Perhaps this is one of the reasons BEC attacks have almost doubled across our entire incident dataset, as can be seen in Figure 36, and now represent more than 50% of incidents within this pattern.

Attack type doesn't appear to have much of an effect on click/open rate. The median fail rates for attachment and link campaigns are 4% and 4.7% respectively, and the median click rate for data entry campaigns is 5.8% (though the data entry rate is 1.6%).

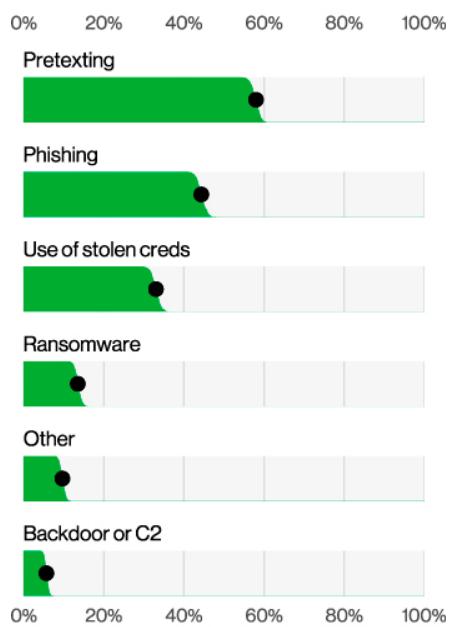


Figure 35. Action varieties in Social Engineering incidents (n=1,696)

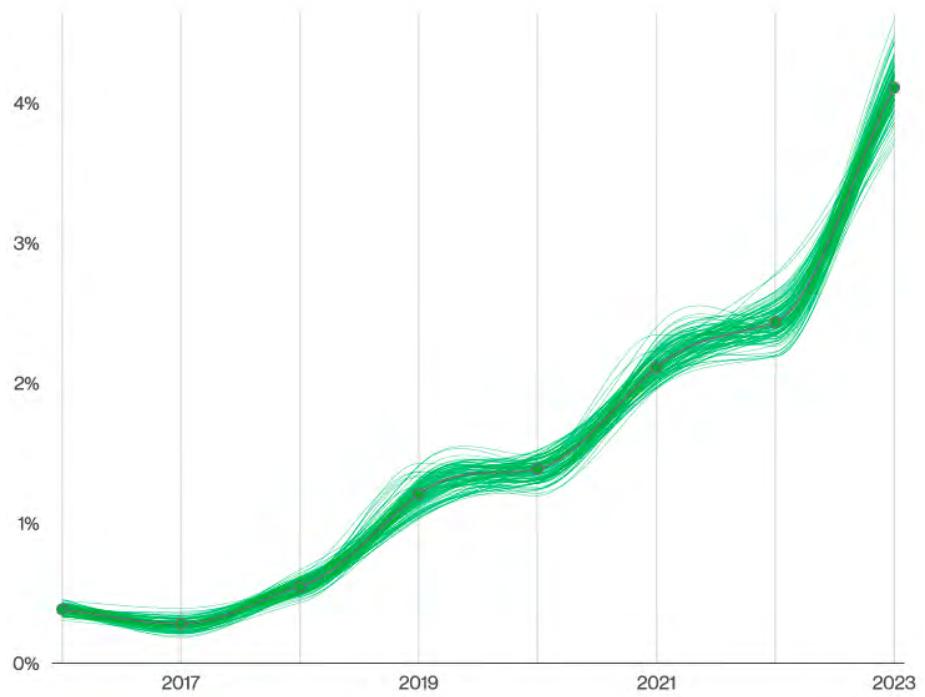


Figure 36. Pretexting incidents over time

Basic Web Application Attacks

Summary

While representing approximately one-fourth of our dataset, these breaches and incidents tend to be largely driven by attacks against credentials, with the attackers then leveraging those stolen credentials to access a variety of different resources.

What is the same?

Poorly picked and protected passwords continue to be one of the major sources of breaches within this pattern.

Who dunnit?

While it may liven up our humdrum existence to imagine the threat actors behind breaches as characters from a game of Clue (the cyber version),³⁷ it is more likely to have been an average Jane Doe using stolen credentials or some well-known vulnerability.

Frequency	1,404 incidents, 1,315 with confirmed data disclosure
Threat actors	External (100%), Internal (1%), Multiple (1%) (breaches)
Actor motives	Financial (95%), Espionage (4%), Fun (1%) (breaches)
Data compromised	Credentials (86%), Personal (72%), Internal (41%), Other (19%) (breaches)

This pattern, which accounts for 25% of our breaches, consists largely of leveraging stolen credentials and vulnerabilities to get access to an organizations' assets. With this beachhead, the attackers can then do a variety of things, such as stealing key information hiding in emails or taking code from repositories. While these attacks aren't complicated, they certainly are effective and have remained a relatively stable part of our dataset, which prompts us to discuss once again (drum roll, please), the importance of multifactor authentication (MFA) and patch management!³⁸

Relevant ATT&CK techniques

Brute Force: T1110
– Credential Stuffing: T1110.004
– Password Cracking: T1110.002
– Password Guessing: T1110.001
– Password Spraying: T1110.003

Compromise Accounts: T1586
– Email Accounts: T1586.002

Exploit Public-Facing Application: T1190

External Remote Services: T1133

Valid Accounts: T1078
– Default Accounts: T1078.001
– Domain Accounts: T1078.002

Use Alternate Authentication Material: T1550
– Application Access Token: T1550.001

Active Scanning: T1595
– Vulnerability Scanning: T1595.002

³⁷ Was the breach caused by the mysterious Spiderlady via a complicated zero day on an internet-facing server? Or was it perpetrated by the Sophisticated Panda using drones inside a Kubernetes cluster?

³⁸ Yes, it is the "Groundhog Day" of InfoSec topics. I bet you can find it in our past reports!

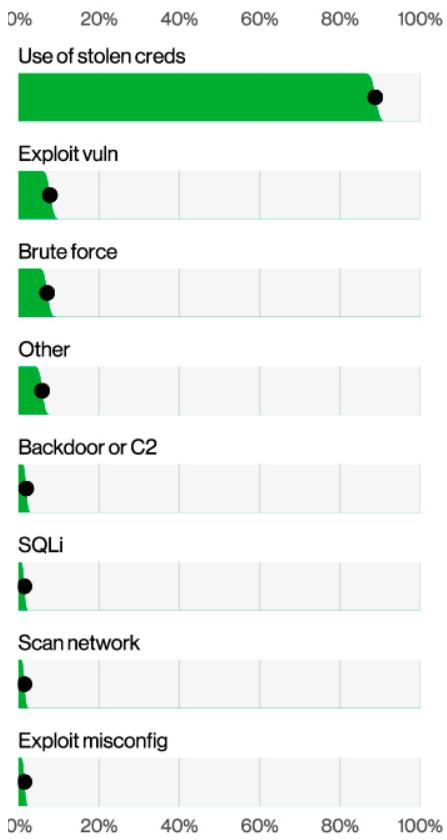


Figure 39. Top Action varieties for Basic Web Application Attacks breaches (n=1,287)

Initial access

86% of the breaches, as you can see in Figure 39, involve the Use of stolen credentials. And where better to use those credentials than against the various web servers that contain our sensitive information? The other major part of the puzzle within this pattern is the use of exploits. This is where attackers have an exploit and the victims just happen to have a vulnerability (handy for the criminal). This typically occurs in only about 10% of the dataset, and while that may sound like an insignificant number of breaches, unpatched vulnerabilities are still the bread and butter for many attackers, with 50% of organizations experiencing over 39 Web application attacks this year.³⁹

Breach escalation

Even though we refer to these attacks as “basic,” they’re not simply “one and done” incidents where credentials are leveraged against a web application and the attacker then goes on their merry way. There is often some sort of middle step (Figure 40). For instance, malware is frequently one of the primary means of maintaining persistence (look at us, using them fancy ATT&CK terms), with Backdoor or C2 in about 2% of the incidents. In other cases, the attackers will leverage their current access to conduct additional attacks.

³⁹ One of the advantages to running these types of attacks is that the server never tires, never sleeps, it just throws exploits at everyone continually, night and day – unlike your humble cybersecurity analyst who needs at least four coffees a day and nine hours of sleep.

Miscellaneous Errors

Summary

Misdelivery, Misconfiguration and Publishing errors continue to be the headliners, and the errors that lead to breaches are most often committed by System admins and Developers.

What is the same?

Employees continue to make mistakes, and sometimes they result in considerable damage to their organizations.

