Testing Time for Antivirus Software

a report by Sarah Gordon

Board of Directors, The WildList Organization International and The European Institute for Computer Antivirus Research (EICAR)

Sarah Gordon was recently appointed Senior Research Fellow at Symantec Research Laboratory. She is on the board of directors of The WildList Organization International and The European Institute for Computer Antivirus Research (EICAR). Previously, she worked with the Massively Distributed Systems Group at IBM's Thomas J Watson Research Laboratory, New York, in the Antivirus Research and Development Team. Her current research projects for Symantec include mapping terrorism to virtual environments and the development of certification models for security software. On-going projects include ethical implications of technology with an emphasis on computer viruses and malicious code. She has been featured in such publications as Forbes ASAP. IEEE Monitor. The Wall Street Journal, Time Digital and The Independent and her work is published regularly in publications such as Computers & Security Journal, Network Security Advisor and Virus Bulletin. Ms Gordon volunteers in an advisory capacity to Virus Bulletin and The Small World Foundation. Providing consultancy services to corporate, educational and government organisations occupies her spare time.

Everyone needs protection from viruses and there are certainly more than a few antivirus products on the market. Over the last few years, various antivirus software vendors have announced exciting new technologies that claim to provide a 'faster, better and more cost-efficient' response to computer virus incidents within organisations.

At the same time, there is little guidance regarding the best way to evaluate the efficacy of such claims. Clearly, there can only be one technology that is faster, better and more cost-efficient than all of the others and it is important to ascertain the way in which to select a product that meets the day-to-day needs of the corporation.

The obvious way to approach this is to investigate an antivirus software test or review to evaluate the product. However, the perfect antivirus product does nothing in the absence of computer viruses and, of course, it is not advisable to deploy multiple products across networks and release viruses to test them. Still, as users are justifiably sceptical of what they cannot see, the problem of measuring the effectiveness of antivirus products rates fairly high on the corporate radar, especially given the devastating consequences that a missed virus can have on the organisation.

As the antivirus industry has matured, there have been significant changes that make the process of choosing a product less difficult. Acquisitions and mergers have consolidated the market into a small number of large names with a smaller number of less popular (but not necessarily less effective) products accounting for the rest of the user base.

In the process, the companies that have survived can leverage the economy of scale that goes with a large user base. As the total number of viruses continues to increase, it is becoming more time-consuming to keep up with the constant search for detection algorithms, therefore, consolidation has allowed the remaining companies to dedicate more resources to virus analysis. However, another aspect is that, arguably, it is now more difficult for lower market share products to compete. This tends to place the consumer at a disadvantage as a market that is dominated by a small number of competing solutions is less homogeneous. This can lead to increased exposure to new types of attack, as well as to a system that is less competitive than it could be.

Correspondingly, the fluctuations in the antivirus industry have also benefited the tester. As the market share of the leading companies has increased, the number of different products that must be tested in order to cover a particular percentage of the marketplace has decreased. This allows a tester to look at individual products in more detail, which, in turn, tends to lead to better tests.

One thing that does not seem to change significantly is the gene pool of potential antivirus product testers. In general, there are four types of testers – academic, certification, popular and in-house/corporate.

As the antivirus industry matures, the number of 'academic' testers appears to be increasing slowly. *Virus Bulletin* has been testing antivirus products since the publication started in 1989. Products for the various platforms are reviewed regularly in *Virus Bulletin's* 'comparative reviews'.

Overseen by security and antivirus expert Dr Klaus Brunnstein, students from the Virus Test Center (VTC) at the University of Hamburg have been designing and performing tests of antivirus software since 1994. The results of these projects are made available to the general public.¹

Otto-von-Guericke University of Magdeberg student Andreas Marx and his antivirus testing projects – in co-operation with his company GEGA Sofware and Medienservice – are relative newcomers to the antivirus testing scene. The tests – sponsored by antivirus companies – provide magazines such as *CHIP*, *FreeX*, *Network World*, *PC Shopping* and *PC-Welt* with results for their published reviews.

How Well Equipped Are You For The Next Virus Outbreak?

