FACTS AND FIGURES

SECURITY REPORT 2017/18

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

The AV-TEST Security Report

The number of newly developed malware programs remains at a consistently high level. But the stagnation registered since 2016 is deceiving, as it only allows for quantitative statements concerning the risk status. Statements as to the dangerousness of malware in circulation, as well as the damage inflicted, are not reflected in these measured values. It is here, however, where the prospects are not as bright: The amounts of damage, along with the number of newly programmed malware samples, are increasing. Thus, there are no signs of abatement, as evidenced by this year's Security Report from the AV-TEST Institute.

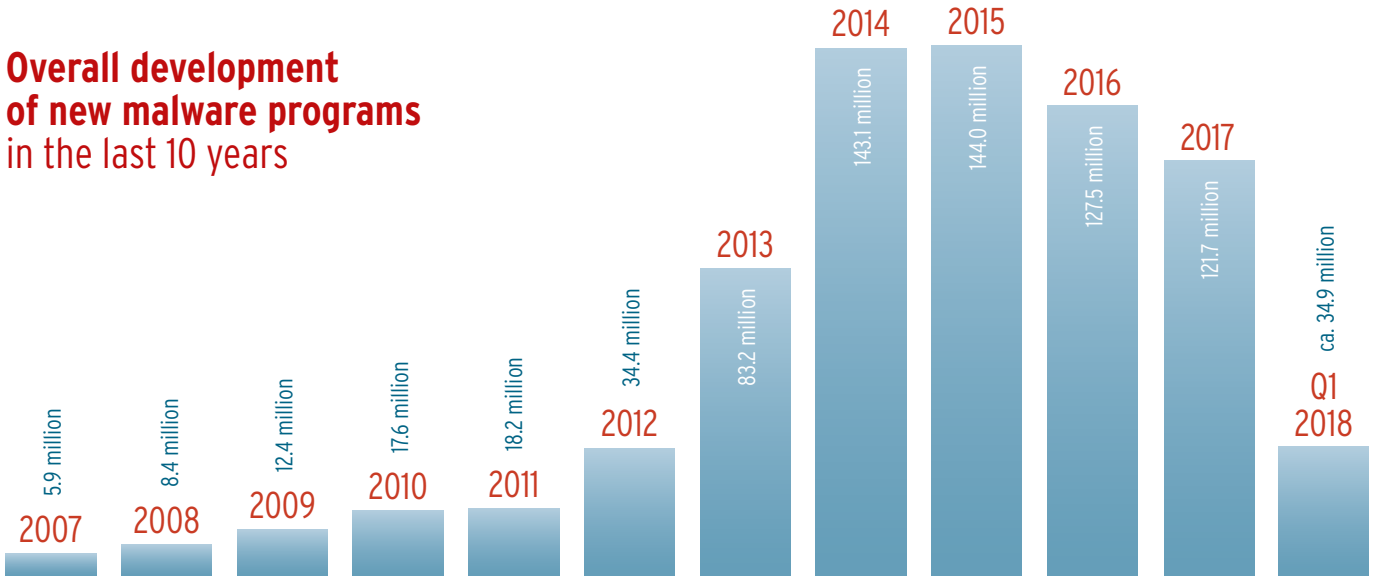
Malware development on a high level

For the year 2016, the detection systems registered declining numbers for newly developed malware, and the AV-TEST Institute predicted this trend also for the subsequent year. And it proved correct, as documented by the 2017 statistics: Last year as well, the number of newly developed malware samples remained below the numbers of the previous year – at least in the first three quarters. In total, this decline is indeed quantifiable, but does not represent a significant change. Whereas in the year 2016, at total of 127,473,381 new malware samples were discovered, in 2017 the total still reached 121,661,167. The speed at which new malware is developed, and to which security systems have to respond, thus declined slightly from 4.0 to 3.9 malware programs per second.

Trend: malware development has doubled

Since 2017, this development, however, has experienced a dramatic swing in the opposite direction: Since October of last year, the detection systems of the AV-TEST Institute have registered practically a doubling of the monthly rates of new malware development. Whereas the measured values of recorded new developments in October 2016 were at just around 7,629,305 samples, they numbered 17,445,659 in the same month one year later. This made last October the month with the second-highest number ever recorded for newly developed malware programs since statistics were first compiled by AV-TEST. Only in August 2014 was a larger malware wave registered.

Overall development of new malware programs in the last 10 years

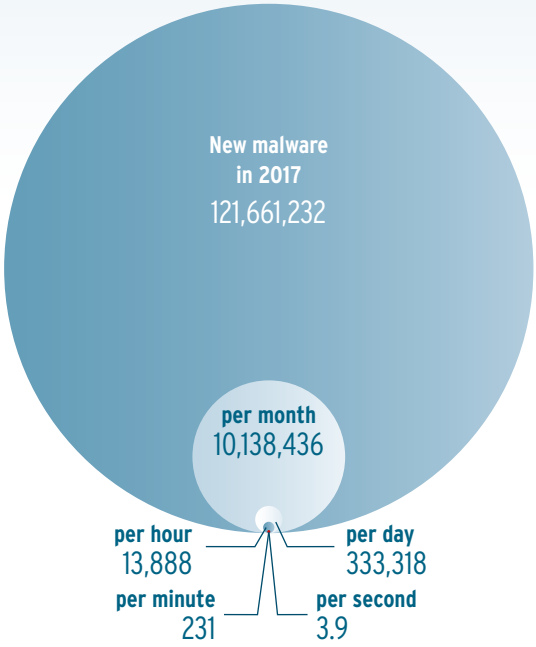


2017 comparable to 2014

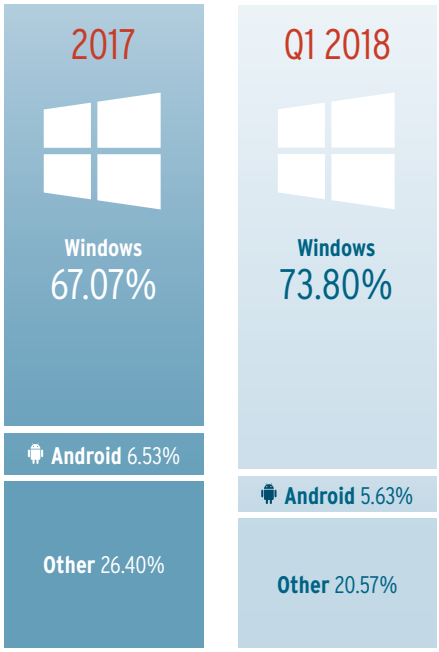
Last year offered cybercriminals similarly favorable conditions for malware proliferation: With „Cloudbleed", criminals found a massive security vulnerability in the server software of Cloudflare used by millions of websites. The freeware „CCleaner" also used by millions was also exploited by attackers for the distribution of malware. And the disclosure of the „Eternal Blue" security vulnerability that had long been secretly used by the NSA offered criminals the opportunity to launch a wide range of ransomware campaigns with malware threats such as „WannaCry", „NotPetya" and „Bad Rabbit", which still persist, albeit with a diminishing level of effectiveness.

The high volume of malware in the last quarter of 2017 reflects a clear trend, as the measurements of subsequent months yielded virtually the same high levels and indicate a doubling of the sample numbers compared to the months of the previous year. An unsettling trend that has been reflected in measurements of the 1st quarter in 2018. To date, the malware database of AV-TEST indicates a total of 771,077,699 malware programs for all known operating systems. Which means that strong virus protection is and will continue to be a clear necessity.

Average malware threat in 2017



Malware detection sorted by operating systems



Ransomware on the decline?

In addition to the purely quantitative assessment of the threat scenario based on proliferating malware samples, a retrospective of the past year compared to the 1st quarter of 2018 also offers additional interesting insights into the economic trend of the „criminal IT industry". This is indicated, for example, by the proliferation statistics of ransomware, which significantly declined in the 1st quarter of 2018. Given the wide fluctuations in the history of ransomware development, however, this short-term observation does not yet allow firm conclusions but only describes the latest trend, which requires further monitoring. Because as an income source, ransomware remains attractive for criminals, which is a function not only of the opportunity for wide distribution per e-mail or through infected websites, but also of the continued strong willingness of the victims to pay, in particular in the corporate sector. Apparently, however, the cybercrime industry has opened up new business models with an even higher „return on investment", yielding even higher profits at the same level of cost.

The age of the crypto miners has begun

And in fact, thanks to the boom involving cryptocurrencies, such as Bitcoin, Litecoin and Ethereum, last year criminals saw the advent of a new and extremely lucrative and sustainable business model. Which, like ransomware, also thrives on the low risk of traceability of anonymous cryptocurrencies, yet at significantly higher profit margins and even lower cost. This involves malware code that shovels digital profits immediately and directly into anonymous online accounts of cybercriminals, minimizing any lost profits – e.g. otherwise occurring due to victims' unwillingness to pay, the restriction to certain operating systems and types of devices, as well as administrative overhead. Thus, it should come as no surprise that the number of malware programs secretly abusing the performance of infected devices to calculate digital currencies, has been experiencing explosive growth. That is why this Security Report dedicates a separate chapter to crypto mining malware from page 11 and goes on to separately document the trend of the latest malware generation in the following chapters based on the security status of individual operating systems.

Windows remains under fire

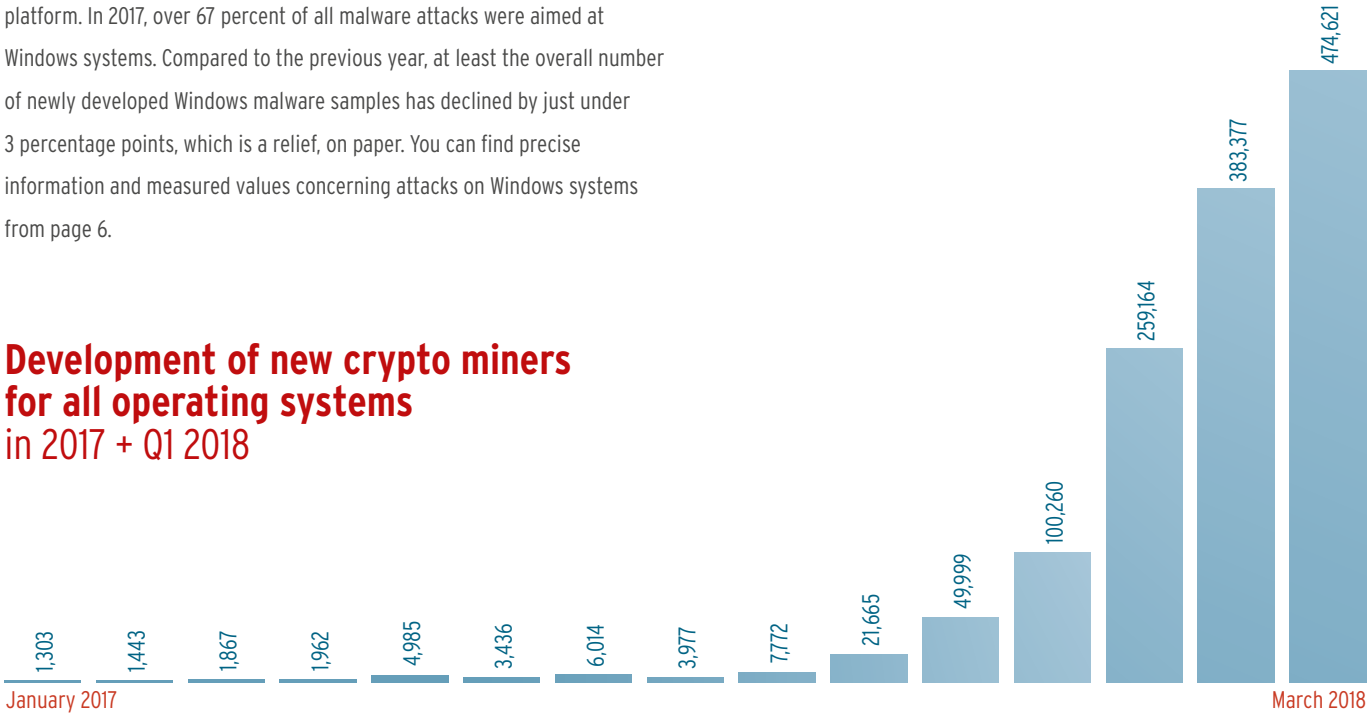
Anyone seeking to efficiently plan and implement large-scale malware attacks is well advised to plant their malware samples in the vulnerabilities of the world's most widely distributed software ecosystem. So, the operating system from Redmond is and will remain the most heavily-attacked software platform. In 2017, over 67 percent of all malware attacks were aimed at Windows systems. Compared to the previous year, at least the overall number of newly developed Windows malware samples has declined by just under 3 percentage points, which is a relief, on paper. You can find precise information and measured values concerning attacks on Windows systems from page 6.

