COMMENT

“ Our industry failed today … ”

Denial of (Anti-Virus) Service

VBS/LoveLetter.A presented a perfect opportunity for *WarLab* to cut its teeth on. *WarLab* (*Wells Antivirus Research Laboratory*) does not develop or support any anti-virus products; our primary focus is on product-neutral services. Since we do not have to pour resources into product design, development, testing, or support, we’re free to step back and decide where research is needed. Our normal, day-to-day operations involve monitoring both the perception and the reality of the virus problem, as well as the anti-virus industry’s response to the problem.

Back in early 1999, anti-virus was still a product. Then W97M/Melissa.A forced anti-virus to become a service. Suddenly, the services provided by the industry became paramount – services like providing immediate updates, instant information, and 24x7 support. Then, on 4 May, 2000, VBS/LoveLetter.A stress-tested the anti-virus industry.

Early in the day (Nevada time), while we were monitoring VBS/LoveLetter.A, an unforeseen issue became extremely obvious – the anti-virus industry as a whole was being pushed to new limits. We quickly realized that this was a golden opportunity to test that which was normally untestable. Therefore, we set out to test the anti-virus industry’s ability to function in the midst of an unprecedented crisis. To this end, we spent most of the day monitoring several key factors – doing so only intermittently so as not to add to the problems we found.

Here’s what we monitored – reports on the spread of the VBS/LoveLetter.A; anti-virus update availability; anti-virus update accessibility; anti-virus tech support accessibility; the efficiency of real-time product updating.

The results of our day of stress-testing the industry were disheartening. It was evident that the industry was unprepared for an event of this magnitude. Sadly, users were undoubtedly encountering the same problems we were. The bigger US anti-virus research and information Web sites were simply unavailable at first. We couldn’t get to *SARC*, *AVERT*, or *Trend* at all for much of the day. This changed by quitting time in the western USA (after European and most US businesses were closed).

The same was the case for the tech support phone lines, which were either busy or had long waits (we chose not to wait since real users needed help). Interestingly, we called one tech support line and got a recorded message that ‘a new virus’ had greatly increased wait times. Callers were told to go to a specific Web site which, of course, was inaccessible. When we tested real-time virus updating we were successful, but the downloads were painfully slow. Such systems seemed to be the only recourse we could deem successful.

Yet even then, one update we downloaded automatically (at 1pm Pacific Standard Time), did not detect VBS/LoveLetter.A. Since tech support was out of the question, we made a personal call to someone we knew in the lab. We were told that the correct update was going up as we spoke. Pity the poor user who assumed their successfully downloaded file would protect them.

Now, if we extrapolate our results to users in general, an ominous image takes shape. Users were hit today and many had no way to get help. Those who needed to download updates in order to stop their local epidemic were doomed to failure. Assuming an update was actually available, it was inaccessible. Even assuming some persevered in their calls to tech support and got through, how would they get the all-essential update?

We have a problem. By extension, our users have a problem. Our industry failed today to protect many of those who depend on us. The problem is one of accessibility of services. Therefore, we as an industry must provide a solution to this new problem.

Joe Wells, WarLab
Thursday, 4 May, 2000