Antigen for **Microsoft Exchange and Lotus Domino**

Don't be caught out waiting for signature file updates from your single engine provider when the next virus strikes. The Antigen File Filter[™] can be customised to block e-mail file attachments by file name, type, or wild card. Alternatively, if there is a new e-mail borne worm virus on the loose, rest assured that Antigen Worm Purge [™] will automatically delete the identified threat, eliminating entry into your groupware environment. With Antigen you can enable up to five of the leading virus scan engine technologies to be employed simultaneously for maximum pre-emptive protection. Just another way that Antigen keeps you ahead in the security

game. Today, over 5 million groupware seats are virus-free because of Sybari's Antigen technology. To download your free Evaluation Copy of Antigen for Microsoft Exchange or Antigen for Lotus Domino, please visit our website at: www.sybari.com. With Antigen in place, you too can "be Well Equipped for the Next Virus Outbreak" and keep your organisation protected against e-mail borne viruses and security threats.

Sybari Software Europe

General Yagüe, 6. 28020 Madrid. Spain Phone: +34 91 296 26 00 · Fax: +34 91 296 26 01











www.sybari.com Sybari Software UK. 500 Chiswick. High Road. London W45RG. UK. Phone: +44 (0) 208 956 2855 · Fax: +44 (0) 208 956 2854 Generally, *Virus Bulletin*, the University of Hamburg and the University of Magdeburg all provide topquality tests from a perspective that is sound scientifically. However, they have not been without problems² and should not be relied on solely when selecting 'the best product'.

These tests have tended to be more focused on overall virus detection than installation, configuration and other less quantifiable features that are, in the long run, almost as important as virus detection. After all, if a product is not useable in a specific environment, it will not be used.

Even the detection results, while impressive at first glance, may not be wholly relevant to every organisation. For example, a test may report on detection within archivers that an organisation does not support or test in a configuration that is alien to that environment. Therefore, relying on an overall score from any of these tests could be detrimental to the antivirus software selection process.

The tests also tend to produce a lot of information and can be difficult to interpret due to the amount of data, its format and, in some cases, a lack of agreement on language or terms. For example, the University of Magdeburg results are sometimes available only in German and are not accompanied by any documentation of the test methodology.

The University of Hamburg provides copious documentation, but refers to detection as 'unreliable' if the product does not use a certain virus name, thereby giving the impression that a product which did detect a virus quickly through a good heuristic is unreliable. *Virus Bulletin* provides more of an editorial commentary on other product features and is a good adjunct to the university tests, but it provides less information at any one time than the other tests. In addition, these tests will not consider factors that are specific to every organisation and, therefore, some users have turned to 'certified' products as a way to ensure that their needs are met.

ICSA Labs – a division of TruSecure Corporation – and West Coast Publishing's *Secure Computing* are commercial testers with various for-fee certifications to antivirus product developers. As most of the top products are certified, to some degree, by both ICSA and *Secure Computing*, while these certifications provide a good base-line, they are not entirely helpful as differentiators between products from the standpoint of detection. This could change in the future if more stringent criteria evolve, but it should certainly highlight a product if it is not capable of certification. The 'popular' testing category includes tests that are aimed at a more generalist population, usually by non-specialist magazines. Historically, these tests have achieved legendary inaccuracies and have, on occasion, chosen products in what seems like an arbitrary manner. This reputation is becoming increasingly underserved.

As publications gain a more complete understanding of the issues surrounding the testing of antivirus software, tests have become increasingly welldesigned, therefore, unless someone is capable of discerning the accuracy of a review either by knowledge of the industry or knowledge of the reviewer, it is a mistake to put too much credence in one particular review of a product.

Overall, the important thing to remember is that even the best testing authority can make a mistake. It is crucial not to base an entire decision on only one test or on tests from only one organisation. It is vital to construct a solid overview, pulling from many different sources, in order to choose the right product for an organisation.

The most difficult and controversial aspect of antivirus product testing is the role of the 'company' testers, i.e. those testers who evaluate antivirus software for use in their own company. As the antivirus industry does not generally provide virus samples to customers, some corporate testers obtain virus samples from various sites on the World Wide Web (WWW) to perform their inhouse tests.

This may seem like an acceptable practice, but the fact is that almost no companies have the in-house skill set with which to build and maintain a representative virus library to conduct exhaustive tests adequately nor the facilities to work safely with live viruses. The potential liabilities for this type of scenario generally discourage corporations from incurring the risk.