Android remains critical

Conversely, the intensity of attacks on Google's mobile platform continue to increase: 6.5% of all malware in 2017 targeted Android devices. Compared to the previous year, an increase of 0.88 percentage points. What sounds marginal has a devastating effect in reality, as up to now, only few mobile devices under Android provide a security app, much less deploy effective virus protection. At the same time, one out of three Android devices used worldwide is running on an out-of-date version of the operating system (Version 1.1 to 5.1.1) for which no more security updates are available. No more than 5.2% of all Android users are running the current Android 8 aka „Oreo" version equipped with security updates!

Nonetheless, versions of most apps can continue to be run on unsecured devices, including online banking apps and other applications with which critical information is transmitted and legally valid transactions are completed. The situation for attackers almost doesn't get any better than this. After all, the massive availability of devices poorly protected or not at all saves the cost and time-intensive development of new malware programs. Why waste time and money for new „products" if the old ones still yield sufficient profits?

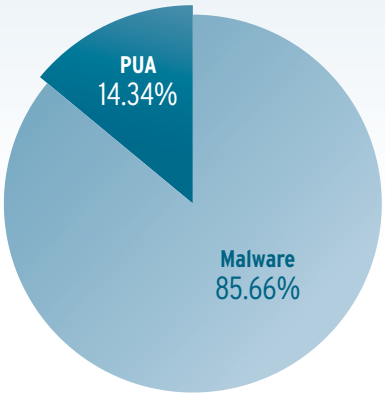
Development of new crypto miners for all operating systems
in 2017 + Q1 2018



Relief for Apple?

Whereas Apple users were confronted with a 370% rate of increase in malware in 2016, the year 2017 brought some relief, at least on paper: The share of total malware volume declined by 0.23%. Nonetheless, this is no reason for an all-clear signal, because many macOS users would probably still reply to the question „Which virus protection software do you use?" by shrugging their shoulders. This does mean, however, that 0.21% of all malware is sufficient for attackers to be successful with macOS users. For this, attackers in 2017 had an arsenal of 37,768 malware programs available. You can find out all the tricks at their disposal starting on page 14.

Ratio of PUA to malware in 2017



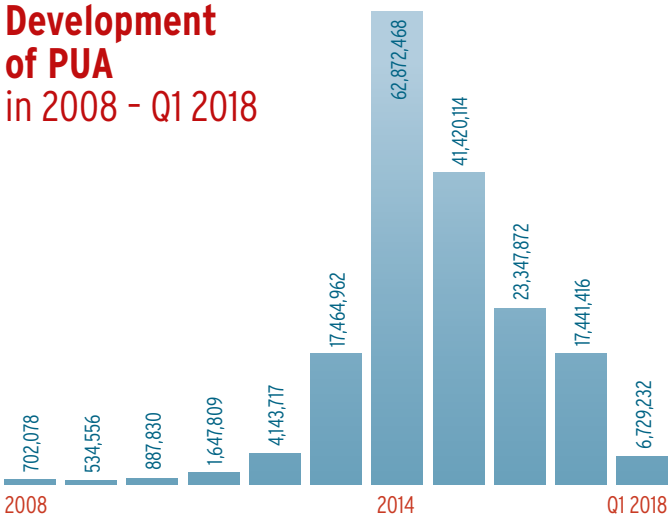
IoT devices in the crosshairs

Already in 2016, storm clouds were gathering for Linux-based systems: The number of newly developed malware programs tripled compared to the previous year. This trend continued unabated in the following year. Compared to 2016, the number of new malware developments increased from 25,671 to 64,087 samples, so that above all Linux-based IoT devices, most of which are connected unprotected to the Internet, ought to be easy prey. You can read about the dangers lurking on routers, smart TVs and the wide and constantly-expanding field of smart-home devices, and why the Internet of Things is especially in the crosshairs of cybercriminals, from page 23.

User tracking on the decline

When we look back on how last year developed, there was also some positive news, however. Thus, we can report that there was continued decrease in 2017 of the spying on user behavior by means of potentially unwanted applications (PUA). Unlike the malware detected by the AV-TEST systems, while PUA do not constitute a direct threat for infected systems, these spy programs do secretly record data, pop-up unwanted advertising and can noticeably ramp down the performance of hardware. That is why it was at least positive to report a noticeable decline in PUA.

Development of PUA in 2008 – Q1 2018



Trend 2018

This Security Report encompasses not only the data status for the year 2017 but also takes into account the measured values of the AV-TEST analysis systems for the first quarter of 2018. Thus, it is already possible to recognize trends for the current year, backed up by data. Whereas the overall malware trend in 2017 was still declining, it was on a noticeable upturn in the 1st quarter of 2018. January already started off with strong increases in malware. While virus scanners were required to defend against 8,852,322 new malware programs in the first month of the previous year, this January they were already subjected to 13,695,241 such programs.
This trend continued consistently in the measured values of the entire 1st quarter of 2018.

Security Status
WINDOWS

After a phase of relief, the number of attacks by new Windows malware noticeably picked up again in 2017. But not only the quantity of malware programs is increasing. New, sophisticated attack variants make the defense more difficult and create decisive economic advantages for cybercriminals.

Number one target of attack

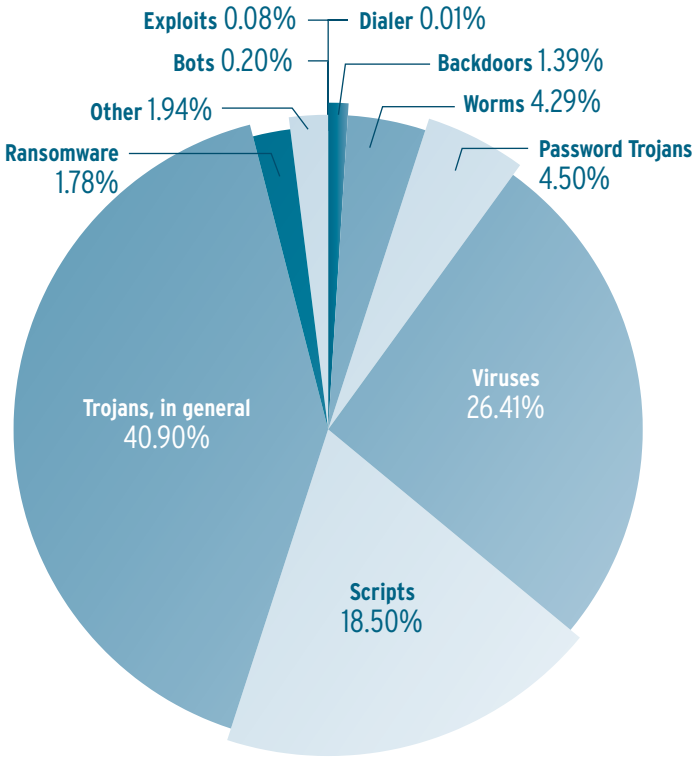
Measured in terms of worldwide user numbers, Windows remains the number one operating system. The players in the „malware industry" are in full agreement, and so Microsoft systems are still cybercriminals' main target of attack. While the number of new malware developments has declined since 2015, last year it experienced a noticeable rebound. As a result, the detection systems of the AV-TEST Institute determined for 2017 the overall total of 81,598,221 in newly developed malware samples, registering a 14% increase over the previous year (71,430,700 samples). Seen overall in terms of all operating systems, more than 67% of all malware programs targeted Windows users in 2017.

Forced to innovate

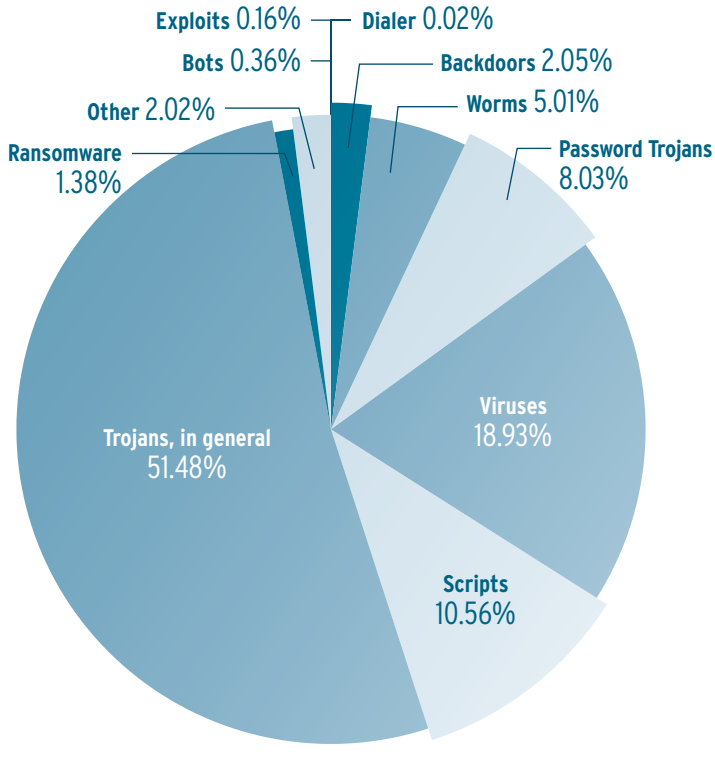
One cause for the increasing activity in the development of new Windows malware samples could actually be a positive trend. Because last year, Microsoft managed to significantly boost the immune system of Windows through clear improvements of the defense mechanisms in the operating system. As a result, the internal system malware defense, „Windows

