virus BULLETIN


# THE THREAT AND SECURITY PRODUCT LANDSCAPE IN 2017

# THE THREAT AND SECURITY PRODUCT LANDSCAPE IN 2017

*Martijn Grooten*
Virus Bulletin

## INTRODUCTION

WannaCry; (Not)Petya; Bad Rabbit; FIN7; Triton; The Lazarus group; Fancy, Cozy and Energetic Bear; The Shadow Brokers; Oilrig; Platinum; Dragonfly; Pegasus. 2017 has seen no shortage of attacks targeting individuals, companies, critical infrastructure, and sometimes even entire countries. It can be mind boggling to think about what is going on, especially when one realizes that the attacks we know about are only the tip of the iceberg. It sometimes feels as if we are all playing a game, the rules of which are still being written.

In the context of these attacks, it would be easy to consider the more 'mundane' malware that infects millions every day as mere background noise – but to treat it as such would be wrong, ignoring both the highly professional organizations that are behind most cybercrime campaigns and the serious damage suffered by both individuals and organizations.

Moreover, there is often a surprising overlap between the *modi operandi* of targeted attacks and those of opportunistic malware attacks. Both types of attack tend to exploit human gullibility first and foremost, and techniques seen in targeted attacks, such as the ETERNALBLUE exploit, often make their way into cybercriminal toolkits.

The role security products play in defending against such attacks can be both overstated and understated.

Overstated, because no matter what the marketing spiel would have you believe, there is no silver bullet against any kind of digital threat. At best, a product can significantly reduce the likelihood of a successful infection.

At the same time, it is wrong to understate the importance of this attack mitigation and the difference it can make. For every successful ransomware attack there will have been hundreds, possibly thousands, of similar attacks that have been stopped somewhere in their tracks.

In this report, we both look at the recent state of such opportunistic malware attacks and provide some context as to how likely it is that such attacks would be blocked by a security solution. We hope to show that, despite all the sensational headlines, the situation is not all doom and gloom.

We also want to use the opportunity this report gives us to thank all of the vendors and individuals we have worked with in 2017 for their cooperation, and in particular *Project Honey Pot* and *Abusix* – two organizations that have, for years, been providing the spam feed used in *Virus Bulletin*'s VBSpam tests.

We look forward to continuing current collaborations and developing new ones in 2018!

## BACKGROUND

This report does not deal with the threat of vulnerable smart devices on the Internet of Things (IoT), but taking a look at today's IoT threat landscape can be helpful in understanding how far we have come regarding the security of our laptops and desktop machines.

It is not uncommon for a security researcher to discover that a smart device has an undocumented backdoor, that it is using a default and rarely changed password on a public service (such as HTTPS), or that it is otherwise remotely accessible. In the early 2000s, the situation for *Windows* desktops and (the then less common) laptops was somewhat similar in the sense that, once connected to the Internet, such a device could be infected with malware within 20 minutes[1].

A combination of operating system hardening, the addition of built-in firewalls, security software and NAT has significantly reduced the ease with which a PC can be attacked. The average PC simply isn't 'listening'

[1] Though the security of early *Microsoft* operating systems left much to be desired, it is only fair to point out that this was the case for *any* operating system at the time. The vulnerability exploited by the Blaster worm, which was the Mirai of its time, was patched quickly and it was far more complicated than a default password or an undocumented telnet device.

to the Internet, so even if a particular service is found to be vulnerable, it is hard for an attacker to exploit it at scale.

(As an aside, PCs are often listening to the internal network, for example using the SMB protocol. Following WannaCry, which exploited an SMB vulnerability in order to propagate within networks, other malware families, such as Trickbot, have started to use the same technique for lateral movement. It is likely that such techniques will become common in malware.)

Consequently, almost all attacks use one of two protocols to infect users: SMTP or HTTP, more commonly referred to as email and web.

## YOU'VE GOT (UNWANTED) MAIL

Malicious email is increasingly treated as a separate problem from spam, but we believe we are justified in considering it a mere subcategory. Spam and malicious email campaigns are sent using the same networks, often of compromised devices (botnets), the only difference being the presence/absence of a malicious attachment or, less commonly these days, a malicious link.

Though measuring spam is notoriously difficult, experts agree that spam levels have decreased significantly since a peak towards the end of the last decade. Part of this can be attributed to various prominent takedowns of spammers' infrastructure, starting with the shutting down of the rogue *McColo* ISP nine years ago. The fact that many ISPs block outbound connections on port 25 (the standard port for SMTP) for home users will have helped too, as will the fact that outbound spam filtering has become more common.

However, there is another reason for the decline in spam for which there is less reason to be cheerful: from a botherder's point of view, there are often more profitable things to do with a compromised machine – activities that often attract less unwelcome attention[2] and that directly target the wallets of the device owners. This is also why, among the countries that send a lot of spam, we find many that have a relatively high Internet penetration rate compared to the average standard of living. For understandable reasons, those with less money to spend will care less about the hygiene of their devices.

In the most recent VBSpam test, we found that one in four of all spam emails were sent from machines in Vietnam or India. To put this into context, in 2016 Vietnam was listed 13th in the world when it comes to the number of Internet users; the USA had more than five times as many users yet sent less than a third of the spam[3].

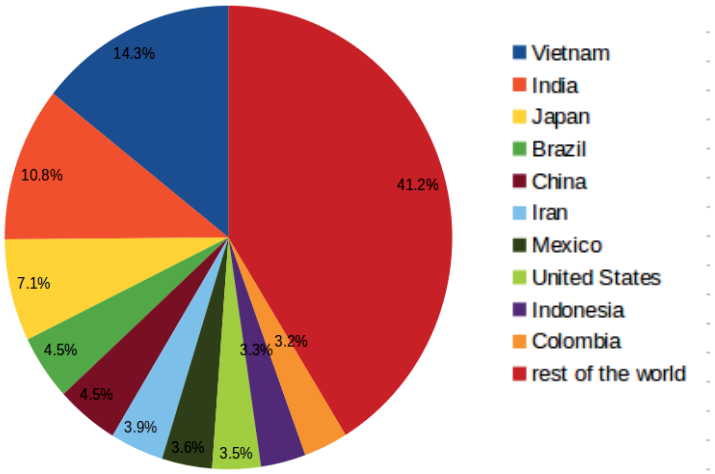



*Figure 1: Spam sources by country. (Note: these numbers are indicative only. Virus Bulletin is well aware that different sources report different numbers.)*

[2] Whether attention is welcome depends on the particular type of malware: banking trojans, information stealers, remote access trojans and malicious proxies all try to remain as well hidden as possible. Ransomware, on the other hand (once it has encrypted all the files on the victim machine), attempts to attract as much attention as possible – but by this time, blocking the device's Internet connection will do nothing to reduce the damage.

[3] http://www.internetlivestats.com/internet-users-by-country/.

An equally telling factoid about the spam botnet landscape is that Necurs, one of the most prominent spam botnets and one responsible for many malicious spam campaigns, has not infected any new machines for several years.

