Malwarebytes
cyberprotection

2022 THREAT REVIEW

Cyberprotection starts with understanding the latest attacks, cybercrimes, and privacy breaches

Contents

1

EXECUTIVE SUMMARY

In 2021, malware returned with a vengeance.

The Covid-19 pandemic hit global economies hard in 2020, including the criminal underground—and malware detections fell appreciably. A year later, as coronavirus restrictions were eased around the world, malware roared back into our lives at record levels. Malware's "Covid bounce" was visible everywhere, in detections for almost all types of malicious or unwanted software, on Windows and on Macs.

Chickens came home to roost in 2021 too. Apple walked the walk on privacy while repeatedly stumbling over the consequences of its secretive and restrictive nature. Microsoft released its most secure Windows version yet, but wrestled repeatedly with pernicious vulnerabilities in its legacy software.

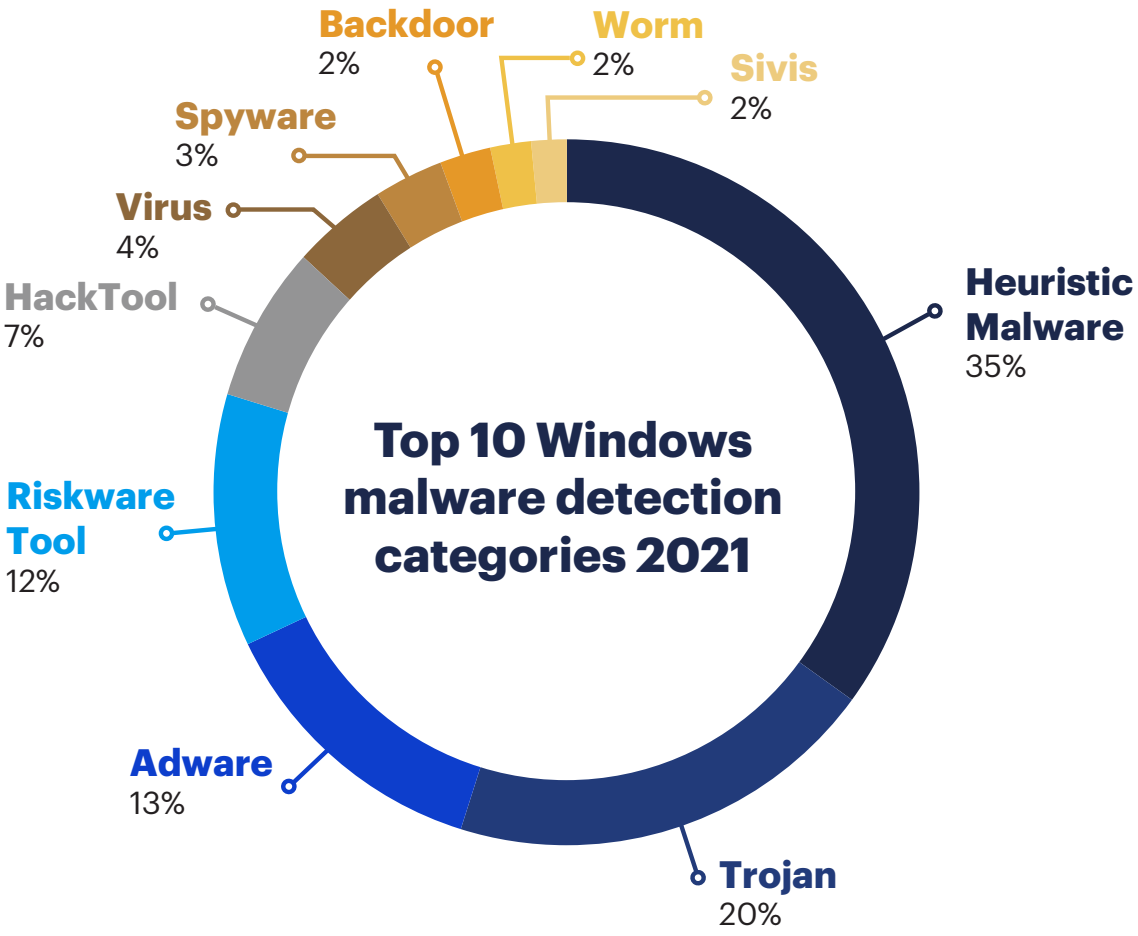
The mounting cost of complexity and technical debt was increasingly evident too. From Google Chrome's 18 zero-days to December's big reveal that everything, everywhere could be put at risk by an unsung logging library, the lesson of 2021 was that while better patching is vitally important, we will not patch our way to security.

In the last year, events in cybersecurity punctured the public consciousness repeatedly, and terms like "SolarWinds," "Colonial Pipeline," "HSE," "Kaseya," and even "Log4j" took on larger-than-life new meanings. But although the incidents those names now represent will linger in memory, 2021 is most likely to be remembered as the year that ransomware was discussed by presidents and hunted by the military. The ransomware epidemic isn't over, and it may not even have peaked, but the threat it poses to businesses, supply chains and critical infrastructure is no longer in doubt, and the forces arrayed against it have never been so formidable.

2

THE YEAR IN MALWARE

WINDOWS



The "Covid bounce"

In 2020, the restrictions put in place to slow the progress of the coronavirus pandemic created a significant depression in economic activity around the world. In that year, malware detections on Windows business machines fell 24 percent—a reminder that cybercrime is a business too. In 2021, malware came roaring back.

As cryptocurrency values soared, detections of malware that mines cryptocurrencies on victims' computers increased more than 300 percent.

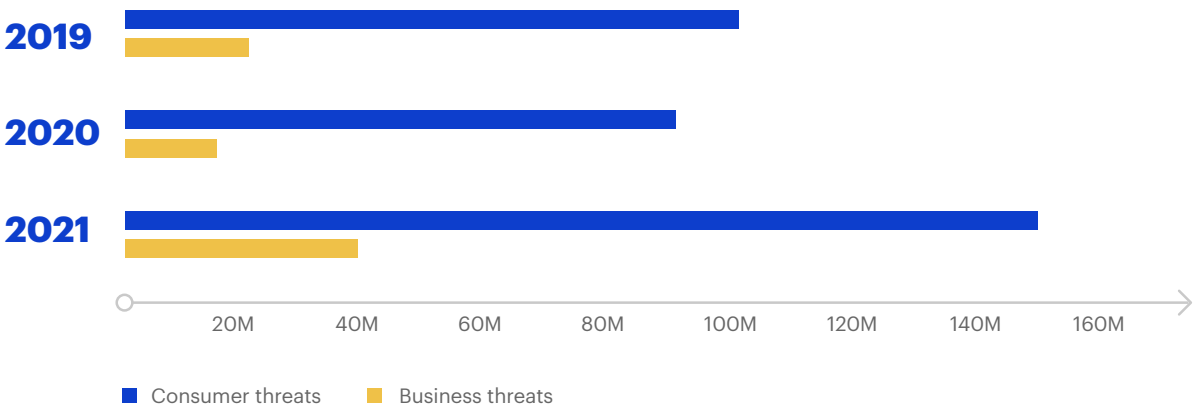
Last year, Malwarebytes detected 77 percent more malicious software than in 2020. As cryptocurrency values soared, detections of malware that mine cryptocurrencies on victims' computers increased more than 300 percent. In addition, adware, spyware, and worms jumped by 200 percent from the previous year, a solid indicator of what we should expect in 2022. Detections on Windows home computers increased 65 percent while detections of threats on Windows business computers rose 143 percent.

In addition to causing trillions of dollars of lost economic activity in 2020, the pandemic also saw a mass migration of knowledge workers from offices to homes. When this happened, a huge pool of potential targets dried up, leaving cybercriminals scrambling to find alternative methods of attack.

Last year, as Covid restrictions eased, and cybercriminals learned how to target organizations whether they were in offices or homes, malware detection numbers climbed precipitously. And they didn't simply return to the pre-Covid status quo, they soared past 2019's numbers, too.

In 2021, the detection numbers for Windows business threats were 85 percent higher than in 2019, and consumer threat detections were 47 percent higher.

Windows malware detection totals 2019-2021



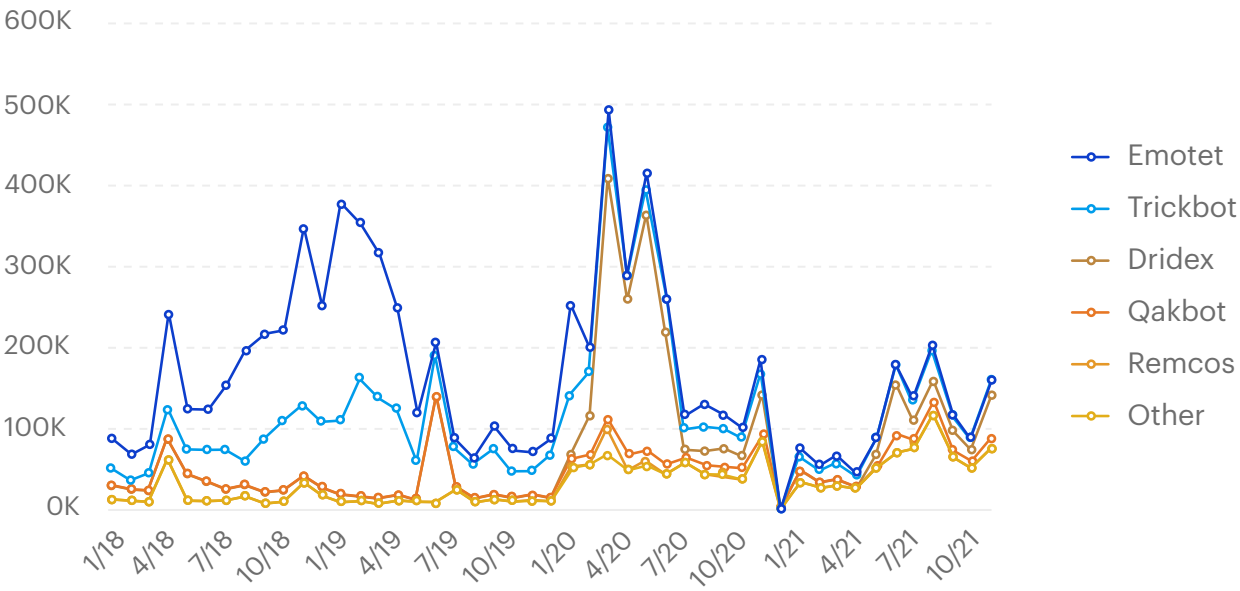
Changing of the guard

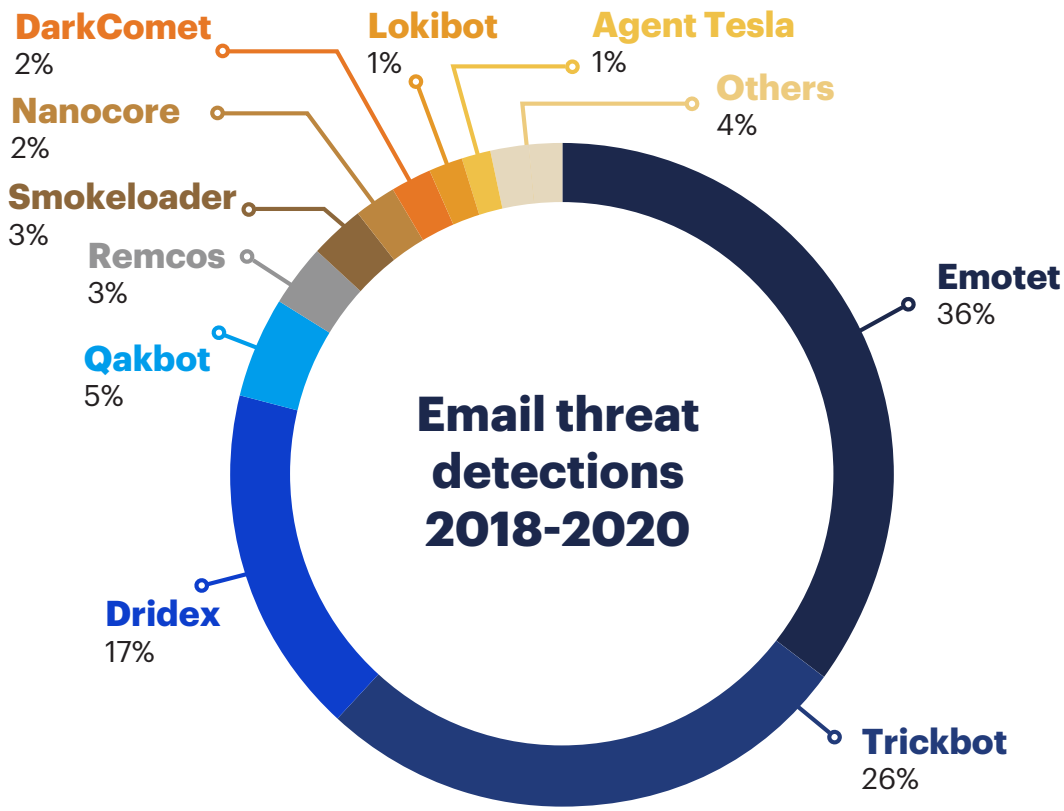
The "Covid bounce"—an increase in detections after a Covid-induced drop—is also visible in the amount of malware sent by email in 2021. However, although it's true that email threat detections increased by 56 percent between the first and second half of the year, the trend over the last four years is actually one of significant decline.

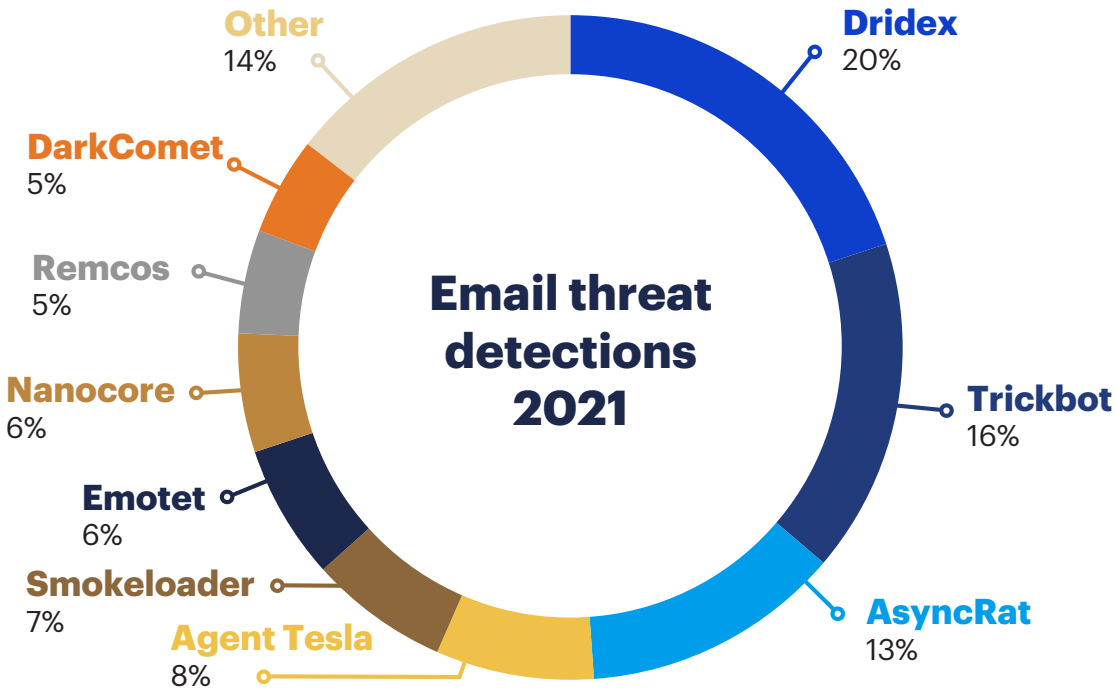
As the volume of malicious email detections has declined, the pattern of detections has changed too. Between 2018 and 2020, the email threat landscape was dominated by vast numbers of Emotet, TrickBot, and Dridex, which accounted for between 75 percent and 90 percent of all email detections. That picture has now changed. In 2021, Emotet, TrickBot, and Dridex made up just 42 percent of detections, and the space they vacated was filled by six other malware families operating at a similar scale.