Distribution of malware under Windows

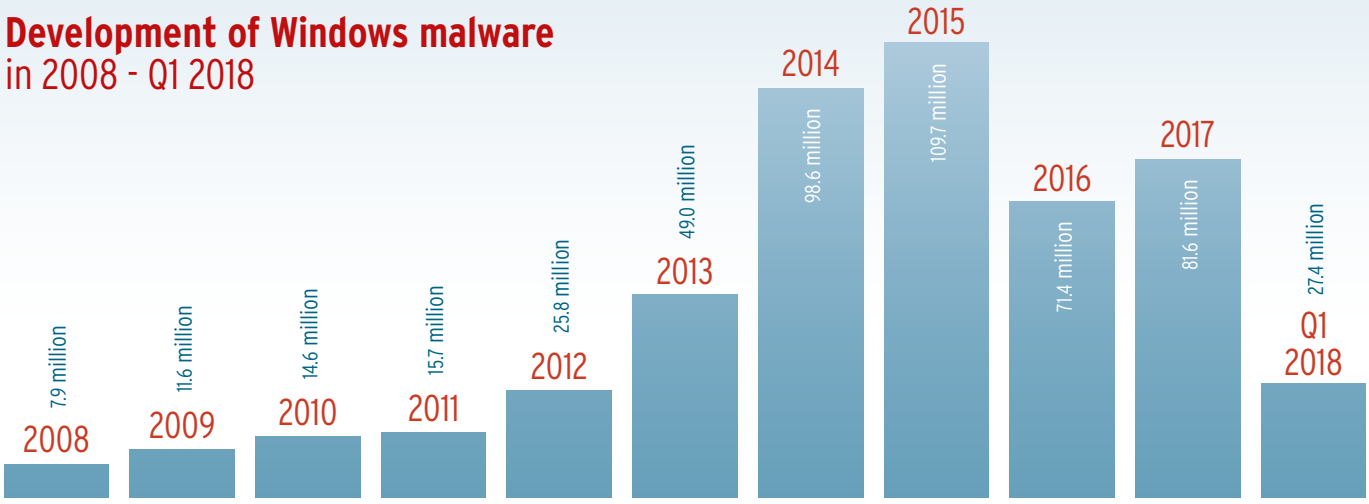
2017



Q1 2018



Development of Windows malware in 2008 - Q1 2018



Defender" and „Security Essentials" achieved significantly higher detection rates in the AV-TEST Institute's annual tests than in recent years.

Conversely, this trend, however, means for criminals that they have to adapt their „products" to the new scenarios, should they continue to seek business success with their malware programs on Windows systems. This became apparent above all in the last quarter of last year, because since October 2017, the number of new malware developments doubled over the previous month. This exponential leap later tapered off, but since that time, it has remained on a significantly higher level than in the previous quarters of the year 2017.

Distribution of malware under Windows

A look at the distribution of various malware types for Microsoft operating systems indicates the form of attacks that criminals in 2017 found the most promising. The quantitative analysis of the distribution of new malware codes provides insights into which malware classes criminals invested the most time and money in 2017, and at least provide clues as to which criminal „business plan" was the most lucrative in the mass proliferation of malware code. It should be considered that the relevant developments throughout the year are also subject to additional factors, such as the discovery of exploitable security vulnerabilities in operating systems or standard applications running on them.

Disguising, spoofing, spying, stealing

With a total of 40% of all malware programs for Windows, Trojans very clearly dominated the arsenals of cybercriminals in 2017, however, security programs define malware samples of all types under this general category. The fact that criminals choose these means should come as no surprise, after all, successfully infiltrated Trojans are able to unleash virtually unlimited destruction on infected systems. By corresponding malware functions, the malware code allows attackers access to the system and offers the opportunity of uploading any number of malware codes after the fact. In addition to clandestine transmission of all types of stored data, Trojans are also equipped with a comprehensive arsenal of additional malware functions, which is why they are considered the „Swiss Army knife" in the toolbox of cybercriminals, with which they can not only steal data, but can also restrict, block, delete and modify it.

Moreover, Trojans offer their masters comprehensive spying functions; in addition to opportunities to capture passwords for various online accounts or the targeted search for certain files, they also allow secret activation of built-in cameras and microphones. This function makes them interesting not only for criminals but also for police and other government surveillance agencies in many countries.

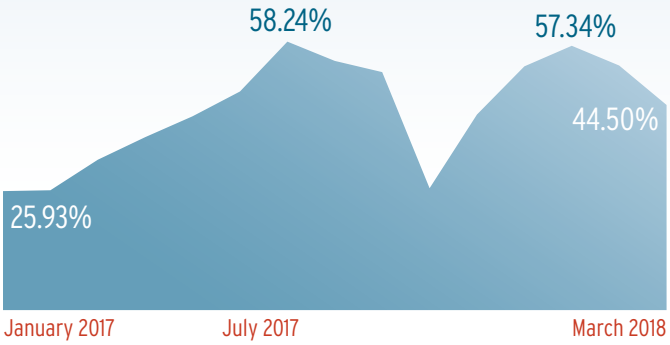
In addition to their flexible malware code, the increasing attractiveness of Trojans is also buoyed by the many opportunities for distributing them. Disguised as an e-mail attachment or a freeware program download, embedded in other applications or as a drive-by download when visiting infected websites – the opportunities of distributing Trojans on a wide scale are as myriad as the comprehensive malware functions are numerous.

This is also underscored by the growth rates of this class of malware: Whereas Trojans were still in third place among Windows malware programs in the last AV-TEST Security Report with 23.74% – behind viruses (37.6%) and worms (25.44%) – things turned around dramatically in 2017. In this, it is interesting to observe that the already high ranking of Trojans in malware statistics of the AV-TEST Institute's detection systems is also joined by additional sub categories of this malware class. Given their special malware functions, AV-TEST tracks banking Trojans and ransomware separately and not under the general category of „Trojans".

TOP 10 Windows malware in 2017

1	RAMNIT	21.54%
2	AGENT	13.78%
3	VIRUT	6.37%
4	VIRLOCK	6.25%
5	ALLAPLE	4.69%
6	VB	3.98%
7	SIVIS	2.39%
8	UPATRE	2.03%
9	INJECTOR	2.00%
10	KRYPTIK	2.00%

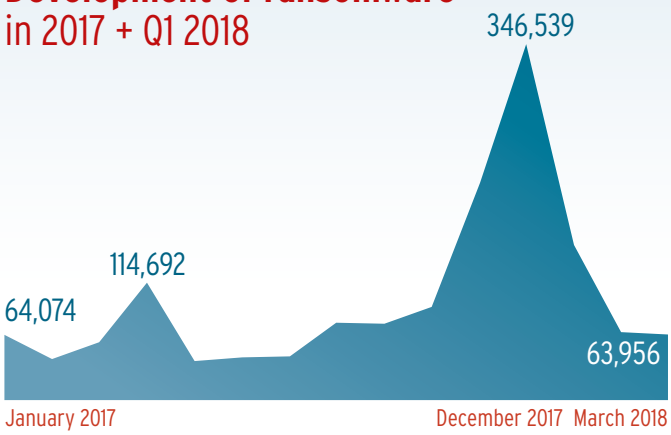
Development of Trojans, in general, in 2017 + Q1 2018



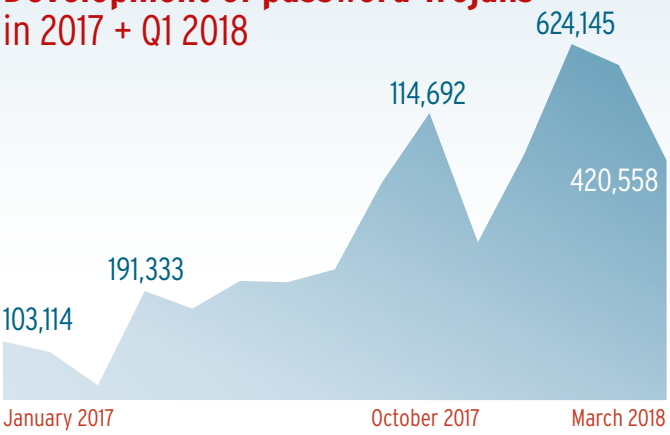
The year of digital blackmail

The year 2017 was not only reported in the media as „Year of Ransomware", the growth rates measured by AV-TEST also confirm that digital blackmail has become established as a reliable business model for cybercriminals. Compared to the previous year, the number of blackmail Trojans increased from 0.94 to 1.78 percent, practically doubling in size. Despite the low proportion of ransomware with respect to all malware programs registered, the success model of this malware should not be taken lightly. Because even with a small number of victims, cybercriminals already earn big profits with ransomware, at a relatively low overhead compared to other malware programs. And thanks to anonymous online currencies, the money flows immediately and directly into their accounts, without any additional overhead and with a very moderate risk, yet with maximum damage for those affected.

Development of ransomware in 2017 + Q1 2018



Development of password Trojans in 2017 + Q1 2018



Cybercrime attacks with NSA support

The consequences of the NotPetya ransomware were extremely drastic. The global logistics firm, Maersk, alone reported damage amounting to several hundred million dollars. With its container vessels, this shipping company transports just under 20% of the entire world trade. Due to the ransomware attack on June 27, 2017, it suffered a total failure of all IT systems: 45,000 client computers, as well as 4,000 servers around the globe were said to have failed; in a 10-day Herculean feat, technicians reinstalled or restored 2,500 different programs, reported Maersk Chairman Jim Hagemann Snabe at this year's World Economic Forum in Davos. The Chairman of the Board said that in fact, the company actually came out mildly, as normally it would've taken the global Maersk Logistics six months to get everything back up and running.

Other companies, including the pharmaceutical giant Merck, which suffered damages of over 300 million as a result of the NotPetya attack, along with the logistics company FedEx, were among the victims. But like Maersk, they were not even the actual target of the ransomware attack, as there was never any ransom demanded during the attack. The common thread of all those affected was that they had business operations in Ukraine and accordingly had to pay taxes there. And thus, they became collateral victims of a targeted attack against the tax software MeDoc used mainly in Ukraine. The attackers distributed NotPetya from April 14 to June 22 in three waves of attack as an infected program update of the Ukrainian tax software. There is a high probability that NotPetya was a targeted state cyber attack against Ukraine.

For the NotPetya attacks, the perpetrators used exactly the same Windows vulnerabilities that had been exploited for government attacks – these, however, came from an entirely different place. Already in August 2016, the hacker group „Shadow Brokers" published part of the program code of a cyber weapon that they captured during a hack of the NSA department „Equation Group". This 256 MB file provided at least a small inkling in 2016 as to the enormous potential in the government-developed malicious code. The situation, however, only became volatile on April 14, 2017. On that day, „Shadow Brokers" decided to publish the entire code of the cyber weapon on the Internet – the launch of the ransomware „WannaCry".

How long the NSA used the now freely-accessible exploits by the name of „Eternal Blue" in the server message block (SMB) of virtually all Windows systems (CVE-2017-0144) is disputed. Some estimates suggest it was over five years. The fact is that Microsoft patched the vulnerabilities of the network protocol under the ID „MS17-010 – Critical" on March 14, 2017. May 12 marked the launch of the first widespread cyberattacks of WannaCry. And as it turned

out, the decisive security update from Microsoft had not been installed for two months on at least 230,000 computers in 150 countries. Those affected included above all hospitals in the UK, but also large companies such as FedEx, Renault, Nissan, Deutsche Bahn, as well as the Chinese oil company PetroChina. Even government bodies such as the Russian Ministry of the Interior, the Romanian Foreign Ministry and Internet service providers such as Telefonica and MegaFon were suddenly confronted with digital blackmail, to be paid in Bitcoin.

In October 2017, the ransomware „Bad Rabbit", primarily geared towards Eastern Europe, shut down the Russian news agency Interfax, as well as the airport of Odessa, the Metro in Kiev, along with several Ukrainian ministries. The malware also cropped up in Russia, Turkey, Japan and South Korea, as well as Germany and the United States. Some „old adversaries" from the ransomware family, e.g. the malicious codes „Cerber" and „Locky" (see Security Report 2016/17) were also still up to their destructive game in 2017.

