



Anti-Virus Comparative

Anti-Virus E-Mail Support Response
&
Time needed to release an update with
reliable detection
for one specific submitted virus

Date: July 2006

Last revision of this report: 16th August 2006

Author: Andreas Clementi

Website: <http://www.av-comparatives.org>

1. Introduction

This is the first AV support test we have done, and, due to statistical insignificance, will probably be the last in this form¹. This test was inspired from some articles in VirusBulletin magazine (e.g. the Polip case²), aiming to get a view (from ONE user's perspective) of how AV vendors react to email support requests. In this case the request was from a user infected by an undetected polymorphic virus. As it is just one situation of one sample tested here, it is not very meaningful, but it does give some tips and ideas for possible future improvements, both for the user and for AV vendors³.

2. Tested Anti-Virus vendors

The following vendors were observed in this test: AVIRA (formerly H+BEDV (AntiVir)), Avast, AVG, Dr.Web, BitDefender, F-Prot, F-Secure, Kaspersky, Eset (NOD32), Norman and VBA32.

AEC Trustport and GData AVK were not tested, because they rely on signatures/engines which come from other vendors (so they may just forward the mail to e.g. BitDefender, Kaspersky or Norman, which are already being tested).

F-Secure has its own virus lab and uses its own engine in the product as well as a third-party engine, so theoretically they can add a signature for this virus themselves, which is why we included them. McAfee and Symantec were not tested in this case, because they already detected this virus; reliably (detecting all replicants/files infected by this virus).

Symantec was the first AV to provide reliable detection of this virus (May 2005)⁴ and later McAfee (August 2005)⁵. It is important to note that Anti-Virus vendors have received samples of this virus several times over the last year (including from AV-Comparatives). As it was also included in our test-set, this virus has also been included in the set of missed samples sent to vendors after our tests. Other AV vendors (like Symantec, etc.) also shared this virus in June 2005 with other AV vendors via their monthly collections.

So every of the tested AV vendors already had this virus in their lab, but as there was no report of its being in the wild (i.e. it was not a real threat), they probably gave very low detection priority to it and did not add it.

In this observation test we look to see what happens when a user is infected by this virus and requests help from the AV vendor.

The earliest instance (from 2003) of a (non-working) sample called and detected as Bakaver was available on a vX (virus exchange) site and was detected by most av vendors (even though it is non-working). It seems like a (working) variant of the Bakaver virus may have been written by the author in the year 2003, but was sent to the AV vendors at the beginning of 2005.

Files infected by the Bakaver virus can not be disinfected and have to be replaced after deletion (one good reason why every user should regularly use a backup/image tool/software – polymorphic viruses can leave files unusable).

¹ Note: this is not a worldwide outbreak response test, but just a response test to one virus reported by one user.

² Virus Bulletin, July 2006, pp. 4-8

³ AV vendors are asked to forgive us for having conducted this test without advance notice, but we did not want to bias the result by alerting companies.

⁴ <http://www.symantec.com/avcenter/venc/data/w32.bakaver.a.html>

⁵ http://vil.nai.com/vil/content/v_135557.htm

3. Description

This is a summary of information about the Bakaver virus based on the description on Symantec's virus description site:

Bakaver is a polymorphic virus that infects certain portable executable files, changes some registry key in order to change the windows sound to baka.wav⁶. It does NOT infect any files that have the following properties: smaller than 65536 bytes, created or modified in last 20 days, containing the numbers 0, 2, 4 or 9 in the file, containing repeated letters in the filename or [filenames] beginning with certain antivirus strings or files that are protected by Windows System File Checker. Additionally, if a folder contains more executables than other file types, it will not infect the files in that folder.

More details can be found on the Symantec site.

<http://www.symantec.com/avcenter/venc/data/w32.bakaver.a.html>

Nowadays, the majority of malware is static malware like Trojans, and actual viruses (replicating malware) are getting rarer. However, virus analysts have to be prepared for any kind of malware, including complex polymorphic viruses.

Replicating the Bakaver virus is difficult, as it replicates only under certain specific conditions. So, it requires that a virus analyst takes a closer look at the sample to see how it works; in order that they can release a reliable detection routine. With a polymorphic virus it is not possible only to add the submitted file which makes it, in our opinion, a good choice to see how AV vendors react if a user is infected by this virus and require a signature update.