Frequency	602 incidents, 512 with confirmed data disclosure
Threat actors	Internal (99%), Partner (2%), Multiple (1%), External (1%) (breaches)
Data compromised	Personal (89%), Medical (19%), Other (10%), Bank (10%) (breaches)

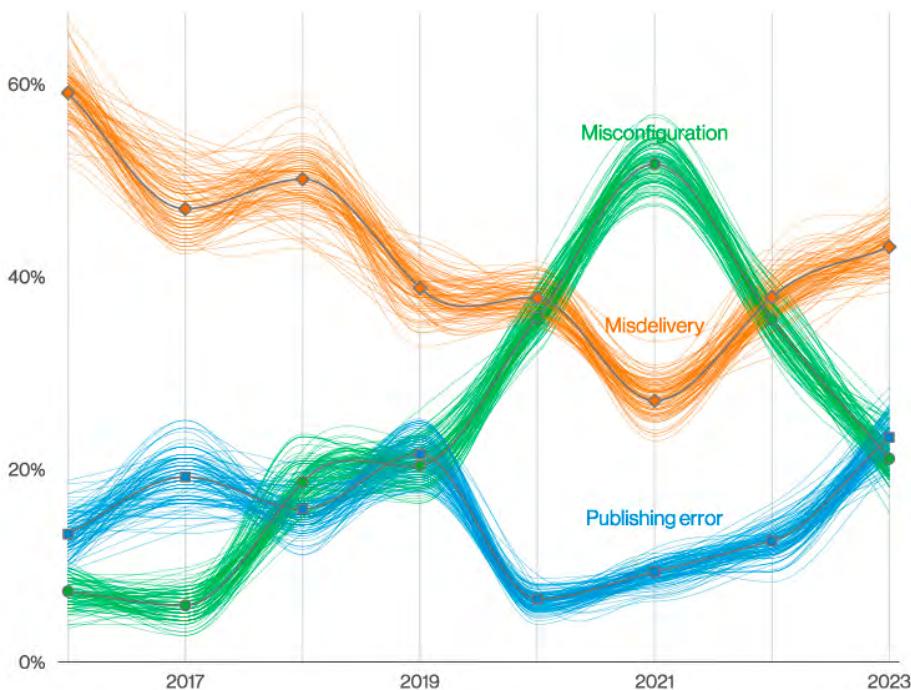


Figure 41. Action varieties over time in Miscellaneous Errors breaches

You can't find good help these days.

The great English poet and essayist, Alexander Pope once quipped, “It is hard to hire people who don’t screw things up.” Well, it was something more or less along those lines—just take our word for it. Regardless of who said (or did not say) what, the Miscellaneous Errors pattern continues to comprise a decent chunk of our breach data. If you are a “glass half full” kind of reader, you may take comfort in the fact that this year, error-related breaches are down to 9% as opposed to 13% last year. If you are a “glass half empty” reader, you may simply attribute it to reporting since last year we had 715 error incidents and 708 with confirmed data disclosure as opposed to 602 incidents, with 512 confirmed breaches this year.

It's my favorite mistake.

Perhaps “favorite” is too strong a word. Misdelivery (sending something to the wrong recipient) accounts for 43% of breach-related errors in our dataset (Figure 41). Publishing errors (showing something to the wrong audience) is in second place at 23%. Finally, Misconfiguration, the much-loved action type of the lazy person, comes in third and accounts for 21% of error-related breaches. This might tempt us to think that people are unreliable—perish the thought. However, you can rely on them to at least keep things interesting by switching up their mistakes to help keep you on your toes.

In fact, as Figure 41 illustrates, Misconfiguration and Misdelivery have ebbed and flowed over the last few years as if they were part of the choreographed dance of celestial bodies. In last year's report, Misdelivery and Misconfiguration converged, but this year Misdelivery is in the ascendancy,⁴² whereas our old faithful dog, the Publishing error, is once again meeting Misconfiguration on its downward slope.

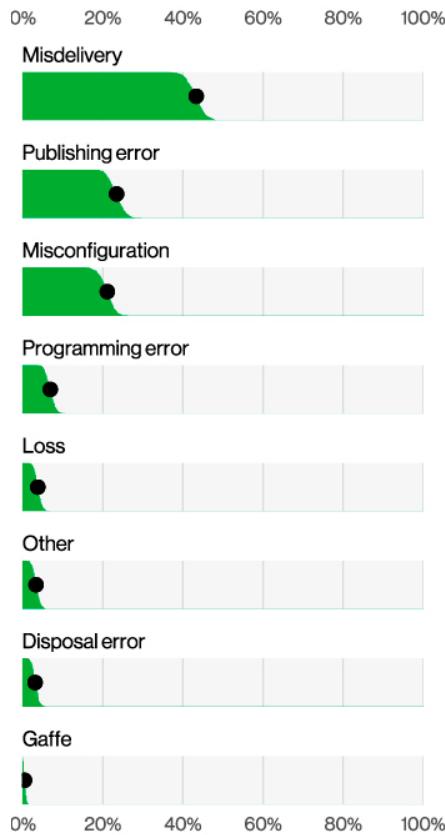


Figure 42. Top action varieties in Miscellaneous Errors breaches (n=450)

If we drill down a little deeper (Figure 42), it's easy to see that these three Error types have won the popularity contest by a wide margin. However, the team is saddened to see that Gaffe is always at or near the bottom (considering how many of those we make ourselves).

As illustrated in Figure 43, the majority of errors that lead to breaches are committed by Developers and System admins, along with a sprinkling of End-users. Given the Error action types that are most often found in breaches, it is hardly surprising that those who have more responsibility for maintaining the data and the upkeep of the environment are also those who are most frequently responsible. Speaking of responsibility, the error vector of Carelessness appeared in 98% of cases. Yikes! Maybe Pope was on to something.



Figure 43. Top actor varieties in Miscellaneous Errors breaches (n=89)

CIS Controls for consideration

Control data

Data Protection [3]

- Establish and Maintain a Data Management Process [3.1]
- Establish and Maintain a Data Inventory [3.2]
- Configure Data Access Control Lists [3.3]
- Enforce Data Retention [3.4]
- Securely Dispose of Data [3.5]
- Segment Data Processing and Storage Based on Sensitivity [3.12]
- Deploy a Data Loss Prevention Solution [3.13]

Secure infrastructure

Continuous Vulnerability Management [7]

- Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets [7.6]

Application Software Security [16]

- Use Standard Hardening Configuration Templates for Application Infrastructure [16.7]
- Apply Secure Design Principles in Application Architectures [16.10]

Train employees

Security Awareness and Skills Training [14]

- Train Workforce on Data Handling Best Practices [14.4]
- Train Workforce Members on Causes of Unintentional Data Exposure [14.5]

Application Software Security [16]

- Train Developers in Application Security Concepts and Secure Coding [16.9]

⁴²If you were born under the sign of Misdelivery you should expect good news soon. 3, 9, 13 and 33 are your lucky numbers.

Denial of Service

Summary

As Denial of Service continues to dominate our incidents, so do the capabilities of mitigation services. However, there has been a resurgence of low volume attacks that still cause issues to corporations.

What is the same?

Denial of Service attacks continue to be ubiquitous and have remained in the top spot of incidents for several years now.

Frequency	6,248 incidents, 4 with confirmed data disclosure
Threat actors	External (100%) (incidents)

We will not be denied.

As the name would imply, the Denial of Service pattern covers all of those attacks that try to keep you from streaming your next episode of "Below Deck," watching your next TikTok movie or loading your timeline on Twitter.⁴³ Sadly, all of this can obviously add up to the nuisance of having to acknowledge the real world and the people around us. We can all agree that would be terrible indeed.

However, as some of our readers may know, organizations still actually need the internet to be up and running in order to conduct business. Every year, DoS shows up as a huge volume of Incidents in our datasets, stemming from several different mitigation service partners, including Verizon's own. They are all doing an excellent job in preventing those Incidents from having any significant impact on organizations. In that light, even though the Denial of Service pattern has consistently taken the top spot in Incidents for the last several years (Figure 44), there is really not a lot of nuance to be discussed here, apart from our usual suggestion to invest in some sort of mitigation service if you care about the continued availability of your network presence on

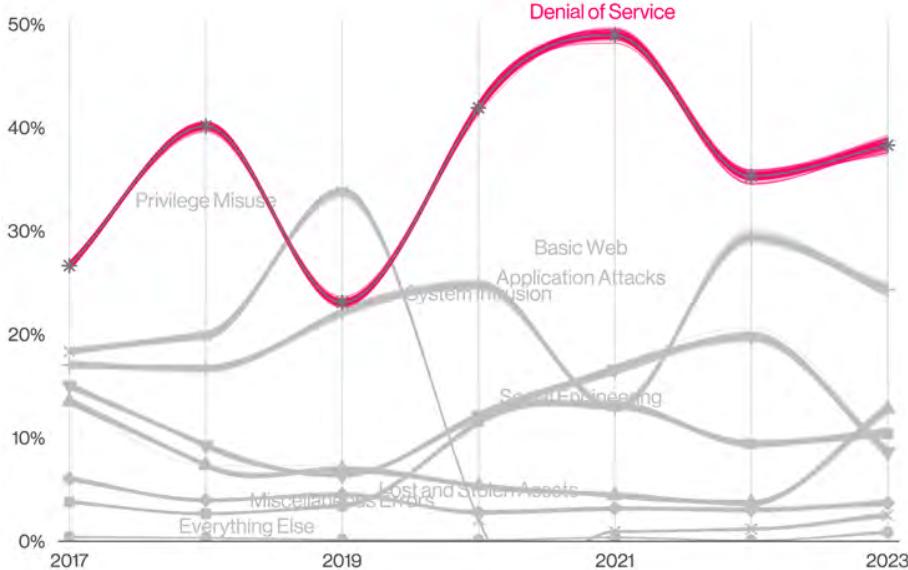


Figure 44. Patterns over time in incidents

⁴³ Not sure if we can blame our usual threat actors for this one.

the internet. This is not due to a lack of nuance in the DDoS dataset overall but more a reflection of a lack of the typical details that we traditionally analyze such as Actors, Assets and Attributes.

Even so, it didn't feel right to deny our readers a Denial of Service section, as there are still important trends and information that are necessary to be reviewed. It's important to realize they're still there, even if you can easily solve them. Also, it is a respite to not have to write about Ransomware for a couple of pages.

We are going to need a bigger pipe.