Although it's true that email threat detections increased by 56% between the first and second half of the year, the trend over the last four years is actually one of significant decline.

Email threat detections 2018-2021




DarkComet
2%
Lokibot
1%
Agent Tesla
1%
Others
4%
Nanocore
2%
Smokeloader
3%
Remcos
3%
Qakbot
5%
Emotet
36%
Email threat detections 2018-2020
Dridex
17%
Trickbot
26%


Other
14%
Dridex
20%
DarkComet
5%
Remcos
5%
Email threat detections 2021
Nanocore
6%
Trickbot
16%
Emotet
6%
Smokeloader
7%
AsyncRat
13%
Agent Tesla
8%

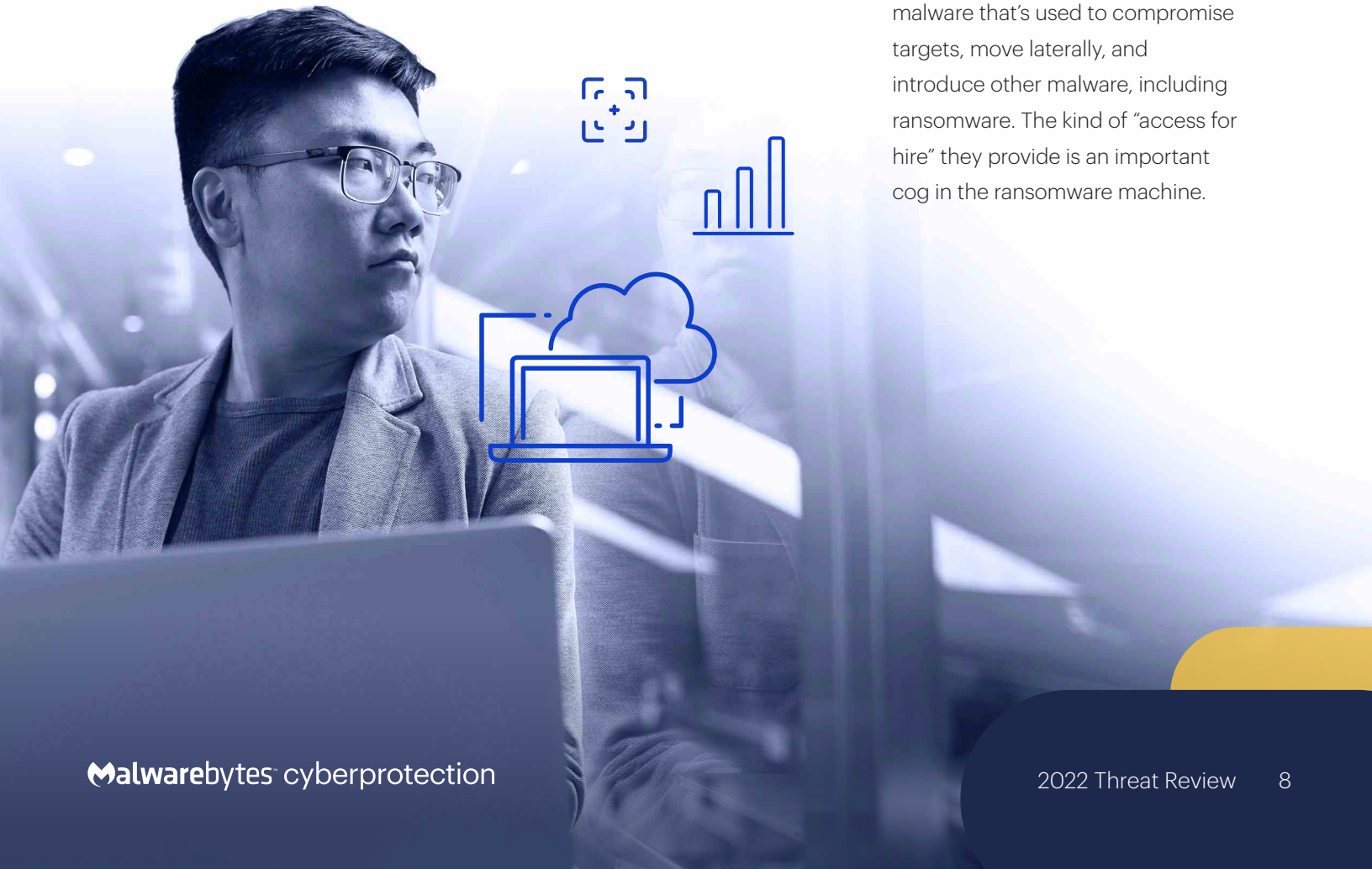
Threat actors appear to be using fewer emails in a more targeted way.

A small part of the change can be explained by Emotet disappearing for about six months, after a coordinated action by multiple law enforcement agencies in January 2021. But the truth is that Emotet detections had already declined massively by mid-2019, pre-dating even the effects of the pandemic.

So what's behind the general decline in email detections?

In 2020, we saw different threats predominate, such as spyware, information stealers, remote access trojans, and keyloggers. This trend continued until people started heading back to the office in late 2020 and early 2021. The old guard of email threats, focused on lateral movement and complete network compromise, seem to have been a poor fit for the work-from-home environment.

Threat actors also appear to be using fewer emails in a more targeted way. Ransomware showed that careful targeting can be extremely lucrative and malicious email operators may have followed suit. Emotet and TrickBot both started life as banking trojans before transforming into malware that's used to compromise targets, move laterally, and introduce other malware, including ransomware. The kind of "access for hire" they provide is an important cog in the ransomware machine.



Ransomware

The notable exception to the "Covid bounce" was ransomware, which decreased 38 percent in 2021. It didn't go away, of course. In fact, 2021 was widely regarded as the worst year for ransomware ever. Attacks like those on Colonial Pipeline, Ireland's Health Service Executive, and JBS—the world's largest meat processing company—raised it to the level of a national security threat in the USA, and made it a topic of discussion at meetings between world leaders.

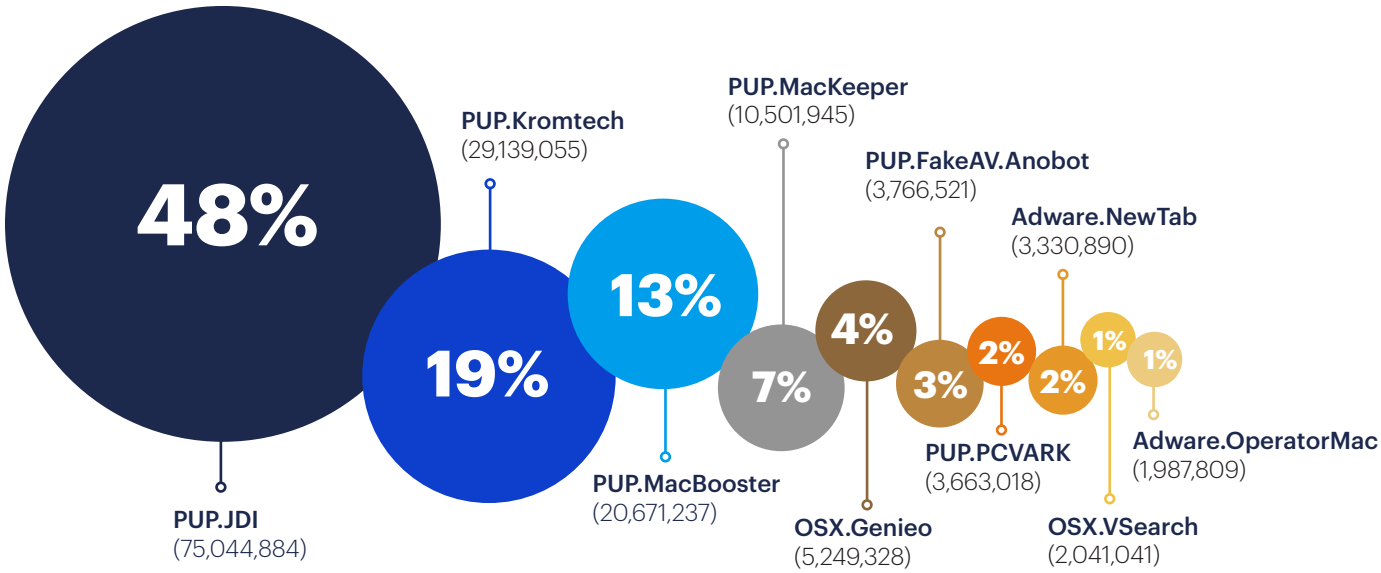
The decrease in detections is most likely a simple side effect of the way ransomware is used. Over the last few years ransomware operators have achieved huge year-on-year increases in the amount of money they can demand by focusing their resources on fewer targets. Ransomware operators are rarely interested in compromising individual machines any more, their targets now are entire organizations. Attacks are bespoke, and the ransomware is run as the final act in network compromises that can be months in the making. By the time it is activated, ransomware is often being run by attackers that have acquired enough power and network insight to disable or work around security software. If an attack is stopped it is likely to be stopped as the attackers breach the network, or as they prepare their attacks, which would not register as a ransomware detection, but something else.

Ransomware operators are rarely interested in compromising individual machines any more, their targets now are entire organizations.

Ransomware caused so much pain in 2021 that it became a concern discussed at the highest levels of government. What followed was a full-throated response involving global law enforcement cooperation, international diplomacy, and even the US military. This undoubtedly disrupted some of the higher-profile ransomware groups in the second half of 2021. How ransomware gangs respond to this change in the risk/reward calculation will be one of the most important questions of 2022.

MAC

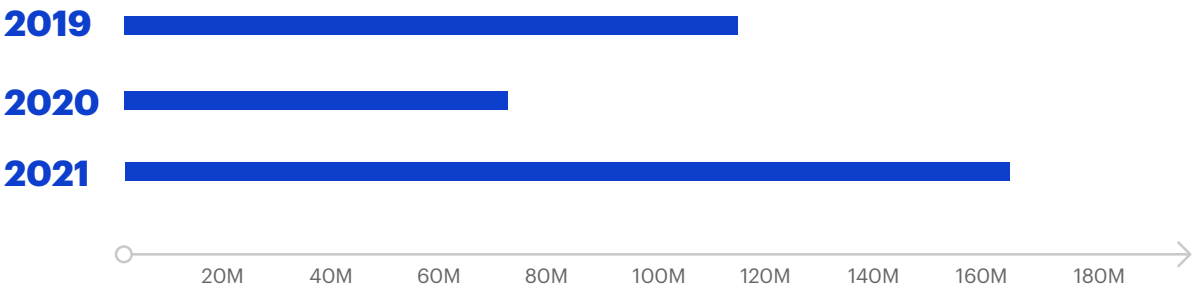
Top 10 Mac detections 2021



The "Covid bounce"

On Macs, detection numbers continued to be dominated by Potentially Unwanted Programs (PUPs) and adware in 2021. The year saw a surge in detections for both, and the same "Covid bounce" seen in Windows malware detections—a dip in 2020 followed by a huge rebound in 2021.

Mac detection totals 2019-2021

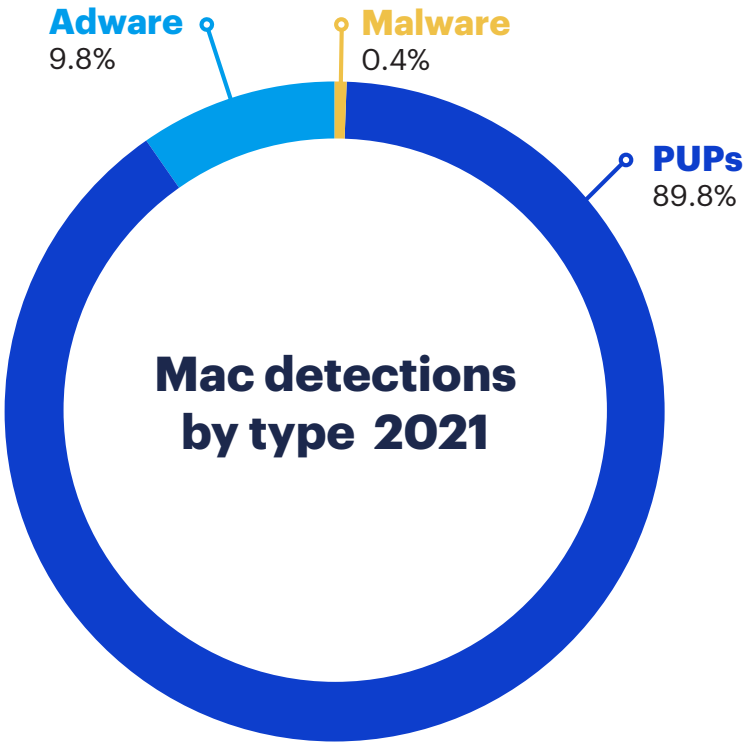


200%

The number of detections on Macs increased 200% year-on-year in 2021.

The number of detections on Macs increased more than 200 percent year-on-year in 2021, to 164 million, an increase of 35 percent on 2019. To put the increase into perspective, in 2021 Malwarebytes saw 75 million detections for just one unwanted app: PUP.JDI, the same as the total number of detections of all types on Macs in 2020.

The exception to the "Covid bounce" on Macs was malware (which has always been dwarfed by the quantity of PUPs and adware on that platform). The number of new malware families discovered in 2021 was relatively low compared to previous years, and most of the new malware was never discovered in the wild, or was discovered in extremely small quantities.



Apple introduced TCC (Transparency, Consent and Control) to make it harder for malicious actors to access important data on Macs.

In the last few years, Apple has introduced a range of security features designed to make it harder for malicious actors to access important data on Macs, notably the Transparency, Consent and Control (TCC) framework, which begs the question: Is TCC behind the apparent chill in Mac malware?

Research demonstrates this is unlikely. TCC has made it a little more challenging to access meaningful data on a Mac, but bypasses are easily found. The lack of detections, and the sparse number of new families, is more likely to be the result of proof-of-concept malware samples, discovered by researchers but never released into the wild. Another possibility is that the malware was not designed for mass infection but was tightly targeted, and that might indicate a change of course by malware authors in response to TCC, but it is far too early to say.

If TCC is having a chilling effect on Mac malware it will be a welcome development, but the bigger picture for Macs remains the vast headache of PUPs and adware.

