FACTS AND FIGURES

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

SECURITY REPORT 2016/17

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

本文档由Linux公社 www.linuxidc.com 整理

欢迎点击这里的链接进入精彩的Linux公社 网站

Linux公社（www.Linuxidc.com）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

Linux公社是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。

Linux公社（LinuxIDC.com）设置了有一定影响力的Linux专题栏目。

Linux公社 主站网址：www.linuxidc.com 旗下网站：www.linuxidc.net

包括：**Ubuntu 专题** **Fedora 专题** **Android 专题** **Oracle 专题** **Hadoop 专题** **RedHat 专题** **SUSE 专题** **红旗 Linux 专题** **CentOS 专题**

Linux 公社微信公众号：linuxidc_com

The AV-TEST Security Report

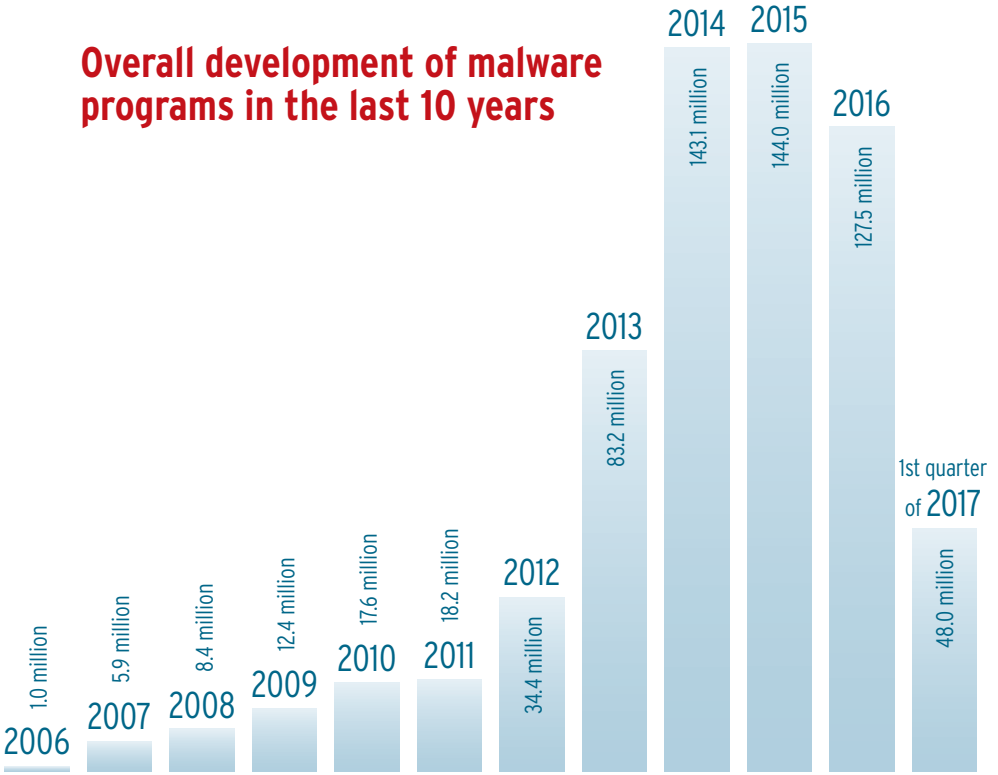
The best news right off the bat: Compared to the previous year, the detection systems of AV-TEST showed a slight decline in the development of malware programs for the year 2016. Overall, that is a pleasing trend, however by no means any reason to celebrate, as evidenced by the AV-TEST Institute's statistics of this year's Security Report.

Declining malware statistics

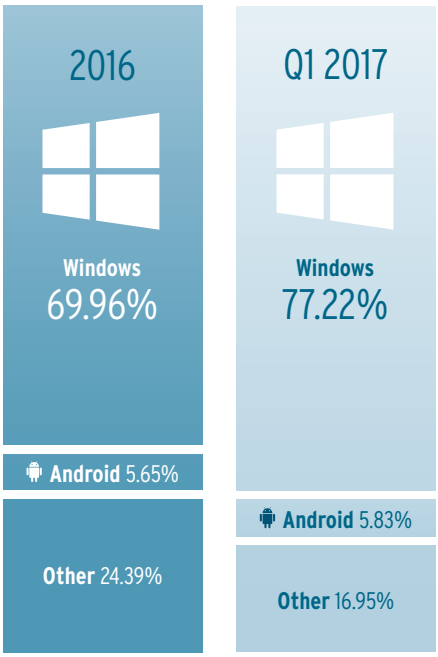
It remains positive to note that the declining malware trend in 2016 provided some relief, at least quantitatively. Thus, compared to 2015, detection systems were required to seek out and defend against 14% fewer malware samples. In total, this amounted to precisely 11,725,292 fewer newly developed malware programs than in the previous year. It should not be forgotten, however, that the volume of newly developed malware in 2016 still represented the second-highest since the beginning of measurements by the AV-TEST systems. In addition, 2015 saw skyrocketing growth in malware programs and in comparison to 2014, practically a doubling of the sample statistics. The overall number of malware programs for all operating systems currently exceeds 640 million.

Without wanting to belittle the positive trend for 2016, the fact remains that there have been several short-term downward trends since the beginning of measurements in 1984, a total of six times, without seriously influencing the clear, long-term trend – towards more malware. Despite declining numbers, in 2016, the AV-TEST analysis systems still recorded an average of 350,000 new malware programs per day, i.e. roughly four new malware samples per second. An assessment of the threat potential cannot be meaningfully made on the analysis of quantitative factors alone. But more on that topic in the course of this report.

Overall development of malware programs in the last 10 years



Malware detection sorted by operating systems



本文档由Linux公社 www.linuxidc.com 整理

Quality, not quantity?

Yet not only with respect to declining numbers in the overall field of malware, last year is remarkable. Even within the malware classes detected by AV-TEST, as well as among the developments of attack targets, the year 2016 represents a significantly measurable watershed, and clear trends can be identified:

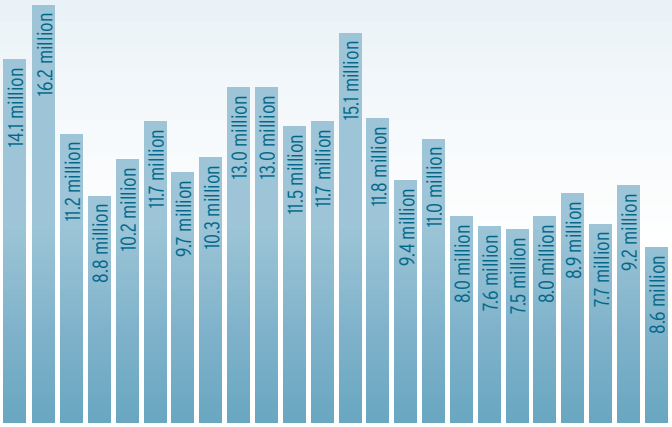
The quantity of malware codes programmed exclusively for Windows systems is declining. Attackers are increasingly developing malware programs for other operating systems. Compared to the previous year, their number is increasing by just under 10%, whereas the number of pure Windows malware is declining by just under 13%.

Windows remains the most widely attacked operating system. In the year 2016, as many as seven out of ten newly programmed malware programs targeted the Microsoft platform.

Apple devices are more and more under fire: Compared to the previous year, the quantity of malware for macOS has tripled.

Users of Android devices are also subject to a fast-growing quantity of malware: Compared to the previous year, the number of malware programs targeting the myriad of devices with Google's operating system has more than doubled.

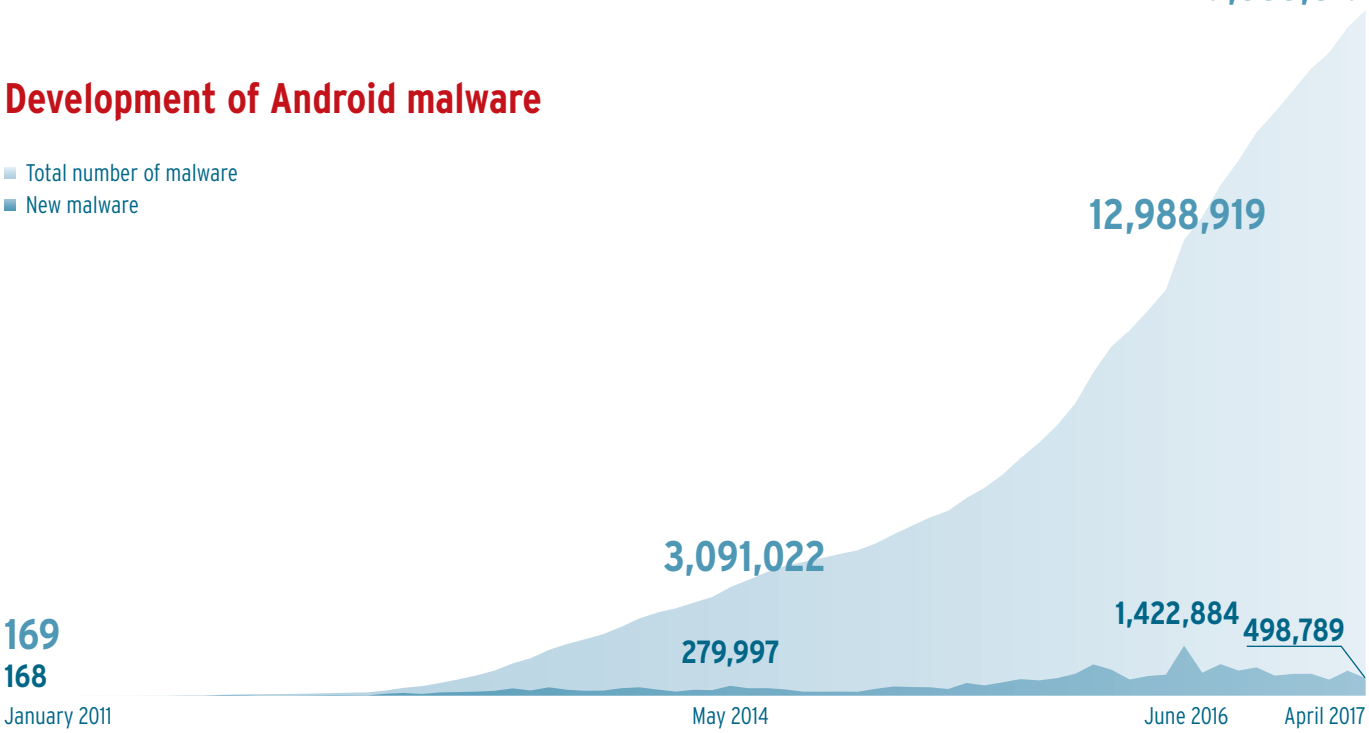
Total occurrence of new malware



Linux systems were under fire in 2016 as well: The number of attacking malware programs tripled compared to the previous year.

