Bitdefender

2021 CONSUMER THREAT LANDSCAPE REPORT

Executive summary

Digital activity has reached an all-time high during the pandemic, with careless consumer behavior further darkening the global cyberthreat landscape.

The world of interconnected smart devices continues to present security challenges. Neither the mobile device industry nor the IoT ecosystem made significant changes in their security posture, which means that many of the issues we've seen in the past are still present. Whether we're looking at Android trojans or stalkerware on Android devices or the deplorably vulnerable IoT infrastructure, cybersecurity remained a necessary tool to stay safe in 2021.

Throughout 2021, spammers and malicious actors have kept busy creating and distributing fraudulent correspondence across the globe. Spam topics and delivery tactics were once again strengthened by the socio-economic changes brought on by the pandemic, with spammers continuing to piggyback on coronavirus-related subjects. As the global population settled into its second year of lockdowns and travel restrictions, cyber behaviors rooted in 2020 quickly solidified taking a heavy toll on the security and privacy of consumers. Theme-wise, spammers built an impressive spam menu experimenting and building upon previously delivered spam campaigns with a clear focus on four major spam categories that include malware distribution, extortion, scams and phishing.

Of the many threats we've seen targeting Windows systems last year, five key categories have remained in place: Exploits, Trojans, Ransomware, Coin-Miners, and Potentially Unwanted Applications (PUA). Macs face slightly less variance in terms of malware. On macOS, we analyze Trojans, Potentially Unwanted Applications (PUA), Adware and Coin Miners.

Key findings

- Trojans are the most common type of malware on both Mac and Windows
- The US and Latin America are the overall most targeted regions by cyber actors
- Coin mining is most prevalent in regions with abundant computing power
- Australia registers considerable coin mining activity using Macs, with 25% of the global average
- Ransomware is more concentrated in high-yield industries and regions than ever before
- PUAs make up a third of all threats directed at Windows systems
- The US received the largest share of global spam emails by volume (40%)
- Healthcare-related spam accounted for an average of 19% of the global spam volume
- Only 21% of Bitdefender Digital Identity Protection users lean towards a low-key digital identity
- Official Android stores remain an important infection vector, despite their supposed inherent security
- The US is the most affected country by stalkerware with a 60% share
- The most common smart devices in people homes are not the most vulnerable
- DDoS attacks remain the biggest threat to IoT devices

WINDOWS THREAT LANDSCAPE

Windows threat distribution

Of the many threats we've seen targeting Windows systems last year, five key categories have remained in place:

Exploits – leveraging known, unknown (zero-day), or unpatched vulnerabilities

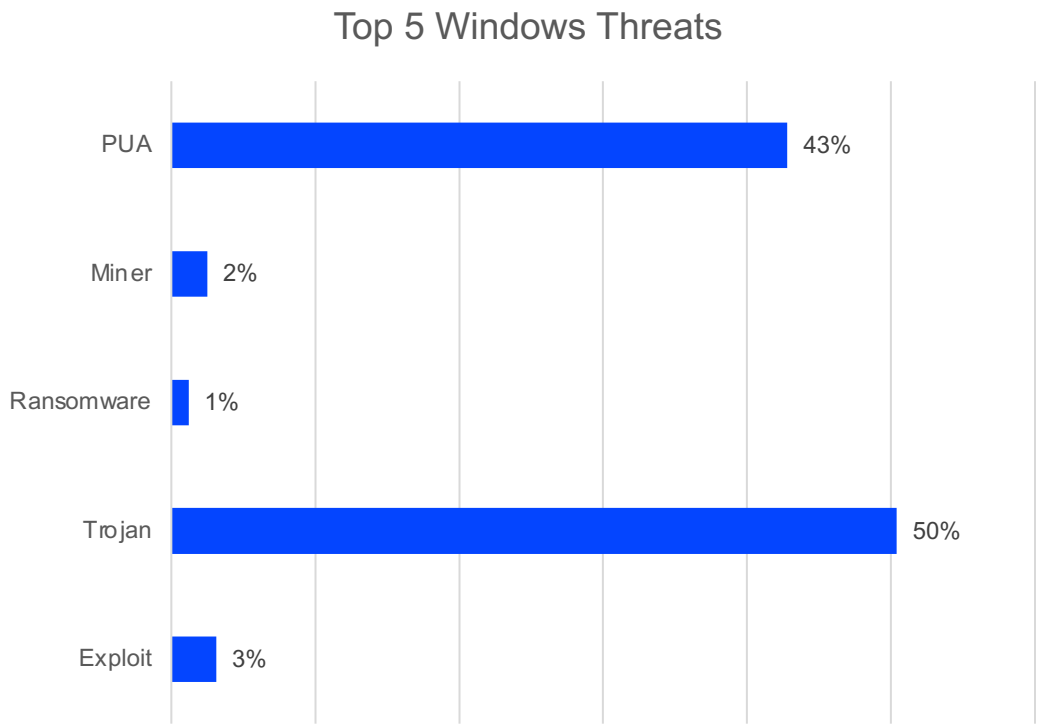
Trojans – exfiltrating data from infected systems, spreading laterally to compromise other endpoints, and downloading additional malware

Ransomware – stealing and encrypting data; demanding ransom to restore systems refrain from leaking data

Crypto-miners – stealthily hijacking CPU power to mine cryptocurrency for the bad guys

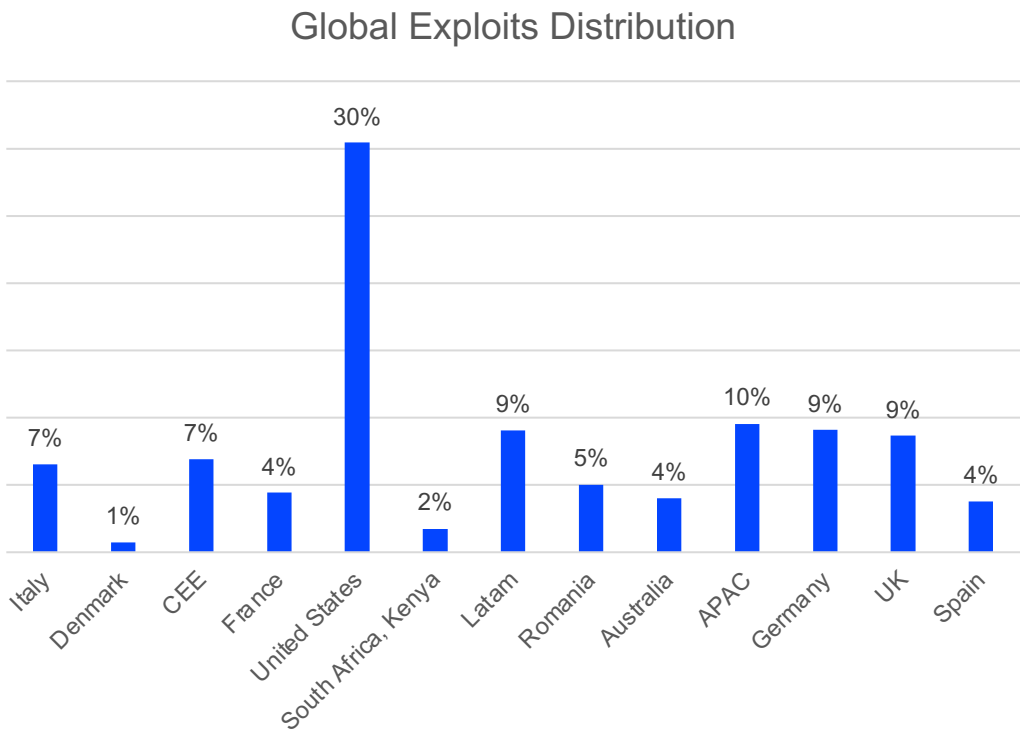
Potentially Unwanted Applications (PUA) – causing usability and performance issues by installing additional applications and displaying aggressive ads

The vast majority of threats detected on Windows platforms in 2021 were trojans, with a 50% share, including specific families like Trickbot, Emoted, Dridex, AgentTesla and many other generic detections. Trojans make up the bulk of the threat spectrum because they are often detected in the primary stages of a given attack. Trojans are extensively used to serve up secondary payloads to achieve the true scope of the attack, not least of which are ransomware, crypto miners and malware designed to exploit unpatched vulnerabilities. Potentially Unwanted Applications (PUAs) are also a prolific metric, despite not being considered actual malware. As the chart below shows, most of the threat landscape is dominated by malware classified as Trojans, and PUAs.



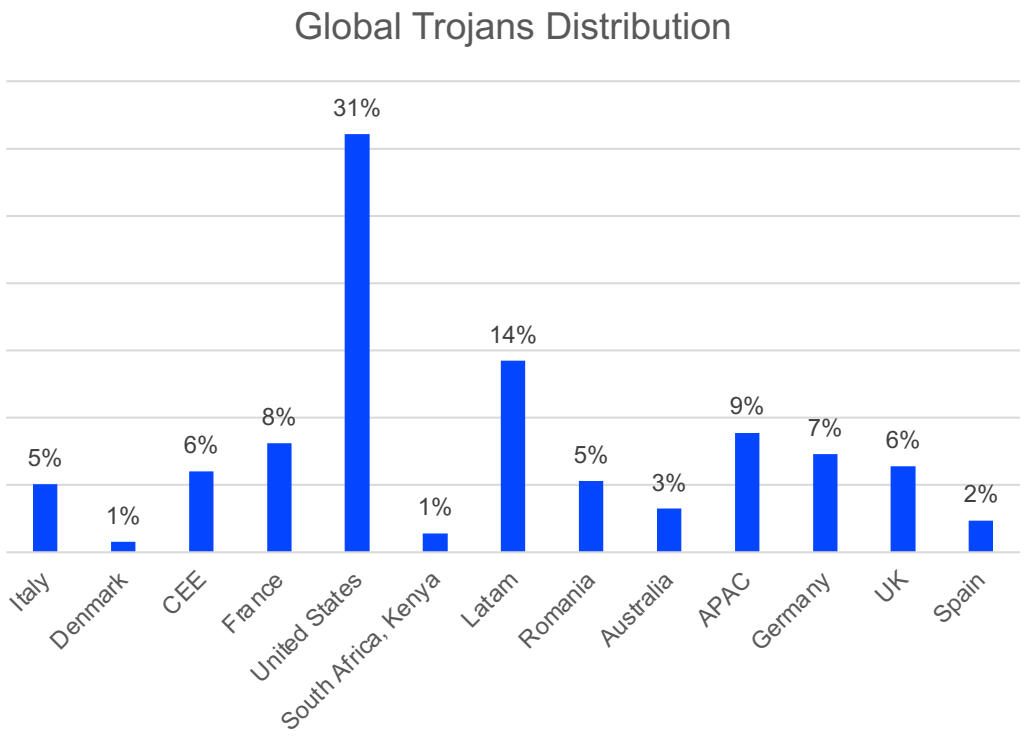
Exploits

2021 saw a fairly even distribution of exploit-based attacks, with the US registering a notably higher number of attempted attacks – as is typically the case, year after year. Second in line was the Asia-Pacific (APAC) region, with a 10% share, followed by Latin America, Germany and the UK with 9%, Romania at 5%, Central-Eastern Europe along with Italy at 7%, and France, Spain and Australia at 4%. Regions like South Africa and Denmark saw comparatively few attacks, but still enough to make our list.



Trojans

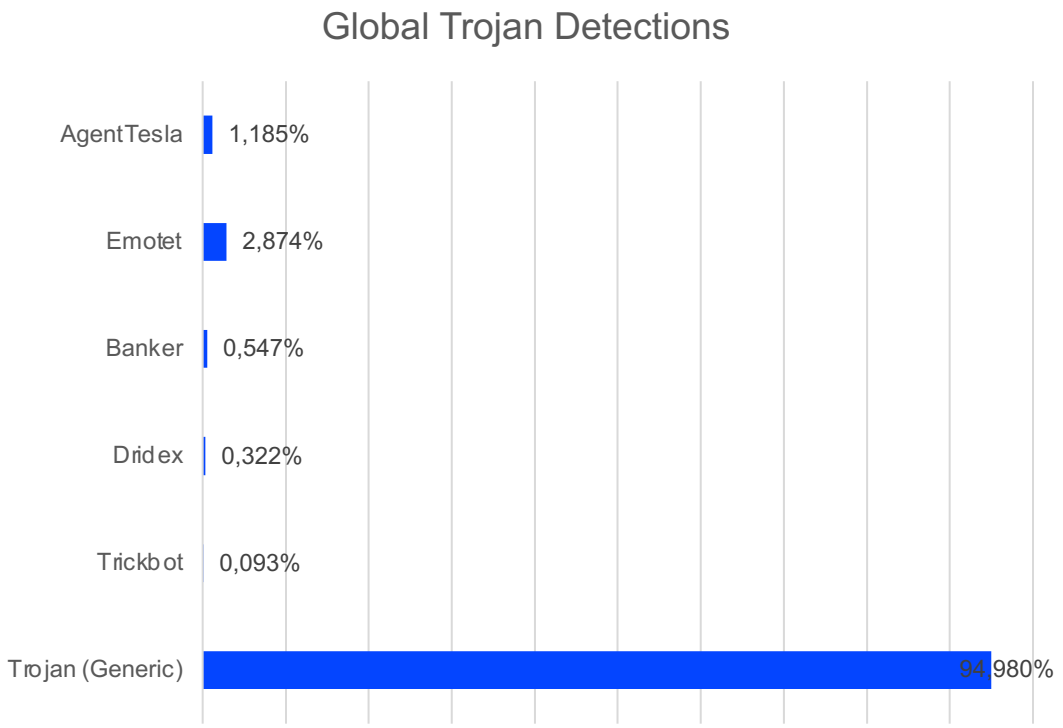
In 2021, Trojans were used extensively against high-profile targets. Despite international efforts to dismantle big-name Trojans like Trickbot, Emotet, Dridex and AgentTesla, cybercriminals continued to leverage these infamous malware families. However, their notoriety has dwindled to oblivion, as the numbers indicate only a handful of highly targeted attacks. Nonetheless, they remain on the map of the top threats to Windows endpoints globally.



Global Trojan distribution

As in previous years, cybercriminals extensively leveraged Trojans to harvest credentials, steal sensitive data, deliver ransomware or hijack computing power to mine cryptocurrency.

Note: Generic trojan detections may include different strains/samples of Emotet, AgentTesla, Dridex and Trickbot. Our AI malware detection technologies don't always generate or assign the same name/strain/variant to a blocked threat.

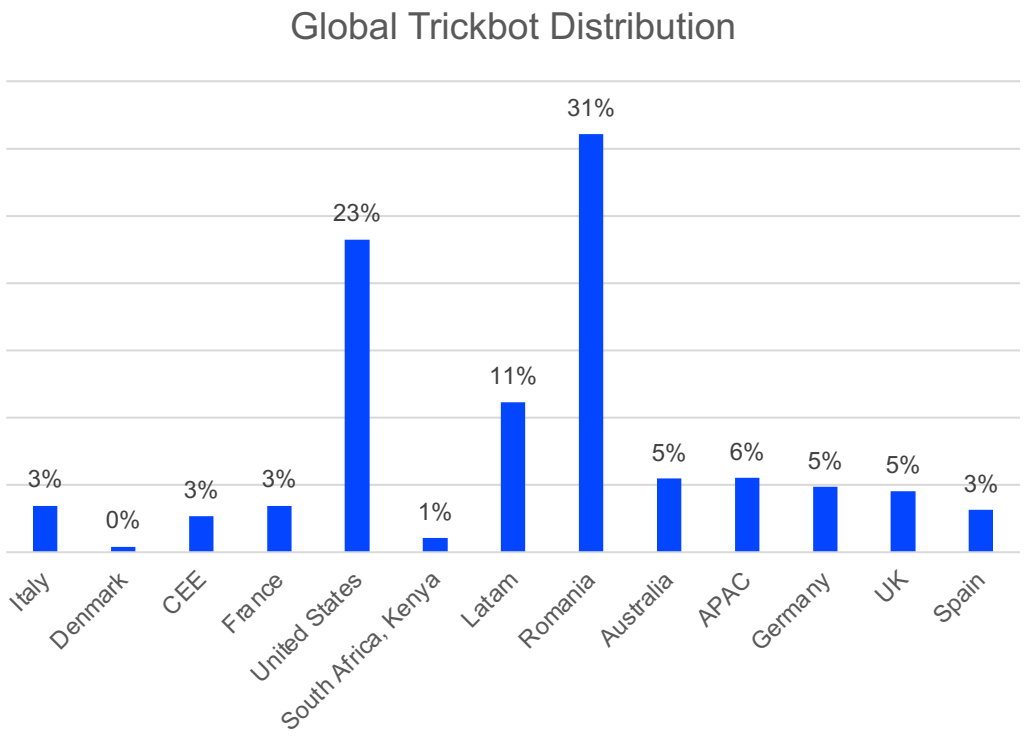


Trickbot

Trickbot is not only used to steal data and harvest credentials. It has also been used in ‘access-as-a-service’ attacks to infect systems with ransomware. It is propagated by executables, batch files, email phishing, Google Docs and even fake sexual harassment claims. It is designed to worm its way across the target network and compromise endpoint after endpoint, gaining persistence.

While the US again stands out with a considerable share of attacks, at 23% of the global average, Romania curiously tops the chart in attempted Trickbot infections in 2021, with a 31% share of global attacks leveraging the infamous malware. Latin America is the only other territory registering a double-digit figure (11%) in Trickbot activity.

The numbers may seem surprising at first glance, but they’re not. Compared to the intense Trickbot activity of 2020, 2021 was very calm. As international police worked hard to dismantle Trickbot operations, the botnet’s share shrunk to a paltry 1%.



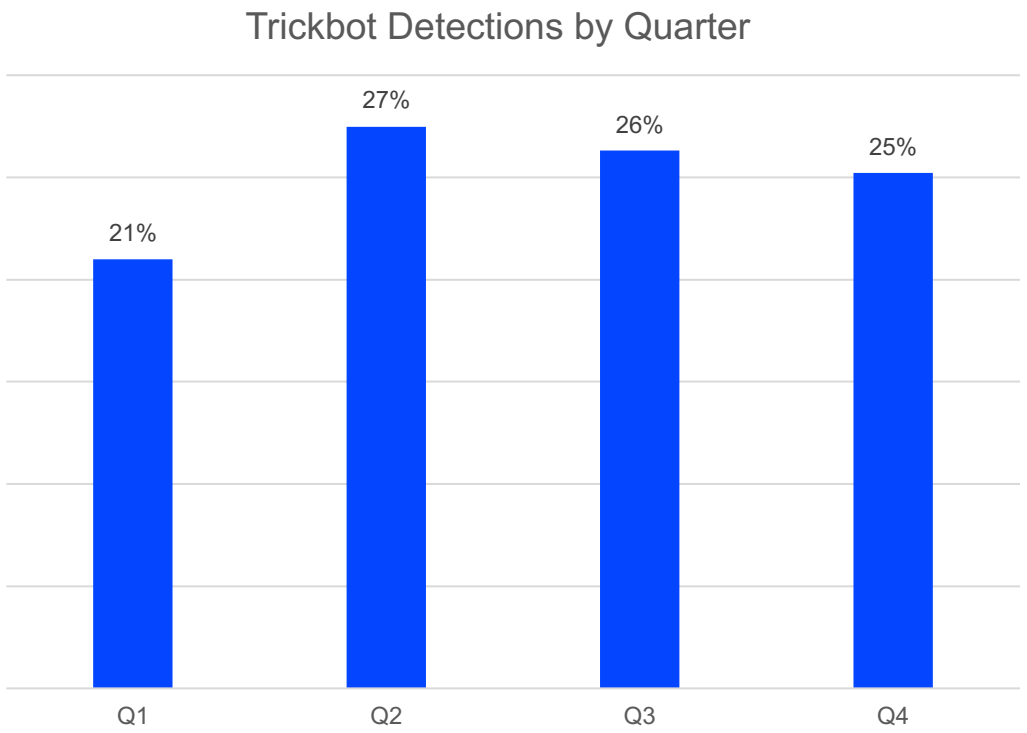
Trickbot detections by quarter

Trickbot is not only used to steal data and harvest credentials. It has also been used in ‘access-as-a-service’ attacks to infect systems with ransomware. It is propagated by executables, batch files, email phishing, Google Docs and even fake sexual harassment claims. It is designed to worm its way across the target network and compromise endpoint after endpoint, gaining persistence.

While the US again stands out with a considerable share of attacks, at 23% of the global average, Romania curiously tops the chart in attempted Trickbot infections in 2021, with a 31% share of global attacks leveraging the infamous malware. Latin America is the only other territory registering a double-digit figure (11%) as far as Trickbot activity goes.

The numbers may seem surprising at first glance, but they’re not. Compared to 2020, when Trickbot activity was intense, 2021 was very calm. As International police worked hard to dismantle Trickbot operations, the botnet’s share shrunk to a paltry 1%.

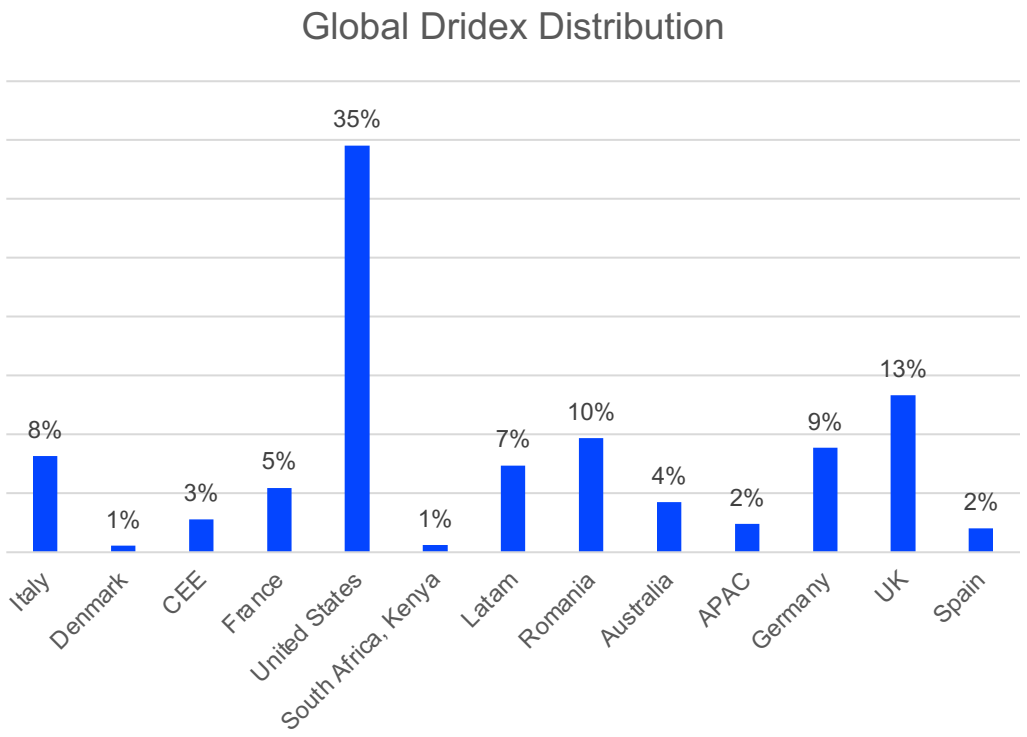
But since Trickbot activity was overall much lower than in previous years, the notorious Trojan was likely used only in a handful of targeted attacks. These low detection rates should come as no surprise. Efforts by governments and cybersecurity vendors in the past two years have nearly extinguished the botnet’s operations. Yet Trickbot doesn’t seem to be completely out of the picture. Samples still crop up in our telemetry, albeit more scarcely than before, suggesting that cybercriminals still rely on its unique capabilities. In any case, Trickbot is no longer central to any particular botnet or crime ring at the moment.