Apple becomes a victim of its own secrecy

Apple's secretive and restrictive nature is increasingly at odds with the public trend towards openness and transparency, and in 2021 this caused some real problems.

macOS Security patches

In 2021, researcher Josh Long debunked the widely-accepted view that Apple provides security updates for the three most recent versions of macOS.

There were many bugs in 2021 that were fixed for only some of the (at the time) "current three" systems. Those aware of the discrepancies theorized that these bugs may not have affected all three systems, but

Long was able to show this wasn't the case. A concrete example was later found in the worst way, when malware—OSX.CDDS—was discovered that exploited a vulnerability on Catalina (macOS 10.15) that had been patched in Big Sur (macOS 11) seven months earlier.

In the absence of a clear communication from Apple, the safest assumption is that only the current macOS version will get security patches reliably.

Epic lawsuit

Last year, Epic sued Apple over what it deemed to be unfair business practices. The lawsuit shone a light into some of Apple's less-popular practices, including its requirement that iOS devices can only install apps from the App Store.

Among other things, the lawsuit revealed the surprisingly rudimentary nature of the App Store's security screening process. Despite this, it is clear to us that opening iOS to apps not installed via the App Store would cause a rise in malware on Apple phones and tablets. However, it is also clear that the screening process alone is not enough to completely prevent iOS malware and that Apple's restrictive nature makes detecting malware on iOS almost impossible. Scam apps have become good at finding their way on to the App Store, and malware can be installed via vulnerabilities (another area in which Apple is, at best,

Apple walked the pro-privacy walk in 2021 when it introduced App Tracking Transparency.

reluctantly communicative), as in the case of NSO Group's sophisticated Pegasus spyware.

Threading the privacy needle

Apple walked the pro-privacy walk in 2021 when it introduced App Tracking Transparency, which required iOS apps to ask permission before tracking users' data. Finally given the choice, four out of five users opted out, costing Facebook, YouTube, Snap, and Twitter an estimated $10 billion in lost revenue in the first six months.

However, it wasn't all plain sailing for the world's most valuable company.

Stalking via Apple's AirTags

In 2021, Apple released AirTags, its answer to Amazon's Tile tracking devices. Unlike Tile, which needs to be near somebody with the Tile app, AirTags can be tracked as long as they're in range of any iPhone, which makes them far easier to track and, unfortunately, ideal for stalking. Slip one into a woman's purse or her car, and suddenly you can see where she is at all times.

Initially, iPhones would alert users if they detected an unknown AirTag traveling with them, if it hadn't been in range of its owner's phone for a reported three days. Of course, three days is a long time, and in the case of intimate partner abuse, the timer would reset every time the victim and their abuser were together. Worse, the alerts only worked if the person being stalked had an iPhone.

Apple did shorten the delay, after criticism, and released an Android app for alerting to the presence of an unknown AirTag later. These measures were still seen as insufficient by many though and AirTags are likely to remain a point of contention between Apple and privacy advocates.

CSAM protection controversy

In August, Apple announced plans for a highly controversial initiative: Identifying Child Sexual Abuse Material (CSAM) on iPhones.

One part of the plan involved monitoring the text messages of a child enrolled in a family account for CSAM images and alerting the parent. This drew harsh criticism, due to concerns about false identification of images as sexual, outing gay teens to potential abuse at the hands of homophobic parents, and more. Apple was reminded by many that not all relationships between children and parents are healthy ones.

The second, and even more controversial part of the plan involved installing a scanning feature

In August, Apple announced plans for a highly controversial initiative: Identifying Child Sexual Abuse Material (CSAM) on iPhones.

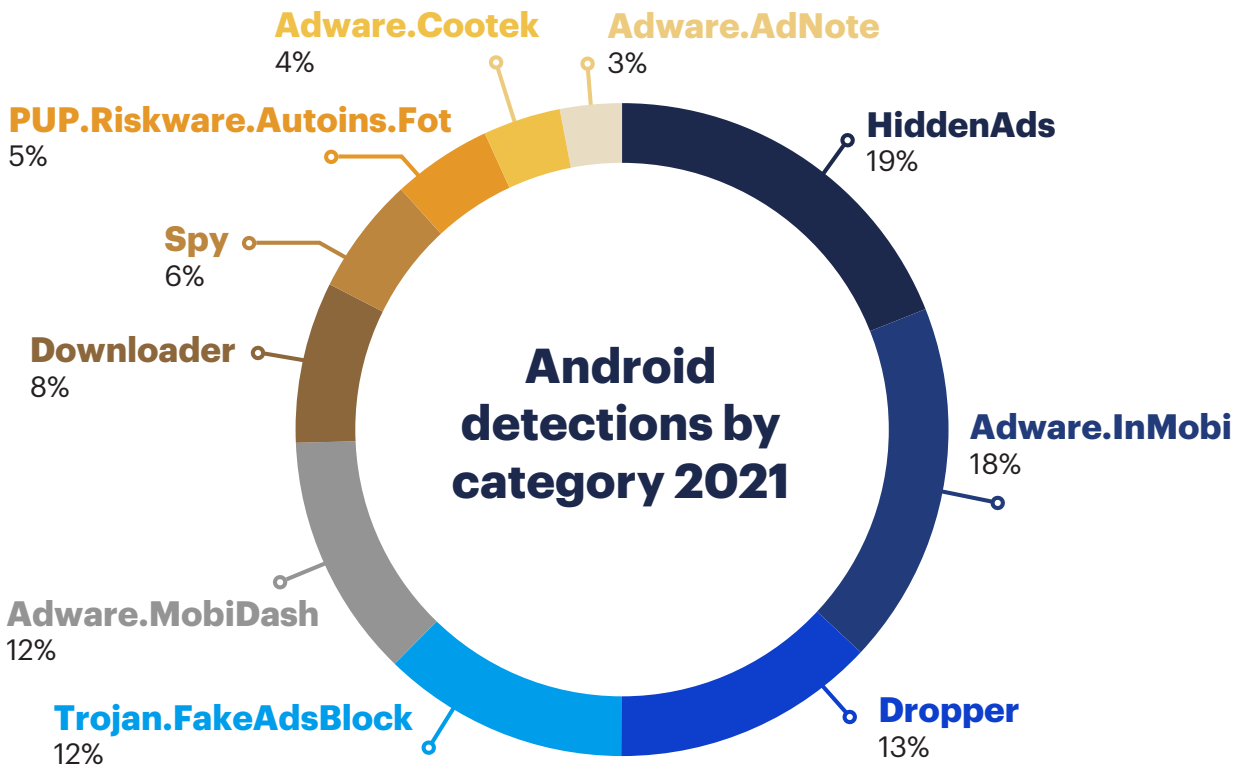
on devices that would compare all photos uploaded to iCloud from the device against a database of known CSAM material. This was meant to happen entirely on the phone, to avoid concerns about having images sent off the device. If a certain number of matches were found, they would be forwarded to Apple for review. Apple would then alert the authorities, if the images were found to be CSAM.

Many had concerns about false positives, which were seemingly borne out by the ease with which people were able to trick a reverse-engineered version of Apple's algorithm.

People also had concerns that the same technology could be used to identify known images of other things, such as people of interest to repressive regimes. The possibility of Apple being forced to use this technology to do the will of governments as the price of doing business in their countries was considered a huge danger.

After much criticism, Apple delayed the release of these features indefinitely.

ANDROID



Apps that make money through ads continued to dominate the Android detection landscape in 2021. One of the most prevalent, Android/Adware.MobiDash, racked up 133,179 detections by hiding in the code of legitimate apps that were repackaged and uploaded to third-party app stores. Meanwhile, Android/Adware.AdNote, which posed as various office-type apps on Google Play, was detected 25,314 times.

Pre-installed apps like the dangerous Android/PUP.Riskware.Autoins.Fota (Autoins Fota) continued to cause significant headaches too. Despite a sharp drop in detections from the previous year, Autoins Fota was still detected 37,701 times in 2021.

Other serious malware, in the form of the closely related Android/Trojan.FakeAdsBlock (FakeAdsBlock) and Android/Trojan.HiddenAds (HiddenAds) trojans were detected 129,876 and 192,919 times respectively.

Of course, the numbers alone don't tell the full story.

The adware numbers can mask a serious problem and help to perpetuate a misunderstanding—that serious threats don't or can't exist on Android.

Adware, everywhere

The detection numbers for Android are dominated by adware, which is often more of a nuisance than a danger. But the adware numbers can mask a serious problem and help to perpetuate a misunderstanding—that serious threats don't or can't exist on Android.

The presence of dangerous malware on Android is often overlooked simply because it's outranked by Adware in detections, and because it often looks different than the threats we are familiar with from other platforms.

Most of the malware types that we've seen on Windows have made it to mobile in some form—including banking trojans, remote access trojans (RATs), and even ransomware. But Android and Windows are very different platforms, and different threats are more or less effective on each.

For example, ransomware is more effective on Windows than Android. Windows machines tend to hold more business-critical data and are often networked to other potential targets, allowing attackers to target entire networks instead of individual devices. Recovering encrypted machines is also much harder on Windows than Android, which is often backed up to the cloud by default and just a factory reset away from recovery.

On the other hand, stalkerware is far more effective on Android than Windows. Android devices typically travel everywhere with their owners, are rarely off, are stuffed full of highly personal information, and bristle with cameras, GPS, mics, and other sensors. By comparison, few people take a powered-on Windows laptop with them wherever they go.

Stalkerware is a very dangerous form of malware, but it is typically used in a targeted way. Detections for it will always be dwarfed by adware that relies on reaching the largest number of people possible.

Scale matters for adware and there are a number of factors behind the vast ocean of it sloshing around the Android ecosystem. Perhaps the most significant is simply the central importance of legitimate advertising as a source of revenue for app developers. This makes adware harder to screen for and, crucially, easier to get onto Google Play.

Adware usually comes packaged in a Software Development Kit (SDK) that's easy to add to an app. There are a lot of legitimate ad SDKs too and there is a strong incentive for their developers to push what's acceptable, which creates a blurred line between what's allowed and what isn't. Although many app developers tack adware SDKs on to their projects deliberately, plenty do it by accident. To make matters more confusing, what's OK one day may be classified as adware the next, pushing a popular app with a well-intentioned developer over the line and causing a spike in detections.

Also, it shouldn't be ignored that there are fewer serious legal ramifications for people caught spreading adware than malware, which changes the risk/reward calculation.

The most prevalent Android malware in 2021 was HiddenAds, a large family of trojans that aggressively display ads wherever they can.

To make matters more confusing, the most prevalent malware on Android also makes money through ads, which might lead the casual observer to assume it's just another form of adware. It is not.

FakeAdsBlock and HiddenAds

The most prevalent Android malware in 2021 was HiddenAds, a large family of trojans that aggressively displays ads wherever it can: In notifications, on the lock screen, in full pop-up screens, in the default browser. Last year, 463 different variants were detected a total of 192,919 times.

A close cousin of HiddenAds is another frequently detected piece of Android malware, FakeAdsBlock, a stealthy trojan that masquerades as an ad blocker. Like HiddenAds, it makes money by showing users ads and is far more dangerous and intrusive than run-of-the-mill adware.

FakeAdsBlock shows full screen ads when the default browser is opened, in notifications, and via the home screen widget. It even has a fake Facebook Messenger notification that opens to ads when clicked. And good luck finding this nasty malware in the App info list—it has no identifying icon or name, just a blank box at the top of the list. (This blank box tactic has become a favorite among many forms of malware, and is also used by HiddenAds.)

It can do all these things largely thanks to the extra permissions it asks for when installed, under the pretense that they are required in order to block ads. The *Display over other apps* permission is an accessibility feature that allows it to display content over other apps. The *Install unknown apps* permission allows an app to install apps and malware from places other than the relative safety of Google Play.

Pre-installed malware

Pre-installed malware continued to be a serious issue on mobile devices from budget manufacturers in 2021. As its name suggests, pre-installed malware is already installed on a new device when a user receives it. What makes it so dangerous is that it is installed at the system level and is therefore very difficult to remove.

Some pre-installed malware can be removed by connecting an infected device to a computer and sending it commands using the Android Debug Bridge (ADB), a technique that is far beyond the comfort level of most users. But even that technique isn't enough to shift the most stubborn pre-installed threats, which are coded into the system apps a device needs to function.

Pre-installed malware continued to be a serious issue on mobile devices from budget manufacturers in 2021.

For example, in 2021, Gigaset mobile devices were infected with a pre-installed system app called Update—actually Android/PUP.Riskware.Autoins.Redstone (Redstone) malware—which was used to download other malicious apps, such as HiddenAds, and required an update from the manufacturer to shift permanently.

Redstone is another name for the most frequently detected malicious system app in 2021, Autoins Fota. The good news, though, is that detections for it dropped last year by about 50 percent, year-on-year.

Some of the decrease is likely a result of the US Government-funded Lifeline Assistance program getting manufacturers to clean up their act. The program is a Federal Communications Commission initiative that makes communications services more affordable for low-income consumers. In early 2020, Malwarebytes discovered that the UMX U683CL, a phone provided to some of the most vulnerable people in the USA by the Lifeline Assistance program, came pre-installed with a malicious, unremovable Settings app that had trojan dropper capabilities.

PRIVACY

2021 was a year of surveillance. The public saw the tragic, real-life impacts of targeted domestic spying with stalkerware, and learned that targeted, digital surveillance of individuals by governments was almost common. They also learned about the cottage industry of hackers that make such machinery possible—discovering vulnerabilities, building exploits, and selling their services to any country willing to pay.

As pandemic restrictions are lifted and the world begins to move about more freely, people need data privacy more than ever. As we learned this past year, simply too much is at stake.

As pandemic restrictions are lifted and the world begins to move about more freely, people need data privacy more than ever. As we learned this past year, simply too much is at stake.

Stalkerware-type apps

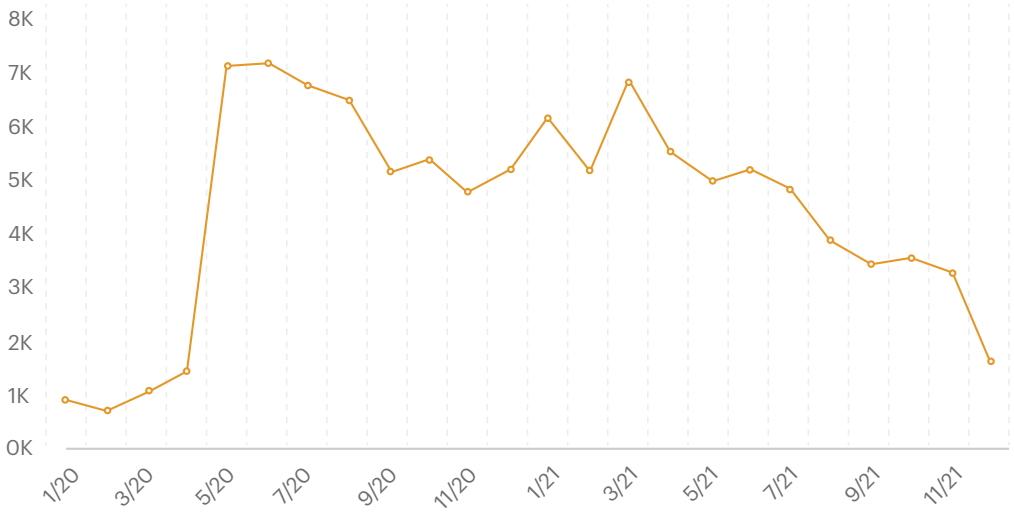
For years, Malwarebytes has tracked the prevalence of stalkerware, which is a term used to describe surveillance apps that are installed on a person's device—often a partner—without their consent. These apps can access a device's GPS location, web browsing history, photos, videos, emails, and phone call logs and audio. Stalkerware also has a known intersection with domestic abuse, where abusers use the information from apps as a lever to control the subject of their stalking.