One important point we should touch on is the growth of median and above median percentiles in bits per second of DDoS attacks (see Figure 45).⁴⁴ The median grew a whopping 57%⁴⁵ from 1.4 gigabytes per second (Gbps) last year to 2.2 Gbps now, and the 97.5 percentile grew 25% from 99 Gbps to 124 Gbps. This is to be expected

as costs of bandwidth and CPU processing become more accessible and available and suggests a trend that is hard to break on escalating competition between the attackers and mitigating services. Just make sure your contracted service can clear that bar, and most of the impact will likely be absorbed. Let the machines fight it out Transformers-style and crack open a cold beverage while you worry about all the other attack patterns afflicting your corporation.

Even as the volume of garbage in our networks grows, some attacks have a more subtle touch. A point of attention that some of our partners brought to us was the growth of distributed DNS Water Torture⁴⁶ attacks in, you guessed it, shared DNS infrastructure. It is basically a resource exhaustion attack done by querying random name prefixes on the DNS cache server so it always misses and forwards it to the authoritative server. It is quite silly when you think of it, but it can be a heavy burden with some simple coordination by the threat actors'-controlled devices. Make sure to check on your DNS infrastructure resiliency and check for options with your mitigation service as well to make sure you are protected against these attacks too.

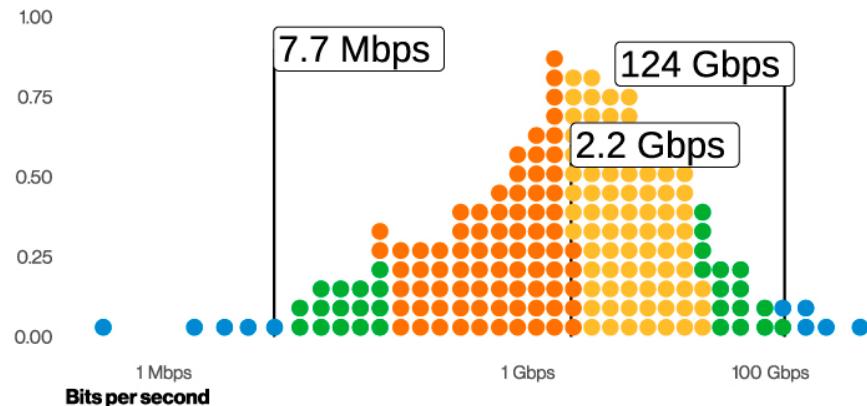


Figure 45. Bits per second in DDoS incidents (n=10,622)

⁴⁴ Be sure to discuss this at parties. You'll be wildly popular.

⁴⁵ I bet you thought our inflation numbers in the U.S. were bad, huh?

⁴⁶ This is NOT a subtle name!

Lost and Stolen Assets

Summary

This pattern continues to be a problem for organizations because these small (and not so small) devices are just so portable. We've seen their capacity to store large amounts of data increase over time, while employees' ability to misplace them (or External actors to steal them) remains predictably common.

What is the same?

Devices and media are still more likely to be lost by Internal actors than stolen by External ones.

Frequency	2,091 incidents, 159 with confirmed data disclosure
Threat actors	External (92%), Internal (68%), Multiple (60%), Partner (1%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Personal (87%), Medical (30%), Other (21%), Bank (13%) (breaches)

Where go my laptop?

The headline in this pattern is "Your stuff is gone," which isn't really a news flash. Whether the missing item(s) had "help" in the form of someone stealing a laptop, or was accidental, as in classified printed documents being mislaid in high-level government officials' residences, the more portable an asset is, the more it needs protection against loss and theft.

This is a pattern where we see a high percentage of incidents not resulting in confirmed data breaches—largely because the status of confidentiality disclosure remains "at-risk" rather than "confirmed" due to the loss of custody of the asset in question. The exception is printed material, since no controls exist to shield documents from view once printed. Similar to last year, we again have less than 10% of the incidents as confirmed data breaches.

While stolen devices certainly represent a risk to organizations, employees are much more likely to cause a breach accidentally through loss. This fact has held true year over year on a consistent basis, as shown in Figure 46.

What is going missing, you may ask? Unsurprisingly, it's the portable user devices, such as laptops, and mobile phones. In fact, phones have become quite the commodity (Figure 47). Considering the fact that no one ever seems to put them down, it's hard to believe so many are lost.

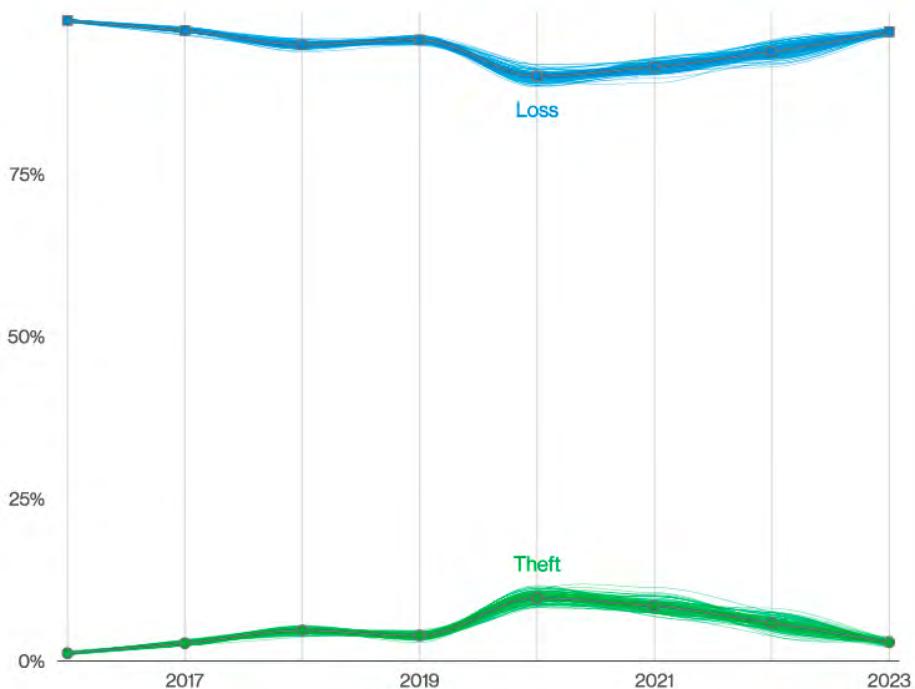


Figure 46. Top Action varieties in Lost and Stolen Assets incidents

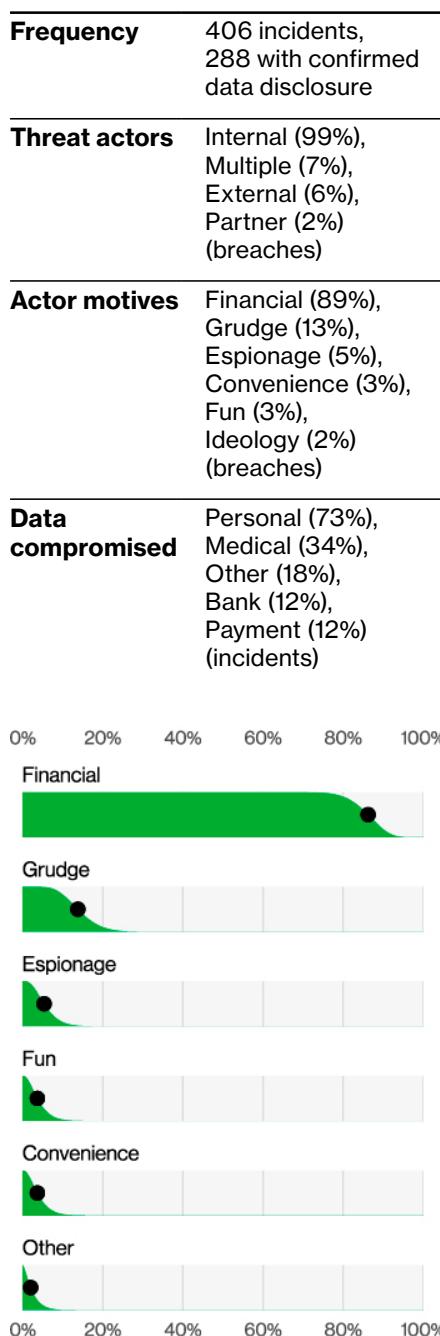
Privilege Misuse

Summary

Your employees continue to use their access to commit breaches and, in some cases, initiate fraudulent transactions. We saw more collusion between multiple types of actors this year.

What is the same?

This pattern continues to be dominated by the Internal actor, by definition. Most are motivated by financial gain, and Personal data continues to be a favorite target.



My employees love me!

People may think they are somehow immune to a data breach. They may put their trust in their security controls, thinking they have amazing, impenetrable defenses. They may put their trust in “flying under the radar” or believe they are too small to have a breach. But this kind of thinking largely assumes breaches come from the outside, from the “bad actors” that are external to the organization. What they fail to take into account is the risk of an insider breach. “Surely, MY people wouldn’t do that!” they say. But of course, they would—and don’t call me Shirley.

The hard fact to face is that some of our employees also cause data breaches for malicious reasons. The most common nonaccidental Internal actor breach is Privilege abuse. This is just what it sounds like—employees abusing the access they have been given to do their jobs to steal data instead. They are significantly more likely to do this for their own financial gain (Figure 48). We know, it’s a shocker.