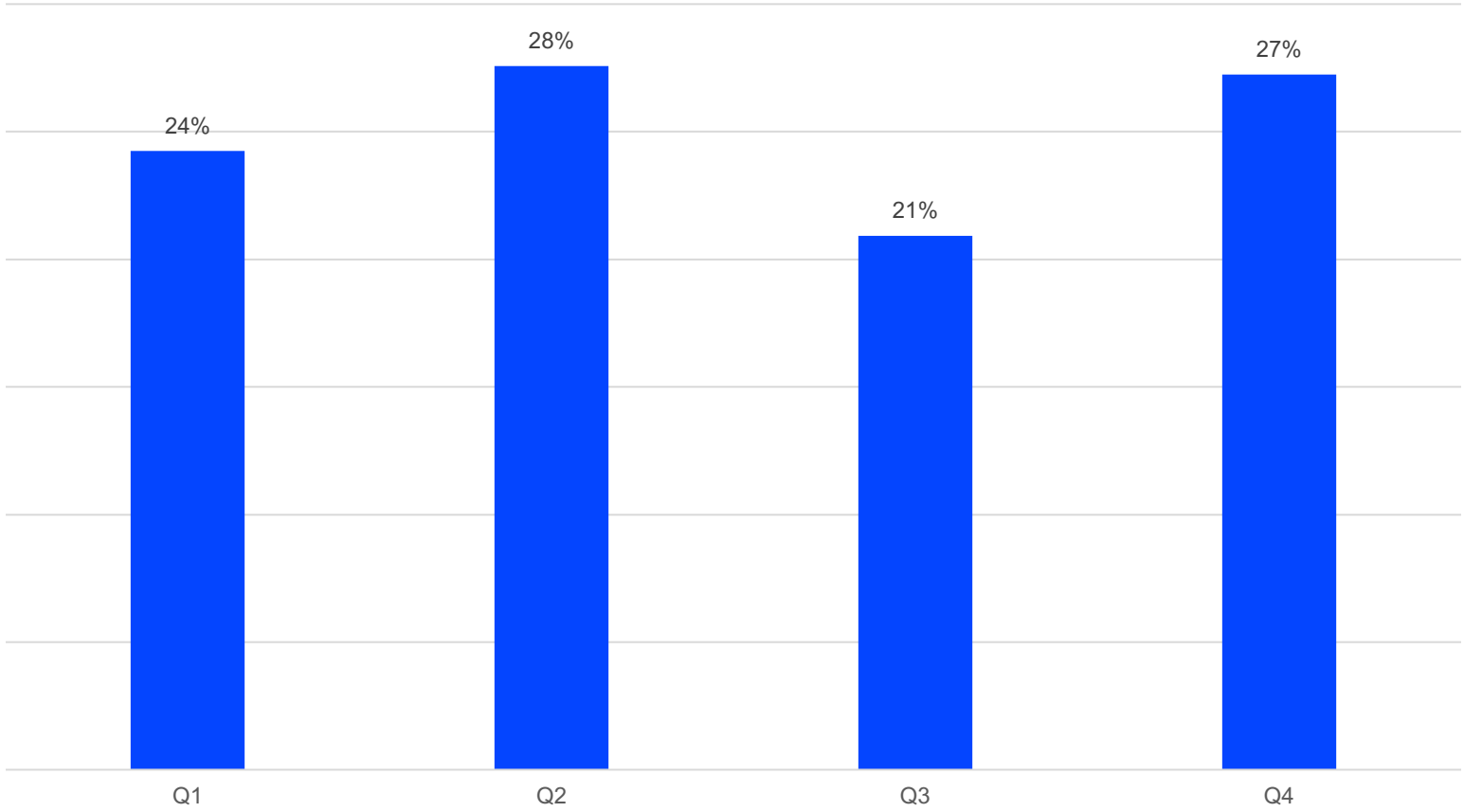
Dridex

Dridex is notoriously specialized in stealing bank credentials via tainted macros. Successful Dridex infections typically end up with fraudulent transactions. Like with Trickbot, international efforts have dented its operations by identifying and charging those responsible for developing and operating the malware.

Dridex attacks were mostly detected in the US, UK, Romania, Germany and Italy, with other territories recording far fewer attempts by those wielding the banking Trojan.

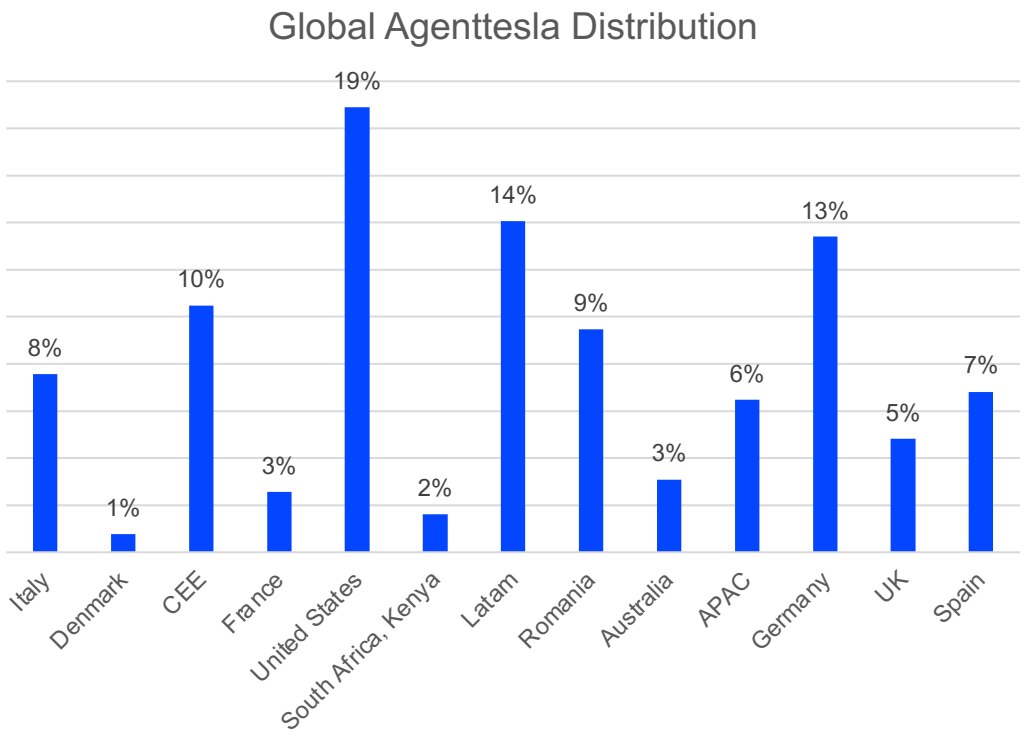


Dridex Quarterly Evolution

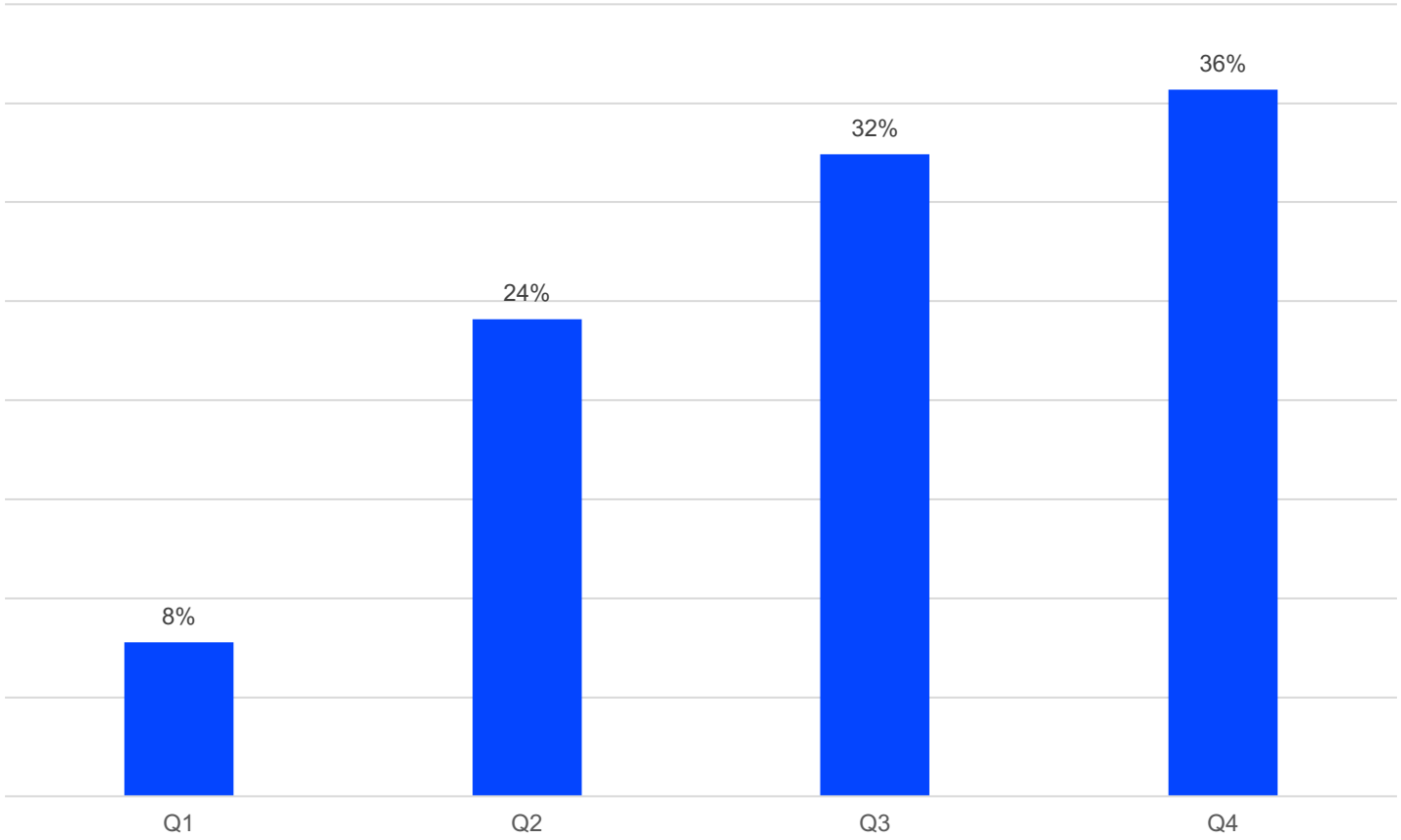


AgentTesla

The AgentTesla Trojan typically arrives via spam email. Threat actors use it in password-stealing and surveillance campaigns. Essentially a keylogger, AgentTesla was mostly active in the US, Latin America, Germany, CEE, Romania and Italy. Attackers used spray-and-pray techniques to infect as many internet users as possible and did not discriminate between targets. AgentTesla attacks notably increased from quarter to quarter, peaking in the final months of 2021.



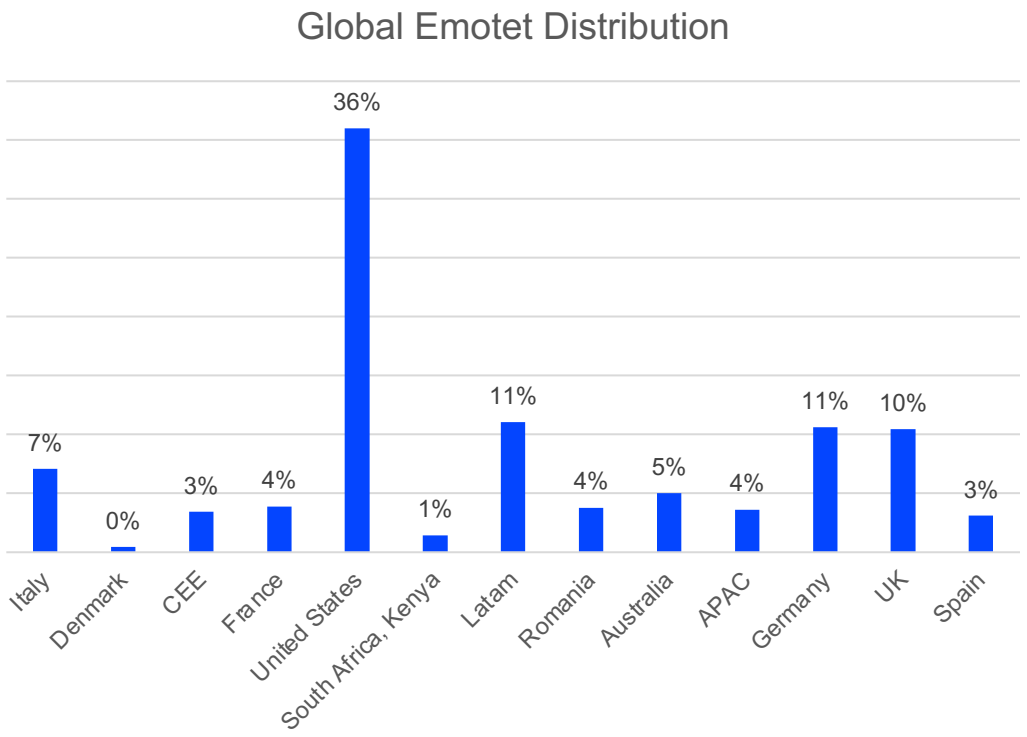
AgentTesla Quarterly Evolution



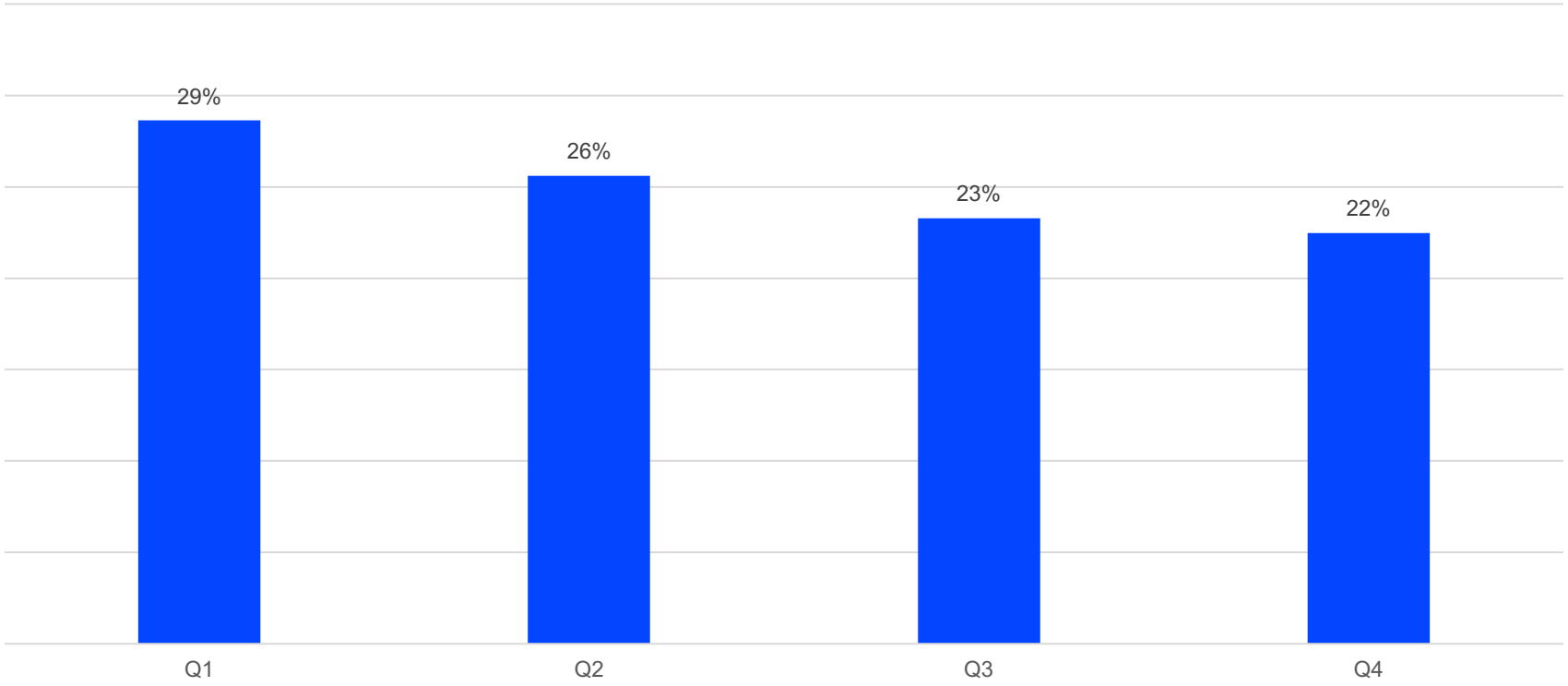
Emotet

Emotet malware initially debuted as a simple banking Trojan aimed at stealing credentials from infected hosts. In recent years, Emotet operators reconfigured the malware to work as a ‘loader’ and deliver second-stage payloads, which can be anything from spyware to ransomware. Like Trickbot and Dridex, Emotet has had a tiny market share among Trojans in general (due to the reasons stated in the Trickbot section).

Threat actors have historically used Emotet as part of a botnet rented out to affiliates. Inspired by a typical Infrastructure-as-a-Service (IaaS) model, malicious actors have used the botnet to buy access to already-infected computers and deploy ransomware. As with previous threats, Emotet was mostly detected in feasible geographies.



Emotet Detections by Quarter



Unlike AgentTesla, Emotet-based attacks peaked in the first quarter of 2021 and progressively decreased by year's end, albeit ever so slightly.

Ransomware

2021 was an active year for ransomware operators. Solar Winds, The Colonial Pipeline, Kaseya and Brenntag are just some of the big names involved in high-profile ransomware attacks that the US Treasury tied to $5.2 billion worth of payments during 2021 alone.

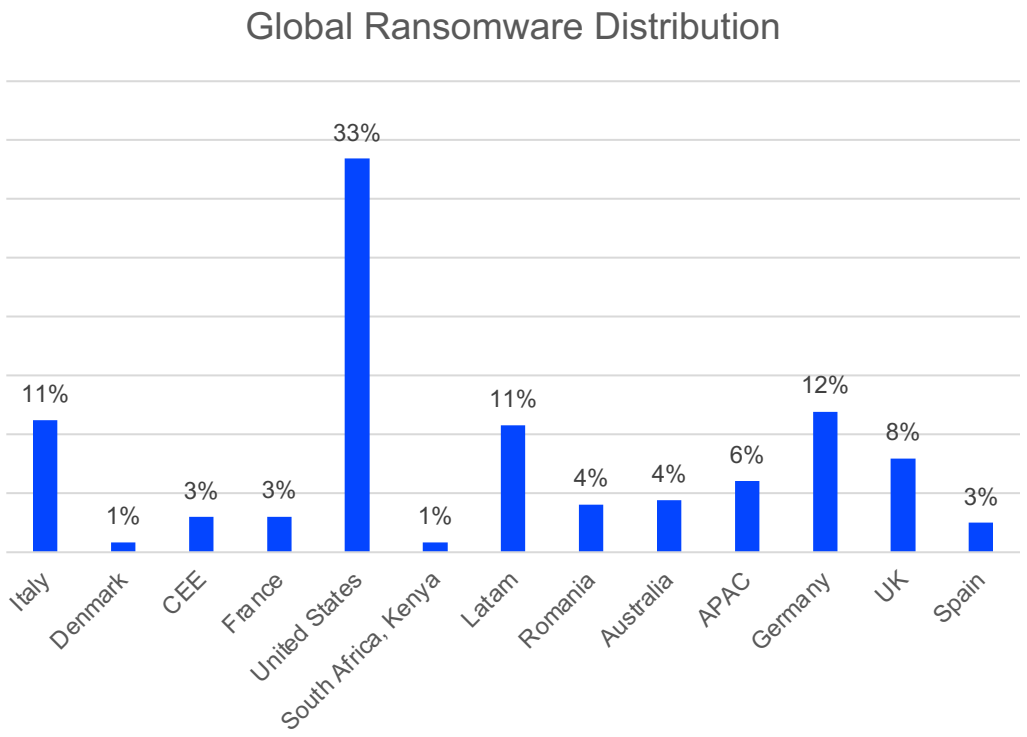
Ransomware reports are typically more common in high-yield geographies, and 2021 was no exception. Extortionists favored territories with big-name companies and large critical infrastructures – key traits that indicate a victim is likely to pay up. Let's not forget that ransomware is increasingly becoming a business targeting, well, businesses.

Global ransomware distribution

The US takes the lead of the pack, with 33% of attacks targeting the North American territory, followed by Germany with a significant 12% share, Latin America and Italy with 11%, UK and APAC with 8% and 6% respectively, Romania and Australia with 4% each, and CEE, France and Spain with 3% each.

The smaller numbers tell an interesting story as to how extortionists distribute their efforts across the globe, depending on what they believe is a high-yield or low-yield target territory. In previous years, ransomware attacks were more evenly distributed across the globe. In recent times, attacks seem to be much more concentrated on profitable territories and industries (more on that below).

For example, Australia and Romania – at first glance, two vastly different regions – registered an almost identical number of attempted ransomware attacks in 2021. Even though Romania (the 83rd largest country) is tiny compared to Australia (the sixth largest country), population count differs only by a few million. And since extortionists target entities big and small based on different extortion models, the number of attempted attacks sometimes evens out between two completely different regions. Conversely, the territories least targeted by cyber threats tell a similar story, as evidenced by the small-but-similar attack rates shared by South Africa and Denmark. So, while ransomware itself is not an agonistic cyber-threat, extortionists won't discriminate between latitude and longitude or culture.