Malwarebytes separates stalkerware-type activity into two categories—monitor apps and spyware apps. In 2020, detections of monitor and spyware apps saw an unprecedented spike at the moment much of the world went into some form of lockdown, and levels of stalkerware stayed at unprecedented highs for the rest of the year.

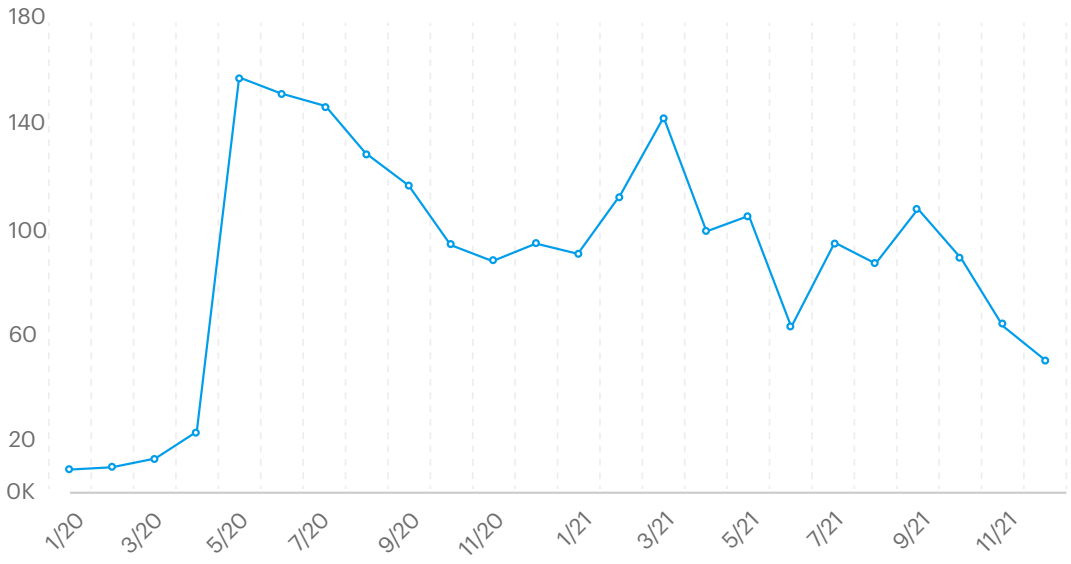
In 2021, Malwarebytes recorded a total of 54,677 detections of Android monitor apps and 1,106 detections of Android spyware apps. This represents a 4.2 percent increase in monitor detections and a 7.2 percent increase in spyware detections year-on-year, making 2021 even worse than 2020, and the worst year for stalkerware so far.

However, although the overall numbers are up, detections have taken an unmistakable downward turn since last year's peak.

Android monitor app detections 2020-2021



Android spyware app detections 2020-2021



In the second half of 2021, average monthly detections for monitor apps fell by 39 percent, to just 3,459 detections per month, compared to an average of 5,654 detections per month in the first half of 2021. The same trend happened with spyware too: Average monthly detections fell by 20 percent in the second half of the year compared to the first half.

What's at play here?

When stalkerware saw its distressing uptick in 2020, Malwarebytes, in consultation with other domestic abuse support networks, hypothesized that the increased stalkerware activity came about because of the real-world physical restrictions put in place to combat COVID-19 around the world. The increase was also detected by other members of the Coalition Against Stalkerware, and coincided with news reports of increased calls to domestic abuse agencies.

In 2021, many governments loosened their coronavirus restrictions, allowing the public to mix and travel more freely. And, just as the sudden increase in stalkerware detections mirrored the sudden, mass imposition of restrictions, the gradual decline in detections appears to reflect their gradual easing.

Abusers may simply have turned to other forms of technology as stalkerware became more widely detected.

2020's tidal wave of stalkerware also led to increased awareness of the stalkerware problem, which turned into action in 2021. Last year the Federal Trade Commission issued its second-ever enforcement action against a stalkerware developer, and Google removed several ads that promoted stalkerware.

The decline in stalkerware is welcome, but the causes for it are not clear and it is too early to celebrate. It is increasingly easy for abusers to monitor their targets using off-the-shelf technology designed for other purposes. Abusers may simply have turned to other forms of technology as stalkerware became more widely detected. Or they may have returned to previous patterns of control and abuse as restrictions eased.

Thankfully, the Coalition Against Stalkerware continued to grow in 2021, increasing its contributors and accepting more expertise so as to expand its stalkerware detection threat list, which antivirus vendors can use to improve their own detection tools. As a founding member, Malwarebytes will continue to share intelligence with the Coalition Against Stalkerware to improve industry-wide detections while also guiding the domestic abuse support networks within the coalition through thorny, technical questions of detection, removal, and prevention.

Pegasus proved popular

In the summer of 2021, several newspapers published explosive

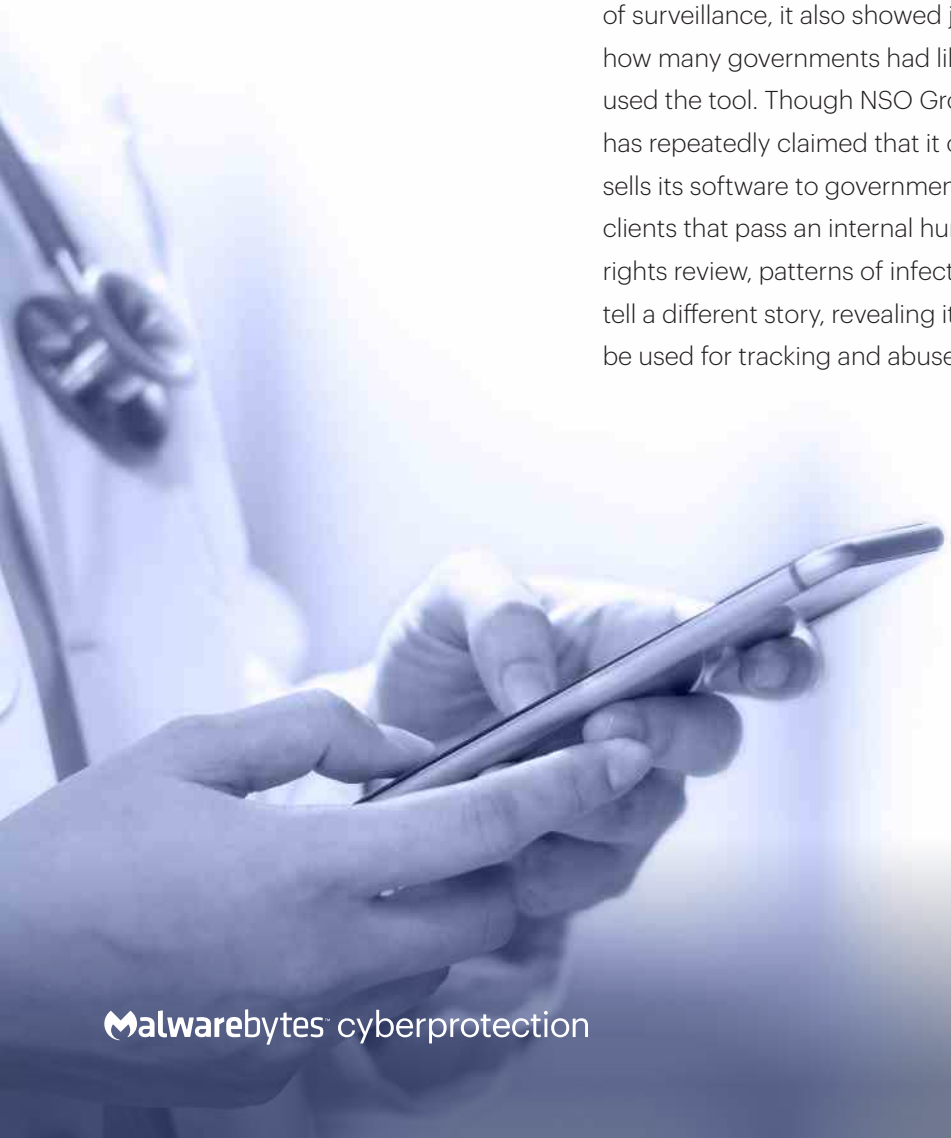
Reporting showed that the security defenses in even the most advanced smartphones were no longer enough.

details of a highly sophisticated spyware tool called Pegasus that targeted iOS devices. The spyware, developed by the Israeli firm NSO Group, was known to many security and privacy professionals but became an almost household term following reports by the Pegasus Project.

According to the reporting, the spyware was used to target the phones of diplomats, presidents, prime ministers, and one king, along with a princess who made a daring attempt to escape Dubai.

The reporting on Pegasus did not just present new, harrowing tales of surveillance, it also showed just how many governments had likely used the tool. Though NSO Group has repeatedly claimed that it only sells its software to government clients that pass an internal human rights review, patterns of infection tell a different story, revealing it to be used for tracking and abuse by authoritarian governments. The invasive tool has reportedly been used by governments in India, Saudi Arabia, Bahrain, Azerbaijan, Mexico, the United Arab Emirates, Morocco, Hungary, and Rwanda. But even the origin of surveillance betrays the broad power of Pegasus, as it can reportedly crack into iPhones in other countries, no matter the distance.

Worryingly, the reporting also showed that the security defenses in even the most advanced smartphones were no longer enough. If a government wanted to perform targeted, digital surveillance



on a person, it would likely be able to do so, no matter a device's model, year, or operating system.

Months after the The Pegasus Project published its revelations, the US Department of Commerce added NSO Group to its "Entity List," forbidding US companies from doing business with the Israeli outfit. Just weeks later, though, enforcement action from the private sector followed. In a deep-pocketed counter in November, Apple sued NSO Group for its alleged targeting and hacking of Apple users, and it donated $10 million to cybersurveillance researchers, like those at Amnesty Tech and Citizen Lab that have documented the use of Pegasus for years. Apple also promised ongoing technical support to Amnesty Tech and Citizen Lab, and it announced its intent to notify Apple users that it suspected were being targeted by NSO Group's spyware.

If a government wanted to perform targeted, digital surveillance on a person, it would likely be able to do so, no matter a device's model, year, or operating system.

Just one month later, Google's Project Zero contributed additional research, as Ian Beer and Samuel Groß published details of an indiscriminate watering hole attack infecting iPhones that visited several compromised sites. This was not Google's first brush with NSO Group—the company is supporting a separate lawsuit, alongside Microsoft, Cisco, and VMWare, filed by WhatsApp against NSO Group for its alleged efforts to utilize a vulnerability in WhatsApp to hack users.

3

TRENDS

A matter of national security

2021 will be remembered as the year when cybercrime, and ransomware in particular, were elevated to the status of "national security threat."

On the afternoon of August 25, 2021, in The White House's East Room, the leaders of multiple major tech companies gathered together to listen as President Joseph Biden described, "the core national security challenge we're facing, the American people are facing, and our economy is facing"—cybersecurity.

President Biden's remarks simply reflected a fact that his administration had accepted for months, which is that cybersecurity had become a matter of national security, and it was up to the Federal government to step in.

Beginning in early 2021, the United States and several other governments began a worldwide crackdown on cybercrime that involved everything from covert investigations to public policy changes to closed-door meetings between superpowers. Ransomware gangs were upended. Malware networks were infiltrated.

Computers, cash, and cars were all seized. And finally, it looked like there might be a solution to the growing problem of cybercrime—putting the criminals in jail.

In January, in coordination with law enforcement from multiple countries, the US helped take down the Emotet botnet and then—in an extremely rare move—deliver code to Emotet infections instructing them to delete themselves at a later date. In February, President Biden signed an executive order aimed at improving the security of American supply chains from various threats, including "cyber-attacks." In May, such an attack struck, when Colonial Pipeline's services were shut down for days due to ransomware. The oil and gas supplier, pressed on all sides, paid the ransom.

Days later, President Biden signed another executive order, this time upping the security requirements for any software that the Federal government purchased for internal use. And shortly after that, the Department of Homeland Security issued its first-ever cybersecurity rules for pipeline companies in the US.

During this flurry of government activity, threat actors raced ahead with increasingly devastating attacks.

In June, to avoid a similar lockup like that experienced by Colonial Pipeline, the meat processor JBS paid $11 million to its ransomware attackers for a decryption key. Less than one month later, the most

Colonial Pipeline's services were shut down for days due to ransomware. The oil and gas supplier, pressed on all sides, paid the ransom.

devastating ransomware attack in history shut down businesses worldwide, as a popular Remote Monitoring and Management (RMM) tool called Kaseya VSA was compromised. The attacks on Kaseya led to ransomware infections not only on Kaseya's customers, but on the clients that those customers supported.

Both attacks were reportedly the work of REvil, a ransomware gang that many believed operated with the tacit approval of the Russian government because of that country's apparent unwillingness to clamp down on the cybercriminals' activity. As Malwarebytes Labs showed last year in a new analysis, many ransomware gangs are allowed to operate freely so long as they ensure that their ransomware does not target or harm anyone in Russia or the Commonwealth of Independent States (CIS). In fact, of the most prolific ransomware families used in attacks in the first half of 2021, not a single one ran effectively in the CIS.

That setup was the standard for years, until 2021.

In July, President Biden reportedly told Russian President Vladimir Putin that the US was ready to hit back—and would take "any necessary

action"—should it continue facing cyberattacks from Russian threat actors.

Though Russian law enforcement would eventually hit back against REvil in January 2022, the US government didn't wait around to work its own counter-offensive. According to exclusive reporting in The Washington Post, the US Cyber Command, in coordination with another foreign government, compromised REvil's infrastructure so thoroughly that one leader ran off in fear.

"The server was compromised and they are looking for me," wrote one of REvil's believed leaders after discovering that the traffic of the group's website had been diverted. "Good luck everyone, I'm taking off."

The chase to stop REvil was just one of the many campaigns launched by global law enforcement to stop cybercriminals last year.

The thread that linked many of the most important cybersecurity events of 2021 was old, insecure code.

In June, the FBI announced that it had clawed back 63.7 of the 75 bitcoins that Colonial Pipeline paid its attackers just the month prior. It was the first major win for the Justice Department's Ransomware and Digital Extortion Task Force, which, according to earlier reporting, had been formalized just months prior. In the same month, Ukrainian law enforcement officials arrested multiple individuals for their alleged involvement in working for the Cl0p ransomware gang. In a showy video released to the public, police seized the criminals' vehicles, including a Mercedes Benz, a Lexus, and a Tesla.

