FACTS AND FIGURES

SECURITY REPORT 2018/19

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

The AV-TEST Security Report

With the detection of the 900 millionth malware sample, the development of malware programs broke a sound barrier in mid-May 2019. At the end of 2018, the number of programs detected by AV-TEST's analysis systems was still around 856.62 million. In 2018, this marks a reversal of the downward trend in malware development noticeable since 2015, as already forecast in the analysis of the last security report.

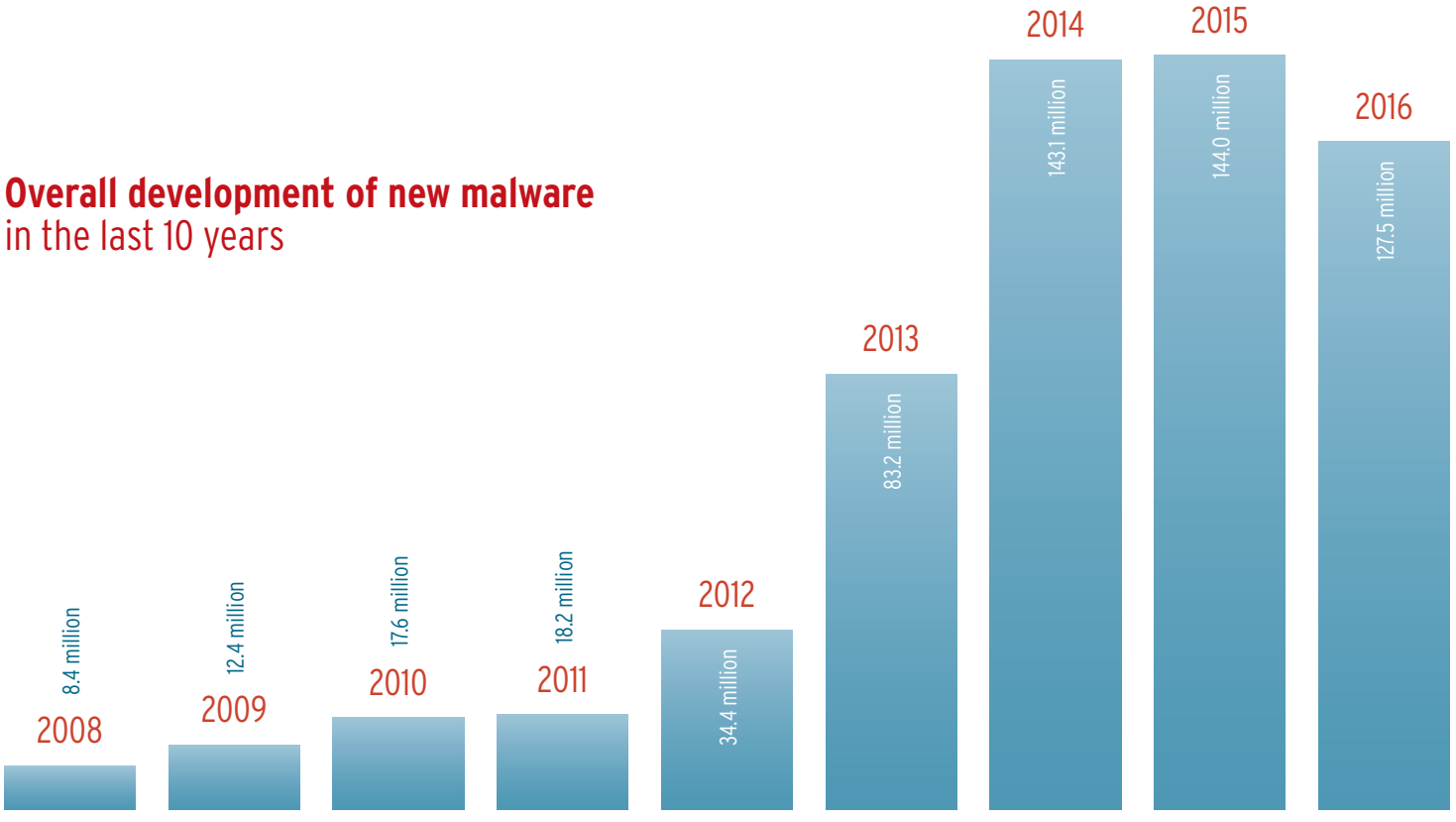
Increasing attacks on macOS and IoT

While Windows systems continue to be the focus of industrially organized criminal groups, the number of malware programs for Apple's operating system macOS has almost tripled. Beyond the mass proliferation of malware, worrisome trends have become apparent in the analysis of the statistics of last year, as well as the first quarter of 2019. Thus, for example, the digitalization of industrial operational technology (OT) and IoT systems without sufficient protection offers rapidly growing potential for targeted attacks and a wide open flank, as demonstrated by the security report from page 19.

Increasing malware rate and peak of security gaps

With the increase in new malware developments in 2018, the quantitative threat scenario is mounting: Whereas in 2017, protection programs still had to fend off an average of 3.9 malware programs per second, by 2018 that number had already increased to 4.4 per second and thus 376,639 new malware samples per day!

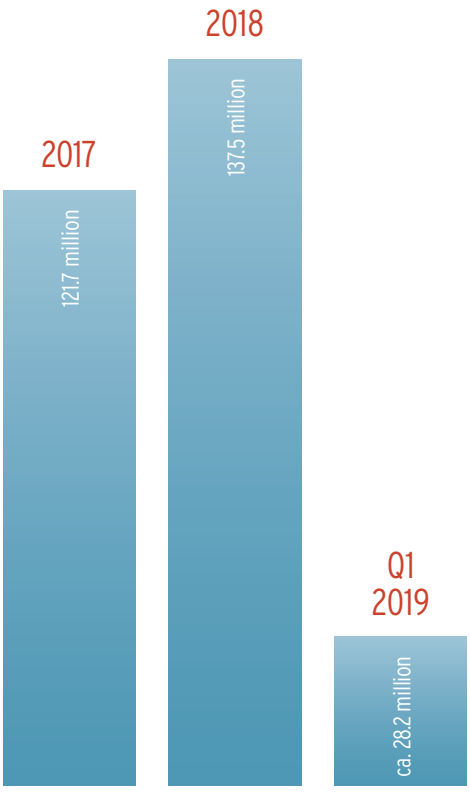
Overall development of new malware
in the last 10 years



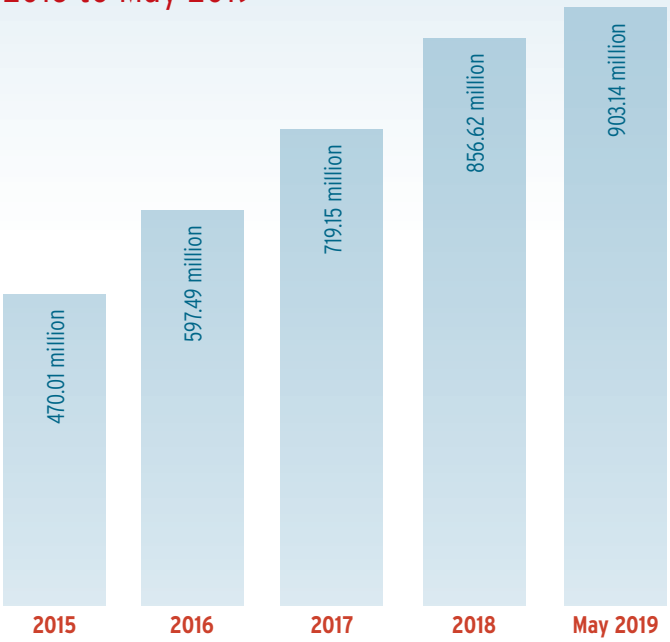
The hardware worst-case scenario: Meltdown and Spectre

Probably among the most severe security leaks are the „Meltdown" (CVE-2017-5754) and „Spectre" (CVE-2017-5715 ff) hardware leaks published at the beginning of January, which defeated the security architecture of microprocessors at the hardware level. This enabled attackers to read out sensitive memory content and thus obtain passwords and other highly sensitive content from memory areas of programs and operating systems that were actually not accessible. This affected all devices with CPUs by the manufacturers Intel, ARM and AMD – this means virtually all PCs, servers and smartphones, networked consumer products, right down to industrial equipment.

Shortly after both hardware leaks were made public in January, the analysis systems of the AV-Test Institute noticed a sharp uptick in possible malware codes for the vulnerabilities. These malware samples were based on the known proof-of-concept code and targeted mainly Windows, macOS and Linux. They mostly involved test samples, however, which manufacturers of affected products and the suppliers of security solutions used to evaluate product safety or for patching their systems.



Total malware
2015 to May 2019



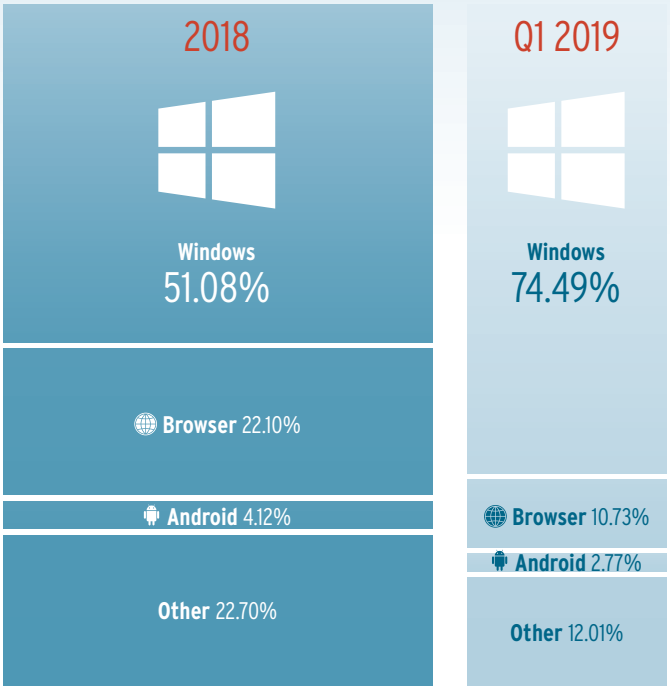
Because chip and device producers, not to mention software manufacturers, were already informed about the discovery of the vulnerabilities in June 2017, at least relevant comprehensive patch libraries were already available at least from leading manufacturers shortly before February 2018. However, this still did not apply to all vulnerable devices. And because the availability of security updates does not automatically mean that they will also be installed, it's safe to assume that the Meltdown and Spectre gaps are continuing to be used from a large number of systems for the proliferation of malware code.

The serious hardware gaps were joined in 2018 by „Foreshadow" (CVE-2018-3620 ff), which also affected processors from Intel and AMD and enabled the infiltration of malware. And in 2019 as well, potential attacks on hardware gaps such as „ZombieLoad" (CVE-2018-12130) continue to keep manufacturers, criminals and security experts on their toes.

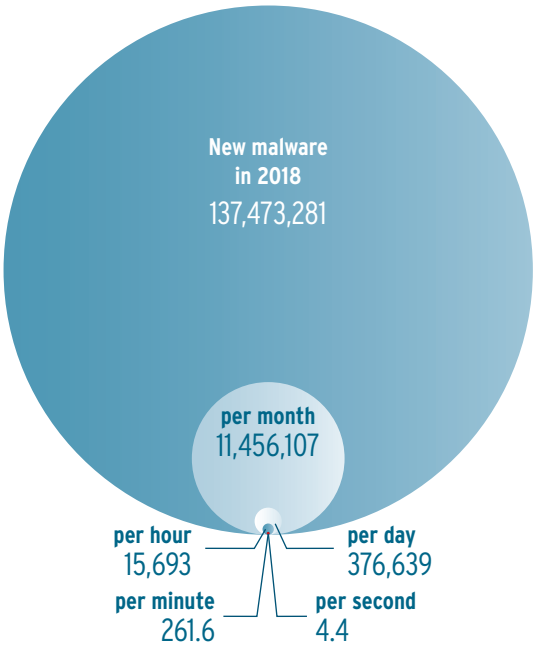
Windows remains the main target of attacks

Compared to the previous year, the conventional malware industry continues to concentrate on Windows systems. More than half (51.08 percent) of all newly developed malware programs in 2018 targeted the world's most widely used operating system from Redmond. Due to the continuously increasing defensive performance from protection programs, not only for consumer users but also in the field of corporate computing, cybercriminals apparently felt it necessary to crank out new malware codes at a higher rate. The significantly improved detection performance of the internal Windows security module, Microsoft Defender, documented in the regular tests by AV-Test Institute, also contributed to this trend. Out of the necessity of continuing to be commercially successful with Windows malware, the malware industry had no choice but to continuously optimize its products – an additional clue towards explaining the growing percentage of malware. This report contains detailed evaluations on Windows malware from page 6.