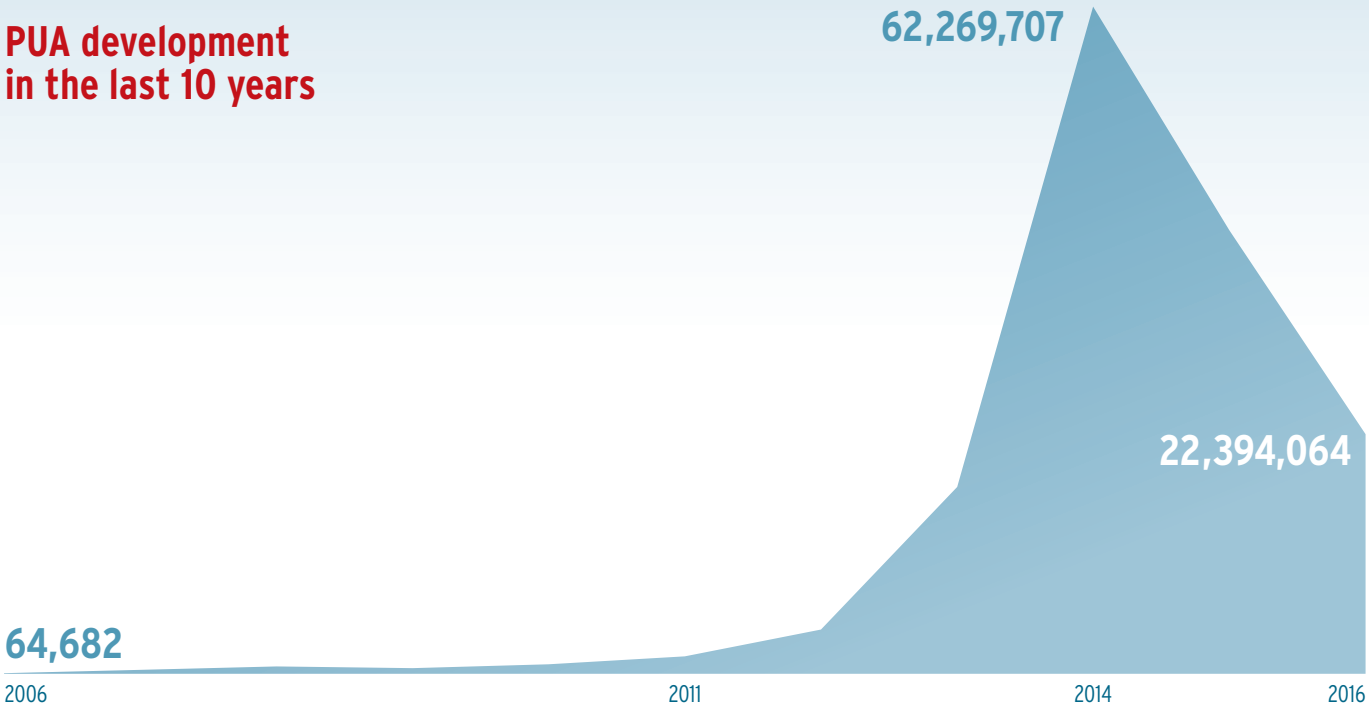
Due to the rapidly increased numbers of potentially unwanted applications (PUAs) with which the advertising industry spied on the surfing behavior of users in the years 2014 and 2015, the AV-TEST researchers dedicated a separate chapter to this class of malware in the last Security Report. However, the number of new PUA samples decreased by half in the year 2016, compared to the previous year, to a mere 22,394,064 newly registered samples.

Development of Android malware



本文档由Linux公社 www.linuxidc.com 整理

PUA development in the last 10 years



Trend 2017

This Security Report encompasses not only the data status for the year 2016 but also takes into account the measurement results of the AV-TEST analysis systems for the first quarter of 2017. Thus it is already possible to recognize trends for the current year, backed up by data.

The Q1-2017 numbers confirm the trend that Apple users will not find pleasing. The rising attack statistics already observable in 2016 are increasing further – by a significant rate: Thus, the overall number of malware programs for macOS doubled within the first four months of this year! There was also a marked increase in the recorded attacks on Linux systems, which are often also connected to the Internet unprotected like computers under macOS. For attackers, obviously a worthwhile target.

According to initial forecasts, there will be a reversal of the hopeful trend for Windows users, Because the declining rate of attack of 2016 is not being confirmed by the new measurement results of the AV-TEST systems. In the first quarter of 2017, the number of malware programs was on the upswing again, currently by just over 7% compared to the annual value of the previous year.

The trend towards a decline in the number of PUA samples was confirmed in the first quarter of this year. In April, the AV-TEST systems detected a mere 724,633 samples. The last result that low was in March 2013. Despite the enormous decline, it is still too early for anyone to let down their guard, and the experts at the AV-Test Institute will continue observing the PUA trend.

In-depth analysis of the overall numbers presented here can be found in the individual chapters of the Security Report.

本文档由Linux公社 www.linuxidc.com 整理

WINDOWS
Security Status

Also in 2016, the operating systems of Microsoft remained the number one target of criminal online attacks. However, the number of attacks declined by 13% compared to previous year. Why? An analysis of the AV-TEST measuring results provides the answer.

Over 600 million adversaries for Windows

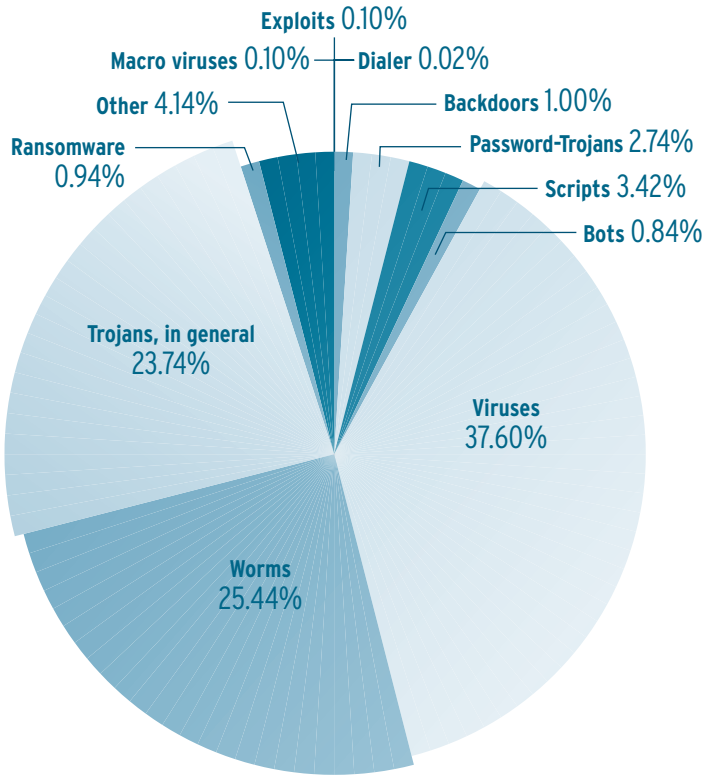
Despite a significant decline in the number of malware samples detected by the AV-TEST systems, there is no reason for Windows users to let down their guard. Windows is and will remain the most frequently attacked operating system. It is true that the number of malware samples in 2016 declined by 15% compared to previous year. However, the fever curve rose again by 7% in the first quarter of 2017. At the time this report was concluded at the end of June 2017, there were already 600 million malware programs detected by AV-TEST targeting the frequently used operating system from Redmond. Without good virus protection, the Internet is by no means safe anymore.

Viruses, worms and Trojans

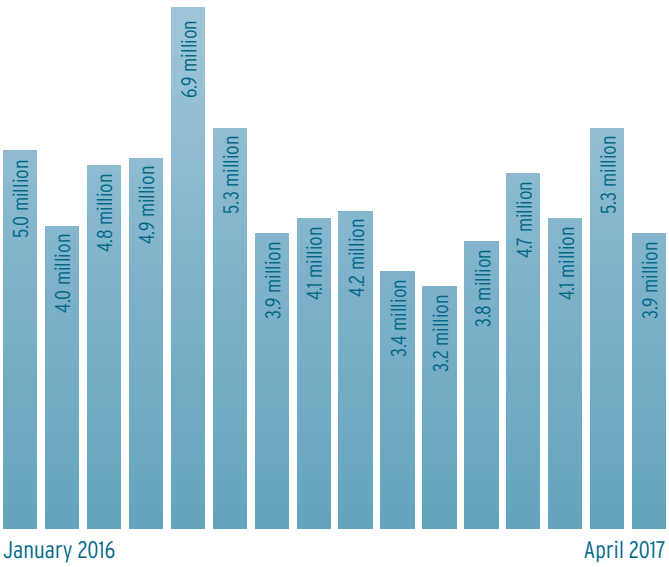
One look at the growth of Windows malware indicates precisely which types of malware programs were the most lucrative for cyber criminals in 2016. Because just as any other product on the market, malware programs also need to turn a profit for their developers. Only malware offering a proper return on investment is worth further development, i.e. investing time and money. The economic success of malware can be gleaned from several key parameters.

