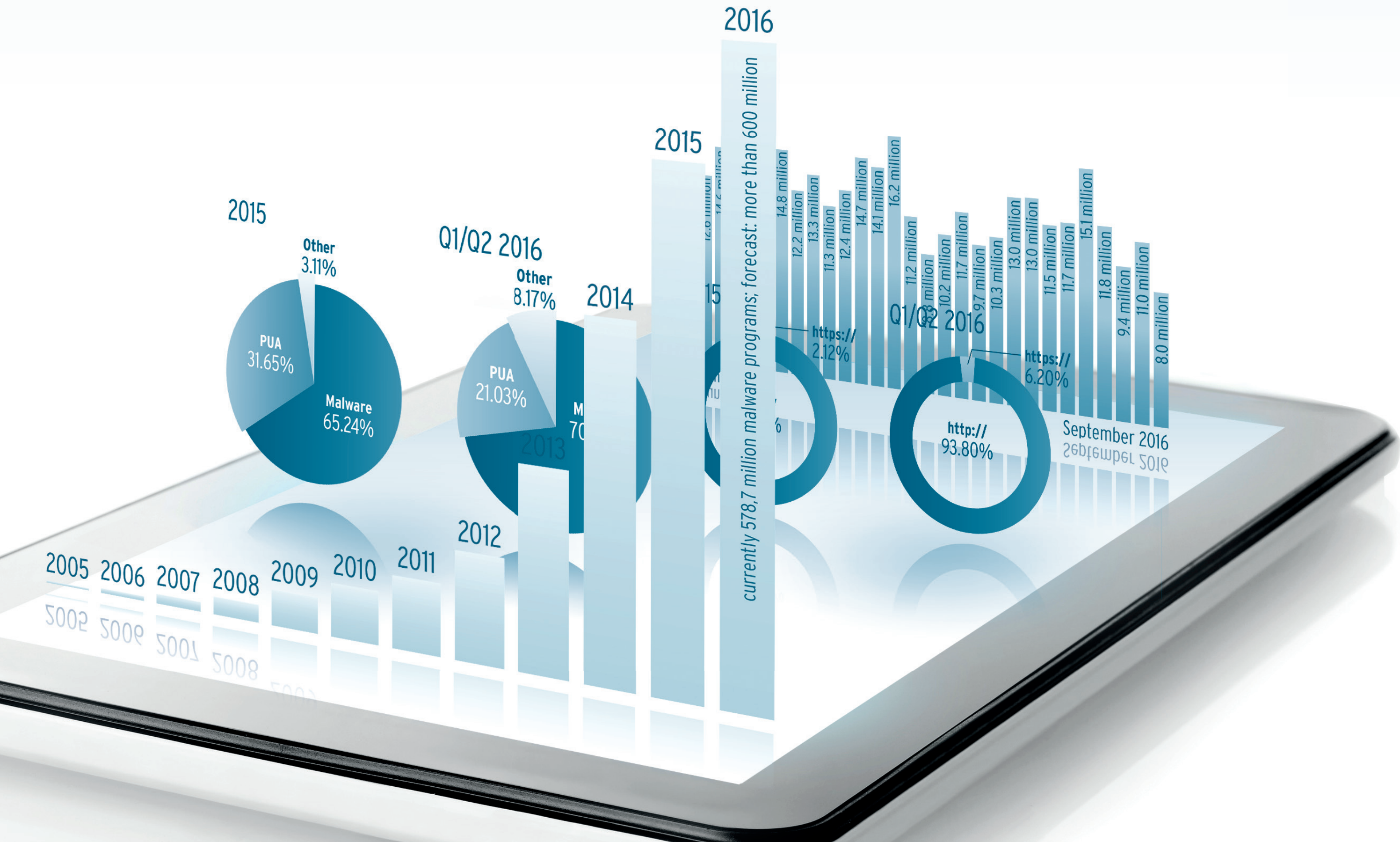
NUMBERS AND STATISTICS

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

SECURITY REPORT 2015/16

The AV-TEST Security Report 2
WINDOWS Security Status 4
macOS Security Status 7
ANDROID/MOBILE Security Status 9
INTERNET THREATS Security Status 12
PUA Security Status 14
Test Statistics 18



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

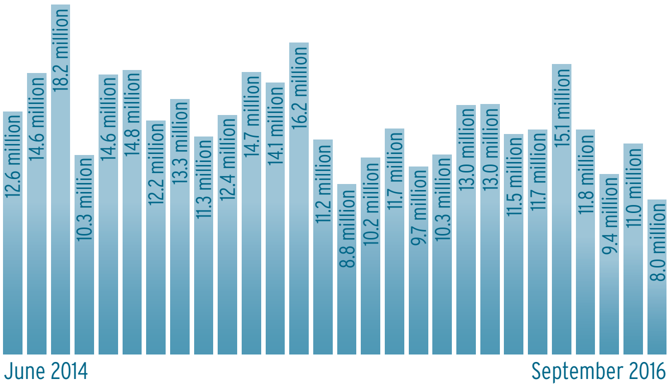
The AV-TEST Security Report

Cyber criminals think like businesspeople, and they have to. Because in their line of business, competition is growing tougher all the time. Finally the efforts they expend – from malware programming, through distribution, right down to monetization – have to pay off financially. And even if they manage to flout all other laws, they are forced to conform to those of the marketplace if they want to be successful. This is also confirmed by the numbers in this year‘s security report from AV-TEST.

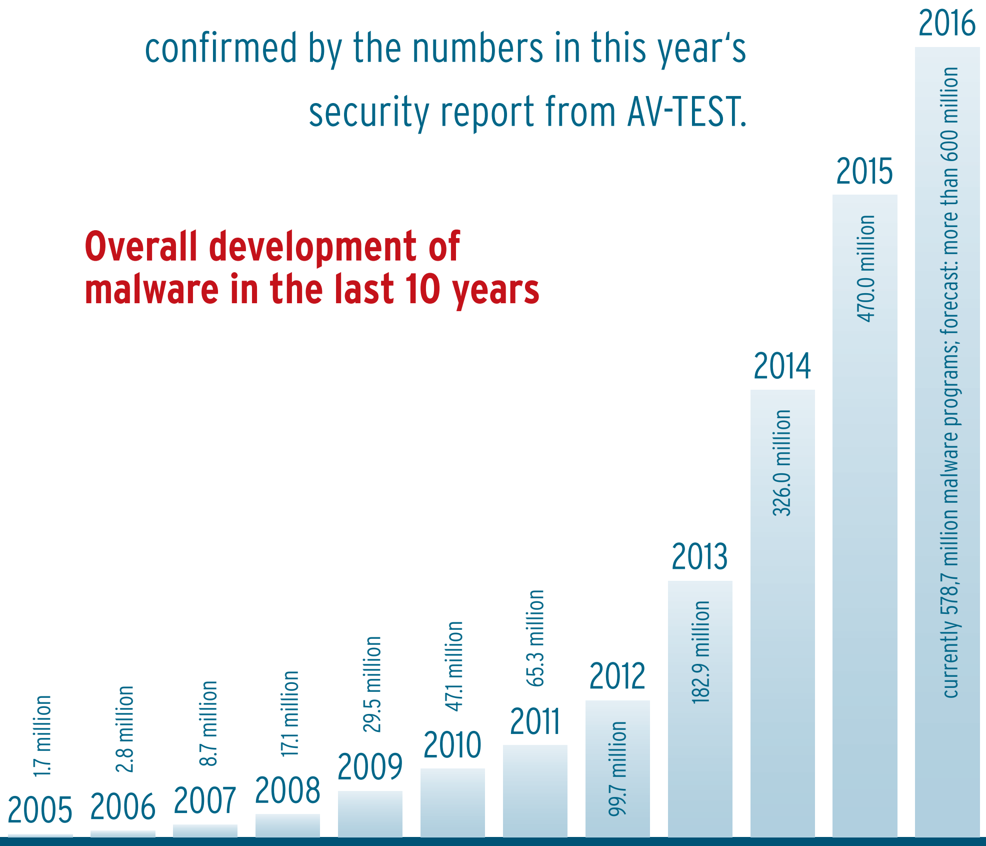
600 million vs. Windows

Thus, the development and distribution of malware adheres to strict economic principles. One of them says: "It's all about economies of scale." Accordingly, the number of malware has grown steadily since the initial tests by AV-TEST in the year 1984. Upon completion of this report, the number of known malware for Windows PCs in the AV-TEST database was at 578,702,687, with strong signs of growth. Currently, 12 million new Windows malware samples come "onto the market" each month. And so it is safe to assume that the number of malware programs targeting the Redmond operating system will break the sound barrier of 600 million even before the end of this year.