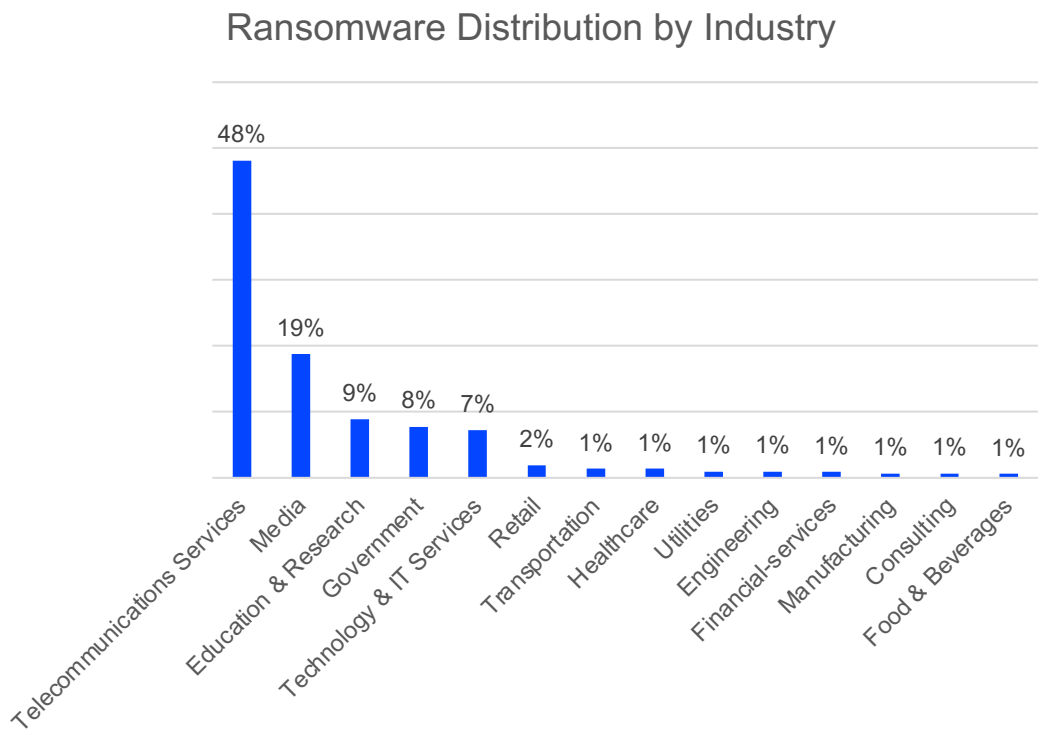


Ransomware Distribution by Industry

Things tend to look a tad different when we zoom in closer to peek at the distribution of attacks by industry. By far the most attacked sector is Telecoms. In 2021, Bitdefender solutions blocked 48% of global ransomware attacks in the telecommunications industry alone. Media takes second place at a distant 19%, followed by Education & Research at 9%, Government at 8%, Technology & Services at 7%, Retail at 2%, and several other verticals, each with 1% of the pie. Those numbers at the end may be small, but that's only because of the sheer number of attacks pounding the left side of the chart, day in and day out.

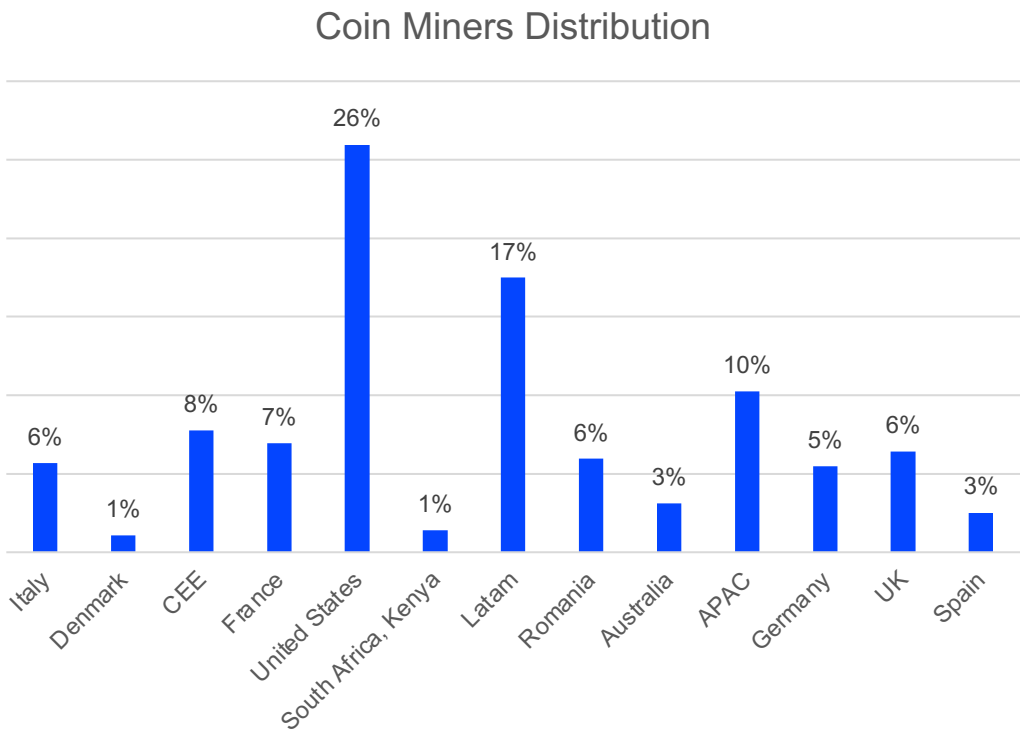
The reason the telecoms industry drew such a massive share of attempted attacks is because the industry is highly targeted industry by prospecting attackers. Telecom operators sit on troves of corporate data, financial data, and the personal data of billions of customers worldwide. Even if a wireless operator refuses to pay ransom, data stolen in an attack can be monetized on the dark web for phishing, fraud, identity theft and everything in between. So it stands to reason that telcos must defend themselves the hardest from ransomware. And indeed, many of them do, using state-of-the-art enterprise security from Bitdefender.

Virtually every industry out there has had a run-in with ransomware. The numbers may not be as high for every vertical, but make no mistake – from Agriculture and Mining to Construction and Aerospace, no industry is left unvisited by prospecting extortionists.



Coin miners

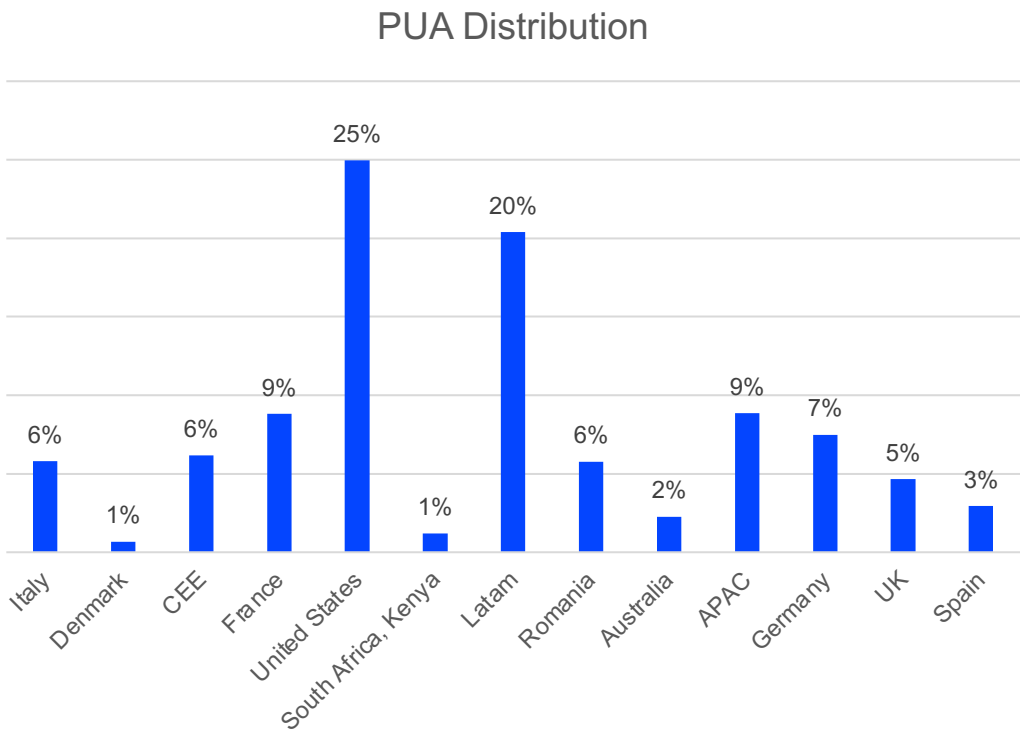
There's no shortage of ways to get infected with a coin-miner. From data breaches to PUAs to warez downloads, coin miners crop up all the time in our data, and 2021 was no exception. Like most threats analyzed in this report, coin mining is mostly prevalent in high-yield regions where computing power abounds. As such, the Americas again take the lion's share, with a combined 33%, trailed by the Asia-Pacific region with 10%. Other areas analyzed here are seeing fairly-even, single-digit distribution. Mining has been fairly even throughout the year, with a slight increase in reports towards the second half of the year.



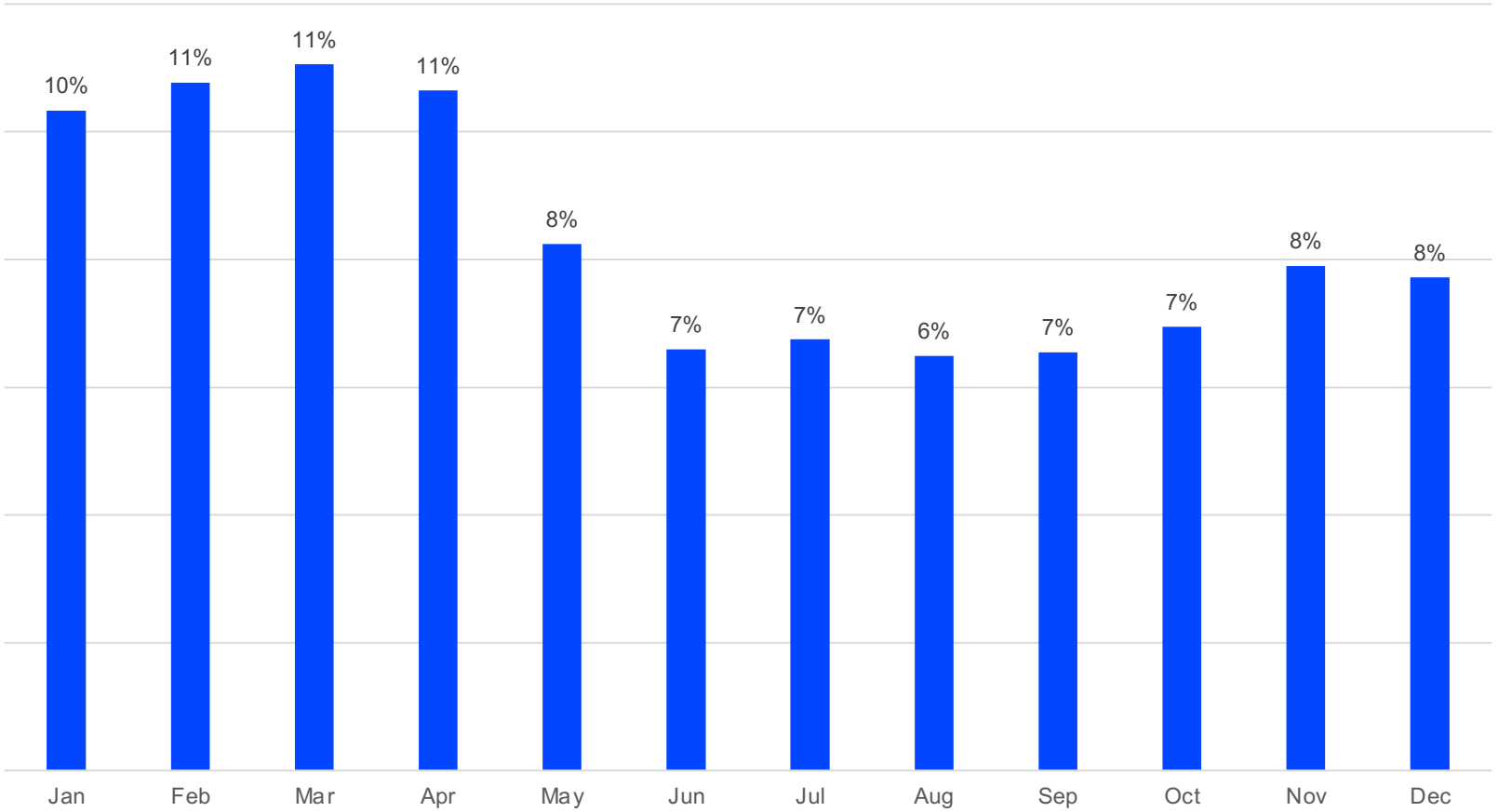
Potentially Unwanted Applications (PUA)

Accounting for a third of all threats directed at Windows systems, PUAs walk the thin line between malware and nuisance. While PUAs generally only hog system resources, often they also display aggressive ads and offer secondary downloads that might hide actual threats, like crypto miners or data-stealing malware.

PUA operators prefer large territories with massive PC user bases. The US and Latin America again make up the bulk, with 25% and 20% of PUA reports, respectively. This high concentration of PUA activity on a single continent leaves all other areas in the single digits, as shown below. The only single-digit region where PUA activity is fairly concentrated compared to others is France, with 9% of PUA reports. Unlike crypto miners, PUAs seem more active in the first half of the year. Such activity is not necessarily tied to any single event, as PUA downloads fluctuate globally from month to month.



PUA Activity (Global)



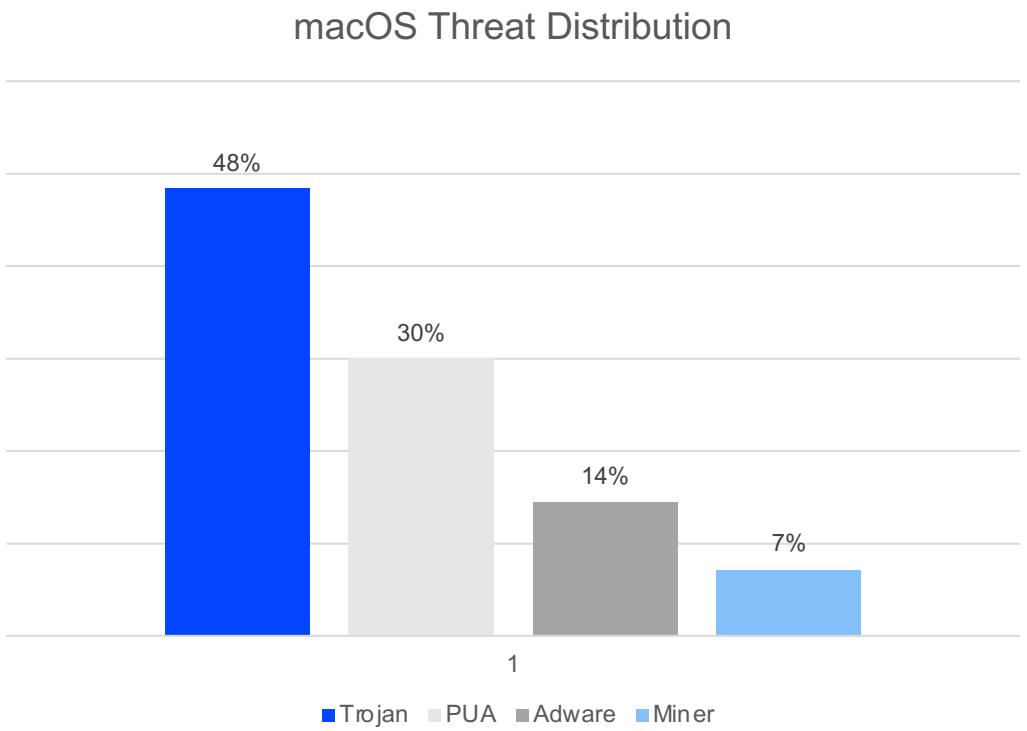
macOS THREAT LANDSCAPE

macOS Threat Distribution

With about 15% of the desktop market, Apple's Mac operating system has a large enough share to draw the attention of cybercriminals. Unlike Windows, which dominates the desktop market and faces a plethora of threats, the macOS environment enjoys less variance in terms of malware. However, this doesn't make Macs less vulnerable. The gap between these two ecosystems means that malware tailored to infect Macs is better suited to its goals.

Excluding platform-agnostic threats like social engineering, macOS typically faces four key threats: Trojans, Potentially Unwanted Applications (PUA), Adware and Coin Miners.

Trojans, disguised as legitimate programs designed to give attackers access to the target system, constitute the biggest single threat facing macOS, with a 48% share. PUAs make up almost a third of the threats targeting Macs, followed by Adware with a 14% share, and CoinMiners, with 7%.

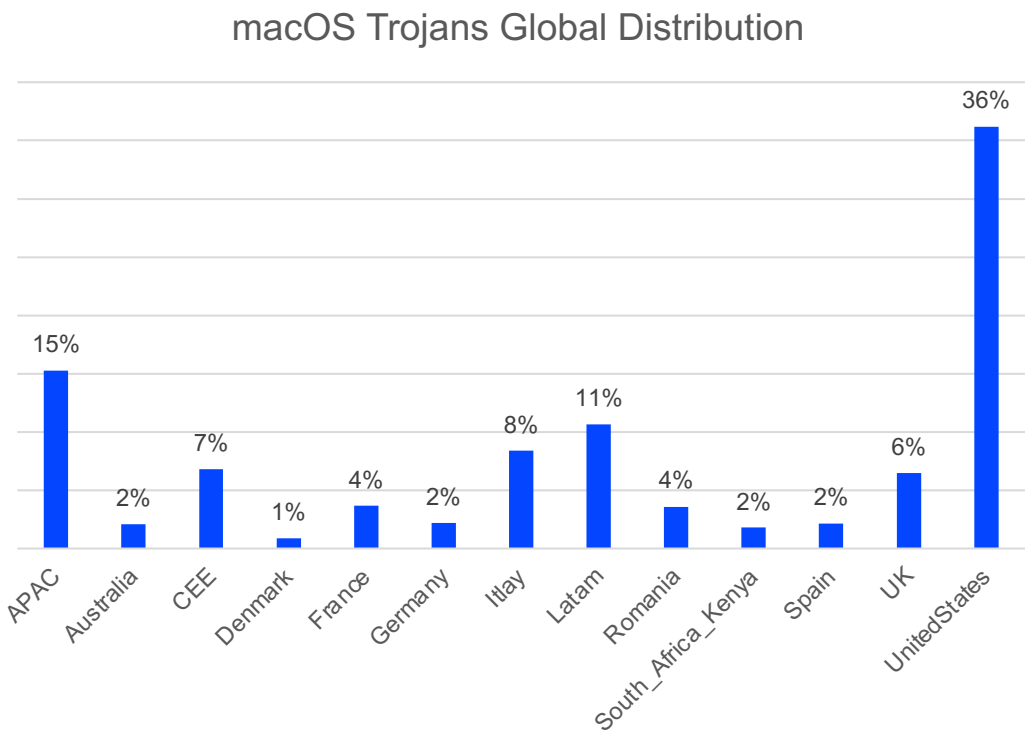


Trojans

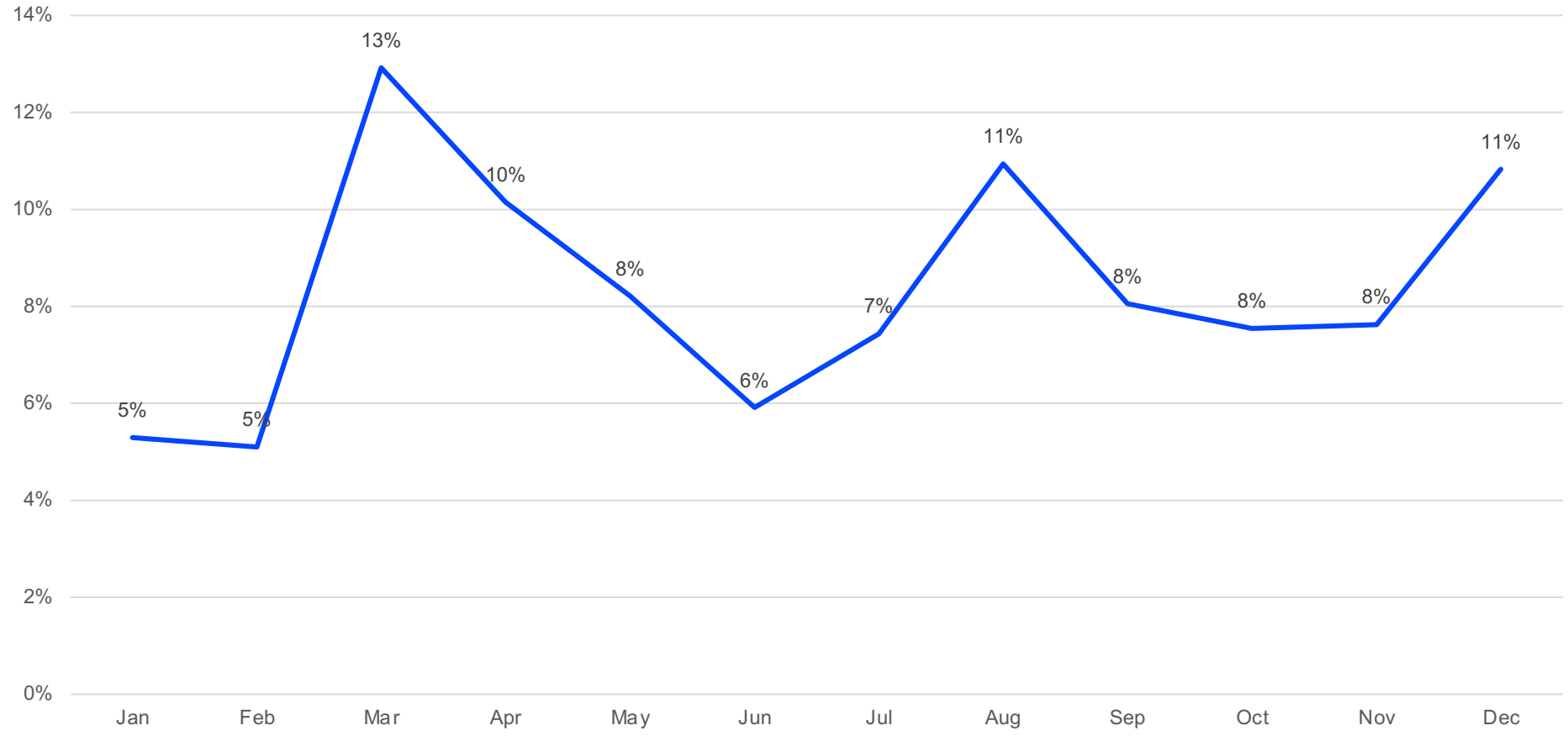
The delivery method for Trojans on any given platform typically involves social engineering techniques like spam and phishing, infected websites, or scams leveraging the victim's favorite social networks. On Macs, a fair amount of Trojan infections also occur through warez sites – hotbeds for pirated downloads. Whatever the vector, Trojans are the biggest single threat to Macs, and most of those attempted attacks were picked up in the US, which registered 36% of Trojan activity targeting macOS globally in 2021 – unsurprisingly so, considering the US likely has the biggest macOS install base in the world. The Asia Pacific region registered 15% of the attacks unfolding last year, followed by Latin America with 11%.

In the single-digit ranking, Italy stands out with 8% of Trojan-based attacks, surpassing the 7% accrued by all of the Central and Eastern Europe regions. Next are the UK with 6%, and Romania and France with 4% each. Less targeted territories like Spain, South Africa and Australia registered only a 2% share each. Denmark in 2021 was almost exempt from Trojan attacks on Macs, registering just 1% of the total.