Already the mere frequency of occurrence of a malware code can provide information on how successful it is. Thus, in 2016, traditional viruses dominated the malware market for Windows. With more than 37%, one

Distribution of malware under Windows in 2016



Development of new malware for Windows in 2016 and 1st quarter of 2017



本文档由Linux公社 www.linuxidc.com 整理

out of three malware samples represented this class. One reason for this naturally lies in the method of their proliferation: As non-independent program routines that only reproduce upon activation through the victim, by infecting more and more program files, they are destined for explosive, often uncontrollable proliferation already in the program code. However, this type of proliferation makes it easier for scan engines to detect malicious codes like these. In order for viruses to be successful, they therefore need to appear in numbers, as unlike other malware programs, they are not capable of controlled distribution.

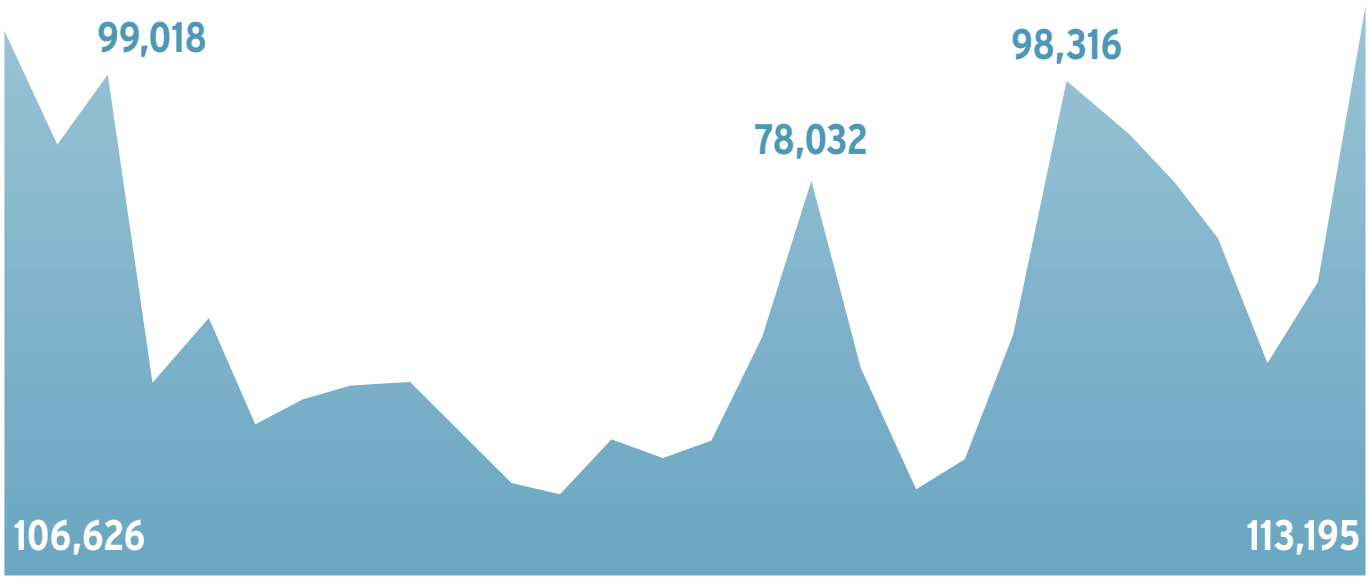
Worms also occurred on a massive scale in 2016. 25.44% of all malware detected could be classified in this malware class. Cyber criminals appreciate the self-replicating malicious code above all due to its high speed of proliferation and the wide array of possible functions. Computer worms can utilize practically any possible path for infecting systems. Thus, they can proliferate using infected USB sticks, within networks, as well as a drive-by or direct download and via email. On infected computers, the download any additional malicious code, i.e. Trojans.

Trojans were also heavily represented in 2016, with over 23%. 2.74% password Trojans, along with 0.94% ransomware are added to what is already a heavily-distributed class of malware. Because both malware families of the "Trojan" class were classified separately in this report, due to their significance.

Ransomware: the high-tech malware

There is no indication based on proliferation statistics that 2016 was also the "year of ransomware". Comprising not even 1% of the overall share of malware for Windows, the blackmail Trojans appear to be more of a marginal phenomenon. The fact that this assessment was already quite wrong in the previous year can be explained by this class of Trojan's mode of action, along with the damage caused by this Trojan class. In order to generate the desired profits for its developers, no distribution comparable with traditional viruses is necessary: ransomware involves "high-tech malware", which seeks its victims above all in a targeted business environment. For instance, emails infected with ransomware are sent out almost exclusively on weekdays, as proven by the measurement results of the AV-TEST systems.

Development of ransomware in 2016 and 1st quarter of 2017



本文档由Linux公社 www.linuxidc.com 整理

Highly-complex encryption

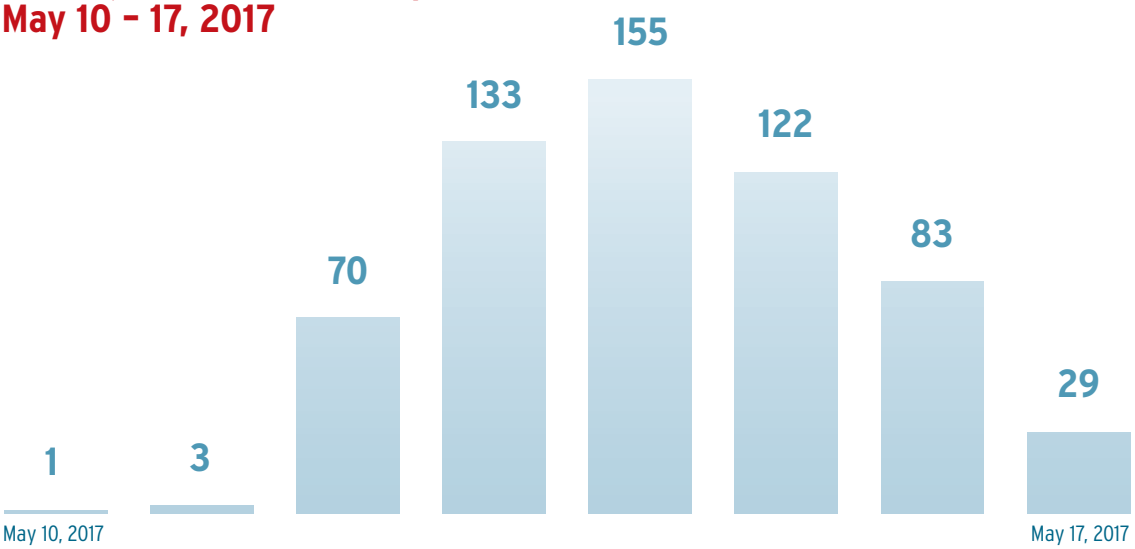
The malware samples encrypt files or entire computers with highly-complex, state-of-the-art encryption protocols. In doing so, high key lengths are used, e.g. for the RSA cryptosystem, keys between 1024 and 4096 bits, for ECDH up to 192 bits and for AES up to 256 bits – which means these keys virtually cannot be cracked. What's more, blackmail Trojans use sophisticated server infrastructure for generating, administering and issuing the keys with which victims can decrypt files and computers against ransom payment. Practically any available online currency, including its anonymous server infrastructure, can be used for processing the online blackmail. In this way, massive numbers of low blackmail sums between 100 and 500 Euros can be extorted and laundered through currencies such as UCash and PaySafeCard. But large sums, such as during the online blackmail of the Hollywood Presbyterian Medical Center in Los Angeles in February 2016, are also easy to extort. The cyber criminals cashed in on the blackmail sum of 15,000 Euros conveniently, anonymously and free of charge via bitcoin.

Highly complex and highly flexible

Yet the selective distribution also manifests the performance capability of ransomware: With targeted attacks, cyber criminals in 2016 took aim at critical sectors; in particular, public administrations, healthcare system and retailers became victims of selective ransomware campaigns, mostly triggered by email attachment. The precision with which criminals are able to deploy ransomware is seen in the attacks by the ransomware GoldenEye at the beginning of December 2016. In the first wave, the malware disguised as a job application email attacked almost exclusively human resource departments of companies.

The fact that ransomware is also suited for mass infections was stunningly proven by the WannaCry attacks in May of this year with more than 230,000 infected widows computers in over 150 countries. This case shows the level of development standards such malware has reached, which criminals lease as a service. Thus, WannaCry infected computers via zero-day exploits, which the US intelligence agency NSA previously used to eavesdrop on computers worldwide. Through a break-in by the hacker group "The Shadow Brokers", these Windows exploits hoarded by the NSA became freely available over the Internet and were utilized for the ransomware WannaCry. While Microsoft quickly offered patches for the operating systems involved, operating system updates, along with regular backups, are often neglected by consumers and companies alike. As a result, large sections of the British healthcare system, including several hospitals, the large Spanish provider Telefonica, as well as the German railway company, Deutsche Bahn, proved to be far too vulnerable.

Development of WannaCry
May 10 – 17, 2017



本文档由Linux公社 www.linuxidc.com 整理

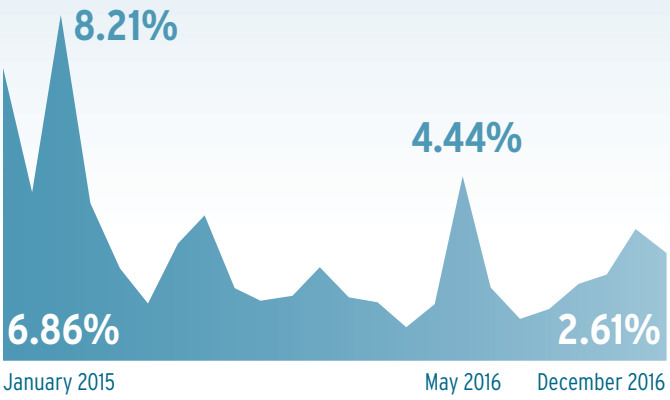
Attacks on the SWIFT banking system

Password and banking Trojans also exhibited an interesting trend in 2016. While the proliferation (2.74%) of these extremely specialized forms of malware slightly declined overall compared to the previous year (3.02%), it is in no proportion to the damage caused. This was significant, especially at the beginning of the year. Already in February 2016, the Bangladesh Central Bank lost over $81 million through a malware attack. Also in February, a similar attack was launched against the New York Federal Reserve. But it didn't stop there.