So we pretended to be a genuine user, and made it clear that a real infection was involved. We sent the following email support request to the global support email address AND to the viruslab email address, just to ensure that someone read our mails.

Hello,

Please help me!

Since today I notice in our company that something is wrong with our computers: the windows sound has changed and sometimes I also observe abnormal disk activities. I think I located one file which could cause it (see attachment - the password is "virus"). The attached file is a WinRAR demo file which we received recently from a friend and installed not long ago. We use Windows XP Professional with SP2.

We use your Anti-Virus product but it did not found anything during an on-demand scan with latest updates :(I also discovered a new file in the windows folder called "baka.wav" which I think is maybe related to the virus/trojan.

Could you please check the files and send me as soon as possible a signature update in order to clean out the PC's (cleaning all infected files from this virus/trojan)? Currently we turned off all our computers in order to stop the infection until you provide us an update or solution to help us, in order that we can again work as usual. Thank you in advance for your response!

Regards,

xxxxxxx

⁶ Baka seems to be a japanase or philippin word for „stupid“.

We tried to make an overview of how long it usually takes to add detection (based on our feelings and experience over the last years):

Submitted malware which seems to come actually infected customers:

Global outbreaks	As this is an emergency and updates have to be released very fast, it usually takes not more than a few hours after they receive the sample. How long the AV vendors need to react in such cases has been documented in detail by AV-Test.org
Static malware	may need several minutes to check and an update can be released within a few hours
Simple viruses or worms	may need up to several hours
"Difficult" viruses	may need up to several days or some weeks

Submitted malware from non infected customers and/or with low possibility of becoming widespread:

Malware with media interests (e.g. PoC malware, like Win32.Gatt) or of malware families which are know to be a potential threat (e.g. Banker, Bots, etc.)	may take anywhere from a few hours up to several days
Malware which is submitted only because it is available on some VX site (which may be just garbage) or other kind of very low risk malware	may take weeks / months/ years

Basically the release speed of a signature for a specific virus always depends on priorities. This is determined by number of infected computers, where the sample was found, the particular customer, type of malware, time of the day/week, etc.

But in any case - if someone is infected - he wants to get his PC cleaned as soon as possible and get supported by his Anti-Virus vendor. Even better would be if the PC does not get infected at all, but for that, the malware would need to be detected (even if it was only virus submitted by the author to the av company - there is always the possibility that some user gets infected by this malware).

NOTE: The names of the companies were removed on purpose, in order to avoid incorrect conclusions by users (as it is statistically insignificant) and also to avoid possible abuse by some vendors to discredit other antivirus companies.

4. Responses

Only human responses are listed - automatic receipt responses are not listed. Please note the differences between the time (and quality) of support responses and the time required to provide a (reliable) detection. If a vendor provided incorrect information about the sample or did not provide a reliable detection in order to remove all infected files, the verdict "FAILED" is given. We try not to comment too much on the answers or the feelings we had with some responses, but it can be imagined that some replies were not really satisfying.

Please note that it is OK if some AV vendors need days or even a week to provide an update, but only if the released update will then provide an accurate protection (reliable detection which detects all files infected by the submitted virus).

Thursday, 13th July 2006

- 14.15 The mail with the text showed on page 3 of this report and with the sample (an infected WinRAR file) and the baka.wav is sent to the AV vendors (to the support email address AND to the viruslab email address).
- 14.43 **Vendor 2** (a Virus Analyst) replies that the file is clean.
We replied with another sample of this virus and asked if they are really sure that the file is not malicious.
Verdict: **FAILED** Ⓢ
- 14.59 **Vendor 5** Support recommends performing a boot time scan and if that does not help to wait for the response of the viruslab.
We replied that the boot time scan did not help and that we will wait for the viruslab analysis.
- 15.27 **Vendor 7** VirusLab replied that a Win32 virus was found appended to the submitted file and that they will add detection for this virus in the upcoming pattern database update.
- 15.39 **Vendor 2** (the same Virus Analyst) says **again** that the file(s) are clean and not malicious.
We replied that we want another opinion from another analyst of Vendor 2.
- 16.36 **Vendor 2** (another virus analyst) replies: "We are sorry. We have rechecked this file and found EPO virus inside. It's detection will be added soon (approximately on Saturday)."
We replied asking what an EPO virus is and why it can not be detected within e.g. some hours (what a customer would probably ask).
- 17.09 **Vendor 2** (a Senior Virus Analyst) explains in very good detail what an EPO virus is and why it will take some days to add detection for it (needs hard testing before a routine can be released).
- 17.13 **Vendor 6** support replies that the virus is non-trivial polymorphic and that signatures for its detection will be available tomorrow.
- 20.59 **Vendor 11** Technical Support replies, saying that the file contains virus code and that a priority update will be released tomorrow.