Figure 48. Internal actor motives in Privilege Misuse breaches (n=59)

Industry	Incidents				Breaches			
	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	16,312	694	489	15,129	5,199	376	223	4,600
Accommodation (72)	254	4	2	248	68	4	1	63
Administrative (56)	38	8	14	16	32	8	11	13
Agriculture (11)	66	1	5	60	33	0	3	30
Construction (23)	87	7	1	79	66	4	1	61
Education (61)	496	63	15	418	238	28	8	202
Entertainment (71)	432	13	3	416	93	10	1	82
Finance (52)	1,829	70	30	1,729	477	38	18	421
Healthcare (62)	522	28	15	479	433	23	15	395
Information (51)	2,105	45	110	1,950	380	23	19	338
Management (55)	9	1	0	8	9	1	0	8
Manufacturing (31–33)	1,814	37	24	1,753	259	18	15	226
Mining (21)	25	2	0	23	13	2	0	11
Other Services (81)	143	7	2	134	100	6	1	93
Professional (54)	1,396	176	54	1,166	421	85	32	304
Public Administration (92)	3,270	87	110	3,073	582	48	39	495
Real Estate (53)	83	15	5	63	59	10	2	47
Retail (44–45)	404	62	44	298	191	33	28	130
Transportation (48–49)	349	13	25	311	106	8	13	85
Utilities (22)	117	12	6	99	33	3	3	27
Wholesale Trade (42)	96	42	22	32	53	23	11	19
Unknown	2,777	1	2	2,774	1,553	1	2	1,550
Total	16,312	694	489	15,129	5,199	376	223	4,600

Table 2. Number of security incidents and breaches by victim industry and organization size

Accommodation and Food Services

NAICS
72

Frequency	254 incidents, 68 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 90% of breaches
Threat actors	External (93%), Internal (9%), Multiple (1%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Payment (41%), Credentials (38%), Personal (34%), Other (26%) (breaches)
What is the same?	We are seeing the same three attack patterns hitting this sector as we did last year—but the order has changed. External actors continue to target this industry because of the lucrative data the members hold.

Summary

Payment card data continues to be the top target for Data types in this sector, unsurprisingly. The use of RAM scrapers continues to be a favorite tool of the Financially motivated attackers that regularly plague this sector.

I'll just scrape that off.

System Intrusion is the top pattern in this sector for the second year running. Included in this pattern, among other things, is a collection of various types of malware. Approximately one-third of cases involved the use of Ransomware, and much of the remainder consisted of RAM scrapers. In fact, RAM scrapers targeting the PoS is the favorite combo in this sector, which likely comes as no surprise to those trying to maintain their defenses.

Payment card data was targeted 41% of the time, which is the same percentage we saw last year, but since Credentials and Personal data fell as a proportion of the whole, they have taken a back seat to credit cards. Along with the increased focus on the data type of Payment cards comes the motivation of Financial. Last year, we saw the Espionage motive in 9% of the breaches, but this year, it is all Financial all the time.⁴⁸

Give a person a phish and you feed them for a day!

Social continues to have a considerable presence in this sector. While Phishing and Pretexting (the main difference between them is how hard the adversary must work to make it happen) are the main social engineering concerns in Accommodation, they are too close to call for the top spot. Most of these social attacks are coming in via email, so make sure it is easy for your employees to report any questionable attempt quickly. There is nothing like having your employees be your first line of defense—they are certainly already on the front line of targets.

⁴⁸Honestly, what isn't though?

Educational Services

NAICS
61

Frequency	497 incidents, 238 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Social Engineering represent 76% of breaches
Threat actors	External (72%), Internal (29%), Multiple (1%), Partner (1%) (breaches)
Actor motives	Financial (92%), Espionage (8%), Convenience (1%), Fun (1%) (breaches)
Data compromised	Personal (56%), Credentials (40%), Other (25%), Internal (20%) (breaches)
What is the same?	System Intrusion and Miscellaneous Errors are yet again two of the top three patterns for this industry. The ratio of External and Internal actors is nearly the same as last year.

Summary

Basic Web Application Attacks dropped out of the top three to be replaced by Social Engineering. Ransomware continues to play a large role in breaches in this vertical.

Who saw that coming?

In a move that shocked faculty, staff and students alike, last year's much lauded salutatorian, Basic Web Application Attacks, has dropped out (of the top three patterns). Miscellaneous Errors is still present (isn't it always?) and has increased slightly from last year. As you may have guessed, these errors are the usual suspects: Misdelivery, Publishing errors and Misconfiguration.

Social Engineering clawed its way to the number three position, increasing from 14% last year to 21% in 2023 (Figure 52). This rise is primarily represented by Phishing attacks, which showed up in 18% of breaches, and Pretexting scenarios (4%).

Hacking was present in 40% of breaches, with the Use of stolen credentials appearing in 31% of them. Not to be outdone, Malware also showed up in 40% of breaches, with Ransomware present in 30% of those breaches. Let's review that finding for the exam: Ransomware was responsible for almost one-third of all breaches in the Educational Services vertical. In spite of this impressive showing from both Hacking and Malware, the System Intrusion pattern, while maintaining its number one spot, decreased slightly from last year.

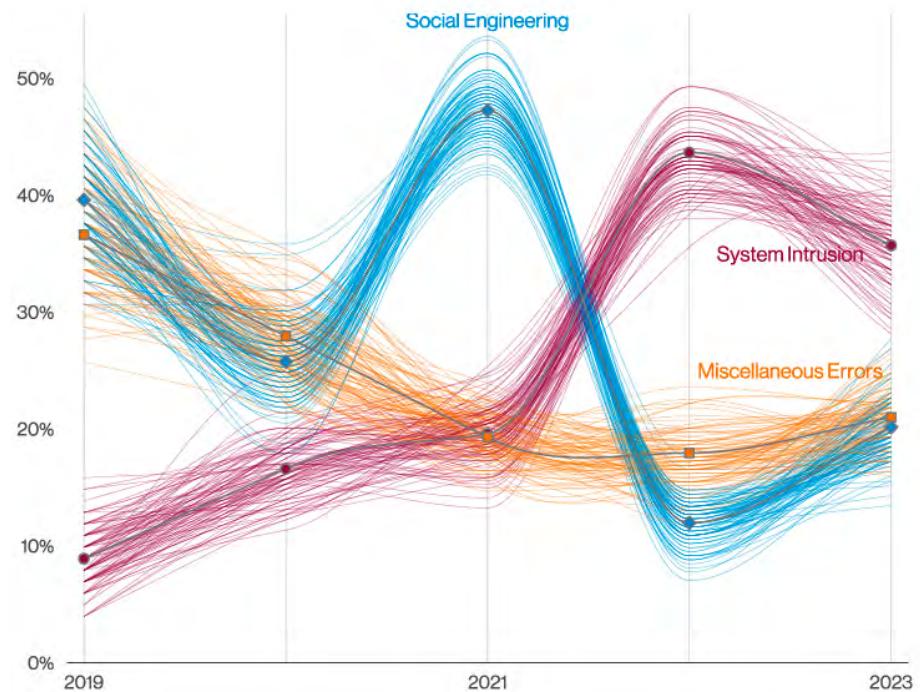


Figure 52. Patterns in Education breaches

Financial and Insurance

NAICS
52

Frequency	1,832 incidents, 480 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 77% of breaches
Threat actors	External (66%), Internal (34%), Multiple (1%) (breaches)
Actor motives	Financial (97%), Espionage (3%), Convenience (1%), Ideology (1%) (breaches)
Data compromised	Personal (74%), Credentials (38%), Other (30%), Bank (21%) (breaches)
What is the same?	The top three patterns remain the same, but their order of ascendancy has rearranged. Personal data, very useful for fraud, continues to be the most desired data type stolen.
Summary	With Basic Web Application Attacks as the top pattern, we know that the adversaries are successfully gaining access without too much effort. This, combined with the Misdelivery error, indicates there is room for good controls to cover a decent percentage of attacks in this sector.

These attacks are so basic.

"We were compromised by a highly sophisticated cyberattack." So reads a large percentage of data breach notification letters. But really, just how sophisticated is a brute-forced password? Or better still, credential stuffing where you don't even have to guess the password—you've acquired it from another breach! The Basic Web Application Attacks pattern is the most prevalent in this sector, which means those not-so-complex attacks are succeeding splendidly for the adversaries. Why put forth a great deal of effort when just a little will do?

Make them work for it.

Rounding out the top three is the pattern that requires adversaries to actually put forth a bit of effort, System Intrusion. While it dropped from 27% to 14% this year (allowing Miscellaneous Errors to dominate), it remains a serious issue. This illustrates that at least some of the time, adversaries had to trot out their more sophisticated techniques in order to get the job done. Interestingly, Ransomware is decreasing as a favorite tactic in this pattern for this sector. We discuss it more in depth in the "Incident Classification Patterns" section in case if you skipped that part. We know, some of you just read the DBIR for the pictures.

Wait—did I give you that?

Another prominent attack involves Internal actors making mistakes. Misdelivery—where protected data is sent to the wrong recipient—is the most common. Sometimes it is a matter of paper documents going to the wrong people, and other times it is just the electronic version that goes astray. Either way, extra care needs to be given to catching these kinds of Errors before they cause a data breach.

Healthcare

NAICS
62

Frequency	525 incidents, 436 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 68% of breaches
Threat actors	External (66%), Internal (35%), Multiple (2%) (breaches)
Actor motives	Financial (98%), Espionage (2%), Fun (1%), Ideology (1%) (breaches)
Data compromised	Personal (67%), Medical (54%), Credentials (36%), Other (17%) (breaches)
What is the same?	The top three patterns remain the same, although the order has changed. Internal actors making mistakes continue to trouble this sector.