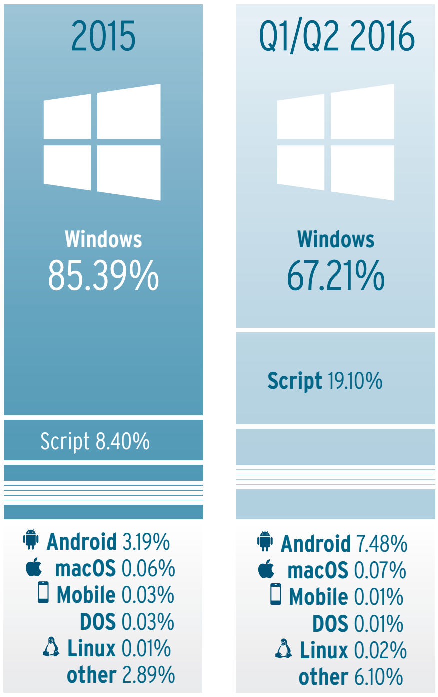
Total occurrence of new malware



Overall development of malware in the last 10 years



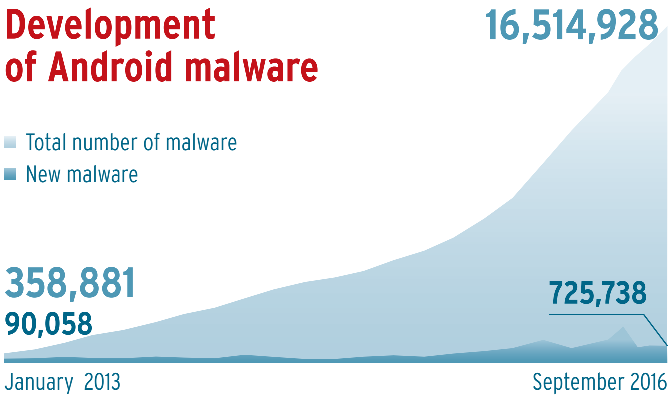
Malware detection sorted by operating systems



Android increasingly under fire

When it comes to targeting their attacks, criminals also follow strict economic principles and go where the market is. As a result, in 2015 the absolute majority of malware, 85 percent, targeted Windows, the world's most widely-used operating system. Coming in second, with more than three percent, but clearly an also-ran, was Android, the most widely-used mobile platform. And comprising a mere 0.06 percent, Apple's operating systems ranked third in 2015 on the popularity scale of malware attacks. Naturally, Linux, along with operating systems for mobile devices, were under attack, too. The share of malware programs for these platforms was negligible, however, which still says nothing about the risk potential of attacks launched on these platforms.

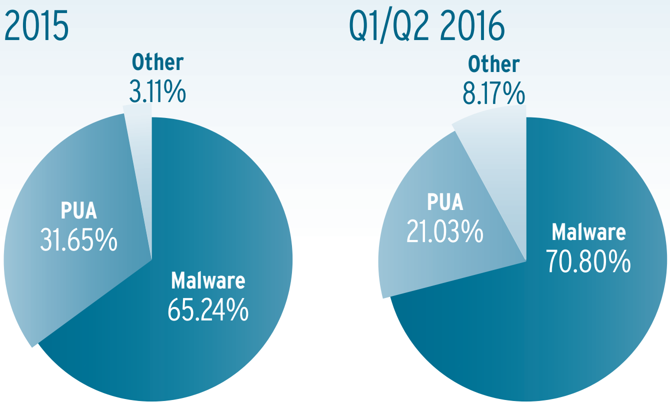
Development of Android malware



Trend 2016

The test results of the AV-TEST detection systems indicate in the current year a significant trend away from Windows and towards Android. Thus, the number of malware samples for the Microsoft system declined from 85 to 67 percent over the previous year. By contrast, Android is becoming significantly more attractive to criminals. The increase from 3 to 7.4 percent sounds more harmless than it really is, as there was in fact a doubling of the malware numbers. As a result, the AV-TEST systems recorded already 12,998,160 malware programs for Android by mid-June of this year. In the prior month of May alone, there was an increase of just under one million new harmful applications. So it is surely a trend worth keeping an eye on, as criminals are apparently massively expanding their activity in the Android field.

Total number of malware



PUA: attack by the industry

But malware was not the only threat for Internet users in 2015. While attacks through malware are clearly attributable to criminals, there is looming danger to privacy from a completely different corner: In addition to growing numbers of malware samples, the AV-TEST Institute also saw an extreme increase in PUA in 2015. These potentially unwanted applications often come piggyback onto the device with downloads of useful programs and apps. PUA is deployed by the advertising industry to track personal information concerning user and movement patterns and to display unwanted, personalized advertising. What's more, PUA usually operates secretly and without the consent of the user. To the extent that industrial spy tools such as these can be identified as malware and blocked by antivirus programs remains a subject of heated controversy. In the detection systems of AV-TEST, PUA represented just under one third of the online risks in 2015. Because attacks to users' privacy are ever-increasing on all platforms, AV-TEST is dedicating an entire chapter to PUA development in this security report.

Trend 2016

In the first half of this year, the AV-TEST systems recorded a decline of PUA. Whereas the numbers recorded last year were still at 31 percent, thus far they have declined to 20 percent. However, this only represents a trend. And because thus far, there is no clear policy apparent both in the detection by antivirus manufacturers as well as in the self-regulation and commitment on the part of the advertising industry, AV-TEST will continue to keep a watchful eye on PUA proliferation.

WINDOWS Security Status

The Microsoft ecosystem by far sustains the most attacks and the highest number of malware samples of all operating systems. More on this topic below:

Windows as the main target of attack

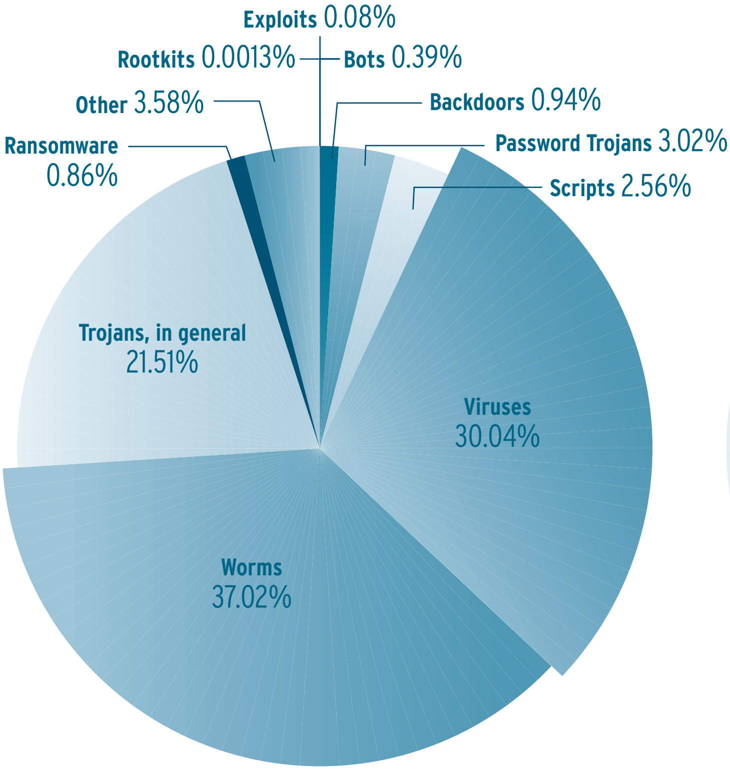
As a strategic target, Windows systems, not least due to their high prevalence, were especially in the crosshairs of criminal threats in 2015. In this, 99.69 percent, or virtually all of the attacks registered by the detection systems of AV-TEST were aimed at the 32-bit versions of this widely-used operating system. Because malware that works on 32-bit versions can also successfully attack 64-bit versions, special 64-bit malware is an absolute rarity (0.31 percent).