It is, however, worth keeping in mind that spam is not just being sent from long-since unpatched *Windows* PCs. Today, a lot of spam is sent from compromised web hosts. The fact that such hosts often have fast Internet connections, and that sending high volumes of emails is less likely to arouse suspicion, has made these servers an attractive target for spammers.

Spam sent from smart devices is also on the rise. While we may never know whether, four years ago, a fridge really did send spam[4], IoT botnets have been found to be engaged in sending spam.

The decline in spam and the improved quality of spam filters (often sold as email security solutions) have made spam mitigation a rare success story in the world of security. True, we all get spam emails delivered to our inboxes, and we occasionally have to fish a legitimate email out of our spam folders, but it has not meant the end of email.

Things are a bit more complicated when it comes to malicious spam though, and vendors focusing their attention on this particular sub-threat is both understandable and justified. Here too, however, things are not as bad as they are often portrayed.

To start, it is good to understand that the malware sent in spam campaigns is rarely the final intended payload. The first reason for this is that it allows those behind the campaign to deliver different payloads depending, for instance, on the geographic location of the user: in a country where few would be able to afford a ransom of a few hundred dollars, a cryptocurrency miner may be more profitable than ransomware.

The second reason is that few email security solutions would allow any kind of portable executable (PE) file to be delivered, regardless of whether or not it is malicious.

The 'downloader' attached to the email is thus, through necessity, a file type that users would be likely to receive legitimately, such as a *Microsoft Office* document or a PDF file. For the same reason it must be a file type that might legitimately require some kind of user interaction, such as enabling macros, clicking a link, or allowing an application to be started (for the actual payload to be downloaded) – otherwise the attachment would be blocked too[5].

This has an important consequence for the ability of a security product to block such malicious emails: the malicious activity is not present in the attachment itself, meaning that, in order to detect and block the campaign, a security solution has to rely on similarities between the file and other previously seen malware (for example the use of particular domains, or certain obfuscation techniques). This, in part, explains the low detection rates reported for many malicious email campaigns.

There are a number of silver linings though. The first is that, though it would technically be trivial to make small modifications to each individual attachment, spammers often don't bother. In *Virus Bulletin*'s most recent VBSpam test, almost 6,000 malicious spam emails contained just 33 different attachments; the most common attachment was present in almost a quarter of the emails.

The second silver lining is that malicious spam is also *just spam*. Spam tends to be blocked very well, and not just based on the content of the email: it is quite telling that, in our most recent tests, the overwhelming majority of malicious spam was sent from IP addresses that appeared on all the common IP blacklists.

Malicious spam is a real concern, and it only takes one email for your devices to be infected with ransomware. But it is important to remember that only a very small percentage of malicious spam is actually opened – and even once opened it still has to hope for a gullible user *and* bypass the endpoint anti-malware solution that (hopefully) is running on the device.

[4] https://www.virusbulletin.com/blog/2014/01/your-fridge-sending-spam/.

[5] JavaScript attachments are a good example of this – for some time they were also popular for delivering malware via email. However, as such files are increasingly blocked by email providers (regardless of their content), spammers have turned away from them.


*Figure 2: Malicious spam campaigns that required a user to double click 'to unlock content' were common in the second half of 2017, and were very prominent in the most recent VBSpam test.*

## SURFING TO MALWARE

Web traffic and email are like the famous Russian reversal jokes: while you visit websites, email visits you (i.e. is being sent to you). This has long made using the web to deliver malware less attractive for malware authors. After all, how many users go out of their way to get infected?

It turns out that, while no one willingly goes out of their way to get infected, social engineering can do a lot to get users to infect themselves. A web search for free versions of paid-for software turns up plenty of results where users can download software with varying degrees of maliciousness.

A more prominent web-based threat, however, is that of drive-by downloads: sites that infect a user with malware without there being any user interaction. For obvious reasons, the ability to execute code (malicious or not) on a machine would be a particularly unwanted feature of browsers, so drive-by downloads need to exploit a vulnerability in a browser or, more commonly, a plug-in. *Adobe*'s *Flash Player* is notorious for being used in drive-by downloads, just as *Oracle*'s *Java* plug-in has been used in the recent past.

Such sites – which include sites that have been deliberately set up, compromised sites, and sites where malicious third-party code is injected via advertisements – rarely target a single vulnerability, but probe the browser for a number of vulnerabilities, after which they deliver a payload depending on the various characteristics of the user and their browser. The tools used for this purpose are referred to as 'exploit kits'; they are a prime example of the commoditization of cybercrime.

Exploit kits became notorious with the appearance of the Blackhole kit in early 2011. After the arrest of the main author of Blackhole in the autumn of 2013, the exploit kit landscape became more varied, with kits such as Angler, Nuclear and Neutrino appearing on the scene. For various reasons, these three kits have all disappeared and the landscape has been relatively quiet for some time, with RIG now the most prominent player, while kits such as Magnitude and Kaixin are more localized.

Exploit kits are not easy to block, in part because often they don't simply download the actual payload. Rather, they use various techniques to 'reconstruct' the malware locally – techniques that are opaque to anyone listening in on the wire; simply scanning all potentially malicious file types that are being downloaded thus isn't sufficient.

There has also been a recent trend for exploit kits to deliver fileless malware, which often involves some malicious PowerShell being executed that is never stored on disk.

Despite all this, and despite the tendency for exploit kits to change quickly, security solutions aren't powerless against them. *Virus Bulletin*'s VBWeb tests have shown that various solutions are able to block almost all of those they are served in real time; in several cases, the products even blocked all of the hundreds of kits seen in a test.

Finally, it is important to note that, more than other kinds of threats, drive-by downloads exploit vulnerabilities. It is extremely rare for these vulnerabilities not to be patched. Patching one's operating system, browsers and plug-ins remains the most important thing one can do to fend off drive-by downloads.

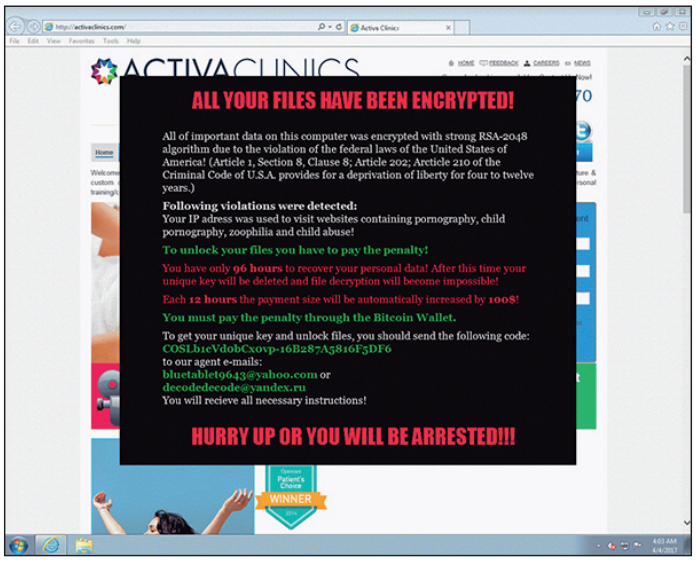



*Figure 3: The Matrix ransomware delivered via a drive-by download.*

## ALL IS NOT LOST: ENDPOINT MALWARE DETECTION

Good security on both email and web traffic will result in an enormous reduction in the amount of malware that makes it onto an endpoint. It won't reduce it to zero though, and there are other ways in which malware can end up on such an endpoint – a vulnerable USB drive, for example. For this reason, it is important also to protect the endpoint itself.

