FACTS AND FIGURES

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

# SECURITY REPORT 2019/2020

# The AV-TEST Security Report

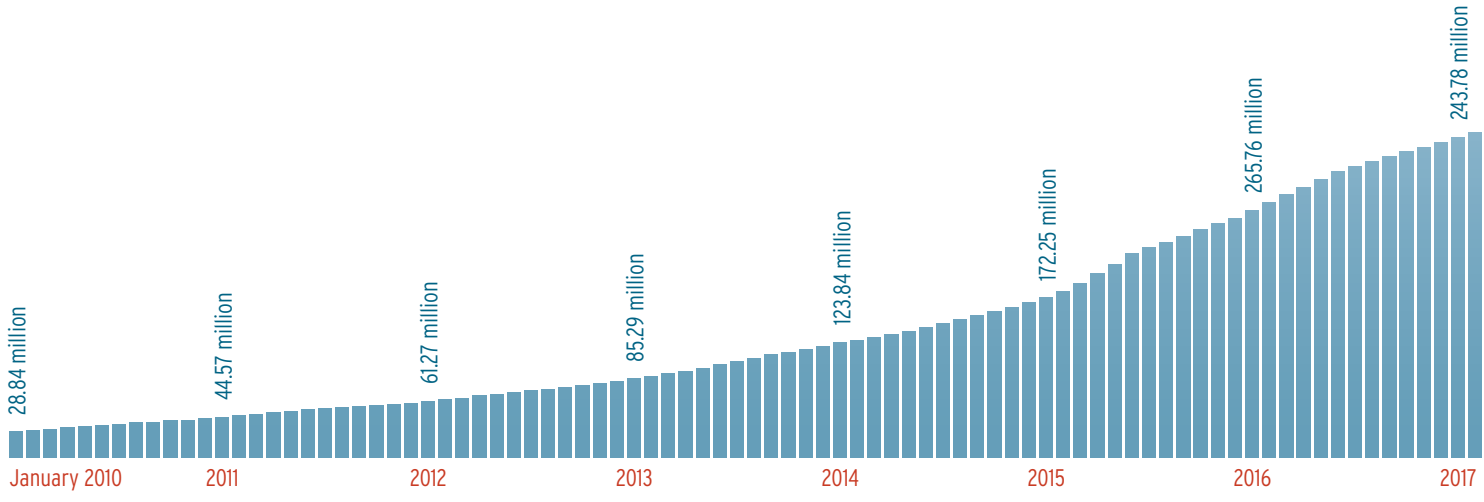
As the evaluations of malware numbers of the AV-Test Institute's detection systems illustrate, the new trend in the malware industry observed in 2019 clearly continued in the 1st quarter of 2020. The development of malware is divided up into two areas: While on the one hand the automated production of mass malware for broadly-based online attacks continues to grow sharply, on the other hand cybercriminals are increasingly developing sophisticated malware for specialized attacks. In this, a combination of specially-developed attack tools is deployed, which is precisely adapted to the previously identified digital infrastructure of the victims.

## Mass malware with a massive rate of increase

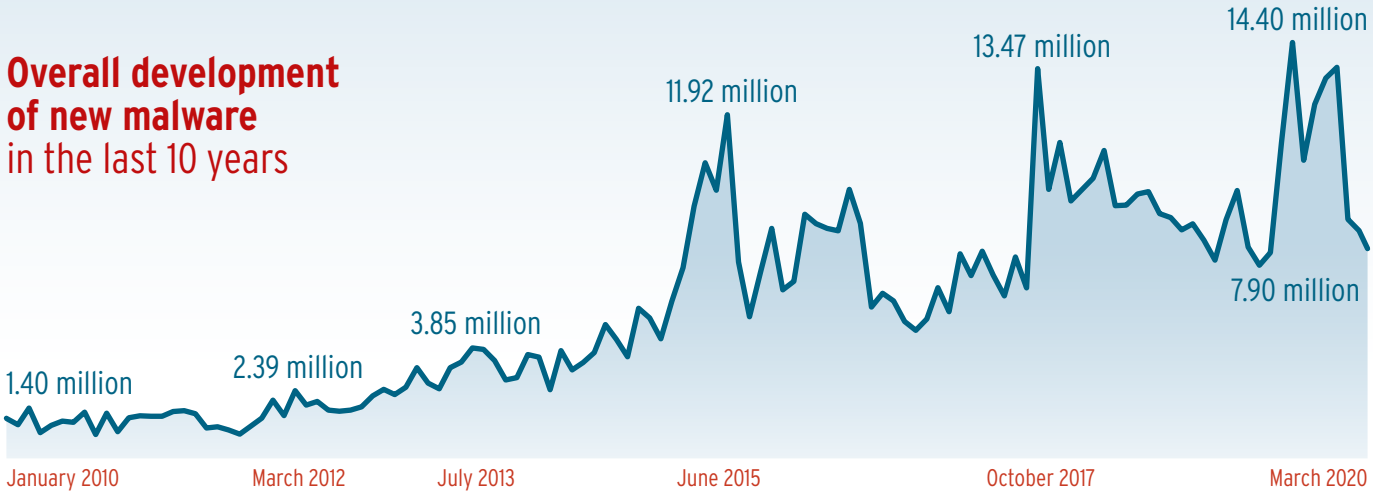
In 2019, the use of mass malware, i.e. malware programs created automatically, reaped considerable profits for cybercriminals. Accordingly, the rate of this malware, distributed mainly in large campaigns per e-mail and over the Internet, continued to grow heavily. With more than 114 million (114,312,703) newly-developed malware applications, the malware industry once again broke the sound barrier in 2019 and was more active than ever before. Up to that time, the detection systems of the AV-Test Institute had identified the year 2018, registering over 105 million newly-developed samples, as the most active year of criminal players.

The analysis of the latest detection statistics for the first quarter of 2020 indicates that this year will also see significant growth rates in the use of mass malware: Already in the first quarter of the current year, the AV-TEST systems have registered over 43 million newly-programmed samples. Accordingly, by the end of 2020, there will be an anticipated explosion of newly-developed malware applications, which could level off for the entire year at more than 160 million samples – and thus reach a new dimension. In the long-term view of the AV-Test Institute, the malware industry is thus proving to be more active than ever and is anticipated over the course of the year to surpass the overall threshold of 700 million known malware programs. As a result, the threat scenario posed by mass malware could reach a new dangerous peak in 2020. Currently, the development rate of new malware is at 4.2 samples per second!

## Total malware in the last 10 years

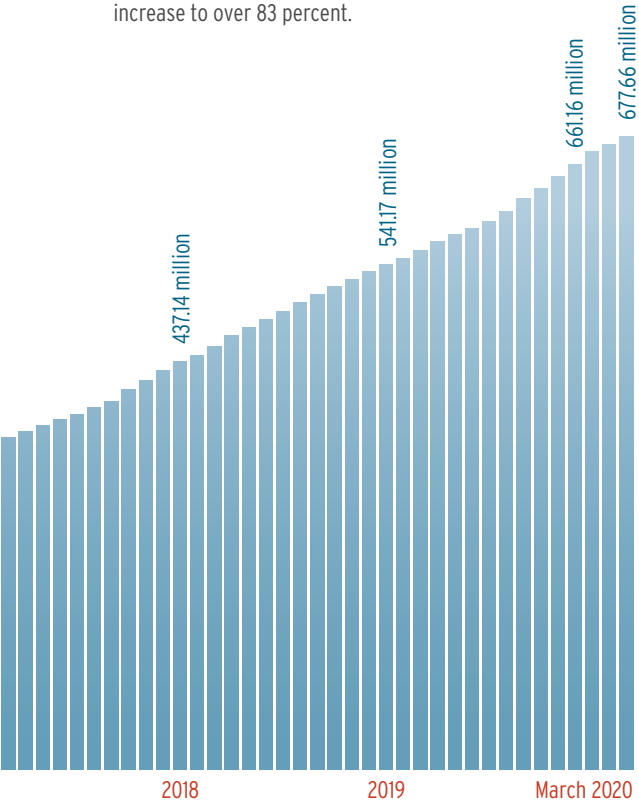


## Overall development of new malware in the last 10 years




## Increasing detection rates increase development pressure

A precipitating factor for this dramatic development can be viewed as a positive, because among other reasons, the mass development of new malware samples can be explained by the high level of protection currently provided by security products. This is true especially for protection solutions for Windows systems. Because the majority of all malware still targets the operating system most widely used by far around the world. In 2019, over 78 percent of malware codes newly-developed by cybercriminals targeted Windows systems. In the first quarter of 2020, this value continued to increase to over 83 percent.




Entrepreneurs, albeit driven by clearly criminal motives, are on the one hand attracted to the wide level of distribution enjoyed by the operating system from Redmond. On the other hand, it is a known fact that Windows systems are still not sufficiently protected so as to become an unattractive target for criminals. And thus they develop industrial scale mass malware for systems connected to the Internet, whose protection mechanisms are not up to the state of the art of countermeasures. The number of all detected and analyzed malware programs for Windows at the time this report went to print was 517,465,709 samples. You can find precise data and analyses concerning the threat scenario for Windows systems from page 8.

## AV-ATLAS: the threat intelligence platform from AV-TEST

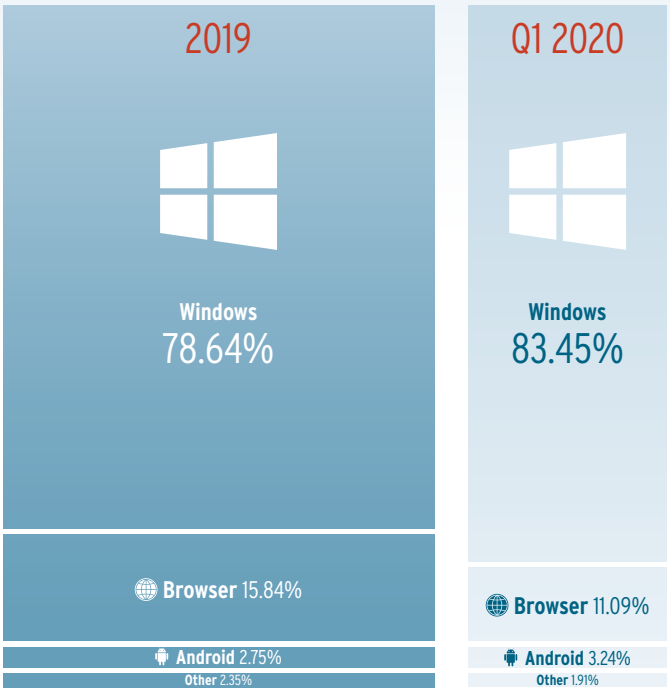
In 2019, AV-TEST launched its AV-ATLAS threat intelligence platform (av-atlas.org). Over the course of this development, the institute's in-house detection systems were calibrated in terms of measurement technology. Such a step allows not only for a much more precise analysis of malware samples, prevents duplications and false positives, but also retroactively enables an adaptation of the detection figures to the state of the art in technology. As a result, there may be some changes in numbers compared to the published statistical findings in previous security reports. With the AV-ATLAS, the AV-Test Institute constantly offers new statistics and evaluations on the current threat situation.