Whereas Internet worms were still ranked No. 2 in 2016 with over 25% of the malware programs deployed by cybercriminals, in 2017 they were practically no longer further developed. Reaching a mere 4.29%, last year they were part of a rapidly extinct class.

Trend 2018

The development of new ransomware exhibited a severe decline in the first quarter of this year. The share in terms of overall malware registration dropped from 1.78 to 1.38 percent. A measurable value, which allows no conclusive statements on the development of this category of malware throughout the entire year of 2018. It can be presumed, however, that cybercriminals who gained initial experience with ransomware have moved on to a new and more lucrative business model, also based on cryptocurrencies, which is even more attractive. For this reason, the Security Report is dedicating a complete chapter to the malware category of coin miners.

The rate of new developments of Trojans in general is increasing by over 10%. In this, at least every other malicious code programmed in the first quarter of 2018 is a Trojan. There is an even clearer trend in separately recorded password and banking Trojans: Their number nearly doubled from 4.52 to 8.03 percent. Conversely, the proliferation of traditional viruses has continued to fall below 20% of the entire share of detected malware.

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/.

Breakthrough of CRYPTO MINERS

The anonymity of many cryptocurrencies guarantees cybercriminals optimal business platforms. Because currencies such as Bitcoin offer direct extortion of victims without having to involve intermediaries. This minimizes risk, and at the same time saves on „personnel costs". That is why even criminal visionaries rely on the blockchain. In 2017, the malware industry increasingly developed malicious code for mining digital currencies by exploiting third-party resources.

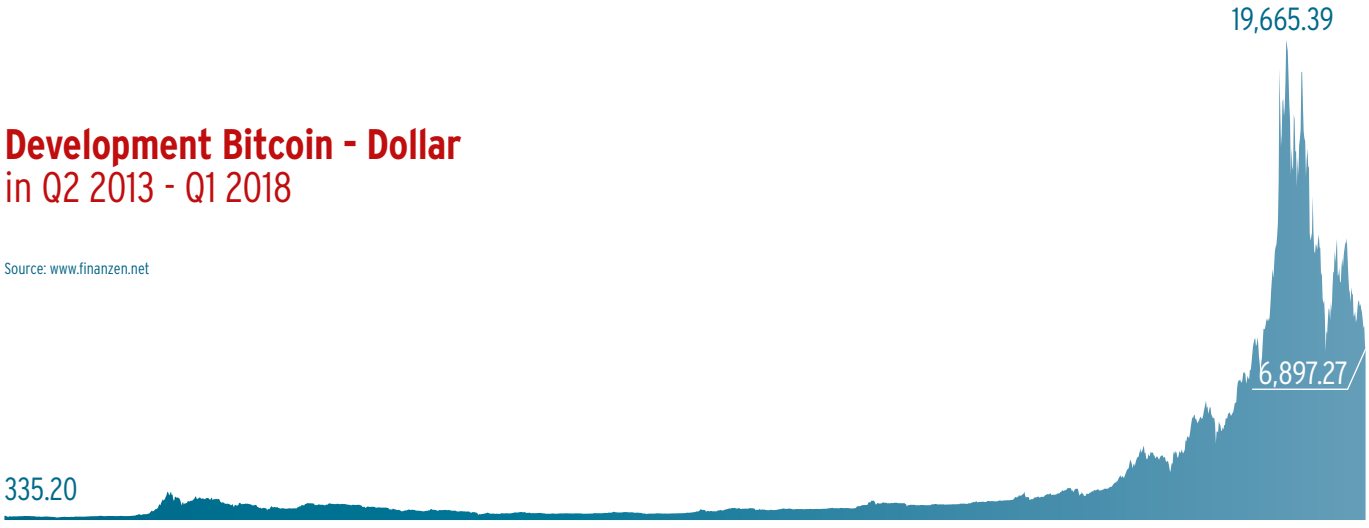
Anonymity is attractive

Through the successful use of ransomware, cybercriminals have already gathered positive experiences with cryptocurrencies. Because the use of digital currencies, whose basic principles involve anonymous use, is already an attractive feature per se for criminals. The lack of regulation by banks or other equivalent institutions is another basic pillar of over 4,500 cryptocurrencies currently in existence. Only roughly 1,000 of them are actually traded, but unlike the crypto money Bitcoin, first launched in 2009, all others enable the virtually anonymous exchange of large sums of money. As a launch currency with by far the largest market capitalization, the conversion of large Bitcoin sums into hard currency, however, is heavily monitored. With US$153,225 million, today's most well-known digital currency now accounts for 37 percent of the overall volume of all cryptocurrencies in existence. Bitcoin exchanges can only be made to a regular bank account and are thus personalized and in turn traceable. Since 2014, companies such as Chainalysis have analyzed and monitored Bitcoin transfers, documenting them and creating relationships between blockchain addresses and real accounts for the US fiscal authorities, among others.

That is why criminals have been flocking to cybercurrencies under less scrutiny and with less distribution such as Litecoin, Ethereum, EOS, Tronix and Monero. These also follow the principle of anonymous financial transactions. This means that both the owners of digital coins and the amount of cryptocurrency owned by them remain anonymous thanks to individual encryption. The same is true for transaction partners. Although all the transactions made within a currency system are publicly visible, no one knows who is making them, however.

Development Bitcoin - Dollar
in Q2 2013 - Q1 2018

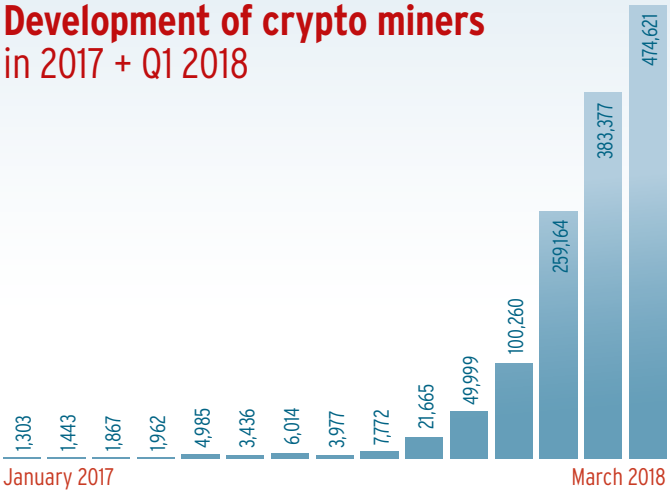
Source: www.finanzen.net



Stealing or mining

In principle, there are two ways for criminals to obtain digital currency. The first consists of searching through third-party computers for stored coins and stealing them. The balance of a cryptocurrency consists solely of a relevant numerical code. It provides information as to the number of coins within the system of a cryptocurrency. These numerical codes can be stored as a secret private key, but also translated into barcode and printed out. This makes the keys for accessing a balance, however, easy prey for computer criminals. Similar to passwords, they can be spied on and stolen using malware programs. Due to the low distribution, however, attacks are only worthwhile if the victim is known, the attack can be targeted, and access can be gained to a sufficient quantity of poorly-secured coins. After all, such targeted attacks require some planning and are appropriately complex.

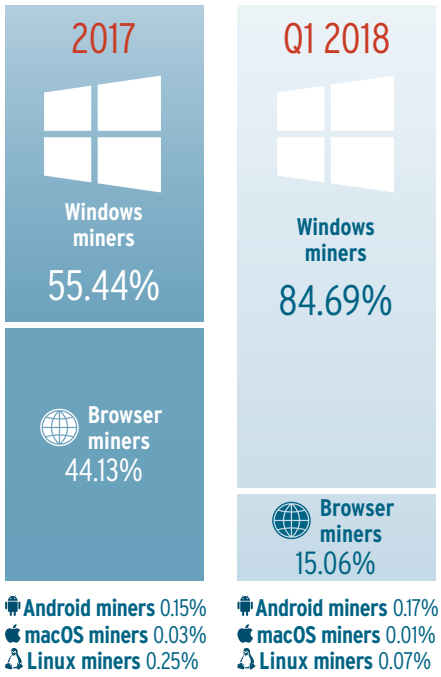
Development of crypto miners in 2017 + Q1 2018



The second way of obtaining cryptocurrencies at other people's expense requires significantly lower overhead, which is why it is much more lucrative: the mining of cryptocurrency through exploitation of third-party CPU resources. The computing power of third-party hardware is used to solve cryptographic tasks within the crypto blockchain. As a „reward" for the right answer, the appropriate blockchain issues shares of the currency predefined in it. When launching a currency blockchain, the computational tasks for mining are relatively simple and can also be completed with a low computing workload. Each cryptocurrency is a self-contained system with a predetermined coin quantity and a predetermined total value. With each coin mined within such a currency system, however, the complexity of the computing tasks, and thus the necessary computing power, increases. Users can create pools and combine the computing power of their hardware to mine in a network. Sometimes, this activity operates in a gray area, however, where the mining function is hidden in free applications for smartphones and tablet PCs, for example. Browser addons, with which operators of online services make their users mine for them during the dwell time on the website, are also becoming increasingly widespread.

And this is precisely where the cybercriminals come in: Instead of extorting cybercurrency from their victims via ransomware, from the fourth quarter of 2017 they increasingly turned to using the CPU power of infected hardware for coin mining. Since September of last year, the detection systems of the AV-TEST Institute have measured a significant increase in the number of samples of coin mining malware, which increased exponentially into the first quarter of 2018. Whereas during mid-year, the number of new developments of mining malware averaged 3,500 samples per month, the rate doubled from September and since then has risen almost unabated to 470,000 new samples per month. By the time this report was completed, the sum total of mining samples collected by AV-TEST since 2010 had already exceeded one million.

Distribution of crypto miners by operating systems

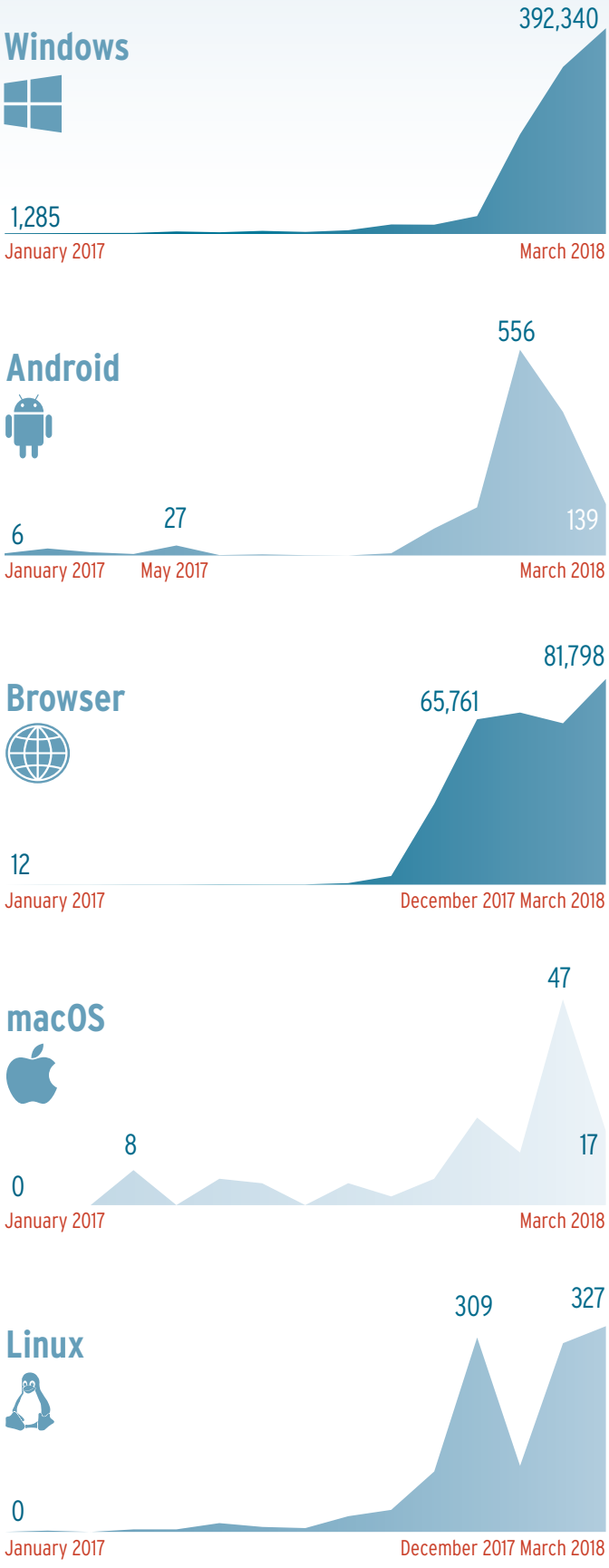


Windows becomes a mining platform

A look at the distribution of mining malware by operating systems clearly indicates that criminals are still developing their business model in 2017. At that time, more than half of all coin miners are targeting Windows systems (55.44 percent). The other half (44.13 percent) is trying to siphon off the CPU power of infected hardware via browsers and other Internet connectivity software.