Summary

Ransomware actors continue targeting this sector and are increasingly causing confirmed data breaches in the process. Errors (particularly Misdelivery) are prevalent as well. Finally, don't discount the insider threat in this industry.

A sector under siege

The Healthcare vertical is highly targeted by ransomware gangs, which results in both the loss of use of their systems—potentially with life-threatening consequences—as well as data breaches. While the number of ransomware incidents peaked in this industry in 2021, the last three years have seen a jump in data breaches (where the data is confirmed to have been stolen as well as the encryption triggered) caused by ransomware. This combination of attacks by adversaries is resulting in more data being compromised in addition to the usual chaos of staff being forced to do their jobs without the systems they rely upon.

Mitigating these attacks takes time—if the organization even has reliable, tested backups of the systems compromised—and resources. If both are scarce in your organization, prevention and early detection are your best friends. Don't ignore the threat this type of attack represents when you are planning your controls.

Sorry 'bout that

The Miscellaneous Errors pattern remains prevalent in healthcare. The action variety of Misdelivery is a consistent people problem. This is the mistake that happens when data that is supposed to go to a certain person (or group) actually ends up going to someone entirely different. Sometimes it is in the form of that spreadsheet with

sensitive employee health information accidentally being sent to a much wider distribution than planned (those email groups can be so similar—thanks a lot, autocomplete). In other cases, it is a mailing error with paper documents that are placed in such a way that too much information is visible in the envelope's clear window. Who wants their letter carriers to know about their embarrassing condition? Customers (patients) are understandably upset.

Where's my gruntle?

Ah, the disgruntled employee—so often the perpetrator of malicious actions and wreaking the kind of havoc only an insider can achieve. While the Privilege Misuse pattern is no longer in the top three for this industry, it remains a consistent problem. Snooping from curiosity—more the bored employee than the actively hostile—is common in Healthcare as well. But this is also a sector in which we see evidence of collusion, multiple actors working together to make their breach dreams a reality. If only this diligence could be put toward their legitimate work tasks, these employees could be top performers. The industry's only defense for when someone loses their gruntle is fast detection of unusual data access patterns. This remains a challenge for any industry where internal actors are motivated to cause trouble.

Information

NAICS
51

Frequency	2,110 incidents, 384 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 77% of breaches
Threat actors	External (81%), Internal (20%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (92%), Espionage (8%) (breaches)
Data compromised	Personal (51%), Credentials (37%), Other (35%), Internal (19%) (breaches)
What is the same?	System Intrusion remains the top pattern in this vertical, and it is still dominated by Financially motivated external actors.

Summary

Miscellaneous Errors continues the downward trend it has exhibited for the last several years and loses its position in the top three to Social Engineering. Denial of Service attacks account for 70% of incidents in NAICS 51.

Make no mistake, information is power.

Over the last few years, errors have played a diminishing role in breaches within the Information vertical. That downward trend continues this year, so much so that it has fallen to number four and accounts for only 13% of breaches (Figure 53). Good on ya, Information folks! Securing your assets from the bad guys is hard enough without unwittingly exposing assets yourself.

Social Engineering, on the other hand, has slowly crept up and captured the number three position with 20% of breaches. In some industries, we see a much higher degree of Phishing than we do of its more complicated cousin, Pretexting. In the Information vertical, however, the two social actions are not far apart, with Phishing at 15% and Pretexting at 11%. As mentioned elsewhere in this report, Pretexting is definitely on the rise.

Please listen closely as our options have NOT changed.

As always, external actors (the vast majority of which are Organized crime) are behind most attacks in this vertical. In fact, last year, we showed only External and Internal actors. This year we did see an increase (albeit very small) in the categories of Partner and multiple actors at 1% each. Granted,

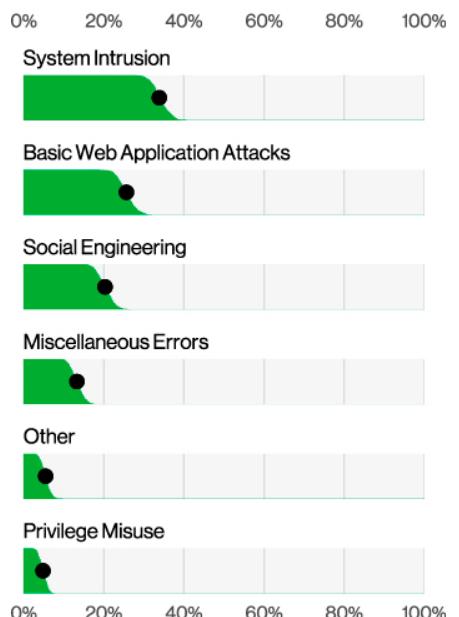


Figure 53. Patterns in Information sector breaches (n=384)

those are not big numbers, but it is of interest to see them reappearing in this industry for the first time in a couple of years. As one would expect, the vast majority of attacks, regardless of who was committing them, were Financially motivated. The motive of Espionage was still present at 8% of breaches but is significantly lower than last year's 20%. The most likely reason for the change is the move away from web apps and servers and toward spy balloons and remote viewing.

Manufacturing

NAICS
31-33

Frequency	1,817 incidents, 262 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 83% of breaches
Threat actors	External (90%), Internal (11%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (96%), Espionage (4%), Convenience (1%) (breaches)
Data compromised	Personal (60%), Credentials (38%), Other (37%), Internal (18%) (breaches)
What is the same?	The top three attack patterns remain the same, but their order has changed slightly. Financially motivated external actors continue to wreak havoc in this industry.

Summary

Hacking and Malware actions are pacing each other in the race for the top two spots. While Social Engineering attacks are still alive and well, they are a distant third. For incidents, do not discount Denial of Service attacks against this industry's infrastructure to disrupt the ability to meet deadlines.

In our postmodern world, we rely on gadgets and gizmos galore to make it through our day—certainly more so than at any other time period in history.⁴⁹ The importance of Manufacturing truly cannot be understated as it relates to how we exist and interact with each other on a daily basis. The Manufacturing industry is aware of this and consequently is continually looking for the next big thing that we all think we can't live without. Cybercriminals know it as well and are constantly maneuvering in an effort to cash in.

This year we can see in Figure 54 the same top three patterns that we saw in last year's report, albeit in a slightly different order. Social Engineering (23%) and Basic Web Application Attacks (17%) changed places in the lineup, while System Intrusion remains in first place at 42%.

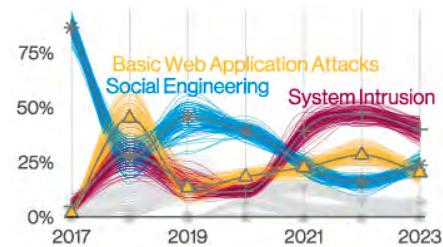


Figure 54. Patterns over time in Manufacturing incidents

As Figure 56 illustrates, when we drill down into what attack actions most often occur in the Manufacturing vertical, we see that Hacking and Malware attacks are occurring at almost exactly the same rate and that Social attacks continue to make a strong showing. Ransomware, which accounts for a large part of the breaches in the System Intrusion pattern, continues to slowly trend upward in this vertical for the third year in a row (Figure 55).

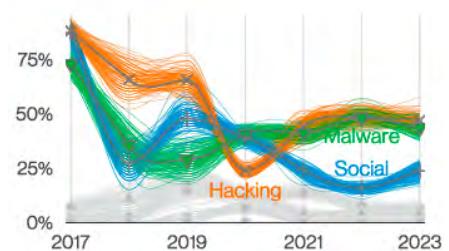


Figure 56. Select Actions over time in Manufacturing breaches

From an incident perspective, it is still mainly about Denial of Service attacks. DoS attacks account for approximately 67% of incidents in this vertical. This has been a rising trend over the past few years, so if your organization resides in this industry, it is definitely something to keep an eye on.

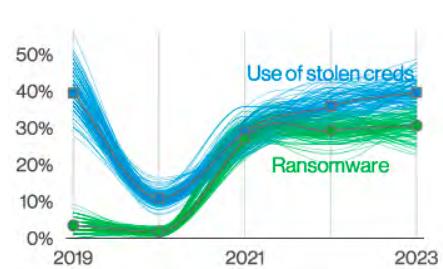


Figure 55. Action varieties over time in Manufacturing breaches

49 And believe me, we have lived through several of them.

Mining, Quarrying, and Oil & Gas Extraction + Utilities

NAICS
21+22

Frequency	143 incidents, 47 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 81% of breaches
Threat actors	External (80%), Internal (20%) (breaches)
Actor motives	Financial (63%–93%), Espionage (4%–32%), Grudge (1%–21%), Ideology (0%–15%), Convenience/Fear/ Fun/Other/ Secondary (0%–7% each) (breaches)
Data compromised	Personal (50%), Internal (33%), Other (26%), Credentials (24%) (breaches)
What is the same?	System Intrusion and Basic Web Application Attacks remain significant causes for concern in this industry.

Summary

Ransomware is responsible for approximately one out of three breaches in this vertical. Social Engineering, in spite of its overall rise, has decreased in this industry.

Dig around and find out.

Due to the smaller number of incidents and breaches reported to us from NAICS 21 and 22, we have to dig deep (pun intended) at times to have a statistically relevant population. Even so, because of the smaller sample size, we are sometimes still forced to use ranges rather than definite percentages. However, as both these sections are considered critical infrastructure and are not too dissimilar, we do our best to find useful and interesting nuggets where we can. Are you a member of these industries? If so, please consider becoming a DBIR contributor to help us provide more useful analysis.