## Android and MacOS systems running around without protection software

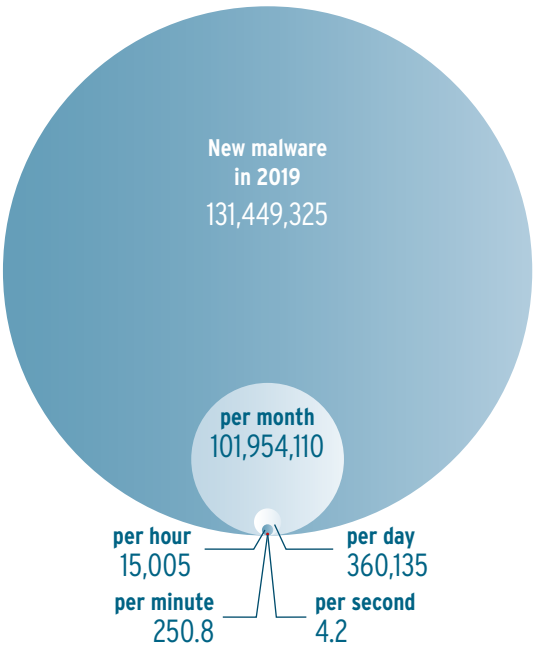
The AV-TEST systems registered a slight decline in the rate of newly-developed malware on the most widely-distributed mobile operating system from Google. The operating system reached its peak in malware growth in the year 2017 with 6,201,358 newly-programmed samples. Since then, the number of new Android malware samples has been declining, in 2019 reaching the lowest level in three years with 3,170,140. Although this trend is actually welcome, falling malware statistics do not automatically mean a diminished threat scenario for users of Android devices. Moreover, the trend of the first quarter of this year already indicates a resurgence of malware trends for Android.

For MacOS as well, the detection systems of AV-TEST in 2019 indicated declining, yet persistently high malware statistics. Whereas the previous year, with over 90,000 newly-programmed malware applications represented a glaring milestone in the trending history of MacOS malware, new developments reached approximately half that number in the subsequent year, remaining below 60,000. If the statistics of this year's first quarter continue, an additional decline in new Mac malware can be anticipated. At least statistically, the number of new malware samples for Apple computers is expected to level off at roughly 40,000 new samples towards the end of the year.

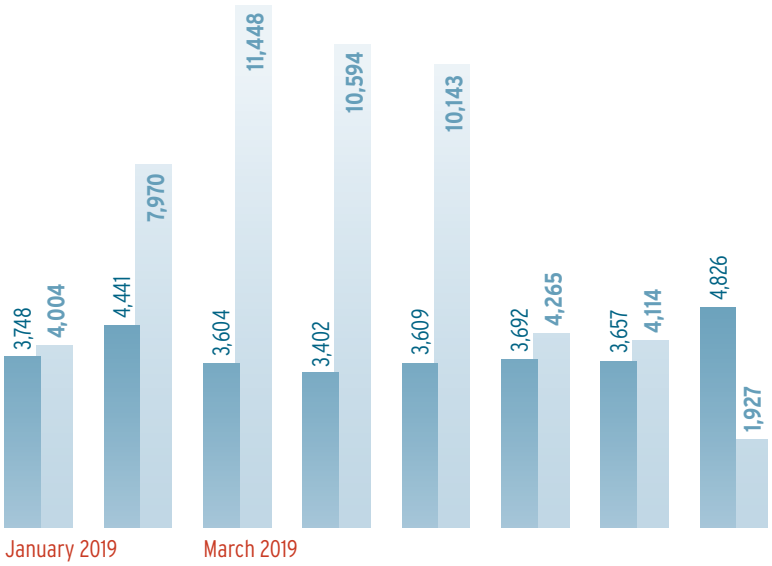
## Distribution of malware



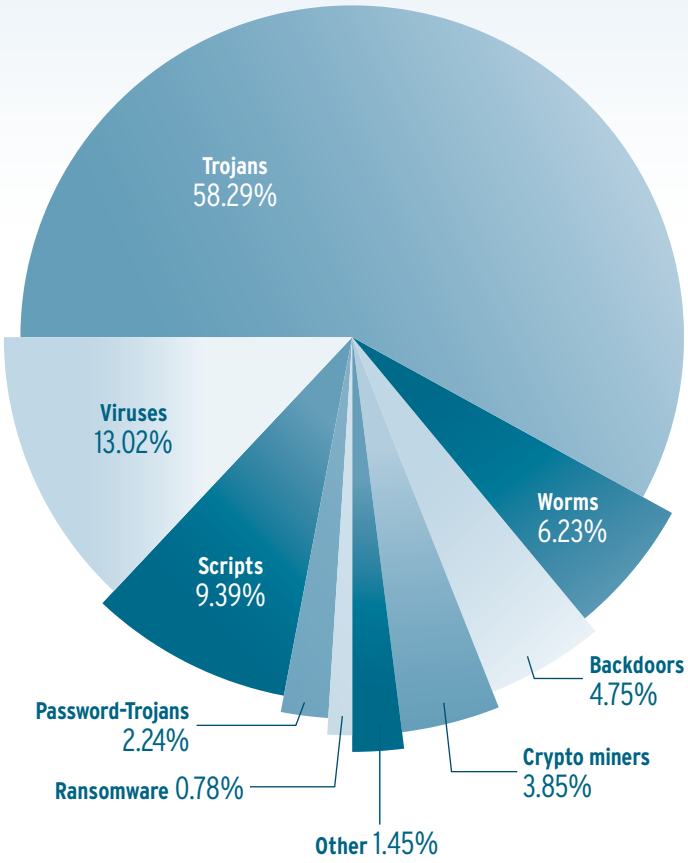

## Average malware threat in 2019




## MacOS: ratio of malware to PUA in 2019 + Q1 2020



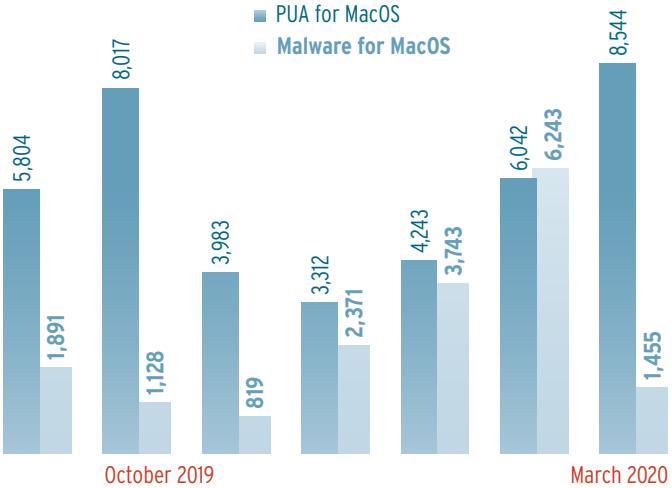
## Overall malware distribution in 2019



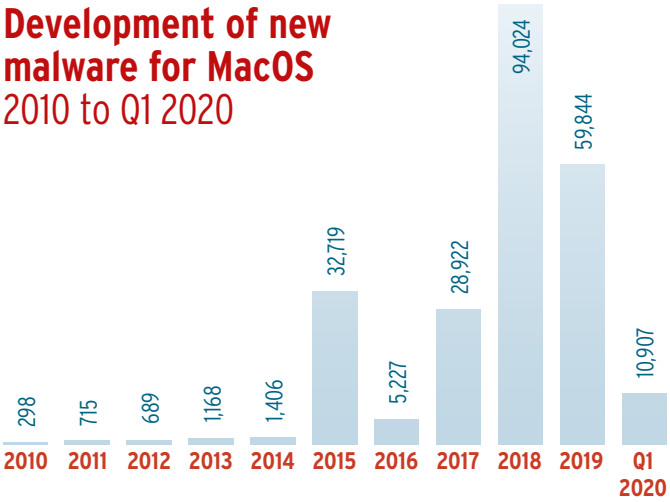

Overall, both these estimates and declining malware numbers are to be taken with a grain of salt, however, as they do not automatically equate to a diminished threat scenario. Both operating systems, not only Google's mobile system Android but also Apple's MacOS, compare negatively with Windows in the sense that the deployed user devices are largely operated without effective protection software. Notably, as evidenced by regular tests by the AV-Test Institute, there are a large number of even free apps and antivirus solutions for both systems, with which a decent level of security could be reached. You can find more precise analyses on the threat scenario for Android devices in this report from page 12, for devices under MacOS from page 16.

## Trojans: the most popular all-purpose weapon

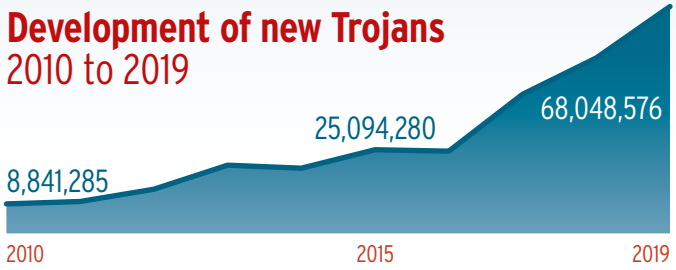
Accounting for a 58 percent share of malware incidence for all operating systems, last year Trojans once again proved to be cybercriminals' weapon of choice. That should come as no surprise: This malware category enters target devices through virtually all available digital channels. Trojans can be transmitted merely by visiting infected websites, they travel well concealed in large spam waves per e-mail, lurk in seemingly harmless software and app downloads, and hide in would-be music and movie files. Yet they can also be delivered with extreme precision into systems of potential victims, i.e. by calling up QR codes or via storage media laid out as bait, such as supposedly lost USB sticks.