This changes dramatically in the first quarter of 2018, as the number of coin miners for Windows systems rises disproportionately by almost 30 percent to 84.69 percent. As with other malware, cybercriminals are targeting their bread-and-butter Windows systems as their main target. It remains to be seen whether this is merely a trend. Perhaps the potential computing power to be hijacked is an argument for relying on Windows, as opposed to platforms such as Android or different IoT devices. However, due to the high acceptance of antivirus software here, there is also a higher risk that newly programmed malware will be quickly detected. It remains to be seen whether criminal software developers will switch to other, less closely-monitored operating systems, exploiting virtually unprotected resources from IoT devices or continue a systems-agnostic approach, working with browser malware. In this context, it should not be forgotten that cryptocurrencies still represent virgin territory even for noncriminal economists. In this respect, the fact that cybercriminals are already using malware for cryptocurrencies speaks for their speed of innovation. Due mostly to the lack of regulation with regard to new technologies, such „new markets" are of particular interest to criminals, especially in their early stages.

Development of crypto miners in 2017 + Q1 2018



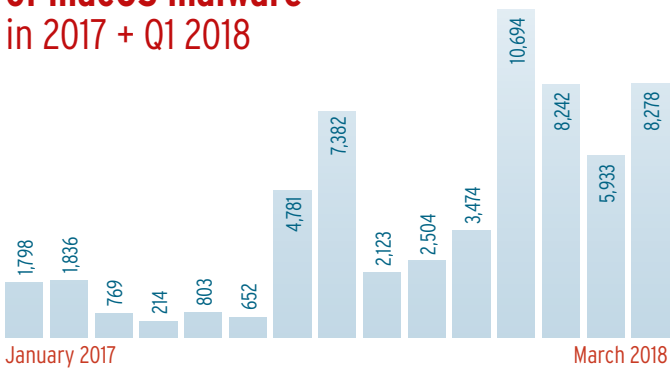
Security Status macOS

On the one hand, Apple users are only affected by a negligible proportion of newly programmed malware. On the other hand, a proper antivirus application is not running on every Mac machine. However, as malware development for the operating system from Cupertino indicates, this would be advisable. Because the malware percentage for the Apple universe is constantly increasing.

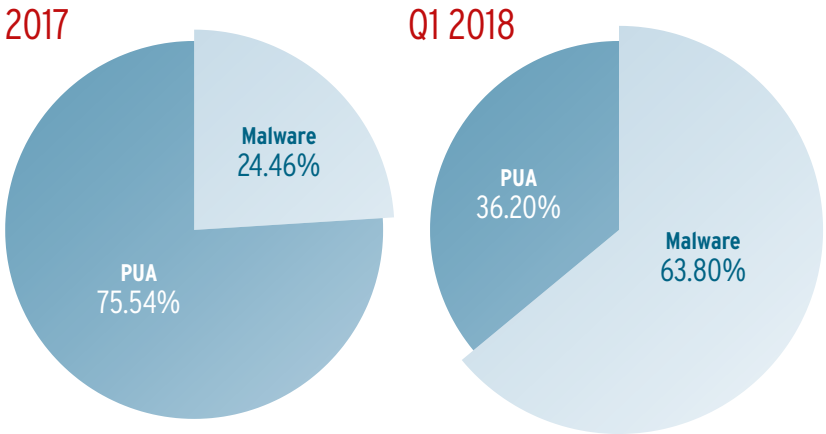
Fivefold increase in macOS malware

In last year's Security Report, the AV-TEST Institute's measurement systems recorded a dramatic increase in malware figures for macOS of 370 percent over the previous year. This development relentlessly continued in 2017. While a total of 6,959 newly programmed malware samples targeted Apple computers in 2016, this figure increased fivefold to 37,030 new malware samples last year. In this, the volume of malware developed for macOS has been increasing steadily for ten years now, reaching a sum total of 78,929 samples when this report was completed.

Development of macOS malware in 2017 + Q1 2018



Distribution of malware under macOS



Development of macOS malware in 2008 - Q1 2018

Malware surpasses PUA

This means that in December for the first time, new malware for Mac exceeded the number of unwanted spy applications (PUA) in terms of new malware development. While the spyware tools of the advertising industry remained the primary threat to Apple users – and especially to their privacy – into December 2017, the tide has since turned, and the malware authors are now taking over the helm.

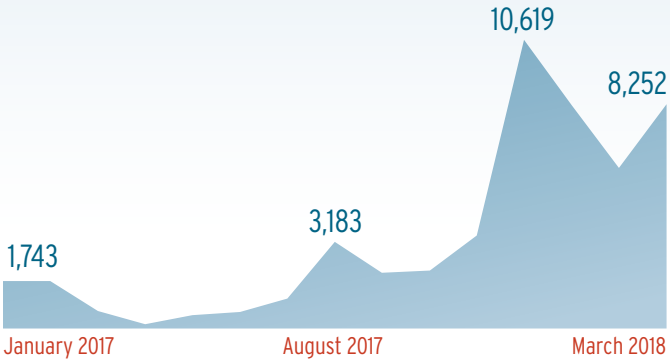
macOS under fire from Trojans

In 2017, four out of ten malware programs for macOS were Trojans (40.93 percent). Otherwise, malicious scripts played an outstanding role with 12.66 percent in the malware detected and analyzed by AV-TEST systems. Viruses, worms and other types of malware categories relevant on Windows systems, for example, are irrelevant or at best play only a minor role for Mac computers, and do not show up as a percentage. Ransomware so widespread on Windows systems practically does not occur on Mac systems.

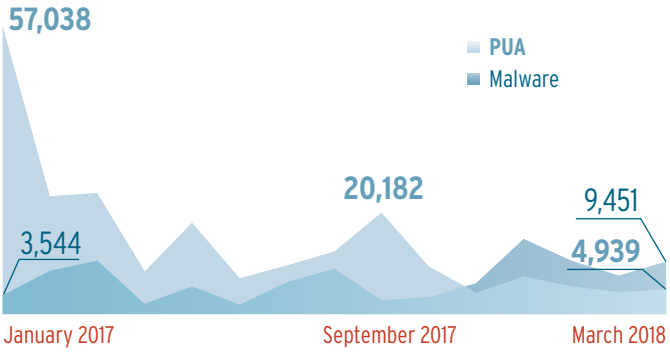
TOP 10 macOS malware in 2017

1	FLASHBACK	35.75%
2	MACONTROL	22.30%
3	FBJACK	20.93%
4	MACKONTROL	6.46%
5	KERANGER	3.38%
6	HACKBACK	2.71%
7	FACELIKER	1.50%
8	MORCUT	0.96%
9	OLYX	0.83%
10	KRYPTIK	0.57%

Development of Trojans, in general, under macOS in 2017 + Q1 2018



Development of malware distribution under macOS in 2017 + Q1 2018



Trend 2018

The dominance of Trojans in macOS systems continues dramatically into the first quarter of 2018, doubling in number and reaching over 86 percent of the total amount of malware written for Apple. The distribution of new scripts is thus diminished from 12.66 to 0.04 percent. The number of newly authored malware samples (63.8 percent) exceeds the newly developed PUA samples (36.2 percent) by a ratio of 3:1 and thus creates a completely different threat scenario for the Apple cosmos.

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 ANDROID

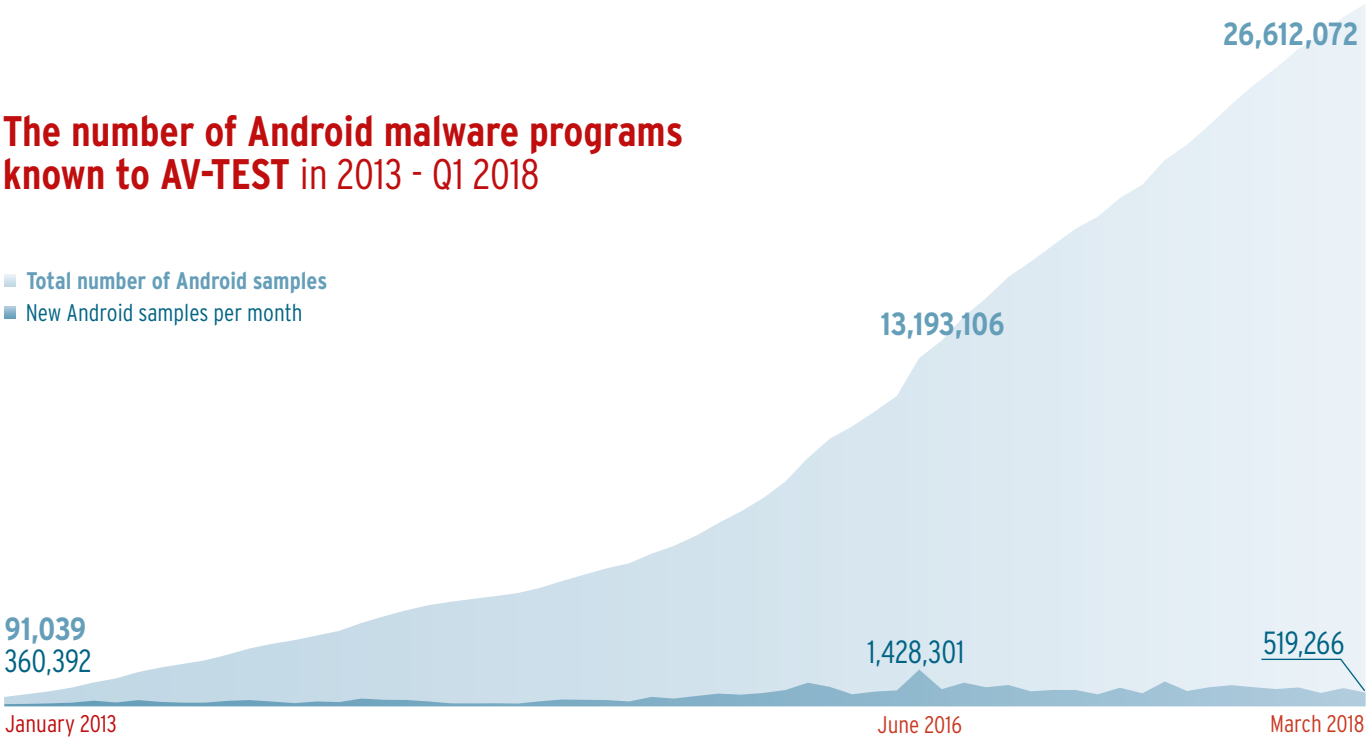
Android users are increasingly coming under fire: The number of malware programs for Google's operating system has more than doubled compared to the previous year. But not only the volume of malicious code is constantly increasing, the complexity of the attacks is also intensifying. In addition, the malware developers of mobile malware made some fundamental decisions with significant ramifications.