This is where the oldest of security products enters the stage: the anti-virus solution. It is a common misunderstanding that anti-virus, now more commonly referred to as anti-malware or endpoint security, simply looks for malicious file hashes and is thus powerless against the hundreds of thousands of new malware files seen each day – malware that often has a very short timespan.

Whether an anti-virus solution is one of the more traditional types or a 'next-gen' solution (the difference between which is often smaller than marketing departments may want you to believe), it typically has multiple layers. The first layer may look at whether the file has previously been seen; the second layer may look for patterns seen in the file; the third layer may emulate the file in order to look beyond packers and code obfuscation; the fourth layer may look for malicious activities once the malware is executed and block them before they do any harm[6].

These four layers (which are not intended to provide a comprehensive overview of all of the activities of all anti-virus products) make it increasingly difficult for malware authors to add variation at scale to prevent detection: it is trivial to make small hash-breaking changes to a file; it is a lot harder to make changes that don't show similar patterns. Making malware execution vary in a significant way is very hard to achieve at scale.

[6] This fourth layer is not currently covered in *Virus Bulletin*'s anti-malware test. However, it is tested by other testing agencies; for a more complete picture, we recommend that those interested in this aspect consult other test reports too.

Years of testing anti-malware solutions has taught *Virus Bulletin* that no product is perfect. But it has also demonstrated that such solutions are far from powerless, even when it comes to static detection – although, as discussed in the section on email threats, it does matter whether products are shown the final payload or a downloader that doesn't contain the actual malicious activity.

## FALSE POSITIVES AND VULNERABILITIES

In the previous sections, we discussed various digital threats and what security products do to stop them. However, security products add two threats of their own.

The first of these is false positives (FPs): legitimate emails that are blocked, legitimate websites one is prevented from visiting, mission-critical software that isn't able to run. No security product is able to avoid false positives, and all of *Virus Bulletin*'s tests include a false positive test – to prevent products from simply blocking all email, or all files. A product cannot achieve a *Virus Bulletin* certification if it has a significant false positive problem, and we encourage those considering purchasing a security solution to look for a product with a low false positive rate.

More important than a low FP rate, however, is the way in which false positives are handled: does the product block the file, email or website without giving the user an option to declare it a false positive? Does it give the user a simple way to declare a false positive, and thus continue their work? Or does it require a systems administrator to do so?

There is no 'right' answer to the way in which false positives are handled, but it is worth remembering that some of the most damaging attacks were initially blocked, but then later allowed by a user who considered themselves wiser than the security solution.

It is not just products that need to avoid false positives: software developers, email providers and website developers all need to make sure they avoid using techniques that are commonly used for malicious purposes, and that they are as transparent as possible. Though *Virus Bulletin* takes a strict approach when it comes to false positives, in the majority of cases, it isn't just the security product that is to blame.

The second threat that comes with security products is that of the products themselves being leveraged in an attack. This has long been a hot topic in the security community and it is rare for a security product not to have been the subject of a clever proof-of-concept attack.

It is worth noting, though, that such attacks are rarely used in practice, and that for most users and organizations security solutions provide far more benefit than any harm they could potentially cause. Users should require their vendors to have both good vulnerability disclosure and firm patching policies. Thankfully, many security vendors have recently improved greatly in this respect.

There are limited cases though, where security or privacy concerns mean that using a security product could cause more harm than benefit. Users who find themselves in such situations should consider stronger measures such as extreme device hardening, or simply disconnecting a device from the Internet.

## VIRUS BULLETIN'S SECURITY PRODUCT TESTS

For more than two decades, *Virus Bulletin* has been testing security solutions of various kinds. Currently, we run three tests: an anti-malware test (VB100), an email security test (VBSpam), and a web gateway test (VBWeb). Apart from test reports, which are published four to six times a year, *Virus Bulletin* also tests products privately alongside the public tests, and even conducts standalone tests. Many vendors we work with use the test results and feedback generated by the tests as a third-party quality assurance.

All of *Virus Bulletin*'s tests aim to show which products are doing well, and to help products perform better in the future. While we don't shy away from reporting on products that didn't pass a test (barring exceptional circumstances, a vendor that has agreed to have its product included in a public report can't back out once the test has started), by running the tests regularly, we hope to make it easy to determine whether a lacklustre performance is a one-off glitch or whether there is a more fundamental problem with the product. Our favourite experiences are

those where a product has performed poorly several times and, sometimes after a temporary withdrawal, returns to appear near the top of the pack.

Many governments and organizations make a *Virus Bulletin* certification a requirement for any security solution that is to be purchased. We can certainly stand behind that, but we are the first to admit that there are other criteria to be considered, and we urge potential buyers to consult other test reports as well as other relevant information before making a purchasing decision. Just as one shouldn't rely on a single security product, no single test provides a full picture either.

For details on *Virus Bulletin*'s various tests, their methodologies, and past results, we refer to our website, www.virusbulletin.com. Vendors that are interested in having their solutions tested, whether publicly or privately, should contact *Virus Bulletin*'s testing team at vbtest@virusbulletin.com.

The following pages display the results tables from each of *Virus Bulletin*'s VB100 and VBSpam tests in 2017, followed by an alphabetical list of product vendors and the certifications (VB100, VBSpam and VBWeb) their products achieved in 2017.

| **VB100 February 2017 certification tests** | On demand | On access | Clean sets | | VB100 |
|---|---|---|---|---|---|
| | Standard WildList | Standard WildList | FP | Warnings | |
| Avast For Linux | 100.00% | 100.00% | | | VIRUS 100 |
| Bitdefender Endpoint Security | 100.00% | 100.00% | | | VIRUS 100 |
| eScan Anti-Virus For Linux | 100.00% | 100.00% | | | VIRUS 100 |
| ESET File Security for Linux/FreeBSD | 100.00% | 100.00% | | | VIRUS 100 |

| VB100 April 2017 certification tests | Windows 7 | | | | Windows 10 | | | | VB100 |
|---|---|---|---|---|---|---|---|---|---|
| | FPs | FP rate | WildList misses | WildList catch rate | FPs | FP rate | WildList misses | WildList catch rate | |
| adaware antivirus free | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| adaware antivirus pro | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Arcabit Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Avast Free Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| AVG Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Bitdefender GravityZone Security for Endpoints | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| BullGuard Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| CompuClever Antivirus PLUS | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Cyren Command Anti-Malware | 35 | 0.01% | 0 | 100.00% | 35 | 0.01% | 0 | 100.00% | X |
| Defenx Security Suite | 2 | 0.00% | 0 | 100.00% | 2 | 0.00% | 0 | 100.00% | X |
| Emsisoft Anti-Malware | 0 | 0.00% | 6 | 99.76% | 0 | 0.00% | 6 | 99.76% | X |
| eScan Internet Security Suite for Windows | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| ESET Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Essentware PCKeeper Antivirus PRO | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| ESTsecurity ALYac | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |