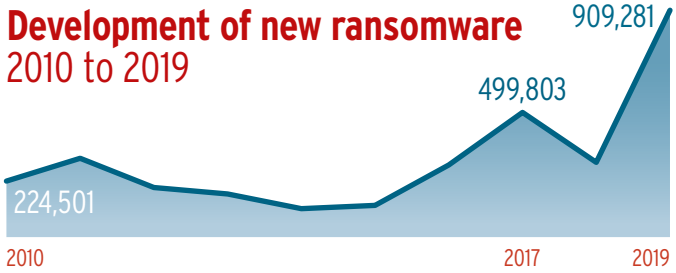

## Development of new malware for MacOS
2010 to Q1 2020



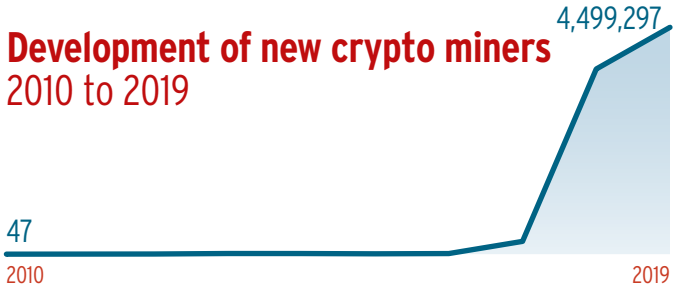
## Development of new Trojans
2010 to 2019



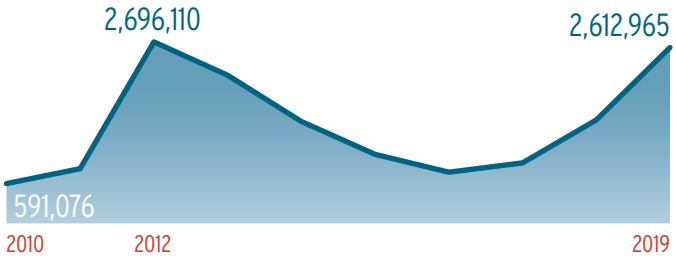

## Development of new ransomware
2010 to 2019



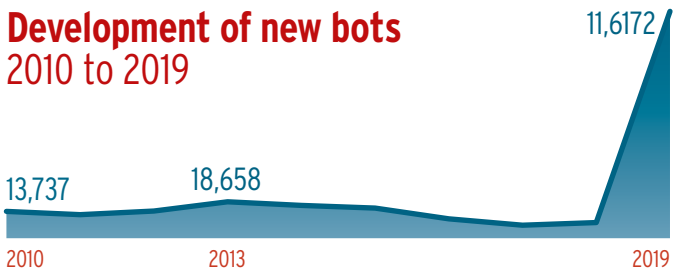

## Development of new crypto miners
2010 to 2019




## Development of new password-Trojans
2010 to 2019




## Development of new bots
2010 to 2019




In addition to comprehensive malware functions that Trojans contain, they can retroactively load virtually any malware code onto hijacked systems, which is why they are frequently only the first wave of an attack. If a sufficient number of systems is infected, cybercriminals proceed to add specialized malware code. Depending upon the criminal business model of the attackers, the payload may involve ransomware for blackmailing users, bots, and crypto miners for abusive use of hijacked CPU power and bandwidth or various other malware functions. This business model was so manifestly successful in 2019 that the cybermafia further boosted the use of massively distributed Trojans in the first quarter of this year, and as a result, the current Trojan rate is 66.82 percent.

## Ransomware as a growth market

Last year, extortion through ransomware proved to be an additional lucrative source of income. The trend of this malware tripled in 2019 compared to the previous year, reaching the highest level to date of over 900,000 samples. The same applies to the rapidly increasing number of crypto miners. The illegal mining of cybercurrencies at the expense of users with systems infected with such special malware has apparently turned out to be a lucrative source of income. The last Security Report by the AV-Test Institute already anticipated this trend.

## Attacks follow the laws of economics

As mentioned at the beginning of the report, the majority of the attacks launched per malware targeted Microsoft systems. Thus, cyber-criminals act according to strict economics. Because in addition to wide distribution of a target system and the subsequently anticipated profit, vulnerability also plays an important role in the economic considerations of the malware industry. Thus, a look at discovered and published vulnerabilities of various manufacturers, such as is apparent in the evaluations of the CVE online service, shows that in this respect, Microsoft is by far the most lucrative target. It may be true that Android and Debian are number one and two in terms of the number of security gaps in products discovered last year. But a Windows system already follows in third place, and seven more are among the Top 20. Seen overall, Microsoft thus earned the dubious honor in 2019 of being the number one manufacturer in terms of having the most known security leaks. Such statistics are naturally also of interest to criminals who earn their money with the development of mass malware.

## APT: trend towards targeted attacks

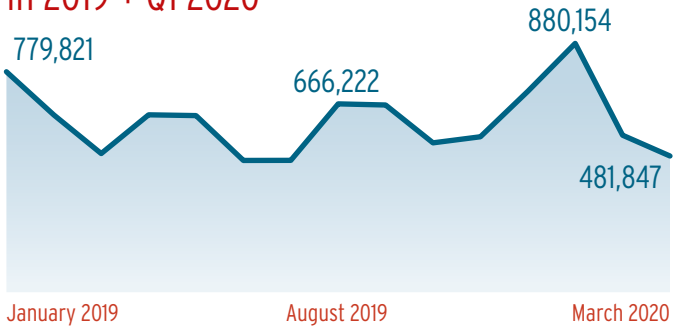
The massive increase in targeted attacks by means of Advanced Persistent Threats (APTs) can hardly be quantified for various reasons: First, these types of tactical attacks are strategically prepared long in advance and staged against companies and organizations that manage extremely valuable information. Moreover, such attacks, normally leveled by state-organized attackers against ministries, research, and production facilities as well as financial firms and other institutions of a country, are seldom made public. Yet it is a fact that companies in particular are increasingly required to introduce special defensive measures against targeted attacks on their digital infrastructure. Since 2006, this has been underscored by listings in the database of the Center for Strategic and International Studies (CSIS). The AV-TEST Institute responds to the increase in already known APT attacks with a testing and certification program of security solutions aligned with the MITRE standard. You can find information on the tests for evaluating effectiveness in fending off APT attacks on our website.

## PUA: unwanted, yet widely distributed

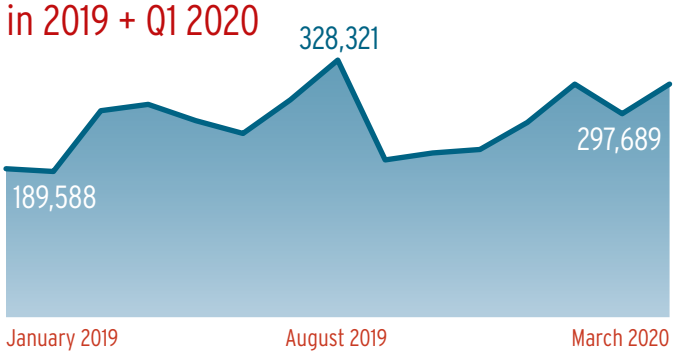
In addition to malware attacks, Internet users also need to protect themselves against another threat, however: potentially unwanted applications, or PUAs for short. This spyware is often pre-installed when devices are delivered with software bundles, yet much more frequently it sneaks onto the devices when downloading programs and apps. The source is usually the advertising industry that uses PUAs to detect and analyze personal information such as user behavior and movement patterns. In exchange for the unwanted and usually secretly queried data, the user receives personalized advertising.

Whereas these industrial snooping tools have been on the retreat in Windows systems for years, their numbers are heavily increasing in the Android environment. And among MacOS systems, the number of PUA samples in 2019, totaling 52,095, was even nearly on the same level as the overall rate of malware (60,674 samples). In the first quarter of this year, the number of such snoop software for Macs even exceeded the rate of malware: Whereas the AV-TEST systems detected 11,441 new malware samples, the PUA rate was already at 18,829 samples. Accordingly, this category of malware in particular is developing into a new threat for Mac users.

**Windows: development of new PUA**
in 2019 + Q1 2020




**Android: development of new PUA**
in 2019 + Q1 2020



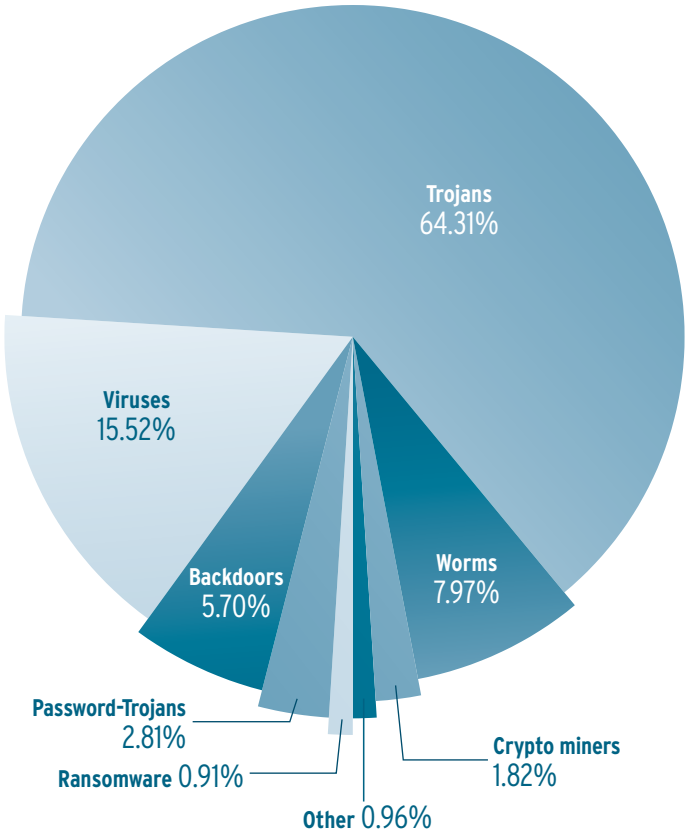
# Security Status WINDOWS

No other operating system is so much the focus of the malware industry. There is a good reason for this: No other operating system achieves a similar degree of distribution. So any cybercriminal seeking business success has their sights clearly set on one target: Windows systems. It should be noted, however, that attacks on the operating system from Redmond are no longer the business of amateurs. Because the high degree of penetration and effectiveness of current security solutions in turn requires rapid speed and innovation in the development and distribution of mass malware and sophisticated techniques in targeted attacks.

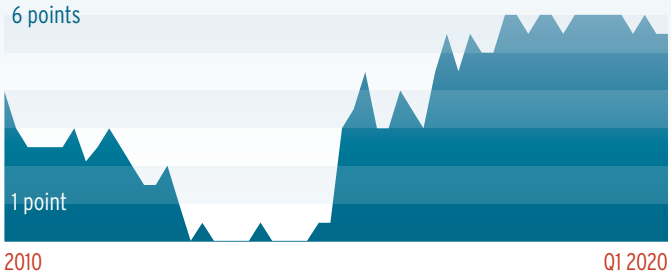
## Bullseye on the market leader

According to the CVE database, Microsoft, with more than 660 officially reported dangerous security gaps last year, earned an unflattering image and the number one position among the least secure operating systems. 357 of all potential Windows vulnerabilities for attacks alone were attributable to the current Windows 10 operating system. Also exhibiting a high degree of vulnerability were Windows Server 2016 and Windows Server 2019. Somewhat lagging behind was Windows 7, which at the beginning of this year was officially put out to pasture by Microsoft and is no longer provided with updates and security patches. Nonetheless, the Windows oldie remains highly popular according to the latest evaluations: In the rankings of the first quarter of this year, Windows 7, remaining at 30 percent, still achieved the number two ranking of the most widely-used operating systems in the world. The clear market leader is Windows 10, which is running on just over half (51.38%) of all worldwide computers connected to the Internet.