Distribution of malware



Average malware threat in 2018

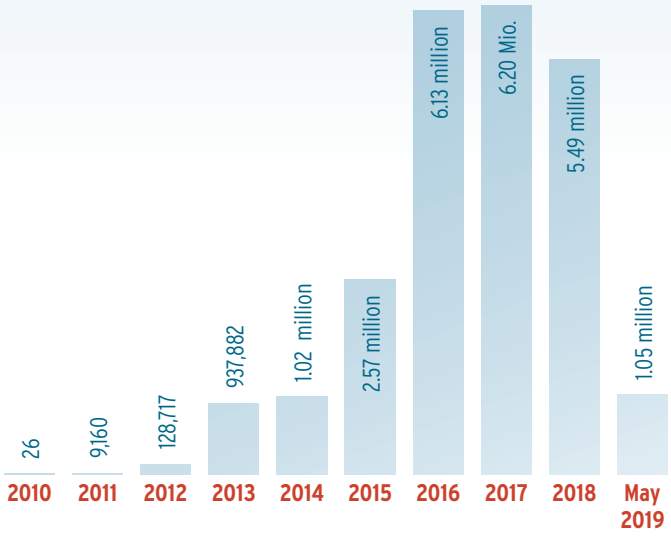


AV-TEST optimizes malware evaluation

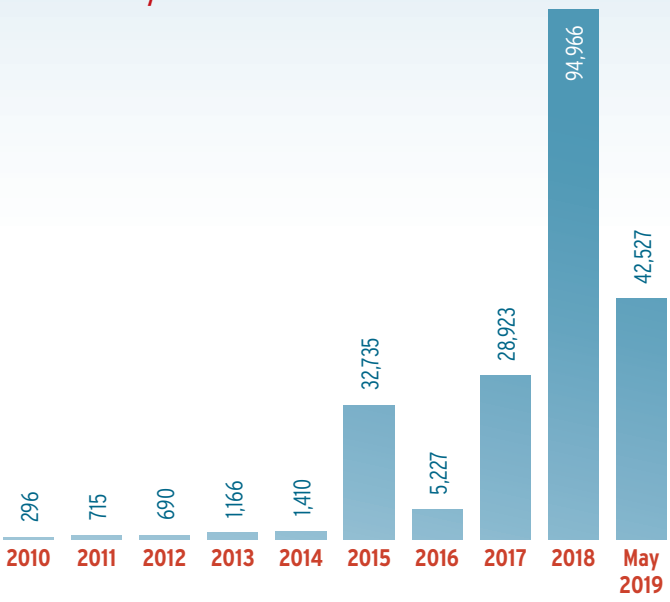
In comparison to malware evaluation in previous security reports, the AV-Test Institute has taken a much more deliberate approach to the classification of malware among various platforms and operating systems, and has done so even retroactively. Thanks to more precise recording, the malware statistics for Windows systems in particular deviate from previous security reports. This is due, for example, to the recording of browser malware, which was previously counted under Windows systems or under the category of „Other".

Dedicated information on the slightly improving trend in the malware situation for Android, the world's most widely used operating system for mobile devices, is available in this report from page 12.

Development of malware under Android
2010 - May 2019



Development of malware under macOS
2010 - May 2019



macOS malware almost tripled

Whereas the rate of new malware developments for Android, the largest mobile operating system, experienced a slight lull in 2018 compared to the previous year, the sample numbers of new malware for macOS nearly tripled. In terms of percentages, the share of Mac malware, with 0.15% of the overall total of newly developed malware programs, was negligibly low. It should not be forgotten, however, that the 94,966 new malware samples in the year 2018 face off against a massive number of Apple devices without sufficient virus protection. Because just as with mobile devices under Android, with respect to the installation rate of effective protection programs on Apple computers, there is lots of room for improvement. More precise information on the malware situation for Apple devices is available from page 16.

Business models for criminals: crypto miners versus ransomware

In addition to the classic malware success model consisting of theft of sensitive data, as well as interception and abuse of bank and account information, cybercriminals also relied on new business fields: blackmail through encryption of relevant data and systems of the victims by means of ransomware, as well as the mining of crypto currency by means of secret exportation of third-party computing power and IT infrastructure by crypto miners. Whereas the sample number of ransomware recorded by AV-TEST was trending downwards, exactly the opposite was the case for crypto miners last year. This report illuminates how these statistics look exactly and what insights they offer from page 24.

Security Status WINDOWS

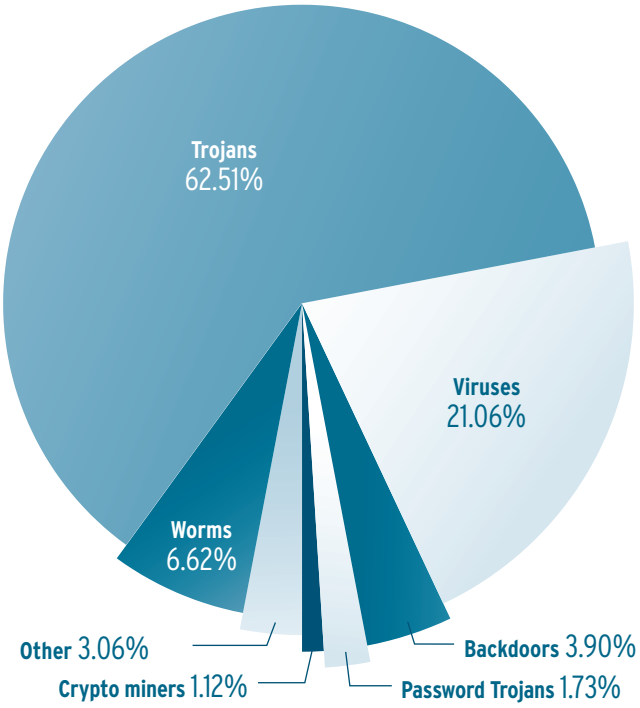
Monocultures often suffer under increased infestation. Thus, it should come as no surprise that Windows, as the most widely used operating system in the world, has always by far drawn the most malware attacks. The prospect of cashing in with Windows malware is far more likely than in the case of attacks on other operating systems. Thus, in 2018, more than half of all malware programs, exactly 51.08%, targeted the basic software of most private PCs and corporate computers.

Overall moderate malware trend

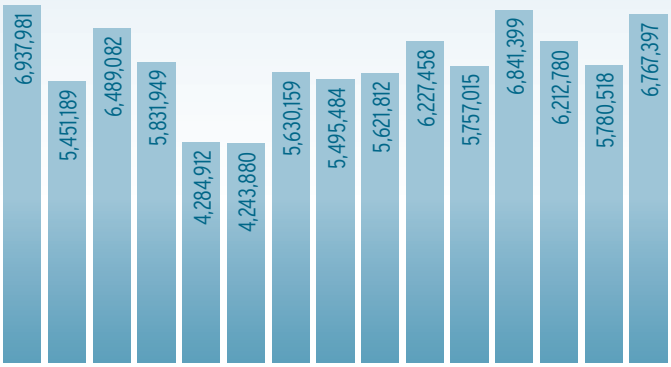
Right at the beginning of the year, in January, to be precise, the detection systems at the AV-TEST Institute reported the highest level of newly developed Windows malware for the year 2018. With just under 7 million new malware programs in that month alone, last year started out as anything but reassuring for users of Windows systems. AV-TEST systems last measured an even greater malware surge, well over 10 million new malware samples in one month, in June 2015.

Yet the development of new windows malware also turned out to be subject to strong fluctuations in 2018. And thus the development rate of new windows malware samples ebbed away toward the middle of the year. In the months of May and June, the detected values drastically declined only to just over four million new samples per month. Only to continually increase again from that point on, however.

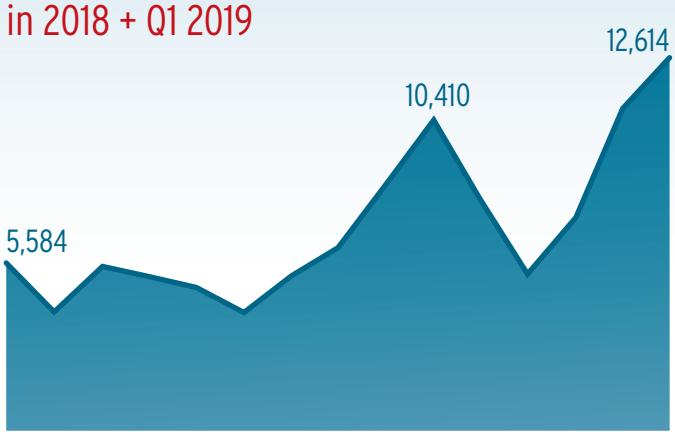
Distribution of malware under Windows in 2018



Windows: development of new malware in 2018 + Q1 2019



Windows: development of new exploits in 2018 + Q1 2019



Massive increase of exploitable Windows gaps

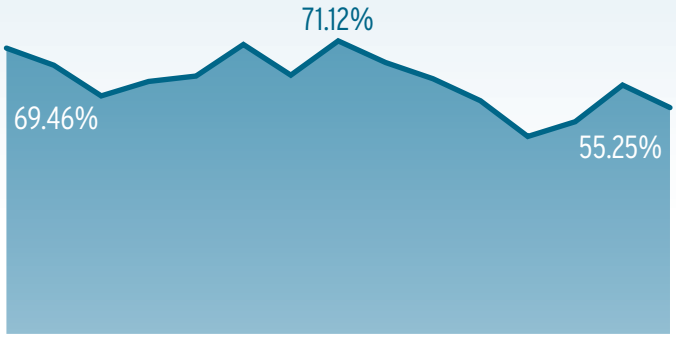
If one compares what throughout 2018 was indeed a constant, yet moderately increasing number of Windows malware samples to the available exploitable vulnerabilities in Windows programs, a more precise image emerges. Because compared to the previous years, the number of Windows exploits grew sharply. Especially from the middle to the end of the previous year, their rate of increase almost grew exponentially. In October 2018, the number of exploits for Windows systems reached a critical high mark of 10,000 samples per month, but by the end of the year, declined again to practically half. That is why overall, with respect to the massive increase of exploits, the development trend of new malware turned out to be somewhat moderate for the entire year of 2018.

Trojans remain threat No. 1

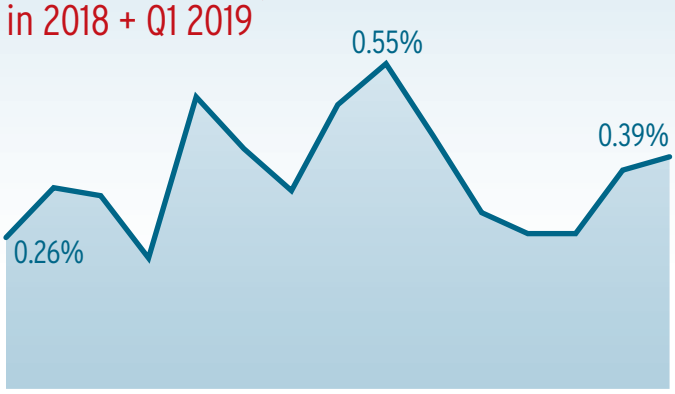
Once again in 2018, Trojans turned out to be the first tool of choice by cybercriminals by a large margin before all other classes of malware. It is no wonder, as Trojans, both in terms of functional variety and opportunities to distribute them, are unsurpassed by any other class of malware. Last year, these universal tools from cybercriminals comprised nearly 2/3 of all malware programs developed for Windows (62.51%). By a wide margin, they are followed by classic computer viruses (21.06%) and Internet worms in a distant third place (6.62%).

The analysis systems from AV-TEST recorded the largest share of the Trojan surge as malware code under the designation of „Agent". In this, despite a similar malware code, it involves larger variance of classic Trojans with a different scope of functions. The „Agent" category designation thus subsumes generic Trojan detections without attributing them to a particular Trojan family. It generally involves standard Trojans with the task of infecting a system in different ways and subsequently reloading malware code selected by the attacker. Hijacked systems can thus be abused in various ways over the long-term.

Windows: development of new Trojans in 2018 + Q1 2019



Windows: development of new ransomware in 2018 + Q1 2019



At the beginning of the year 2018, malware code loaded retroactively by Trojans with great certainty involved password Trojans, ransomware and crypto miners. Because all three classes of malware subsumed under the category of Trojans were conspicuous at the beginning of the year due to unusual proliferation statistics. In the same period, comprehensive campaigns were detected for mass distribution of infected spam mails around the globe. The point of origin usually involved large botnets such as „SmokeLoader". During the relevant time period, its infected spam messages frequently contained infected Microsoft Word documents with manipulated macros, which enabled attackers to gain remote control over infected systems, in addition to retroactively loading various malware functions. Virtually at the same time, criminal operators of the „SmokeLoader" botnet managed to vastly expand their network of hijacked computers through variously devised measures. One of these measures involved clever psychological use of the public disclosure of the hardware vulnerabilities Meltdown und Spectre. By means of well-placed websites in search engines, the criminals, among other means, offered fake security updates for download, the installation of which in turn gave them control over the computers of concerned users.