Friday, 14th July 2006

- 5.55 **Vendor 1** added detection for this virus. Detection reliability: **100%** (all replicants detected). Seems like Vendor 1 provides a reply only if the support gets contacted thru their website contact form. ☹
Anyway - Verdict: **PASSED ☺**
- 9.53 **Vendor 3** replies, asking to run a *special tool*.
We replied that our office is closed until an update to remove the virus is released. We resent the infected file (other vendors are able to analyze and provide an update without the information gathered by that tool), so they should not require more information about our PC's. Sending the tool generated information would be of use for example where a Trojan is involved, or when the submitted file is not the cause or container of the infection, but in this case, they simply needed to take a closer look at the submitted file.
- 11.03 **Vendor 4** VirusLab replies, saying that they found a new virus in the submitted file and that a signature will be integrated in one of the next updates.
- 14.37 **Vendor 11** added detection for the virus, but unfortunately, the detection is not reliable. As this is a polymorphic file infector, detecting only the submitted files is of no help (no reliable detection).
Verdict: **FAILED ☹**
- 15.53 **Vendor 10** added detection for the virus, but the detection is not reliable (not all replicants detected).
Verdict: **FAILED ☹**
- 18.49 **Vendor 9** Support replies that the viruslab team will add detection soon. (**when???, after 1 month still nothing**)
- 21.03 **Vendor 10** Support replies, saying that it is a new virus and that it can be detected with a patch released a few hours ago, but that the files have to be restored from backup, as they can not be repaired.
We reply asking if a scan with Vendor 10 and the new update will definitely remove all infected files from our PC (as we know it does not).
- 21.55 **Vendor 10** replies, saying that the update will find all infected files and attaching the update module to the mail.
We reply that Vendor 10 found and removed - in the computers with the infection symptoms - only one infected file (the submitted file), and that we do not know if this is a good sign or not. We also said that we hope to have from now on virus free computers. Theoretically they should think that it is unusual that a file infector is the only infected file and that no other files are detected. Hopefully they will investigate further the case and provide a more reliable detection.
- 21.57 **Vendor 6** added detection of the virus, but unfortunately, also here the detection was not reliable (not all replicants detected).
We replied to the first mail Vendor 6 sent yesterday asking them to please inform us as soon as an update which will detect and remove all infected files on our computers is released.
Verdict: **FAILED ☹**

Note also the dates given by the vendors when the update will be released and look when they really released a signature update to cover this virus.

On Saturday and Sunday nothing happened...

Monday, 17th July 2006

8.11 **Vendor 3** replied that the submitted file is WinRAR (which is true, but it is WinRAR with a virus inside) and that this is a false positive, and (according to them) Symantec have already removed detection for it while McAfee still haven't. (But the file is really infected and can be replicated, Symantec has NOT removed detection for it and McAfee will also not, because it is NOT a false positive.)

Verdict: **FAILED** Ⓢ

We reply asking why then the windows sound has changed.

10.43 **Vendor 5** replies that the file is clean and that we should send a HijackThis log file.

Verdict: **FAILED** Ⓢ

We reply asking if they are sure that the file is clean, because a friend who has another product installed says that the file is infected by a virus.

13.05 **Vendor 5** replies saying that this new Bakaver virus will be in the next update. (**when???, after 1 month still nothing**)

17.46 **Vendor 4** added detection for the virus, but unfortunately, the detection is not reliable. As this is a polymorphic file infector, detecting only the submitted files is of no help (no reliable detection).

Verdict: **FAILED** Ⓢ

Tuesday, 18th July 2006

15.23 **Vendor 3** replies that it is hard to say why the windows sound changed, but they do not think that WinRAR (the submitted file) did it.

15.38 **Vendor 8** support replies that the file seems to contain a new virus and that detection will be added in near future. (when???)