Android – the ideal target for attack

At 6.53 percent, only a very small portion of the total malware in 2017 targeted Android devices. In comparison to more than 67 percent Windows malware, this looks negligible. However, Android is the main target of cybercriminals after Windows. One reason for this is naturally the widespread distribution of Android devices. According to StatCounter, two out of three smartphones worldwide run on Google's operating system. Another reason is due to the fact that unlike Apple's iOS, Android is an open system. This means that the resources for app development are open to everyone and that, in addition to Google's Play Store, other platforms for distributing Android apps, and thus malware, are also available.

Add to this the high market diversity of various manufacturers with a large number of different devices. It plays into the hands of cybercriminals that many of these devices are not supplied with the latest Android version and therefore are not running at the latest patch level. According to Google, the current Version 8 aka „Oreo" has been installed on not even two percent of the devices at the time this report was created. And last but not least, security software is not installed on every Android device by any means. All in all, these are optimal opportunities for attackers to earn money with Android malware, because the devices offer almost identical functionality and connectivity to corresponding online services just like Windows PCs.

The number of Android malware programs known to AV-TEST in 2013 - Q1 2018



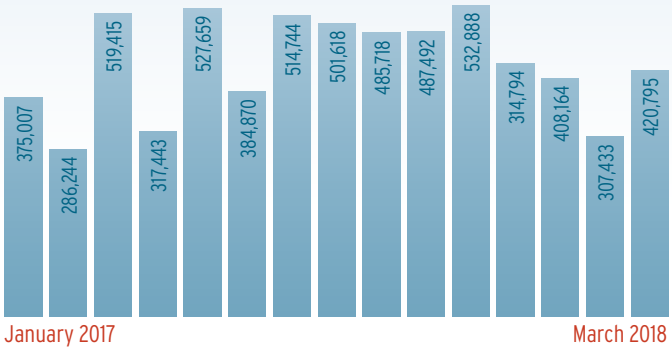
As a result, the number of malicious apps has been steadily increasing since the introduction of Android. At the time this report was completed, the number of Android malware samples collected by AV-TEST was exactly 28,335,604 million. It is interesting to note that with the exception of a few peaks, the development of new malware has been declining steadily since May 2016.

Android ransomware on the decline

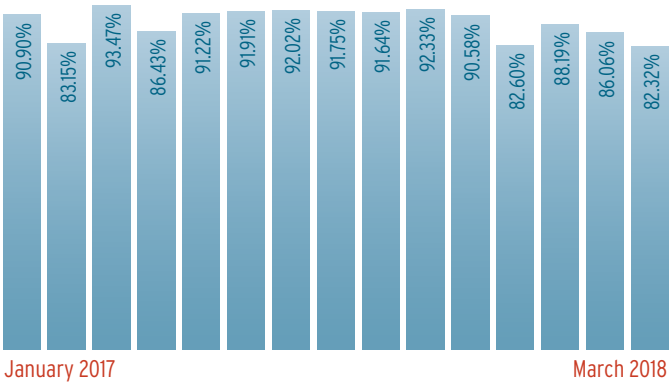
In 2017, anyone talking about Android malware was basically referring to Trojans. Representing over 90 percent of all Android malware programs, they are the all-round tool of cybercriminals. They are suitable both for spying on data and for reloading other malicious codes. They can also include more highly-specialized Trojans like ransomware, for example. And indeed, the AV-TEST systems recorded a noticeable blip of over 2.5 percent of the total share of malware for this category in the second quarter of 2017. After that, the wave of registered blackmailer malware codes declined again to barely measurable values.

This could mean that ransomware on mobile devices does not pay off for criminals. One reason for this is certainly that users store far less and possibly less important data on the relatively small storage space of most mobile devices compared to PCs. As thus far, most ransomware attacks can still be defused by performing a factory reset on the devices, the willingness of victims to pay is presumably much lower than with infected PCs. AV-TEST will continue to monitor the development of Android ransomware.

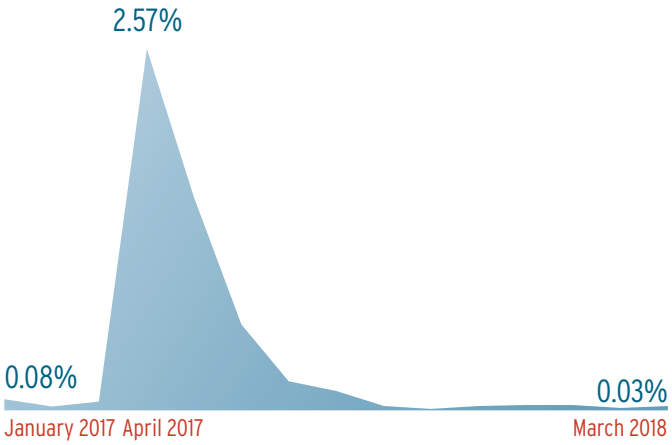
Development of new Android malware in 2017 + Q1 2018



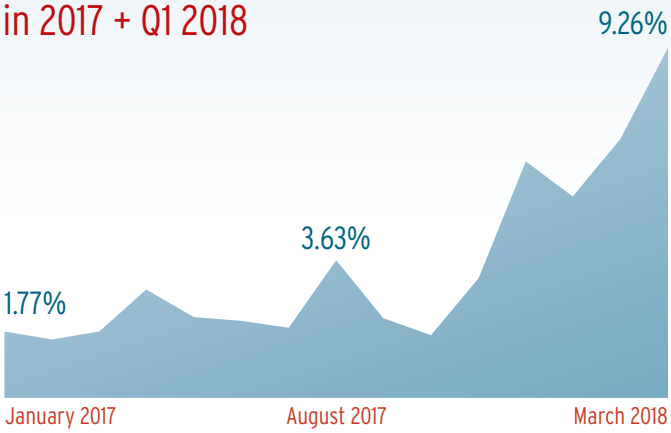
Development of Trojans, in general, in 2017 + Q1 2018



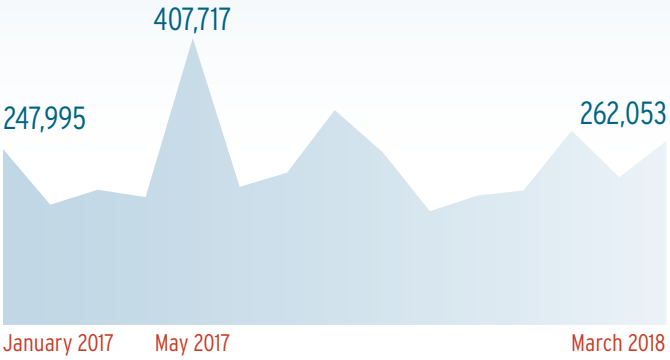
Development of ransomware in 2017 + Q1 2018



Development of password Trojans in 2017 + Q1 2018



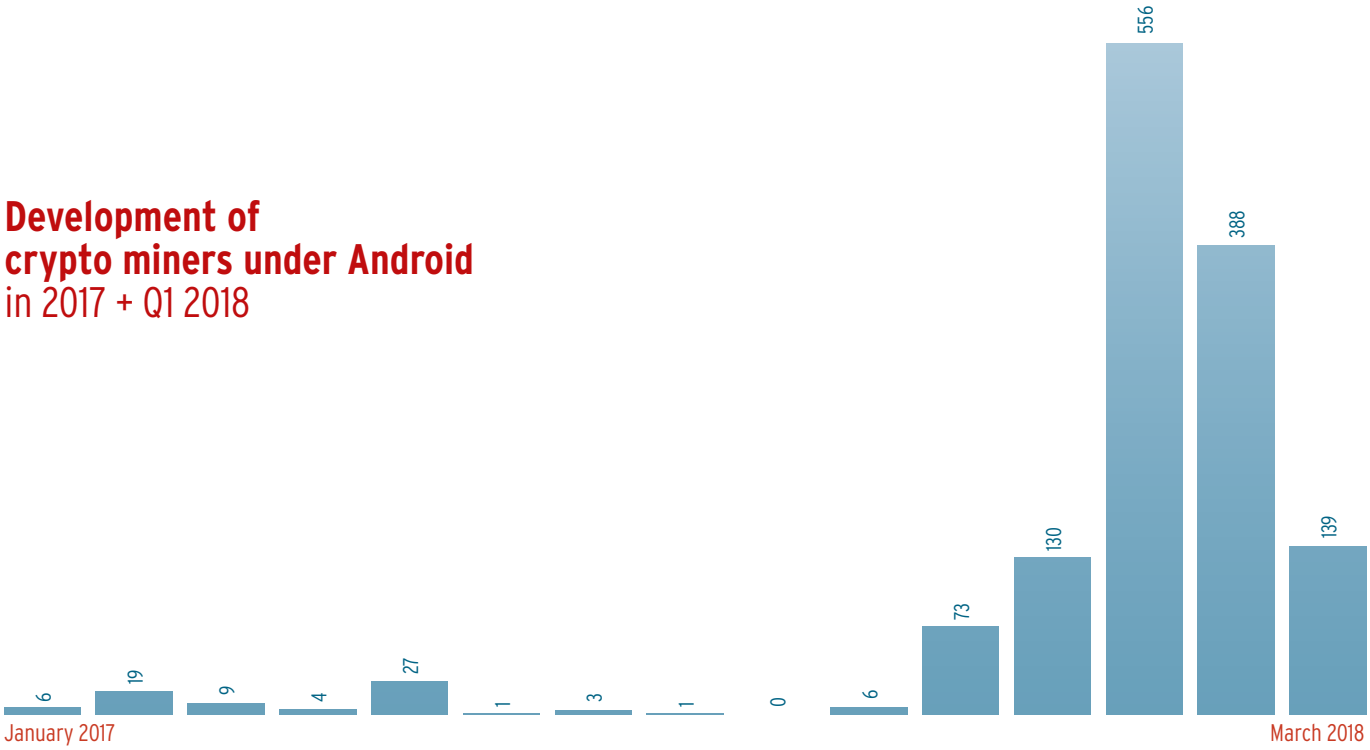
Development of new PUA samples in 2017 + Q1 2018



Number of banking Trojans tripled

Instead attackers in 2017 increasingly and directly targeted the accounts of mobile device users. Banking and password Trojans experienced a relevant boost last year. At the beginning of the year, the share of this Trojan category was still below 2 percent yet had already tripled to over 6 percent by the end of the year. Obviously, malware developers are benefiting from the increasing trend to handle more and more banking transactions and purchases via smartphones and tablets, as well as through corresponding apps.