As seen by the proliferation of password and banking Trojans measured by AV-TEST, in the first quarter of last year, there were extremely many samples of similar malicious codes active. Some of them were most certainly used for attacks on the SWIFT (Society of Worldwide Interbank Financial Telecommunication) banking network. Using special malware, criminals gained access to banking computers connected to the payment system. The Belgian service provider later confirmed this also in a warning to its customers, 3,000 financial institutions around the globe. The attackers were alleged to have been able to assume the identity of authorized users and engage in transactions in their name, as stated in the letter. The Brussels company, however, declined to disclose which banks were involved and how high the financial losses were. At the end of April, SWIFT issued a relevant security update.

The monetary success of banking Trojans is obvious: In proportion to the effort, the attack on a few SWIFT users is naturally far more lucrative than mass attacks on consumer PCs or computers of small enterprises.

Development of password Trojans in 2016



TOP 10 Windows malware 2016

1	ALLAPLE	7,628,795
2	VIRUT	5,689,139
3	RAMNIT	5,020,383
4	VIRLOCK	3,092,764
5	AGENT	2,890,132
6	PARITE	1,811,675
7	SALITY	1,514,886
8	LAMER	1,422,229
9	MIRA	1,364,763
10	SMALL	1,284,994

The Top 10 Windows malware samples

Because viruses, worms and Trojans were among the most widely distributed malware samples in 2016, it is hardly any surprise that the Top 10 Windows malware samples were made up of the classes.

Once again this year, the Windows worm Allaple, active since 2006, defended the number one spot on the ranking of most widely-distributed malware. It successfully proliferates when infected websites are visited. Once it has penetrated a Windows system, it replicates itself from computer to computer, even in password-protected networks, whereby as a polymorphic malware sample, it constantly changes its program code, which makes detecting the malware more difficult. Its various samples comprised over 15% of the entire malware detection for Windows systems!

本文档由Linux公社 www.linuxidc.com 整理

Virut, Ramnit, Parite, Sality, Lamer and Small involve computer viruses in a traditional sense. They infect vast number of files and proliferate through different channels, including infected websites, PDF downloads and even infected files on portable storage media such as USB sticks.

Ranked No. 4, Virlock is a truly sophisticated piece of program code among the Top 10. This ransomware is constantly being further developed and belongs to the few programs that can encrypt not only individual files but also complete systems. What's more, variants of Virlock do not function exclusively as ransomware but can also infect files and thus proliferate like a virus. In this manner, Virlock struck cloud storage systems in 2016 by proliferating via infected files, which were synchronized by several users per cloud.

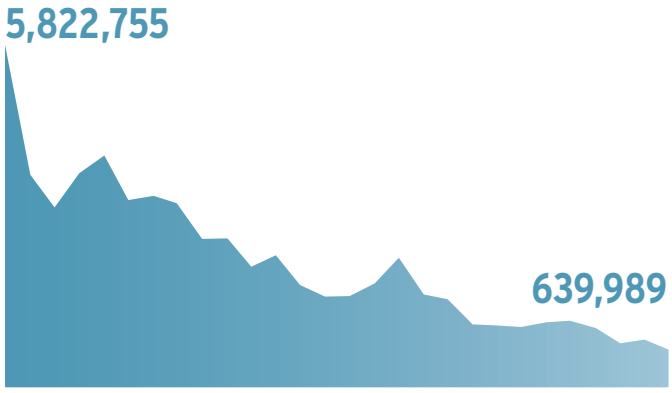
Trend 2017

In the first quarter of this year, there's been a clear trend towards more traditional viruses for Windows, the share of which in the malware distribution compared to 2016 is increasing from 37 to 46%. The number of Windows Trojans also considerably increased in the first quarter of 2017, climbing from 23 to over 30%. This trend is also followed by the number of detected ransomware samples, growing by one-third to 1.55% and is seeing a decline in Internet worms, which with a percentage drop from 25 to 6% are clearly among the losers in the malware market.

PUA: Windows spying on the decline

In concluding the chapter, there is a positive trend: The spying of Windows users by means of spy programs through the advertising industry was noticeably curtailed in 2016. And this trend has continued in the first quarter of this year. This development is even more significant when including the data from the year 2015: Whereas Windows users wanting to protect their privacy were still confronted with 6 million new samples of potentially unwanted applications in January 2015, their rate had dropped to below one-sixth by April 2017.

Development of PUA for Windows in 2016 and 1st quarter of 2017



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/home-windows/.

本文档由Linux公社 www.linuxidc.com 整理

macOS Security Status

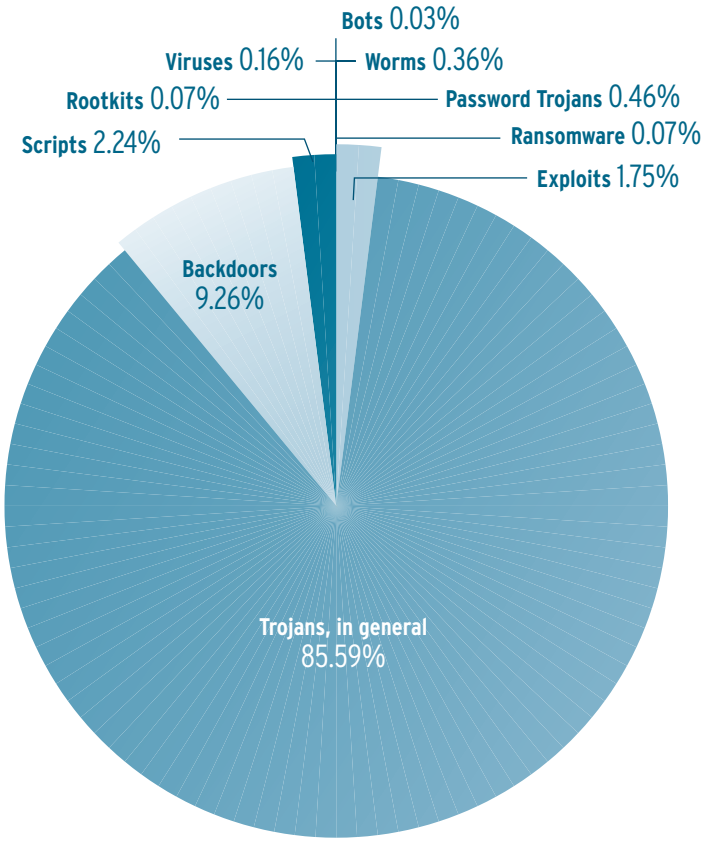
Apple's operating system already shed the myth of absolute security several years ago, and not even absolute Mac fans still venture onto the Internet unprotected. Which is a good thing, because the number of malware samples for computers from Cupertino exploded in 2016.

As safe as a bank?

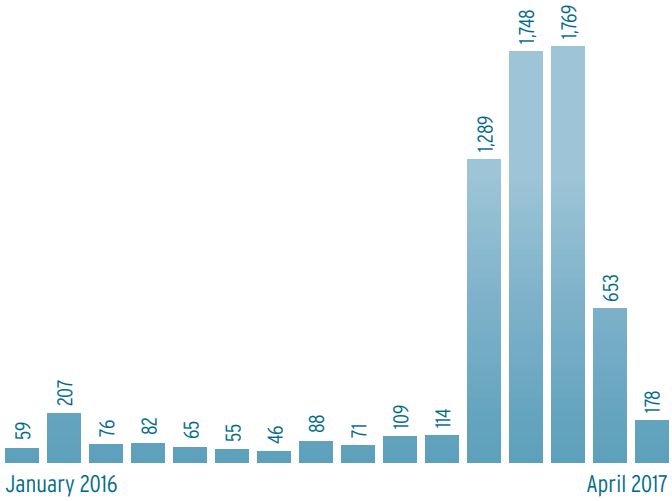
With an increase rate of over 370% compared to the previous year, it is no exaggeration to speak of explosive growth. However, it is also important to keep an eye on the overall number of malware programs with which criminals try to cheat Mac users: Whereas in 2015 there were a moderate 819 different malware threats targeting macOS, Apple users in 2016 already had to protect their devices from 3033 malware samples.

As a proportion to hundreds of millions of malware programs for Windows, that still sounds harmless. But it indicates a dangerous trend, as a massive boost in malware samples for macOS simply means that this market is becoming increasingly more interesting for criminals. In other words: The peaceful days for Apple users are now gone, if not already in 2014 with the mass infection of Macs with the Flashback Trojan. However, some Mac users still trust in a false sense of security which was also fueled by advertising claims from Apple.

Distribution of malware for macOS in 2016



Malware development for macOS 2016 and 1st quarter of 2017



本文档由Linux公社 www.linuxidc.com 整理

Cyber criminals in the development phase

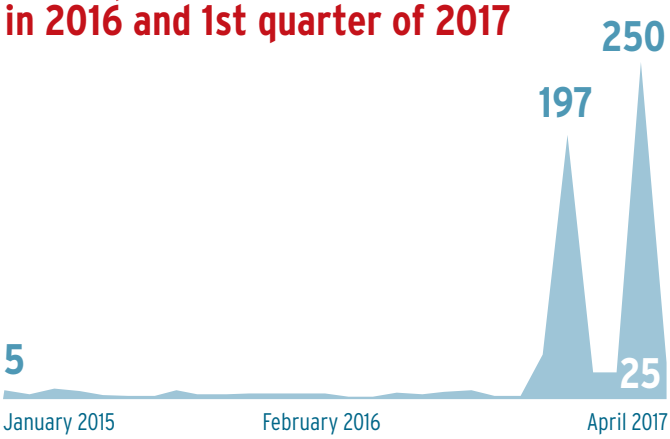
The growth in the number of malware samples began in December 2016. Prior to that, the number of malware threats was practically at the level of the previous year. This means that since then, cyber criminals have been in the experimental phase, trying out which malware and how much time and effort are worthwhile for infecting the operating system from Cupertino. This assumption is also confirmed by the distribution of various malware samples and their development.