| VB100 April 2017 certification tests contd. | Windows 7 | | | | Windows 10 | | | | VB100 |
|---|---|---|---|---|---|---|---|---|---|
| | FPs | FP rate | WildList misses | WildList catch rate | FPs | FP rate | WildList misses | WildList catch rate | |
| Fortinet FortiClient | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| G DATA Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| IKARUS anti.virus | 12 | 0.00% | 0 | 100.00% | 12 | 0.00% | 0 | 100.00% | X |
| K7 Total Security | 2 | 0.00% | 0 | 100.00% | 2 | 0.00% | 0 | 100.00% | X |
| Kaspersky Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| MSecure Endpoint ATP | 70 | 0.02% | 0 | 100.00% | 70 | 0.02% | 0 | 100.00% | X |
| NANO Antivirus Pro | 1 | 0.00% | 0 | 100.00% | 2 | 0.00% | 0 | 100.00% | X |
| Quick Heal Seqrite Endpoint Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Quick Heal Total Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Tencent PC Manager | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| ThreatTrack VIPRE Internet Security Pro 2016 | 0 | 0.00% | 20 | 99.21% | 0 | 0.00% | 0 | 100.00% | X |
| Total Defense Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Total Defense Premium | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| TrustPort Antivirus Sphere | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| VirIT eXplorer PRO | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |

| VB100 June 2017 certification tests | Windows 7 | | | | Windows 10 | | | | VB100 |
|---|---|---|---|---|---|---|---|---|---|
| | FPs | FP rate | WildList misses | WildList catch rate | FPs | FP rate | WildList misses | WildList catch rate | |
| adaware antivirus pro | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Arcabit Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Avast Free Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| AVG Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Bitdefender GravityZone Security for Endpoints | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| BullGuard Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Clearsight Antivirus Business | 0 | 0.00% | 15 | 99.77% | 0 | 0.00% | 15 | 99.77% | X |
| CompuClever Antivirus PLUS | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Cyren Command Anti-Malware | 3 | 0.001% | 2 | 99.97% | 3 | 0.001% | 2 | 99.97% | X |
| Defenx Security Suite | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Emsisoft Anti-Malware | 0 | 0.00% | 9 | 99.86% | 0 | 0.00% | 9 | 99.86% | X |
| eScan Internet Security Suite for Windows | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| ESET Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Essentware PCKeeper Antivirus PRO | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Fortinet FortiClient | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| G DATA Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| IKARUS anti.virus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |

| VB100 June 2017 certification tests contd. | Windows 7 | | | | Windows 10 | | | | VB100 |
|---|---|---|---|---|---|---|---|---|---|
| | FPs | FP rate | WildList misses | WildList catch rate | FPs | FP rate | WildList misses | WildList catch rate | |
| INCA nProtect AVS | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| K7 Total Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Kaspersky Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| MSecure Endpoint ATP | 9 | 0.002% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | X |
| NANO Antivirus Pro | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Panda Endpoint Protection | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Panda Free Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Quick Heal Seqrite Endpoint Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Quick Heal Total Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| TeamViewer ITbrain Anti-Malware | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Tencent PC Manager | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Tencent PC Manager – TAV | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Total Defense Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Total Defense Premium | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| TrustPort Antivirus Sphere | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| VirIT eXplorer PRO | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |

| VB100 August 2017 certification tests | Windows 7 | | | | Windows 10 | | | | VB100 |
|---|---|---|---|---|---|---|---|---|---|
| | FPs | FP rate | WildList misses | WildList catch rate | FPs | FP rate | WildList misses | WildList catch rate | |
| adaware antivirus pro | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Arcabit AntiVirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Avast Free Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| AVG Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Bitdefender Endpoint Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| CompuClever Antivirus PLUS | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Cyren Command Anti-Malware | 0 | 0.00% | 2 | 99.97% | 0 | 0.00% | 2 | 99.97% | X |
| Defenx Security Suite | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Emsisoft Anti-Malware | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| eScan Internet Security Suite for Windows | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| ESET Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Essentware PCKeeper Antivirus PRO | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| ESTsecurity ALYac | 0 | 0.00% | 2 | 99.97% | 0 | 0.00% | 0 | 100.00% | X |
| Fortinet FortiClient | 1 | 0.0003% | 0 | 100.00% | 1 | 0.0003% | 0 | 100.00% | X |
| G DATA Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| IKARUS anti.virus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |

| VB100 August 2017 certification tests contd. | Windows 7 | | | | Windows 10 | | | | VB100 |
|---|---|---|---|---|---|---|---|---|---|
| | FPs | FP rate | WildList misses | WildList catch rate | FPs | FP rate | WildList misses | WildList catch rate | |
| K7 Total Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Kaspersky Endpoint Security 10 for Windows | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| NANO Antivirus Pro | 2 | 0.0005% | 0 | 100.00% | 1 | 0.0003% | 0 | 100.00% | X |
| Panda Endpoint Protection Plus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Panda Free Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Quick Heal Seqrite Endpoint Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Quick Heal Total Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| STOPzilla AntiVirus 8.0 | 0 | 0.00% | 2 | 99.97% | 0 | 0.00% | 0 | 100.00% | X |
| TeamViewer ITbrain Anti-Malware | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Tencent PC Manager | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Total Defense Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Total Defense Premium | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| TrustPort Antivirus Sphere | 2 | 0.0005% | 0 | 100.00% | 2 | 0.0005% | 0 | 100.00% | X |
| VirIT eXplorer PRO | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |

| VB100 October 2017 certification tests | Windows 7 | | | | Windows 10 | | | | VB100 |
|---|---|---|---|---|---|---|---|---|---|
| | FPs | FP rate | WildList misses | WildList catch rate | FPs | FP rate | WildList misses | WildList catch rate | |
| adaware antivirus pro | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Arcabit AntiVirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Avast Free Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| AVG Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Bitdefender Endpoint Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| CompuClever Antivirus PLUS | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Cyren Command Anti-Malware | 0 | 0.00% | 0 | 100.00% | 1 | 0.0003% | 1 | 99.96% | X |
| Defenx Security Suite | 1 | 0.0003% | 0 | 100.00% | 1 | 0.0003% | 2 | 99.93% | X |
| Emsisoft Anti-Malware | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| eScan Internet Security Suite for Windows | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| ESET Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Essentware PCKeeper Antivirus PRO | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| ESTsecurity ALYac | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Faronics Anti-Virus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Fortinet FortiClient | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| G DATA Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| IKARUS anti.virus | 0 | 0.00% | 0 | 100.00% | 2 | 0.0005% | 0 | 100.00% | X |