2018: Are crypto miners supplanting ransomware?

In the last security report, not least due to the measured values of the first quarter for 2018, AV-TEST announced the „age of the crypto miners" and was thus correct. The forecasts based on ransomware measurements of the first quarter also turned out to be true. And thus digital blackmail by means of ransomware, the good news for 2018, has been on a downward trend since the beginning of the year. On the one hand, the anonymity of digital currencies ensures criminals a high level of security in bilking their victims, and the use of ransomware requires far less overhead compared to the business with other malware programs. On the other hand, the business model lives and dies with the willingness of the involuntary customers to pay. And that is precisely what appears to be declining in private households. As a result, a stagnating new development rate of ransomware samples can be witnessed, which has leveled off at approx. 20,000 samples per month.

Windows: development of new crypto miners in 2018 + Q1 2019

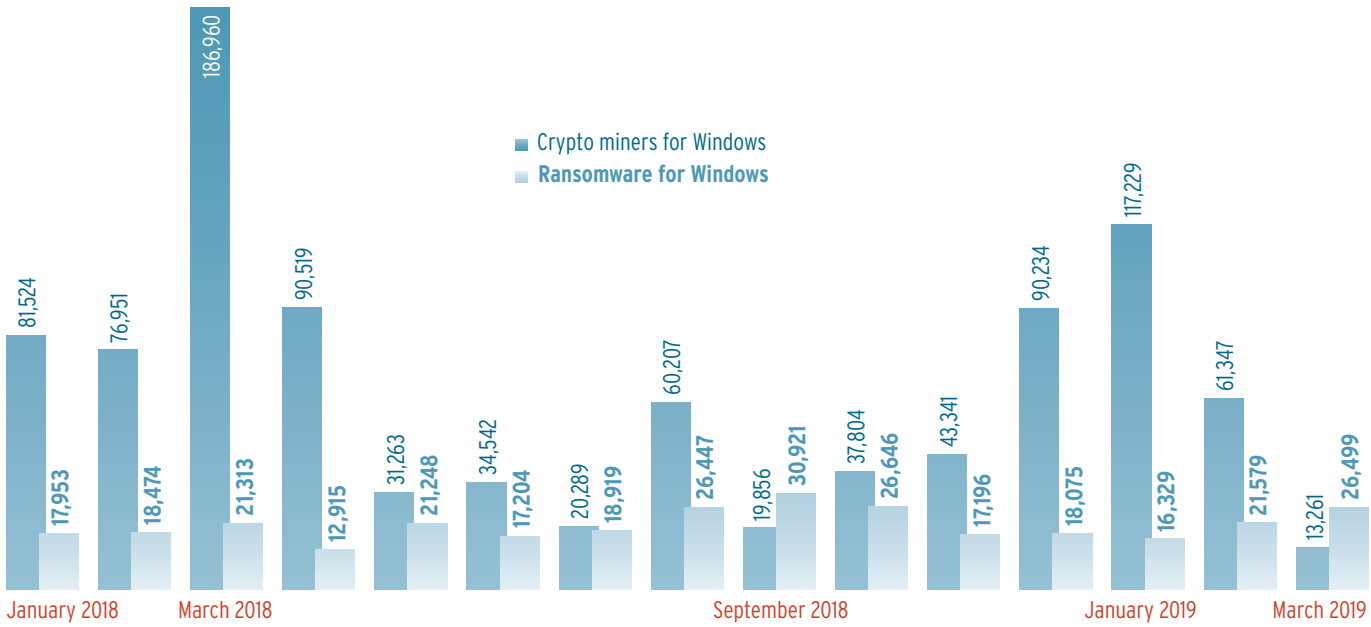
In addition to detecting ransomware samples, as well as their proliferation pathways via infected websites or malware emails, the AV-TEST Institute deploys a tool developed in-house for in the analysis of the effectiveness of cyber blackmail. It monitors the bitcoin wallets specified in blackmailer emails and in ransomware. This allows the experts from Magdeburg not only an overview of the blackmail campaigns currently underway, as well as those completed, but also the proof of received payments into the bitcoin accounts used by cybercriminals.

Crypto miners in the development phase

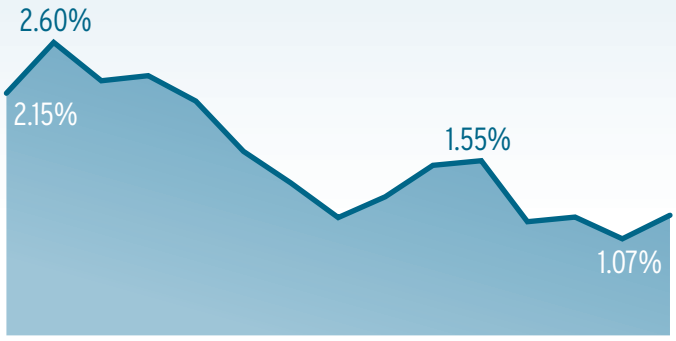
Contrary to the ransomware trend, the use of crypto miners increased sharply in 2018 as expected, yet was subject to severe fluctuations. The proliferation of new malware samples for the mining of digital currencies found its high point in the first quarter of last year. The detection systems of AV-TEST recorded over 180,000 samples in March. From this point on, all the way into July, the detected sample numbers slipped sharply. Overall, the review of 2018 indicates three peaks in the proliferation of new crypto miner samples. Because in August, as well as in December, the measurements peaked again, albeit not as severely as before in January. In August, exactly 60,207 samples were in fact measured. In December, that number shot up to 90,234 detected samples.

The volatile appearance of crypto miner samples would seem to suggest that developers were still testing their products or, in times when the sample numbers increased, were forced to adapt to new conditions, e.g. through increased detection by security programs. The business with crypto miners is only worthwhile for criminals if by means of the largest number of infected systems possible, for the longest period of time, sufficient computing power is available to work in the blockchain. Accordingly, the aim of attackers is to

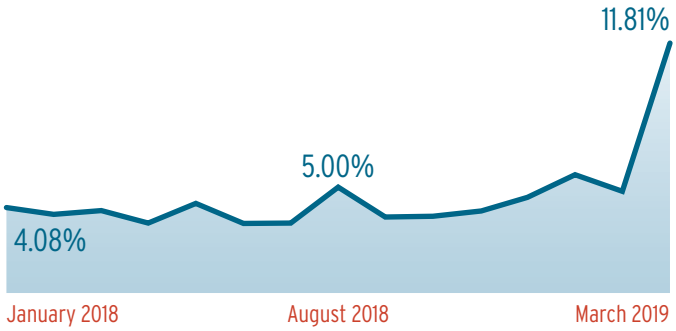
Windows: development of new crypto miners compared to ransomware in 2018 + Q1 2019



Windows: development of new password Trojans in 2018 + Q1 2019



Windows: development of new backdoors in 2018 + Q1 2019



be able to use the resources of third-party systems discreetly for the longest period of time possible. With first-generation samples, it would hardly seem possible to elude the scans of the latest security programs. Accordingly, criminals have to continuously enhance their crypto miners if they wish to be successful with this malware over the long-term. The three significant spikes last year in the detection statistics could suggest such development stages. This report dedicates a full chapter to crypto miners from page 24.

Password Trojans nosediving

With password Trojans, criminals increasingly exploited access data to online accounts of their victims in the first quarter of 2018. From January to April, the high proliferation statistics of this Trojan family, with numbers well over 130,000 new samples per month, remained quite constant. Yet towards midyear, the numbers declined nearly to one-half. And in August, with exactly 58,304 different samples, they reached their low point. Since then, no sample rates above the significant 100,000 mark have been reached again, and it remains to be seen whether cyber gangsters are currently relying on other malware that promises more success with less time and effort.

As opposed to ransomware blackmail and the comparatively elegant abuse of third-party computing power by means of crypto miners, the abuse of third-party account data requires some level of logistics and division of labor. Above and beyond the creation and distribution of malware, it requires a good deal of time and effort collecting, evaluating and implementing the stolen account information. Moreover, banks and other financial service providers have since reacted significantly more quickly to conspicuous account activities. This means that the time and effort is increasing for criminals, at a time when the margins are dwindling. It remains to be seen whether the business with third-party online data will remain lucrative for criminals.

TOP 10 Windows malware 2018

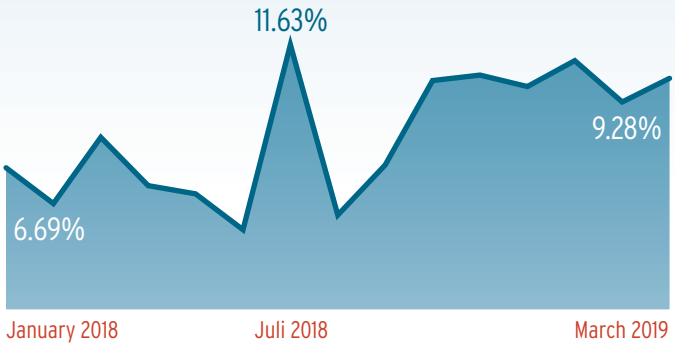
1	AGENT	11.21%
2	SIVIS	5.05%
3	KRYPTIK	4.84%
4	VIRLOCK	4.57%
5	LUDBARUMA	3.78%
6	VIRUT	3.59%
7	RAMNIT	2.79%
8	ADLOAD	2.63%
9	UPATRE	2.16%
10	LAMER	2.00%

Other malware classes and PUA

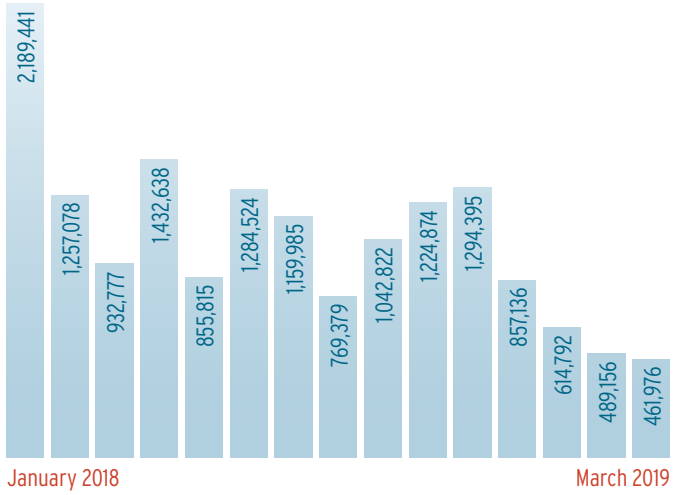
Whereas security programs for Windows mainly had to combat the recurring surge of Trojans in 2018, the new development rates of other traditional malware classes exhibited a downward trend or stagnated in comparison with the previous years' statistics from 2017. This held true not only for Internet worms, which did not exceed the threshold of 100,000 new samples per month in 2018, but also for malware scripts which only comprised 0.15% of the overall malware detected. While dialers and rootkits were recorded by the detection systems of the AV-TEST Institute, statistically at least, they played no relevant role in 2018 due to insufficiently low sample numbers.

Additional good news is the downward trend of tracking tools for monitoring user behavior, as well as other potentially unwanted applications (PUAs). This software, operating in a legal grey area, recording the browsing habits of users and forwarding them to companies, for example, appears to no longer be worthwhile, at least under Windows, and is therefore severely in decline. This can also be seen as a success of antivirus software manufacturers for Windows, who despite major resistance of the industry, reported PUAs as a threat to the users of their security programs.

Windows: development of new worms in 2018 + Q1 2019



Windows: development of new PUA in 2018 + Q1 2019



Trend 2019

The data recorded in the first quarter of 2019 essentially confirmed the trend of the previous year. A severely increasing number of Windows exploits follow the development statistics of Trojans, which continue to make up the lion's share of malware newly developed for Windows. The share of specialized Trojans, including crypto miners, is increasing. Also for ransomware, AV-TEST systems indicate a slightly rising trend in the first quarter, as opposed to the numbers of the previous year. The development numbers of new password Trojans, by contrast, have been continuously declining to below 1% of the total volume of malware.