Unlike with Windows computers, cyber criminals obviously do not consider traditional viruses useful for use on Mac systems. So the share of this malware class is extremely small at 0.16%. Among other reasons, this may also be due to the fact that the software architecture of the operating system is not particularly suited for the proliferation patterns of this malware.

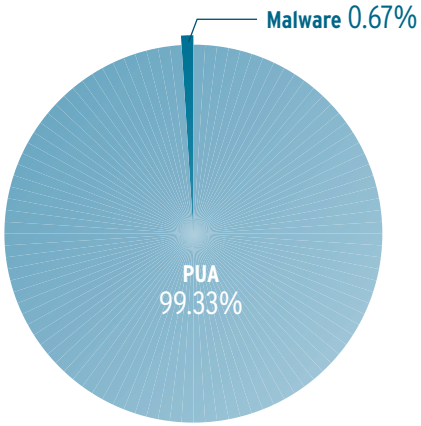
Criminals seem to be more interested in trying to gain access to economically exploitable data through backdoors. In the experimental kitchens for Mac malware, the backdoor programs enabling secret access to third-party systems made up a total of 9.26% of all malware in 2016. This was exceeded in 2016 only by the extreme number of Trojans, which criminals obviously believe will have the greatest success for macOS: 86.12% of all Apple malware threats belong to this class – by contrast, the share of blackmail Trojans (0.07%) and password Trojans (0.46%) is still negligible.

Development of Trojans, in general, in 2016 and 1st quarter of 2017

Development of Backdoors in 2016 and 1st quarter of 2017



Distribution of malware under macOS in 2016



Trend 2017

To enable better analysis of this trend, it is worth looking at the statistics of the first quarter in 2017. They indicate a wavelike occurrence of large quantities of bots with spikes at the end of last year and the beginning of this year, as well as identical patterns with Trojans. And this is a telltale sign that criminals are now in the trial phase of relevant malware, testing which malicious code delivers the most relevant economic results. The second quarter may already begin to show a clear trend in this area. One thing can already be said for sure based on the statistics for the first quarter of 2017, however:
The attacks on macOS are increasing. Compared to the previous year, the number of malware samples has continued to increase, this time by over 140% to a total number of 4348.

本文档由Linux公社 www.linuxidc.com 整理

Top 10 of the Mac Malware

Flashback, an old nemesis, leads the ranking of Mac malware. The malware program, known since September 2011, apparently cannot be eradicated and is constantly being further developed. Originally disguised as an Adobe flash installation file, the Trojan later sneaked through unpatched Java security gaps as a drive-by download in the browser onto the computer. Flashback continues to enjoy a wide proliferation with more than one out of four Mac malware registered by AV-TEST systems last year being a Flashback sample.

It is indeed true that the share of blackmail Trojans is negligible in the overall number of Mac malware threats, but that statistic alone says nothing about the success of a malware program. The best example is Number 3 among 2016 malware threats, one of the first ransomware samples for Apple computers. Already in the last security report, AV-TEST made reference to KeRanger, which in the first two quarters of 2016, as a newcomer, already climbed to Number 8 among the Top 10 malware. The malware threat, which targets OS-X users and encrypts documents, entered Mac computers, among other methods, as a disguised BitTorrent software transmission. Here's the sneaky part: After the infection, KeRanger waits three days before the malware begins encrypting documents.

TOP 10 macOS malware 2016

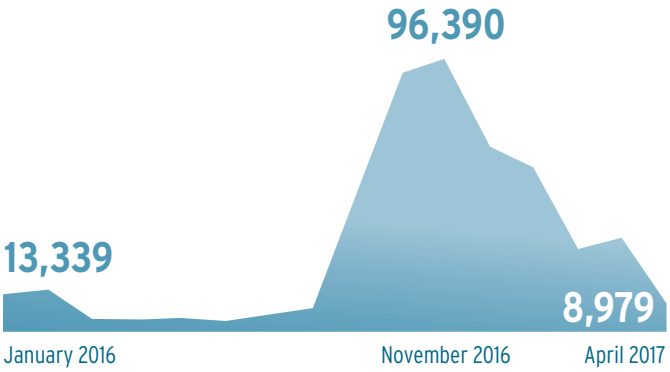
1	FLASHBACK	633
2	MACONTROL	254
3	KERANGER	195
4	XCODEGHOST	163
5	HACKBACK	140
6	JAHLAV	112
7	GETSHELL	105
8	OPINIONSPY	64
9	MORCUT	64
10	OLYX	46

Mac users spied on

Apparently the data of Mac users is extremely lucrative to the advertising industry. At least, it is difficult to reach any other conclusion based on the share of PUAs in the overall number of threats for Apple's operating system. Because in the overall distribution, the massively increasing number of malware samples for Mac OS does not even constitute 1%. With over 99%, the majority of the malware threats were clearly from PUA samples.

One look at the growth of the spy tools in the advertising industry reveals a dramatic rise in the sample numbers in the fourth quarter of 2016. In the absolute peak phase in November, the number of new samples reported by the AV-TEST analysis systems was just under the hundred thousand mark. Since then, it has experienced an equally dramatic plummet, recovering at the normal value of below 20,000 new samples per month. It can be assumed that there is a test phase for adapting the malware threats to new detection patterns of the macOS protection functions.

Development of PUA in 2016 and 1st quarter of 2017



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/.

本文档由Linux公社 www.linuxidc.com 整理

ANDROID
Security Status

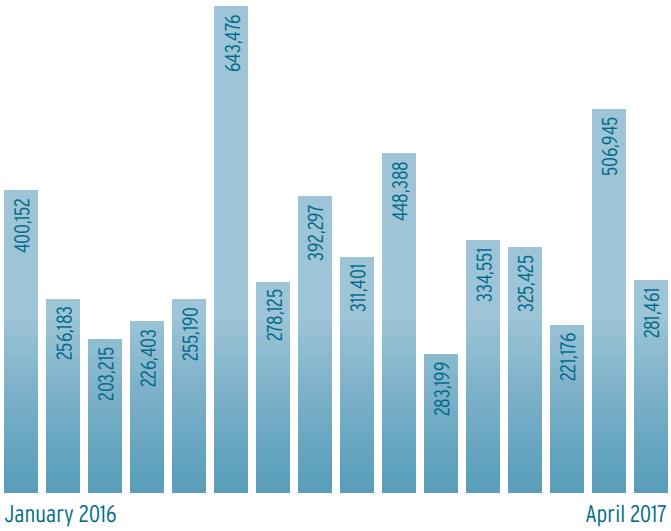
The numbers sound out loud and clear: Anyone seeking to make money by attacking mobile devices will choose Android devices as a target. For other mobile platforms, the development of malware programs is simply not profitable. That is why the share in overall malware development for iOS, Windows Mobile and others has dropped to below meaningful percentage points, whereas the number of new threats for Android has doubled compared to the previous year.

Wavelike attacks

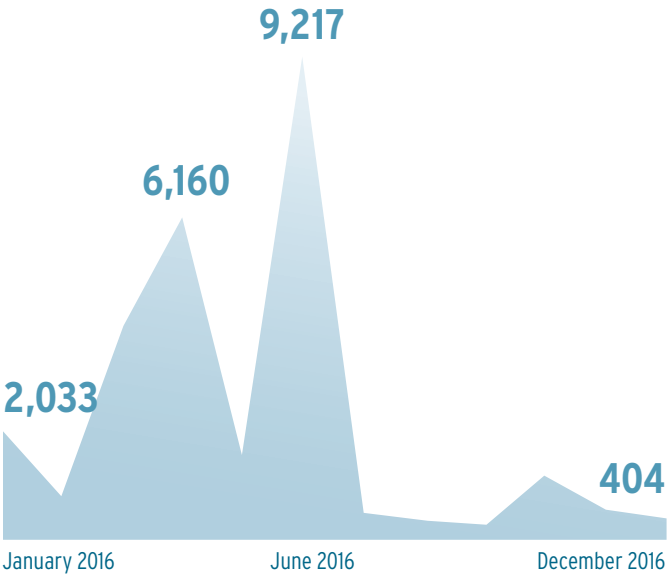
In examining the malware development from 2015 to 2016, one thing becomes clear – in addition to the doubling of the detected sample volume of over 4 million new malware programs for Android in the year 2016: From the beginning of 2016, criminals pushed malware onto the market in waves, which indicates tests of new malware or new proliferation paths, e.g. trying out new Android exploits. The peaks of this trend in 2016 were in January, August and October. The largest spike, however, occurred mid-year in June. In that month, AV-TEST systems measured extreme activity and exactly 643,476 new malware programs for Android, representing the highest number since the Google operating system was published.

And indeed, at that time, Android offered criminals numerous vulnerabilities through which malware could be infiltrated. Accordingly, Google was forced to respond. The patch day in July exceeded all previous updates by far: Google fixed over 100 flaws with two brief successive security updates, roughly one-third of the leaks were security-critical and pertained, among other things, to the crypto libraries OpenSSL and BoringSSL as well as USB drivers. With the largest Android patch up to now, Google did indeed close a multitude of known vulnerability gaps; for June 2016, however, the protection systems of AV-TEST revealed a total 9217 exploits for all Android versions overall, also an impressive peak number.