Attacks leveraging Trojans were spread out fairly evenly throughout the year, with only a few spikes, in March, August and December. As the graph below shows, the start of the year saw considerably less Trojan activity than the months that followed.



macOS Trojan Activity



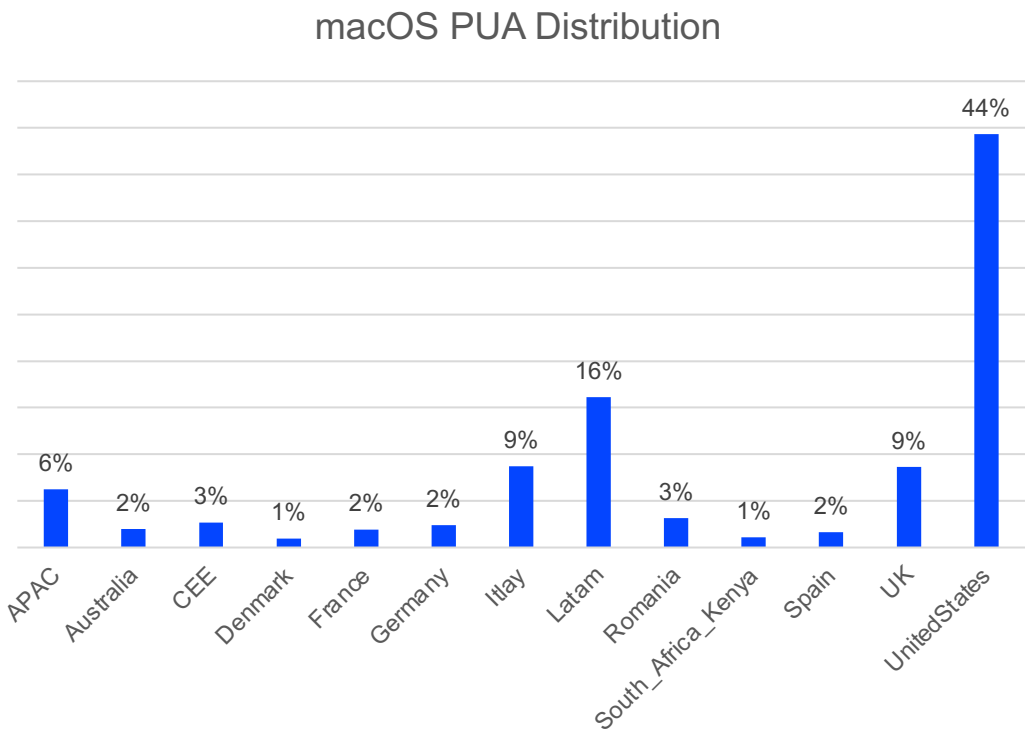
Potentially Unwanted Applications (PUA)

PUAs walk the thin line between nuisance and hazard, only rarely acting as a vessel for actual cyber threats. However, PUAs do affect user experience quite a bit.

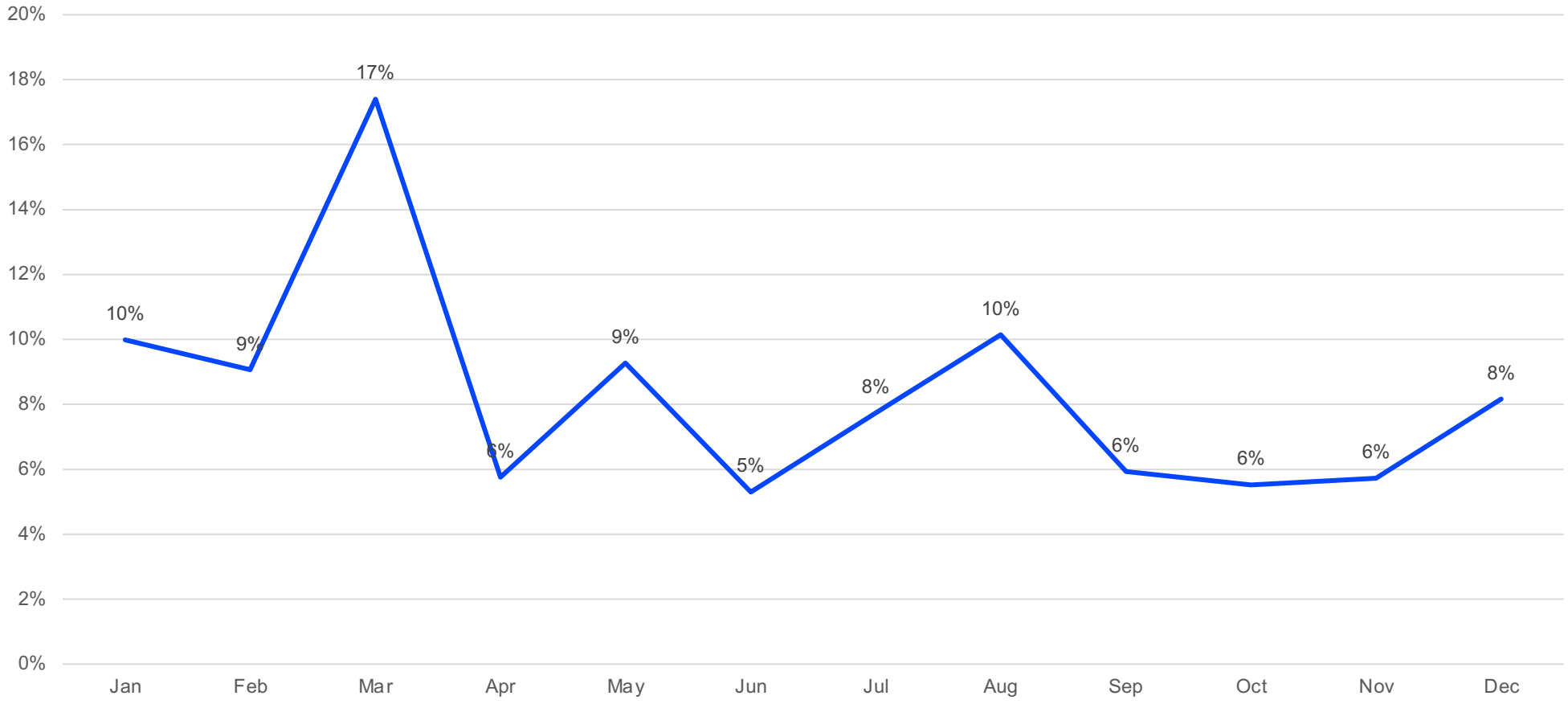
PUAs are most commonly found as freeware, repackaged applications, system cleaners or other utilities with hidden functionality like data tracking and coin mining. PUAs sometimes also hijack the user's browser, altering its functionality, like changing the default search engine and installing plugins without consent. Some of the most aggressive PUAs also modify third-party apps, download additional (unsolicited) software, and alter system settings.

A recent PUA we are analyzing in our labs is a type of scareware that claims the system is exhibiting problems that require immediate attention. Unsurprisingly, the solution to these problems sits behind a paywall. Under the hood, these scareware PUAs lack the code to back those claims.

In 2021, PUAs were by far mostly prevalent in the US where 44% of all attempted installs occurred. Latin America takes second place with a distant 16%. The rest of the regions analyzed in this report are in the single digits, with Italy again standing out, at 9%. This time, it is joined by the UK, also with 9% of attempted PUA installs. The APAC region registered a 6% share, while the rest of the geographies recorded much smaller numbers. The presence of PUAs on Macs spiked in the February – April period. Reports were relatively even throughout the rest of the year.



macOS PUA Activity



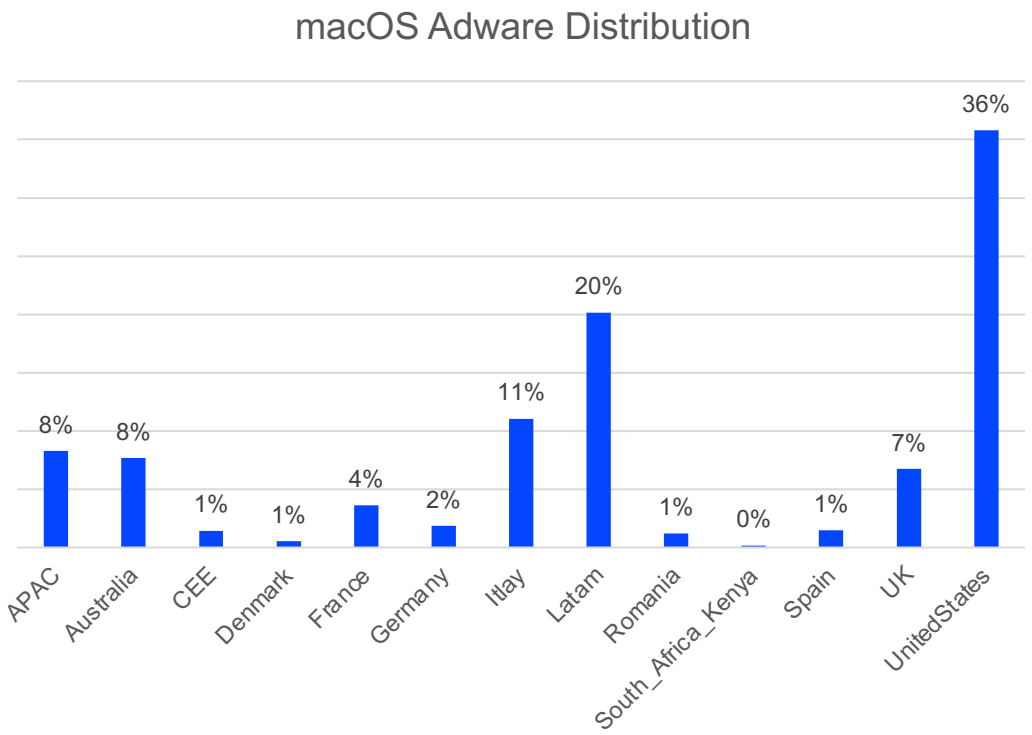
Adware

Adware enables some developers to make money out of advertising other products, sometimes in an aggressive way and with spyware-like behavior.

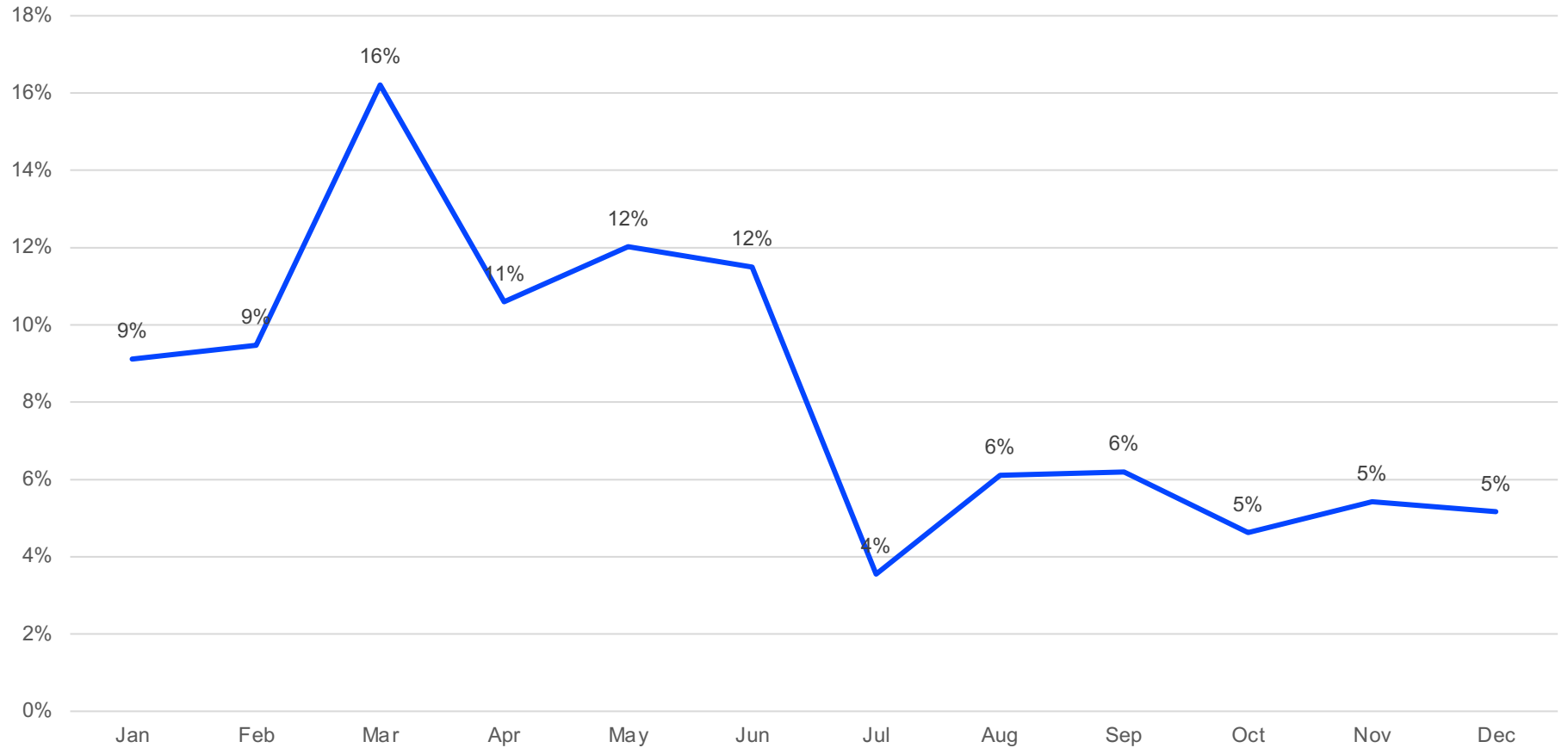
Spotting adware is easy, even with the naked eye, as it forces you to click through to a website against your will to generate artificial revenue for those controlling it. Users typically get infected with adware from Trojans, browser extensions or warez downloads. Adware can sometimes also adopt scareware behavior and is considered a true cyberthreat. Adware may even sell your data to third parties.

As with most other threats, Adware is most prevalent in high-yield territories like the United States (36%) and Latin America (20%), while Italy registers high targeting of its Mac user base with Adware. Australia and the APAC region have also been targeted fairly extensively, together registering 16% of global Adware activity. The UK registers 7%, while the rest of Europe is in the low-single digits. Africa has been virtually exempt of Adware attacks in 2021.

Attempts to infect Macs with Adware spiked between February and June, with the month of March registering the peak, at 16% of attempted infections. The second half of the year marked a considerable decline in Adware activity targeting macOS computers.

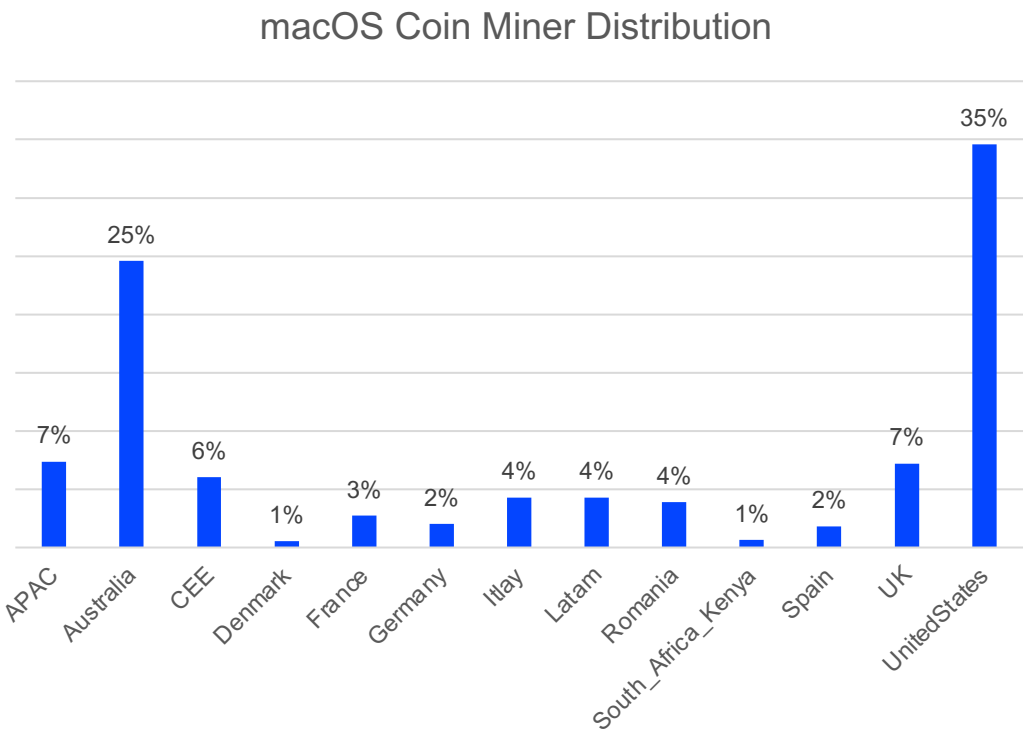


macOS Adware Activity

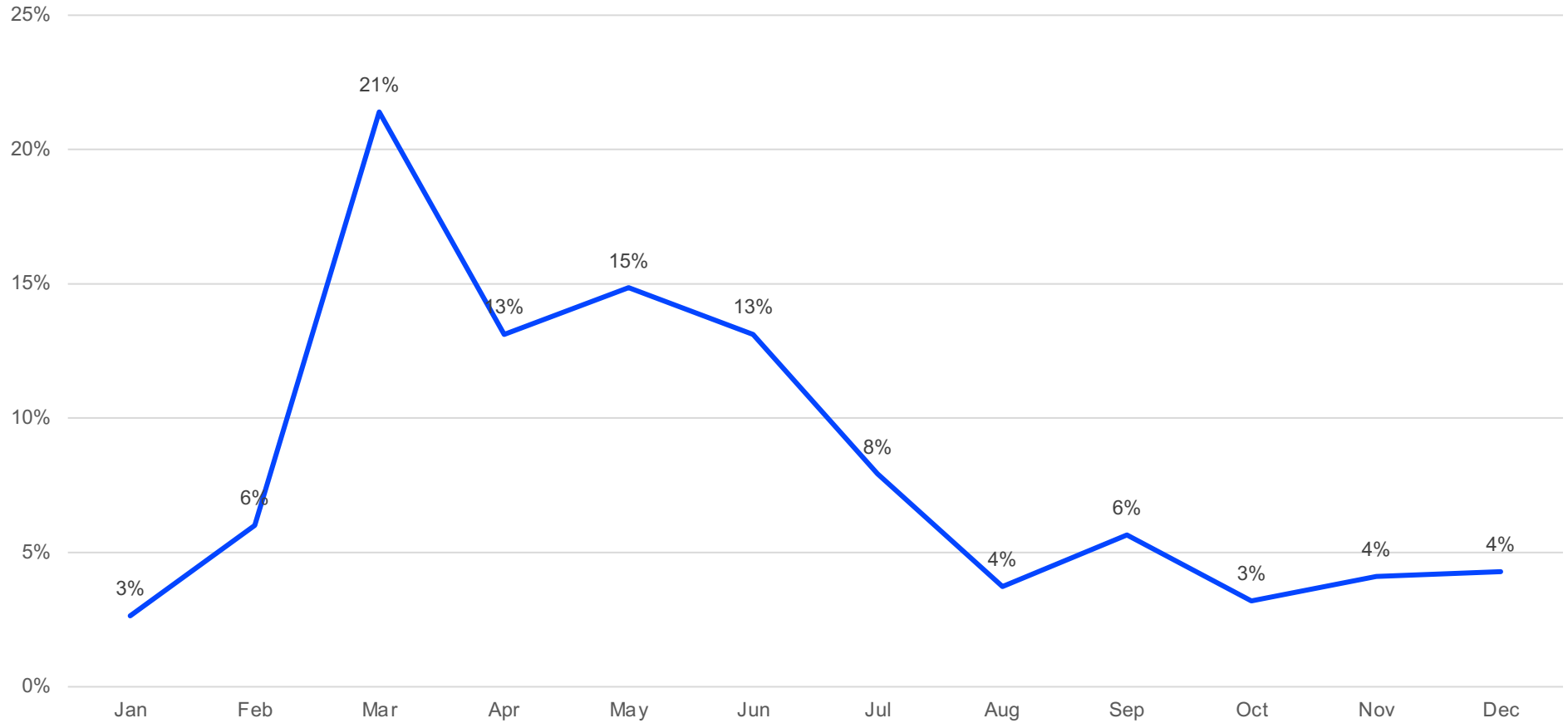


Coin miners

Mining cryptocurrency remains popular. Most of the malicious mining targeting Macs stems from Trojan infections. However, some coin mining activity is also done by users who willingly leverage their Macs' computing power for personal gain.



macOS Coin Mining Activity



ANDROID THREAT LANDSCAPE

Android security is not getting any better

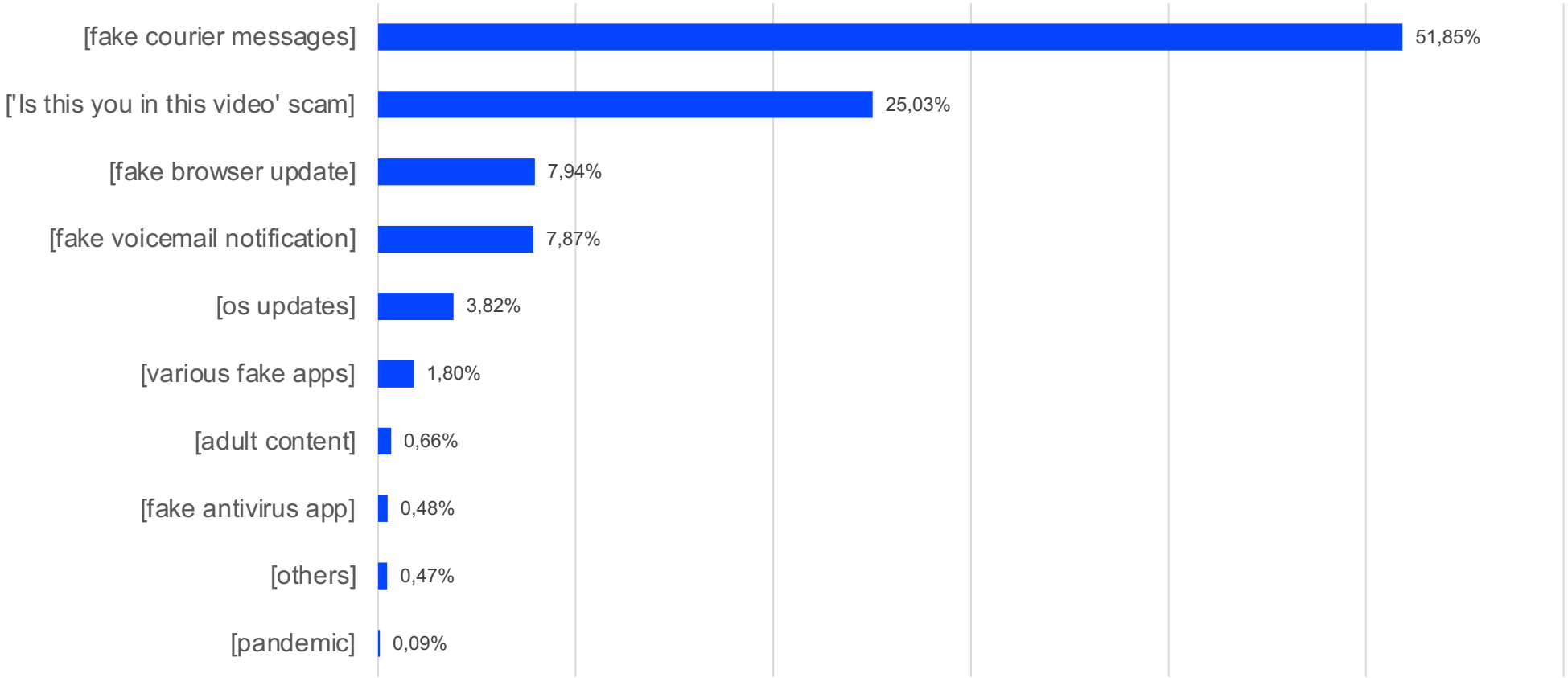
Android rules the mobile world with its 70% market share, which means it's more exposed to risks than other platforms.