Trend 2016

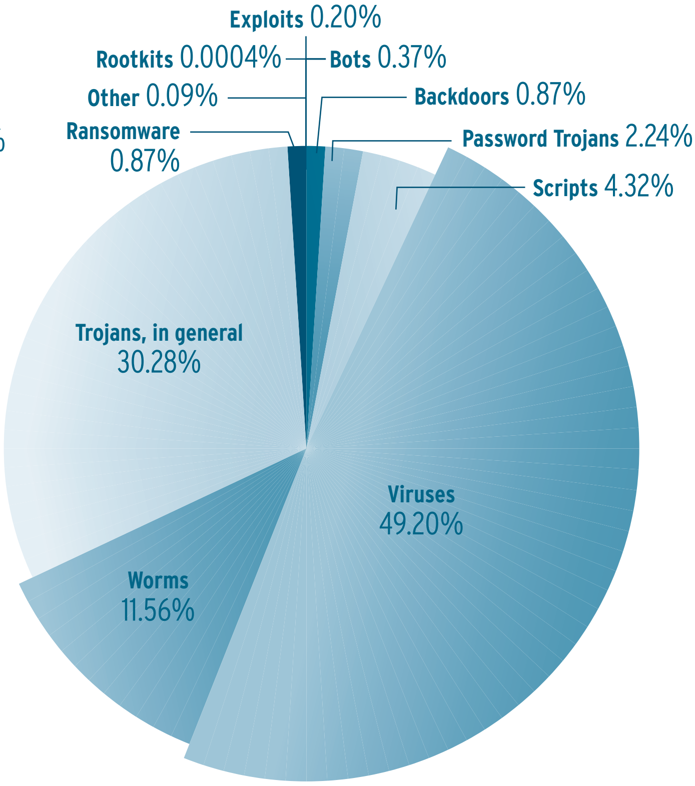
The first half of the year also confirms this development. Windows remains the main target of attack, however, almost exclusively the 32-bit versions (99.7 percent). The incidence of special 64-bit Windows malware is continuing to decline.

Distribution of malware under Windows

2015



Q1/Q2 2016



A big can of worms was opened in 2015

For malware attacks on Windows users, criminal attackers in 2015 deployed worms extremely often. More than one third of all malware detections involved this pesky variant. Worms proliferate independently and usually enter PCs via infected websites. But also via mail, P2P networks, through chat applications and even by means of Bluetooth connections, they can hijack the computers of their victims. Given their high potential for proliferation, they have often been deployed to infiltrate large networks, which they subsequently made exploitable for the attackers with any desired reloadable malicious code.

In second and third place, traditional computer viruses followed, as well as the large army of specialized Trojans, including banking Trojans and the widely distributed ransomware in 2015. Together with worms, these malware types already constituted 92 percent of the total number of malware waiting to take Internet users by surprise in 2015. With the exception of malicious scripts, with which attackers manipulated websites so as to automatically carry out malware code attacks on visiting Windows PCs (2.56 percent), all other types of malware remained in the range of below one percent.

Trend 2016

Up to the middle of this year, the number of Internet worms deployed for attacks noticeably declined compared to the previous year, indicating a shift from 37 to just under 11 percent. Conversely, the distribution of traditional viruses and Trojans, however, is sharply increasing. Thus, virus distribution alone is increasing by 19 percent compared to last year!

TOP 10: worms and ransomware reach top rankings

As a result, the Top 10 of the most widely-distributed malware programs of the year 2015 are exclusively made up of worms, viruses and Trojans.

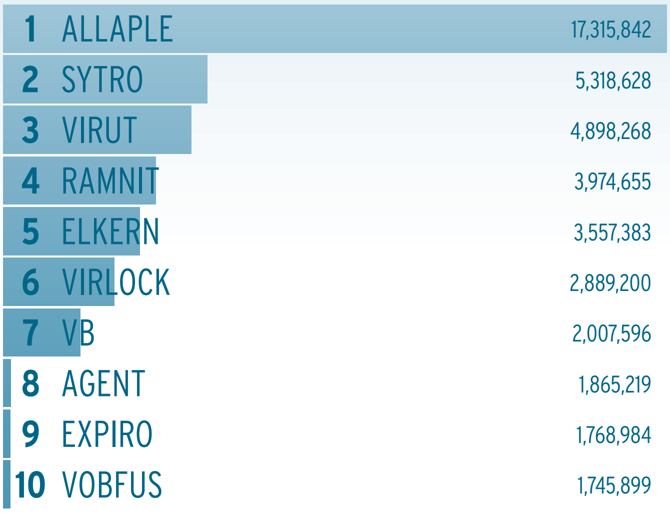
The Internet worm "Allaple" achieved the dubious No. 1 ranking as the world‘s most active malware threat in 2015. This pest has been wreaking havoc already since 2006: Through infected websites, it hijacks PCs through unpatched Windows vulnerabilities and, via basic brute force attacks, it can even launch attacks on servers with weak password protection. It belongs to polymorphic viruses. This means that it changes its code with each stored copy for proliferation. In doing so, it presents a tough challenge for basic virus scanners. In addition to spreading malware code, Allaple formerly had a clear mission: Through infected systems, it carried out DoS attacks on websites of Estonian Internet providers. While in 2010 the programmer of the malware code, a 44-year-old Estonian, was already revealed, convicted and sent to jail for 2 1/2 years, his worm continues to cause mayhem on the Internet.

At No. 2 among the Top 10 of the most widely-distributed malware threats is also an Internet worm. However, in 2015 "Sytro" replicated itself almost exclusively via email from infected systems. And this occurred on a massive scale, as it is equipped with its own SMTP engine. The mail worm was first spotted at the end of 2006.

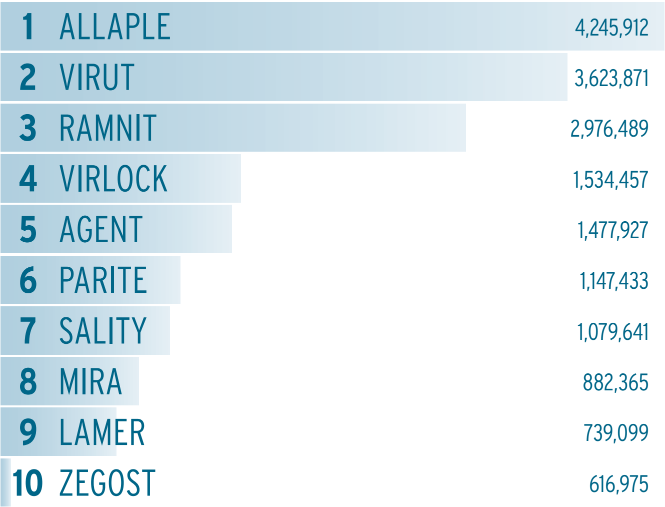
"Virut" and "Elkern" at No. 3 and 5 are also an old nemesis to virus experts: While the traditional HTML virus Virut was already finding its way onto PCs since 2007 via infected websites through browser gaps, Elkern has already been active since 2001, destroying files on infected computers it hijacked via infected data packets from file sharing networks.