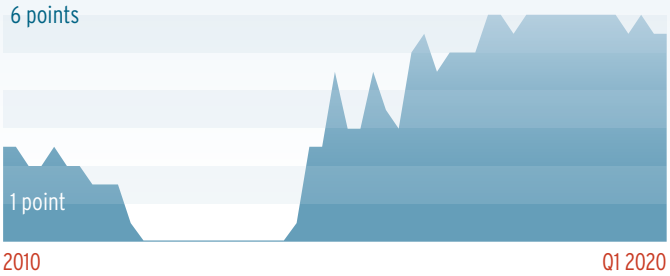
## Distribution of malware under Windows in 2019



## Protection Windows Defender Antivirus Home 2010 - Q1 2020




## Protection Windows Defender Antivirus Business 2010 - Q1 2020




Obviously, consumer users got on board prior to Windows 7 support being phased out and switched over to the successor system. In many other areas, e.g. in industrial manufacturing, government entities such as administration and educational institutions, hospitals, not to mention companies and banks, frequently the rule applies, „Never change a running system". Because changing an operating system here is often a considerable cost factor, the switchover rate is accordingly assumed to be much lower than in the consumer segment.

## Windows gaps actively exploited like never before

In addition to the known and published Windows gaps, naturally there are also those that were not known or are not known to either the public or the manufacturer. Unfortunately, only few of such „secret" security leaks are communicated to the manufacturers; instead, they are used by intelligence agencies for investigative and monitoring purposes. This means such software gaps are traded at high prices on the black market. A practice that is rightly subject to regular, severe criticism both by software manufacturers and data protection and civil liberties advocates. And in addition to possible backdoors in the operating system, security vulnerabilities in widely-used applications as well as the firmware of connected devices make the risk scenario all the more severe. Thus, in 2019 Google, Oracle, Adobe, Cisco, and IBM landed in 2nd to 6th place of the Top 10 manufacturers with the most security gaps. The Adobe Reader alone, used worldwide, reached an impressive 342 known vulnerabilities.

In 2019, the malware industry reacted accordingly to the largest number of security vulnerabilities to date for Windows and the software run on that operating system: The levels of detected Windows exploits for utilizing relevant security gaps reached the highest level compared to the past 10 years. Especially from August to November, the exploits exhibited more than exponential growth. Significant increases were already seen at the beginning of the year, however. By comparison: In the prior year, the overall annual figure did reach 71,377 samples. In 2019, this figure virtually doubled to exactly 130,776 newly-programmed exploits.

The high development rate can in turn be interpreted as an indication of two positive developments last year: First, Microsoft, as the supplier of the operating system with the most security leaks, was quick to release patches. This fact puts cybercriminals under pressure to produce assembly line malware samples in order to remain economically profitable. In addition, the embedded Windows defense systems proved to be reliable protection against automated mass malware. In the regular certification tests over the past year, Microsoft's consumer product, „Microsoft Defender Antivirus" garnered the AV-TEST rating as „Top Product" five out of six times. Which among other things was due to the reliable detection and defensive performance against widely-distributed and frequently-occurring malware. The business solution from Microsoft exhibited even better test results in 2019 and was even able to defend the title of „Top Product" in six out of six annual tests.

## Windows: development of new exploits in 2019 + Q1 2020


## Windows: development of new Trojans in 2019 + Q1 2020


## Increase of Windows Trojans of over 35%

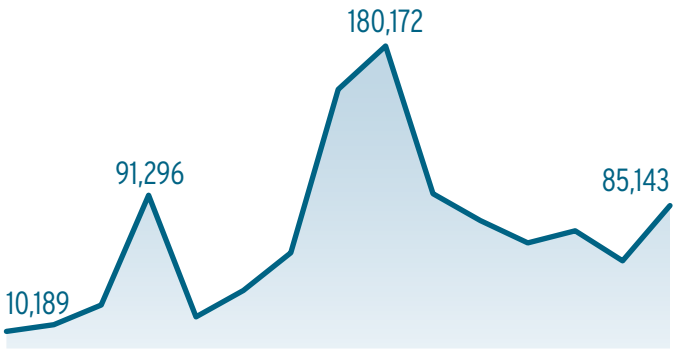
Wherever criminals were successful at infecting Windows systems, Trojans are generally used to spearhead the attack. On the one hand, to enable access to hijacked systems for as long as possible, and on the other hand, to upload specialized malware containing other malware functions.

Accordingly, the rate of new development for Trojans reached its highest level thus far in 2019. The prior year's figure of 42,594,399 was exceeded by last year with a number totaling 57,612,235, representing an increase of more than 35 percent. Overall in 2019, Trojans with 64.31 percent made up the largest share by far of the Windows malware deployed by criminals. There were two remarkable waves of Trojans, one starting in August and one in November of last year, thus ushering in the highest danger level for Windows users in 2019.

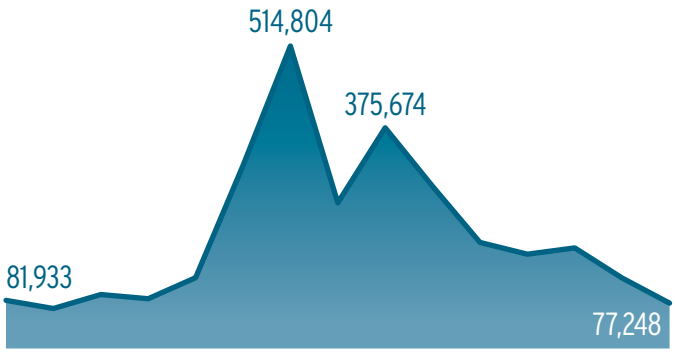
Because virtually at the same time the first Trojan wave was unleashed, several other campaigns of malware categories were launched as well. According to the analyses of the AV-TEST detection systems, this included bots, ransomware, password Trojans and crypto miners in particular.

The bottom-line conclusion is that from mid-year until the end, there was an unmistakable movement by criminals in the direction of monetizing by means of unleashed mass malware. Beginning with the extortion of Windows users through the blockage or encryption of Windows folders or entire systems, through capture of login data for online accounts of all kinds, right down to abuse of third-party infrastructure, bandwidth, and CPU power in order to mine cryptocurrencies such as Bitcoin. In particular, alternative currencies, such as Binance Coin (BNB), Litecoin and Bitcoin Cash, came into the crosshairs of criminals in 2019, not least thanks to their high rate of market capitalization.

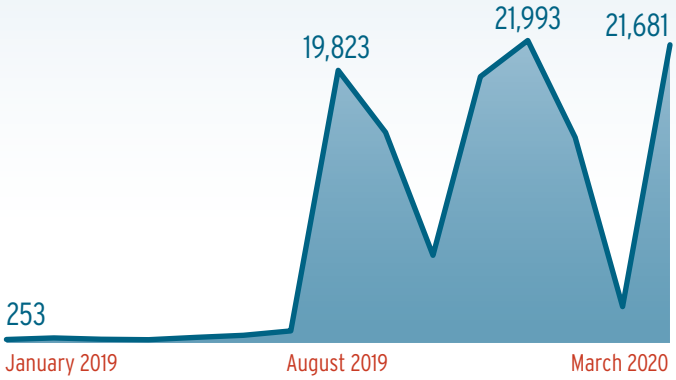
## Windows: development of new ransomware in 2019 + Q1 2020



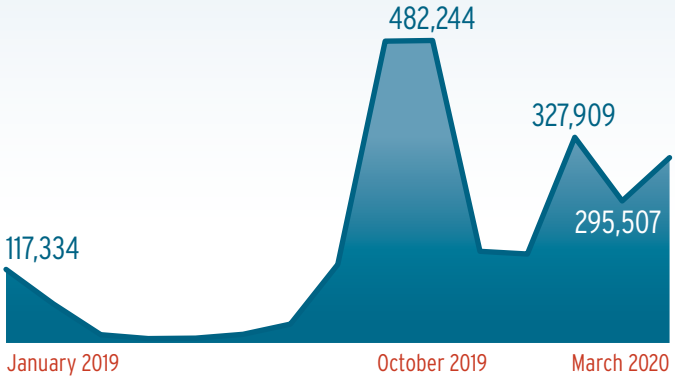

## Windows: development of new password-Trojans in 2019 + Q1 2020



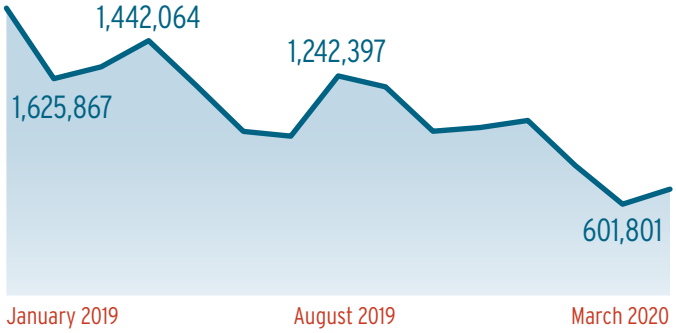
## Windows: development of new bots in 2019 + Q1 2020




## Windows: development of new crypto miners in 2019 + Q1 2020




## Windows: development of new Viruses in 2019 + Q1 2020




# Trend 2020

**While the development of password Trojans in the first quarter of this year experienced a decline, the development rates of crypto miners, bots and ransomware are seeing a resurgence. As a ratio, the share of Trojans to other malware categories climbed further to 69.63 percent. It is remarkable that compared to the previous year the rate of traditional viruses declined by more than half (from 15.52% to 7.57%) and this malware class is therefore continuing to drastically lose its significance in the arsenal of cybercriminals.**

## TOP 10 Windows malware in 2019

| | | |
|---|---|---|
| 1 | AGENT | 8.19% |
| 2 | VIRLOCK | 5.81% |
| 3 | DINWOD | 5.06% |
| 4 | VIRUT | 3.71% |
| 5 | KRYPTIK | 2.99% |
| 6 | DELF | 2.74% |
| 7 | UPATRE | 2.71% |
| 8 | INJECTOR | 2.59% |
| 9 | SIVIS | 2.46% |
| 10 | WABOT | 1.87% |

AV-TEST
av-test.org

**AV-TEST GmbH regularly evaluates on a bimonthly basis all relevant antivirus solutions for Windows on the market. The latest test results can be downloaded for free on the website under https://www.av-test.org/en/antivirus/.**

