

Marketing Proposal for Norman Firewall: Automated Virus Analysis for the World

In a nutshell: Norman firewall runs at our site. Its capability normally includes the ability to determine if a file received is infected, and to not pass such a file through. This standard capability includes the ability to notify the sender of the infection, and to notify the intended recipient of the infection (and why the file was not transmitted to them.)

An enhanced firewall will not merely determine if a file is infected, but will provide a comprehensive write-up of the virus.

- This description will be prepared "live", and include a name (where any scanner can name it), behavioral analysis, report on how our product (NVC.SYS, Binder, BootGuard, NVC.EXE, and NSCAN.EXE) deal with it.
- If the virus is new, it will be assigned a number and added to the collection.
- If the virus is new, a program will obtain a string and checksum for detection, validate the string and checksum, and add it to the database.
- If it is possible to write removal instructions using VDL, our software will do this. The VDL file will then be available for use by the customer, after our salesrep has made contact, if this is appropriate in the circumstance.
- if new, a scan string will be obtained and sent with description and sample to Norway and Malaysia.
- The report on the virus will be printed on a local printer, along with a fax cover page and info on the caller, for use by the sales department. They will call the sender voice, describe the virus, ask if we can help, send lit

via mail or electronically, the write-up by fax or other method.

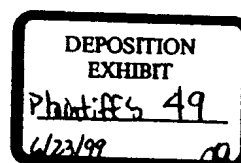
- Information produced (detection and removal instructions, description) will be stored for subsequent retrieval. The system will "learn", and a virus will only be "new" once.
- Information will be automatically prepared for V-Base developers, who will include the information in the next edition.
- Information on the incident will be automatically tabulated, for our own virus prevalence study. The information will include the precise virus name, the date, the number of infected machines, the country.

Benefits to the Public

- Competent virus analysis is rarely provided by any vendor. Users have a chronic need to know more about a virus that has infected their machine than they are provided with.
- Anti-virus products false alarm from time to time. Such alarms cause substantial anxiety. The service could reduce the anxiety when the detections done by one product prove to be "false."
- When a user gets a virus, they want to know what product(s) will detect and ideally remove it. We will be able to answer the question: NVC.SYS can prevent and warn; on boot viruses, it can remove; BG can remove; BD can remove if previously installed; in selected cases, NPSR with a VDI. can remove. We can also provide information on which other scanners detect the virus, and what they call it.

Benefits to Norman

- Image. The anti-virus capabilities of the firewall and of Norman will be demonstrated to the world. Also, by using the Internet, CompuServe, and operating as a BBS, we associate ourselves with the future. No other vendor will be able to catch us.



- Lead generation, providing precise information on what virus the prospect has, at the time they are infected, along with all name and address information, automatically. And they pay for the call!
- Collection Improvement. The system should give Norman the world's most comprehensive collection of viruses, and maintain us in this position.
- Automation of some internal processes (such as V-Base development.)

Expected Costs/Time to Complete

- One firewall machine (hardware and software). Labor in refining existing tools (eg., RUNVIRUS, Virus Analysis Toolkit, NSCAN, NPSR.)
- The virus analysis and reporting components should be ready in beta stage by January 1. Problems not addressed by January 1: removal of any virus that encrypts one or more bytes of a file; scanner-based means of detecting a polymorphic.

NDDS0296