At No. 4, "Ramnit" first appeared on the radar of virus experts at the AV-TEST labs in the beginning of 2010. The virus exploits a wide variety of pathways to spread over the Internet. This includes infection via FTP download, attacks over infected websites, portable storage media, and even in combination with PUA, it can smuggle its way onto a computer. Its mission: hunting for dial-up data for online banking accounts and for credit card data. In doing so, the sophisticated malware leaves almost nothing to chance. It searches through typical program folders and storage areas for password files, monitors Internet access to banking portals in order to funnel money through it during

TOP 10 Windows malware 2015



TOP 10 Windows malware Q1/Q2 2016



bank transfer transactions via a man-in-the-browser attack. When Ramnit finds something, it sends the highly sensitive information via a secretly established Internet connection to the individual behind the attack.

With "Virlock", ransomware is also represented among the Top 10 of the most widely distributed malware programs of 2015. This encryption Trojan is the only malware sample in the Top 10 that was spawned or first detected in the year 2015. Virlock also belongs to the polymorphic malware threats, thus also making it extremely difficult for security programs to hunt it down, due to its constantly changing code. Apart from that, security programs have to follow more stringent rules as it is when detecting ransomware: For crypto-malware like Virlock, speed is of the utmost essence. Because once it is active on an infected system, the malware immediately begins encrypting certain files and folders, including EXE files, archive files, audio, video and image files, as well as the "My Documents" folder. The more quickly a security program reacts, the less time remains for the malware to hijack key files. If it reacts too slowly, the PC protection may become affected itself, as Virlock encrypts not only EXE files but also certificates.

Trend 2016

The first half of the year saw not only shifting positions but also changes in the Top 10 malware. Along with Parite, also a virus which constantly alters its program code, four additional new players have entered the Top 10.

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/.

AV TEST
av-test.org

macOS
Security Status

Hardware on which an Apple operating system is running has always been considered safe per se. But appearances can be deceiving. While there is considerably less malware than for Windows, Mac users still need to be protected.

The Mac fortress: just an illusion

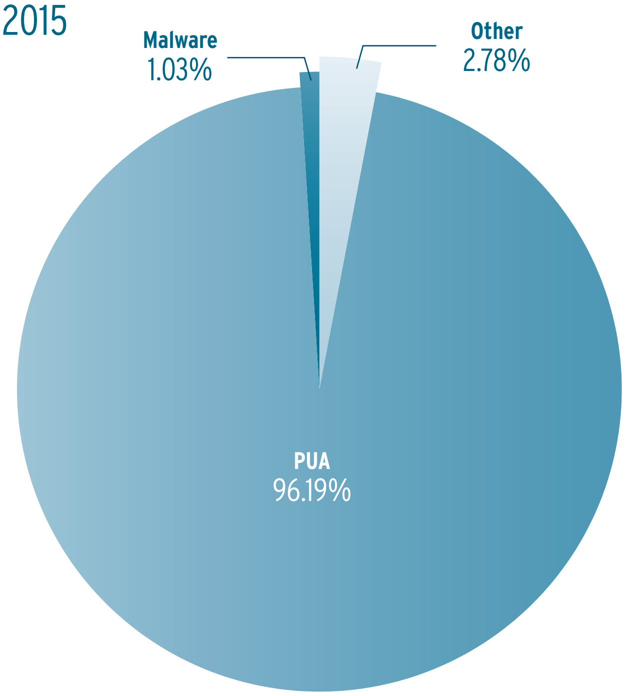
"It's a pretty sure bet that your Mac cannot be infected with a virus. It is far more likely for other security-relevant or technical issues to occur that have nothing to do with malware threats, however." Many users of the hardware and software manufacturer recite this official Apple statement almost like a mantra when the subject of malware threats for Apple systems is raised. And that's the bottom line for many users: I use a Mac, so I don't need virus protection. This motto applies even where Macs are used in a business setting, which is possibly a miscalculation.

Mac threat: small but oh boy!

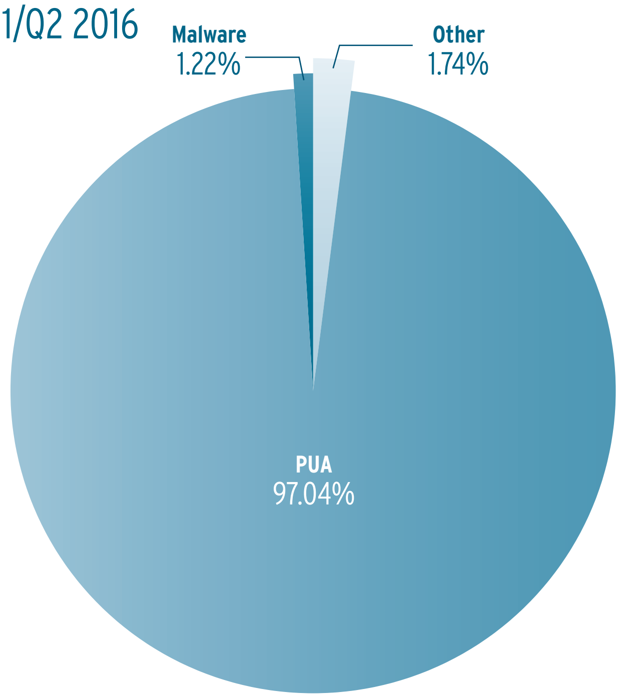
In reality, the number of malware programs identified by AV-TEST scan systems for Apple's Mac platform is minuscule compared to Windows. A mere 819 malware threats targeted Mac users in 2015. But as with Windows and Android, these quantitative parameters say nothing about the quality of an attack unleashed by the malware samples deployed. On the contrary, you could hypothesize that attackers do not need to program a large number of malware applications to obtain important data from Mac users, as they almost never protect their machines with antivirus solutions anyway.
It cannot be said for sure how frequently Mac users are actually subject to malware attacks. The fact is, however, that no later than 2014 during the "Flashback" wave of infection, Apple had to retract its bold statement that

macOS malware

2015



Q1/Q2 2016



"a Mac cannot be infected". Back then, the Flashback Trojan hijacked some 600,000 Mac computers through a Java exploit in macOS X, previously believed to be impenetrable, forcing them into a botnet as computer slaves.

For older, non-patched Mac versions, Flashback was still a risk in 2015, as the AV-TEST systems indicate: Among the top 10 malware threats, the Trojan is No. 8.

Ranked No. 2 was the Trojan "Jahlav", which in the first quarter of this year ascended to the No. 1 position among Mac threats. The malware threat can reload random malware code from the Internet on infected Macs and launch processes unnoticed in the background. Jahlav comes as a video codec per download on the Mac.

TOP 10 Mac malware 2015

1	AGENT	116
2	JAHLAV	89
3	GETSHELL	67
4	XCODEGHOST	65
5	MORCUT	63
6	MACNIST	52
7	YISPECTER	39
8	FLASHBACK	23
9	OPINIONSPY	18
10	TUNEUPMYMAC	16

Trend 2016

Also in this year, we don't expect to see any excessive attack waves on Mac computers. The fact is, however, that malware for macOS exists, and so does the necessity to take precautions against viruses.

TOP 10 Mac malware Q1/Q2 2016

1	JAHLAV	102
2	XCODEGHOST	84
3	GETSHELL	60
4	MALWARE	28
5	TINYV	23
6	ACEDECEIVER	20
7	WIRENET	18
8	KERANGER	17
9	OCEANLOTUS	14
10	FLASHBACK	13

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/.