Possibly the best solution to this impasse is for the person who is assigned to ensuring that the corporate antivirus software is up to the task makes informed use of the work of the other testers that have been outlined, as well as to make use of a tool to test the other, non-virus-related properties of the product – the European Institute for Computer Anti-Virus Research (EICAR) test file (available from http://www.eicar.org).

The EICAR test file is an American Standard Code for Information Interchange (ASCII) file that is detected by most antivirus products as a test file. This

Feel Secure....



If your business had a weak link, what would happen to your Information Security? Would your records and data be at risk?

From:

- Accidental loss
- Sabotage
- Disclosure
- System failure
- Theft

You need to be sure that your resources are safe and at the same time prove to clients that careful guidelines are in place to ensure protection. BS 7799 Information Security Management is a code of recommendations which can help you produce a successful and sustainable security system.

SGS' BS 7799 certification will tighten up your system, making your security strong enough to satisfy you and your customer's requirements.

PROTECT - your information with a Security Management System.

BS 7799 and SGS making sure that you keep a strong hold on your security of information.

SGS United Kingdom Ltd

...With BS 7799

For further information please contact:

SGS United Kingdom Ltd SGS House 217/221 London Road Camberley Surrey GU15 3EY

Tel: +44 (0)1276 691133 Fax: +44 (0)1276 691155

email: ukics@sgsgroup.com website: www.sgs.co.uk

Expertise everyday, everywhere

enables the tester to measure the enterprise installation and reporting features of a product, as well as its potential to detect viruses in incoming e-mail or on access. Therefore, many of the benefits of testing with live viruses are realised without the risks that are associated with this activity.

In addition to the changes within the different groups of testers, there have also been some more general trends in the testing of antivirus products. The most important of these trends are the change in focus towards the detection of 'in-the-wild' viruses and the introduction of non-viral 'malware' to some test sets.

Although there are more than 50,000 computer viruses known at this time, only a fraction of these has ever been encountered on a real user's computer, i.e. spreading actively in the wild. These viruses are tracked by The WildList Organization International (http://www.wildlist.org).

While tests of products have previously focused on the detection of all known viruses, modern tests tend to focus on the in-the-wild test results, which reflect the threat to a group of computers more accurately. This trend is to be encouraged and, while a product should certainly score well against a zoo collection, exceptional performance over a prolonged series of reviews in in-the-wild tests is paramount.

A more controversial shift has been the introduction of non-viral malware to antivirus software testing criteria. Whereas viruses possess the property of selfreplication, malware has a much looser definition, which leaves it somewhat 'in the eye of the beholder'. This non-replicating malware can range from 'back-orifice'-type servers to scripts that format a hard drive automatically.

The concept of malware itself, let alone in the wild, is a difficult one, so it is not entirely clear that an antivirus software product can, or even should, be expected to ever provide adequate protection against all forms of malware. Therefore, when examining software tests, it is important to understand whether the test sets that are used are limited to only computer viruses or if they also include other forms of malware.

A product scoring poorly on malware detection, while flawless when it comes to detecting viruses, could have a lower overall score than a product that detected viruses first time, every time. Therefore, it is important to consider the role that

74

antivirus software should play in preventing malware within an organisation and understand that antivirus software is not designed to protect from all forms of malicious software or security problems. No product will do it all consistently. For that, a comprehensive solution must be sought and tests relied on that actually measure what the product was designed to do.

Future Developments

The last few years have witnessed many changes in the testing and certification world. Consolidation of the industry, the growth of the certification industry and a better understanding of the virus problem itself have all led to better, more meaningful tests. This has benefited the corporate decision-maker directly by providing more complete tests that are centred more tightly around the areas of the product that are of importance in the corporate environment. Today's tests provide a solid, albeit not perfect, measure of product capabilities for the detection of viruses.

One factor that has helped the selection process of antivirus software, as well as limiting the spread of new computer viruses, is that users seem to be less likely to test products themselves, either by testing against virus collections gathered via the Internet or by modifying existing viruses. This helps to limit mishaps, as well as to limit the creation of new viruses under the auspices of 'tests'. Judicious use of the nonviral EICAR test file allows the user to perform installation and alerting tests without exposing them to the liability that live viruses introduce.