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

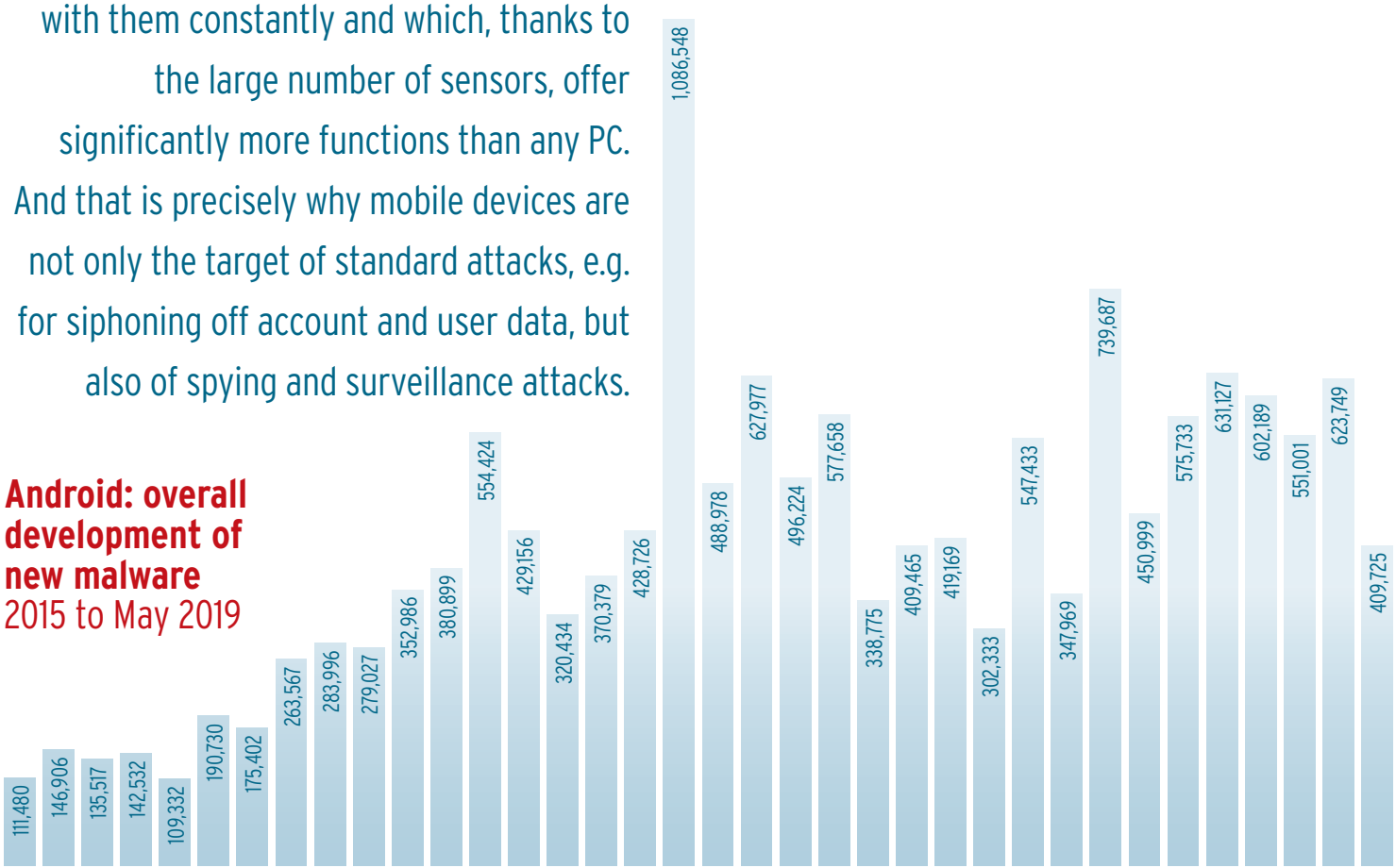
Mobile phones became „smart“ in 2007 with the introduction of apps. Along with the opportunity to offer proprietary applications for third-party users online, the hacking methods of cybercriminals unfortunately also became more sophisticated. And since that time, they have continued to develop new malware for devices, which users carry with them constantly and which, thanks to the large number of sensors, offer significantly more functions than any PC. And that is precisely why mobile devices are not only the target of standard attacks, e.g. for siphoning off account and user data, but also of spying and surveillance attacks.

Declining rate of newly-developed malware

Compared to the previous high point of the rate of newly developed malware in June 2016, the development numbers from last year are actually quite a relief: By comparison, the number of new malware programs for Android systems has practically been cut in half. Last year, on average, criminals distributed 616,459 malware applications per month for the mobile operating system used most commonly worldwide. Accordingly, at least from a purely quantitative perspective, this is a positive development

However, and this is the other side of the coin, the degree of specialization of malware has significantly increased. Unfortunately, the declining malware statistics are therefore no cause to let one's guard down. Primarily, the quantitative decline is based on reduced numbers of classic Trojans. With over 90% of all new developments, they continue to make up the lion's share of all malware samples for Android. However, malware programs with a high level of specialization and a targeted malicious effect are heavily increasing, including crypto miners, password Trojans and ransomware. Accordingly, there is a noticeable trend towards malware with which criminals can earn money directly and without major detours.

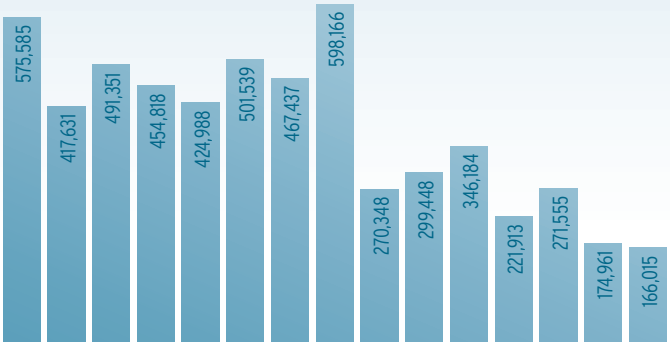
Android: overall development of new malware
2015 to May 2019



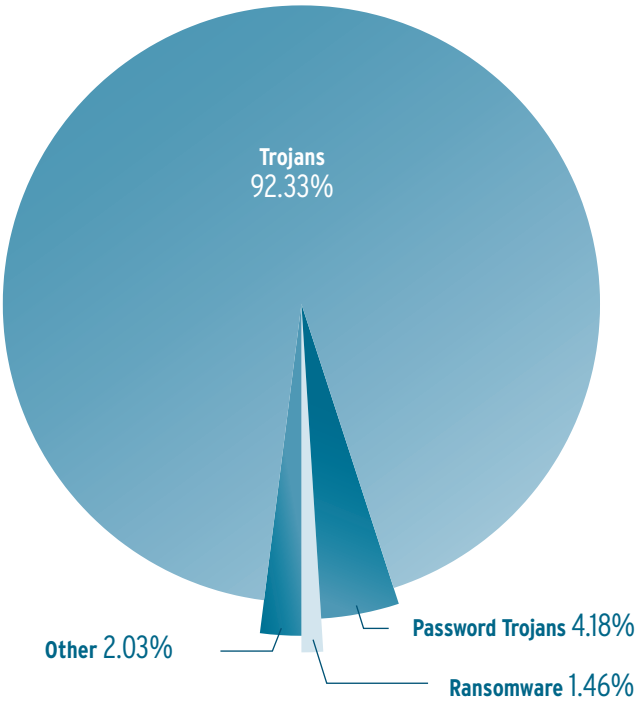
Banking malware goes high-tech

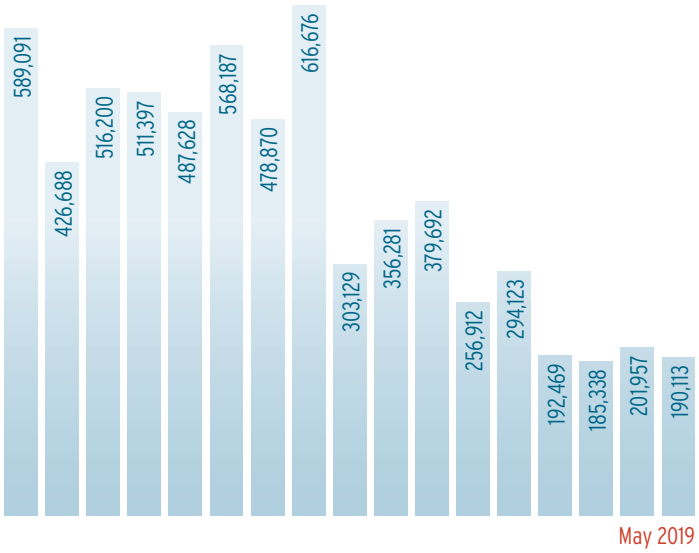
The increasing distribution and acceptance of banking apps has actually not gone unnoticed among cybercriminals. Worldwide, there is hardly a bank that doesn't offer its own app. And such banking apps are used not only for two-factor authentication when using a PC for online banking, rather more and more often, access is provided directly via the mobile device. Alongside established banks, in 2018, more and more financial service providers, so-called fintechs, offered apps for mobile banking on an Android basis. These financial institutions offer no other access to the user's own account then via the relevant app. Accordingly, the development of malware programs designed to steal login information of online accounts, or phishing, evolved into high-tech malware. An example for this is the development exhibited by the banking Trojan „Anubis" over the course of the year. The malware for siphoning off account access data received modifications throughout the year designed to prevent its detection by security apps. The malware, which is for example installed on the device disguised as a battery app, takes over control of the motion sensors of infected mobile devices. If the sensor data shows no motion, the malware assumes it is in a sandbox for detection of malware and it plays dead.

Android: development of new Trojans in 2018 + Q1 2019

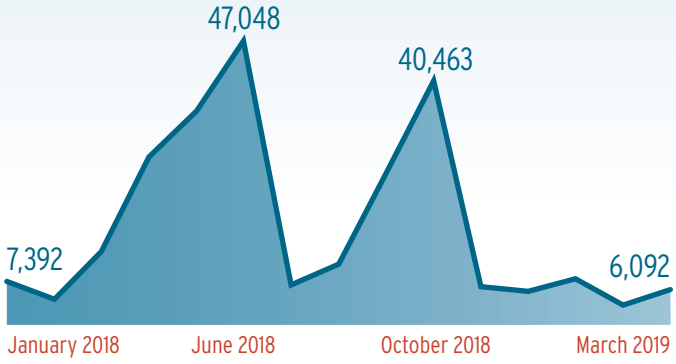


Android: distribution of malware in 2018

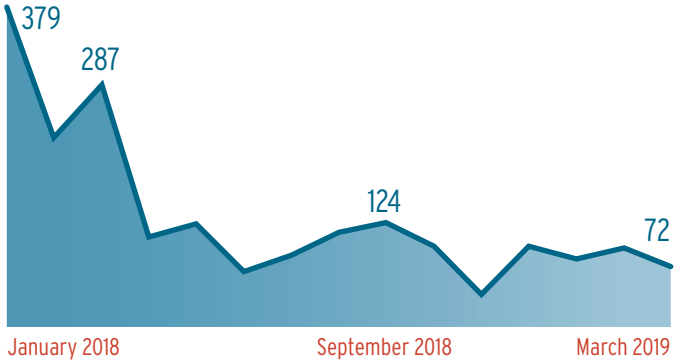




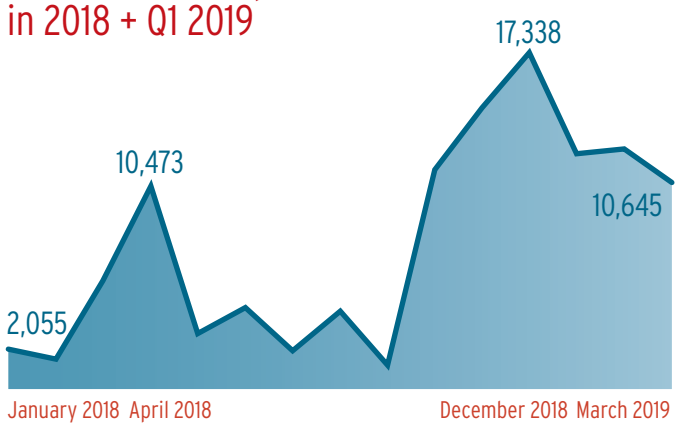
Android: development of new password Trojans in 2018 + Q1 2019



Android: development of new crypto miners in 2018 + Q1 2019



Android: development of ransomware in 2018 + Q1 2019



The latest state-of-the-art appears to be the banking Trojan „Gustuff", discovered in the first quarter of 2019. This high-tech malware can steal not only login details of over 100 banking apps, as well as more than 30 crypto currency apps, but it can also automatically carry out transactions with these details. To do so, Gustuff launches relevant apps independently in the background and autonomously initiates transactions via stolen account data to preconfigured accounts.

„Easy money" with Android

In the first quarter of last year, Android-based crypto miners also began to soar, but have since declined and in the first quarter of 2019, they stagnated to development rates of below one hundred new samples per month. It is to be assumed however, that criminals will constantly try to tap into the ever-increasing computing power of mobile devices, as soon as the technical development of their malware allows it to remain on the user devices undetected for long periods of time. This assumes that crypto miners are developed in such a way that they are not already detected through a severe increase in battery consumption.