The number one pattern this year is System Intrusion. If you have been reading the other sections, you will know that this in no way makes those in this vertical the Lone Ranger. As stated in the patterns section, the System Intrusion pattern is made up of more complex, multistep attacks as opposed to the “get in, grab the loot and scram” type of attacks. Specifically, most ransomware attacks fall into System Intrusion, and approximately one out of three breaches (32%) in this industry were ransomware attacks (Figure 57). Given the high rate of success of ransomware (along with the fact that attackers often take data before they encrypt it, and they do love to post it on their leak sites), seeing so much of it in critical infrastructure verticals is a matter for concern.

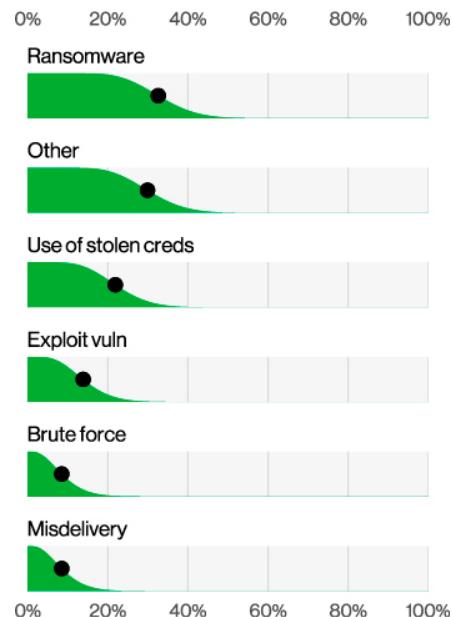


Figure 57. Mining and Utilities top Actions in breaches (n=37)

Last year we commented on the high number of breaches in this vertical that fell into the Social Engineering pattern. This year it has dropped out of the top three completely with Basic Web Application Attacks and Miscellaneous Errors coming in at numbers two and three. In fact, Social Engineering dropped out of the top five. This is mildly surprising due to the uptick we are seeing in phishing and pretexting in other industries. Maybe the criminals don't want to have to actually interact with others to steal money? We can certainly understand that.

When it comes to what the threat actors are taking, personal data accounts for half, and there was a substantial rise in Internal data (33% this year as opposed to 9% last year, as shown in Figure 58). This may be tied to the name and shame ransomware attacks mentioned on the previous page.

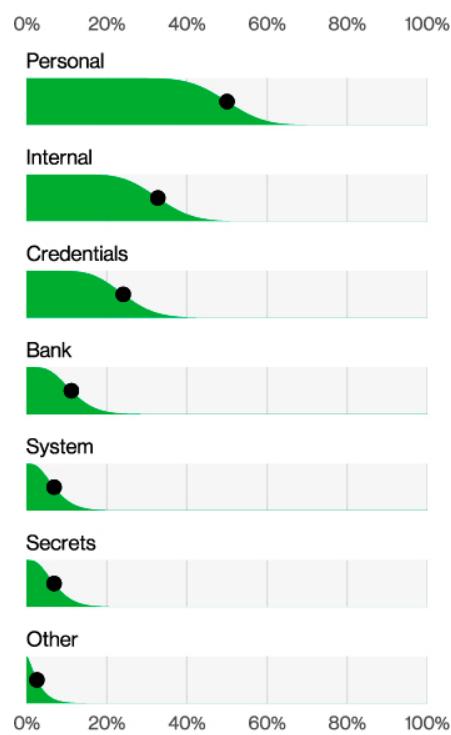


Figure 58. Top Data type stolen in Mining and Utilities (n=46)

Professional, Scientific and Technical Services

NAICS 54

Frequency	1,398 incidents, 423 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 90% of breaches
Threat actors	External (92%), Internal (9%), Multiple (3%), Partner (2%) (breaches)
Actor motives	Financial (96%), Espionage (4%), Convenience (1%) (breaches)
Data compromised	Personal (57%), Credentials (53%), Other (25%), Internal (16%) (breaches)
What is the same?	System Intrusion, Basic Web Application Attacks and Social Engineering continue to be the main threats to organizations in this sector.

Summary

Even though the top patterns haven't changed for this industry, this sector has experienced an increase in Ransomware over the year, with incidents following the same core vectors as the previous year.

This sector could perhaps be considered the lubricant that keeps all industries running smoothly. It consists of many disparate professions, including our lawyer friends [joke redacted by legal], accounting and various other business services. Much like the other sectors they serve, this industry is also affected by the big three patterns of System Intrusion (47%), Basic Web Application Attacks (25%) and Social Engineering (18%).

With regard to action varieties, while we see DoS and Use of stolen creds among the top actions in Figure 59, we also see a good deal of Ransomware. This year, Ransomware accounted for approximately 23% of the incidents in this sector, which is a notable increase from last year's 14%.

If you are wondering how these breaches occur, you need look no further than Web applications (55%), Email (25%) and Desktop sharing software (17%). Considering the frequent usage of stolen credentials and email, it might be a good time to remind folks to implement strong authentication practices and to encourage your team members to keep in mind the importance of staying diligent.

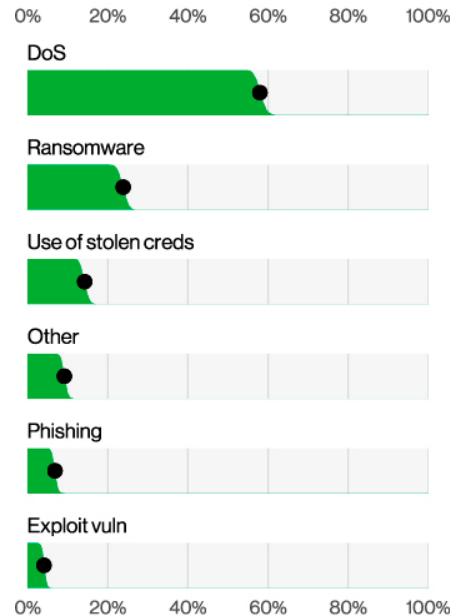


Figure 59. Actions in Professional Services incidents (n=1,351)

Public Administration

NAICS
92

Frequency	3,273 incidents, 584 with confirmed data disclosure
Top patterns	System Intrusion, Lost and Stolen Assets, and Social Engineering represent 76% of breaches
Threat actors	External (85%), Internal (30%), Multiple (16%) (breaches)
Actor motives	Financial (68%), Espionage (30%), Ideology (2%) (breaches)
Data compromised	Personal (38%), Other (35%), Credentials (33%), Internal (32%) (breaches)
What is the same?	This sector continues to be targeted by Financially motivated external threat actors as well as spying Nation-states that are interested in what their rivals are doing. Personal data remains the most often stolen data type.

Summary

This sector continues to make top scores in Espionage-motivated breaches. It is also rich in multiple actor breaches. External and Partner or Internal actors working together to steal data is not the kind of international cooperation we want to see fostered.

That's no moon!

Whether data is stolen by stealthy “weather research” balloons (death stars) floating overhead or by more conventional methods such as phishing, external threat actors are diligently gaining access to data in the public sector. Mind you, when we created VERIS to allow us to categorize breaches, we didn’t expect to see it applied to UFOs being shot out of the sky. But, until it becomes a trend, we will simply tag it as Physical - Other and call it a day for now.

The System Intrusion pattern remains high in this sector. Some intrusions are stuff that movies are made of—complex attacks against a challenging target, where the stakes are high for entire economic systems.⁵⁰ We did see an increase in the Espionage-motivated actors in this pattern this year. In fact, this sector is one where the Espionage-motivated actor is consistently among the highest.

Within the System Intrusion pattern, we saw a slight decrease in Ransomware as a tactic. This doesn’t mean you should ignore it, however, as it remains a favored method of disrupting government workings while generating income for the adversaries.

While it is possible to reach their goals by themselves, these actors are not opposed to recruiting help from within the organization. We see evidence of collusion (multiple actors working in concert) in 16% of Public Administration breaches this year. That is significant, given that we didn’t see multiple Actor breaches the past two years in this sector, and in 2020’s report, it was only at 2%.

What's worse than quiet quitting?

This brings us to the point that internal actor Misuse continues to be a consistent problem in this sector. While prevalent, it is not increasing, so that is at least some good news. In fact, Misuse peaked in 2019 (of the past five years) and has decreased somewhat since then. However, the pairing of the unhappy employee with a motivated external adversary shows the continued need for detective controls. If you can catch this kind of Internal actor-facilitated attack in its early stages, you can mitigate the damage significantly.

We see evidence of collusion (multiple actors working in concert) in 16% of Public Administration breaches this year. That is significant, given that we didn’t see multiple Actor breaches the past two years in this sector, and in 2020’s report, it was only at 2%.

⁵⁰ There are explosions and car chases in there too, we’re sure of it.

Retail

NAICS
44–45

Frequency	406 incidents, 193 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 88% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (2%) (breaches)
Actor motives	Financial (100%), Espionage (1%) (breaches)
Data compromised	Payment (37%), Credentials (35%), Other (32%), Personal (23%) (breaches)
What is the same?	Retail organizations continue to be lucrative targets for cybercriminals looking to collect Payment card data.

Summary

While the same three patterns dominate this industry as many others, Retail has the added bonus of being targeted for its Payment card data in addition to common threats like Ransomware and Basic Web Application Attacks.