However, this is only the beginning. It is inevitable that there will be a gradual integration between generic and specific virus detection techniques in antivirus software over the next 12 to 18 months as it evolves to meet the emergent threats. Networkaware viruses and worms such as Melissa and SirCam have shown that virus-specific techniques are not sufficient to prevent widespread infection by new viruses. Similarly, the inherent drawbacks of postinfection generic techniques and pre-infection heuristics make virus-specific detection a more attractive way to prevent and remove viruses.

Given this situation, a series of products that provide a hybrid approach to the problem is likely to evolve. To measure the ability of the products to do what they must claim to do, new testing models must emerge. These technical developments will present a new set of challenges for testers and to those who rely on them.³

3. An in-depth look at the technical direction that antivirus software development must take and the tests that must evolve in tandem are beyond the scope of this article, but can be found at csrc.ncsl.nist.gov/nissc/2000/proceedings/papers/038.pdf

TO JOIN

The Global Voice of the Information Security Profession

A not-for-profit association of and for Information Security Professionals

Voice of the Security Professional

ISSA is an organization of security professionals dedicated to protecting information resources. We establish the ethical basis for our members unbiased by politics or profits. We are the voice of the Security Profession.

Local Chapters

Over 45 chapters around the world provide local networking and educational opportunities as well as support to get your job done.

Professional Networking

Contacts developed through networking are extremely beneficial for benchmarking security practices and as a resource for you to validate security product functionality. ISSA offers networking opportunities through chapter meetings and the annual conference.

Education

ISSA Chapter meetings, regional events, and the annual conference serve as a vital educational and professional resource. These events offer in-depth and timely information about our industry and an opportunity to further your skills and get solutions and discounts at other information security conferences and training events.

Certification

ISSA endorses the CISSP certification provided by (ISC)2 as the certification for the Information Security Professional. ISSA is a founding contributor of the International Information Systems Security Certification Consortium (ISC)2. Certification provides you with tangible proof of professional competency and serves as a key component in professional skills development.

5

4

Career Growth

Through the networking and educational opportunities ISSA provides, you have a valuable resource to find new employment potentials and have the necessary requirements for the job. ISSA also provides job postings on its web site.

7

Leadership Opportunities

Get involved – promote information security in your company, industry and your community. At the chapter or ISSA Board levels, you can participate, learn and spread the word. Members can earn CPE credits for participation.

Recognition

Member articles are welcome in The ISSA Password newsletter where you can share your ideas about security, management, solutions and innovation. Also, consider being a speaker at the annual conference making a presentation about how you have applied security technology to address risks or ways you have adapted practices to solve problems. Another way to earn CPE credits.

Access to Information

The ISSA web site, http://www.issa.org, provides top-notch information on security technologies and practices. The ISSA Password is the Association's bi-monthly newsletter filled with up-to-the-minute technical, association and chapter news.

Endorsements from others

Check out the opinions of great people regarding the ISSA. See for yourself in the "Quotes from Members" section of the web site.

ISSA Chapters:

Alamo North Coast, Ohio Central Ohio Ottawa Colorado Springs Portland Denver San Diego

- ers: Indianapolis South Florida Los Angeles Tampa Bay Minnesota Toronto New England Hawaii
- New York Metro Capital Of Texas Orange County Chicago Pittsburgh Delaware Valley Sacramento New Mexico
- Silicon Valley Latin America St. Louis Milwaukee North Carolina National Capital Vancouver San Francisco Bay

Baltimore North Texas Central Plains Phoenix Connecticut Puget Sound Greater Cincinnati Netherlands Kansas City South Texas Metropolitan Atlanta Texas Gulf Coast Motor City Utah New Jersey Switzerland

For more information see web site www.issa.org

See how we've grown! Month Membership Jan-99 1782 Feb-99 1734 Mar-99 1686 Apr-99 1688 May-99 1699 Jun-99 1630 Jul-99 1670 Aug-99 1745 Sep-99 1823 Oct-99 1980 Nov-99 2113 Dec-99 2261 Jan-00 2540 Feb-00 2792 Mar-00 3044 Apr-00 2721 . Mav-00 2973 Jun-00 3069 Jul-00 3244 Aug-00 3302 Sep-00 3472 Oct-00 3621 Nov-00 3760 Dec-00 3889 Jan-01 4021 Feb-01 4150 Mar-01 4299 Apr-01 4460 May-01 4482 Jun-01 4500