AV TEST
av-test.org

ANDROID/ MOBILE

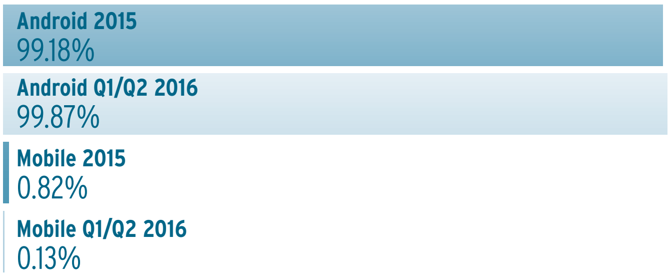
Security Status

When we speak of threats to smartphones and tablets, we also automatically speak of Android. Google's operating system can be used most effectively for criminals.

Market predominance generates interest

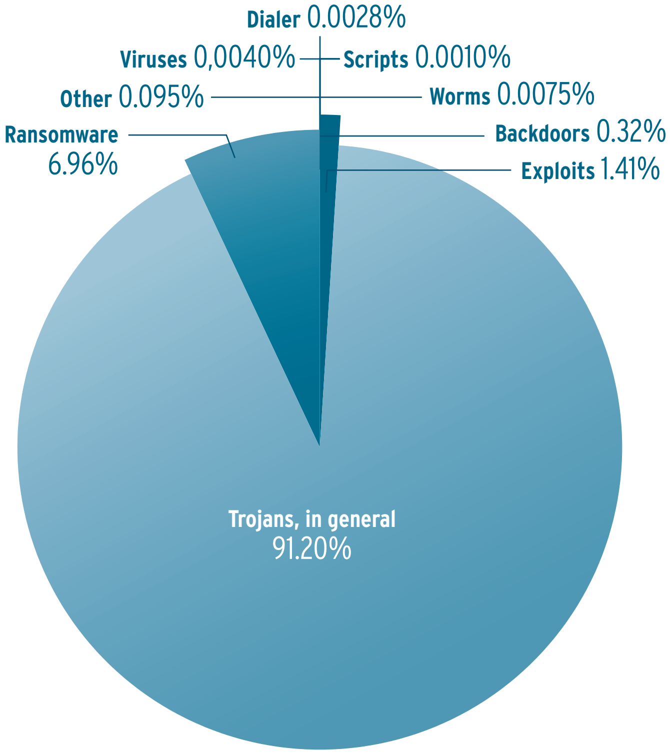
As already indicated, 85 percent of malware programs target the Windows operating platform. This does not mean, however, that users of other operating systems shouldn't be concerned about the safety of their data. It is true that of overall malware, the just over three percent for Android may seem negligible at first glance. However, in preparing this report, the AV-TEST systems detected nearly 17 million malware samples for Android, the most heavily-used mobile platform. Interestingly, criminals were initially quite hesitant in the development of malware for the open-source Google system, launching only a few infected apps in the year 2013. In the beginning, they were satisfied to siphon off small amounts of money via stealth dialer programs.

Android malware vs. mobile

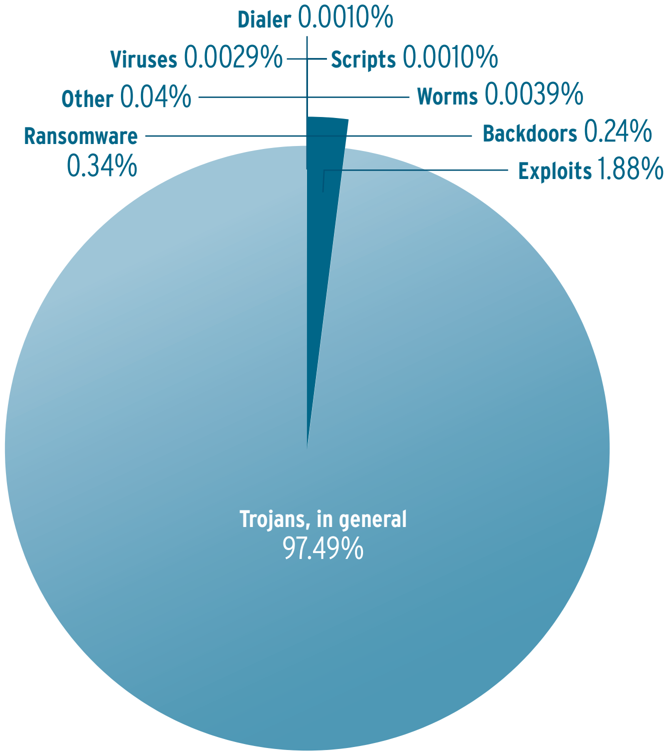


Distribution of malware under Android

2015

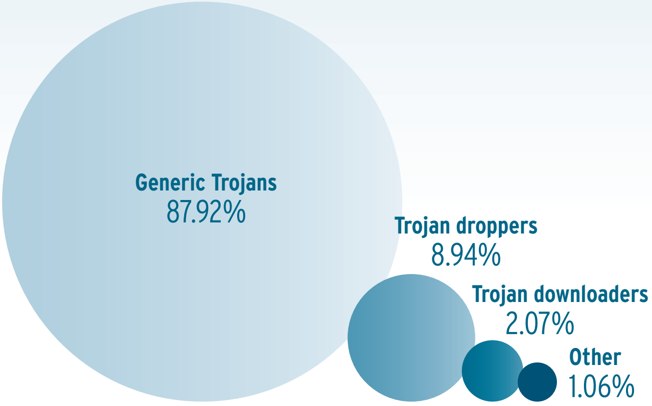


Q1/Q2 2016



But with the increasing distribution and rising sales of smartphones, tablets and other Android devices, the platform more and more became an attractive target for abuse. And with increasing deployment opportunities via a corresponding range of apps, the malware options were also adapted. To that extent, the market situation can be considered cut and dried: And consequently, currently over 99 percent of all malware programs targeting mobile systems are aimed at Android devices. Other platforms are at the moment not of interest to cyber criminals, either due to insufficient market significance, or due to a closed app infrastructure. They can only be exploited with excessive effort. That is why the malware situation surrounding these systems is insignificant here.

Distribution of Trojans under Android in 2015



Trend 2016

AV-TEST monitoring results from the first half of 2016 underscore the 2015 tests: Also in 2016, mobile systems, such as iOS and Windows Mobile, are of less interest to cyber criminals, as Android can be more efficiently exploited by them.

Trojan attacks on Android

Whereas criminals tried their luck with dialers in the initial phase of Android, that gimmick has long since faded away. Of the over 2 million Android malware samples revealed by the AV-TEST systems in 2015, there was only a negligible number of dialers, a mere 58 malware samples. That is little cause for celebration, however, because when we examine the distribution of Android malware more closely, in addition to the sheer mass, we mainly see the "innovative speed" of the cyber criminals. Although the initial makeshift malware samples for Android were first discovered in 2013, a mere four years later, the AV-TEST systems registered the full spectrum of malware codes currently available: In just a short period, the dialers have now been flanked by viruses, worms, malicious scripts, backdoors and Trojans. Consequently, the malware situation for Android devices is increasingly moving in the direction of Windows PCs. This is no surprise, as practically every application, from email to online banking, which just a few years ago had to be completed on a PC, now conveniently functions on a mobile device via corresponding apps. And while Windows users have long since come to the realization that their PCs require virus protection, the use of relevant protection apps on Android mobile devices is not as prevalent by a long shot. In combination with manufacturers' often insufficient and tedious patch releases in response to known security gaps, Android is becoming an optimal target for criminals.

The use of specialized Trojans appears to be especially lucrative for criminals as of late. Because with practically 1.9 million registered samples, this malware class (91.2 percent) represents the main threat to Android users. Even if generic Trojans with 87.9 percent represented the largest share in this malware group in 2015, it is worth also examining the already existing spectrum of code development here: Because in a very short time - at least on a substantial level - all the malware functions that exist for Windows have become available here as well. Thus, the number of encryption Trojans in 2015, for example, was still relatively low at 144,008. Nevertheless, it is worth noting that criminals have rapidly found a way to migrate this extortion model, which obviously works very well on Windows, onto the Android platform. The same is true for criminal hacks into mobile online banking using Trojans: Although not all banks by far offer an app allowing Android users account access, the existing apps are already being attacked by 20,051 Android Trojans specialized in online banking. At just over one percent, these still represent a negligible share of the overall threat potential. With increasing user acceptance of mobile banking, their number will most certainly multiply quickly, however.