Another trick for directly „collecting" money from users of mobile devices are blackmail Trojans. And especially towards the end of the year 2018, the development of new ransomware samples for Google's operating system experienced a large increase. In December, the annual rate with 17,338 newly developed ransomware samples, reached its high point. Assuming the persistently low distribution of protection apps for Android devices, as well as complacency in creating backups with respect to all data that users carry around with them on their devices, ransomware for Android appears to be a promising business model for the future.

TOP 10
Android malware in 2018

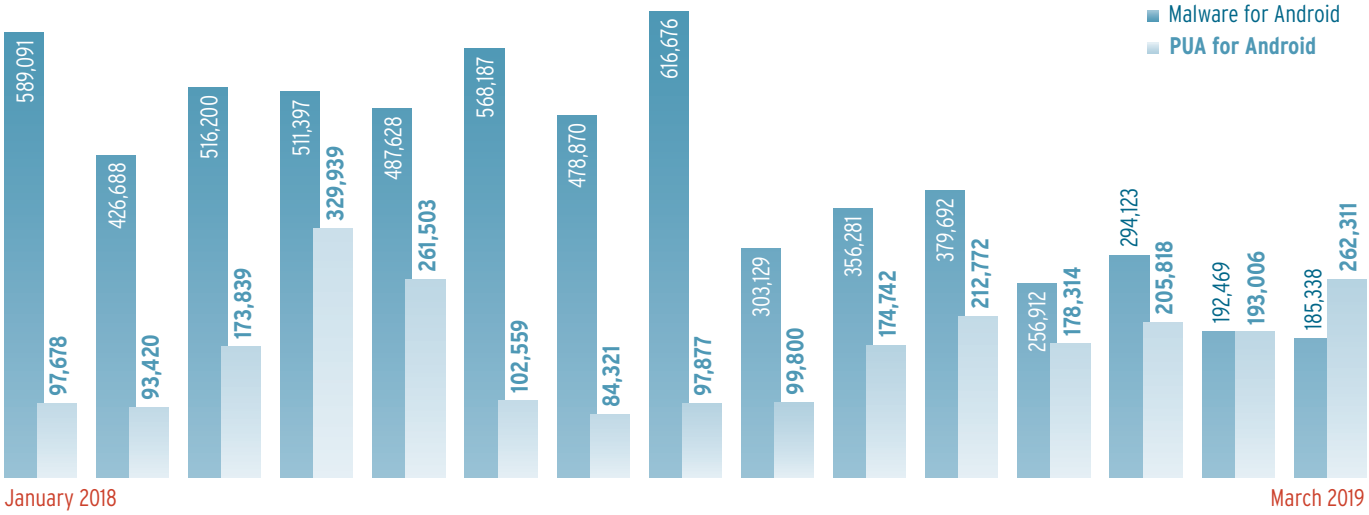
1	SMSREG	23.81%
2	SHEDUN	19.94%
3	AGENT	15.44%
4	SMSPAY	6.92%
5	SMS	5.30%
6	HIDDENAPP	3.00%
7	HIDDAD	1.89%
8	CLICKER	1.86%
9	SMSAGENT	1.57%
10	FAKEAPP	1.23%

Trend 2019

The total rate of Android malware programs indicates a further decline in the first quarter of 2019. This trend results essentially from declining sample numbers among traditional Trojans. This is followed by the rates of highly specialized malware, such as ransomware, crypto miners and banking Trojans. However, these rates merely reflect the quantitative malware development, and the analysis of high-tech malware such as „Gustuff" would seem to suggest that the trend is more towards qualitatively sophisticated malware samples and that the threat level is increasing despite declining sample numbers.

Add to this another negative trend for Android mobile devices: Whereas in most of the other operating systems, the development of potentially unwanted applications (PUAs) is declining, the spying on user behavior for Android devices is increasing. Thus, the number of PUA samples in March for the first time exceeded the number of newly developed malware programs.

Android: development of malware compared to PUA
in 2018 + Q1 2019

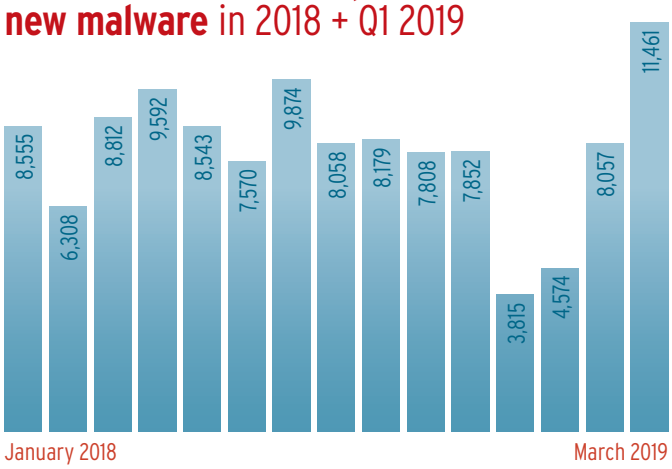


AV-TEST GmbH regularly reviews all market-relevant security solutions for Android mobile devices every two months. The latest test results can be downloaded for free on the website under https://www.av-test.org/en/antivirus/mobile-devices/.

Security Status macOS

Since the integration of the malware scanner Xprotect in Mac OS X 10.6 (Snow Leopard), Apple has admitted de facto that the malware threat also exists for its computing devices. Nonetheless, there is a stubborn rumor, not only among Apple fans, that macOS users supposedly do not need additional virus protection. The AV-TEST Institute provides decisive facts to the often emotional discussion regarding current measurements of Mac malware

macOS: overall development of new malware in 2018 + Q1 2019



Mac's malware curve continues to rise

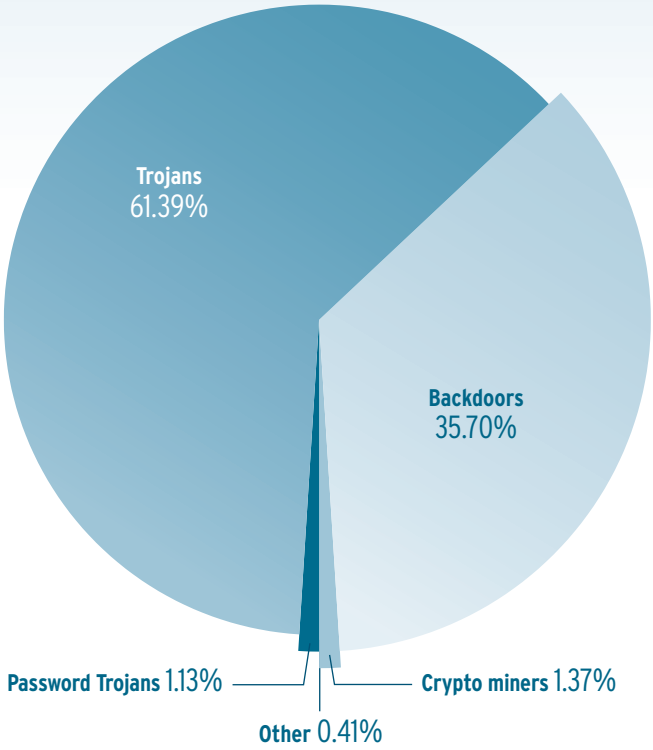
It is true that the quantitative threat situation for Apple users measured strictly in terms of the occurrence of newly developed malware samples is significantly lower than for other standard operating systems. In 2018, the AV-TEST Institute's detection systems discovered an average of 7,913 new malware samples per month for Apple's operating system. In total, precisely 93,265 Mac malware samples were tallied last year. This is the malware rate that Windows systems are exposed to approximately every hour. However, significantly more Windows users protect their systems with anti-virus software. And compared to the „happy years" with low Mac malware development, cybercriminals have clearly identified Apple users as a lucrative target. The just under one hundred thousand malware samples in 2018 speak for themselves.

Apple attacks are Trojan attacks

As with most other operating systems, Trojans are the preferred means for cybercriminals to attack Apple systems. Wholly 61.39 percent of all macOS malware samples in 2018 involved Trojans. In connection with backdoors, which accounted for 35.7 percent of the malware total and thus occupied 2nd place, this is an explosive mix. Because both types of malware aim to load any number of malicious functions onto victim systems after infection.

This is also the goal of the Trojan Flashback, which for the third time in a row has defended its 1st place position in the Malware Top 10 for macOS. Initial Flashback versions disguised themselves as an installation package of the popular Flash Player. However, a new variant of the Trojan offers attackers many more infection pathways, including drive-by downloads via infected websites. If Java code is activated, Flashback will automatically enter Apple computers via the browser. The fact that constant modifications of this malicious code, recognized as early as 2012, still make it a promising vehicle for cybercriminals says quite a lot. Last year, Flashback samples accounted for over 40 percent of all Mac malware (43.33 percent)! But Flashback is not an isolated case. The Malware Top 10 for Apple computers contains lots of „old friends" like „Mac Control", „Getshell" and „Keranger". This illustrates that the pressure to innovate among Mac malware developers cannot be all too great, given the low resistance.

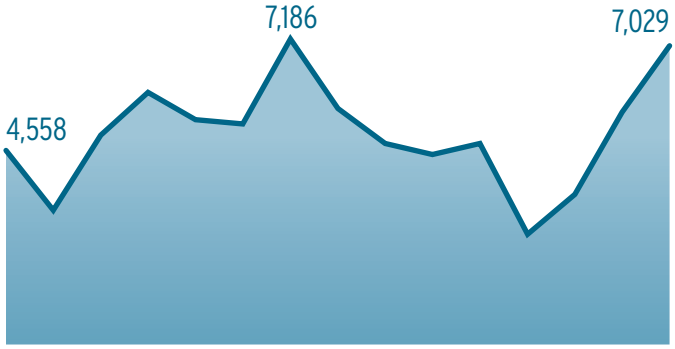
Distribution of malware under macOS in 2018



TOP 10 macOS malware 2018

1	FLASHBACK	43.33%
2	MAC CONTROL	39.74%
3	SHLAYER	10.90%
4	AGENT	1.60%
5	ADLOAD	1.42%
6	APTORDOC	1.13%
7	GETSHELL	0.18%
8	MACNIST	0.16%
9	KERANGER	0.11%
10	XCODEGHOST	0.07%

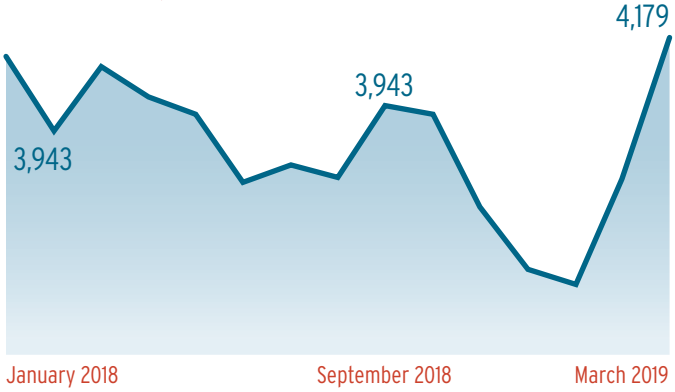
macOS: development of Trojans in 2018 + Q1 2019



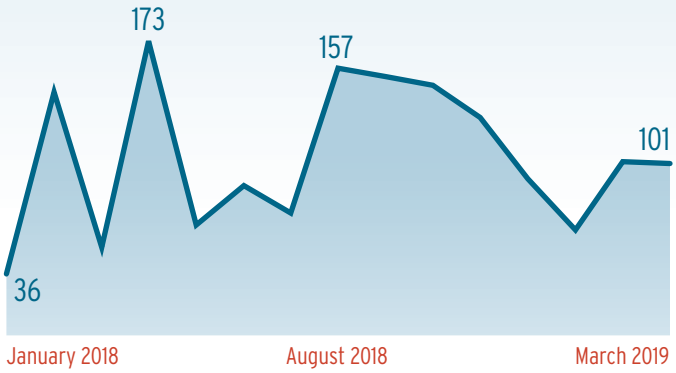
Trend towards malvertising for macOS

But the year 2018 also saw new malware developments such as „Shlayer". Since the end of last year, this Mac Trojan has been using the malvertising trick by leading its victims to infected websites via purchased advertising banners and proliferating in this manner. If the browser launches a corresponding website, the banner redirects to a contaminated website. Here the Trojan then presents itself as an update package of the Flash Player for download. Shlayer instantly shot up to third place in the Malware Top 10 with 10.9 percent of the total Malware volume. Shlayer also seeks to add more malicious code with additional functions.