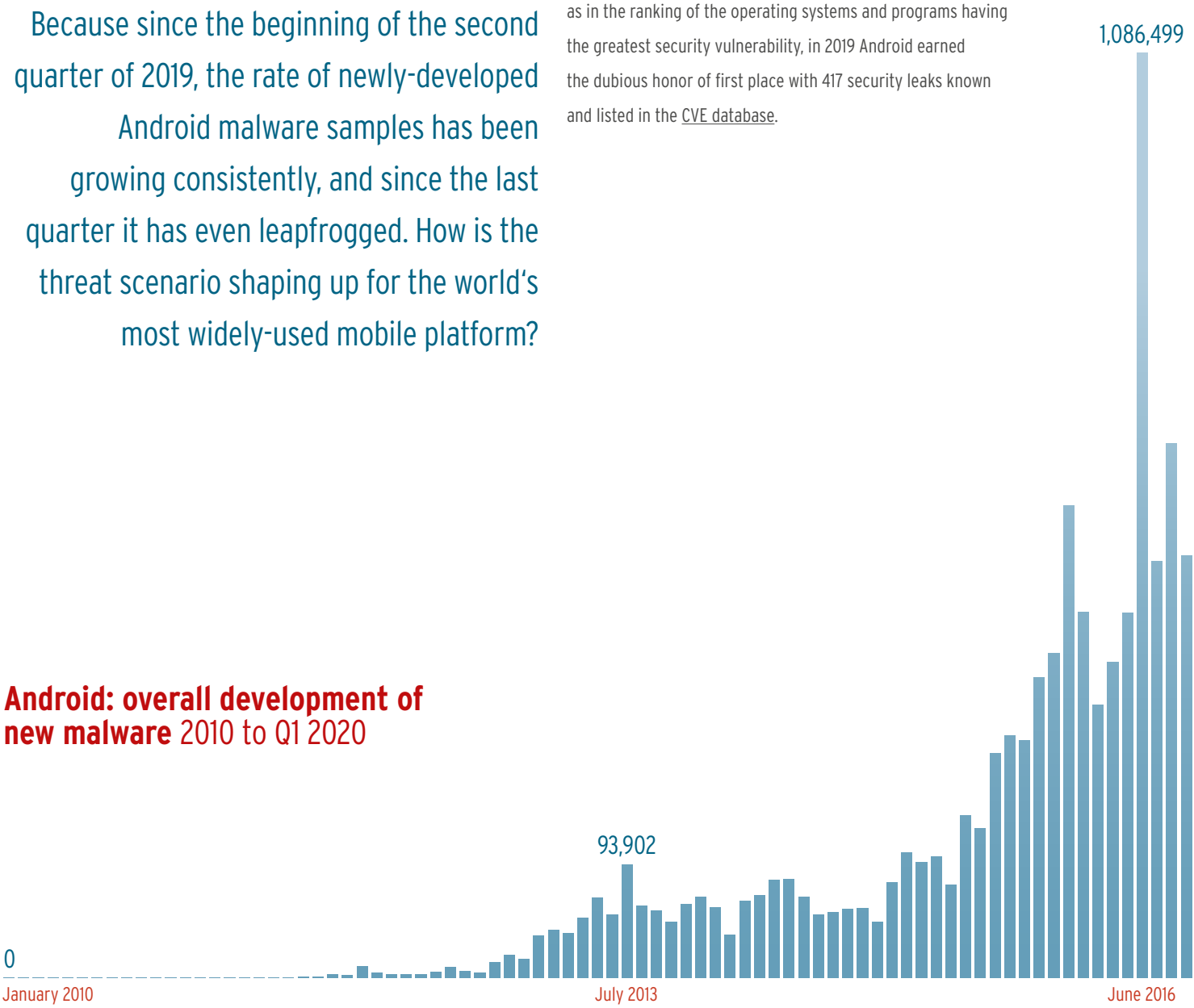
# Security Status ANDROID

Declining malware development rates characterized the year 2018. That was then. Because since the beginning of the second quarter of 2019, the rate of newly-developed Android malware samples has been growing consistently, and since the last quarter it has even leapfrogged. How is the threat scenario shaping up for the world's most widely-used mobile platform?

## Most insecure operating system 2019

One glance at the development curve of new Android malware was comforting both to the owners of the most widely-used operating system for mobile devices and the provider Google over the past four years. Because since the highest level of malware development, recorded in mid-2016, the rate of newly-developed Android malware was clearly retrograde, at the mid-point of last year reaching its lowest point within the past three years. This reassuring trend ended in the middle of last year, however. Since then, the malware curve for Android has experienced a consistent upswing, in the first quarter of this year even exponential growth. This comes as no surprise, as in the ranking of the operating systems and programs having the greatest security vulnerability, in 2019 Android earned the dubious honor of first place with 417 security leaks known and listed in the CVE database.

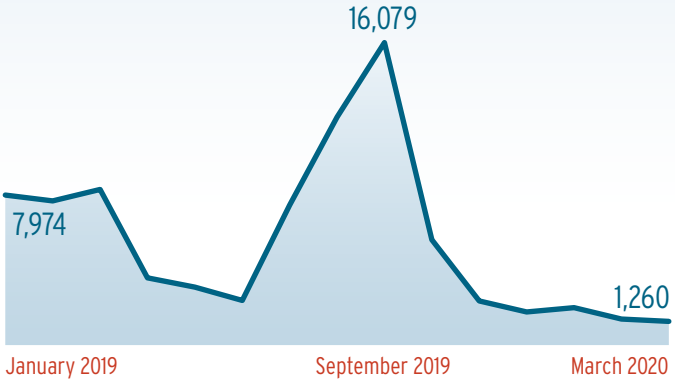
**Android: overall development of new malware** 2010 to Q1 2020



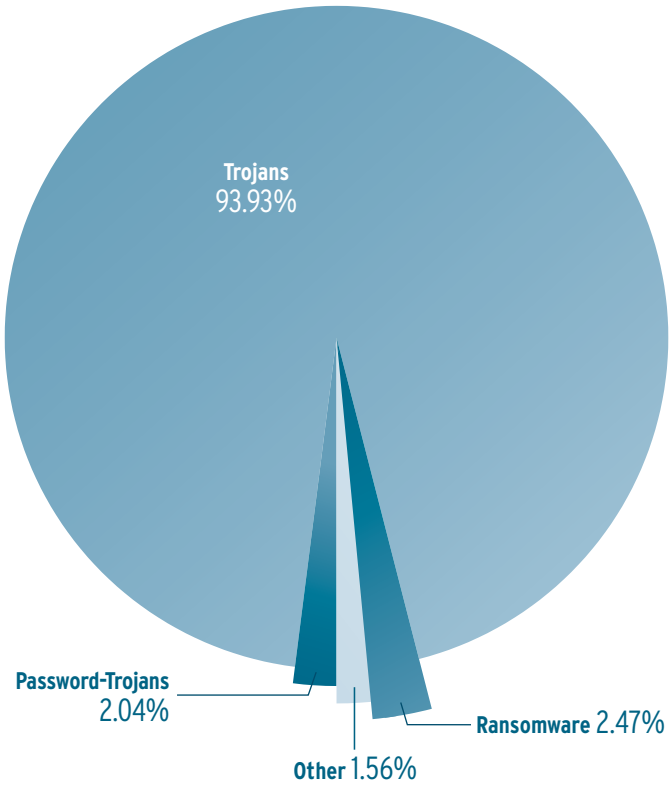
## Over 90% Trojans

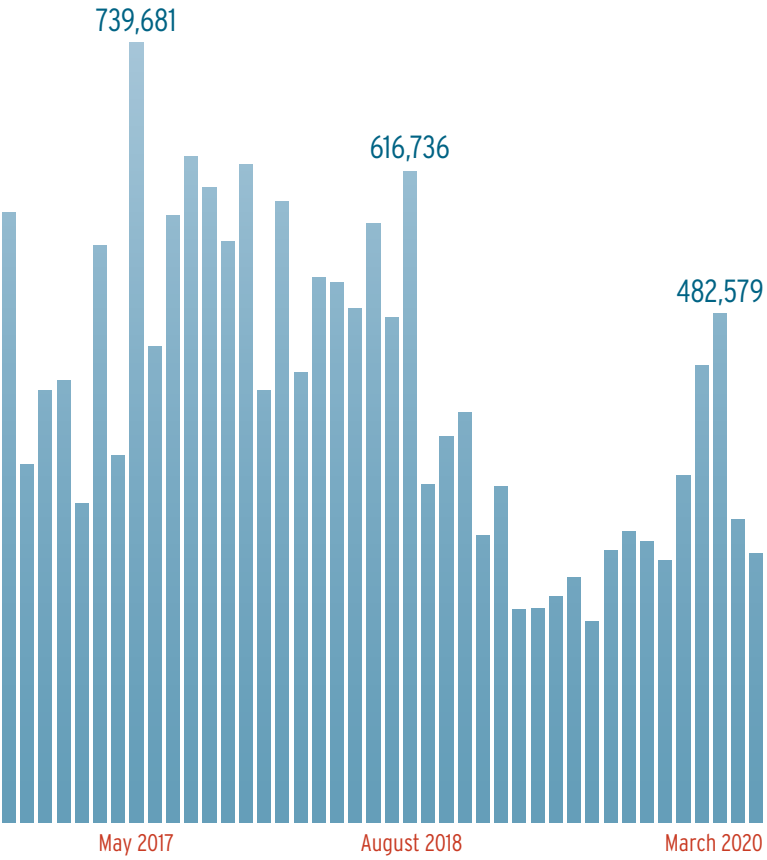
In 2019, Trojans comprised the largest share by far. Virtually 94 percent of the newly-programmed malware code for Android devices is attributable to this malware category. „Hiddad" was a malware sample of this type, which wreaked havoc as an Android Trojan already back in 2018 and last year within the Top 10 Android malware managed to climb from 8th place to 2nd place. Hiddad (18.7%) is an „advertising specialist", which, among other places, hides in apps delivered via Google's Play Store. After the installation of apps infected with Hiddad, the malware skillfully conceals itself by assuming Android-typical file names such as „Google Play Service". It confounds the detection and removal through security apps by deploying super user rights and hiding in Android system folders. On infected user devices, Hiddad displays advertising in certain intervals in full-screen mode and enables its perpetrators to extort cash in this manner.