Wednesday, 19th July 2006

17.36 **Vendor 2** added reliable detection for this virus, which detects all replicants.

17.40 **Vendor 7** added reliable detection for this virus, which detects all replicants.

***After the 19th July 2006 nothing happened
(no replies, no further detection or improvements added)***

Nearly one month passed, and we ceased further observation.

NOTE: The names of the companies have been removed in order to avoid incorrect conclusions by users (as this test is statistically insignificant) and possible abuse by some vendors to discredit other antivirus companies.

5. Summary results

a) Human Support reply to email, stating that the file was infected after first user submission:

1. Vendor 7
2. Vendor 6
3. Vendor 11
4. Vendor 4
5. Vendor 9
6. Vendor 10
7. Vendor 8

1) The following vendors provided wrong replies to the user:

- I. Vendor 2*
- II. Vendor 3
- III. Vendor 5*

* Vendor 2 and Vendor 5 corrected their replies only on 3rd try.

Vendor 1 added very fast a reliable detection for the virus, but we did not receive any reply from them.

b) RELIABLE detection provided within four weeks:

1. Vendor 1
2. Vendor 2
3. Vendor 7

1) The following vendors provided a non-reliable detection to the user:

- I. Vendor 11*
- II. Vendor 10
- III. Vendor 6
- IV. Vendor 4*

* Vendor 11 and Vendor 4 added only the submitted file, but no other replicants are detected.

2) The following vendors did not provide any detection attempt within 4 weeks:

- Vendor 3
- Vendor 9
- Vendor 5
- Vendor 8⁷

Comment: In various ways, all vendors failed in this test (due to wrong analysis/replies, unreliable detection, no detection or no reply). Should a user really have been really infected by this virus, he would be justifiably unsatisfied.

NOTE: Names of vendors were removed on purpose; we will not reveal which vendor corresponds to which number. We will only tell vendors which number represents their company in this report.

⁷ Vendor 8 added reliable detection for this virus shortly after the 4 weeks. The other 3 vendors still do not detect it.

6. Suggestions

For AV vendors:

- A fast answer is not equal to a good or correct answer! (see Vendor 2)
- It would be nice if every AV vendor would send an automatic response that the sample has been received (some - e.g. Dr.Web, Symantec, McAfee, Norman already do this).
- As the user is already frustrated due to an infected PC, a human answer with a solution or status is expected, just in order that the user sees that he is not left alone in the dark.
- Use Vgrep and try to use the same names as other AV vendors already used for the malware. Particularly if it is an older virus (It is not always possible with a new one). Some gave strange new names to this virus
- If a virus analysts is unsure about the nature of a submitted file, he should forward it to a more experienced senior virus analyst before he replies to the customer that the file is clean (not malicious).
- Do not use restrictive submission policies. RAR and ZIP files with at the least the common passwords like "virus" or "infected" should be accepted by the automatic processing systems.
- In some cases mails with password-protected attachments get filtered on some mailrelays, it can be difficult to submit a suspicious file to an AV vendor. It would be good to allow also some alternative way to submit files (e.g. file upload from your website).

For users:

- Before you send a sample to your AV vendor, update your scanner and check if the malware is already detected by your AV product.
- In urgent cases - if not already done - or if no replies arrive after 1 day, users should phone and/or contact the local support by email. This may help to speed up the process and to get better support.
- Include your AV license information in the email.
- Submit a sample only once and tell to the av company if you are currently really infected by this malware (and what system you use, etc.). If you only found this malware somewhere (tell where) without infecting yourself and that you only want to submit this malware for curiosity or in order that the AV company can improve their detection. If they decide to do not add it yet, do not bother them about asking when it will be added, it may be that it is not an important threat, a broken file or just garbage⁸.

Final comment: Users should not be too concerned about the results and observations made in this report, which examined only ONE support request from ONE infected user. Normally users are infected with malware which can be added and detected soon. This was an 'extreme' example to see how Anti-Virus vendors react in a case where a user is infected by a polymorphic virus like Bakaver, as we read some press releases by some AV vendors about their response to another polymorphic virus (e.g. Polip).

⁸ Even if many other products detect something in this files.

7. Copyright and Disclaimer

This publication is Copyright (c) 2006 by AV-Comparatives. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of Andreas Clementi, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

Andreas Clementi, AV-Comparatives (August 2006)