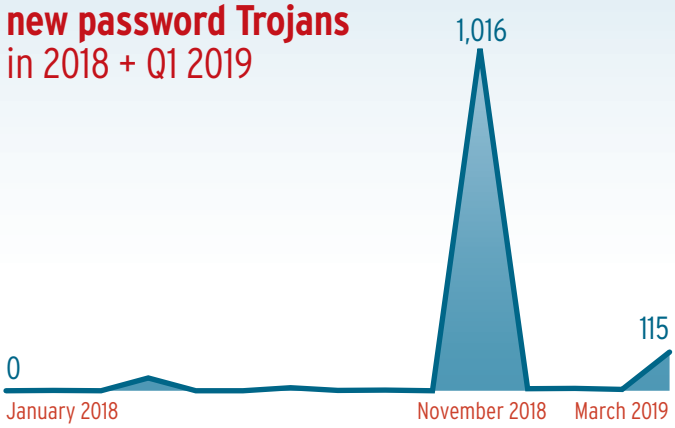
macOS: development of backdoors in 2018 + Q1 2019



macOS: development of new crypto miners in 2018 + Q1 2019



macOS: development of new password Trojans in 2018 + Q1 2019



Mac-users directly cashed out

Measured in terms of pure „unit numbers", it would appear that specialized malware for Macs is a minor threat. The fact is, however, that it exists and that it encounters little resistance. While classic viruses, which account for over 20 percent of Windows malware, are not an issue for Mac computers (0.04%), the use of high-end malware for criminals is worthwhile even in small unit numbers. In contrast to their approach to Windows users, criminals rely directly on malware for Mac users, which can be more or less immediately converted into cash. In 2018, these included in particular crypto miners, password Trojans and ransomware. The potential of abusing the resources of Apple computers, most of which are equipped with powerful hardware, to mine for digital currency was highly popular in 2018. A total of 1,305 malware samples of the crypto miner category were detected by AV-TEST systems for Mac malware (1.31%). This was followed by password Trojans for skimming off account data (1.13%) and blackmailer Trojans (0.16%).

Trend 2019

In the first quarter of 2019, backdoors ceded nearly almost five percent of the total malware distribution to Trojans, which clearly make up the lion's share of Mac malware with over 66 percent. While the importance of crypto miners among cybercriminals is slightly diminishing, the new development rate of ransomware is increasing fourfold. Accordingly, Mac users are recommended not only to use a good antivirus program, but also to make regular backups.

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

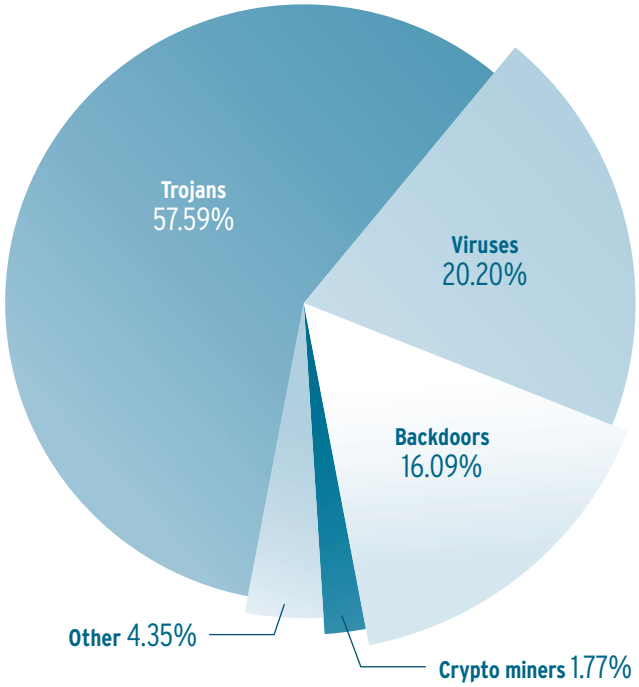
With an almost unmanageable number of networked devices and services, the Internet of Things is an absolute boom sector in IT development markets. However, in the race for lucrative market shares, the IoT industry continues to develop multitudes of Internet-connected products without a sufficient security concept and frequently disregarding even absolute minimum standards of IT security.

Doubling of networked devices in four years

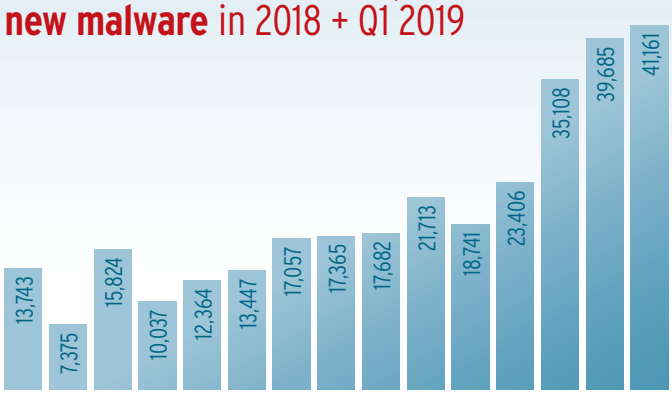
For cybercriminals, the rapidly growing number of unprotected or, at best, poorly protected devices, are an easy and welcome target. The risk is borne by unsuspecting users of networked devices. They rely on non-existent legal requirements and the manufacturers' sense of responsibility and thus risk losing their privacy.

In a recent study, Juniper analysts estimate the total number of devices that will communicate with each other over the Internet of Things by 2022 at more than 50 billion. Compared to the level of 21 billion in 2018, the IoT cosmos is expected to more than double in just four years. The strong growth of the Internet of Things is affecting virtually all areas of our lives and is bound to also change our working environment, along with our leisure time. Such devices and services can make life easier for us, yet the exact opposite may also be the case. Because more and more devices, which we use as a matter of course in everyday life and some of which we would never suspect it, are

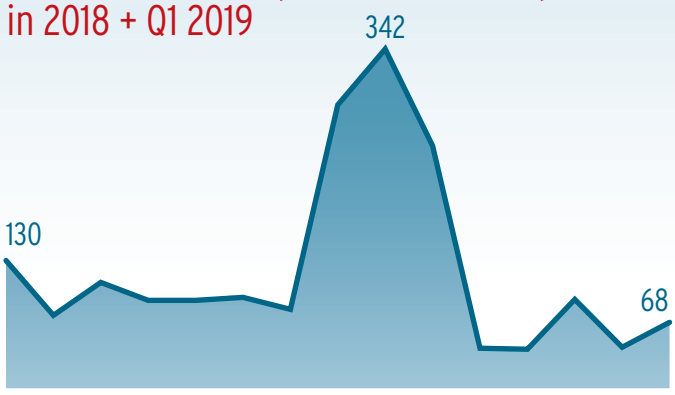
Distribution of malware under IoT in 2018



IoT/Linux: overall development of new malware in 2018 + Q1 2019



IoT/Linux: development of new exploits in 2018 + Q1 2019



connected to the Internet. Instead of television sets, cameras and smart language assistants, in the near future, we will begin to see everyday objects such as vacuum cleaners and toothbrushes collecting information about their users and sending it to the manufacturers and their related business partners.

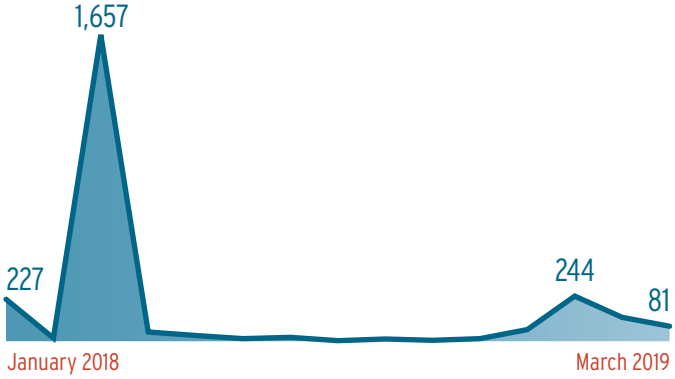
The fact is that security experts like the experts at the AV-TEST Institute have been warning about the dangers of vulnerable IoT devices for years, but these calls continue to fall on deaf ears. And it is precisely the manufacturers of end-user products, especially those that do not originally come from the IT industry, who are committing the same errors that were made 30 years ago with PCs and 10 years ago with smartphones and other mobile devices: Poor or even unprotected access accounts, weak or often non-existent encryption when storing and transporting data, out-of-date software and inadequate or even no security update service, all add up to a field day for attackers for the majority of devices, and the trend is continuing. In addition, the non-IT sector is increasingly offering its devices „smart", i.e. selling them with Internet connections and apps. However, the development of typical IT modules, such as online services and apps, usually takes place through third-party providers. Thus, the providers of networked products often do not know what is in their apps or behind their online services and cannot maintain and validate them or provide their own necessary security updates.

Non-existent standards and old security gaps

Basically, IoT devices and services offer a variety of attack vectors: The main targets of criminals are the user devices themselves, connected apps and mobile devices on which the applications for controlling IoT devices usually run. The back end of the manufacturers used by the server structures and device connectivity, as well as the transmission paths of essential and other recorded data are further gateways for digital attacks. Nevertheless, IoT devices with inadequate IT security continue to take the market by storm. And for the growing number of unprotected devices, a flood of malware is

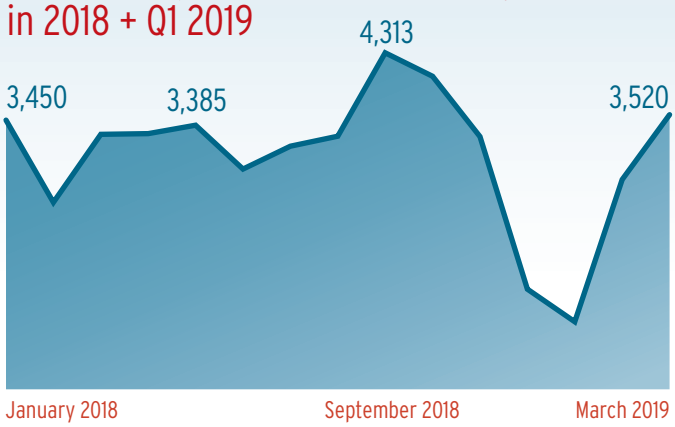
IoT: development of new Gafgyt Trojans in 2018 + Q1 2019

IoT: development of new Hajime Trojans in 2018 + Q1 2019



IoT: development of new Mirai Trojans in 2018 + Q1 2019

IoT: development of new Vit Trojans in 2018 + Q1 2019



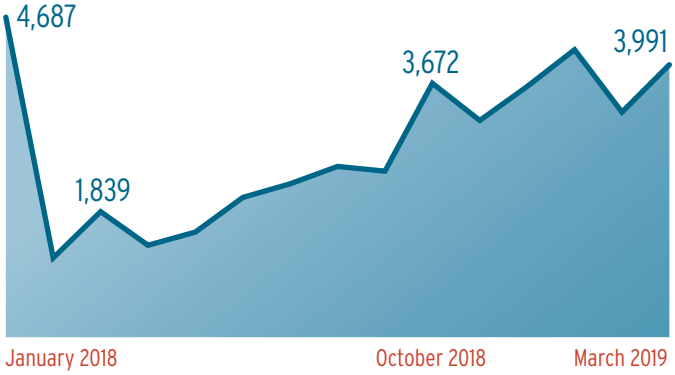
already waiting, which currently mostly wants to commandeer their concentrated and networked computing power.

Given the fact that standard and compatible IoT systems must also run on the microcontroller level, mostly stripped-down Linux versions such as Canonical Ubuntu are used. In the last quarter of 2017, AV-TEST Institute's detection systems recorded a rapidly increasing number of newly developed malware for Linux-based IoT systems. In 2018, the number of new malware developments once again experienced a dramatic increase: 15,730 new malware programs for attacks on IoT devices and infrastructures were developed per month last year. And this already critical value for a rapidly growing group of devices, most of which are online either without protection or with poor protection at best, is dramatically exacerbated in the first quarter of 2019: Within three months, the IoT malware sample rate doubled to its current high mark of over 40,000 new samples per month.

But of course, other IoT operating systems, such as the open source Contiki and RIOT OS systems, along with Google's slimmed-down Android version, Brillo OS, are also vulnerable to attacks. The majority of newly developed malware for IoT systems, at 57.59 percent in 2018, involved the category of Trojans. This was due in large part to an „old nemesis", who already played a lead role in the security reports of the past two years: "Mirai". AV-TEST's detection systems first detected the malware sample in August 2016, and in October 2016 Mirai already unleashed large-scale DDOS attacks against major online services in the US and Europe. Mirai obtained the computing power for this from a botnet of hundreds of thousands of hijacked routers, printers, webcams and online video recorders without effective authentication procedures and with poor or non-existent encryption.