Development of crypto miners under Android in 2017 + Q1 2018



PUA lagging behind Malware

Another significant event over the past year has been the development of new spyware programs in the advertising industry. The main task of these unwanted applications, operating in a legal grey area, is to analyze user habits and locations for the customization of pop-up advertising. At the same time, most of the PUA samples detected and evaluated by the AV-TEST systems are characterized by the annoying insertion of advertising, e.g. on home and lock screens, but also during app use. There is positive news from the year 2017, because the number of new developments in advertising spyware is measurably decreasing. While the advertising mafia launched 4,222,713 newly developed PUA samples in 2016, Android users were required to endure „only" 2,702,098 new spyware apps in 2017.

TOP 10 Android malware in 2017

1	AGENT	35.07%
2	SHEDUN	14.76%
3	TRIADA	9.13%
4	LOCKSCREEN	7.82%
5	SMSPAY	4.68%
6	CONGUR	2.87%
7	BOOGR	2.36%
8	SMSSPY	1.45%
9	SMFORW	1.45%
10	FAKEINST	1.42%

Trend 2018

A clear development in the first quarter is the concentration of the Android malware industry on a new, lucrative market. Because the malware detection of AV-TEST systems indicates an overwhelming spike in the development of Android-based crypto miners. While AV-TEST was able to detect the first malware of this type as early as 2014, the sample statistics increased slightly for the first time in mid-2016 and 2017, indicating an experimental phase with the new malware category. However, these two statistical peaks never exceeded the sample count of 50 samples. Things are looking completely different as of the beginning of this year: With 556 samples in January and 388 new crypto miners in February, the development of mining for cryptocurrencies on mobile devices is gathering significant momentum. Obviously, cybercriminals are in the starting blocks to tap into the increasingly powerful processors of Android devices for illegal coin mining.

While the rate of development for Android malware, including Trojans and ransomware, continues to decline in 2018, the rate of banking and password Trojans is bucking this trend and breaking the sound barrier of 9 percent of total malware detection. Android users continue to be well advised to use security apps.

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/.

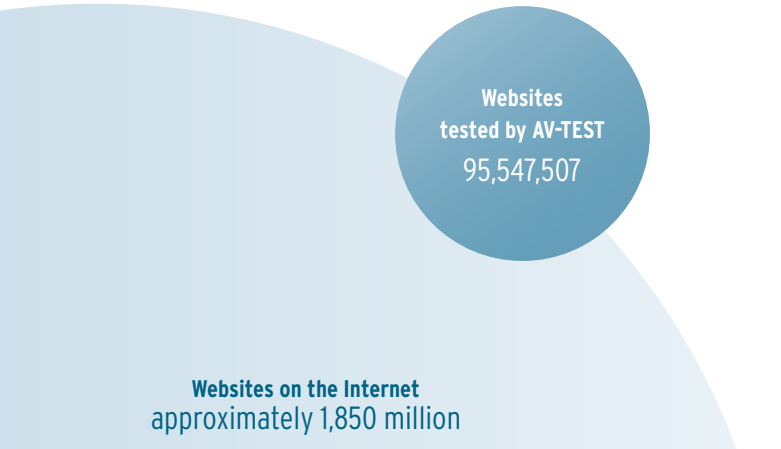
Security Status INTERNET THREATS

E-mails containing viruses, infected websites, attacks via malware download: The depths of online communication offer cybercriminals numerous opportunities to smuggle malware onto their victims' computers. The risk analysis of AV-TEST shows the pathways they prefer.

95 million websites evaluated

For the search engine analysis, AV-TEST systems evaluated in 2017 a total of 95,547,507 websites. In doing so, the Institute also conducted an analysis, along with a ranking of infected top-level domains and the file formats used for malware proliferation. It revealed that attackers still rely on unprotected http pages for spreading malware: 84.26% of all infected websites worked with the unprotected transfer protocol. However, the number of sophisticated attacks also occurring via https continued to increase compared to the previous year. Whereas in 2016, a mere 8% of attacks were launched from https websites, this figure already reached 15.74% in the following year. One reason for this can also be seen in what has already been a vast increase in the number of SSL-encrypted websites. What is in itself a favorable development, is also flanked by the massive increase in the use of free, automatically generated SSL certificates by the service „Let's Encrypt". However, this service was used not only by upstanding consumers and SMEs; its use was also not lost upon criminal profiteers.

Tested websites in 2017



TOP 10 malware-infected domains in 2017

1	COM	52.92%
2	NET	10.32%
3	RU	4.48%
4	GE	3.58%
5	ORG	2.76%
6	SU	2.46%
7	TIPS	2.35%
8	BR	1.76%
9	CO	1.27%
10	ME	1.12%

Ransomware travels by e-mail

In 2017, cybercriminals used a large arsenal to smuggle malware onto their victims' devices, using either a shotgun approach or a very targeted rifle approach. Last year's major ransomware attacks harnessed the traditional transmission pathway for this category of malware, thus spreading „WannaCry" and „Locky", for example, via large e-mail and phishing campaigns. This remained the predominant transmission pathway for ransomware in 2017, as well as the majority of malware transmitted via the Internet – the lion's share being Trojans. Malware such as WannaCry and Petya also spread via infected systems through vulnerabilities in the Windows SMB network protocol.

With 16 percent of all spam e-mails in 2017, Vietnam ranked first among spam senders compared to the previous year. The United States maintained second place, while India lost its former pre-eminent position to Vietnam. After China's 4th place ranking, Germany assumed an ignominious fifth place the spam nations recorded by AV-TEST, with 3.9 percent of the global share of unwanted and often virus-infected e-mails.

Targeted infection per update

The developers of Petya sought another pathway to proliferation by infecting computers located in Ukraine using the bookkeeping software „MeDoc" typical for the country, with the help of infected program updates. A similar attack occurred from October to September through the infection of „CCleaner", a freeware used by millions, from the supplier at that time, Piriform. During the period of the attacks, there could have been 2 million installations of the affected software. Due to a valid certificate in the infected 32-bit version CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191, this was very difficult to detect as malware. As the Talos Team from Cisco, which discovered the malware, found out, 1.65 million infected computers contacted the command-and-control server of the malware.

TOP 10 malware-infected file types in 2017

1	HTML	22.97%
2	PHP	8.90%
3	EXE	5.69%
4	ZIP	4.50%
5	RAR	2.29%
6	HTM	1.13%
7	ASP	0.31%
8	ASPX	0.25%
9	IZLE	0.23%
10	COM	0.10%

Exploit kits remain heavily active

Exploit kits were also very popular among malware in 2017, as they are easily accessible on the web, widely distributed, and their use is extremely economical. The success of exploit kits is guaranteed by the professional, collaborative approach of well-organized criminal gangs working in this sector. Whereas one group markets the malware proliferation tools in underground forums, other criminals always keep the exploit kits for customers up-to-date and thus guarantee „crime-as-a-service" with a success guarantee for a minimum number of infected PCs.

Accordingly, the functions of the malware building block and proliferation kits are always up-to-date: New attack vectors and targets, along with the constant adjustment of the latest exploits and detection methods of virus scanners, promise criminals wide coverage for their malware campaigns. In 2017, the exploit kits „RIG", „Magnitude", „Terror" and „Neutrino" dominated the market, proliferating ransomware, coin miners and banking Trojans, among others. Quite often, the attackers exploited the known vulnerabilities of the Adobe Flash software. Last year, for malware proliferation, cyber-criminals also deployed a vast number of proprietary websites with content that was very popular in search engines. That is why the detection systems of the AV-TEST Institute monitored the five largest search engines throughout the year.

TOP 10 spam senders in 2017

1	VIETNAM	16.0%
2	UNITED STATES OF AMERICA	11.5%
3	INDIA	9.8%
4	CHINA	6.6%
5	GERMANY	3.9%
6	IRAN	3.9%
7	MEXICO	2.8%
8	INDONESIA	2.8%
9	BRAZIL	2.7%
10	ROMANIA	2.6%

Trend 2017

The first quarter of 2018 indicated a significant surge of attacks occurring via https websites: With over 27%, the attacks launched via encrypted websites have increased heavily. By contrast, the Top 10 list of file types infected with malware remains virtually the same.

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.

Security Status IoT

IP camera, smart lighting and smart TVs: There are hardly any households in which there is not at least one device networked with the Internet. In addition, more and more manufacturers are linking to proprietary online services which up to now remained non-networked. It often makes no difference whether such online features are useful or not. And only seldom do security considerations play a role in their development. In the process, manufacturers are unnecessarily putting millions of their customers at risk.

Battle for the market of the future

Even cautious forecasts on the Internet of Things make marketing managers' eyes light up: According to Gartner predictions, companies will invest approximately $1,477 billion in IoT devices and services over the next two years. The chances of earning money in the consumer segment over the same period are even higher, as the market research company estimates the market for consumer products to be even more profitable: Consumer households are expected to spend $1,534 billion for IoT devices by 2020. If this forecast comes true, over 830 million wearables and 20.8 billion networked devices will be sold and deployed around the globe.

Numbers like these are exciting not only for companies but also for cybercriminals. And thus, an explosive mixture is formed: On one side, there are product manufacturers without expertise in IT security, who always want to throw more and more products onto the booming market as fast as possible. On the other side, the cybermafia, with a vast arsenal of already functioning and tested malware programs, is ready to ambush the masses of devices and online services offering them ample vulnerabilities for the proliferation of malicious codes. To that extent, one market fuels the other. The consumers bear the risk and the costs.

IoT malware is on the upswing

Among the recorded malware, there are malicious codes for exploiting the CPU power of Internet-capable devices for DDoS attacks, based on the Mirai model, such as the malware sample „Gafgyt" aka „Bashlite", which with over 21.52 percent ranks No. 1 on the Top 10 list of IoT malware. This Linux Trojan, whose first detection by the AV-TEST systems dates back to January 2012, utilizes, among other things, the shellshock vulnerabilities of the Bash UNIX shell. This enables the malware to infect any unpatched UNIX-based operating system. If the infection is successful, Gafgyt proliferates like an Internet worm in the connected network. The source code of the malware was already published in 2015. Since that time, a significant increase in Gafgyt activity has been measured. The malware forces above all IP cameras and digital video recorders into its botnet, which is then deployed for DDoS attacks, among other things; in this respect it is very similar to Mirai.

Mirai still active

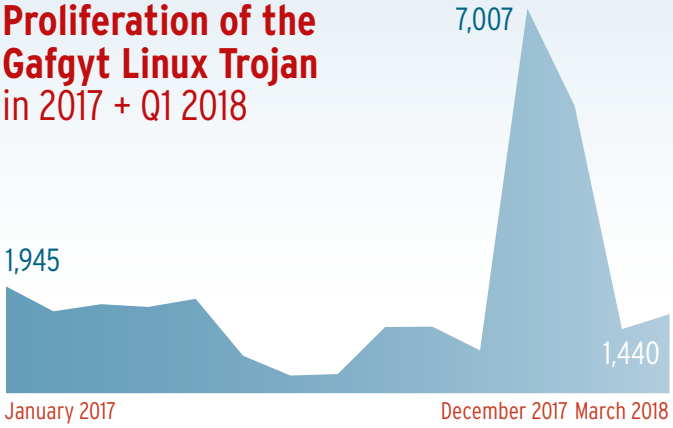
The 2016 attacks led via the Mirai IoT malware temporarily linked over 500,000 infected IP cameras and digital video recorders into what was up to now one of the largest botnets in the world. Through denial-of-service attacks, large portions of the Internet were immobilized. Three American students had originally developed the malware to block the servers of competing Minecraft gamers from the web. Later, the botnet generated by Mirai was used for DDoS blackmail attempts against large Internet and service providers. With this initial major attack, the three students created a temporary public awareness for the danger of unprotected IoT devices. By publishing the Mirai source code on the Internet, however, they created an additional danger.