Ransomware has not been defeated, nor has it disappeared, but the stakes for those involved have undoubtedly changed. By year's end, the ransomware groups behind Avaddon, BlackMatter, and DarkSide had all been shut down, or taken the opportunity to run away into cyberspace. And while voluntary ransomware group "shutdowns" are almost always a prelude to a new ransomware group—sharing many of the same old members—sprouting up again, 2021 was still different. Rarely had the public seen such high levels of activity against cybercriminals from law enforcement, making last year a welcome change.

The mountain of technical debt

The thread that linked many of the most important cybersecurity events of 2021 was old, insecure code. The year began well, with the long-awaited retirement of Flash, but was otherwise notable for a succession of high-profile vulnerabilities in well-established codebases.

In March 2021, users of the on-premises versions of Microsoft Exchange Server scrambled to patch an attack-chain of four zero-day vulnerabilities. The most serious, dubbed ProxyLogon, was discovered

In 2021, no fewer than 18 zero-days were discovered in Google's Chrome browser.

by researcher Orange Tsai, who declared that ProxyLogon wasn't simply a single bug but a "whole new attack surface". That attack surface would go on to yield a series of other serious vulnerabilities and three more attack chains: ProxyShell, ProxyToken, and ProxyOracle.

In June, another old codebase came under the microscope as Microsoft made repeated attempts to fix PrintNightmare, a flaw in its print spooler that allowed anyone to run arbitrary code as SYSTEM—a gift to attackers such as ransomware gangs looking to elevate their privileges. As with Exchange, Microsoft wasn't dealing with a single coding error, but cleaning up a legacy codebase and an entire "generic category" of flaws.

Architectural decisions taken years previously were coming home to roost elsewhere, too.

In 2021, no fewer than 18 zero-days were discovered in Google's Chrome browser, many of them in its JavaScript engine's Just In Time (JIT) compiler. So troubled was the JIT compiler that Microsoft even created an experimental Super Duper Secure Mode for its Chromium-based Edge browser that simply disabled the JIT compiler completely.

But the most extreme example of Internet-scale technical debt was reserved for the end of the year when an exploit with a CVSS score of 10 out of 10 was uncovered in Log4j, an unheralded open-source

logging component embedded into countless Java applications, including some of the world's most popular platforms like iCloud, Steam, Minecraft, and AWS. Not for the first time, questionable security decisions in one piece of code had become part of the fabric of the Internet.

But while code that was difficult to fix was part of the story, code that could have been patched but wasn't remained cybersecurity's enduring headache. Every year there are countless examples of organizations being compromised by known vulnerabilities that could have been patched months or even years previously.

In November 2021, CISA put the federal government on notice that it intended to change things. It issued a Binding Operational Directive that came with a catalogue of critical vulnerabilities that needed to be patched, and a deadline. Federal departments and agencies had six months to fix anything with a CVE issued before 2021, and, from that moment forwards, two weeks to fix anything else that was added to the catalogue. It may yet prove to be transformational. In 2014, Google's Project Zero reset expectations about how quickly patches should be produced. CISA BOD 22-01 could do the same for expectations about how quickly patches should be applied.

The problems that affected Exchange, the Microsoft print spooler, Chrome, Log4j and many others speak of insecure foundations.

The end of the year saw the release of Windows 11. For several years, Microsoft's approach to Windows security has been to create a chain of trust that ensures the integrity of the entire hardware and software stack, from the ground up. The latest version of Windows makes that approach the default, which is why it has such famously stringent hardware requirements. Microsoft's stated intent is to use technologies like virtualization-based security to make entire classes of vulnerability obsolete. It is an approach that should be applauded.

The problems that affected Exchange, the Microsoft print spooler, Chrome, Log4j, and many others speak of insecure foundations. Alongside fast and rigorous patching, we need much wider use of modern, secure programming languages and practices, coupled with the determination to retire old software, languages, frameworks, and expectations too.

The lesson of 2021 was that while better patching is vitally important, we will not patch our way to security.

Overstretched supply chains

At the very end of 2020, Reuters revealed that departments within the United States government, and some private companies, had been infiltrated by suspected nation-state actors. They had done this by breaching the software company SolarWinds almost a year earlier, and tampering with its Orion product, turning it into a backdoor that gave them access into the networks of SolarWinds' most high-profile customers.

It was an audacious, patient, and highly sophisticated attack that put everyone on notice that their security was only as good as the security of their suppliers.

Any lingering sense that this kind of attack, while extremely serious, was something only nation states need worry about were swept aside seven months later. On July 2, the REvil criminal gang used a vulnerability in the Kaseya VSA remote monitoring tool to infect at least 800 separate organizations with ransomware, simultaneously. It was a watershed, and "Kaseya" would quickly join "SolarWinds" in the cybersecurity lexicon as shorthand for a devastating supply-chain attack.

The fragility of our software supply-chains was being laid bare elsewhere too, as code repositories fought off death by a thousand cuts.

Modern programming is as much about assembling software from existing components and libraries as it is about writing new code. To service this need, programming languages and environments now come with package management tools that can fetch and integrate third-party open-source components from vast online repositories, at the press of a few keys. These components often require other third-party components in order to work, and those require yet more components, and so on, in a deep, interlocking web of dependencies.

This makes software development faster and more efficient, but it often forces vendors and end users to put their trust into significant quantities of third-party code of unknown quality and provenance.

The last few years have been punctuated by a series of "near miss" attacks on these repositories where attackers have succeeded in sneaking malicious packages—such as information stealers and keyloggers—on to repositories like NPM, PyPi, and RubyGems, without managing to do significant harm.

2021 saw a notable escalation in the sophistication of these attempts without any of them reaching the watershed status of a SolarWinds or Kaseya. These attempts ring like a series of warning shots, urging us to take the security of the open-source supply chain much more seriously before a significant compromise finally occurs.

Another fragility of the open-source supply chain was made clear at the end of the year when a critical, remotely executable vulnerability was discovered in Log4j, a Java logging component that had made its way into a vast collection of software projects. An insecure design decision, taken in good faith years ago by a tiny group of volunteer maintainers, was inherited by every project that used Log4j, including behemoths like AWS and iCloud, and many of them were left vulnerable to a simple but potentially devastating remote attack.

We have already embedded other people's code deep into every corner of our ecosystem and now we must address how to secure it.

As in so many other areas of technology, the cost of expediency is being paid long after the fact. We are already far beyond the point of deciding whether or not using untrusted third-party code is a good idea. We have already embedded other people's code deep into every corner of our ecosystem and now we must address how to secure it.

4

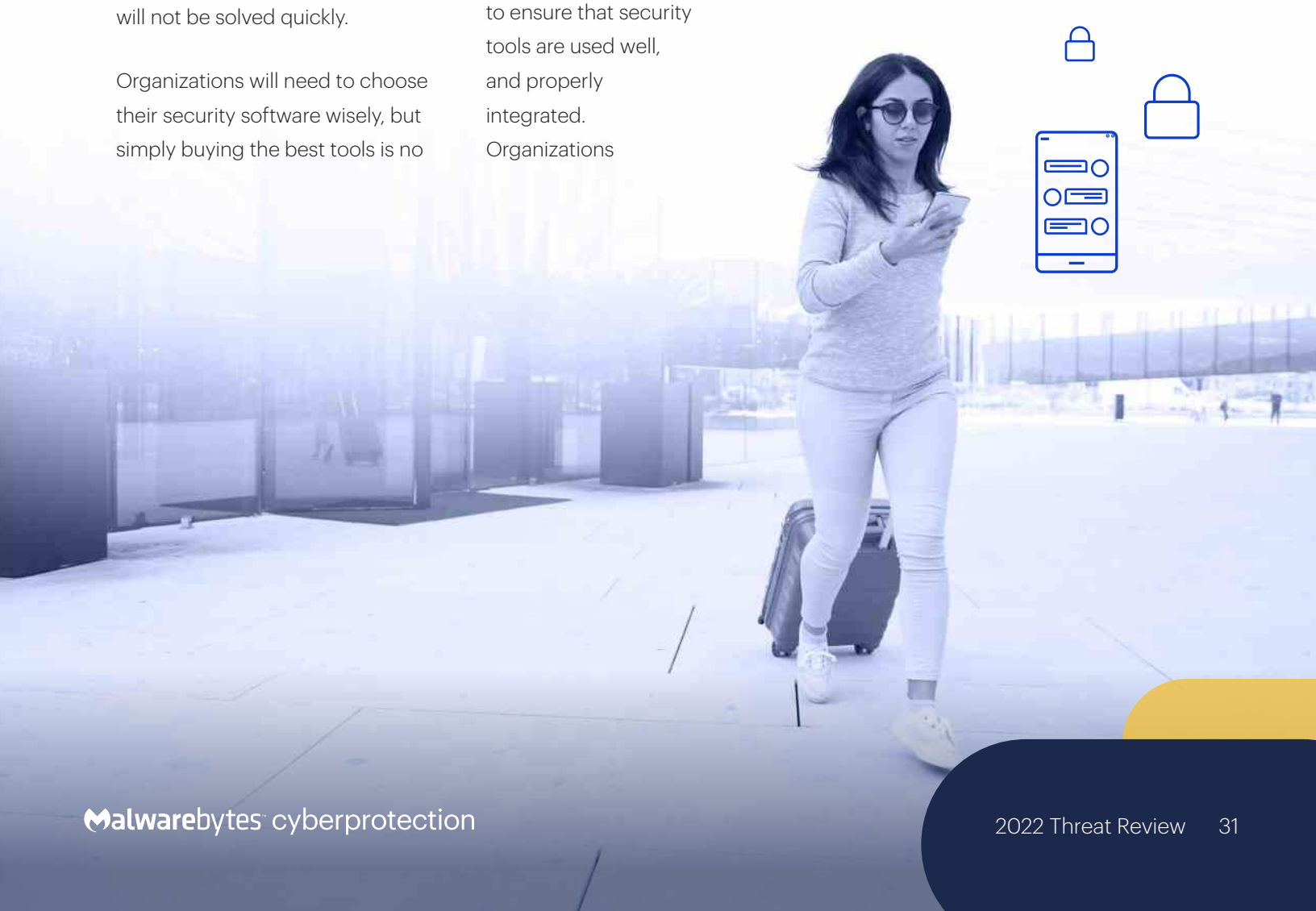
LOOKING TO THE FUTURE

We expect the important cybersecurity trends of the past year to persist into this year and beyond.

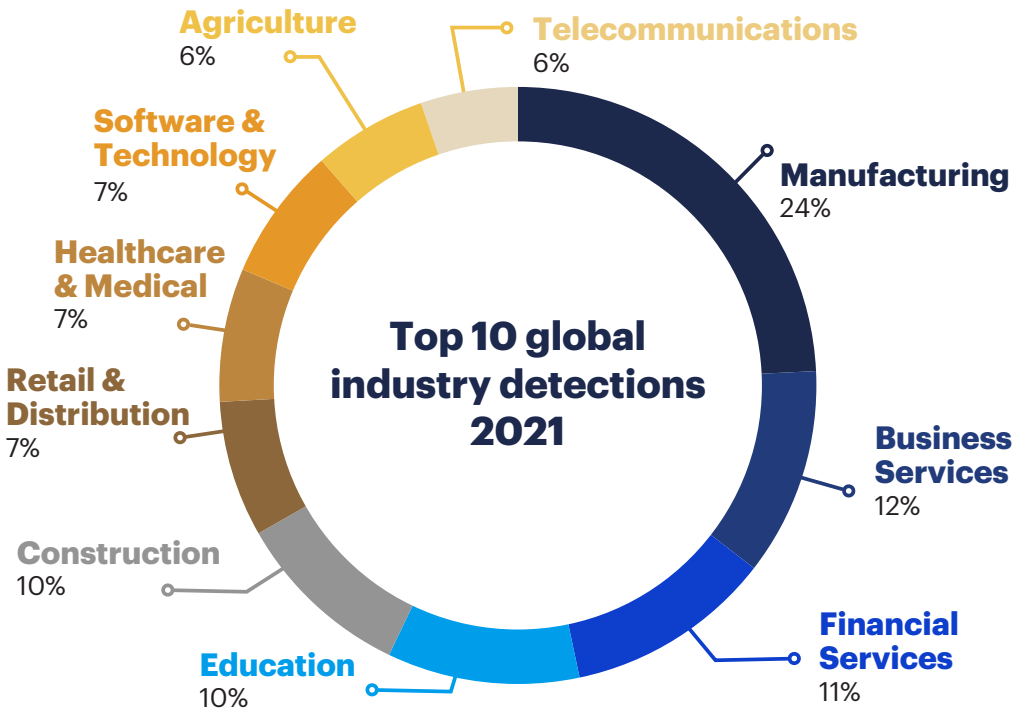
Determined, opportunistic adversaries; unmanageable complexity; Byzantine supply chains; mountains of technical debt; glacial patching rates; ad-driven app ecosystems; the proliferation of technology that can be used for stalking; and our systemic weaknesses to social engineering and ransomware. These problems were years in the making and they will not be solved quickly.

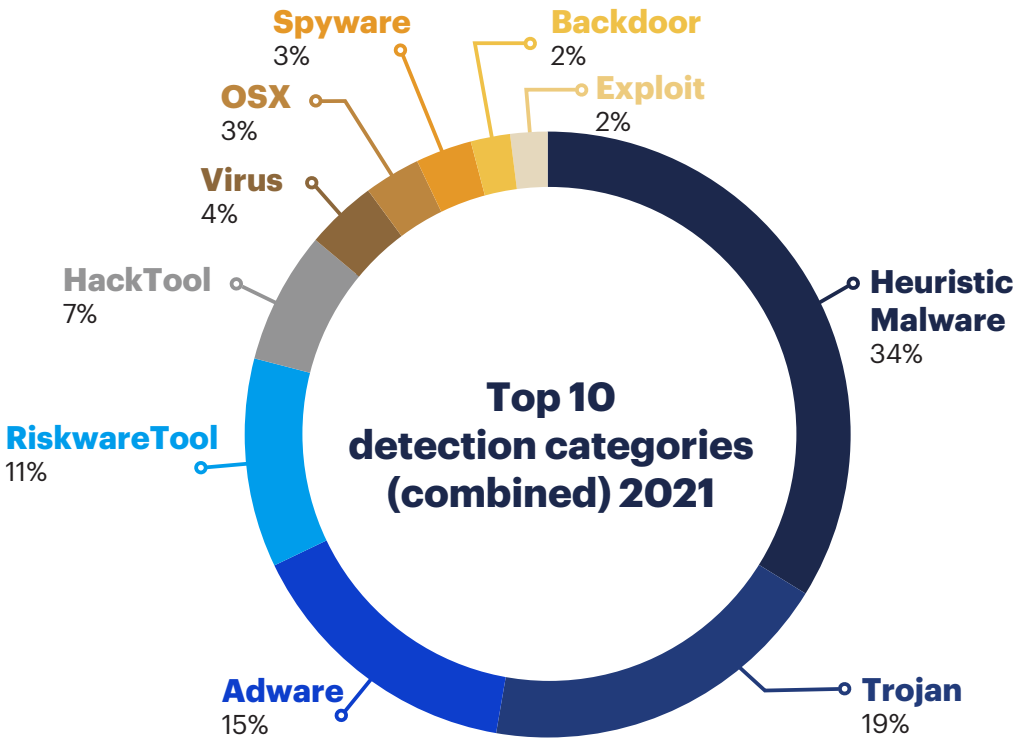
Organizations will need to choose their security software wisely, but simply buying the best tools is no longer enough. IBM's 2020 Cyber Resilient Organization Report revealed what many admins already knew: That some organizations are now reaching a tipping point where increasing the complexity of their security stack is harming security outcomes.