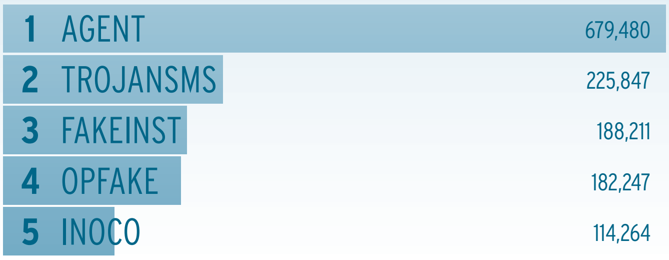
Top 5 Android malware

No. 1 among the most widely-distributed malware programs in 2015 was "Agent". The Android Trojan is remarkable, not only because of its vast proliferation. Because unlike many other malware that enters Android devices via infected apps and thus have to be inadvertently installed by their users, this malware has an additional proliferation tactic: Similar to Windows malware, Agent can hijack unprotected devices of its victims when they visit infected websites. It also spreads primarily via infected apps, however. Once it is on the device, the Trojan can also load other malware or offer attackers the opportunity to downgrade the security settings of the infected device remotely and thus enable the theft of personal information.

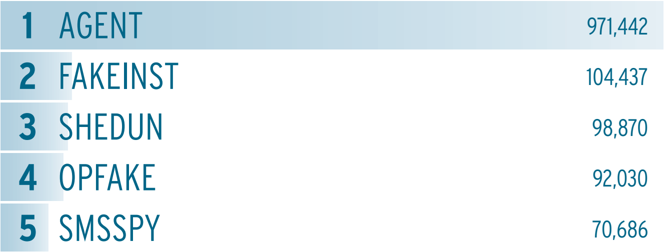
With "TrojanSMS", a true classic of mobile malware programming was ranked No. 2 out of the Top 5 for Android malware: Anyone catching malware from this Trojan family through the installation of a fake app primarily faced the prospect of being ripped off by two different types of attackers: On the one hand, malware samples of this type generated considerable costs through secret use of paid text message services. On the other hand, the access to the text message function by the malware had even greater ramifications. Because the Trojan was also targeting M-TANs for online banking sessions received by text message.

As with TrojanSMS, the following Top 5 Android malware samples rely on the user's committing a confusion error amid what is virtually an unmanageable plethora of apps. That is how the Trojan "FakeInst" disguised itself as a supposed virus protection solution, and the Trojan "Opfake" had the appearance of a mini version of the popular Opera browser. What all these malware samples have in common is that they exploit the text message functions of hijacked devices and are also capable of downloading additional malicious code by the same means.

TOP 5 Android malware 2015



TOP 5 Android malware Q1/Q2 2016



Trend 2016

With "Shedun" (No. 3), a new, powerful malware enters the stage of the Android Top 5. It owes its high level of distribution to the sheer mass of fake apps available to Android devices. The malware conceals itself among just under 20,000 fake apps – including Facebook, Twitter, Snapchat or WhatsApp – downloaded from third-party app stores. Infected devices are rooted in the background and, among other things, deluged with advertising.

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/.

Security Status of INTERNET THREATS

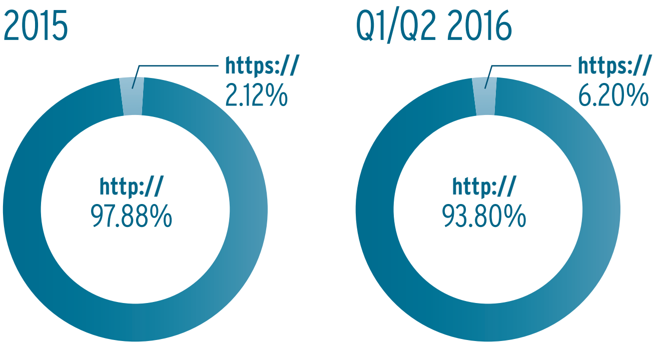
For criminals, the Internet is the most effective pathway for distributing malware. Statistics from AV-TEST labs explain why.

HTTP as an Achilles‘ heel for malware

The AV-TEST analysis systems record and list "Blackhat SEO" and "Webdust PE URL" Web threats currently waiting to ambush Internet users. In particular, this includes websites infected with malware. Already when calling up such infected online sites, malware attempts to hijack visiting PCs via software vulnerabilities. For such drive-by downloads, criminals create their own websites that they advertise by means of vast spam campaigns. But even well-known and frequently-used online sites become hacked and infected for purposes of malware proliferation. As the detection systems of AV-TEST indicate, in 2015 attackers almost exclusively used websites with the unprotected transfer protocol HTTP for distributing malware (97.88 percent). Attacks via HTTPS sites were almost non-existent (2.12 percent).

The ranking of the most frequently-used domains for distributing malware programs last year was led clearly by the top level ".com" domain, which comes as no surprise. It is by far the most widely-distributed domain and can be quickly and easily registered by anyone. Ranked No. 2 on the Top 10 dangerous websites was the Russian ".ru" domain, and even the Soviet Union (".su") came back to life in the realm of cybercrime at No. 4. The ".org" domain was also a tempting target for attackers in 2015, because it is utilized mostly by free software projects and open-source providers. It is conspicuous that European country domains followed close behind. Countries with a well-developed data network and many online users such as Russia, Italy, Germany and Poland were high on the list for attackers in 2015.

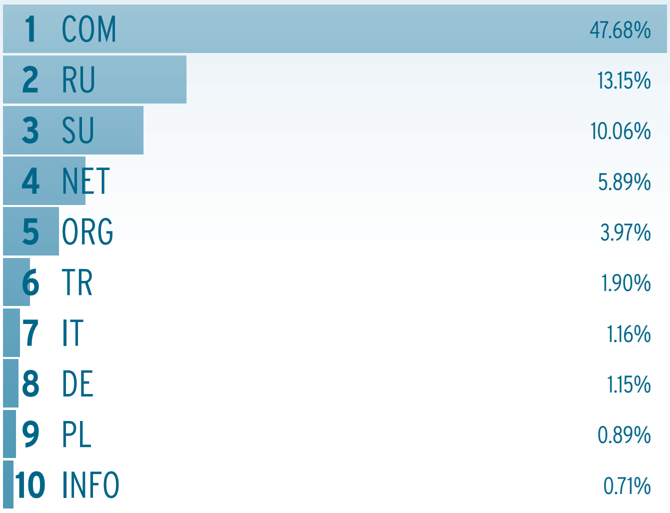
Distribution of malware on encrypted and unencrypted websites



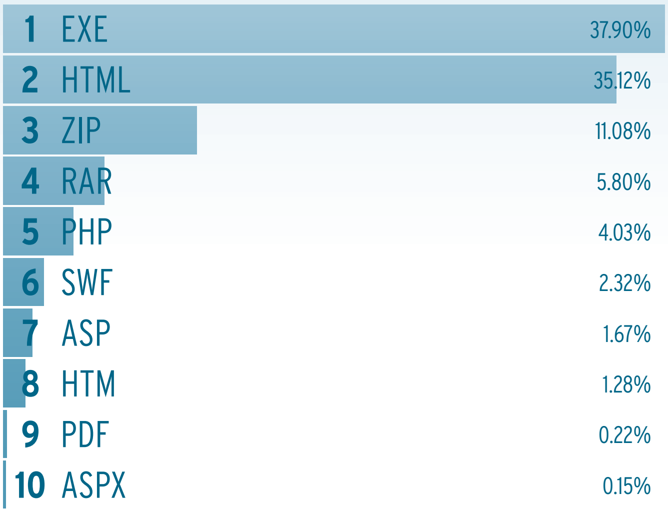
Trend 2016

In the first half of 2016, the number of attacks on HTTPS sites tripled, reaching 6.2 percent. For the domain ranking, the latest results of the AV-TEST systems indicate a geographic shift in the direction of North America and into the English-speaking language group. Thus, US sites have reached No. 7 among malware URLs. By contrast, all European sites except for Germany have disappeared from the Top 10. Germany dropped from No. 6 to No. 8.