Coupled with OS fragmentation, one of the most significant issues of the platform, it's easy to understand why so many threats plague Android every day and why criminals devote time and effort to developing new threats.

2021 was anything but a typical year. The effects of the Covid-19 pandemic influenced the tech world, including cybersecurity and mobile threats. Criminals continued to adapt their tactics to mirror relevant events in society.

An excellent example of this type of tactic resides with the TeaBot and FluBot campaigns, which had a global reach and used vastly different methods to disseminate organically. FluBot spreads through SMS sent from already-infected devices, carrying messages regarding fake voicemail notifications or fake courier messages, among others.

Types of malicious SMS for distributing FluBot



TeaBot is another threat spotted in the wild that spreads through fake apps sometimes hosted in official stores. Attackers went even further and bought ad space in legitimate, widely used Android apps that link to malicious trojan droppers.

For example, a QR code reader app hosted in Google's Play Store was observed spreading 17 different types of TeaBot variants quickly.

On several occasions, Google removed numerous malicious apps from its official store in 2021. Also, researchers found that attackers have been using Samsung's official Galaxy Store to spread malware in the form of Showbox clone apps.

QR Code Reader - Scanner App

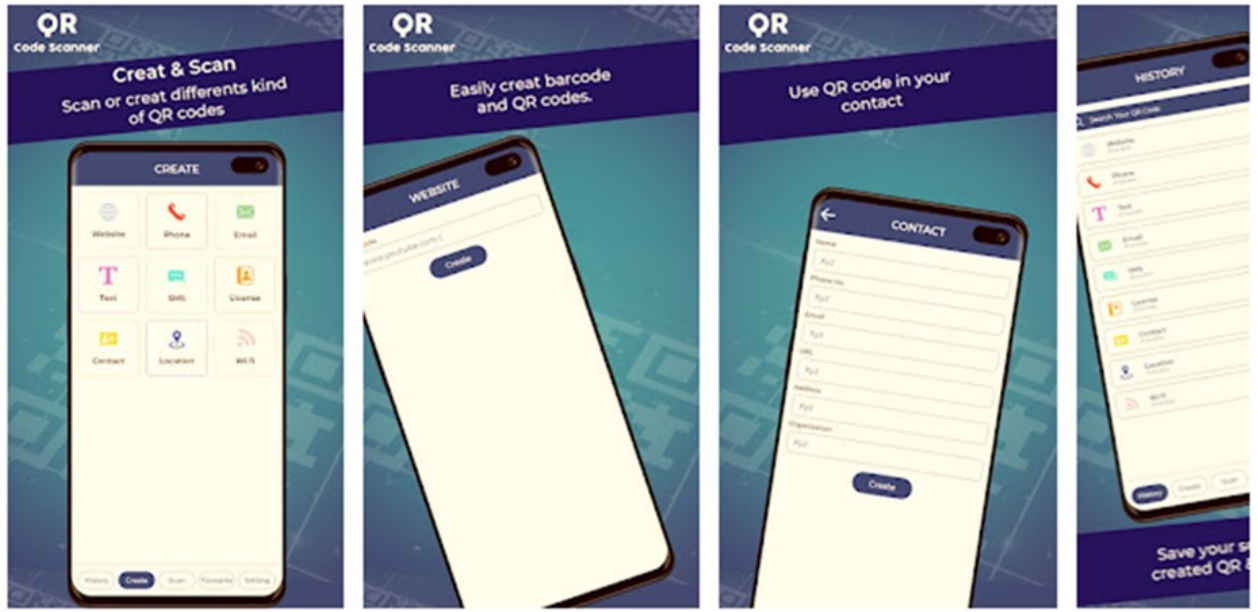
Qr Code Scanner & Generator LDC **Tools**

PEGI 3

This app is available for your device

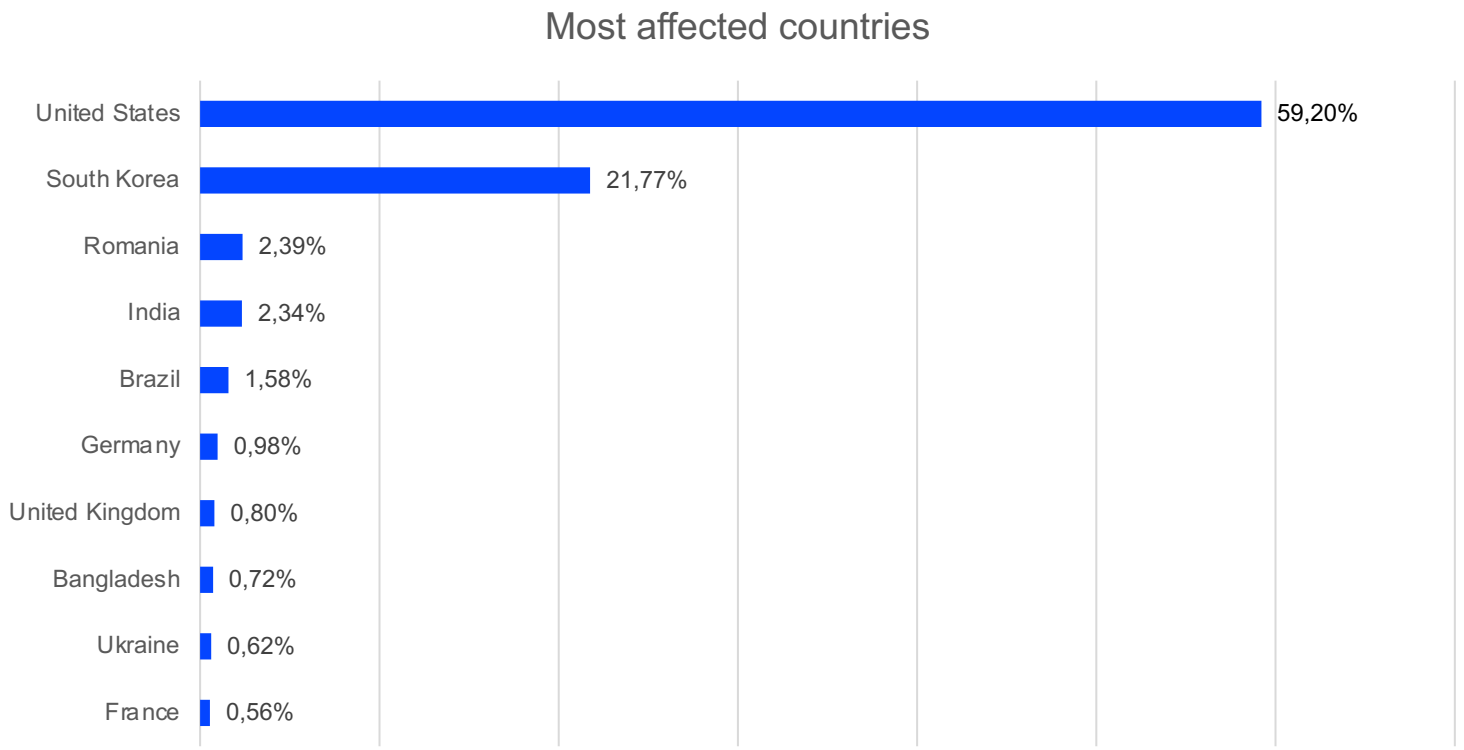
Add to Wishlist

Install



Stalkerware

Stalkerware is a dangerous, insidious type of app that can cause serious harm. Bitdefender's telemetry identifies it as malicious, especially since not all stalkerware apps are evident in their use. In some cases, apps used to transform old phones into surveillance devices could also be deployed as stalkerware.



Scam Alert to the rescue

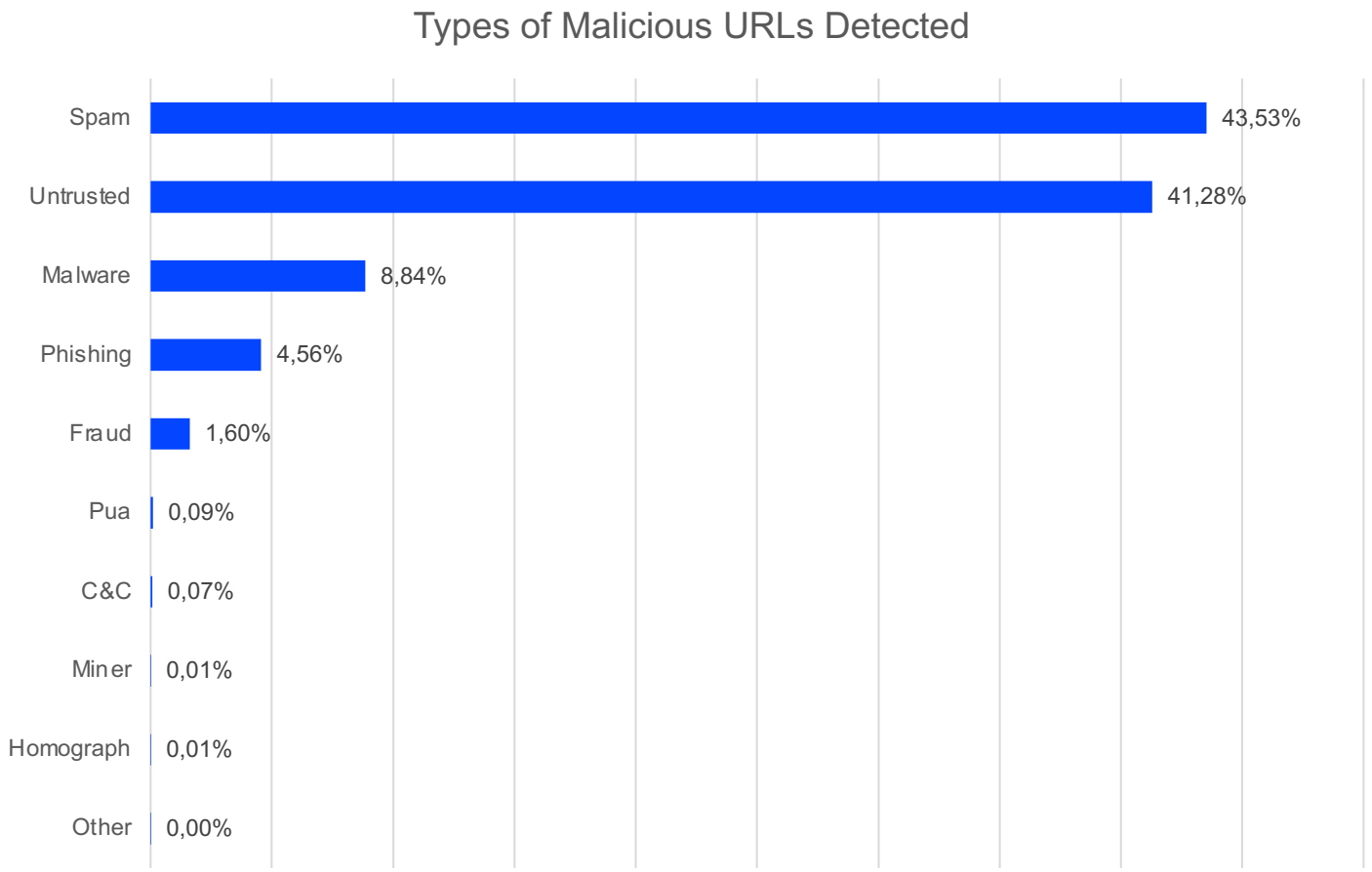
A new feature in the Bitdefender Mobile Security & Antivirus client in the last few months of 2021 helps us paint a complete picture of the scam and fraud landscape.

Scam Alert helps stop attacks in their early stages, long before they could pose a threat to users. It also offers unparalleled visibility that shines a new light on the emerging threats on Android and beyond.

Spam and untrusted URLs

Spam and untrusted URLs go hand in hand in this situation, demonstrating that attackers are rapidly shuffling through compromised domains to outwit security solutions. The bulk of the spam detections see India in the spotlight, as this emerging market has the largest Android penetration globally.

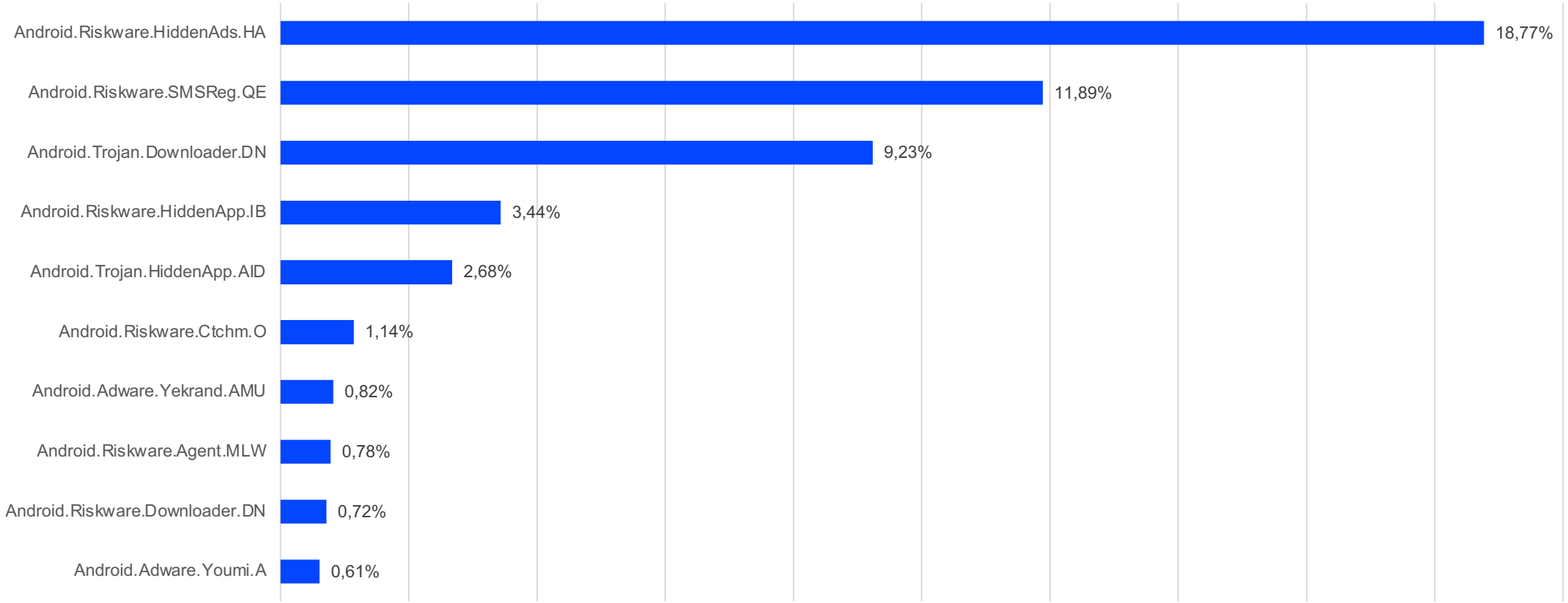
Untrusted domains have some particularity making them possibly unsafe. A secure approach is to consider them untrusted by default.



This takes us to the most common threats in the Android ecosystem. Ranking first in the list are applications that display ads invisible to the average user as a primary means of monetization.

The top 10 is home to several more dangerous apps, including a couple of downloaders that can deploy other malware and a Trojan that offers criminals complete remote access to users' devices.

Most Common Android Threats in 2021



IOT THREAT LANDSCAPE

IoT security is still not a priority for vendors

The Internet of Things (IoT) ecosystem is evolving exponentially, just as predicted. But we have a couple of caveats to consider.

The expansion of 5G networks, the rapid adoption of Wi-Fi 6, as well as two years of lockdown inside homes have pushed even more IoT devices onto the market.

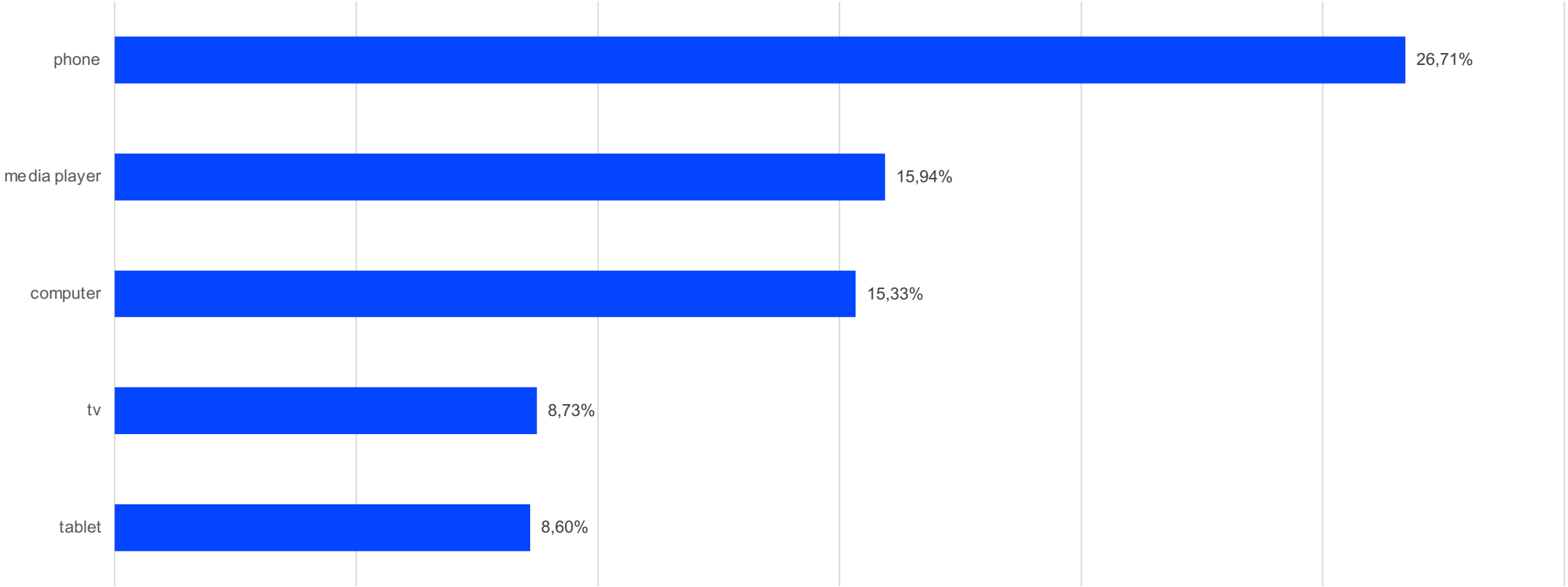
Many of the IoT devices we buy today are orders of magnitude more powerful than just a few years ago, so cybercriminals have many more opportunities to exploit them.

Popular usually means safe

The five most popular smart devices in people's homes include phones and media players. Consumers often misidentify what a smart device is and often fail to properly secure them.

Phones and computers fall directly into this category, but people might think more along the lines of thermostats or washing machines.

Most popular smart devices

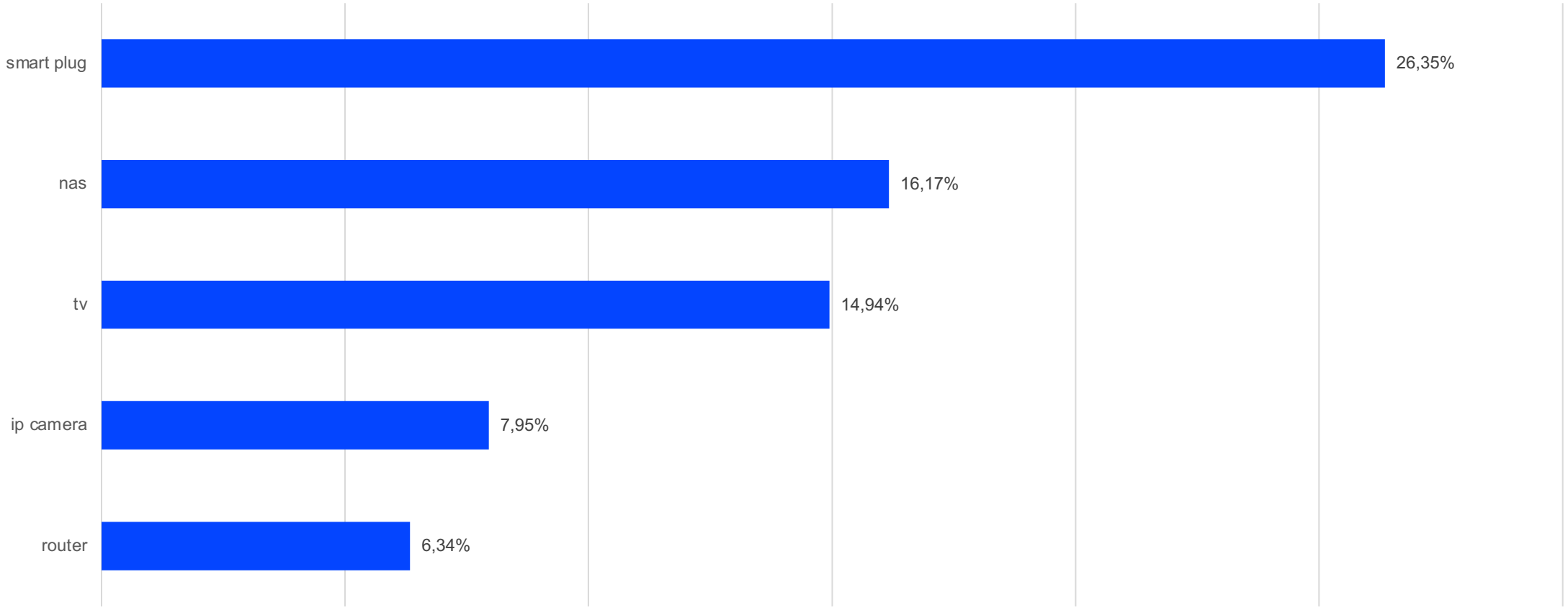


Smart plus are an unwelcomed surprise

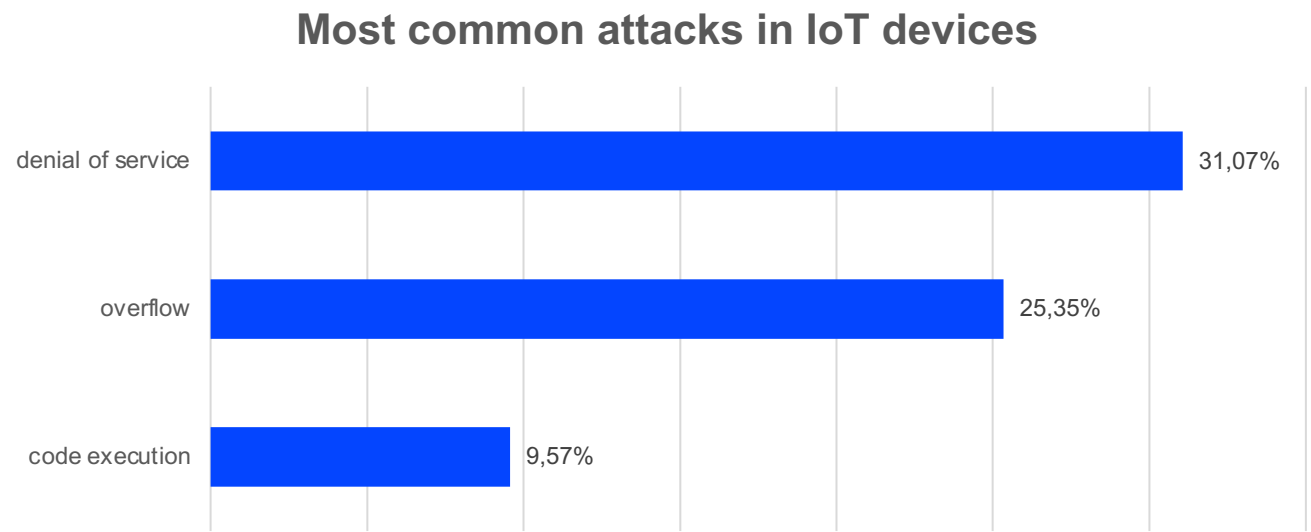
One of the most alarming statistics in the Bitdefender IoT threat landscape is the list of the most vulnerable devices in people's homes. As it turns out, the most popular devices also tend to be the safest. Most problems come from more obscure devices that lack adequate security and support.