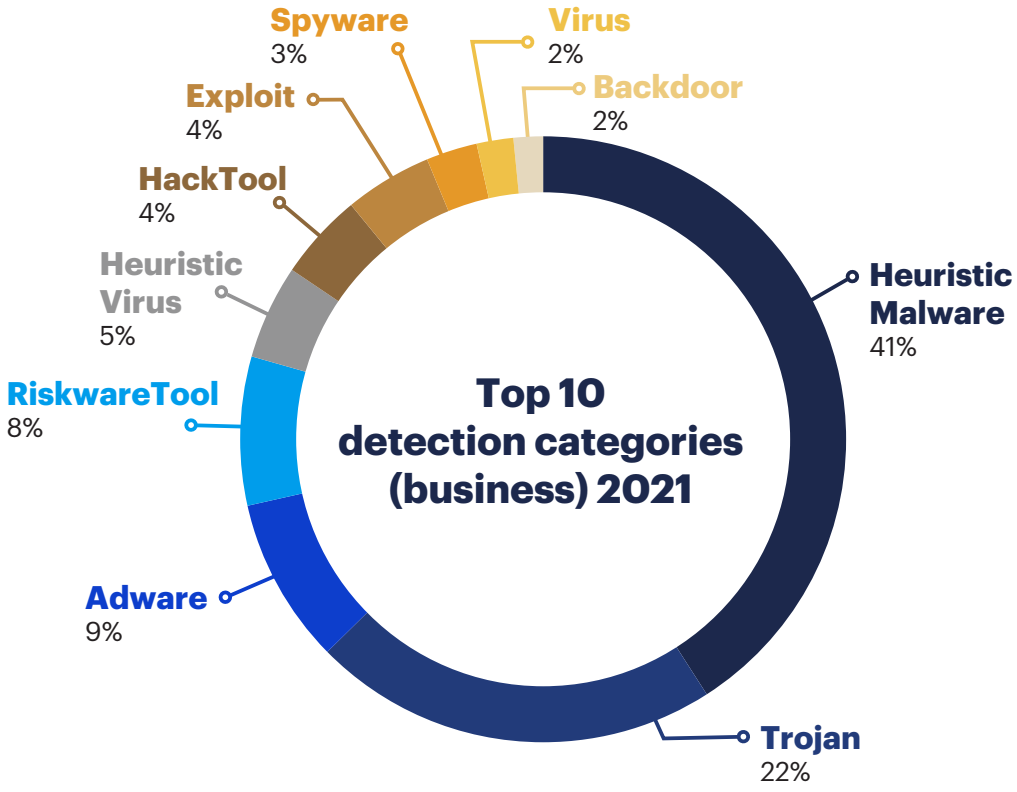
The antidote is to provide the training and resources necessary to ensure that security tools are used well, and properly integrated. Organizations must seek out the best tools, while recognizing that security is a thing they must do rather than a thing they can buy. Doing security right means making every effort to stop attacks, while understanding that breaches are likely inevitable. It means thinking in terms of resilience: Threat hunting, threat containment, safeguarding of critical systems, harm reduction, and swift recovery.

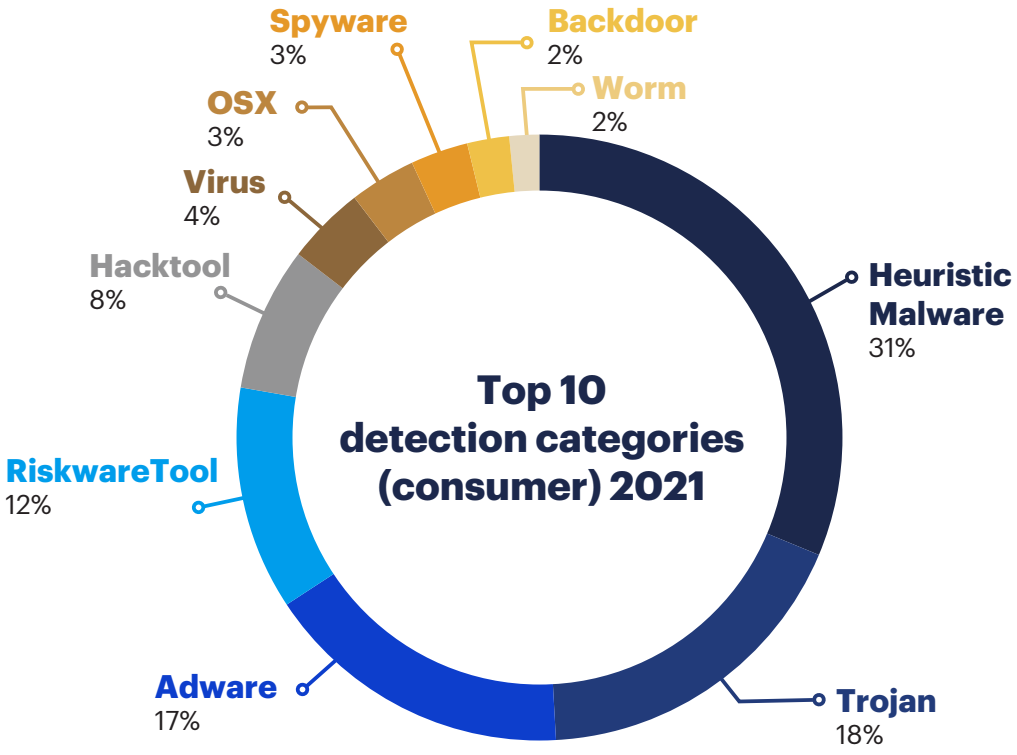


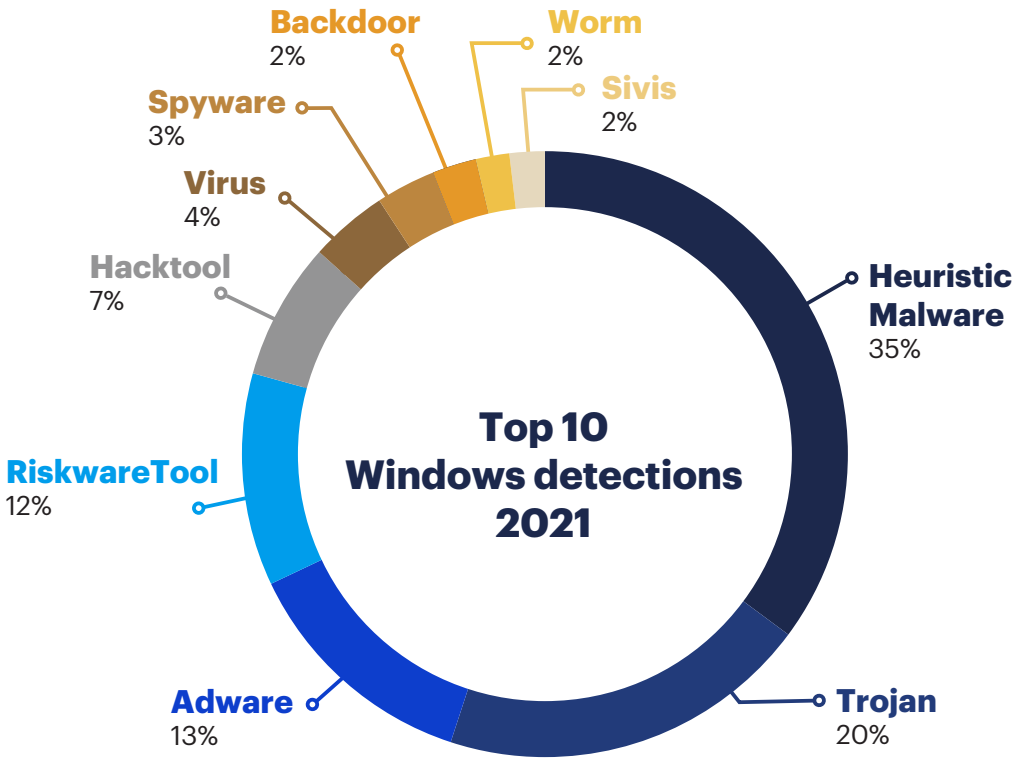
5 APPENDIX

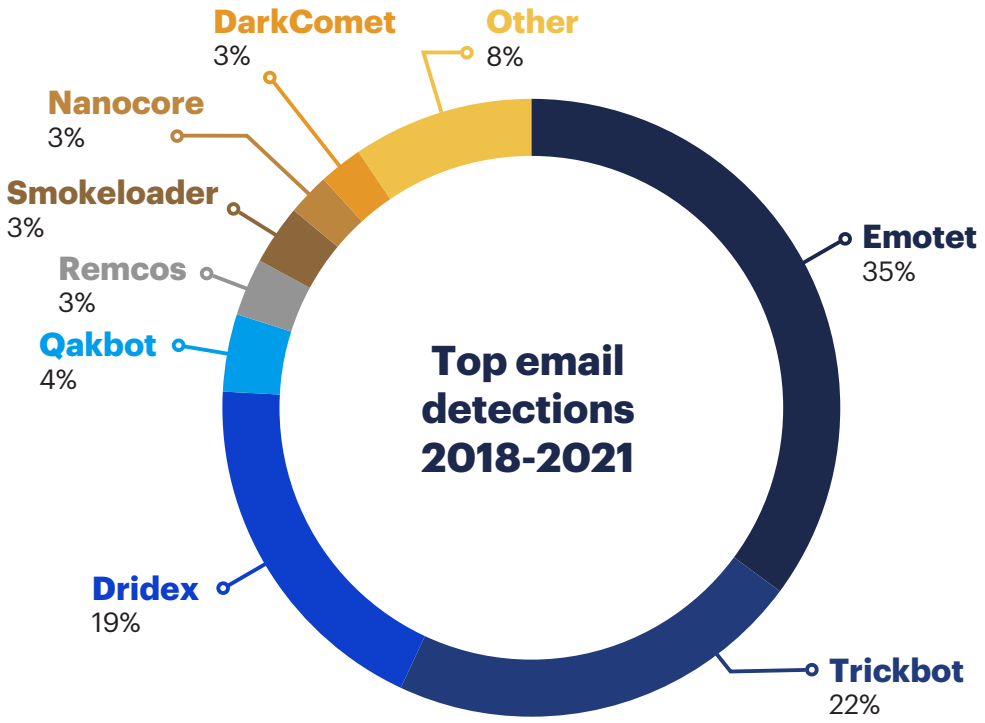

Top 10 global industry detections 2021
Agriculture 6%
Telecommunications 6%
Software & Technology 7%
Manufacturing 24%
Healthcare & Medical 7%
Retail & Distribution 7%
Business Services 12%
Construction 10%
Financial Services 11%
Education 10%

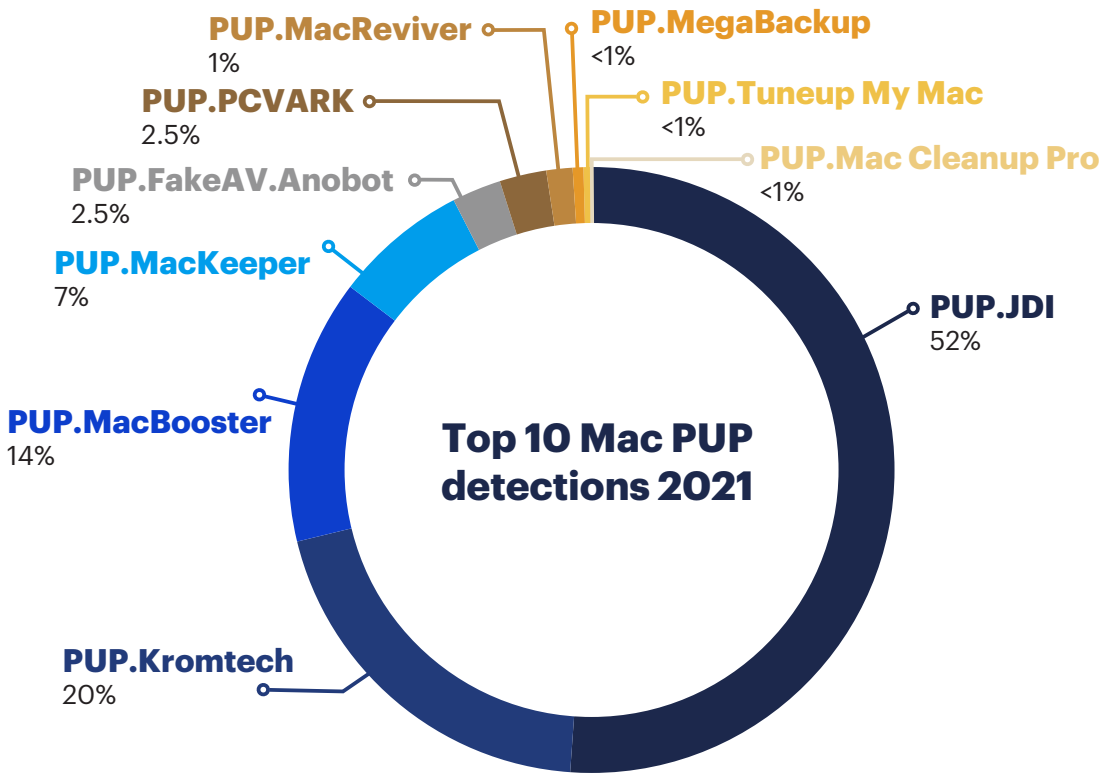

Top 10 detection categories (combined) 2021
Spyware 3%
Backdoor 2%
Exploit 2%
OSX 3%
Virus 4%
HackTool 7%
Heuristic Malware 34%
RiskwareTool 11%
Adware 15%
Trojan 19%