Malware development for Android in 2016 and 1st quarter of 2017



Development of Exploits in 2016



本文档由Linux公社 www.linuxidc.com 整理

Trojans as a primary tool

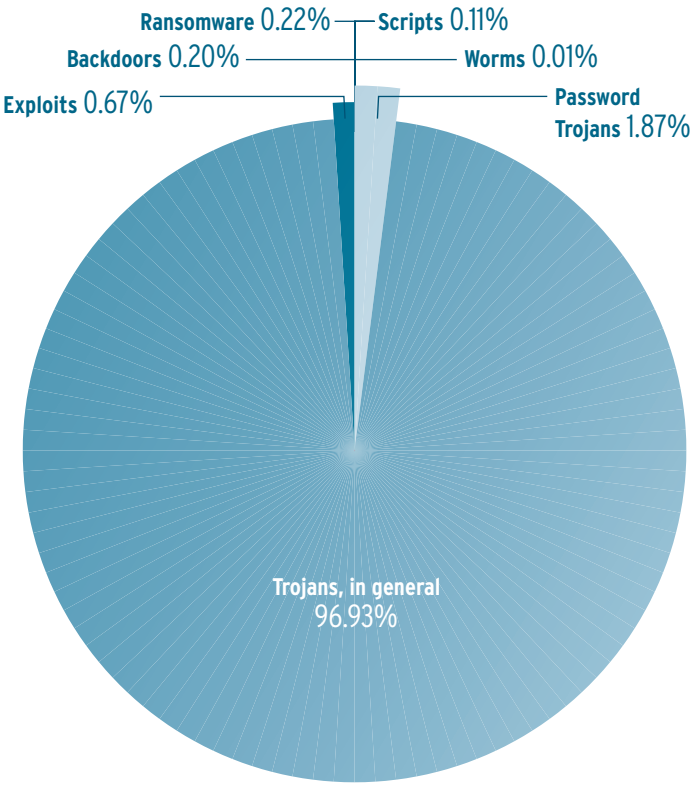
In the year 2016, criminals used apps infected with Trojans most frequently by far. With a share of 97%, one can confidently say that other malware classes played virtually no role in attacks on mobile devices in 2016.

With only 0.22% share in the overall number of Android malware, it is true that blackmail Trojans were represented in low numbers, and in absolute terms, at 8,822, their numbers were declining in 2016 compared to the previous year (12,521). However, in 2016 ransomware represented a risk to mobile devices that should not be underestimated. And the trend in the first quarter of 2017 indicates that the number of ransomware samples has once again sharply increased. As with Windows and macOS, the proliferation statistics for ransomware only allow minor conclusions as to the success of the malware attacks.

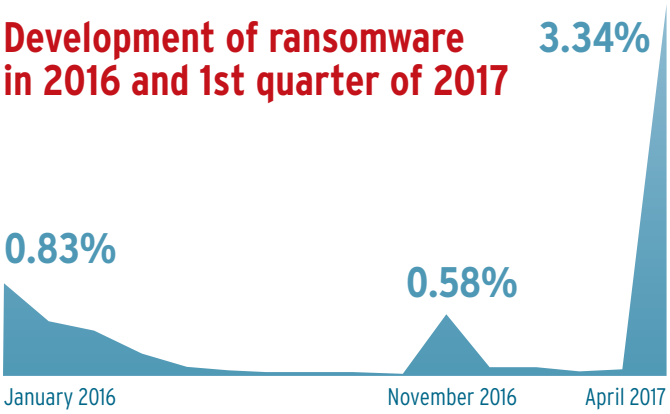
Thus, with "Lockscreen", an Android ransomware entered the Malware Top 10 for the first time in 2016. The malware threat proliferated both via infected apps from sources beyond Google's play store and drive-by downloads. On infected devices, the malware locked the home screen and, depending upon the campaign, demanded ransom for unlocking the device. In the initial versions, the malware was relatively easy to defeat, as the same unlocking PIN was visible in the program code of the malware. Newer versions of Lockscreen, which cropped up over the year, underwent various upgrades. Among other features, some samples were capable of gaining admin rights via the root directory of devices and changing the previous user PIN directly in the device settings.

Another family within the class of "Trojans" gained notoriety in 2016, because also among the password Trojans, the warning systems of AV-TEST indicated a wavelike trend. It had the first of two distinct peaks in the first quarter of the year, subsequently exceeding this in the fourth quarter. At this time, the Android malware Gooligan, among others, was wreaking havoc. The Android Trojan proliferated by means of 80 infected apps from unsecure third-party app stores, infecting a vast number of devices on which the Android versions Ice Cream Sandwich, Jelly Bean and KitKat (version 4) as well as Lollipop (version 5) were running.

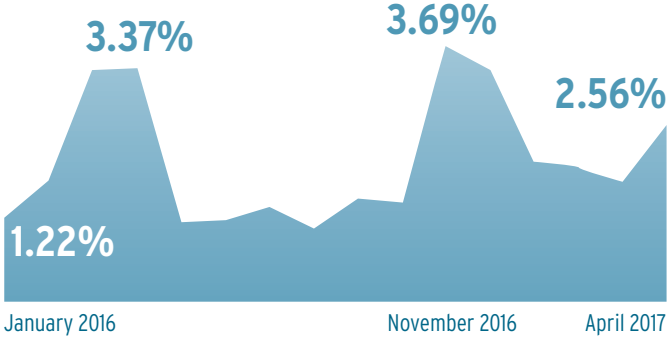
Distribution of malware under Android in 2016



Development of ransomware in 2016 and 1st quarter of 2017



Development of Password Trojans in 2016 and 1st quarter of 2017



本文档由Linux公社 www.linuxidc.com 整理

The Top 10 Android malware samples

As in the previous year, the undisputed number one among the Top 10 were Trojans from the "Agent" family. One reason for this is the method of their proliferation. As with Shedun, these Trojans no longer have to wait until unwitting users actively download them onto their devices. The "Agent" Trojan infects Android smartphones and tablets as a drive-by download. Once it is on the device, Agent downloads additional malicious code, which lowers the security settings and sends private data to servers on the Internet.

Like many other Android malware threats, there was another malware program that also celebrated its dubious high point at Number 2 on the malware Top 10 in June 2016. It has to do with the Trojan Shedun alias HummingBad, which at midyear infected 10 million devices around the globe, proliferating via drive-by download on infected porn websites, among other methods. The majority of devices affected were those running KitKat and Jelly Bean. On these devices, pop-up advertising was fed in. Considerably more dangerous, however, the malware gained access to Google accounts in the background and abused them for automated click fraud.

TOP 10 Android malware 2016

1	AGENT	2,004,880
2	SHEDUN	417,945
3	FAKEINST	136,544
4	SMSSPY	134,384
5	LOCKSCREEN	131,782
6	OPFAKE	109,833
7	TROJANSMS	77,185
8	SMSTHIEF	63,279
9	LOTOOR	58,731
10	SMFORW	55,723

Trend 2017

For Android, the detection systems of AV-TEST experienced increasing numbers in the areas of banking Trojans and ransomware. The share of the latter in overall malware grew to the threefold value over the previous year. Measured in terms of the overall share of malware programs, the number of Trojans has indeed declined slightly. With over 96%, however, also in 2017, they do in fact represent the most lethal weapon of cyber criminals targeting mobile devices.

AV-TEST
av-test.org

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

本文档由Linux公社 www.linuxidc.com 整理

Security Status of INTERNET THREATS

What strategies do criminals pursue in the proliferation of malware? Anyone knowing the answer to that question can mount a targeted defense against threats from the Internet. The detection systems from AV-TEST have been detecting malware attacks around the globe for a long time now. Here is the threat analysis for 2016.

Massive amounts of spam

One look at the malware proliferation strategies of online criminals reveals numerous professional approaches: In distributing their malware programs, the vast majority of cyber crooks relied on the long-standing successful, traditional distribution channels. In particular in the year 2016, devices connected to the Internet were infected with malicious code especially by large email campaigns. International spam campaigns were therefore not only annoying but also highly dangerous. Compared to emails with infected malicious code in the attachment, the crooks frequently relied on digital messages, which attracted unwitting users with embedded links to malware-infected websites. The latest charts based on constantly measurement data can be found on the statistics pages of the AV-TEST Institute.

Germany was also among the most prolific spreaders of "bad news" in 2016. In fact, 3.1% of all spam, also including malware-infected mail, originated from Germany, putting it at Number 8 on the Top 10 of spam-sending countries. Far ahead of Germany, however, are the "spam masters" India, the United States and Vietnam, which in 2016 were responsible for one third of global spam.

Tested websites in 2016

Websites tested by AV-Test
80 Milo.

websites on the Internet
approximately 1,100 Milo.

Top 10 list of spam senders 2016

1	INDIA	12.0%
2	UNITED STATES OF AMERICA	11.9%
3	VIETNAM	11.8%
4	CHINA	5.6%
5	BRAZIL	4.8%
6	POLAND	3.4%
7	IRAN	3.3%
8	GERMANY	3.1%
9	MEXICO	3.0%
10	RUSSIAN FEDERATION	2.2%

本文档由Linux公社 www.linuxidc.com 整理

Exploit kits, hacks and malvertising

For malware proliferation via standard exploit kits, criminals created a vast number of proprietary, infected Internet pages in 2016 as well. It is true that by midyear, the malware toolkits used most often, Angler and Nuclear, had disappeared from the scene, which at least in terms of timing, correlated with the decline of overall malware statistics measured by AV-TEST. However, the much-used tools in the competitive market of exploit kits were quickly replaced by competitor products such as RIG, Magnitude, Sundown and others, with which it was possible to automate vast malware campaigns just as conveniently, also including many ransomware samples. Often the exploit kits in 2016, in an automated approach, utilized gaps in the Adobe applications Flash Player and Reader, as well as the Internet Explorer from Microsoft. The rental prices varied depending upon the exploit kit used. At $1500 per week, the exploit kit Neutrino was by far the most expensive attack tool of the malware mafia. The use of RIG at roughly $200 per week was far more economical.