One notable mention should go to smart plugs, which took the number one spot claimed by network-attached devices for many years. This shows that smart home automation is becoming increasingly popular.

Most vulnerable IoT devices



We know that attackers go after IoT devices, but we also understand how they target them. For the most part, denial of service attacks are the norm. To make matters worse, once an IoT device is compromised, criminals often make it part of vast botnet networks designed with a single purpose; to launch DDoS attacks themselves.

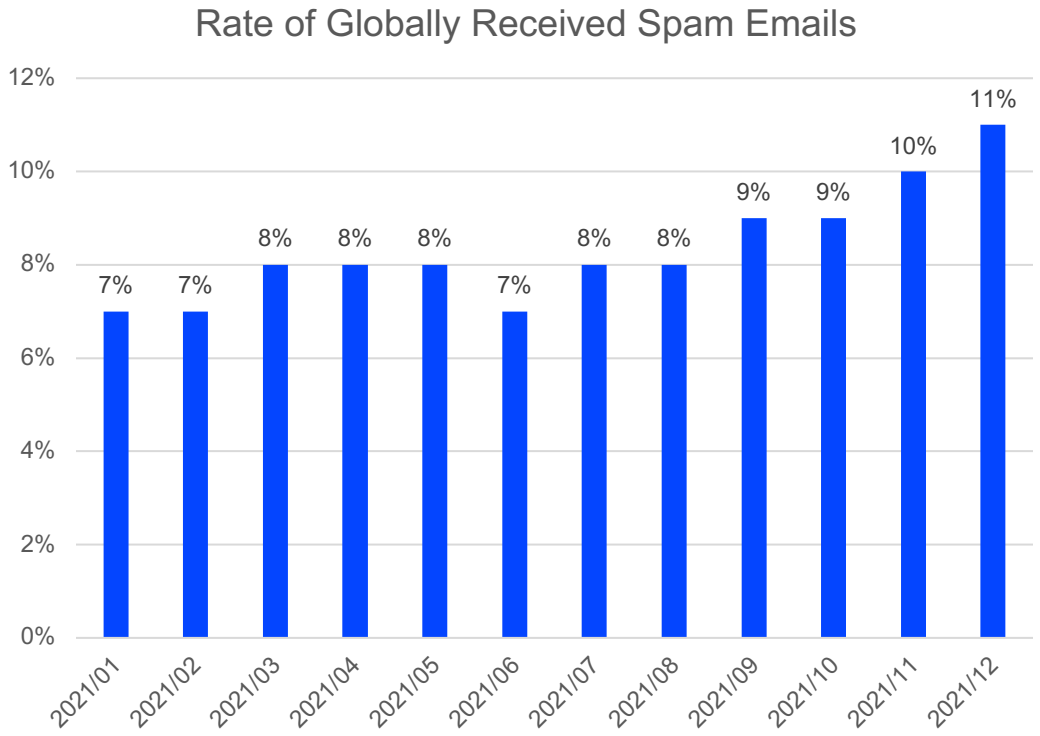


SPAM EVOLUTION

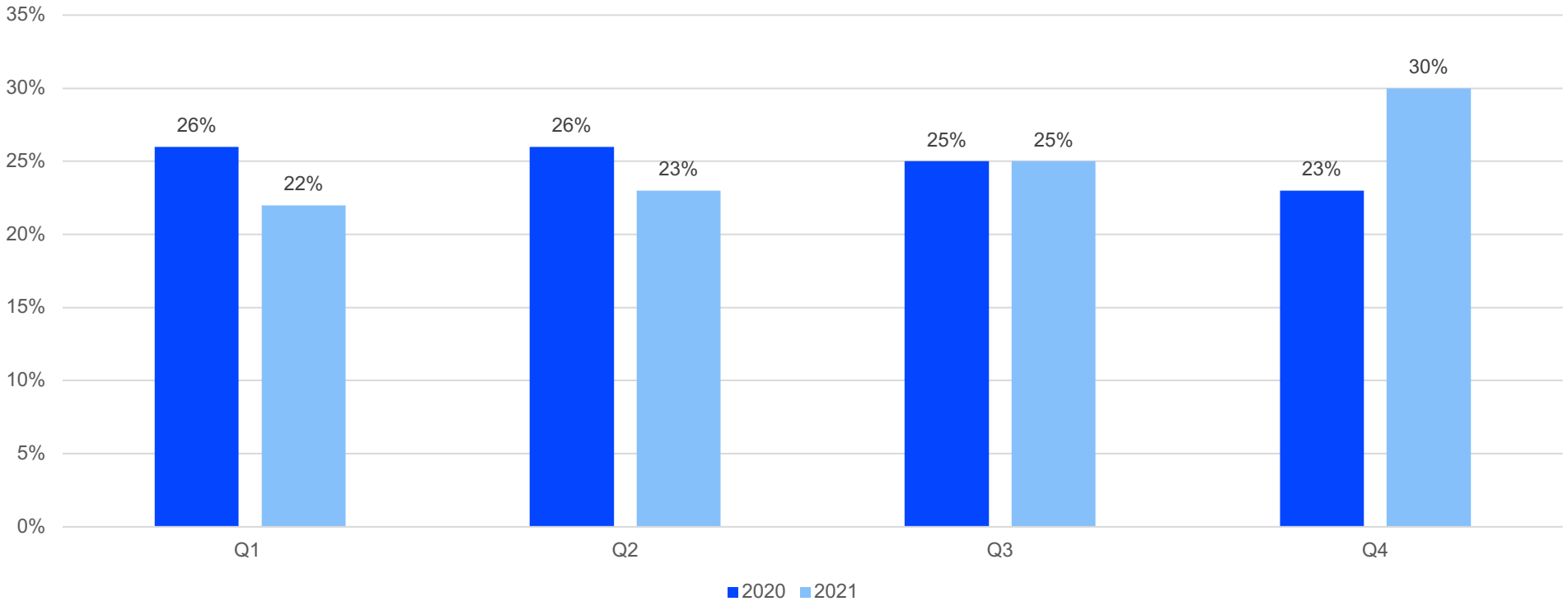
Rate of Globally Received Spam Emails

The socio-economic changes inflicted by the health crisis played an important role in the dynamic of spam and malspam campaigns throughout 2021. With firm social distancing measures established in the first half of the year, spam topics continue to reflect increased digitalization in all industry verticals as well as changes in the cyber behavior of users across the globe.

Despite a decrease in the global spam rate in Q1 and Q2 of 2021, Bitdefender detected a 7% increase in the flow of global spam between October and December 2021. Fifty-three percent of all global spam sent by volume was delivered in the second half of 2021, with more spam in December (11%) than in any other month of the year.



Global Spam Evolution



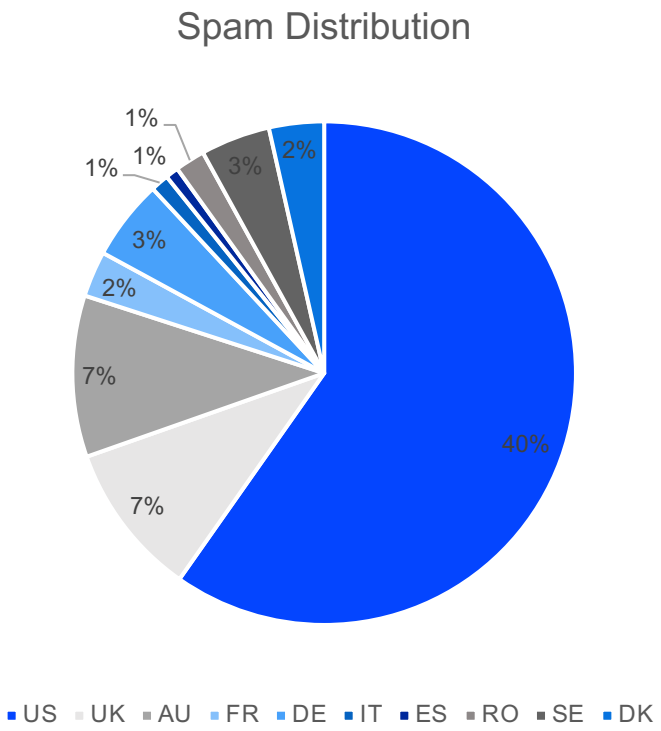
Note: The quarterly percentage of globally received spam is calculated from the entire received spam volume picked up by Bitdefender Labs during a 12-month period

Localized spam distribution

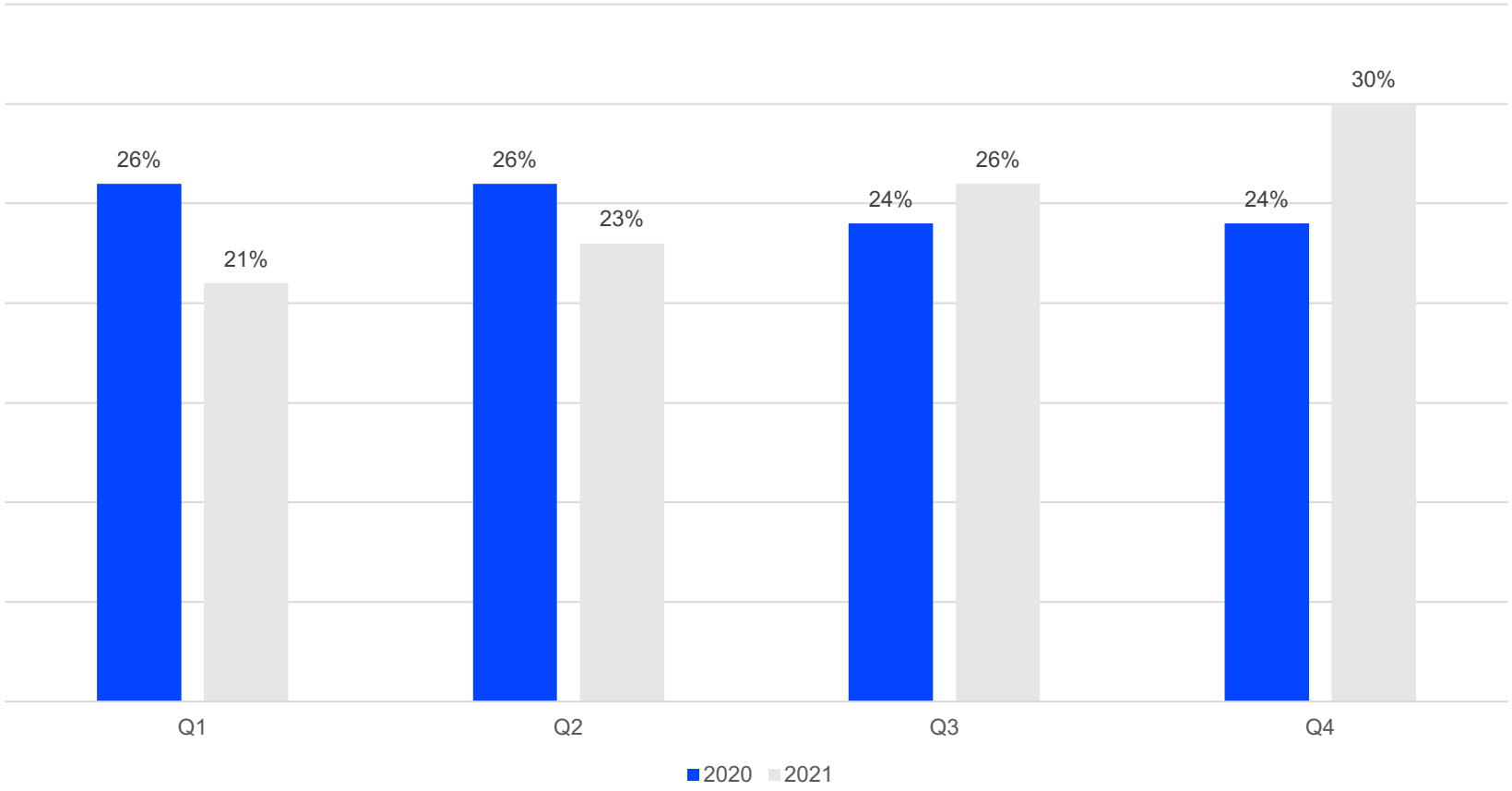
In 2021, the US received the largest share of global spam emails by volume (40%), increasing from 38% in 2020, according to Bitdefender Labs.

Received spam volume in the UK flat-lined at 7%, while Australia gained 4 percentage points (from 3% in 2020) holding the second spot in the global outline of received spam alongside Brits, also at 7%. Sweden and Germany shed 2 percentage points, coming in third place with 3% each.

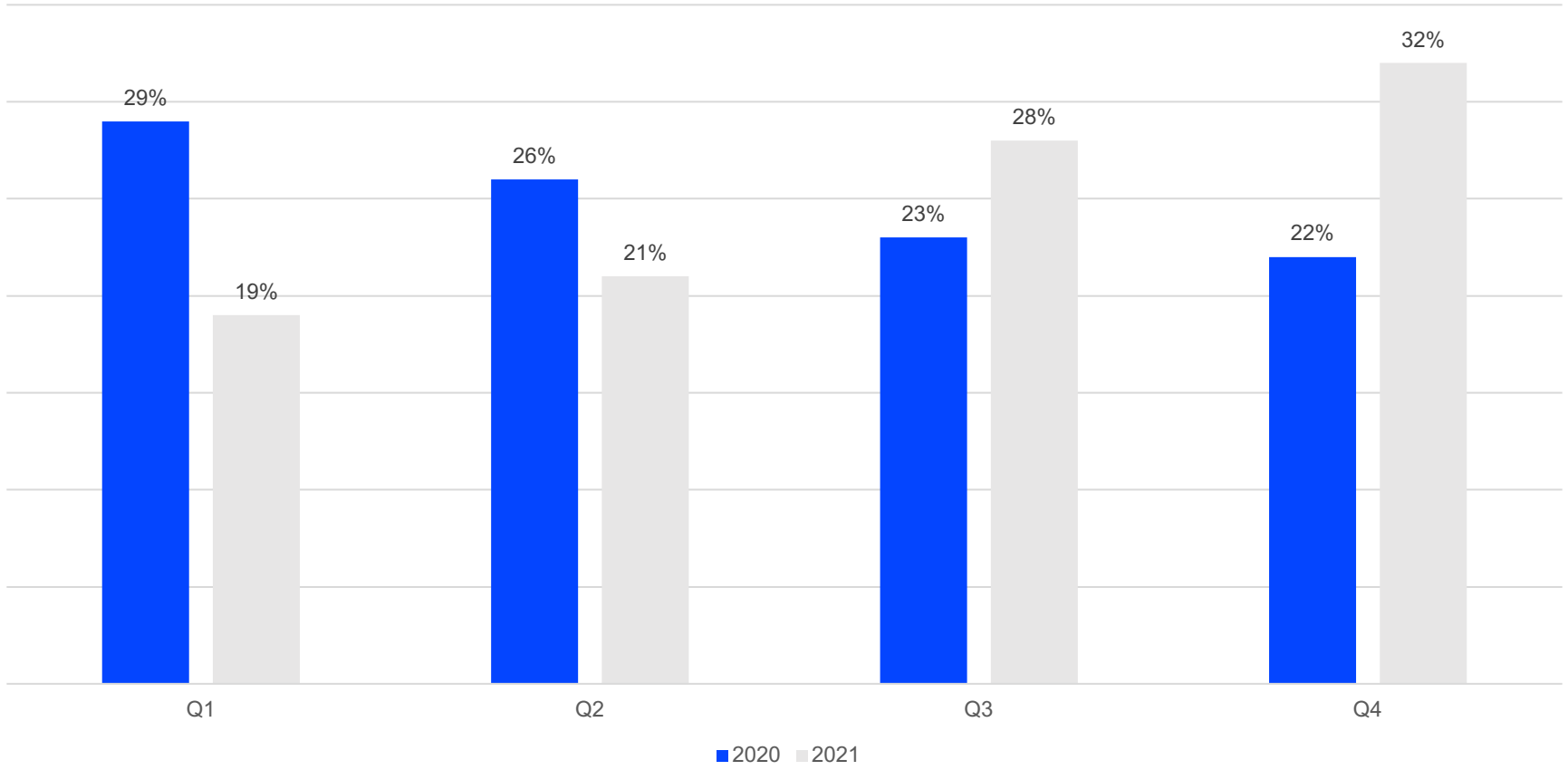
Note: Localized spam percentages are calculated from the entire spam volume received by each individual country during a 12-month period