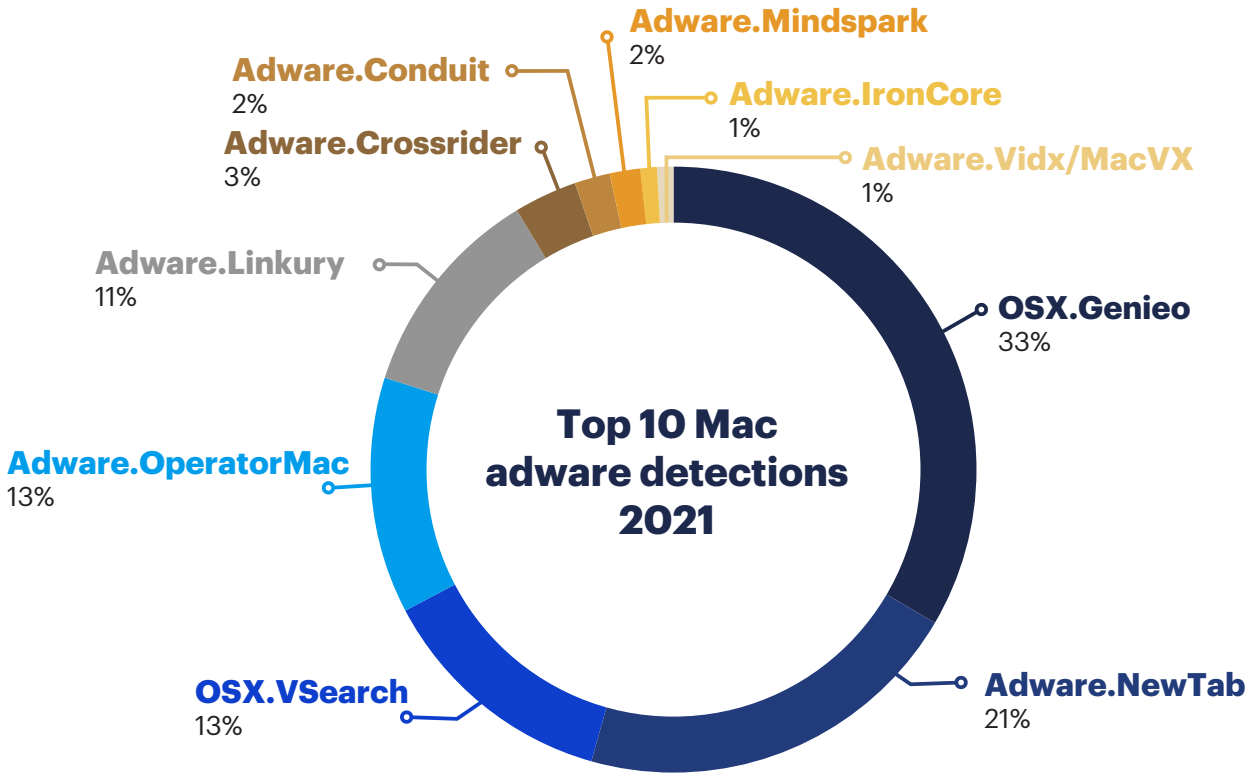

Spyware
3%
Virus
2%
Backdoor
2%
Exploit
4%
HackTool
4%
Heuristic
Virus
5%
Heuristic
Malware
41%
RiskwareTool
8%
Top 10
detection categories
(business) 2021
Adware
9%
Trojan
22%

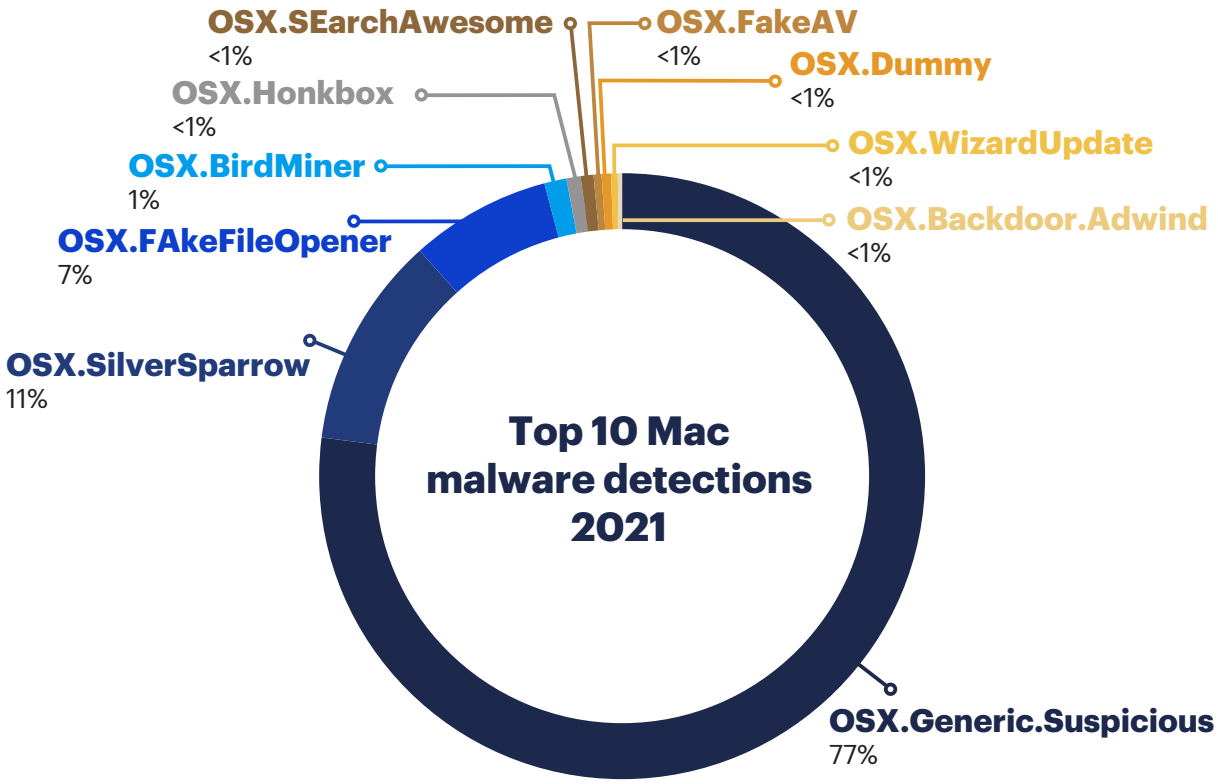

Spyware
3%
Backdoor
2%
Worm
2%
OSX
3%
Virus
4%
Hacktool
8%
Heuristic
Malware
31%
RiskwareTool
12%
Top 10
detection categories
(consumer) 2021
Adware
17%
Trojan
18%

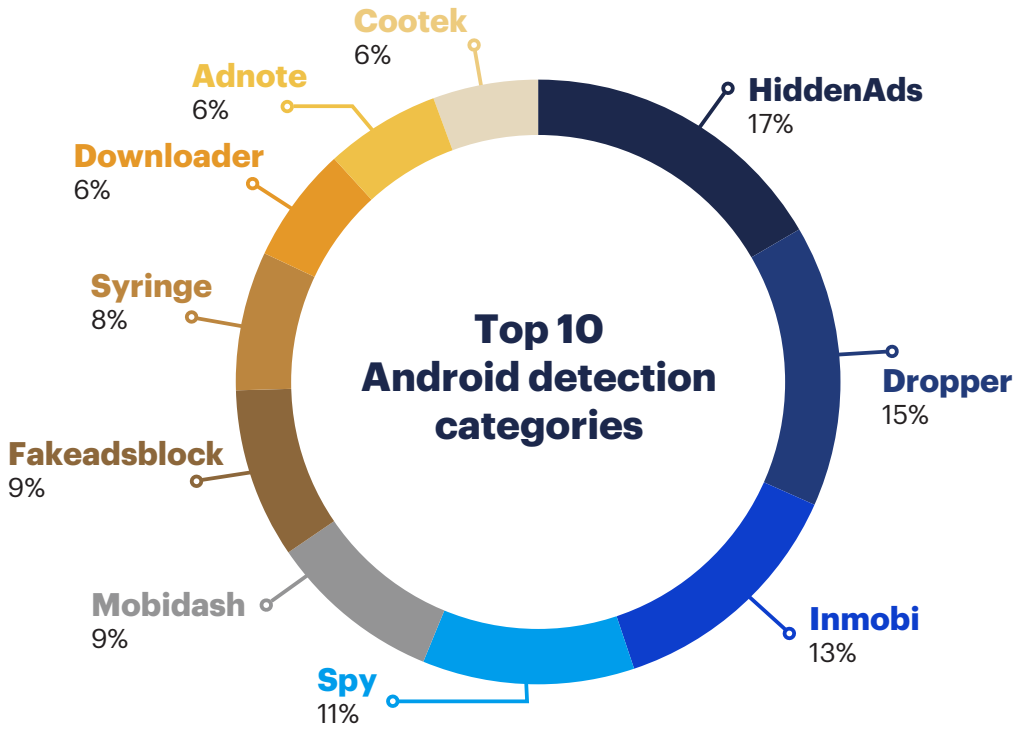

Backdoor
2%
Worm
2%
Sivis
2%
Spyware
3%
Virus
4%
Hacktool
7%
Heuristic
Malware
35%
Top 10
Windows detections
2021
RiskwareTool
12%
Adware
13%
Trojan
20%

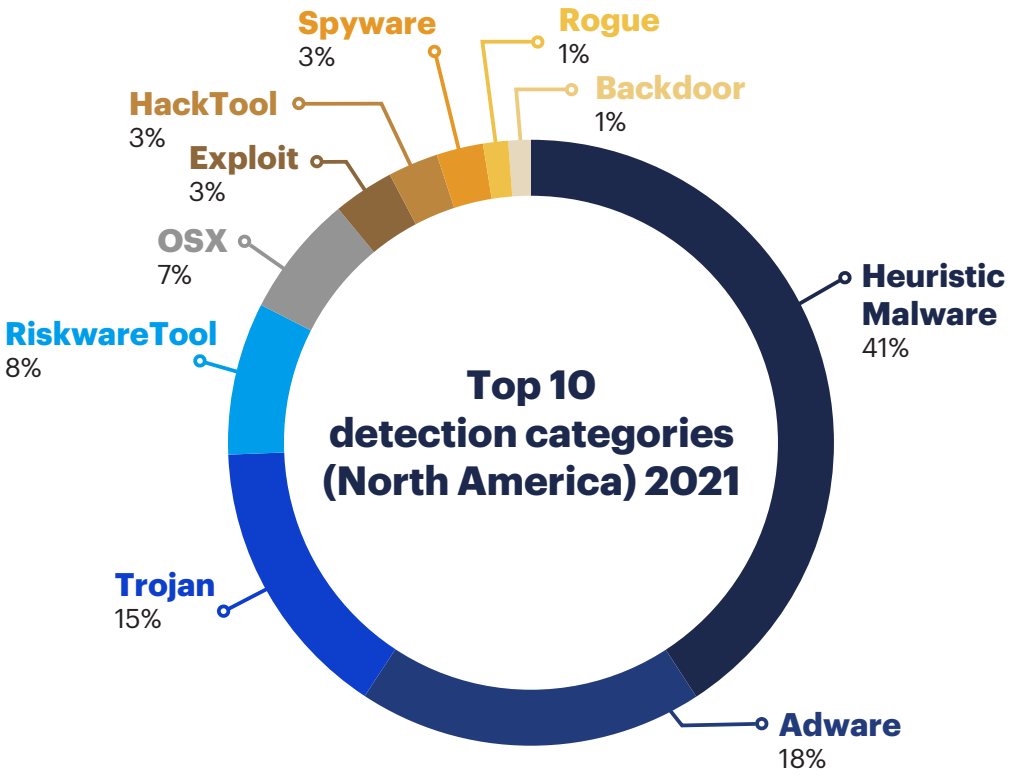

DarkComet
3%
Other
8%
Nanocore
3%
Smokeloader
3%
Remcos
3%
Qakbot
4%
Emotet
35%
Top email
detections
2018-2021
Dridex
19%
Trickbot
22%

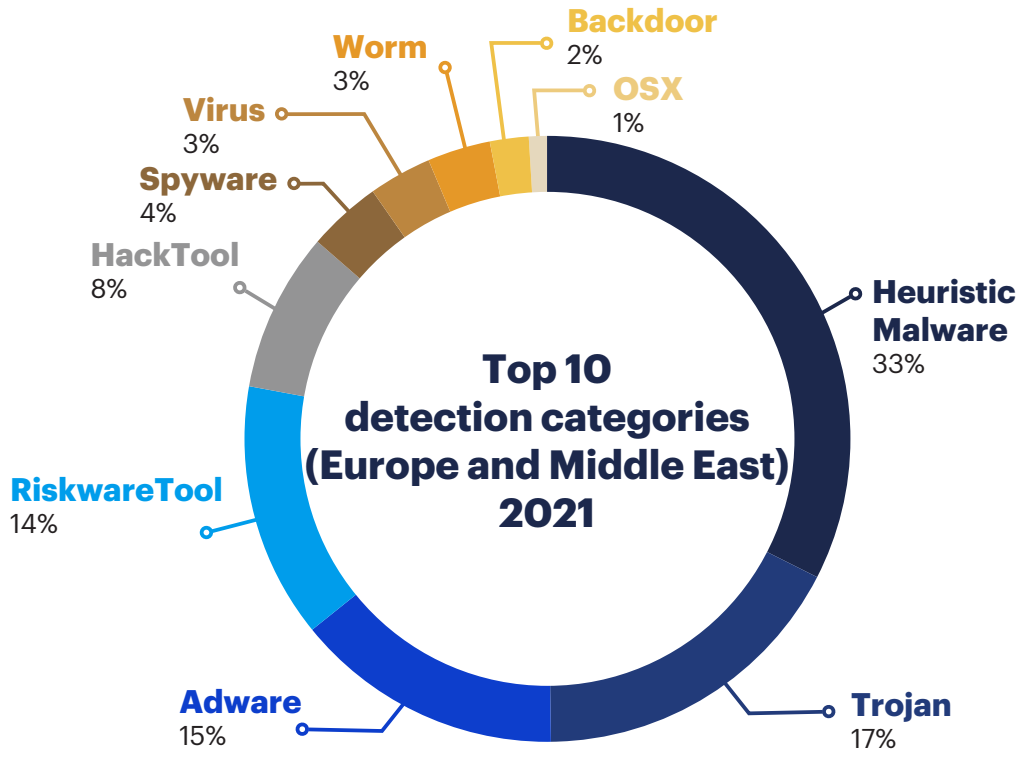

PUP.MacReviver
1%
PUP.MegaBackup
<1%
PUP.PCVARK
2.5%
PUP.Tuneup My Mac
<1%
PUP.FakeAV.Anobot
2.5%
PUP.Mac Cleanup Pro
<1%
PUP.MacKeeper
7%
PUP.JDI
52%
PUP.MacBooster
14%
Top 10 Mac PUP detections 2021
PUP.Kromtech
20%

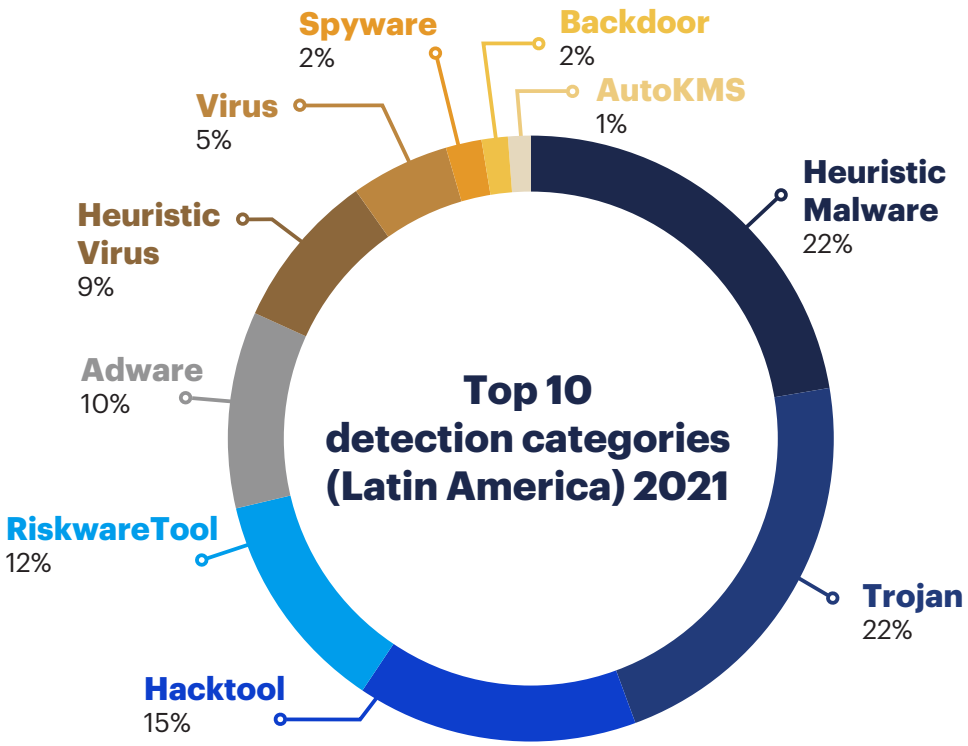

Adware.Mindspark
2%
Adware.Conduit
2%
Adware.IronCore
1%
Adware.Crossrider
3%
Adware.Vidx/MacVX
1%
Adware.Linkury
11%
OSX.Genieo
33%
Top 10 Mac adware detections 2021
Adware.OperatorMac
13%
OSX.VSearch
13%
Adware.NewTab
21%