TOP 10 malware domains 2015



TOP 10 file extensions malware 2015



Dangerous “EXE“

The ranking of data formats most frequently used for the distribution of malware was clearly led by executable "EXE" files in 2015. The share of malware distributed through this format was significantly higher than that of HTML and ZIP formats. An additional data compression format appears at No. 5 on the Top 10 of the most dangerous file formats: the RAR format. In 2015, traditional online formats continued to be a popular way of distributing malware: PHP, HTM and similar formats were frequently used to embed malware in websites. Attacks via infected ASP files often targeted victims who were duped into thinking they had to install Flash player updates. Last year, criminals also relied on the PDF format, because like the compression formats, it is suitable both for sending emails containing malware and for infections via download.

Trend 2016

For the first half of this year, the analysis systems at AV-TEST indicated changes above all among the frontrunners of the Top 10: While criminals continue to use the EXE format for disturbing malware, they are in fact using HTML formats significantly more often. These surpassed executable files in the first half of the year, relegating them to the No. 2 spot on the Top 10.

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/.

PUA Security Status

The number of potentially unwanted applications (PUA) registered by AV-TEST systems are not only steadily increasing, they are also now threatening the privacy of users on all standard platforms.

Windows users main PUA target

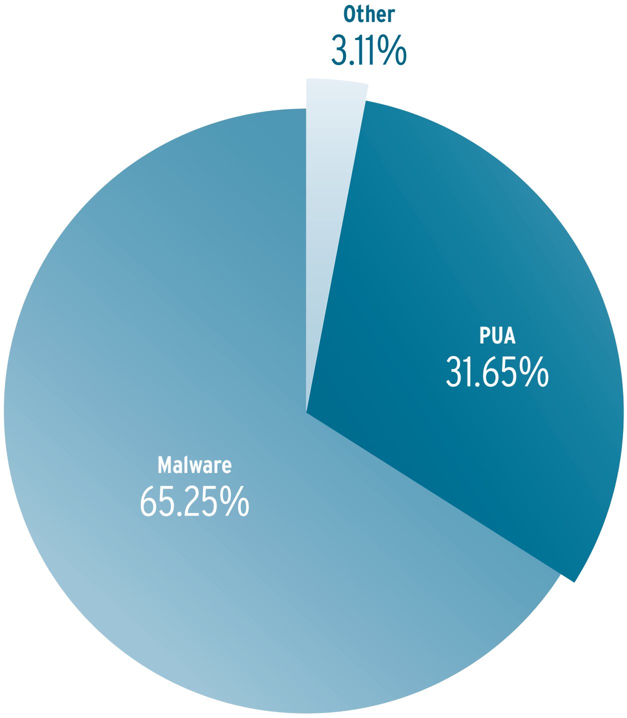
With PUA detections in the year 2015 numbering more than 37 out of over 40 million, above all Windows users fell under the control of the advertising industry (94 percent of all detections). Yet on all other software and mobile platforms, spy applications targeted surfing habits and other personal information of online users. 412 samples were even recorded for Linux. And while the malware statistics for Mac computers in the year 2015 were quite low at 819 samples, it was a whole different story in the area of PUA: Over 76,000 samples were launched to ferret out the online and usage habits of Mac Internet users.

Windows remains the key target of attacks

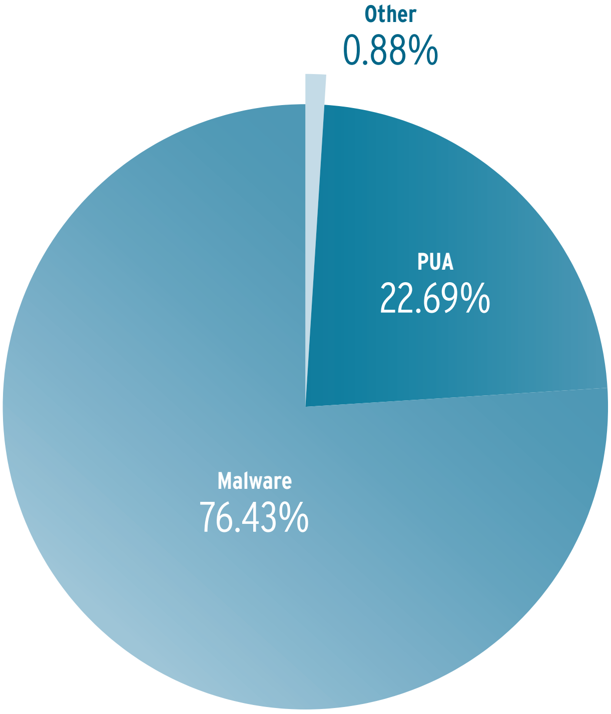
This was most certainly not due to the most frequently-deployed spyware "Multiplug", however, as evidenced by the PUA Top 10. The No. 1 among the Top 10 logs the surfing habits of infected PCs and secretly sends relevant profiles via Internet to advertising firms. It is subsequently possible to selectively modify websites in the browser, as well as to display additional websites with relevant adapted advertising (pop-ups). Multiplug usually enters computers in a bundle with free tools via freeware platforms.

Total number of PUA detections

2015



Q1/Q2 2016



TOP 10 Windows PUA 2015

1	MULTIPLUG	7,655,388
2	BROWSEFOX	4,269,061
3	SOFTPULSE	3,845,293
4	OUTBROWSE	2,463,053
5	INSTALLCORE	1,466,608
6	MORSTAR	1,460,919
7	LINKURY	1,337,107
8	LOADMONEY	1,246,415
9	SOLIMBA	738,053
10	AMONETIZE	601,900

TOP 10 Windows PUA Q1/Q2 2016

1	BROWSEFOX	2,149,379
2	OUTBROWSE	1,117,703
3	INSTALLCORE	761,292
4	ICLOADER	455,582
5	DOWNLOADGUIDE	303,663
6	LOADMONEY	284,867
7	LINKURY	226,756
8	TOOLBAR	222,771
9	ADLOAD	205,302
10	SOFTPULSE	201,883

The No. 2 "Browsefox" is also secretly installed on PCs as part of download freeware. The adware installs add-ons in Microsoft's Internet Explorer, Mozilla Firefox, as well as Google Chrome and modifies the home page of the browsers and their search engine preference. In addition, the malware displays personalized advertising on websites visited and launches pop-up banner ads.

All other Top 10 PUA function by spying on the user behavior and surfing habits according to similar patterns and are detected accordingly by the AV-TEST systems.