## Android: development of new ransomware in 2019 + Q1 2020




## Android: distribution of malware in 2019



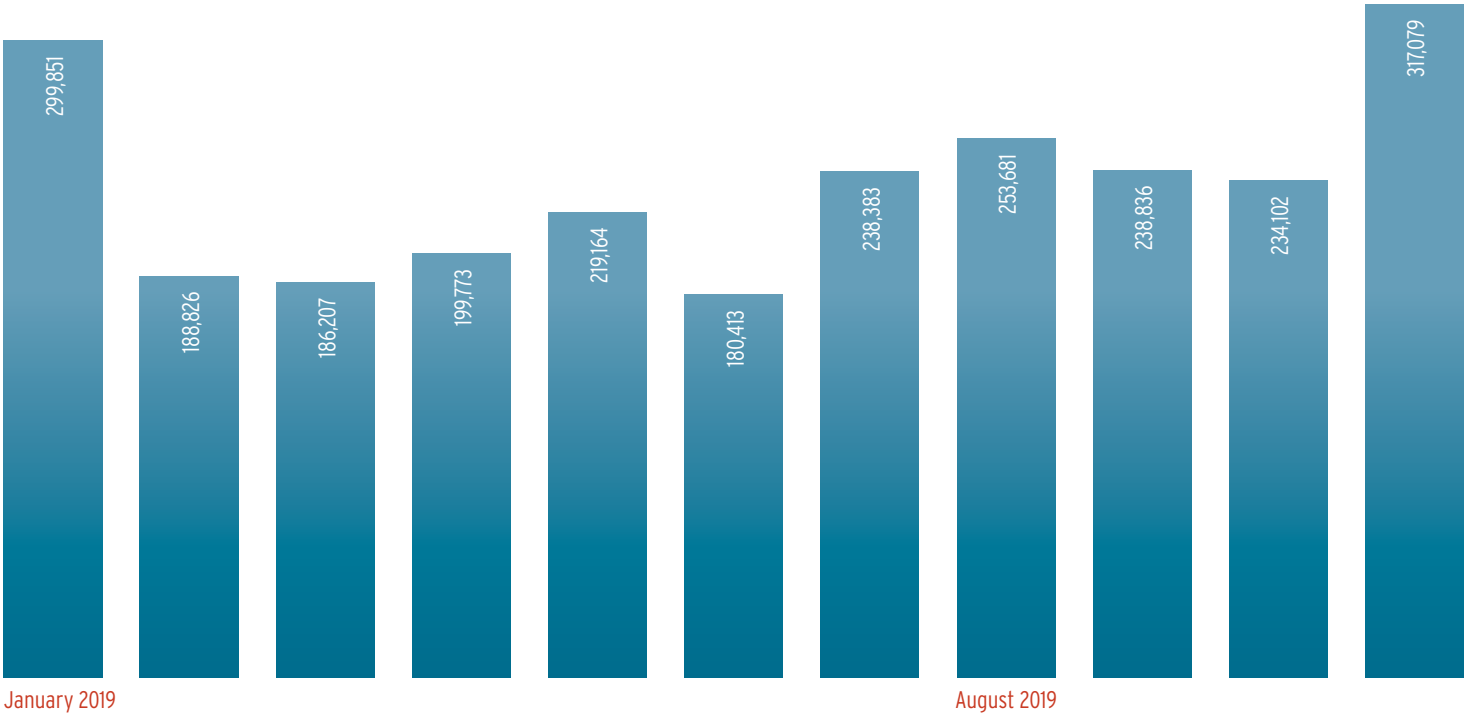
## Android: development of new password-Trojans in 2019 + Q1 2020


The display of unwanted advertising on Android devices is obviously becoming used more and more frequently as a successful monetization strategy. After all, criminals can earn good money with advertising. That is why most malware samples among the Android Top 10 rely on this procedure. The same applies to "Shedun", which in 2019 ranked at Number 3 (9.7%) and was already making money for criminals as far back as 2015.

## Mobile blackmail: Android ransomware

As an additional source of income in 2019, criminal Android specialists deployed ransomware to blackmail device users. Comprising 2.47 percent of the overall share of malware, this malware category is in 2nd place among deployed malware programs. The economic basis for this trend is the fact that mobile devices are now used to the same extent as PCs and notebooks. Add to this the constant availability of the devices as a camera for snapshots, as well as a far lower backup percentage, which means it is extremely seldom that devices blocked by ransomware can be easily restored via a backup to the state prior to the attack. It is worth noting that AV-TEST analysis systems detected over 78,000 newly-programmed ransomware samples for Google's operating system in 2019.

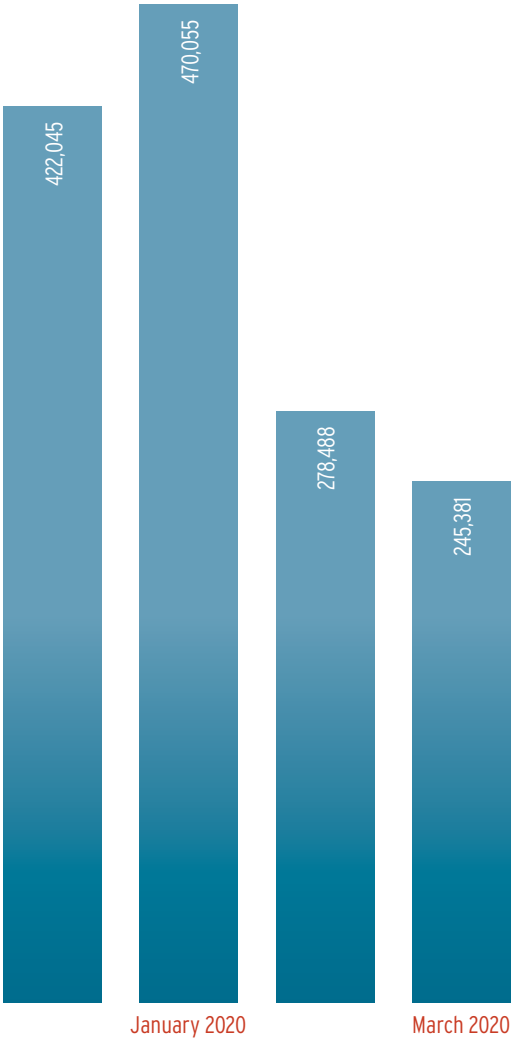
## Android: development of new Trojans in 2019 + Q1 2020



Android Password Trojans ranked third in 2019. This malware is also worthwhile to criminals only because user devices are now used in a large scale for Internet banking and making purchases on online platforms. So skimming off login details and subsequently plundering various user accounts has now become a lucrative target of attack by cyber criminals. Due to the still low penetration of protection apps, there is significantly less urgency to innovate for Android, as opposed to Windows systems. Add to this the free availability of app development tools, the relatively easy access to the Google Play Store, along with the additional opportunity to distribute infected apps via other app stores. And finally, the high market share of Android (approx. 80% worldwide) as well as the disparate, often no longer patched, Android versions still in use, offer a good business climate for criminals.

## TOP 10 Android malware in 2019

| | | |
|---|---|---|
| 1 | AGENT | 26.64% |
| 2 | HIDDAD | 18.71% |
| 3 | SHEDUN | 9.70% |
| 4 | SMSREG | 8.60% |
| 5 | CLICKER | 4.51% |
| 6 | SMSSEND | 3.10% |
| 7 | SMS | 2.45% |
| 8 | FAKEPLAYER | 1.73% |
| 9 | KOLER | 1.60% |
| 10 | LOCKER | 1.49% |




# Trend 2020

**The first quarter of the current year saw a clear decline in mobile ransomware, whose year-on-year share dropped significantly from 2.47 to 0.45 percent. Also in decline is the trend in password Trojans (2.04% to 1.33%). The growth rate of Trojans such as Shedun and Hiddad is exhibiting an increase accordingly. The latter significantly boosted its share in overall malware incidence to over 22 percent. This allows the supposition, at least, that in 2020 cybercriminals are increasingly cashing in on unwanted ads.**

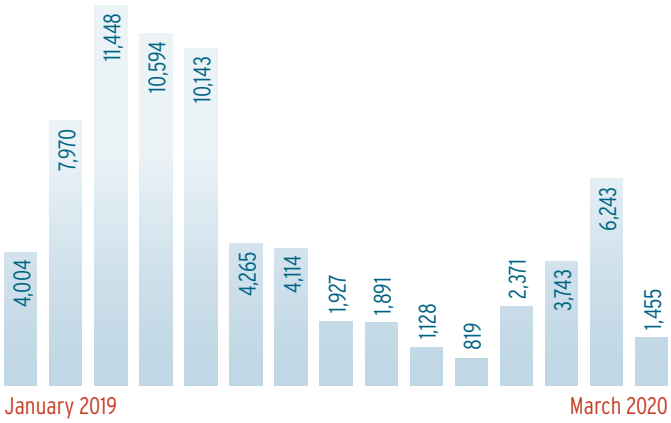
AV-TEST
av-test.org

**AV-TEST GmbH regularly reviews all market-relevant security solutions for Android mobile devices every two months. The latest test results can be downloaded for free on the website under https://www.av-test.org/en/antivirus/mobile-devices/.**

# Security Status MacOS

Good news for Apple users: Overall, the AV-TEST detection systems registered a downward malware growth trend for MacOS systems. However, behind this positive statistic is also the fact that malware has now also become a threat to be taken seriously for Mac and that in 2019 there was a four-year peak in malware development. So this is no reason to let down one's guard, as the analysis of the malware trend for MacOS indicates.

**MacOS: overall development of new malware** in 2019 + Q1 2020



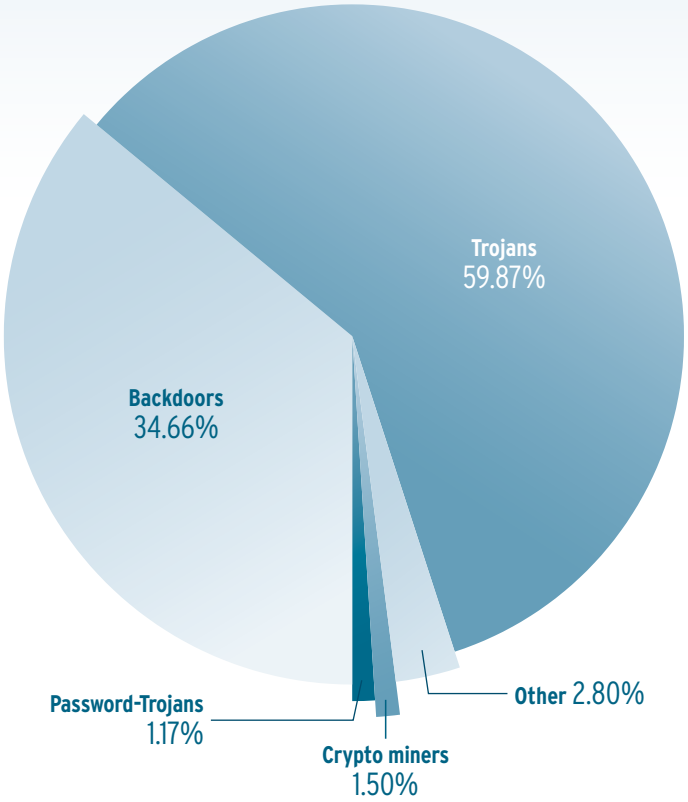

## Old known Trojans and backdoors

The actual good news is overshadowed as soon as attention is focused on malware distribution of last year and the 2019 key indicators are subjected to in-depth analysis. First, you have to scroll down quite a way to find Apple or its current operating system in the list of programs with known security exploits: MacOS X only appears in 44th place. These known vulnerabilities and others were also fully exploited in 2019, however. With only 107, the number of exploits programmed for MacOS last year may appear to be negligible compared to Windows systems. However, they fall on fertile digital soil, which remains hardly protected at all. Because there is still no virus protection running on many Mac systems. Thus we saw a considerable uptick in the trend of exploits in the middle of last year.