Can you breach me now?

Some people turn to the Retail sector as a form of therapy—and we on the DBIR team probably have more dragons, guitars and cuckoo clocks (don't ask) than we really need. Sadly, criminals have been enjoying their own "retail therapy" by targeting this sector for many years. They continue to do so by capitalizing on this industry's heavy use of payment data.

Top actions/ top vectors

When it comes down to how these breaches and incidents occur, it is a roundup of the usual suspects, with both Ransomware and Use of stolen credentials among the top, along with Email and Web applications for vector. However, there is a relatively unique addition to some of these actions—the "Export data" and "Capture app data." This is also one of the few industries where we see "Other" creep up as one of the top actions (Figure 60), and that's largely because there's a variety of secondary actions that actors are using to either deploy their ransomware or find a way to collect payment cards.

If you are in the Retail world and you operate an e-commerce platform, then this section is especially worth paying attention to. Within Retail, we often find the "Magecart"⁵¹-type actors. These criminals find ways of embedding their malicious code within your site's credit card processing page. This allows them to quietly and subtly abscond with your customers' payment data without actually affecting the functionality of your website. Currently, these attacks represent about 18% of Retail breaches. While we freely admit that we don't always know how these Actors were able to access the web application and upload their bad JavaScript, we have seen them use several different tricks (Figure 61).

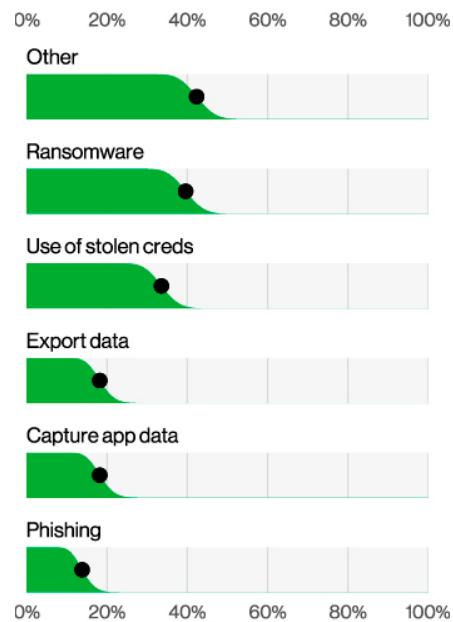


Figure 60. Top Action varieties for Retail breaches (n=182)

⁵¹ In layman's terms, it is when wizards race each other in go-carts.

Stolen credentials: \$5. Domain hosting: \$12. Malicious JavaScript: \$50. Snagging all the fullz: priceless.

Considering the function of this industry, it is hardly surprising to see Payment card data as one of the most common data types breached, accounting for 37% of breaches this year. If you look at Figure 62, you can readily observe that Payment card data has been trending downward since its high-water mark in 2018. However, we are seeing a relatively large increase in Payment card data stolen as compared to last year. Although stealing card data is a tried-and-true method of monetizing data, sometimes the threat actor simply wants a quicker payday. Ransomware has definitely skewed some of the data in this sector, but it seems as if Payment card data is still extremely valuable and will continue to remain a popular target.

This begs the question: Where is this data being stolen from? Because it's difficult to protect something if you don't know what you are protecting. Luckily, we have some data that may help. In our analysis of just payment card breaches in Retail, we found that 70% of breaches originated from Web applications, 17% from Gas terminals and 8% from PoS servers. This once again illustrates how e-commerce has made it way too easy to get what you want, including stolen credit cards. If you are looking for some added incentive, it's worth mentioning that by the time our 2024 DBIR is published, you should all already be compliant with Payment Card Industry (PCI) Data Security Standard (DSS) 4.0.⁵²



Figure 61. Top Action vectors in Retail breaches (n=130)

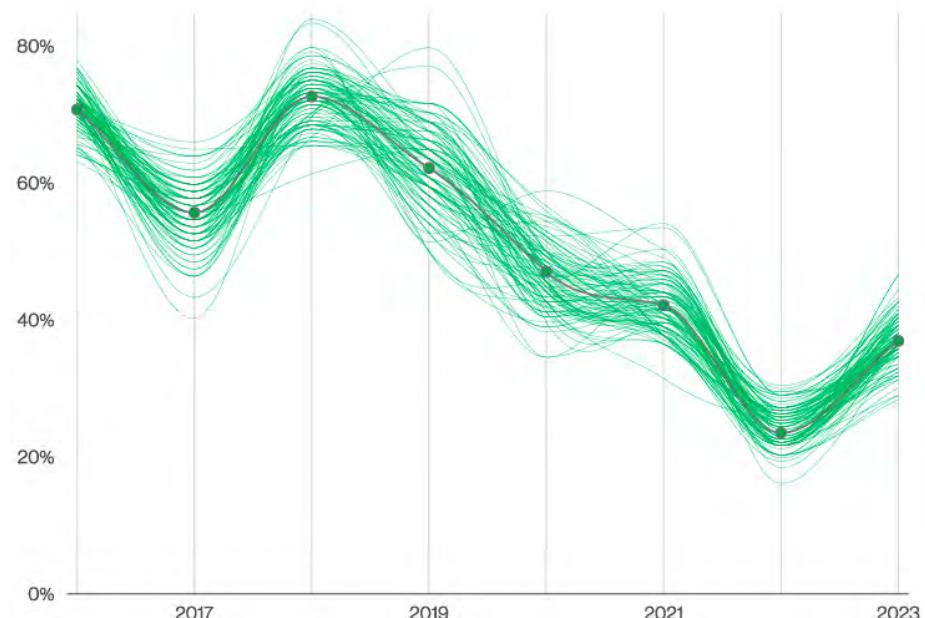


Figure 62. Payment card over time in Retail breaches

⁵² <https://www.pcisecuritystandards.org/resources-overview/>

Small and medium business

“Let’s do some word problems!”

—said no one ever (except math teachers)

In certain prior reports, we have compared and contrasted small and medium businesses (SMBs) against large organizations to determine whether the attack surface differed significantly between them. Increasingly, both SMBs and large companies are using similar services and infrastructure, and that means that their attack surfaces share more in common than ever before. This has led to a convergence of attack profiles regardless of the size of the organization. However, what is very different is the ability of organizations to respond to threats due to the number of resources they can deploy in the event that they are attacked.

The tables on the right illustrate the fact that SMBs and large organizations have increasingly become similar to each other. This phenomenon began several years ago, and by now there is so little difference based on organizational size that we were hard-pressed to make any distinctions whatsoever. Therefore, this year we decided to look at these a bit differently⁵³ by looking at the implementation of security controls for various size SMBs (smaller, midsize and larger) and how they may overlap or differ.

In past reports we have discussed the research we conduct with regard to controls—in particular, the work we have done with MITRE to map VERIS to ATT&CK. This year, we would like to take this research a bit more into the real world and apply it to how you would use these mappings with the appropriate CIS Implementation Group protective controls.

Small businesses (less than 1,000 employees)

Frequency	699 incidents, 381 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Credentials (54%), Internal (37%), Other (22%), System (11%) (breaches)

Table 3. At a glance for SMB

Large businesses (more than 1,000 employees)

Frequency	496 incidents, 227 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches
Threat actors	External (89%), Internal (13%), Multiple (2%), Partner (2%) (breaches)
Actor motives	Financial (97%), Espionage (3%), Ideology (2%), Convenience (1%), Fun (1%) (breaches)
Data compromised	Internal (41%), Credentials (37%), Other (30%), System (22%) (breaches)

Table 4. At a glance for large organizations

53 Again, there is that refocusing thing we keep talking about.

Regions: Introduction

This edition of the DBIR marks the fourth year we have examined cybercrime incidents from a macro-regional point of view. We hope our readers find this broader look at cybercrime useful and instructive. As previously mentioned, our visibility into a certain region is determined by many variables, including contributors, regional disclosure laws and our own data. If your part of the world is not featured in the following pages, please contact us about becoming a data contributor and motivate other organizations in your area to do the same so that we can keep growing and improving our coverage each year. Even if your region is not represented here, this does not mean we have no visibility into the region but rather that we don't have enough incidents in that geography to have a statistically significant section.

We define the regions of the world in accordance with the United Nations M49⁵⁸ standards, which combines the super-region and sub-region of a country together. By so doing, the regions we will examine are as follows:

APAC: Asia Pacific, including Southern Asia (034), South-eastern Asia (035), Central Asia (143), Eastern Asia (030) and Oceania (009)

EMEA: Europe, Middle East and Africa, including Northern Africa (015), Europe (150) and Eastern Europe (151), and Western Asia (145)

LAC: Latin America and the Caribbean, including South America (005), Central America (013) and Caribbean (029)

NA: Northern America (021), including the United States and Canada

As in previous years, we have sliced and diced our data in many ways, and this time we are presenting the data for the various regions a little differently. Long-time readers will recognize the At-a-Glance tables that we put in each major section, only in this case, we've combined them to give you an easy way to see just how similar (and different) each of the regions are with regard to the frequency, top patterns, etc.