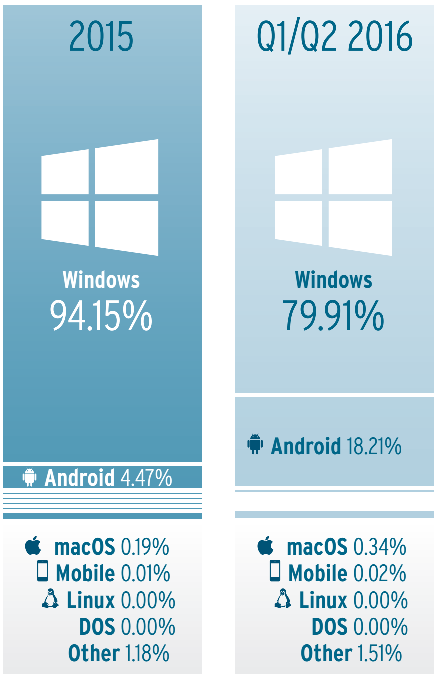
Android increasingly the focus of spying

As already determined, the number of PUA samples for Android detected by AV-TEST increased dramatically from 2015 to 2016. However, this also does not conclusively resolve the question as to what exactly is meant by "potentially unwanted". On the one hand, because it is a legal gray area, and the providers of protection apps offering PUA detection do not wish to unnecessarily walk into the firing line of an army of attorneys representing the advertising industry. On the other hand, because the partly very aggressive PUA versions can hardly be distinguished from traditional malware. Thus, the analysis of some PUA samples in terms of spying on user data reveals mechanisms almost similar to the Trojans clearly belonging to the realm of malware. And with respect to distribution of PUA, the lines separating it from malware are fuzzy. Thus, mobile malware is distributed via infected apps in the same way that PUA enters as a bundle with actually useful apps onto the devices of smartphone and tablet users being spied on. The detection of PUA is naturally additionally hampered by the fact that practically every innocuous freeware app is financed through delivery of advertising.

Of course, PUA for Android and mobile devices of other mobile platforms exhibits different specifications than for Windows PCs. PUA for mobile devices offers personalized advertising within predefined ad boxes of an app or briefly shows full display advertising when an app is launched or closed (interstitial ads). But even the push messaging of devices or the home screen can be abused as an advertising space (icon ads).

Add to this the fact that PUA for mobile devices also offers unethical advertisers information on the movement patterns of device users and can create corresponding profiles for localized advertising. The fact that such mobility data is an extremely hot commodity among advertisers can be seen by the following comparative data for all mobile platforms except Android: While iOS, Windows Mobile and Symbian are practically non-existent, comprising only 0.01 percent of the PUA universe, the number of samples in the first half of 2016 doubled compared to 2015. Far more interesting, however, is the fact that the number of PUA samples for Android in the year-on-year comparison is growing in leaps and bounds - specifically by over 13 percent. Security software for Android is currently still not widely distributed, which means that Android users are easy prey for the advertising industry.

PUA detection sorted by operating systems



Mac: spying instead of malware

It has already been documented in this report that malware for Apple systems is not widely distributed. By contrast, the breaches of privacy of Mac users through PUA paint a whole different picture. Whereas in 2015, the AV-TEST systems registered a mere 819 different malware samples, the number of PUA samples at 76,464 was significantly higher and made up over 96 percent of the overall detection rate of Mac threats.

The PUA Top 10 of last year was dominated by the adware "VSearch". It comes in a bundle with popular freeware downloads onto unprotected Mac computers of unsuspecting users. In the style of a Trojan, the adware embeds itself via a shell script in the cache and secretly sends system and user data over the Internet. What's more, it hijacks the browser settings, changing the home page and displaying pop-up advertising.

With wide distribution, "Macnist" is ranked at No. 2. It involves Trojan-like adware that emerged last year as a browser extension for Safari, Chrome and Firefox. On visited websites, also appearing as spyware under the name of "Yontoo", it launches its own advertising and sends logs on surfing habits to unknown servers on the Internet. The malware entered Mac computers disguised as a would-be plug-in for displaying online movies, but was also found as a media player or download accelerator.

It should be emphasized that the use of a security application is worthwhile even for Mac users. That is why anyone who wants to protect their privacy should choose an AV product that also detects and blocks PUA. In comprehensive tests on security applications for Mac, AV-TEST evaluates at regular intervals which programs offer relevant PUA protection.

TOP 10 Mac PUA 2015

1	VSEARCH	31,796
2	MACNIST	31,504
3	OSX	5,422
4	BUNDLORE	2,023
5	GENIEO	1,872
6	XAMLOADER	1,856
7	INSTALLCORE	393
8	SPIGOT	294
9	KEYGEN	235
10	CROSSRIDER	190

Trend 2016

In the first half of this year, we can see a clear trend; specifically, an attack on the privacy of Android users by the advertising industry.

In the first quarter of 2016, the AV-TEST systems registered a massive increase in potentially unwanted applications for Android, with a growth rate of more than 13 percent compared to last year. At the same time, as an overall proportion, the number of PUA attacks on Windows PCs has practically decreasing by precisely this percentage (14.24%). Thus, the trend is clear: The advertising industry is also increasingly taking aim at Google's mobile platform, Android. This trend is also supported by the comparison of test results of PUA growth for Windows.

TOP 10 Mac PUA Q1/Q2 2016

1	VSEARCH	20,819
2	OSX	8,475
3	BUNDLORE	4,905
4	EXTINSTALL	3,686
5	XAMLOADER	2,303
6	GENIEO	1,368
7	CROSSRIDER	543
8	INSTALLCORE	521
9	SPIGOT	254
10	TOOLBAR	238

PUA development under observation

Today, advertising firms with PUA are still operating in a virtually lawless realm. While most manufacturers of AV products would be technically capable of detecting such attacks on the privacy of online users on all standard platforms, the detection of PUA remains a political matter, however. This is also evidenced by negotiations of the Clean Software Alliance (CSA), a discussion platform of the advertising industry using PUA and providers of security software. The AV-TEST Institute, as an active participant in the previous CSA conferences, will continue to monitor and analyze the development of PUA on all major platforms, and to regularly provide information on the current situation at security congresses.

TEST
av-test.org

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

Test Statistics

As one of the leading institutes in the field of security research, AV-TEST utilizes sophisticated and proprietary analysis systems and test procedures:

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 sample 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 250 servers with storage capacity of over 2200 TB. On the publication date of this annual report, the AV-TEST database contained 578,702,687 malware applications for Windows and 16,514,928 malware programs for Android!

BEST REPAIR 2015
AWARD
Avira Antivirus Pro
AV TEST av-test.org CERTIFIED
BEST USABILITY 2015
AWARD
Kaspersky Lab Internet Security
AV TEST av-test.org CERTIFIED
BEST USABILITY 2015
AWARD
Avira Antivirus Pro
AV TEST av-test.org CERTIFIED
BEST PROTECTION 2015
AWARD
Symantec Norton Security
AV TEST av-test.org CERTIFIED
BEST PERFORMANCE 2015
AWARD
Bitdefender Endpoint Security
AV TEST av-test.org APPROVED CORPORATE ENDPOINT PROTECTION
BEST PERFORMANCE 2015
AWARD
Bitdefender Internet Security
AV TEST av-test.org CERTIFIED

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. 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 10,000 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 2015 over 200 product tests alone were run for consumer and enterprise products. As a result, 171,433 malware attacks and 3,227,191 individual data records for false positive tests were deployed and evaluated per product. Throughout the year 2015, this amounted to 683,123,424 records evaluated by the test experts.

In the monthly Android tests in 2015, the testers evaluated over 160 individual products. In doing so, each evaluated security app had to defend against 29,030 special Android malware samples. As a counter sample, the experts also recorded over 469,128 scans of secure apps, in order to evaluate the vulnerability towards false positives. That is why in lab tests of security products, a total of 1,352,234 scan procedures were monitored 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.

BEST ANDROID SECURITY 2015
AWARD
Bitdefender Mobile Security
AV-TEST av-test.org CERTIFIED
BEST PERFORMANCE 2015
AWARD
Kaspersky Lab Internet Security
AV-TEST av-test.org CERTIFIED
BEST PROTECTION 2015
AWARD
Sophos Mobile Security
AV-TEST av-test.org CERTIFIED
BEST PROTECTION 2015
AWARD
Symantec Endpoint Protection
AV-TEST av-test.org APPROVED CORPORATE ENDPOINT PROTECTION
BEST USABILITY 2015
AWARD
Intel Security McAfee Endpoint Security
AV-TEST av-test.org APPROVED CORPORATE ENDPOINT PROTECTION
BEST REPAIR 2015
AWARD
Kaspersky Lab Virus Removal Tool
AV-TEST av-test.org CERTIFIED

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 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