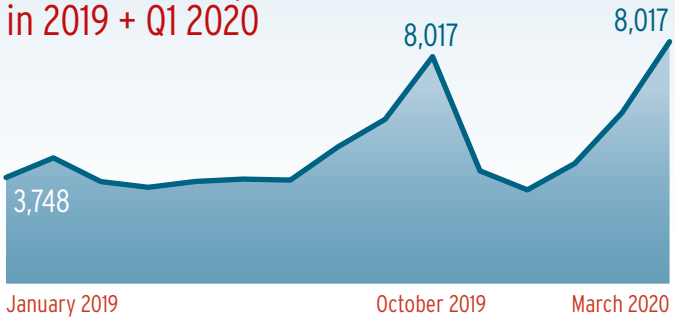
Especially in the first half of last year, the number of available backdoors for MacOS also rose sharply, doubling in quantity. A worrying statistic, especially when considering that apart from Trojans with 34.66 percent, backdoors represent the second-largest group of Apple malware. The percentage of Trojans was 59.87 in 2019. Overall, this means that last year, there were 36,326 Trojans lying in wait for Mac users, a clear and significant threat. Crypto miners (1.5%) and password Trojans (1.17%) also posed a threat to Mac users in 2019, even though in terms of sheer numbers they are clearly underrepresented.

Accordingly, the malware Top 10 are also clearly led by a Trojan and a backdoor, each having an extremely high degree of proliferation. The number 1 position is held by the Trojan "Flashback" (38.36%), a malware sample that has been infecting Mac computers in widely diverse variants for more than 10 years now and often uses a Java exploit for this purpose. If Java is activated in the browser, Flashback enters the computer unnoticed via drive-by infection when the user is visiting a website. Flashback forces infected systems into a remote-controlled C&C server structure and by means of fraudulently obtained administrator rights is capable of subsequently uploading malware components or reading out and secretly forwarding passwords via keyloggers. The fact that even after 10 years, this universal weapon obviously appears to still be a lucrative tool for cybercriminals, does not shed a positive light on the protection state of current Mac computers. As a result, criminals do not have to invest major time and effort to be commercially successful with their malware.

## Distribution of malware under MacOS in 2019




## MacOS: development of new PUA in 2019 + Q1 2020




## MacOS: development of new Trojans in 2019 + Q1 2020


## TOP 10 MacOS malware in 2019

| | | |
|---|---|---|
| 1 | FLASHBACK | 43.33% |
| 2 | MACKONTROL | 39.74% |
| 3 | SHLAYER | 10.90% |
| 4 | AGENT | 1.60% |
| 5 | TINIV | 1.42% |
| 6 | BUNDLORE | 1.13% |
| 7 | APTORDOC | 0.18% |
| 8 | TINYV | 0.16% |
| 9 | ADLOAD | 0.11% |
| 10 | INSTALLCORE | 0.07% |

# Trend 2020

**The trend for Mac malware in the first quarter of this year reveals an exciting development: Whereas the number of newly-developed Trojans has increased dramatically from approx. 60 to almost 90, the bottom has fallen out of the share of new backdoors: Of the 34.66 percent of the previous year, there were a mere 0.3 percent left in the first quarter of 2020. An explanation for this trend could be found in the changes of the security architecture of MacOS. However, this trend required further observation for a clear conclusion. A significant increase is also seen in crypto miners, which at 6.56 percent have increased their share fourfold in the overall volume of malware.**

AV-TEST
av-test.org

**AV-TEST GmbH regularly evaluates all relevant antivirus solutions for Mac on the market. The latest test results can be downloaded for free on the website under https://www.av-test.org/en/antivirus/.**

# Security Status IoT/LINUX

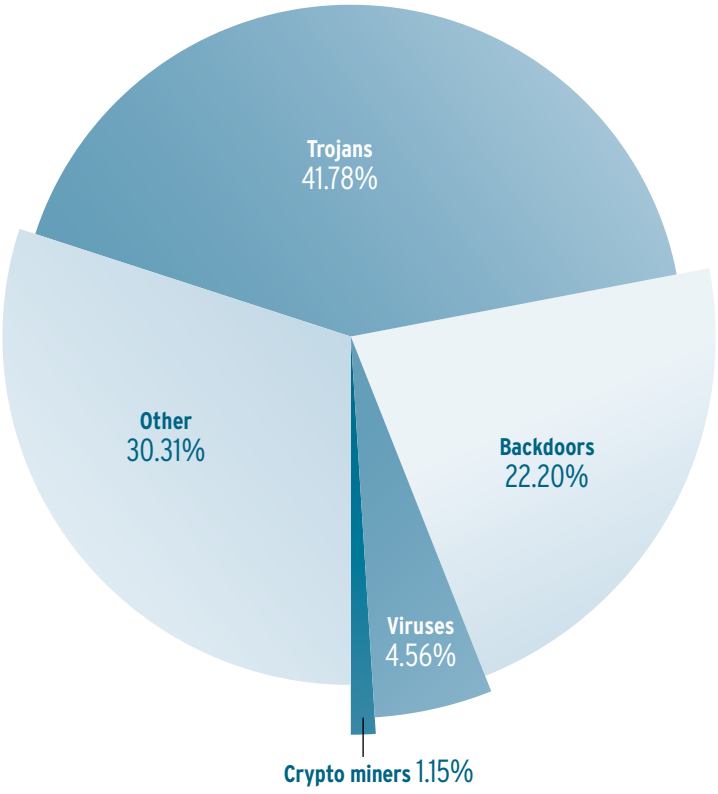
Hardly any IT market sector in recent years experienced growth rates such as those in connection with networked devices (IoT). The consequence for profit-driven cybercriminals is thus unavoidable, and as a result, not only business with legal IoT boomed, but also the shadow economy. But whereas respectable product manufacturers and service providers have to raise awareness and build understanding when it comes to customers' understanding of IT security, criminals can build their business models based on a plethora of poorly protected or completely unprotected IoT systems. And with the increasing penetration of IoT devices in industrial production, medicine, and additional business fields, as well as consumer households, the threat posed by unsecured IoT devices continues to grow.

## IoT malware threats: doubling of the Linux malware rate

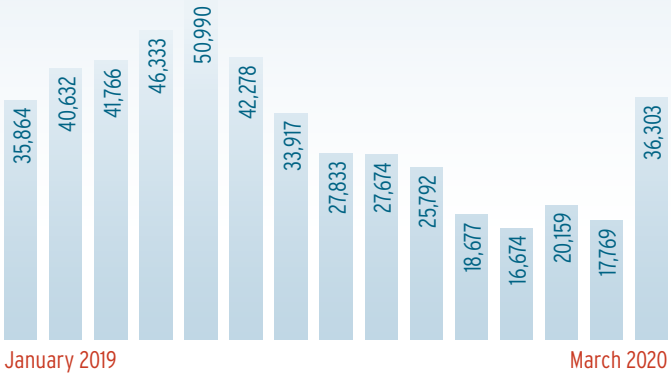
The warnings of the AV-Test Institute in connection with the IoT security situation are anything but new. The 2016 Security Report already dedicated an entire chapter to this topic. And even in the report last year, the warning from the IoT lab was unequivocal: "In the race for lucrative market shares, the IoT industry continues to develop multitudes of Internet-connected products without a sufficient security concept and frequently disregarding even absolute minimum standards of IT security." Hardly anything has changed, however, concerning these facts and the resulting threat scenario.

While there has been little movement in the area of protecting IoT structures since that time, it is a different story on the opposite side. Especially at the beginning of last year, the AV-TEST systems saw exponential growth in malware rates for IoT-typical Linux and Unix versions such as Canonical Ubuntu and others. This trend was already forming at the beginning of the year 2018 in the detection data of the AV-TEST systems; its growth curve

### Distribution of malware under IoT in 2019



## IoT/Linux: overall development of new malware in 2019 + Q1 2020



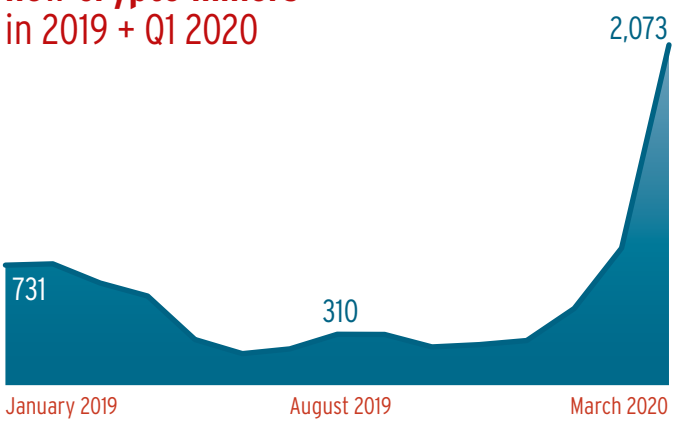

## IoT/Linux: development of new Trojans in 2019 + Q1 2020


in 2019, however, surpassed even the most pessimistic forecasts. Whereas the analysis of new Linux malware samples for 2018 already indicated a total figure of 188,902 newly-programmed malware samples, the AV-TEST systems in 2019 registered 408,430 new samples, more than double.

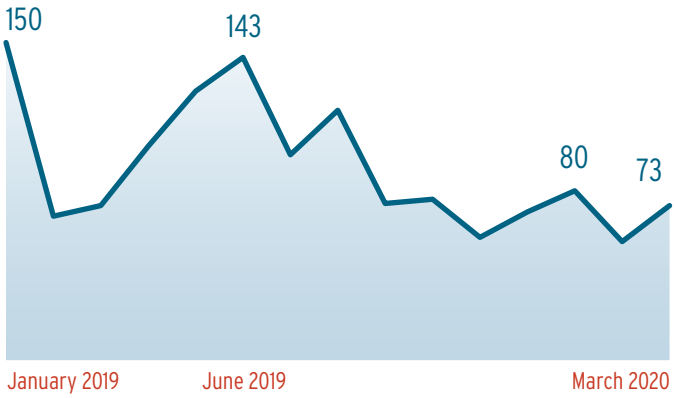
## Still no sign that the lessons from the Mirai attacks have been learned

The lion's share of malware applications for IoT devices on the basis of Linux in 2019 were Trojans with 41.78 percent. Of little surprise and symptomatic for the unsatisfactory response by IoT manufacturers, even towards well-known threats, several variants of the „Mirai" malware sample continue to rank in the Top 10 of IoT malware, representing a whopping 40.84 percent of overall malware incidence. The malware code, originally programmed by kids in September 2016, caused a worldwide attention due to totally haywire distributed denial of service attacks (DDoS) on large online services, including Dyn, Twitter, Spotify, Amazon as well as routers of Telekom Deutschland. Accordingly, surely no manufacturer of IoT devices can claim not to be aware of this threat. In addition, botnets created by the Mirai Trojan continued to proliferate in 2019. New variants of the Mirai malware code work accordingly with new tactics and techniques, and are used, for example, to gain control of digital infrastructures in the industrial IoT sector (IIoT). Thus, cybercriminals were able to defeat poorly protected industrial systems, sabotage them or use their computing power for mining digital currency or staging DDoS attacks.