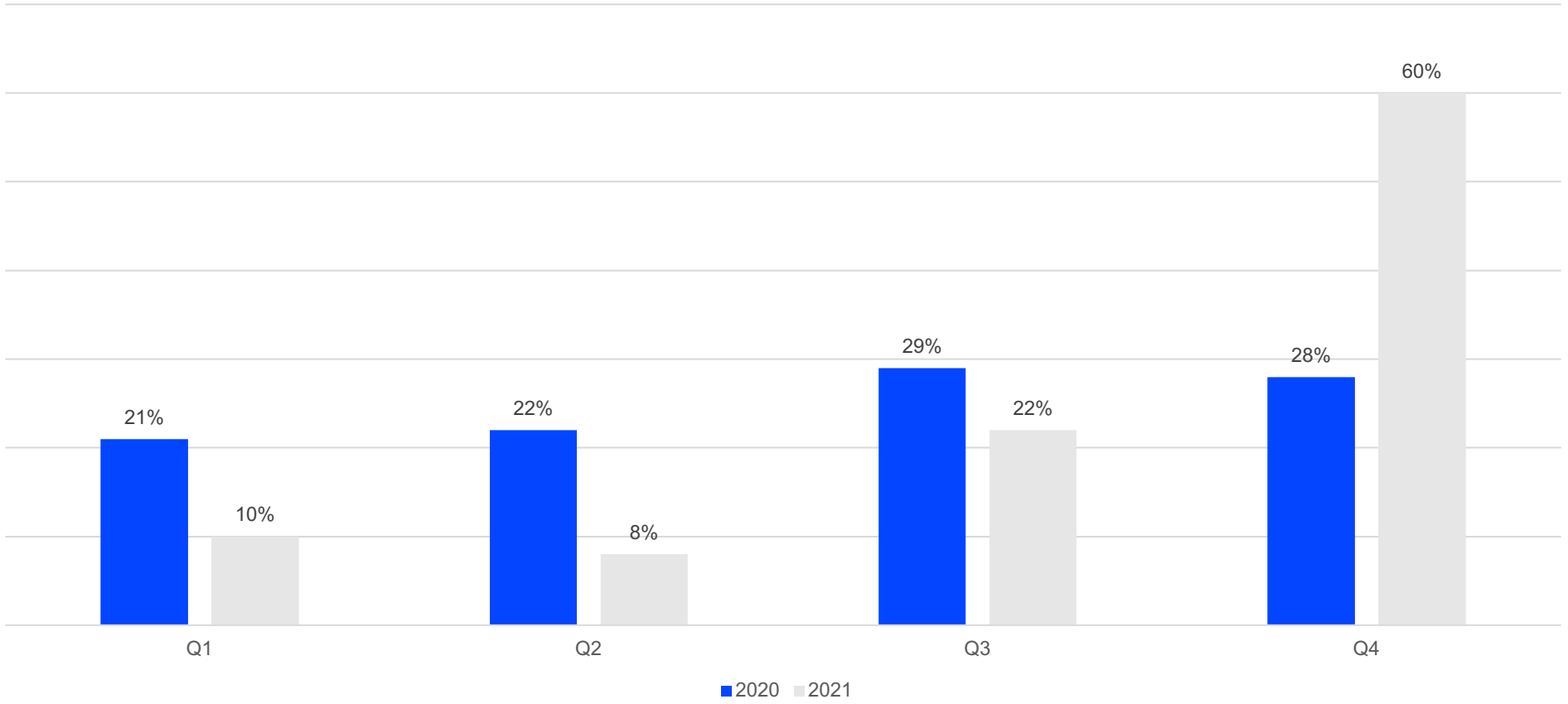
US Spam Evolution



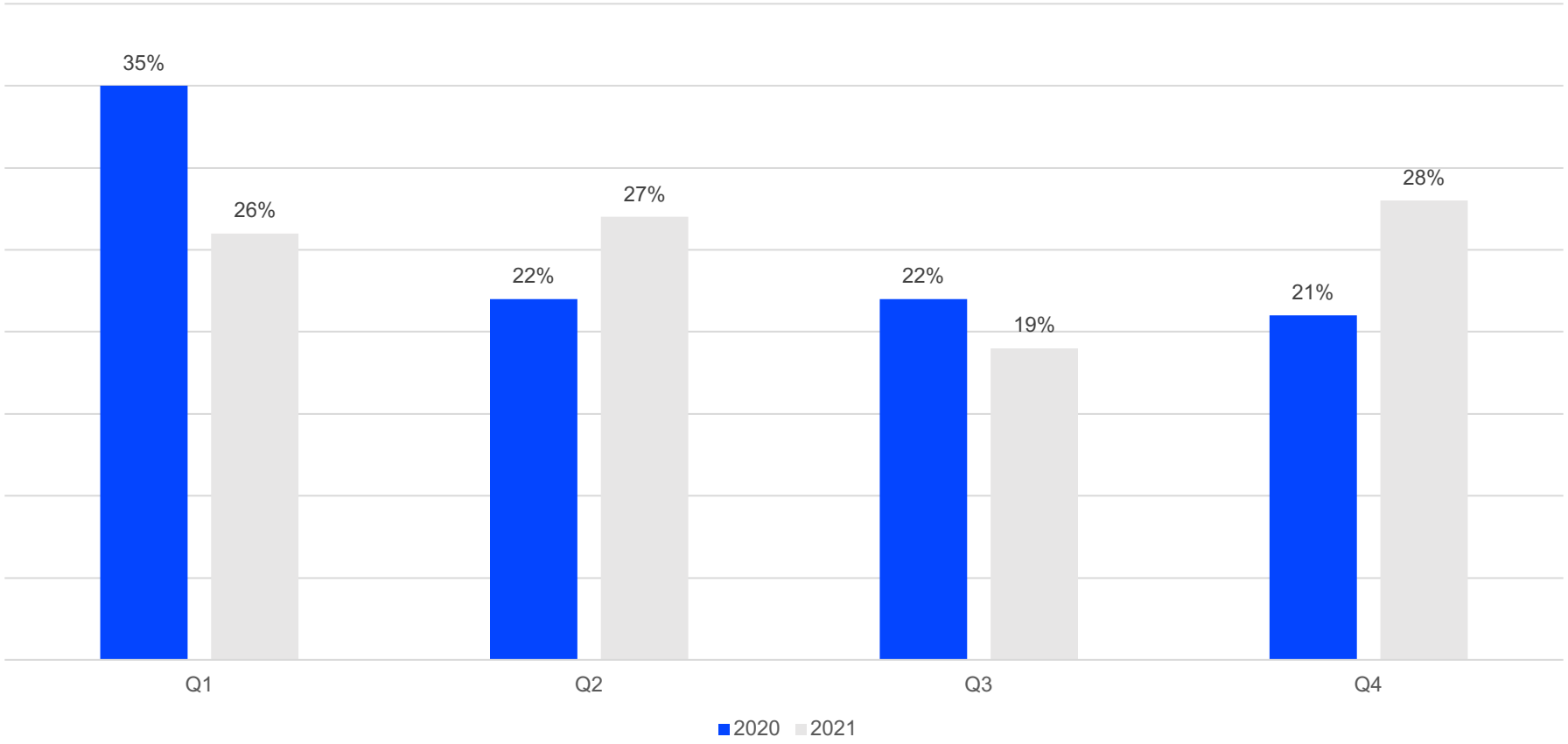
UK Spam Evolution



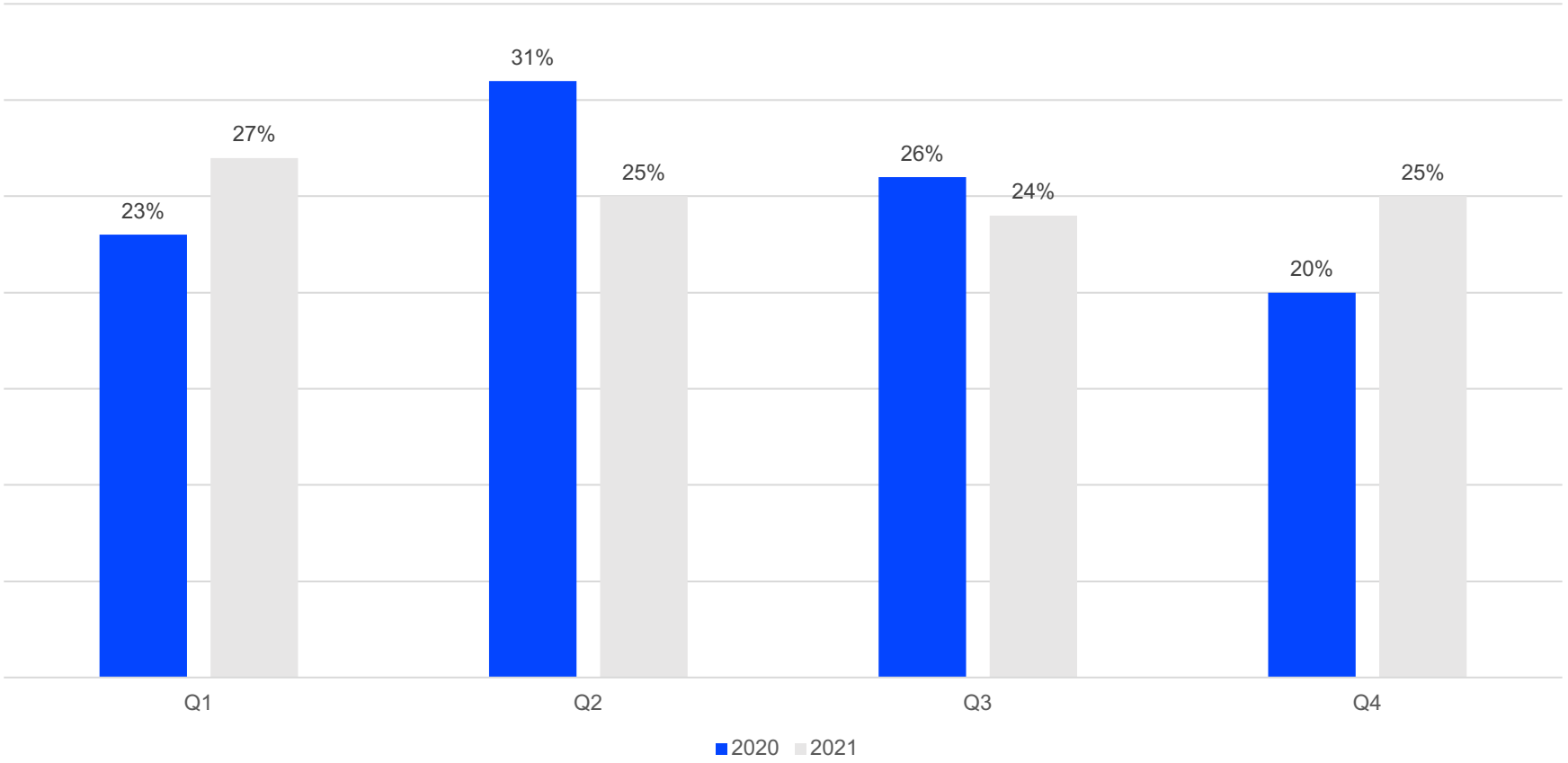
AU Spam Evolution



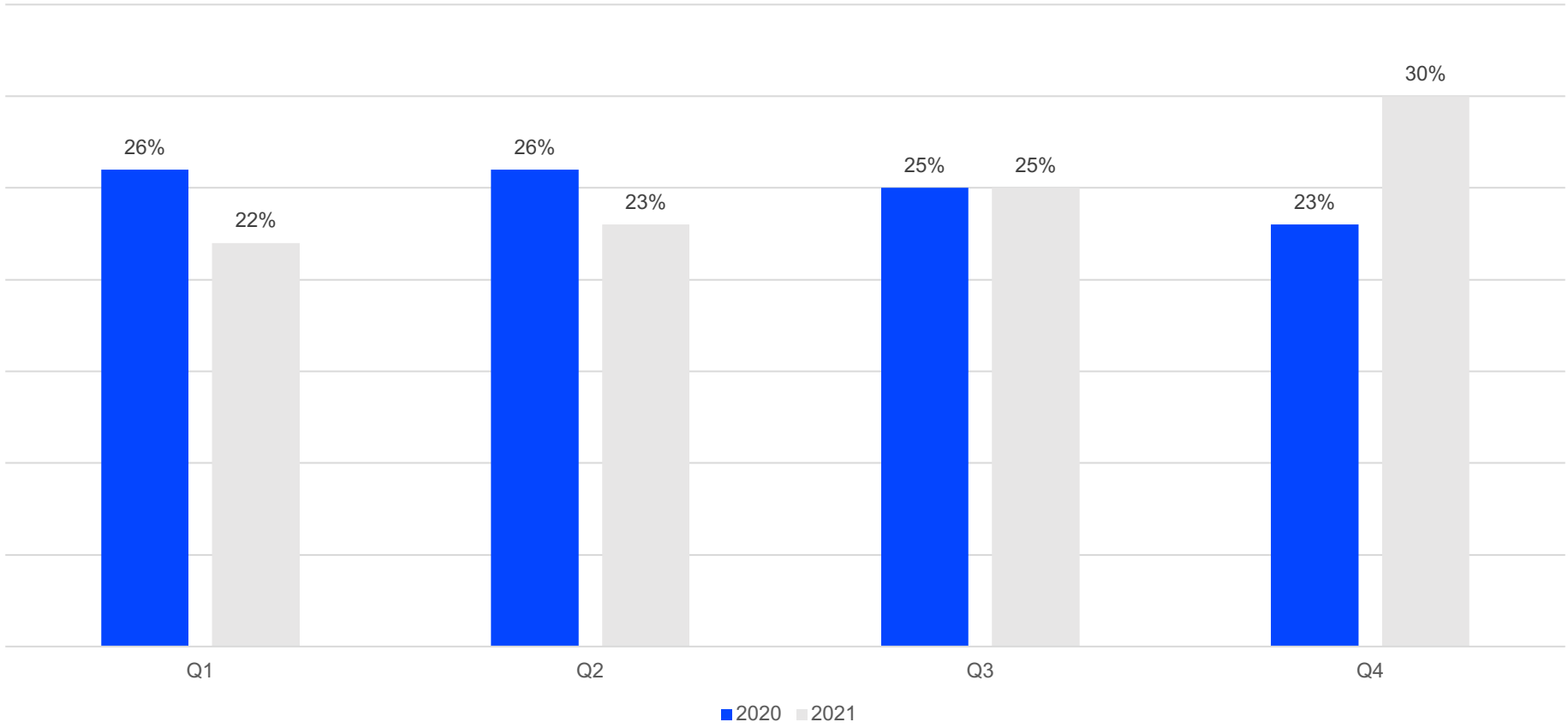
DE Spam Evolution



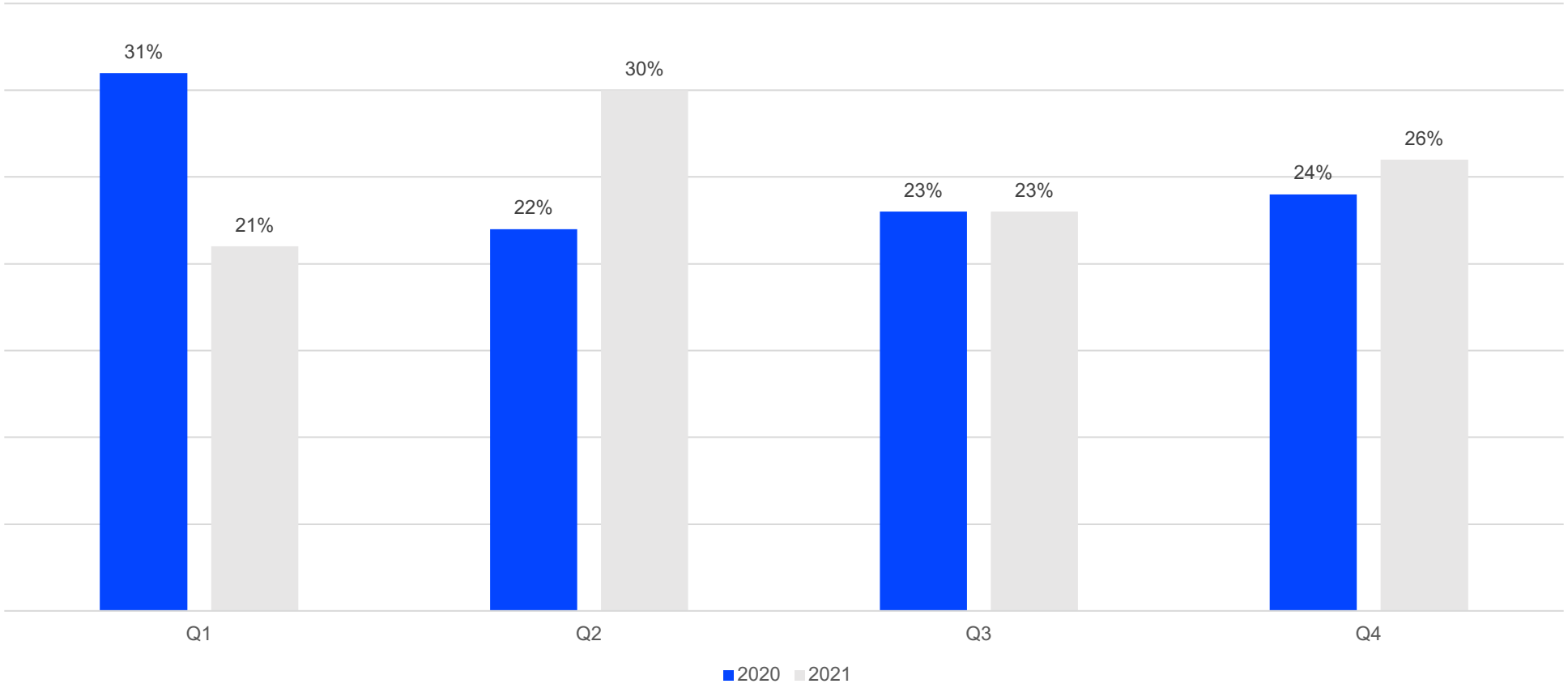
DK Spam Evolution



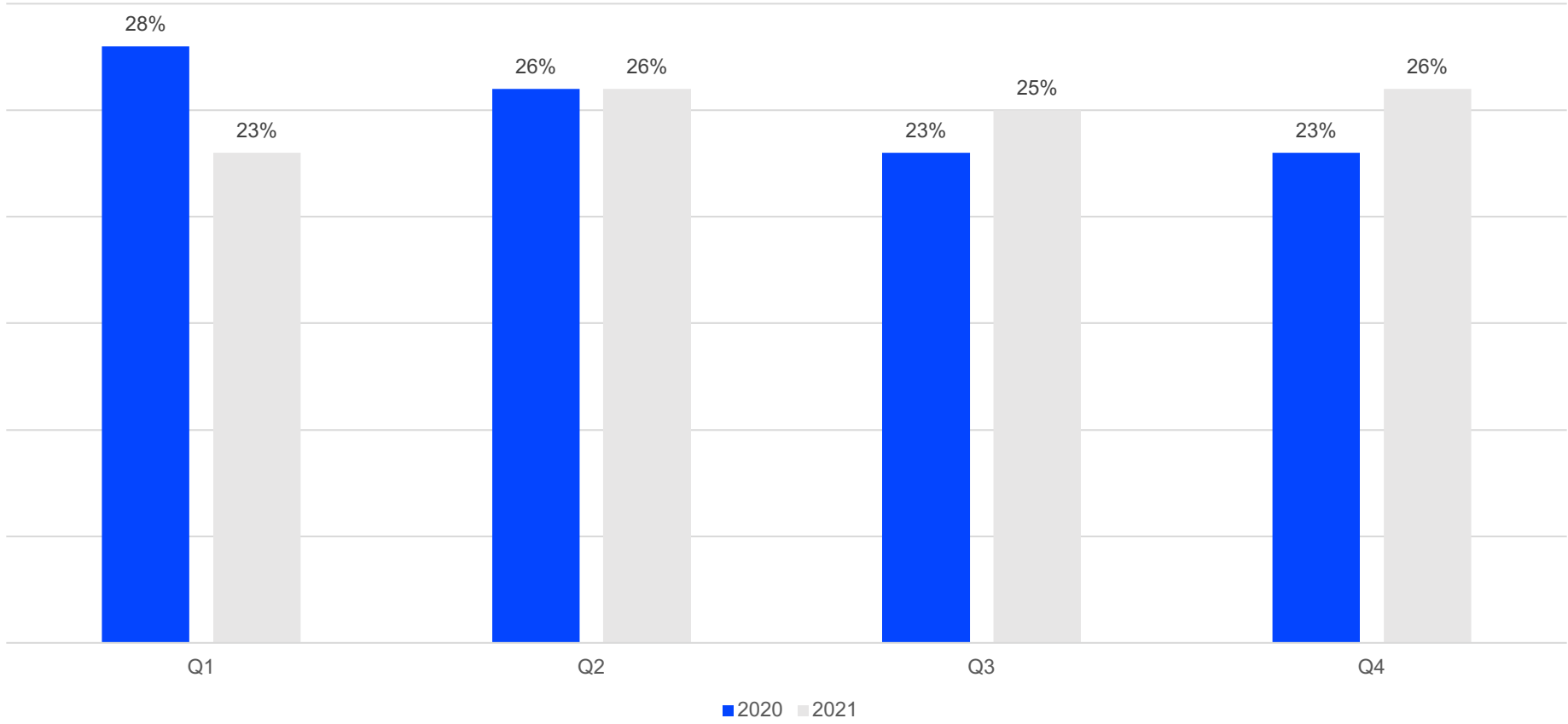
SE Spam Evolution



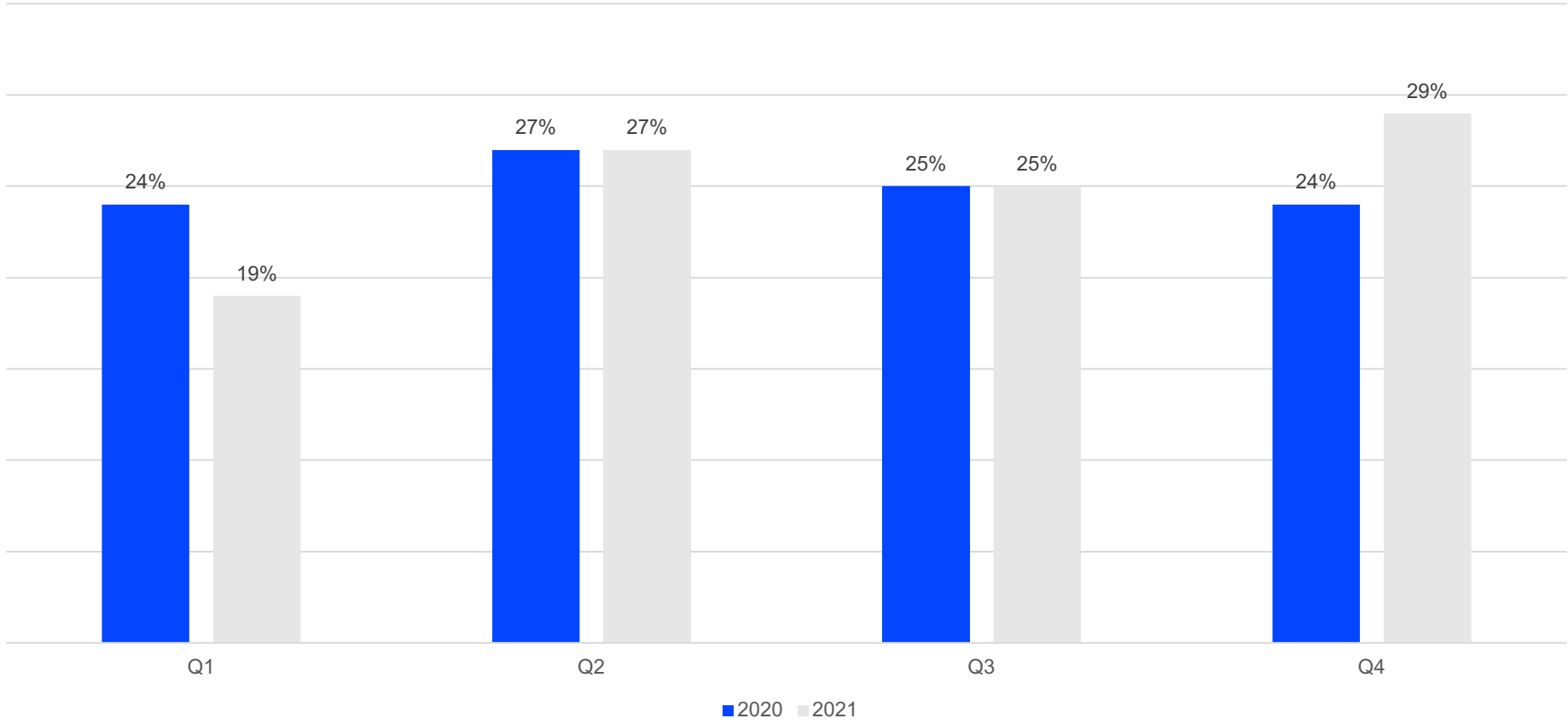
RO Spam Evolution



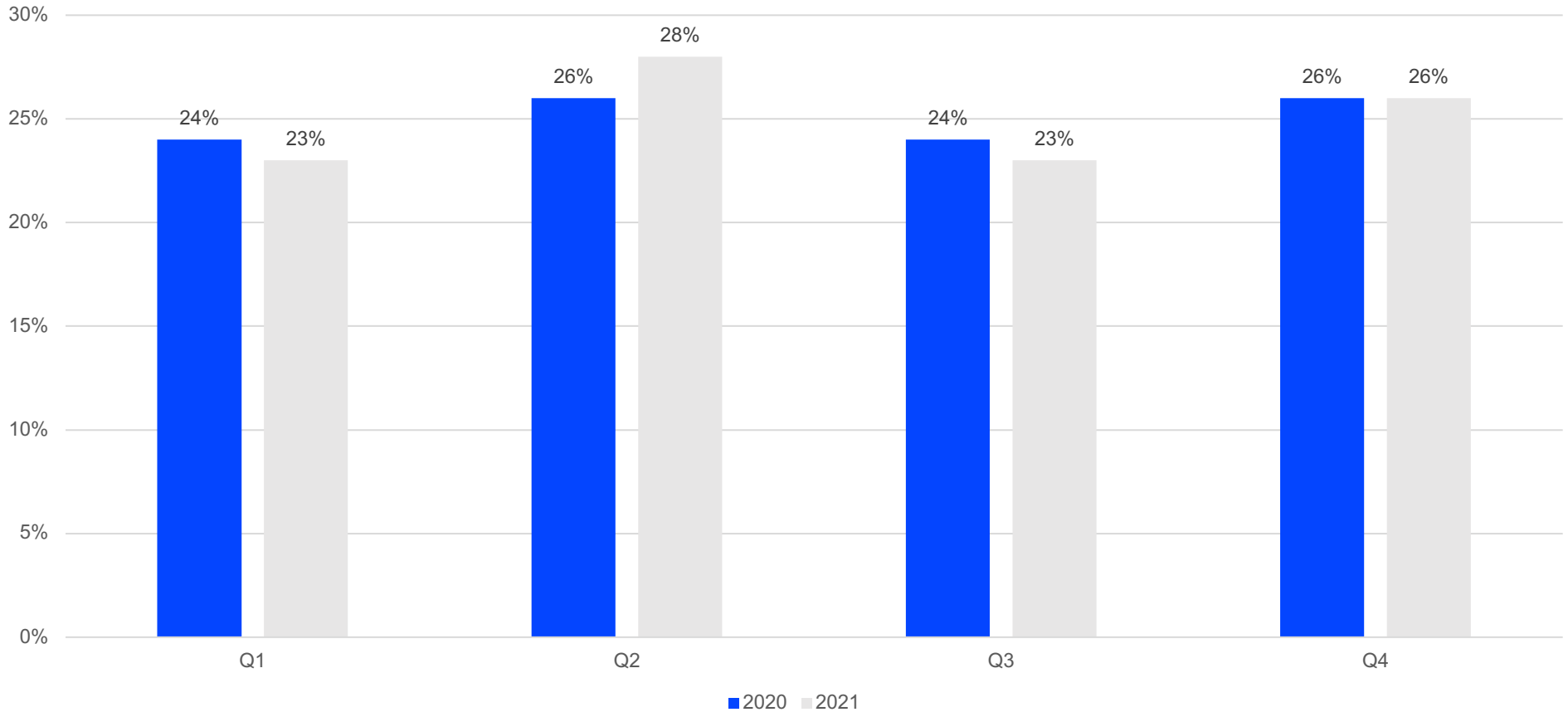
FR Spam Evolution



IT Spam Evolution

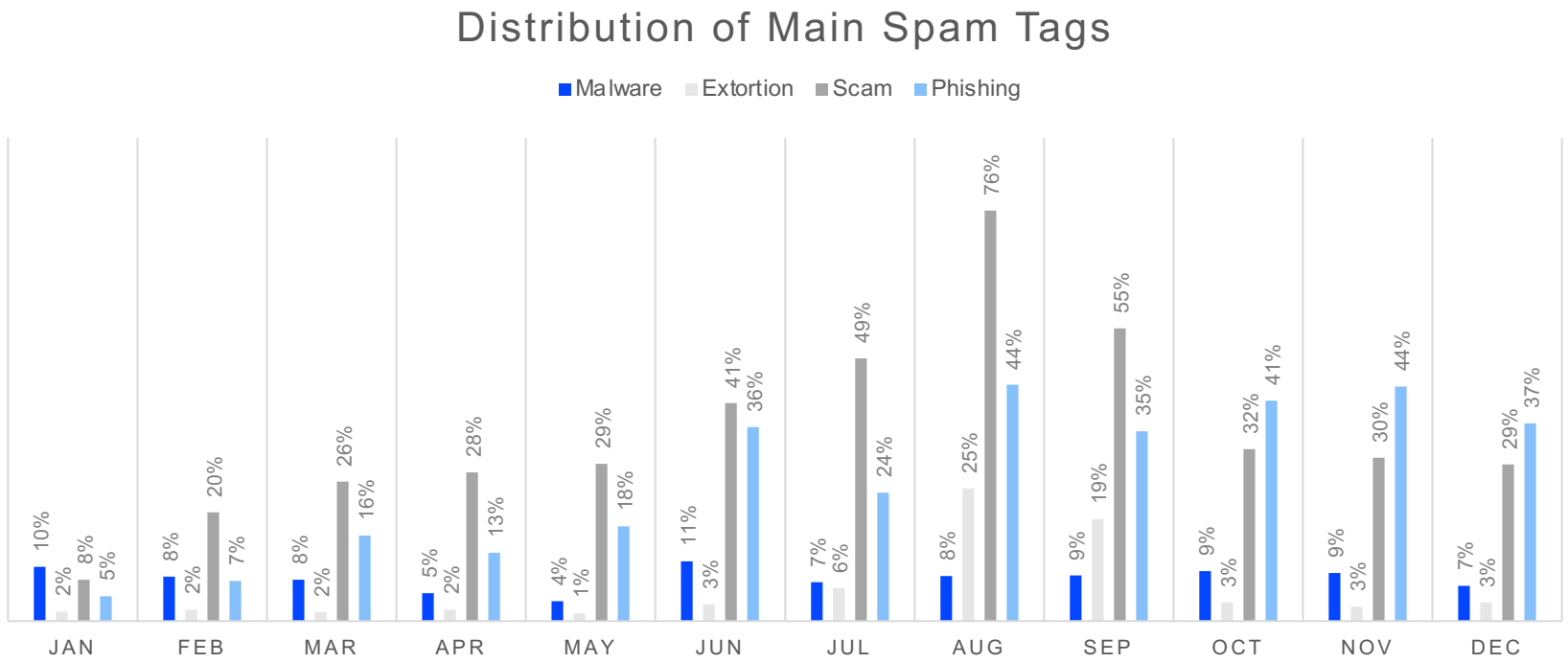


ES Spam Evolution

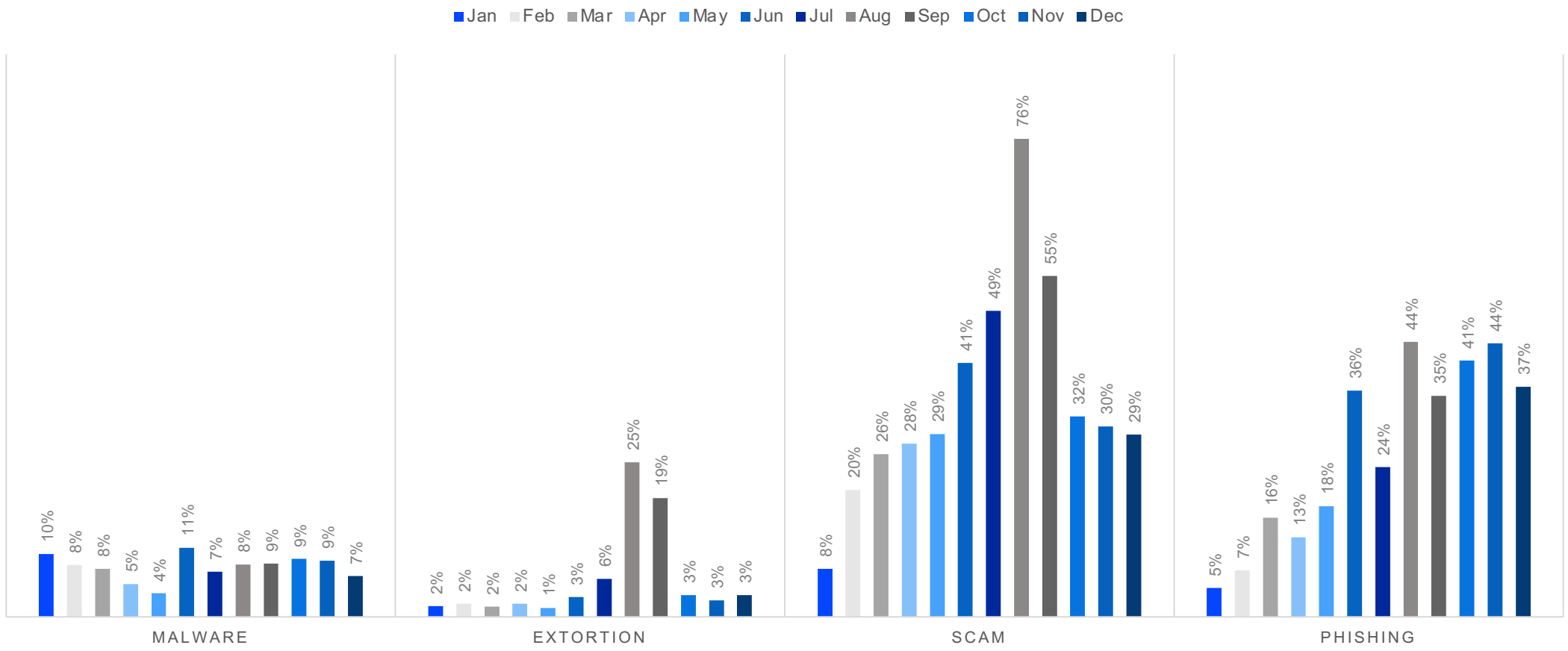


Spam trends

On average, 93% of received emails scanned by Bitdefender antispam filters were marked as spam in 2021, with an average of 35% scams, 27% phishing, 8% malware and 6% extortion emails detected.



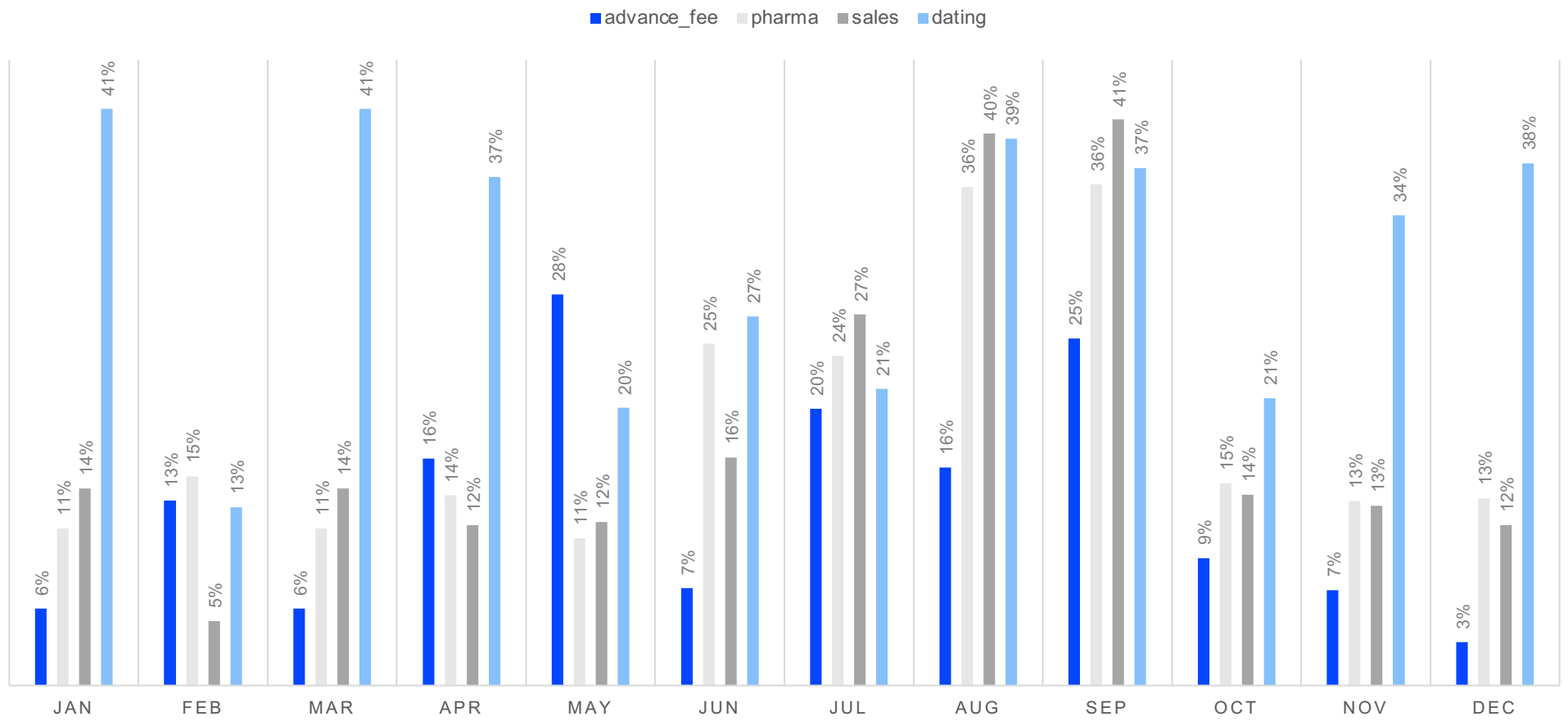
Monthly Distribution of Spam Email Types



Some of the key spam trends of 2020 put down roots in 2021. Covid-19 and healthcare topics remained prevalent among the spam trends of 2021, with scammers pushing bogus compensation emails, surveys, credential-stealing trojans disguised as vaccination registration, and new Omicron tests kits, alongside additional pharma-related scam messages including diet and male enhancement pills, miraculous remedies, narcotics, medical devices and online pharmacies.

Although healthcare-related spam played an important role in the 2021 threat landscape, accounting for an average of 19%, an analysis of received global spam volumes displays spammers' ability to adapt to changes in user behavior. E-mail-based dating scams gained momentum, holding an average of 31% of all received global scams by volume in 2021. Dating spam is followed by advance-fee scams (12% on average) and sales-related spam (18% on average) that promote anything and everything from email marketing lists to fraudulent orders.

Distribution of Email-Based Scam Types



2021 began with a cornucopia of email-based threats, ranging from malicious post-holiday spam campaigns impersonating popular delivery services such as DHL, TNT, FedEx and UPS serving credential-stealing Trojans to tax-season phishing emails.

Phishing for financial information and credentials was a big part of the 2021 spam agenda as well. In Q1, Bitdefender spotted large phishing campaigns targeting the cryptocurrency wallets of Coinbase users, and credential hijacking of AOL aficionados, among others. In Q3, cyber crooks deployed a broad phishing campaign targeting login credentials of DocuSign and SharePoint users. Attacks designed to steal user credentials and compromise financial accounts don't stop here. In July, Bitdefender Labs picked up two phishing campaigns masquerading as legitimate Bank of America correspondence asking users to confirm sensitive banking details and other personal information.

Spammers were quick to capitalize on 2021 data leaks. In Q2, attackers took notice of the scraped email addresses of half a billion LinkedIn users to send phishing emails designed to capture the login credentials of platform users. Extortionists came up with novel attempts to capitalize on data breach victims by exploiting data dumps leaked on dark web forums, including Ledger, the French crypto wallet company.

The spam landscape of 2021 wouldn't be complete without your run-of-the-mill advance-fee scams, gift card giveaways and lottery scams.