In 2016 criminals also used online attacks and website hacks of highly frequented websites and online portals to distribute their malicious codes. At roughly 80 percent, the most frequent attacks occurred on unpatched online web sites created with WordPress. In second place – with roughly 15% of all attacks – were websites created with Joomla!. The attacks occurred mostly on gaps in unpatched versions, and often the attackers searched for a pathway onto the computers of their victims via outdated plug-ins.

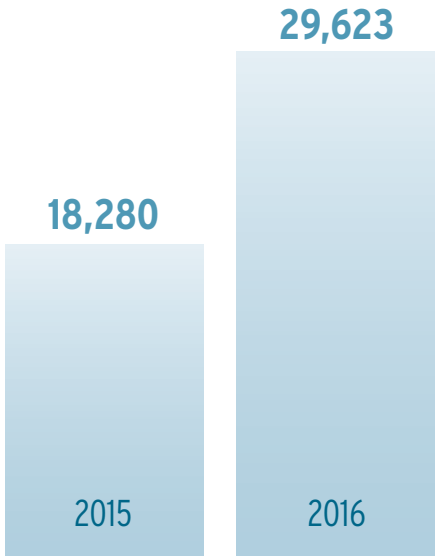
Criminals are also using with increasing frequency legal marketing tools of the Internet economy. A steadily growing trend since 2007 is "malvertising", i.e. the booking of advertising space on large and heavily-frequented websites. In this, the ad sellers of the advertising industry are usually not aware that some of their customers are transmitting malicious code via booked banners, pop-ups, links and hidden iFrames.

160 million websites in the malware check

In a comprehensive test in 2016, the AV-Test Institute examined over 80 million websites and among them, discovered exactly 29,632 Internet offers used as payloads for malware. In the previous year, the same evaluation with the same test scope only yielded 18,280 infected sites. This represents a massive increase of over 60% compared to the previous year!

The precise analyses of the AV-TEST detection systems provide a good account throughout the year 2016, showing the websites from which the greatest danger originates. These definitely include websites not protected by SSL. Roughly 92% of all infected websites were HTTP sites.

Malware embedded in tested websites



Trend 2017

The first quarter of 2017 once again reflects the same trend, by the way: The share of dangerous HTTPS sites declined by roughly 3% down to 4.9% compared to the previous year.

本文档由Linux公社 www.linuxidc.com 整理

TOP 10 malware domains 2016

1	COM	52.35%
2	SU	7.11%
3	ORG	5.04%
4	NET	4.94%
5	RU	4.05%
6	TO	4.04%
7	CO	3.24%
8	UA	1.73%
9	TR	1.37%
10	US	1.04%

The most dangerous websites

The risk of becoming infected with malware when surfing is clearly the greatest on websites with the .com top-level domain (TLD): With over 52%, .com sites are also among the most dangerous sites on the Web. The reason for this is clear: They are the sites users are most familiar with and have the greatest and widest distribution by far. What's more, they can be cheaply and quickly acquired and registered by anyone around the globe. While the choice of domain offers no measurable advantage in terms of the search machine ranking of the website, the positive psychological effect on the end-user of a common TLD is hardly to be underestimated. When in doubt, users are more likely to click on an Internet address with a common TLD. The trust level is simply higher, even if it is misleading. This is also manifest in the clearly declining interest of cyber criminals in other TLDs.

The most dangerous files

With over 33%, the most-used file formats for spreading malware are clearly led by program files in the .EXE format. Following with more than a 10% margin are compressed files with the .ZIP extension, which are also ideally distributed not only as a direct download but also per email (21%). Number 3 is the HTML format (20%).

TOP 10 file extensions malware Q1 2017

1	HTML	39.23%
2	EXE	26.27%
3	ZIP	13.95%
4	RAR	7.85%
5	PHP	6.60%
6	HTM	2.38%
7	ASP	1.84%
8	IZLE	1.74%
9	ASPX	0.10%
10	MP4	0.05%

Trend 2017

The statistics for the first quarter of 2017 clearly indicate a change in the proliferation strategy for malware: Compared to the previous year, the risk of infection through drive-by download is increasing.
At 39%, the number of infected HTML websites leapfrogged by nearly one-third, even relegating executable files to second place. By contrast, among the domains, the trend of 2016 shows a move away from country domains towards standard .COM sites. The number of .COM sites reported as infected increased by 7%.

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/.

本文档由Linux公社 www.linuxidc.com 整理

IoT
Security Status

The advantages of online networking of things of daily use are tremendous. They are already having massive impact on our daily life. This trend cannot be reversed. Although more frightening is the insufficient security of the devices on the market. The AV-Test Institute, with years of independent research work, as well as four-year certification practice, is a pioneer in the key field of IoT security.

Billions of devices without basic protection

According to estimates by financial experts from Gartner, by 2020, over 20 billion devices will be connected to the Internet, most of which, an estimated 14 billion, in private households. This assumes massive investments in hardware. Here Gartner forecasts company expenditures by 2020 of roughly $1,477 billion. Over the same time period, consumers are expected to shell out $1,534 billion for Internet-based devices. But the most profitable already now are the connected online services.

Via these types of cloud applications, billions of devices will be controlled via Internet in the future, data and information will be collected and processed by and on their users. Yet already today, a wide variety of IoT devices are sending, receiving, saving and processing diverse user data, depending upon the area of application. Smart-home bases control complete households through a broad spectrum of sensors: The products range from cameras, through burglary, fire, water and heat sensors, as well as smart lamps, right down to door locks that offer access to the home per app remote control. In the meantime, insurance companies are already developing bonus models for policies on the basis of these sensor systems.

Security by design? Not quite!

In the course of their certification practice, the IoT experts at AV-TEST have discovered again and again, however, that the security of IoT devices leaves very much to be desired. Thus, the IoT technology is developing more and more quickly and entering into ever more areas of our daily life without the device security keeping pace. In doing so, what is already a hardly-manageable spectrum of devices significantly increases the number of exploit opportunities, because producers of most devices usually do not include secure and well-implemented encryption protocols and web interfaces as well as clearly implemented authorization procedures and login processes.

Instead of paying attention to the security on the Web when developing Internet-based devices, the focus is on quick market penetration. Thus far, Internet security has frequently not been part of the product design, instead it is often perceived as an impediment of rapid go-to-market strategies. This is also due to the fact that more and more non-IT manufacturers without any understanding of online risks are producing devices connected to the Internet.

本文档由Linux公社 www.linuxidc.com 整理

Mirai botnet as an eye-opener

Toward the end of last year, the worldwide attacks by the Mirai botnet were surely an eye-opener in terms of the insecurity in the Internet of Things. Detected in August 2016 for the first time by the detection systems of AV-TEST, attacks of the IoT malware in October already caused major online services in the United States and Europe to crash by flooding their servers with address queries. For the DDoS attacks, the bundled computing power of hundreds of thousands of captured routers, printers, webcams and video recorders were harnessed via a botnet. At the end of November, criminals with other variants of the same Linux malware unleashed devastating attacks against DSL routers of Telekom customers. 900,000 devices were taken down. In October, the Mirai code appeared freely available on the Internet. Since then, the AV-TEST systems have been investigating an increasing number of samples with spikes at the end of October, November and beginning of December.

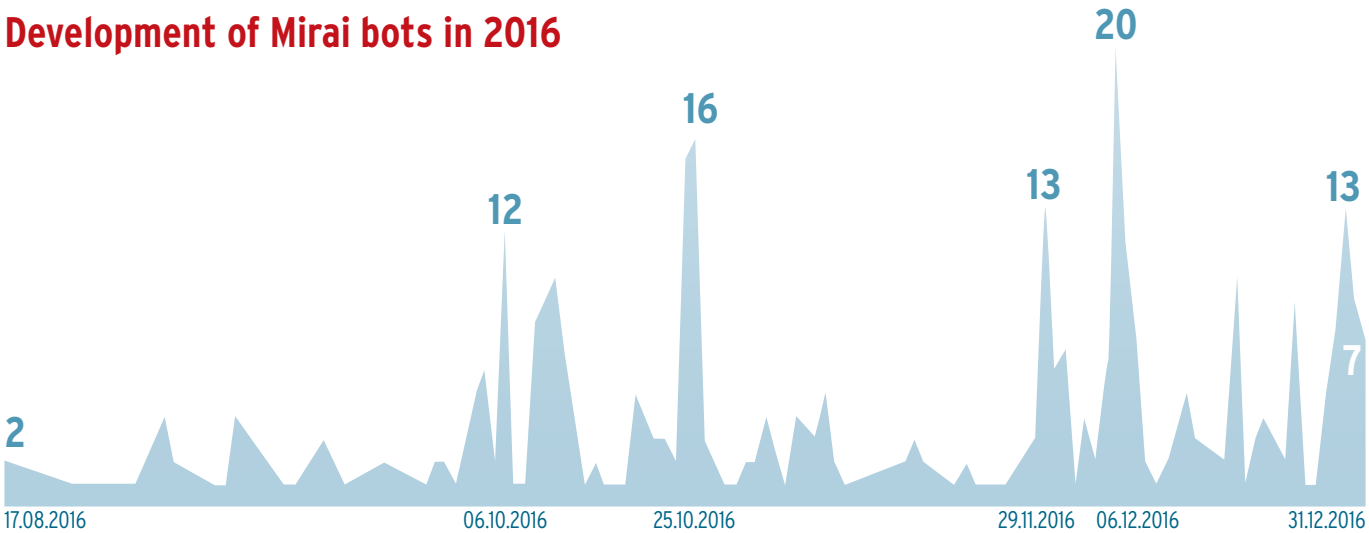
Due to programming errors, the Mirai botnet has not yet developed its full firepower. But it indicates just how high the danger is that emanates from unprotected devices on the web. Thus from devices found in private homes or even as wearables that could have impact on the health of millions of users.

IoT malware? Nothing new!