IoT: development of new Tsunami Trojans in 2018 + Q1 2019

IoT/Linux: development of backdoors in 2018 + Q1 2019



High malware curve versus a low learning curve

Measured in terms of the development figures, the usage of the Mirai malicious code for criminals still seems to be worthwhile. The Mirai code accounted for more than 40 percent of the total malicious code for IoT devices (41.19%) in 2018. Unfortunately, the steep development curve of Mirai samples does not indicate a commensurately high learning curve for device manufacturers, who should have been aware of these dangers since October 2016 at the latest. However, a response does not appear to be forthcoming, and criminals accordingly continue to deploy Mirai successfully for attacks on IoT devices and connected infrastructure. The sample numbers of the main malware for IoT devices have been exploding since the beginning of last year. With 78,186 variants, Mirai clearly leads the ranking, ahead of other IoT Trojans such as „Vit" (37,807 samples), „Gafgyt" (36,769 samples) and „Tsunami" (2,959 samples).

One development that surely makes life easier for cybercriminals is the increasing number of known vulnerabilities in IoT devices and the increasing possibility of attacking them via automated malicious code. The available backdoors are increasing accordingly. Last year, a total of 188,754 of these gateways were available to attackers for Linux systems alone. In the first quarter of 2019, this figure had already reached 115,954!

Other types of threats, such as digital blackmail or the failure of vital IoT devices, services and functions, are another horror scenario for the digitalized civil society. Although current measurements have recorded initial attempts in the field of ransomware, these cannot yet be identified as an acute threat, at least in terms of numbers. On the other hand, Mirai attacks that have already taken place, in 2018 involving roughly 0.01 percent of total malware, indicate that a specialized ransomware code is not necessarily required for IoT-based blackmail models.

TOP 10 IoT malware 2018

1	MIRAI	41.19%
2	VIT	19.93%
3	GAFGYT	19.40%
4	TSUNAMI	1.57%
5	AGENT	1.41%
6	BITCOINMINER	1.25%
7	DDOSTF	1.11%
8	HAJIME	1.11%
9	DOFLOO	0.92%
10	SHELLDL	0.89%

Trend 2019

In addition to the long-standing, systematic collection of new malware samples for IoT devices, which continued to proliferate in first quarter, especially for Mirai, Vit and Gafgyt, the AV-TEST Institute has been analyzing the systematic characteristics of attacks on networked devices with its own honeypot systems since 2017. These reveal alarming numbers: In the first quarter of 2019 alone, there were a total of 3,200,000 attacks on the open IoT systems on the Web! In 41,213 cases, attackers tried to use malware programs to hijack the hardware placed on the Web. In 71.44 percent of all successful malware infections, AV-TEST engineers identified the Mirai code as the attacker's weapon of choice. In addition, Linux shell commands were often used to access the SSH/Telnet connection of the honeypot systems. In most cases, automated attacks were used to circumvent a possible password protection of the devices. The user names used most often in these attempts were „root" and „admin"; brute force attacks on passwords most frequently use the terms „admin" and „default". This indicates, among other things, how important it is for manufacturers of IoT products to require that standard passwords be changed when customers install IoT products!

Incidentally, the United States leads the Top 10 countries of origin responsible for attacks on AV-TEST IoT honeypots, followed by the Netherlands and Germany. China is in fourth place. Russian hackers currently occupy 9th place.

TOP 10
Countries of origin responsible for attacks on IoT 2018

1	US	1,287,700,195
2	NL	40,048,945
3	DE	15,359,619
4	CA	10,412,092
5	ZA	9,345,064
6	GR	6,894,600
7	IN	5,930,786
8	GB	4,292,386
9	RU	3,680,935
10	IT	2,700,082

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/.

2018: The Year of the CRYPTO MINERS

The promising and virtually risk-free business model of profiteering with crypto miners at the expense of third parties turned out to be a complete success for cybercriminals in 2018 and, compared to other types of malware, quickly established itself after an extremely short trial phase. The extent of the threat posed by crypto miners is also manifest in the fact that browser providers such as Mozilla implement protection modules against unwanted mining processes.

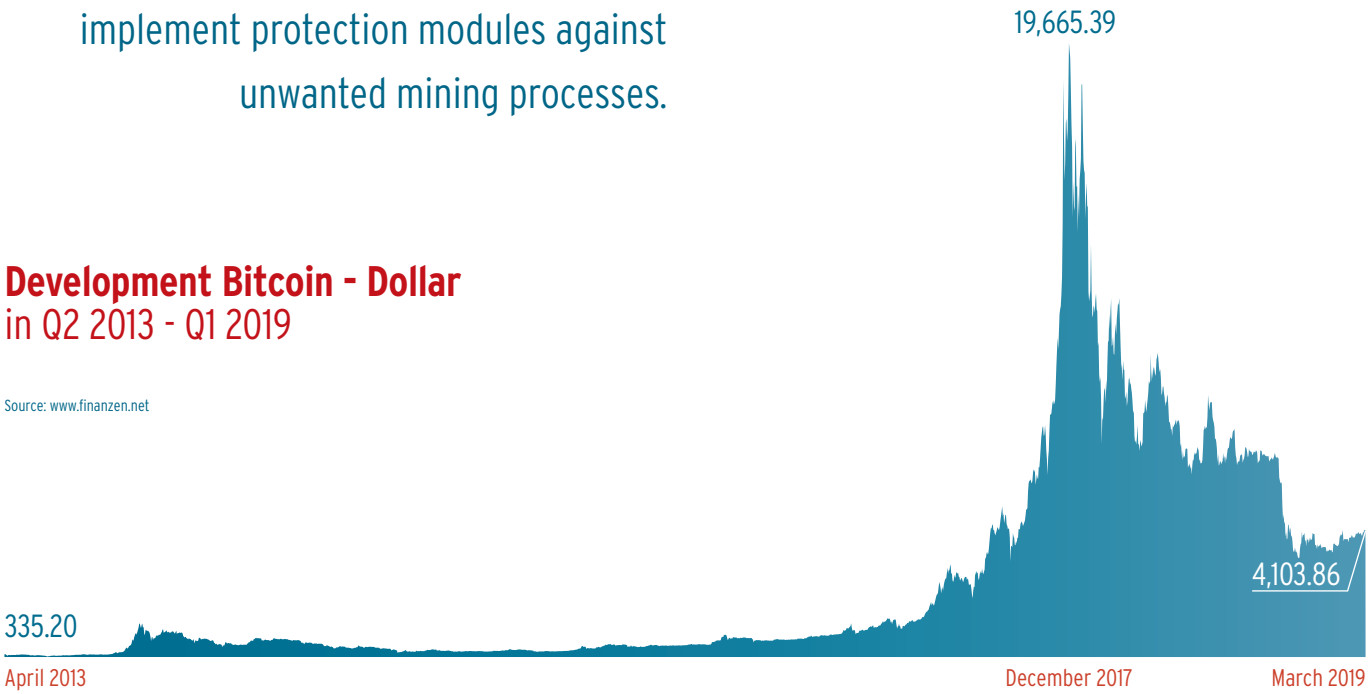
Getting rich at other people's expense

The „business model" works as follows: The one group provides the complete infrastructure and bears all costs for hardware and its computing power. It is also left to cover the costs of operations, such as energy and Internet bandwidth. By contrast, the others simply use software that puts those resources to work, calculating cryptocurrencies, and reap the entire profit for themselves. As only one side wins in this business model, while the other incurs massive damage, of course it is not a voluntary proposition, but works only if the victims of this rip-off remain oblivious to it.

In the 2017 Security Report, the AV-TEST Institute already dedicated an entire chapter to the mining malware necessary for such crooked business, which explains the malware's mode of operation in detail (https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2017-2018.pdf). Towards the end of 2017, AV-TEST's systems recorded for the first time malicious programs for mining digital currencies in greater concentration. In the first quarter of 2018, when the prices of major crypto currencies such as Bitcoin, Etherium, Ripple, Monero and Bitcoin Cash temporarily jumped to all-time highs, the development of illegal mining programs followed suit. With the submission of the last report in the first quarter of 2018, the collection of crypto miners already included more than one million malware samples. Forecast by security experts: This malware will clearly establish itself.

Development Bitcoin - Dollar
in Q2 2013 - Q1 2019

Source: www.finanzen.net

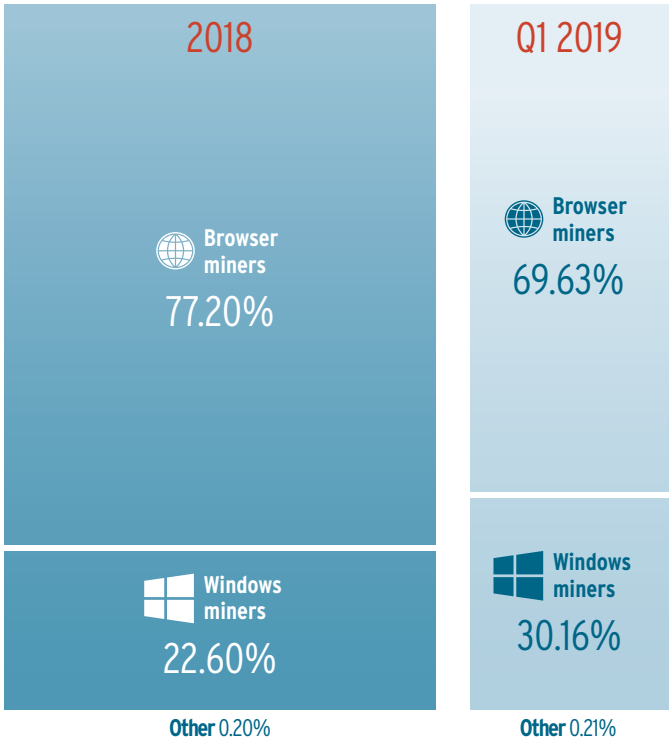


Strong increase in crypto miners

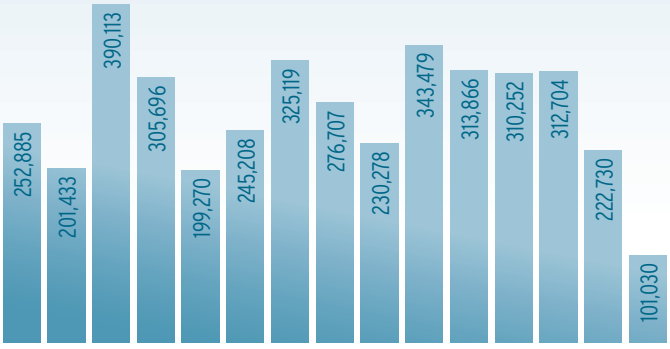
The statistics in the current report confirm this assessment: By the end of the first quarter of 2019, the number of crypto miners had more than quadrupled. By the time this report goes to print, the AV-TEST database contained exactly 4,328,372 different copies of this malware category for all standard operating systems!

In analyzing the development figures of new crypto miners, we can see major shifts in the platforms and operating systems used in the mining for cryptocurrency: Whereas 55 percent of the mining malware was still being run on Windows systems in 2017 and 44 percent was being used in standard browsers, last year indicated a completely different scenario. The use of Windows as a mining platform dropped significantly (to 22.6%) and more than three-quarters of all crypto miners used normal standard browsers to enrich their criminal masterminds at the expense of third parties.

Distribution of crypto miners



Overall development of miners in 2018 + Q1 2019



One can only speculate as to the reasons for these fluctuations with this quite new malware class. As standard programs independent of operating systems, browsers certainly offer criminals a platform with the highest penetration rate for crypto miners. Accordingly, the distribution of such high-tech malware is likely to be most effective for browsers. A further point that speaks for the exploitation of browsers is their direct and constant Internet connection. At the same time, this reduces the risk of being discovered by protection programs.

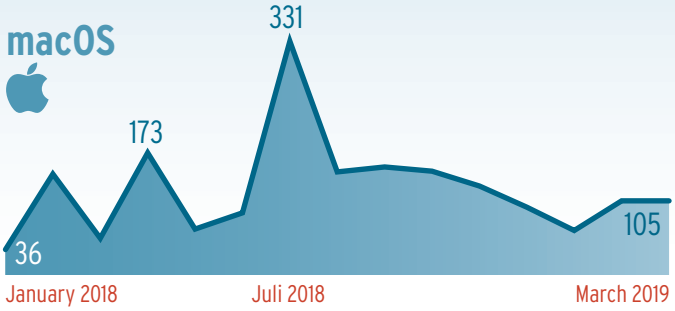
Moreover, when comparing the overall development figures of new mining malware, it seems that there is hardly any comparative data that explain the clearly existing development peaks among crypto miners for the different platforms. For example, the new development of browser-based mining malware shows clear high marks for June and August of last year, for Linux miners in June. By contrast, Windows miners reached their peak in March of last year and macOS had its peak season in July. While comparing prices of the different crypto currencies could certainly unearth exciting results, it is not part of this analysis.