| VB100 October 2017 certification tests contd. | Windows 7 | | | | Windows 10 | | | | VB100 |
|---|---|---|---|---|---|---|---|---|---|
| | FPs | FP rate | WildList misses | WildList catch rate | FPs | FP rate | WildList misses | WildList catch rate | |
| K7 Total Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Kaspersky Endpoint Security 10 for Windows | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Panda Endpoint Protection Plus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Panda Free Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Quick Heal Seqrite Endpoint Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Quick Heal Total Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Rising Security Cloud Client | 41 | 0.01% | 0 | 100.00% | 41 | 0.01% | 0 | 100.00% | X |
| TeamViewer ITbrain Anti-Malware | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Tencent PC Manager | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Tencent PC Manager – TAV | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Total Defense Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Total Defense Premium | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| VIPRE Advanced Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| VirIT eXplorer PRO | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Wontok SafeCentral Security Suite | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |

| VB100 December 2017 certification tests | Windows 7 | | | | Windows 10 | | | | VB100 |
|---|---|---|---|---|---|---|---|---|---|
| | FPs | FP rate | WildList misses | WildList catch rate | FPs | FP rate | WildList misses | WildList catch rate | |
| adaware antivirus pro | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Arcabit AntiVirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Avast Free Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| AVG Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Bitdefender Endpoint Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| CompuClever Antivirus PLUS | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Cyren Command Anti-Malware | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Defenx Security Suite | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Emsisoft Anti-Malware | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| eScan Internet Security Suite for Windows | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| ESET Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Essentware PCKeeper Antivirus PRO | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| ESTsecurity ALYac | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Faronics Anti-Virus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Fortinet FortiClient | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| G DATA Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |

| VB100 December 2017 certification tests contd. | Windows 7 | | | | Windows 10 | | | | VB100 |
|---|---|---|---|---|---|---|---|---|---|
| | FPs | FP rate | WildList misses | WildList catch rate | FPs | FP rate | WildList misses | WildList catch rate | |
| IKARUS anti.virus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| K7 Total Security | 15 | 0.004% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | X |
| Kaspersky Endpoint Security 10 for Windows | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Panda Endpoint Protection Plus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Panda Free Antivirus | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| TACHYON Endpoint Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| TeamViewer ITbrain Anti-Malware | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Tencent PC Manager | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Tencent PC Manager – TAV | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Total Defense Internet Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Total Defense Premium | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| TrustPort Antivirus Sphere | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| VIPRE Advanced Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| VirIT eXplorer PRO | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Wontok SafeCentral Security Suite | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |
| Zemana Endpoint Security | 0 | 0.00% | 0 | 100.00% | 0 | 0.00% | 0 | 100.00% | VIRUS 100 |

| **VBSpam certification tests March 2017** | True negatives | False positives | FP rate | False negatives | True positives | SC rate | VBSpam | Final score |
|---|---|---|---|---|---|---|---|---|
| Axway | 7498 | 1 | 0.01% | 180 | 158878 | 99.89% | SPAM Verified | 99.77 |
| Bitdefender | 7499 | 0 | 0.00% | 27 | 159031 | 99.98% | SPAM + Verified | 99.98 |
| ESET | 7499 | 0 | 0.00% | 2 | 159056 | 99.999% | SPAM + Verified | 99.999 |
| Fortinet FortiMail | 7499 | 0 | 0.00% | 37 | 159021 | 99.98% | SPAM + Verified | 99.98 |
| GFI MailEssentials | 7496 | 3 | 0.04% | 2023 | 157035 | 98.73% | SPAM Verified | 98.33 |
| IBM Lotus Protector | 7498 | 1 | 0.01% | 14 | 159044 | 99.99% | SPAM Verified | 99.91 |
| Kaspersky LMS | 7498 | 1 | 0.01% | 64 | 158994 | 99.96% | SPAM Verified | 99.89 |
| Kaspersky SMG | 7498 | 1 | 0.01% | 133 | 158925 | 99.92% | SPAM Verified | 99.85 |
| Libra Esva | 7497 | 2 | 0.03% | 42 | 159016 | 99.97% | SPAM Verified | 99.81 |
| OnlyMyEmail | 7499 | 0 | 0.00% | 1 | 159057 | 99.999% | SPAM + Verified | 99.99 |
| Scrollout | 7479 | 20 | 0.27% | 1328 | 157730 | 99.17% | SPAM Verified | 97.57 |
| Sophos | 7496 | 3 | 0.04% | 504 | 158554 | 99.68% | SPAM Verified | 99.48 |
| SpamTitan | 7499 | 0 | 0.00% | 236 | 158822 | 99.85% | SPAM Verified | 99.81 |
| Vade Secure MailCube | 7495 | 4 | 0.05% | 434 | 158624 | 99.73% | SPAM Verified | 99.46 |
| ZEROSPAM | 7498 | 1 | 0.01% | 75 | 158983 | 99.95% | SPAM Verified | 99.77 |
| IBM X-Force Combined* | 7497 | 2 | 0.03% | 14133 | 144925 | 91.11% | N/A | 90.96 |
| IBM X-Force IP* | 7497 | 2 | 0.03% | 19205 | 139853 | 87.93% | N/A | 87.77 |
| IBM X-Force URL* | 7499 | 0 | 0.00% | 93057 | 66001 | 41.49% | N/A | 41.49 |
| Spamhaus DBL* | 7495 | 4 | 0.05% | 135620 | 23438 | 14.74% | N/A | 14.47 |
| Spamhaus ZEN* | 7499 | 0 | 0.00% | 10561 | 148497 | 93.36% | N/A | 93.36 |
| Spamhaus ZEN+DBL* | 7495 | 4 | 0.05% | 7949 | 151109 | 95.00% | N/A | 94.74 |
| URIBL* | 7462 | 37 | 0.49% | 97366 | 61692 | 38.79% | N/A | 35.50 |

**The IBM X-Force, Spamhaus and URIBL products are partial solutions and their performance should not be compared with that of other products.*