## IoT/Linux: development of new crypto miners in 2019 + Q1 2020




## IoT/Linux: development of new Exploits in 2019 + Q1 2020



## Crypto miners rely on unprotected IoT infrastructure

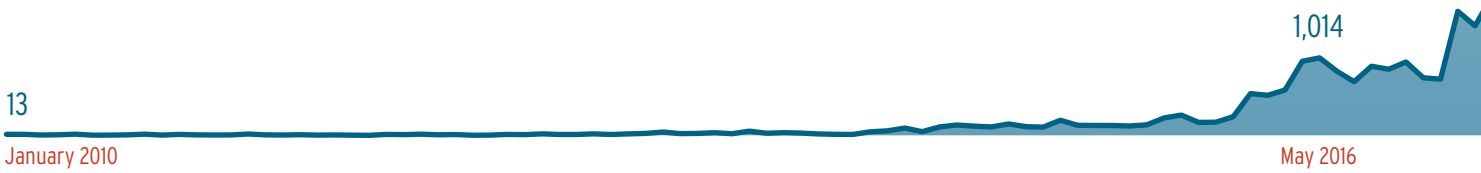
The otherwise virtually unchanged ranking of the most commonly-used IoT malware samples provides a good indication that protection of Internet-based devices is not what it ought to be. Because attackers are still able to get by with new variants of well-known malware codes in achieving economic success.

As a result, the same warnings apply in this Security Report that were already found in the 2016 report: Trojans such as Gafgyt (19.04%), Hajime and Tsunami continue to represent a serious threat to the IoT infrastructure. Yet increasingly, malware codes for direct monetization of third-party resources are joining the top ranks of IoT malware. In 2019, for example, two crypto miners already ranked among the Top 10 for IoT.

One of them, Coinhive, is a malware code which at least originally had a semi-legal scope of application. The JavaScript code was originally used for the browser-based calculation of the cryptocurrency Monero and was included by website providers in their online range as a payment option for online services, for example. While the controversial provider of the script shut down its business in March last year, criminals are apparently continuing to use the available Java code to enrich themselves at the expense of unwitting IoT users. AV-TEST discovered a total of 4,697 new samples of this software category in 2019, and thus an increase of 46 percent compared to the previous year's figures. So there is some evidence that the deployment of third-party resources in the IoT sector is paying off for criminals. "Business models" used on other platforms

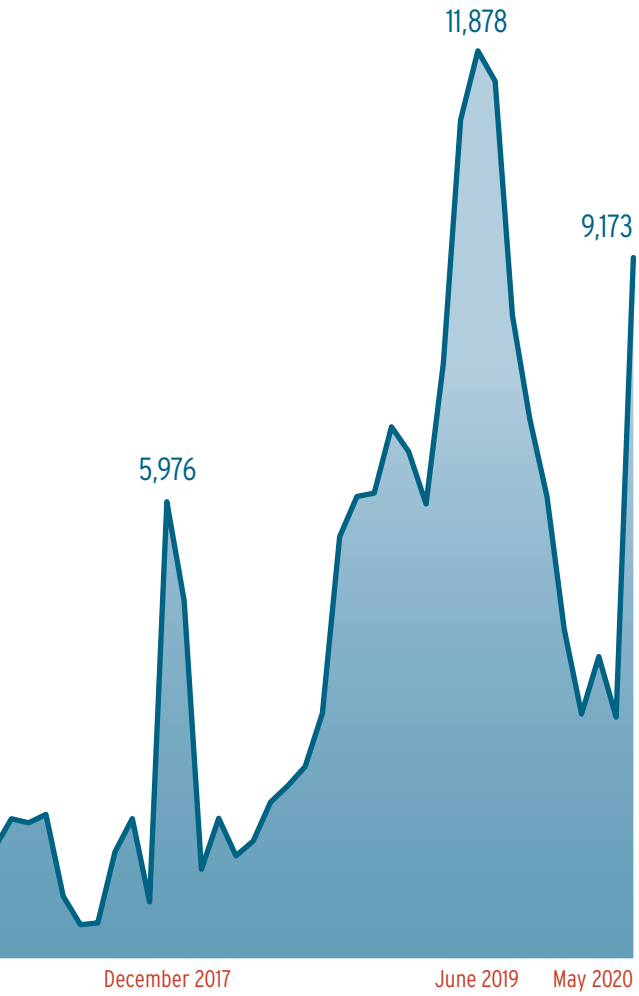
such as digital blackmail through the blocking of devices, are indeed currently being tried out, but thus far they have not become a dominant practice. This is evidenced by the as yet limited penetration of detected IoT ransomware, which numbered exactly 56 samples in 2019. But as IoT devices become increasingly commonplace in industrial manufacturing and medical care, in the foreseeable future, digital extortion rackets through threat of sabotage of IoT could also become a bitter reality. It would behoove device manufacturers and service providers of both sectors to become aware of this danger and to meet it head on.

**IoT/Linux:**
**development of new backdoors**
in 2010 to Q1 2020



## TOP 10
## IoT malware in 2019

| | | |
|---|---|---|
| 1 | MIRAI | 40.84% |
| 2 | GAFGYT | 15.04% |
| 3 | VIT | 4.36% |
| 4 | AGENT | 1.32% |
| 5 | HAJIME | 0.88% |
| 6 | TSUNAMI | 0.84% |
| 7 | COINHIVE | 0.70% |
| 8 | BITCOINMINER | 0.62% |
| 9 | DOFLOO | 0.53% |
| 10 | SHELLDL | 0.40% |




# Trend 2020

**The IoT detection figures in the first quarter of the current year already provide some clues with respect to anticipated malware trends for networked devices. Thus, the rate of Trojans used to infect IoT infrastructure increased considerably from just under 40 to over 65 percent.**

**And the increase in the rate of newly-developed crypto miners corresponds to the previous analysis. These malware samples increased their share of overall malware incidence compared to last year from 1.15 to 4.55 percent.**

## AV-ATLAS supports suppliers with real-time data on IoT attacks

With the launch of the IoT section in the AV-ATLAS Threat Intelligence Platform (av-atlas.org), the AV-Test Institute now also offers real-time threat analyses of virtually all relevant IoT platforms, to guide users and to support manufacturers. The website, available free of charge, offers a query capability both for information on past and current attacks, including logins used, originating servers, type of attacks and the commands used in the process, along with the malware deployed and its precise analysis.

AV-TEST
av-test.org

**AV-TEST GmbH continuously monitors and certifies market-relevant smart home products and IoT solutions. The latest test results can be downloaded for free from the IoT security blog at https://www.iot-tests.org/.**

# Test Statistics

With analysis systems developed in-house and sophisticated testing procedures, AV-TEST guarantees independent tests for IT security products and has thus been the leading Institute in the field of security research and product certification for over 16 years.

## Millions of malware samples for your security

The systems at AV-TEST scan more than 3 million files per day, including a unique multi-virus scanning system for malware analysis for the Windows and Android platforms. Based on these results, a phalanx consisting of over 25 individual virus scanners provides fully automatic pattern detection and analyzes and classifies malware in this manner. The system automatically records all proactive detections as well as response times of respective manufacturers to new threats. Thus, one of the world's largest databases for malware programs is constantly expanding and keeping up-to-date. Its data volume has been growing continuously for more than 16 years on over 40 servers with storage capacity of over 2,500 TB. On the publication date of this annual report, the AV-TEST database contained roughly 700 million malware samples for Windows and more than 28 million malware samples for Android!

## AV-TEST seal of approval for antivirus products



## AV-TEST seal of approval for IoT products



For targeted malware analysis, AV-TEST relies on systems conceived and developed in-house. These analysis systems enable a controlled launch of potential malware codes on clean test systems and record the resulting system changes, as well as any network traffic generated. The analyzed malware is then classified and categorized for further processing based on the system changes observed. Using this method, the AV-TEST systems record and test 1,000,000 spam messages, 500,000 URLs, 500,000 potentially harmful files, 100,000 innocuous Windows files as well as 30,000 Android apps every day.

Among other purposes, the data recorded by the AV-TEST systems are deployed for the monthly tests of security products for Windows. In this manner, in 2019 over 365 product tests alone were run for consumer and corporate products. As a result, 84,477 malware attacks and 8,999,133 individual data records for false positive tests were deployed and evaluated per product. Throughout the year 2019, this amounted to 4,368,921,256 records evaluated by the test experts. In the monthly Android tests carried out throughout the year, the testers evaluated over 153 individual products. In doing so, each evaluated security app had to defend against 51,548 special Android malware samples. As a counter sample, the experts also recorded over 22,825 scans of secure apps per product, in order to evaluate the vulnerability towards false alarms. That is why in lab tests of security products for Android, a total of 7,886,844 scan procedures were analyzed and reproducibly evaluated. 4,103,154 scans hereby involved the specially-developed Android security cluster, which enables parallel real-time tests of Android security solutions.

**1,000,000** SPAM-MESSAGES

**3 million** FILES PER DAY

**4,368,921,256** EVALUATED RECORDS IN 2019

**500,000** URLs

**40** SERVERS

**2,500** TERABYTE

# About the AV-TEST Institute

The AV-TEST GmbH is the independent research institute for IT security from Germany. For more than 15 years, the security experts from Magdeburg have guaranteed quality-assuring comparison and individual tests of virtually all internationally relevant IT security products. In this, the institute operates with absolute transparency and regularly makes its latest tests and current research findings available to the public free of charge on its website. By doing so, AV-TEST helps manufacturers towards product optimization, supports members of the media in publications and provides advice to users in product selection. Moreover, the institute assists industry associations, companies, and government institutions on issues of IT security and develops security concepts for them.

Over 30 select security specialists, one of the largest collections of digital malware samples in the world, its own research department, as well as intensive collaboration with other scientific institutions guarantee tests on an internationally recognized level and at the current state of the art. AV-TEST utilizes analysis systems developed in-house for its tests, thus guaranteeing test results uninfluenced by third parties and reproducible at all times for all standard operating systems and platforms.

Thanks to many years of expertise, intensive research and laboratory conditions kept up-to-date, AV-TEST guarantees the highest quality standards of tested and certified IT security products. In addition to traditional virus research, AV-TEST is also active in the fields of security of IoT and eHealth products, applications for mobile devices, as well as in the field of data security of applications and services.

**You can find additional information on our website, or simply get in touch with us directly at +49 391 6075460.**

**AV-TEST GmbH | Klewitzstrasse 7 | 39112 Magdeburg, Germany**