The successful malicious code continues to be deployed in modified versions, as proved by the statistics of AV-TEST's own honeypot systems. For criminals, the malicious code remains attractive: for many IP cameras, as well as other IoT devices at risk, there are still neither security nor firmware updates available, sometimes not even a relevant update function.

Emphatic warning

Similar to Mirai and Gafgyt, the IoT malware sample „Hajime" has been spreading since the first quarter of 2017. On infected systems with a display, the IoT malware even issues a warning with a self-programmed message: „Just a white hat (hacker), securing some systems. Stay sharp!" The proliferation of Hajime has occurred since April of last year in increasing waves. AV-TEST will also continue to monitor the development of this intruder into IoT systems.

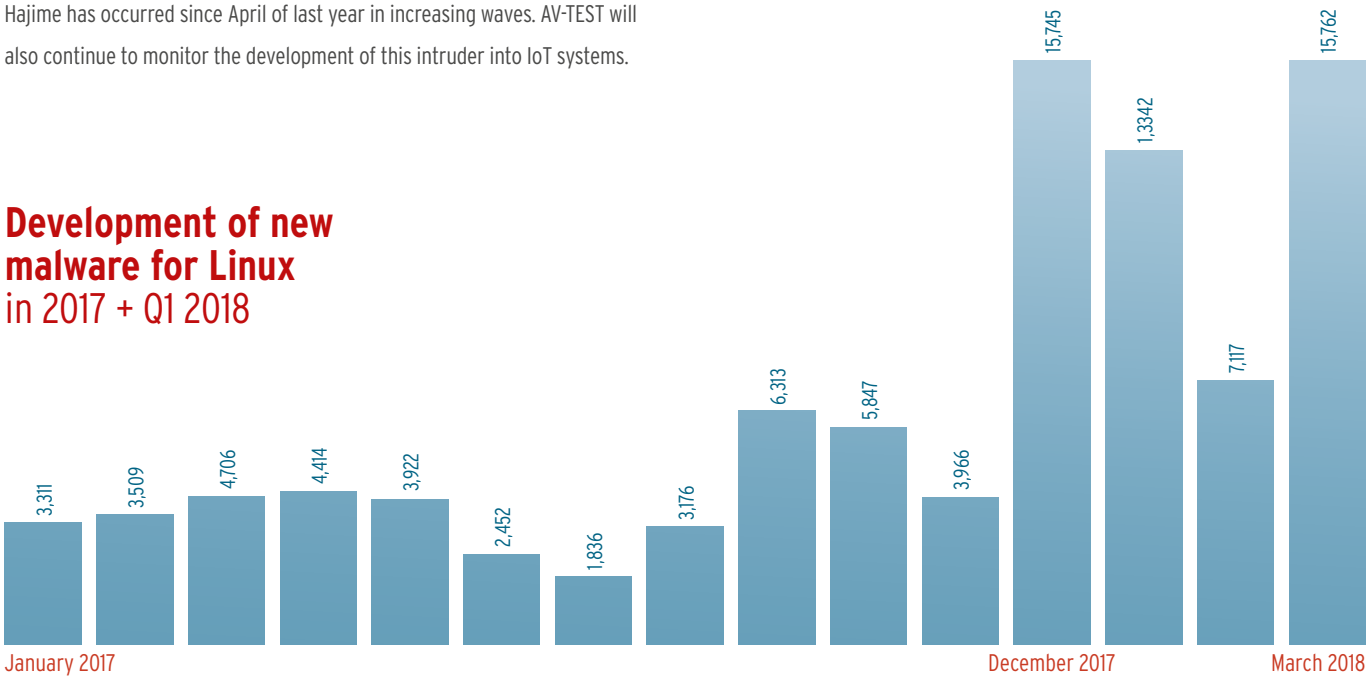
Proliferation of the Gafgyt Linux Trojan
in 2017 + Q1 2018



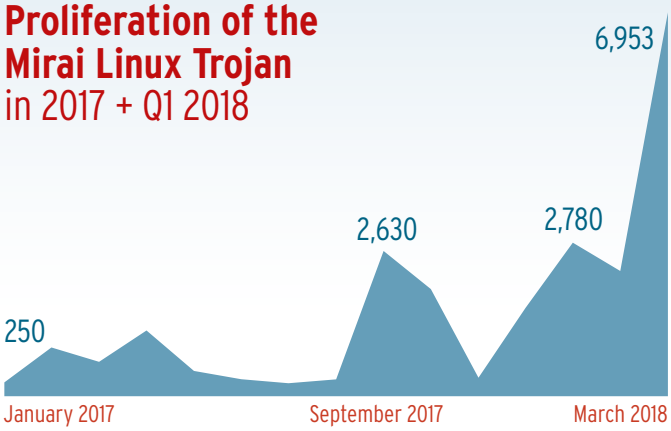
IoT: a coin mining El Dorado

In addition to building up vast botnets for DDoS blackmail, cybercriminals have begun to focus on an additional criminal business plan geared towards millions of unprotected IoT devices. After all, what could be more logical than to deploy the largely unprotected and continuously increasing CPU power of IoT products for computing cryptocurrencies. For IoT and smart-home infrastructures, attackers can deploy malware programs on a Linux platform and have the CPU power of the devices work for them. Whereas coin miners initially utilized the full CPU power for the mining of Bitcoins and other cryptocurrencies, driving

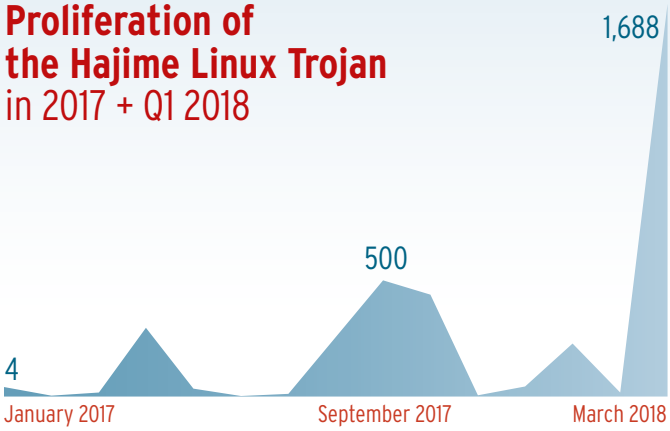
Development of new malware for Linux
in 2017 + Q1 2018



Proliferation of the Mirai Linux Trojan in 2017 + Q1 2018



Proliferation of the Hajime Linux Trojan in 2017 + Q1 2018



the devices to the performance limits until they failed, the new generation of coin miners monitors and regulates the harnessed CPU power, thus preventing failure of the infected host system. Moreover, this strategy means that devices infected with coin miners are more difficult to detect, thus they are available over a longer period of time. The significant measurable use of Linux-based coin miners began in the second quarter of 2017. Since September, the number of samples of this malware category has been constantly increasing, not only for IoT devices, and had grown eightfold by December.

TOP 10 IoT malware 2017

1	GAFGYT	21.52
2	MIRAI	17.12
3	VIT	13.57
4	LOTOOR	5.82
5	AGENT	5.42
6	TSUNAMI	3.34
7	SHELLBOT	2.21
8	SETAG	2.16
9	SH	2.08
10	HAJIME	1.90

Trend 2018

Also in the first quarter of this year, AV-TEST systems registered significant increases of malware for IoT systems. Since then, the malware industry has been developing over 300 new variants of the lucrative category of malware per month. Current trends indicate that in the near future, this development will stagnate on a high level, as cybercriminals are able to access a growing number of mostly unprotected IoT devices. Accordingly, they are under no development pressure. The qualitative development of coin miners will continue, however, and we will see an increasing number of samples with sophisticated CPU management.

In total, the development of malware for Linus-based systems will experience enormous growth in 2018. This can already be gleaned from the measured values of practically all malware classes that can be used for smart home and other IoT systems.

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 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 35 servers with storage capacity of over 2000 TB. On the publication date of this annual report, the AV-TEST database contained 771,077,699 malware applications for Windows and 28,335,605 malware programs for Android!

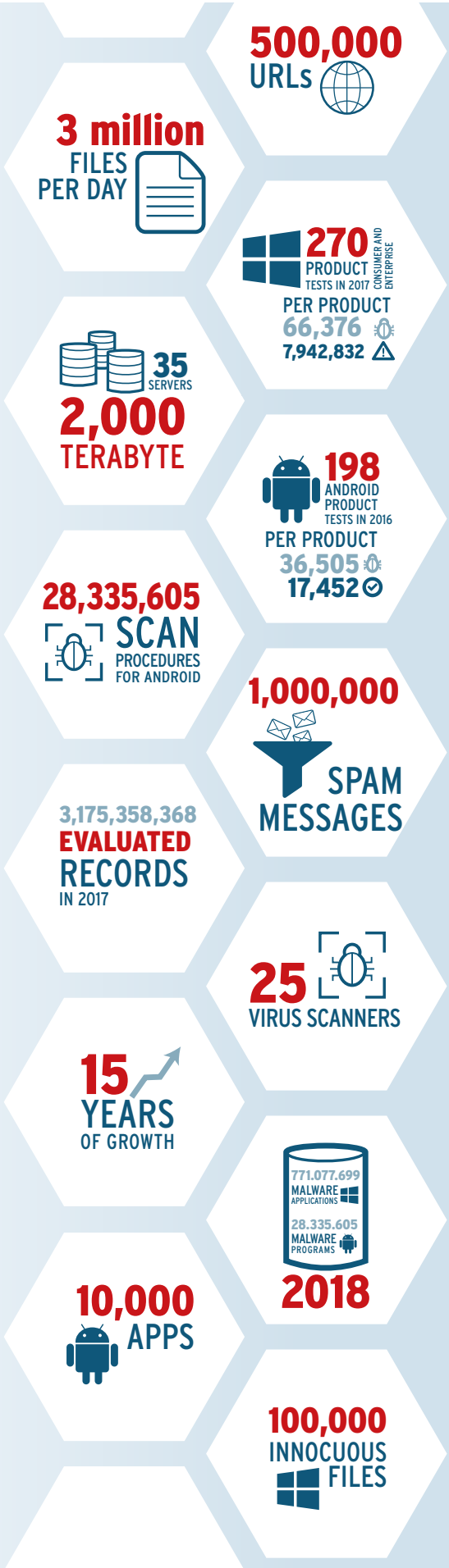
AV-TEST seal of approval for antivirus products

- Home-user products that meet the high certification standards of the AV-TEST Institute are awarded the AV-TEST CERTIFIED seal of approval.
- The AV-TEST APPROVED test certificate is reserved to products from the corporate solutions world.

All market-relevant products for the Windows, MacOS and Android operating systems are evaluated.

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 2017 over 270 product tests alone were run for home user and business user products. As a result, 66,376 malware attacks and 7,942,832 individual records for false positive tests were deployed and evaluated per product. Throughout the year 2017, this amounted to 3,175,358,368 records evaluated by the test experts. In the monthly Android tests carried out throughout the year, the testers evaluated over 122 individual products. In doing so, each evaluated security app had to defend against 36,505 special Android malware samples. As a counter sample, the experts also recorded over 17,452 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 6,582,754 scan procedures were analyzed and reproducibly evaluated. 2,359,358 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.

**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