*(Please refer to the text of the full report on www.virusbulletin.com for full product names and details.)*

| **VBSpam certification tests June 2017** | True negatives | False positives | FP rate | False negatives | True positives | SC rate | VBSpam | Final score |
|---|---|---|---|---|---|---|---|---|
| Axway | 8418 | 0 | 0.00% | 223 | 209245 | 99.89% | SPAM + Verified | 99.82 |
| Bitdefender | 8418 | 0 | 0.00% | 58 | 209410 | 99.97% | SPAM + Verified | 99.95 |
| ESET | 8417 | 1 | 0.01% | 3 | 209465 | 99.999% | SPAM Verified | 99.94 |
| Fortinet FortiMail | 8418 | 0 | 0.00% | 7 | 209461 | 99.997% | SPAM + Verified | 99.997 |
| GFI MailEssentials | 8330 | 88 | 1.05% | 1580 | 207888 | 99.25% | X | 93.85 |
| IBM Lotus Protector | 8417 | 1 | 0.01% | 38 | 209430 | 99.98% | SPAM Verified | 99.91 |
| Kaspersky for Exchange | 8417 | 0 | 0.00% | 159 | 209309 | 99.92% | SPAM + Verified | 99.92 |
| Kaspersky LMS | 8417 | 0 | 0.00% | 129 | 209339 | 99.94% | SPAM + Verified | 99.94 |
| Libra Esva | 8418 | 0 | 0.00% | 23 | 209445 | 99.99% | SPAM + Verified | 99.99 |
| NoSpamProxy | 8418 | 0 | 0.00% | 556 | 208912 | 99.73% | SPAM + Verified | 99.69 |
| OnlyMyEmail | 8417 | 1 | 0.01% | 2 | 209466 | 99.999% | SPAM Verified | 99.90 |
| Scrollout | 8406 | 12 | 0.14% | 56 | 209412 | 99.97% | SPAM Verified | 98.98 |
| SpamTitan | 8418 | 0 | 0.00% | 748 | 208720 | 99.64% | SPAM Verified | 99.63 |
| Vade Secure MailCube | 8418 | 0 | 0.00% | 630 | 208838 | 99.70% | SPAM + Verified | 99.70 |
| ZEROSPAM | 8413 | 5 | 0.06% | 186 | 209282 | 99.91% | SPAM Verified | 99.57 |
| IBM X-Force Combined* | 8417 | 1 | 0.01% | 4584 | 204884 | 97.81% | N/A | 97.75 |
| IBM X-Force IP* | 8417 | 1 | 0.01% | 11955 | 197513 | 94.29% | N/A | 94.23 |
| IBM X-Force URL* | 8418 | 0 | 0.00% | 54470 | 154998 | 74.00% | N/A | 74.00 |
| Spamhaus DBL* | 8418 | 0 | 0.00% | 134631 | 74837 | 35.73% | N/A | 35.73 |
| Spamhaus ZEN* | 8418 | 0 | 0.00% | 12711 | 196757 | 93.93% | N/A | 93.93 |
| Spamhaus ZEN+DBL* | 8418 | 0 | 0.00% | 8140 | 201328 | 96.11% | N/A | 96.11 |
| URIBL* | 8413 | 5 | 0.06% | 69207 | 140261 | 66.96% | N/A | 66.67 |

**The IBM X-Force, Spamhaus and URIBL products are partial solutions and their performance should not be compared with that of other products.*

*(Please refer to the text of the full report on www.virusbulletin.com for full product names and details.)*

| **VBSpam certification tests September 2017** | True negatives | False positives | FP rate | False negatives | True positives | SC rate | VBSpam | Final score |
|---|---|---|---|---|---|---|---|---|
| Axway | 6642 | 0 | 0.00% | 197 | 283408 | 99.93% | SPAM + Verified | 99.92 |
| Bitdefender | 6642 | 0 | 0.00% | 8 | 283597 | 99.997% | SPAM + Verified | 99.997 |
| Cyren | 6642 | 0 | 0.00% | 9063 | 274542 | 96.80% | X | 96.80 |
| ESET | 6642 | 0 | 0.00% | 3 | 283602 | 99.999% | SPAM + Verified | 99.999 |
| Forcepoint | 6629 | 13 | 0.20% | 607 | 282998 | 99.79% | SPAM Verified | 99.80 |
| Fortinet FortiMail | 6631 | 0 | 0.00% | 4 | 282731 | 99.999% | SPAM + Verified | 99.999 |
| IBM Lotus Protector | 6642 | 0 | 0.00% | 33 | 283572 | 99.99% | SPAM + Verified | 99.99 |
| Kaspersky for Exchange | 6642 | 0 | 0.00% | 30 | 283575 | 99.99% | SPAM + Verified | 99.99 |
| Kaspersky LMS | 6642 | 0 | 0.00% | 31 | 283574 | 99.99% | SPAM + Verified | 99.99 |
| Libra Esva | 6642 | 0 | 0.00% | 68 | 283537 | 99.98% | SPAM + Verified | 99.98 |
| OnlyMyEmail | 6642 | 0 | 0.00% | 1 | 283604 | 99.9996% | SPAM + Verified | 99.98 |
| Scrollout | 6636 | 6 | 0.09% | 60 | 283545 | 99.98% | SPAM Verified | 99.29 |
| SpamTitan | 6638 | 4 | 0.06% | 652 | 282953 | 99.77% | SPAM Verified | 99.47 |
| ZEROSPAM | 6641 | 1 | 0.02% | 68 | 283537 | 99.98% | SPAM Verified | 99.83 |
| IBM X-Force Combined* | 6641 | 1 | 0.02% | 9897 | 273708 | 96.51% | N/A | 96.44 |
| IBM X-Force IP* | 6641 | 1 | 0.02% | 13455 | 270150 | 95.26% | N/A | 95.18 |
| IBM X-Force URL* | 6642 | 0 | 0.00% | 122376 | 161229 | 56.85% | N/A | 56.85 |
| Spamhaus DBL* | 6642 | 0 | 0.00% | 262183 | 21422 | 7.55% | N/A | 7.55 |
| Spamhaus ZEN* | 6642 | 0 | 0.00% | 8849 | 274756 | 96.88% | N/A | 96.88 |
| Spamhaus ZEN+DBL* | 6642 | 0 | 0.00% | 7958 | 275647 | 97.19% | N/A | 97.19 |
| URIBL* | 6639 | 3 | 0.05% | 120386 | 163219 | 57.55% | N/A | 57.33 |

**The IBM X-Force, Spamhaus and URIBL products are partial solutions and their performance should not be compared with that of other products.*

*(Please refer to the text of the full report on www.virusbulletin.com for full product names and details.)*

