

## How Fast is Fast?

*Robert Vibert* 2001-07-17

### How Fast is Fast: Vendor Response to New Virus Reports

by *Robert Vibert*

last updated July 17, 2001

---

You've just come across a suspicious file that seems to be causing problems on a machine in your organization. You think it may be a virus, but all of the antivirus programs you use to scan it say the file is clean. What's your logical next step? For many people, the best thing to do is to send the suspicious file to one or more antivirus software developers for analysis. Just what do you think the response from these specialists should be?

A few months ago, I had the opportunity to conduct an experiment with this process. A virus author contacted someone I knew with their latest creation. Although I am a [WildList](#) reporter, I do not come across new malware very frequently - mostly I receive reports of known critters. I was sent a copy of this potential malware, which did not show up as infected on the various antivirus scanners I had on hand. I proceeded to send out a copy of the suspect file to the major anti-virus research labs. I had previously collected and posted the addresses for the submission of suspect files on the [Segura.ca web site](#).

When I sent in the file, I did not know if it was infected or not. It is not uncommon for someone to think they have written a virus, only to discover that it does not function properly. The opinion of the antivirus developer community is that virus authors are not very good programmers in general. As my intermediary told me that he had sent it to a few antivirus companies already, I added the following note to my sample:

"You may already have seen this document. Please let me know the results of your investigations into it. Thanks."

The file was named "virus.doc", which is a pretty strong indication of what it might contain. I did not state that I thought the file was infected, just that I would like to know what they thought about it. My e-mail was sent on a Friday, just after 4:00 pm EST, to about 20 or so antivirus companies. This was, coincidentally, a good test of the weekend response time of some of these antivirus companies. Some fast-spreading malware has been released on a Friday, with the intent of spreading while anti-virus researchers were enjoying the weekend. I

went back to my regular work and awaited the replies.

The responses I received were very interesting, to say the least. As this was a one-time effort, it would not be fair to characterize the vendor on the basis of just this case. However, it may be beneficial to look at how different the responses were, and draw some conclusions on how they can be improved.

### From Blank to Mega Responses

The following table describes the responses to the suspect file that I received from various antivirus companies.

Company	Time until first response	Content of first response	Second and further responses
A	2 minutes	Automated e-mail reply, indicating that the file had been cleaned of malicious content. The content was given a virus name, which suggested it was either mis-identified or generically identified.	67 hours - I received an e-mail asking for a fresh copy to be sent inside a password protected zip file, as the first one had been cleaned. 86 hours - E-mail with an indication that the product's heuristics catches this critter. I was asked where I got it. 92 hours - E-mail asking me for more information on the source of the virus, along with a proposal

			to do a joint press release on this new virus.
B	10 minutes	Automated e-mail reply, acknowledging reception of file.	none
C	20 minutes	Automated e-mail reply, acknowledging reception of file.	none
D	32 minutes	E-mail addressed to me, indicating that the file contained a worm that would spread via Outlook and with an indication that detection is available in a specific signature file. No explanation of whether this signature file was new or an existing one, nor what I needed to do to obtain it.	none
E	3 hours	Automated e-mail reply, asking for more information on the version of antivirus software used and for more details on why I think the file is suspect.	19 hours - E-mail with a copy of their latest signature file attached in a ZIP file, with installation instructions and a link to web page with information on the virus. 44 hours - Correction to

			web page link to information on virus.
F	53 hours	E-mail asking where I got the file.	95 hours - e-mail with 850KB attachment of update files.
G	67 hours	E-mail to me saying that detection will be in upcoming signature file. No indication of when that would be available.	none
H	69 hours	E-mail to me telling me about the virus and stating that their next update will detect it. No indication of when this would be available.	none
I	70 hours	E-mail telling me some details about how it works, but indicating that it is not considered a real threat and detection will not be a priority.	none

As one can see, the range of reply is quite large, as was the type. A few things worth noting in the responses include:

- One virus researcher insisted several times that the sample was not worth wasting his time on. He told me repeatedly that he had no intention of adding detection any time soon. Obviously, he was not driven by marketing concerns.
- Another company decided it had a marketing opportunity at hand and wanted to do a joint press release with me. Needless to say, I explained to them that the sample was now widespread and many other vendors were already adding detection. The fact that

they decided to move in this direction four days after I sent in the sample made me wonder what was going on. In addition, why put out a press release about this virus? There were no indications that it was widespread and no evidence that anyone had actually suffered from it. Their e-mail on the matter did state that they thought that only their product and one other could detect it - perhaps they spotted a reason for some free publicity.

- Ten antivirus companies made no attempt whatsoever to contact me about this sample. They provided no response, no cure, no comment - nada. Would I buy anti-virus software from them? Not likely. No, I'm not going to name names.
- Two companies decided to send large files to me (one more than 2 MB in size) so I could update my system's protection. In no case did I ask for these files, nor indicate that I was using their antivirus software. I find it strange that antivirus companies would send out unsolicited attachments of such a large size - the recipient could become quite annoyed with that company, especially if located at the end of a 14.4 KB dial-up link.
- Two of the largest players in the antivirus world provided no reply other than an automated e-mail. This was most disappointing. It was the second tier vendors who provided the best response in this test.
- There was the strange situation of a lesser known antivirus company detecting the malicious code immediately and then not being able to obtain the file from their filtering system - they required me to send it again, but only a few days later.
- There was also multi-day delay in response from a number of vendors.

## Conclusions

On the whole, I found this experience rather disappointing. I know many people in the antivirus world and am sure that if I asked them directly for an analysis of a suspect file I would get a speedy reply. For this test, I did not disguise my identity, I also used the official, public channels.

As a "Joe Public" user of the analysis services offered, I was not impressed. I would have thought that the speed of response would be faster and more oriented to the customer's specific needs. Perhaps for those customers who have purchased some sort of enhanced support plans it is, but that does not bode well for the majority of users. I can understand that a certain priority system must be put in place to ensure that the important work gets done first. At the same time, the speed of spread of malware is so fast these days that almost any source of a suspect file could be the leading edge of a wave.

I discussed this topic with members of the [Anti-Virus Information Exchange Network \(AVIEN.org\)](#) and found that others had similar experiences. One commented that a suspect file sent to a large anti-virus company took nine days to be analysed.

As a single incident does not make for a solid analysis of the response capability and approaches adopted, I am going to organize a longer-term test of this process with the members of AVIEN, a group that often sees new suspicious files early. We want to determine what the response norms are today, and make suggestions for improvements. I'd also be happy to see comments from readers on their experiences with sending in suspect files.

[Privacy Statement](#)

Copyright 2006, SecurityFocus