Region	Frequency	Top patterns	Threat actors	Actor motives	Data compromised
APAC	699 incidents, 164 with confirmed data disclosure	Social Engineering, System Intrusion and Basic Web Application Attacks represent 93% of breaches	External (92%), Internal (9%), Partner (2%), Multiple (2%) (breaches)	Financial (61%), Espionage (39%), Convenience (2%), Grudge (2%), Secondary (1%) (breaches)	Internal (56%), Secrets (42%), Other (33%), Credentials (29%) (breaches)
EMEA	2,557 incidents, 637 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 97% of breaches	External (98%), Internal (2%), Multiple (1%) (breaches)	Financial (91%), Espionage (8%), Ideology (1%), Fun (1%) (breaches)	Credentials (53%), Internal (37%), System (35%), Other (15%) (breaches)
LAC	535 incidents, 65 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 94% of breaches	External (95%), Internal (5%), Partner (2%), Multiple (2%) (breaches)	Financial (93%), Espionage (11%), Ideology (2%) (breaches)	System (55%), Internal (32%), Classified (23%), Credentials (23%), Other (19%) (breaches)
NA	9,036 incidents, 1,924 with confirmed data disclosure	System Intrusion, Basic Web Application Attacks and Social Engineering represent 85% of breaches	External (94%), Internal (12%), Multiple (9%), Partner (2%) (breaches)	Financial (99%), Espionage (1%), Grudge (1%) (breaches)	Credentials (67%), Internal (50%), Personal (38%), Other (24%) (breaches)

Table 6. At a glance for regions

58 <https://unstats.un.org/unsd/methodology/m49/>

WHITE PAPER

A black background filled with white binary digits (0s and 1s) that are arranged to form various words related to cyber security, such as "virus", "phishing", "spam", "Trojan", and "shining". These words are written in a diagonal, slightly overlapping manner across the entire page.

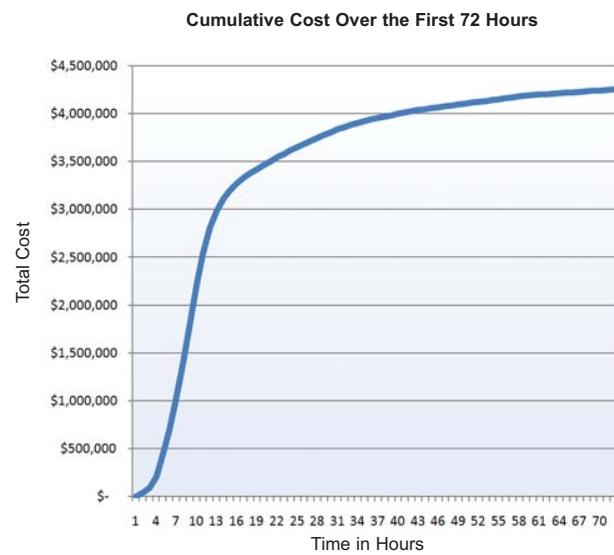
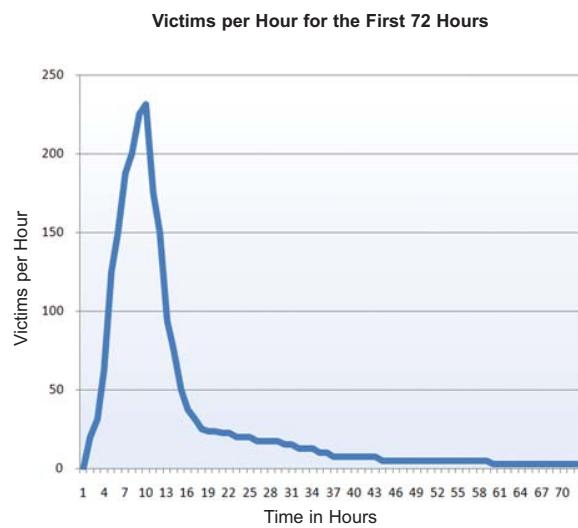
The Cost of Phishing: Understanding the True Cost Dynamics Behind Phishing Attacks

A Cyveillance Report
October 2008

The Cost of Phishing

Attack Details:

The Cost of Phishing



The duration of the phishing attack is a key factor in determining the overall costs of a specific attack. As specifically illustrated in the attack detailed above, we can ascertain that the majority of costs associated with a phishing attack occur within 24 hours of the attack's launch and that after that period, the costs associated with an attack level off significantly.

Acronis

Report
2022



Acronis Cyberthreats Report 2022

At war with ransomware gangs: a year in review

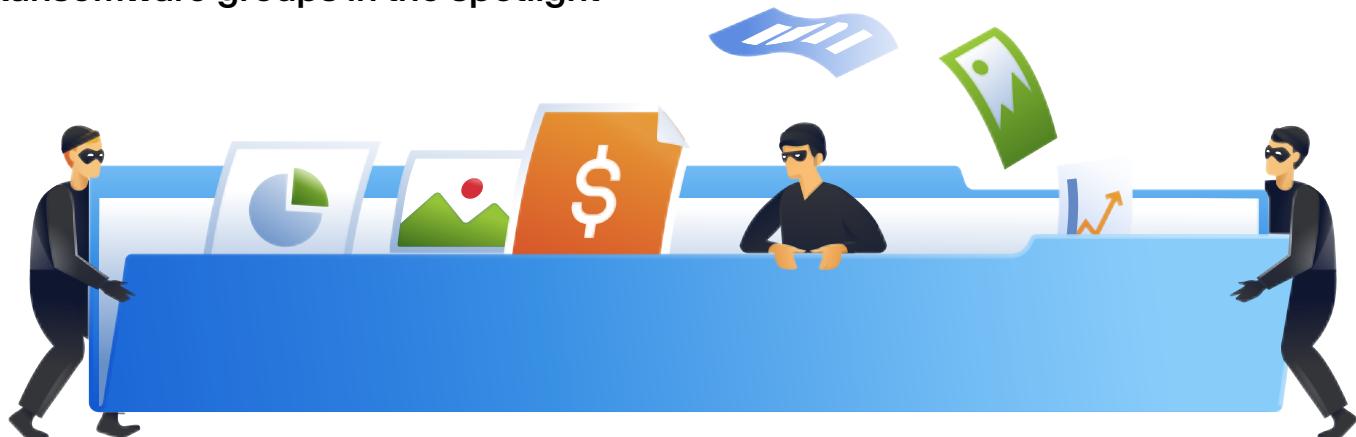
Top 10 countries: ransomware detections by region

Country	Regional ransomware detections percentage in Q3 2021	Regional ransomware detections percentage in Q2 2021	Asia
Japan	31.61%	38.09%	Asia
Israel	8.49%	2.55%	
China	7.92%	8.59%	
India	7.34%	3.65%	
South Korea	5.50%	5.51%	
Turkey	5.44%	5.51%	
Taiwan	4.91%	5.43%	
Philippines	4.70%	4.16%	
Thailand	2.95%	2.55%	
Indonesia	2.75%	2.06%	

Country	Regional ransomware detections percentage in Q3 2021	Regional ransomware detections percentage in Q2 2021	EMEA
Germany	43.37%	45.17%	EMEA
United Kingdom	9.64%	9.46%	
France	9.00%	9.37%	
Switzerland	7.98%	8.45%	
Italy	5.65%	5.50%	
Netherlands	3.28%	4.04%	
Spain	3.07%	2.85%	
Austria	3.01%	3.13%	
Belgium	2.31%	2.33%	
Czech Republic	1.65%	1.38%	

Country	Regional ransomware detections percentage in Q3 2021	Regional ransomware detections percentage in Q2 2021	Americas
United States	79.03%	79.64%	
Canada	12.05%	12.14%	
Mexico	2.20%	2.15%	
Brazil	1.73%	2.09%	
Argentina	0.93%	0.49%	
Colombia	0.86%	0.64%	
Chile	0.44%	0.48%	
Peru	0.39%	0.46%	
Bolivia	0.29%	0.11%	
Guatemala	0.26%	0.22%	

Ransomware groups in the spotlight



AvosLocker ransomware

The ransomware AvosLocker was discovered in late June of 2021. The criminals started searching for affiliates through various DarkWeb forums, as was revealed in a [Twitter post](#). They also announced recruitment for penetration testers who have worked with Active Directory and “access brokers” who have remote access to hacked infrastructure. In another post, they offered ransomware-as-a-service — providing a piece of malware written in C++ with the multithreading capability that overwrites victims’ files — with encrypted content instead of through the creation of file copies. AvosLocker was distributed as spam emails targeting Windows machines and uses AES-256-CBC for file encryption, and RSA-1024 for file keys encryption. It encrypts network shares, and terminates associated processes that may be blocking access.

Malicious websites

An average of 1.9% of endpoints tried to access some malicious URLs in Q3 2021, up slightly from 1.8% in Q2. In October, we have seen a spike to 4.3%, which is related to the spike we saw in phishing emails reaching users' inboxes.

Month	Percentage of users that clicked on malicious URLs
January	3.2%
February	2.9%
March	2.1%
April	1.8%
May	1.9%
June	1.8%
July	1.9%
August	1.8%
September	2.1%
October	4.3%

The largest percentage of blocked malicious URLs in Q3 2021 was 26.8% in the United States, followed by 20% in Germany, and 8.7% in Canada — with 65% of these blocked URLs encrypted by HTTPS, making them more difficult to analyse and filter on the network.

We have observed more groups paying attention to the browser user-agent requesting websites. Automated scanning tools that do not mimic normal users are served clean decoy websites instead of a real payload. A similar fate occurs with solutions that replace URL arguments — like emails addresses — for privacy reasons when they are passed to the website. Some kits have a checksum that can detect this change and serve a benign website instead. There was also a small increase in the known tactic of bait-and-switch scams, where the URL in an email points to an initially clean website, which a few hours later is switched to the final malicious payload, in the hopes that any initial email scanner already marked the link as non-malicious.