| **VBSpam certification tests December 2017** | True negatives | False positives | FP rate | False negatives | True positives | SC rate | VBSpam | Final score |
|---|---|---|---|---|---|---|---|---|
| Axway | 6671 | 4 | 0.06% | 371 | 154316 | 99.76% | SPAM Verified | 99.42 |
| Bitdefender | 6675 | 0 | 0.00% | 55 | 154632 | 99.96% | SPAM + Verified | 99.96 |
| Cyren | 6675 | 0 | 0.00% | 1711 | 152976 | 98.89% | SPAM Verified | 98.83 |
| ESET | 6675 | 0 | 0.00% | 5 | 154682 | 99.997% | SPAM + Verified | 99.997 |
| Forcepoint | 6668 | 7 | 0.10% | 894 | 153793 | 99.42% | SPAM Verified | 98.89 |
| Fortinet FortiMail | 6675 | 0 | 0.00% | 10 | 154677 | 99.99% | SPAM + Verified | 99.99 |
| IBM Lotus Protector | 6675 | 0 | 0.00% | 29 | 154658 | 99.98% | SPAM + Verified | 99.97 |
| Kaspersky for Exchange | 6675 | 0 | 0.00% | 21 | 154666 | 99.99% | SPAM + Verified | 99.99 |
| Kaspersky LMS | 6675 | 0 | 0.00% | 14 | 154673 | 99.99% | SPAM + Verified | 99.99 |
| Libra Esva | 6675 | 0 | 0.00% | 74 | 154613 | 99.95% | SPAM + Verified | 99.92 |
| OnlyMyEmail | 6675 | 0 | 0.00% | 0 | 154687 | 100.00% | SPAM + Verified | 99.97 |
| Scrollout | 6654 | 21 | 0.31% | 54 | 154633 | 99.97% | SPAM Verified | 98.20 |
| Vade Secure Cloud | 6647 | 28 | 0.42% | 533 | 154154 | 99.66% | X | 97.55 |
| ZEROSPAM | 6675 | 0 | 0.00% | 67 | 154620 | 99.96% | SPAM Verified | 99.81 |
| IBM X-Force Combined* | 6674 | 1 | 0.01% | 7224 | 147463 | 95.33% | N/A | 95.26 |
| IBM X-Force IP* | 6674 | 1 | 0.01% | 11004 | 143683 | 92.89% | N/A | 92.81 |
| IBM X-Force URL* | 6675 | 0 | 0.00% | 123778 | 30909 | 19.98% | N/A | 19.98 |
| Spamhaus DBL* | 6675 | 0 | 0.00% | 134744 | 19943 | 12.89% | N/A | 12.89 |
| Spamhaus ZEN* | 6675 | 0 | 0.00% | 5345 | 149342 | 96.54% | N/A | 96.54 |
| Spamhaus ZEN+DBL* | 6675 | 0 | 0.00% | 3967 | 150720 | 97.44% | N/A | 97.44 |
| URIBL* | 6674 | 1 | 0.01% | 136100 | 18587 | 12.02% | N/A | 11.94 |

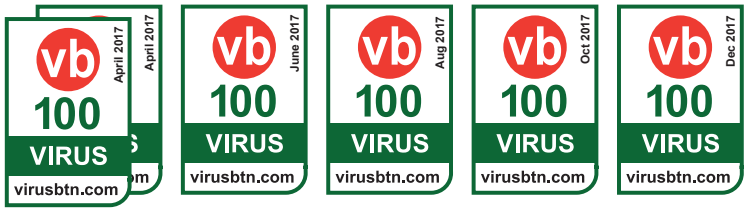
**The IBM X-Force, Spamhaus and URIBL products are partial solutions and their performance should not be compared with that of other products.*

*(Please refer to the text of the full report on www.virusbulletin.com for full product names and details.)*