Throughout the year, spammers have adapted their schemes to media headlines. In Q3, advance-fee scammers impersonated the exiled Afghan president to target users across the globe as news of him allegedly fleeing Kabul with over $100 million in state funds made headlines. Additionally, spammers piggybacked on the pandemic-induced economic fallout and the charity work of Mackenzie Scott in an attempt to trap gullible internet users.

Significant spikes in malicious spam campaigns were noticed in January (10%), June (11%), and between September and November (9%) 2021, according to Bitdefender telemetry.

The themes of malspam campaigns throughout 2021 ranged from tax-related schemes delivering Dridex Malware and resume-based campaigns carrying Async RAT to Agent Tesla attacks disguised as traditional Covid-19 vaccine registrations and new attempts at expanding the malicious spam repertoire via Omicron-themed messages to infect recipients with FormBook malware.

Of course, there was no shortage of fake e-shops and platforms, with attackers using bogus websites and stores to steal users' personal and financial information during the busiest shopping season of the year.

Spam emails redacted in English targeted shoppers across the globe in November 2021. Distinct spam campaigns were picked between November 8 and 11, with a clear affinity for US users, who received 45% of the fraudulent correspondence.

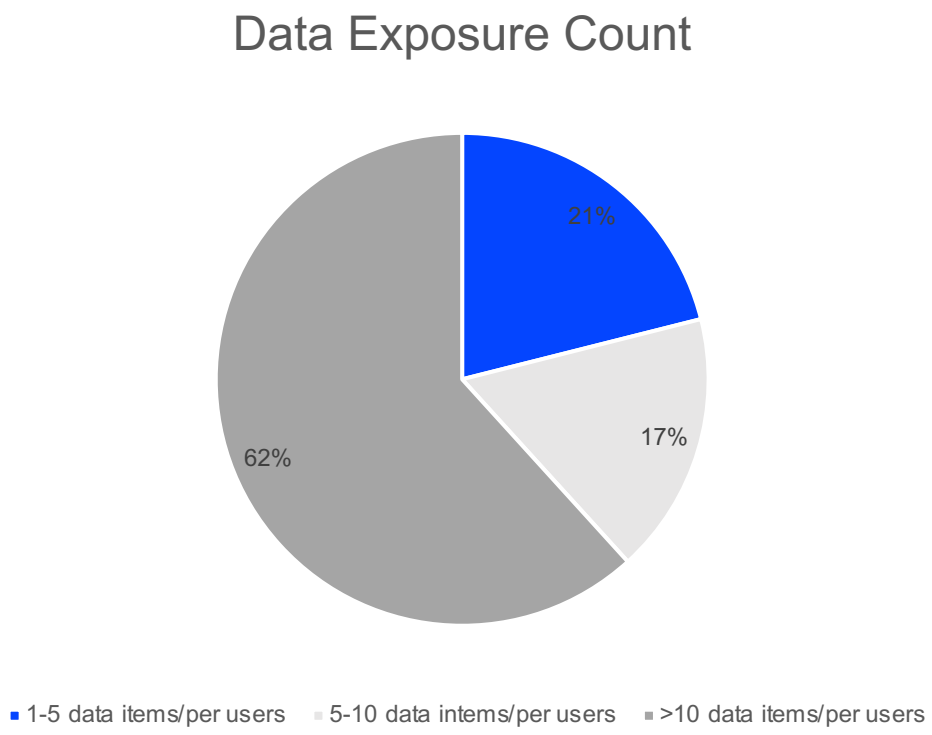
EXPOSED DIGITAL IDENTITIES BREED MALICIOUS ACTIVITY

Data Exposure Count

Digital activity has reached an all-time high during the pandemic, with careless consumer behavior further darkening the global cyberthreat landscape.

According to Bitdefender Digital Identity Protection telemetry, only 21% of users lean towards owning a low-key digital identity, with one to five data items exposed online, while 62% exhibit a lack of concern regarding data exposure, with more than 10 data items publicly available.

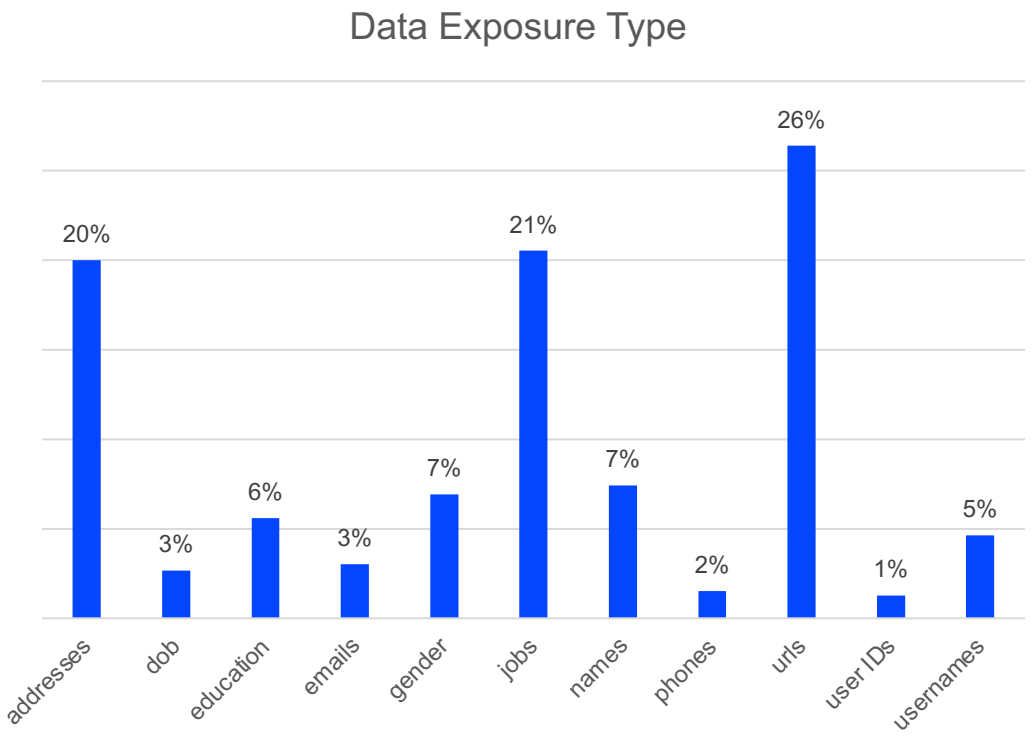
Additionally, even though 17% of users hold an intermediate position in the data exposure count, with five to 10 data entry sets available online, the global average of exposed data sets is 26 unique personal data items.



Data Exposure Type

Regardless of the concerns users express about privacy moving forward in the digital era, users abandon caution amid the Covid-19 pandemic in their eagerness to share personally identifiable information online.

An analysis of Bitdefender Digital identity Protection telemetry reveals that users' URLs (26%), job titles (21%) and physical addresses (20%) are among the most exposed types of personal data found online. These data sets are completed by a variety of additional personally identifiable information including usernames, education background, full names and email addresses and date of birth.



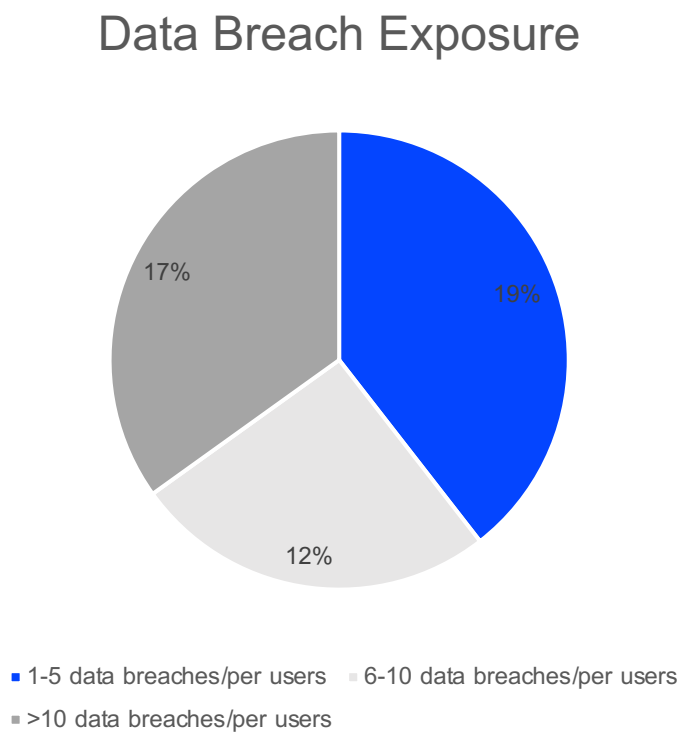
On average, users have willingly exposed

- 2 email addresses
- 3 data points for home or physical address
- 3 data points suggesting their educational background
- 3 user IDs
- 5 data points exposing job background and career information
- 6 URLs linked to social media accounts or platforms

Data Breach Exposure

Nearly half of users have fallen victim to data breaches, with an average of five data breaches each, according to the latest figures from the Digital Identity Protection community.

Specifically, 21% of users have their personal information exposed in one to five data breaches, with a further 12% exposed in six to 10 data security incidents, and 17% in more than 10 data breaches.



The information in this report is based on Bitdefender telemetry gathered from January 1st to December 31st 2021.