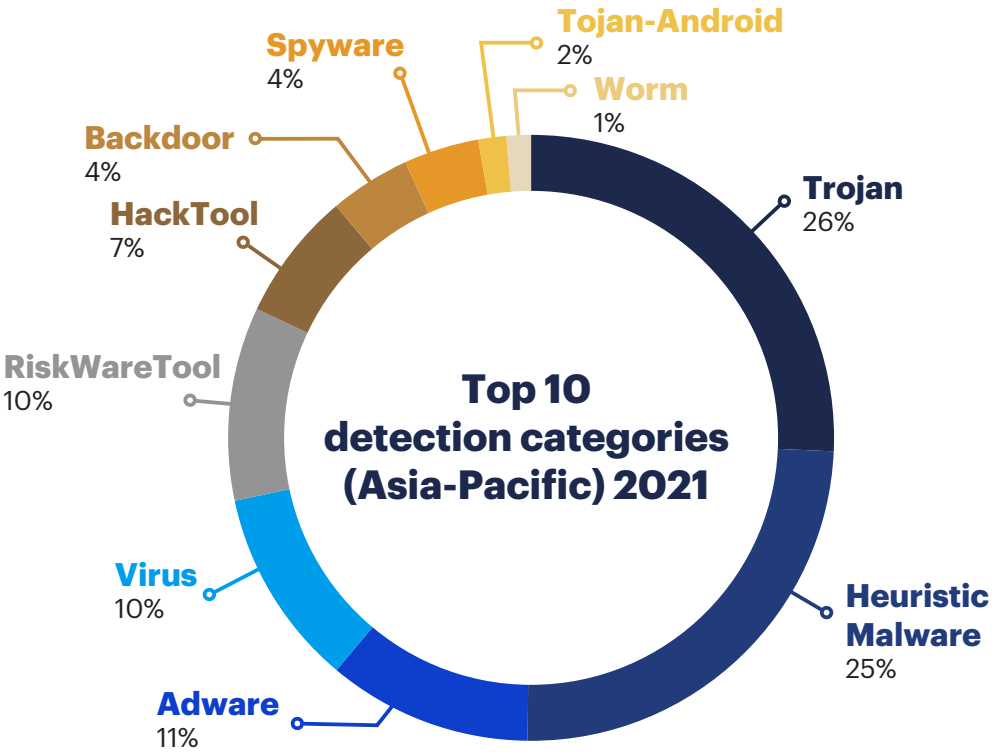

OSX.SEarchAwesome
<1%
OSX.FakeAV
<1%
OSX.Dummy
<1%
OSX.Honkbox
<1%
OSX.WizardUpdate
<1%
OSX.BirdMiner
1%
OSX.Backdoor.Adwind
<1%
OSX.FAkeFileOpener
7%
OSX.SilverSparrow
11%
Top 10 Mac malware detections 2021
OSX.Generic.Suspicious
77%


Cootek
6%
Adnote
6%
HiddenAds
17%
Downloader
6%
Syringe
8%
Top 10 Android detection categories
Dropper
15%
Fakeadsblock
9%
Mobidash
9%
Inmobi
13%
Spy
11%

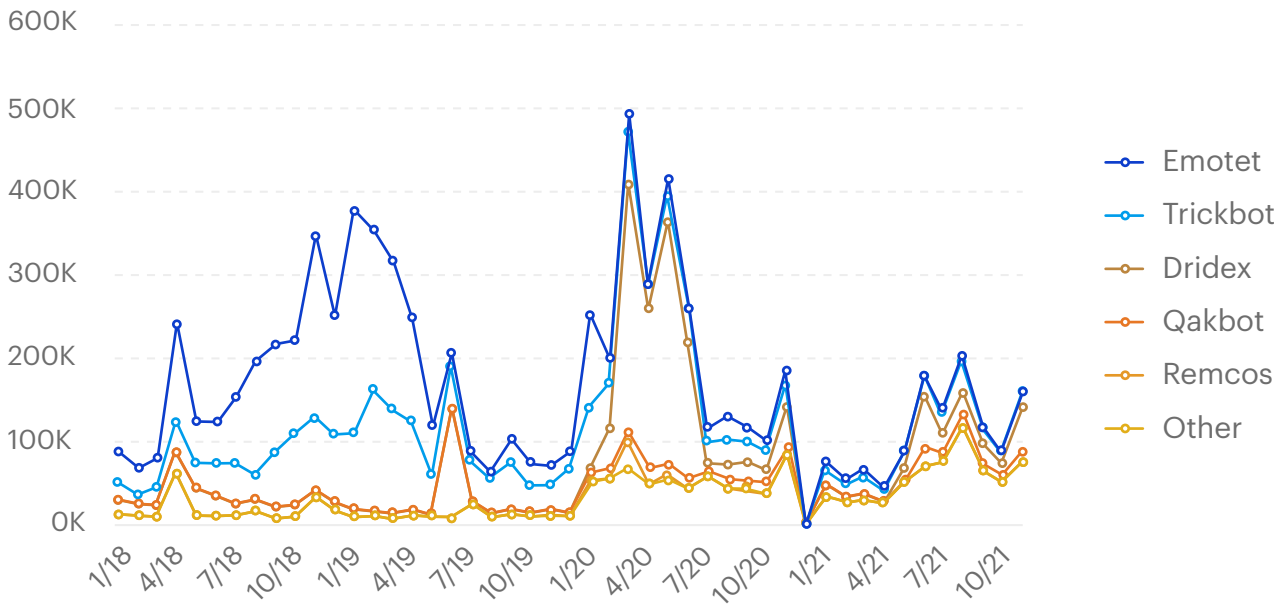

Spyware
3%
Rogue
1%
Backdoor
1%
HackTool
3%
Exploit
3%
OSX
7%
RiskwareTool
8%
Heuristic
Malware
41%
Top 10
detection categories
(North America) 2021
Trojan
15%
Adware
18%


Worm
3%
Backdoor
2%
OSX
1%
Virus
3%
Spyware
4%
HackTool
8%
Heuristic
Malware
33%
Top 10
detection categories
(Europe and Middle East)
2021
RiskwareTool
14%
Adware
15%
Trojan
17%

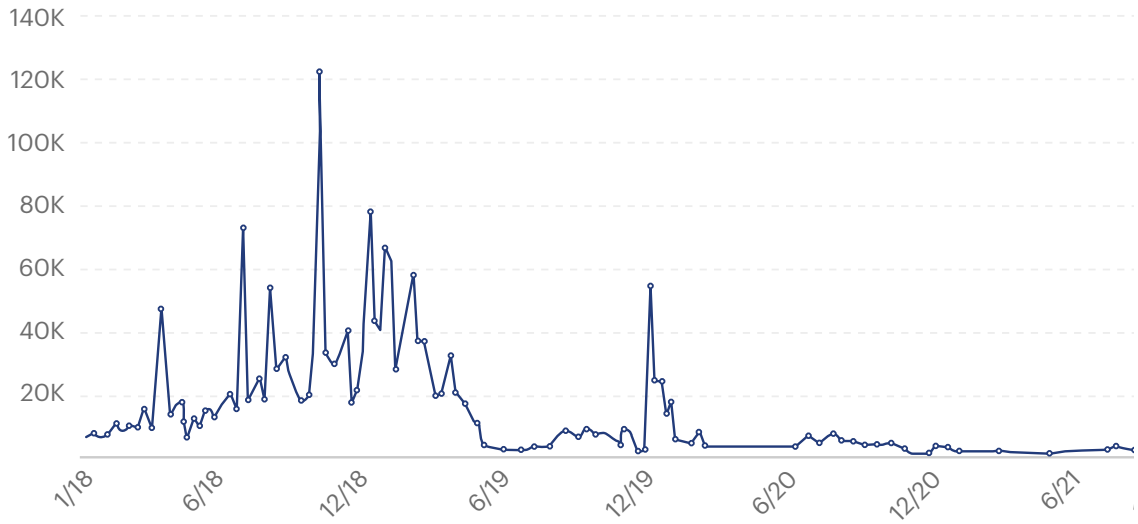

Top 10 detection categories (Latin America) 2021
Spyware 2%
Backdoor 2%
AutoKMS 1%
Virus 5%
Heuristic Malware 22%
Heuristic Virus 9%
Adware 10%
RiskwareTool 12%
Trojan 22%
Hacktool 15%


Top 10 detection categories (Asia-Pacific) 2021
Tojan-Android 2%
Spyware 4%
Worm 1%
Backdoor 4%
Trojan 26%
HackTool 7%
RiskWareTool 10%
Virus 10%
Heuristic Malware 25%
Adware 11%

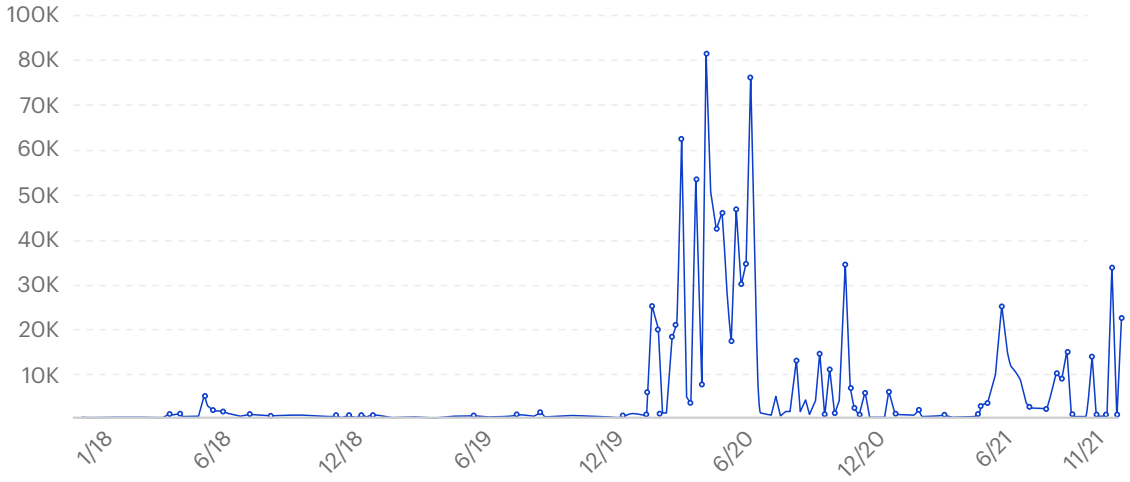
Email threat detections 2018-2021



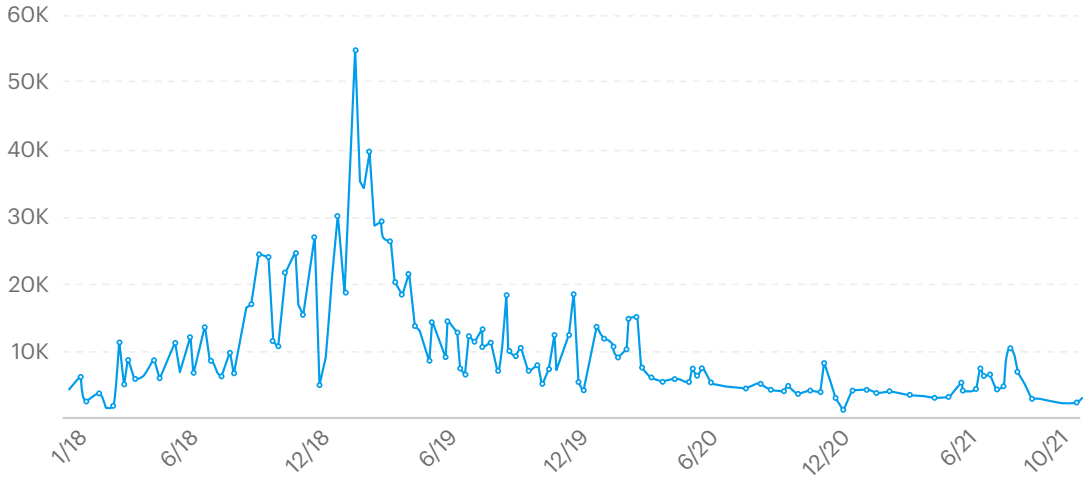
Emotet detections 2018-2021



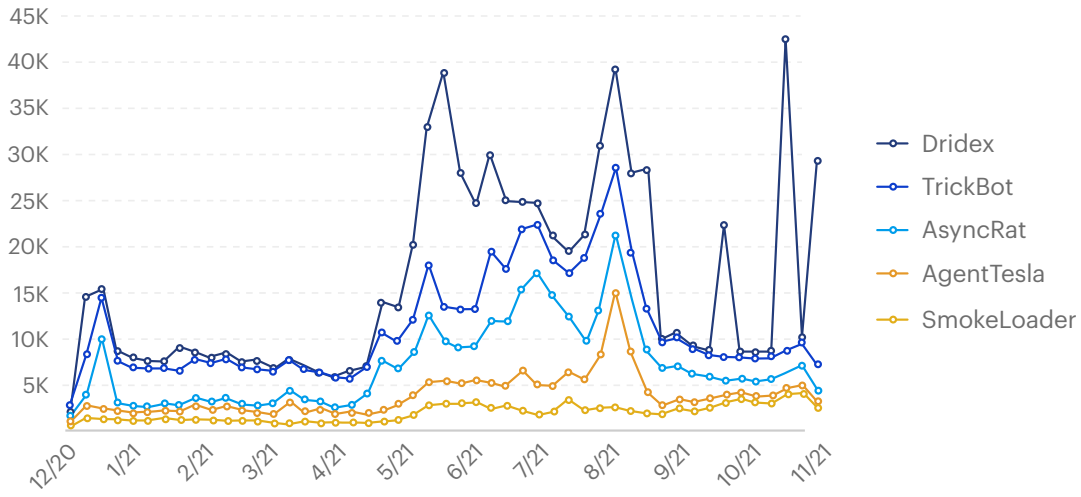
Dridex detections 2018-2021



TrickBot detections 2018-2021



Email threat detections 2021



Malwarebytes cyberprotection

Malwarebytes Inc.

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

USA

+1-800-520-2796