## adaware

www.adaware.com

@officialadaware




## Arcabit

www.arcabit.pl


## Avast

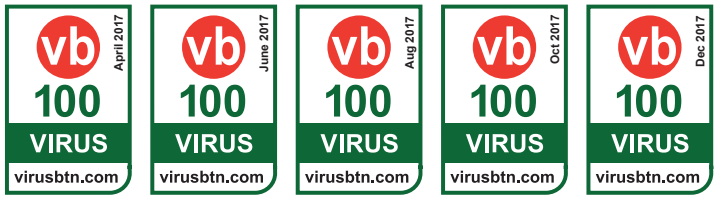
www.avast.com

@avast_antivirus


## AVG

www.avg.com

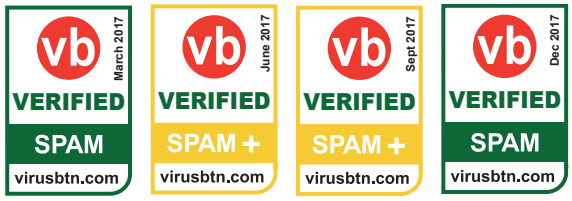
@AVGFree



## Axway

www.axway.com

@axway




## Bitdefender

www.bitdefender.com

@Bitdefender

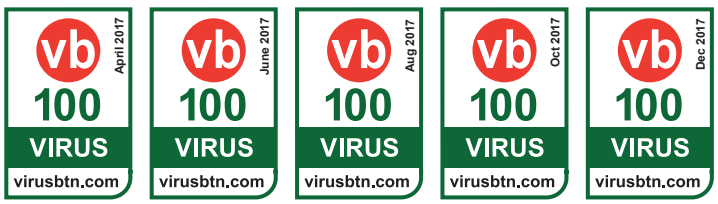

## BullGuard

www.bullguard.com

@BullGuard


## CompuClever

www.compuclever.com



## Cyren

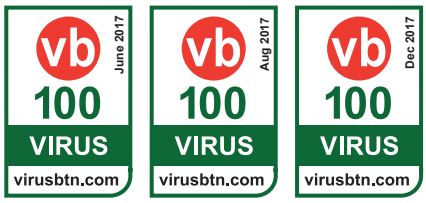
www.cyren.com

@CyrenInc


## Defenx

www.defenx.com

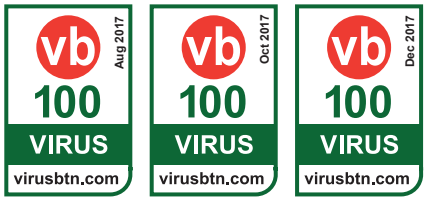
@Defenx




## Emsisoft

www.emsisoft.com

@emsisoft




## eScan

www.escanav.com

@eScan_tweet

## ESET

www.eset.com

@esetglobal

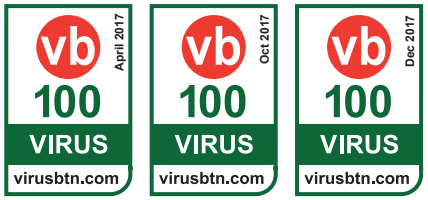

## Essentware

essentware.com

@PCKeeper


## ESTsecurity

www.estsecurity.com




## Faronics

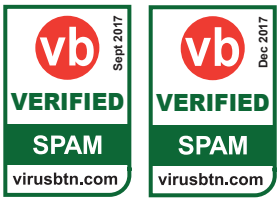
www.faronics.com

@faronics

## Forcepoint

www.forcepoint.com

@forcepointsec




## Fortinet

www.fortinet.com

@fortinet


## G DATA

www.gdata-software.com

@GDataSoftwareAG


## GFI

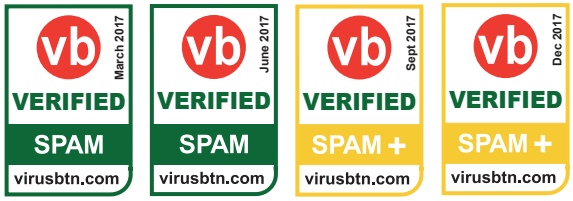
www.gfi.com

@gfisoftware

## IBM

www.ibm.com

@IBMSecurity




## IKARUS

www.ikarussecurity.com

@IKARUSANTIVIRUS


## INCA Internet

www.inca.co.kr

@inca_nprotect

*(Note: product name TACHYON)*


## K7

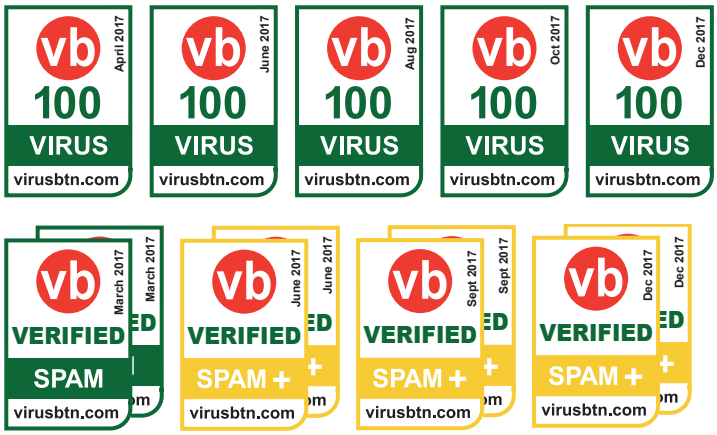
www.k7computing.com

@k7computing

## Kaspersky

www.kaspersky.com

@kaspersky




## Libra Esva

www.libraesva.com

@LibraEsva


## NANO

www.nanoav.ru

@NANOantivirus

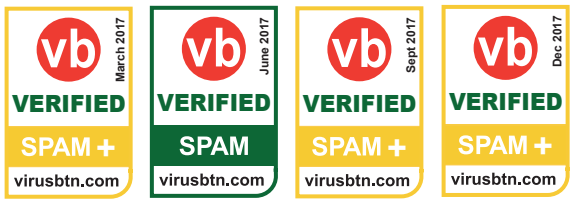

## NoSpamProxy

www.nospamproxy.de

@netatwork_de

## OnlyMyEmail

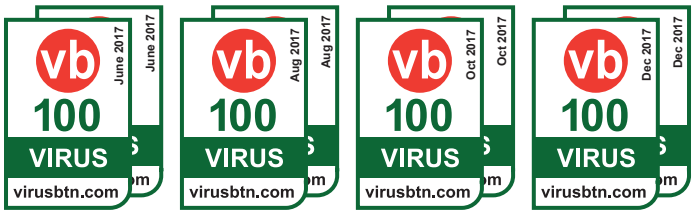
www.onlymyemail.com




## Panda Security

www.pandasecurity.com

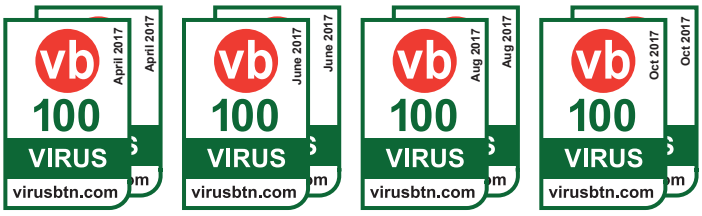
@panda_security




## Quick Heal

www.quickheal.com

@quickheal




## Scrollout

www.scrolloutf1.com

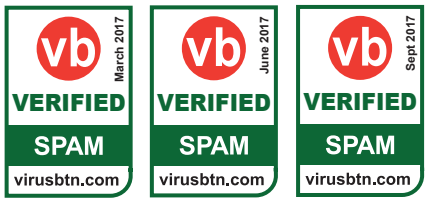
@ScrolloutF1

## Sophos

www.sophos.com
@Sophos


## SpamTitan

www.spamtitan.com
@SpamTitan

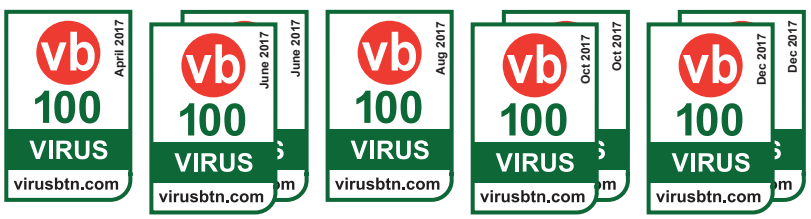



## TeamViewer

www.itbrain.com
@itbrain_help


## Tencent

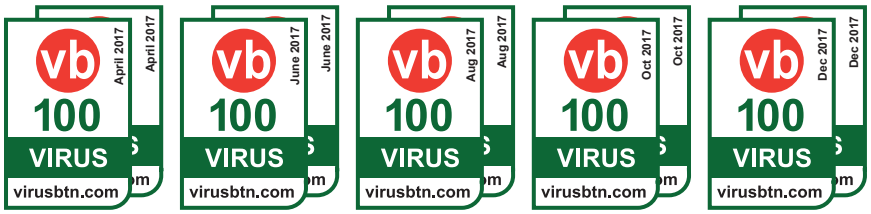
www.tencent.com



## Total Defense

www.totaldefense.com

@Total_Defense




## TrustPort

www.trustport.com

@trustportnews


## Trustwave

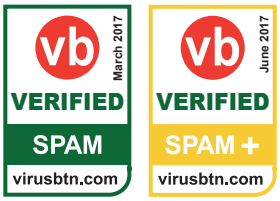
www.trustwave.com

@trustwave


## Vade Secure

www.vadesecure.com

@vadesecure



### VIPRE

www.vipre.com

@VIPRESecurity

*(Note: previously known as ThreatTrack)*


### VirIT

www.tgsoft.it

@viritexplorer


### Wontok

www.wontok.com

@SafeCentral

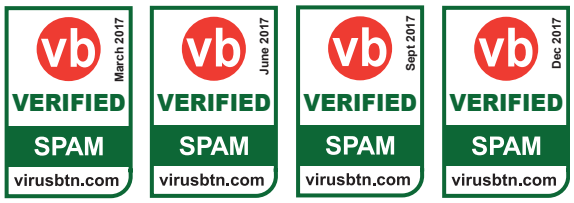

### Zemana

www.zemana.com

@Zemana

## ZEROSPAM

www.zerospam.ca
@zerospam




## OTHER PRODUCTS

In the VBSpam tests, we include some products that are only exposed to part of the email, such as the sending IP address, or domains present in the email. Such solutions are designed to be integrated into a larger solution and, as such, are not expected to block as many emails as a full email security solution. As such, they haven't been certified by *Virus Bulletin*, but it would be incorrect to say these vendors have failed a certification, and we believe that their inclusion in the test is an important one:

### IBM X-Force

www.ibm.com
@IBMSecurity

### Spamhaus

www.spamhaus.org
@spamhaus

### URIBL

uribl.com
@URIBL

**Editor:** Martijn Grooten
**Head of Testing:** Peter Karsai
**Security Test Engineers:** Scott James, Tony Oliveira, Adrian Luca, Ionuţ Răileanu, Chris Stock
**Sales Executive:** Allison Sketchley
**Editorial Assistant:** Helen Martin
**Developer:** Lian Sebe


**Tel: +44 (0)1235 555139 • Email: editor@virusbulletin.com • Web: https://www.virusbulletin.com/**