In addition to browsers and the Microsoft platform, criminals of course also use most other available systems, albeit a significantly smaller share. For example, in 2018 the detection systems of AV-TEST recorded a total of 3,323 miners, which targeted Linux systems and are therefore well suited for use on large servers as well as on mostly unprotected IoT hardware (0.1% of the total). With 1,729 new mining samples, Android followed in fourth place (0.05%), in front of macOS with 1,556 new malware samples. For Apple's mobile operating system iOS the detection systems of AV-TEST could not detect a single crypto miner.

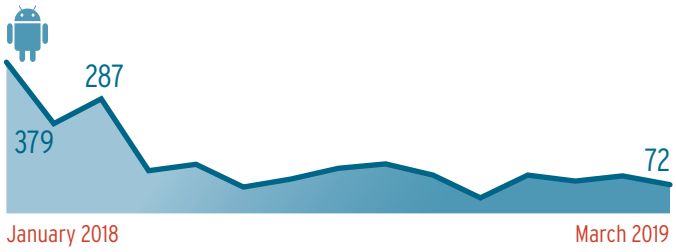
Development of Crypto miners in 2018 + Q1 2019

Windows

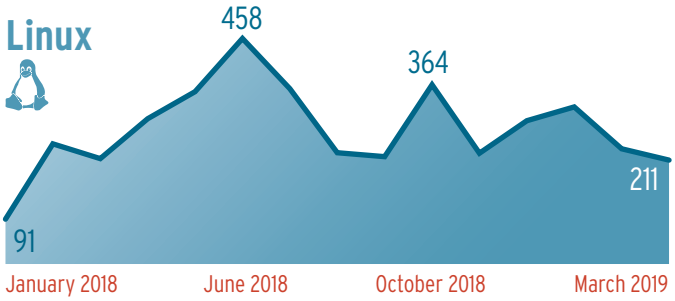
macOS



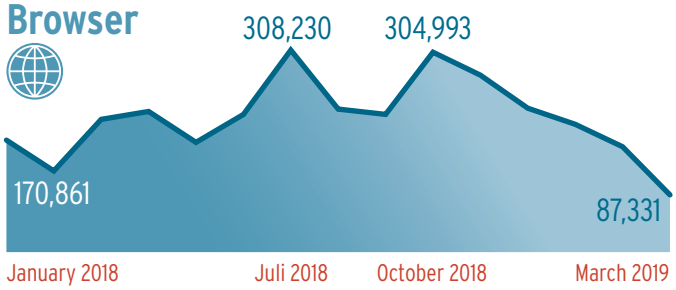
Android



Linux



Browser



Trend 2019

For the first quarter of 2019, AV-TEST's collection systems report a moderate decline in the new development of mining malware, which is mainly due to a decline in the dominant browser malware. Accordingly, the share of Windows miners rose from 22.6 to 30.16 percent. However, these trends should be taken with a grain of salt. On the one hand, the field of crypto miner research is still quite new. On the other hand, this type of malware, like the defined targets of cryptocurrencies themselves, has exhibited extreme exchange rate fluctuations.

Security Status INTERNET THREATS

The starting point of virtually every malware attack has its origin online. Most malware travels from continent to continent in large-scale spam waves. But drive-by downloads via infected websites, mass proliferation of infected apps and automated brute force attacks on unprotected IoT devices are also part of the malware distribution channels of cybercriminals. AV-TEST now bundles a large part of its measurements and worldwide unique analysis data of the institute in its new online portal „AV-atlas“. The system not only provides real-time information on the incidence of malware, but also scans sources and origins and enables state-of-the-art malware monitoring.

Contaminated mass mails

One of the main infection vectors for spreading malware is and remains the dispatch of e-mails. These can be targeted spear phishing attacks on certain victims whose behavior has been scoped out long in advance on social media platforms, for example. Or it may involve widespread mass mail campaigns that retrieve account data, transport infected files in attachments, or use an interesting link to direct masses of victims to infected websites. At the time this report was completed, 77.6 percent of all malware-infected websites referred to in spam emails were registered under the top-level domain (TLD) „COM“. This was followed by ORG (4.7%) and NET (3.2%). The first country-specific TLD to follow is the „ME“ identifier of the small Southern European Republic of Montenegro.

These websites transmitted infected data packets upon launching in the browser. Most frequently, the HTML format was used. In 21.1% of cases, the infected websites distributed their malware code in the format of the web programming language. With a significant margin, this is followed by the standard ZIP compression format (2.6%) and only then by executable file formats ending in EXE (2.3%).

TOP 10 Dangerous URLs according to top-level domains in 2018

1	COM	77.6%
2	ORG	4.7%
3	NET	3.2%
4	ME	2.8%
5	ID	2.8%
6	TO	2.3%
7	TV	2.2%
8	LV	1.7%
9	PL	1.7%
10	TIPS	1.2%

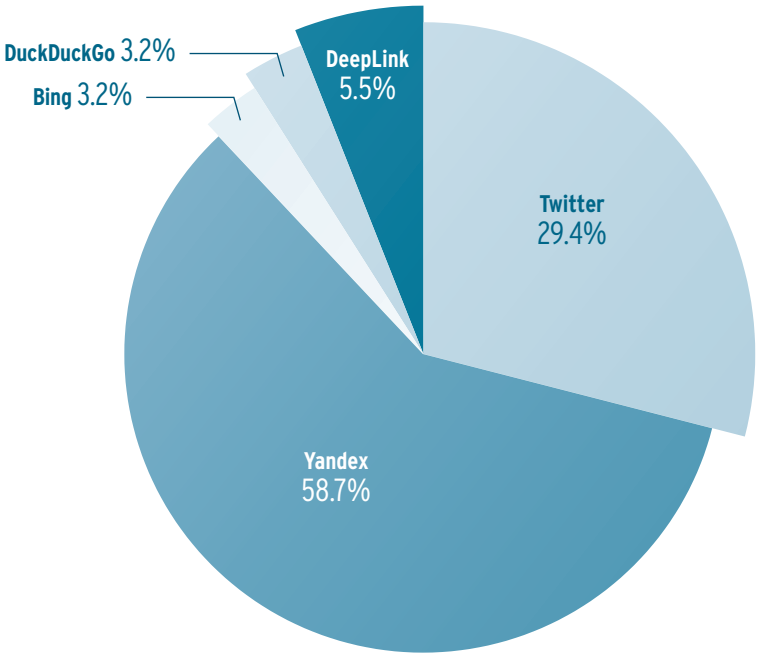
Malvertising via search engine

Within the scope of so-called malvertising, criminals rent trending domains on search engines with extremely similar-sounding terms in the URL and advertise the infected websites via search engines. For this purpose, the AV-TEST Institute checks common search engines for links to infected websites. With over half of all infected websites (58.7%), the Russian search engine Yandex proved to be the most vulnerable to the spread of links to malware-infected websites. With 29.4 percent, the US microblogging service Twitter followed, via which criminals also jump on trendy topics on a grand scale in order to direct as many victims as possible to websites linked in the tweet via tweets that appeal to the masses. These two services rank far ahead of alternative web services such as DuckDuckGo (3.2%) on cybercriminals' list. Microsoft's search engine Bing ranks fifth (3.2%), Google plays no role at all in this comparison due to insufficiently low numerical values.

TOP 10 Malware Payloads 2018

1	NO EXTENSION	71.4%
2	HTML	21.1%
3	ZIP	2.6%
4	EXE	2.3%
5	PHP	1.4%
6	RAR	0.6%
7	HTM	0.3%
8	ASP	0.2%
9	KZJV	< 0.1%
10	JPG	< 0.1%

Dangerous URLs by source in 2018



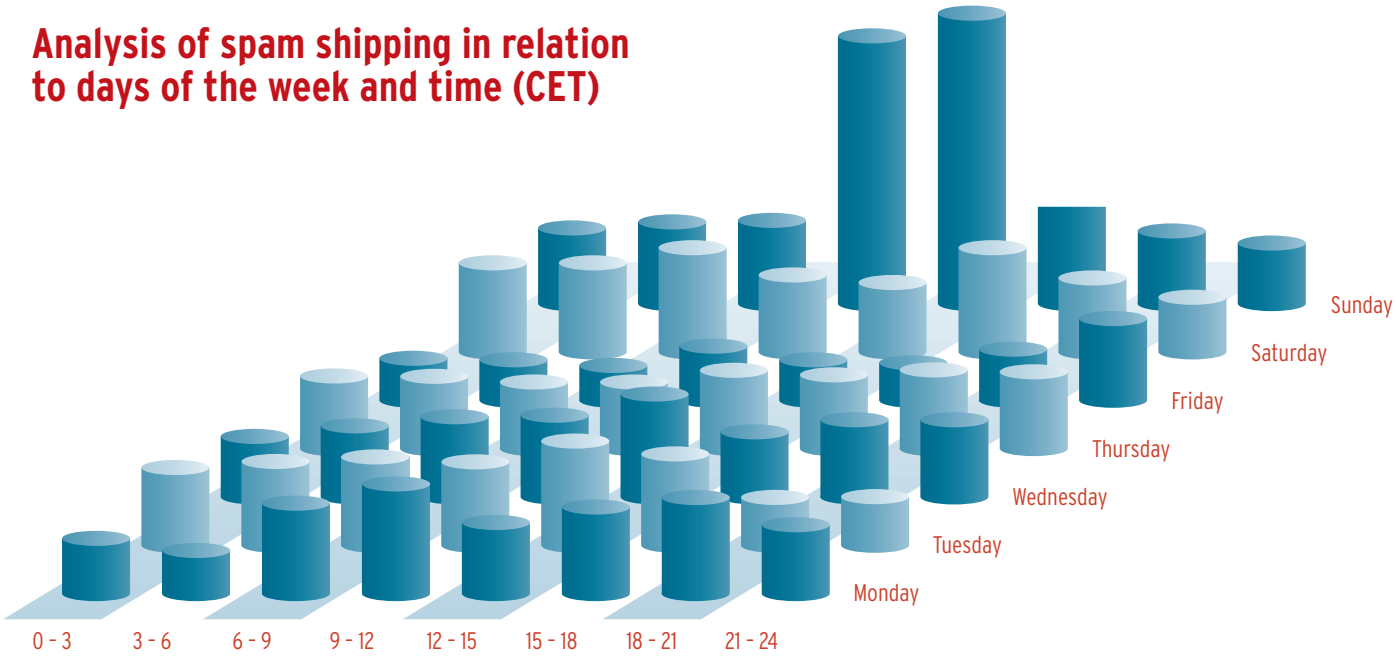
The Spam Top 10

One of the largest spam senders in 2018 was Brazil, which ranked No. 1. The South American country accounted for over 14 percent of the world's total volume of unsolicited mass e-mails. It was closely followed by the Russian Federation, which was only 0.3 percentage points behind Brazil. Japan followed in third place with just under ten percent of the world's spam volume. According to AV-atlas, most contaminated e-mails arrive on Sundays in the morning and noontime (CET).

TOP 10
Spam senders in 2018

1	BRAZIL	14.6%
2	RUSSIAN FEDERATION	14.3%
3	JAPAN	9.5%
4	UKRAINE	5.3%
5	UNITED STATES OF AMERICA	5.2%
6	INDIA	4.6%
7	INDONESIA	4.5%
8	BANGLADESH	3.6%
9	CHINA	2.8%
10	COLUMBIA	2.2%

Analysis of spam shipping in relation to days of the week and time (CET)



AV-TEST GmbH regularly evaluates all relevant protection solutions on the market also with regard to Internet threats. The latest test results can be downloaded for free on the website under https://www.av-test.org/en/antivirus.

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 15 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 15 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 more than 900 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 2018 over 315 product tests alone were run for home user and business user products. As a result, 78,121 malware attacks and 9,026,094 individual data records for false positive tests were deployed and evaluated per product. Throughout the year 2018, this amounted to 3,811,191,904 records evaluated by the test experts. In the monthly Android tests carried out throughout the year, the testers evaluated over 123 individual products. In doing so, each evaluated security app had to defend against 72,818 special Android malware samples. As a counter sample, the experts also recorded over 34,516 scans of secure apps per product, in order to evaluate the vulnerability towards false positives. That is why in lab tests of security products for Android, a total of 7,700,742 scan procedures were analyzed and reproducibly evaluated. 5,035,258 scans hereby involved the specially-developed Android security cluster, which enables parallel real-time tests of Android security solutions.

About the **AV-TEST Institute**

The AV-TEST GmbH is the independent research institute for IT security from Germany. For more than 10 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 proprietary analysis systems 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.

AV-atlas
The Threat Intelligence Platform by AV-TEST

With AV-ATLAS, the AV-TEST Institute offers comprehensive tools for real-time threat analyses.
https://av-atlas.org/en/

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