Without wanting to spread fear unnecessarily: The attacks by the Mirai botnet were surely only the beginning. Due to programming errors and the public-oriented attack variant, DDoS, the malware programs of this type were relatively easy to locate. Yet virtually none of the IoT devices offered any effective protection against the Mirai infections. Because it was not possible to retroactively secure them via safety updates and patches, nor do they have any protection concept against malware infections built into the design. And that is why the devices attacked by Mirai continue to be on the hit list of other IoT malware that existed long before Mirai. This includes, for example, malware threats of the Bashlite family, which had also targeted IoT devices running under Linux in 2016.

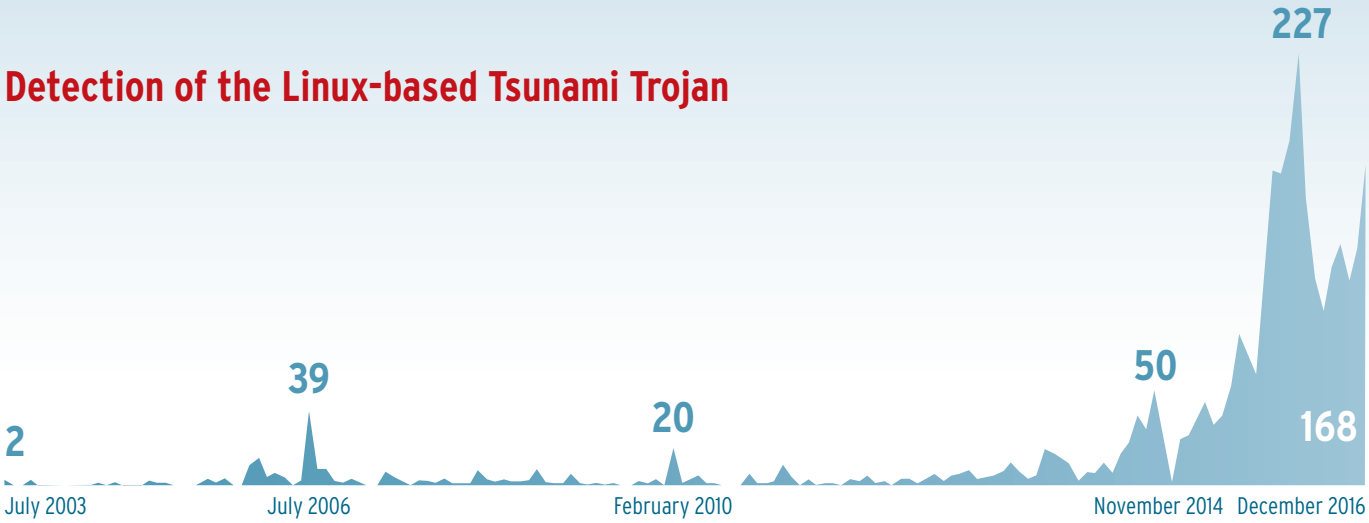
Other Linux malware, such as the Tsunami backdoor, has been causing trouble for several years now and can be easily modified for attacks against IoT devices. The detection systems of AV-TEST first detected the Tsunami malicious code in the year 2003. Although, at that time, practically no IoT devices existed, the Linux backdoor already offered attack functions which even today would be suitable for virtually unprotected attacks on routers: In this manner, Tsunami can download additional malicious code onto infected devices and thus make devices remote controllable for criminals. But the old malware can also be used for DDoS attacks. The Darlloz worm, known since 2013, as well as many other Linux and Unix malware programs, have similar attack patterns which AV-TEST has been detecting and analyzing for years. Thus, IoT malware is anything but a new threat. The new aspect is the constantly growing number and mass proliferation of IoT devices that go online without effective protection.

Development of Mirai bots in 2016



本文档由Linux公社 www.linuxidc.com 整理

Detection of the Linux-based Tsunami Trojan



Human – machine interface

People allow these IoT devices to come very close to their person or they even wear them constantly on their bodies: Because nowhere is the acceptance of IoT currently higher than in the field of sports, fitness and health. From the physician search app that provides a pollen warning to people with allergies, through fitness trackers that shares an online account with the blood pressure monitor and cardio scales, right down to devices that record medical data such as blood glucose and forwards them to the treating physician online. According to a current study from the digital association Bitkom e. V., one out of two smartphone users now also uses health apps.

Instead of ePrivacy, a sell-out of user data

IoT user data and connected online services are assuming an ever-greater significance. And thanks to increased comfort, e.g. through voice activation such as Amazon's Echo, Google's Home Assistant, Apple's Siri and additional system, this technology will gradually become barrier-free and more easily used by all generations. However, in the process, many protective barriers that have existed thus far will also fall when it comes to recording, storing, forwarding and using data. As studies from AV-TEST revealed, privacy policies either did not exist, were not correct or not understandable for 80% of the eHealth apps. And instead of accepting the privacy of users according to statutory rules, the providers sell to advertising networks the data they record through their apps by means of data recording tools and tracking instruments of third-party providers from the advertising industry. AV-TEST has documented this automated data forwarding.

Safety as a feature and competitive advantage

The attacks through the Mirai botnet were not the only ones and will not remain the only ones. That is why the AV-Test Institute recommends prescribing relevant minimum security standards and testing models as basic protection for IoT devices and services. The test and certification procedures developed by the AV-Test Institute use precisely this approach: They check for fundamental controls in the area of authentication, as well as the granting of secure online interfaces, the secure and legally compliant recording, storage, transmission and processing of data, as well as practical data protection. In this, the encryption for data transmission between devices, apps and cloud services is also proving to be a decisive component. The security of IoT devices and well-implemented protection of user data will increasingly become a competitive advantage. On the basis of the IoT certificate for Smart Home and eHealth products, customers will recognize secure and harmless devices in terms of statutory data protection.

AV-TEST GmbH regularly evaluates and certifies all relevant smart home devices and IoT solutions on the market. The latest test results can be downloaded for free from the IoT security blog at https://www.iot-tests.org/.

本文档由Linux公社 www.linuxidc.com 整理

Test Statistics

With proprietary analysis systems 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

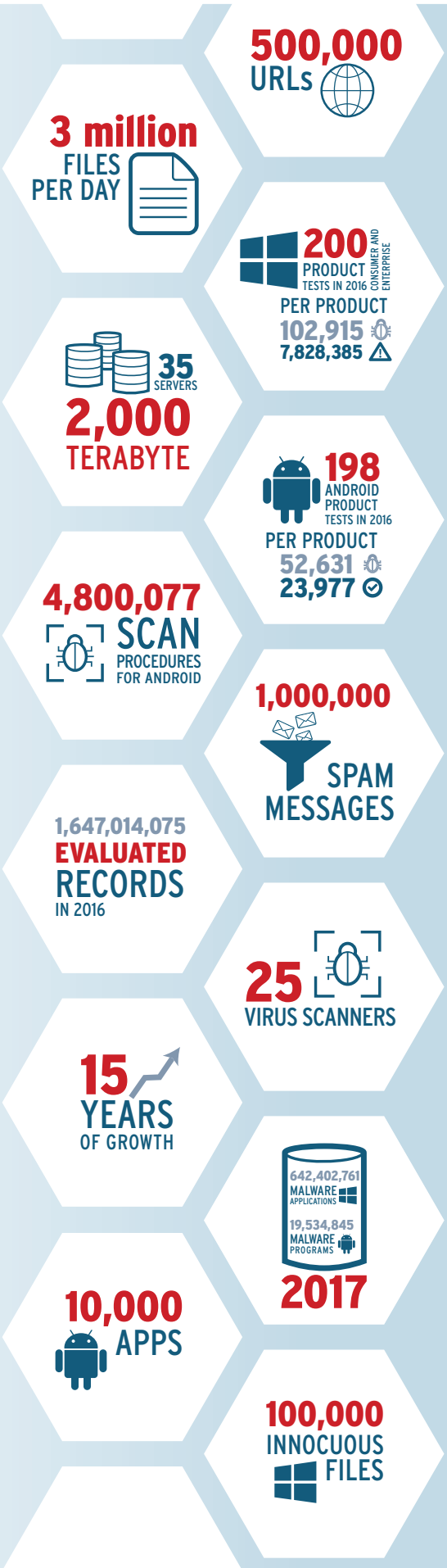
The "VTEST Multiscanner" system alone scans more than 3 million files per day. VTEST is a multi-virus scanning system offering malware analysis for Windows and Android platforms. Based on these results, a phalanx consisting of over 25 individual virus scanners provides fully automatic pattern detection and analyzes and classifies malware in this manner. The system also automatically records all proactive detections as well as response times of respective manufacturers to new threats. Thus, VTEST is constantly expanding one of the world's largest databases for malware programs. 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 642,402,761 malware applications for Windows and 19,534,845 malware programs for Android!

For targeted malware analysis, AV-TEST deploys "Sunshine", a proprietary development. The analysis system enables a controlled launch of potential malware codes on clean test systems and records the resulting system changes, as well as any network traffic generated. Based on these analyses, malware is classified and categorized for further processing. 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 10,000 Android apps every day.

本文档由Linux公社 www.linuxidc.com 整理

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 2016 over 200 product tests alone were run for consumer and enterprise products. As a result, 102,915 malware attacks and 7,828,385 individual records for false positive tests are deployed and evaluated per product. Throughout the year 2016, this amounted to 1,647,014,075 records evaluated by the test experts. In the monthly Android tests carried out through the year, the testers evaluated over 198 individual products. In doing so, each evaluated security app had to defend against 52,631 special Android malware samples. As a counter sample, the experts also recorded over 23,977 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 4,800,077 scan procedures were analyzed and reproducibly evaluated.

Every year, AV-TEST honors the best security solutions with the institute's awards. The products receiving the AV-TEST awards set new benchmarks in the test categories of protection, performance, usability and repair for consumers and corporate users.



本文档由Linux公社 www.linuxidc.com 整理

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

本文档由Linux公社 www.linuxidc.com 整理