SOFTWIN

B-HAVE – THE ROAD TO SUCCESS

A CASE STUDY IN THE SUCCESSFUL DEPLOYMENT OF NEW ANTI-MALWARE TECHNOLOGY

"Speed is the name of the game"

bitdefender
secure your every bit

IN OCTOBER 2004, AV-Test, an independent testing organization based in Germany, made public the results of a new kind of test, which aimed to see how fast signatures[1)] were launched for new ITW (In-The-Wild) viruses. The average response time was judged to be an accurate measure of the safety offered, since the faster the response the less the chances of clients getting infected by a new virus (i.e. the *"window of opportunity"* of the virus is smaller).

The study covered the last nine months of 2004, and it released average response times for all antivirus producers. BitDefender came out first, with an average reaction time of two hours, compared to an industry average of 8 hours.

However, self-propelled worms (malware which does not require user intervention to spread), such as the infamous Witty worm, may take minutes, not hours, to infect a sizable portion of the vulnerable population. The limitations of the signature model are evident when considered in this light, as signatures may well arrive too late.

This limitation was eventually addressed by means of a new technology developed in the BitDefender Labs, which enabled clients' computers to identify many new viruses on their own, without the need of first receiving a signature from a central server.

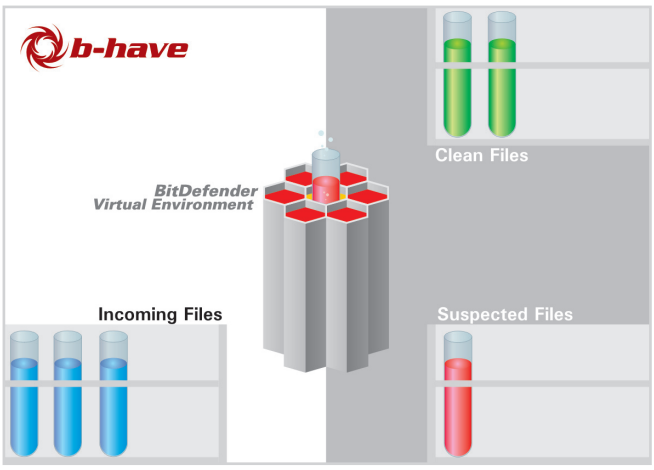
Average response times of AV companies in the last 9 months		
Less than 2 hours:	-	-
Less than 4 hours	**1**	**BitDefender**
	2	Kaspersky
Less than 6 hours	3	AntiVir
	4	Dr. Web
	5	F-Secure
	6	Panda
	7	RAV
Less than 8 hours	8	Quickheal
	9	Sophos
Less than 10 hours	10	AVG
	11	Command
	12	F-Prot
	13	Norman
	14	Trend Micro
	15	VirusBuster
Less than 12 hours	16	Avast
	17	eTrust
Less than 14 hours	18	Ikarus
	19	McAfee
Less than 16 hours	20	eTrust with VET engine
	21	Symantec
Overall response time: about 10 hours		

Courtesy of Andreas Marx (www.av-test.org) October 2004

In April 2005, at the CeBit fair in Hanover, Germany, BitDefender CTO Bogdan Dumitru introduced a new technology to the public:

"What this really does, in layman terms, is create a virtual computer-inside-a-computer, where pieces of software that look suspicious are run to see if they try to do any of the things that viruses and worms usually do. From there on, well, if it looks like a duck and it quacks like a duck, we'll shoot it," declared Bogdan Dumitru, BitDefender CTO.

The technology was phased in gradually, after adequate in-house and field testing, as Viorel Canja, Head of Research at BitDefender Labs, had announced during the same event: *"This BitDefender technology has been two years in the making. The detection rates we've seen in tests are quite good, and further refinements should bring us even closer to our stated goal of* ***60% detection with behavioral heuristics only****."*



[1)] Virus signatures are, quite simply, rules pertaining to what a file "looks like", a bit like fingerprints. However, many files (esp. viruses) look different in memory (or in the virtual environment) than they look on disk or in transit, because they modify themselves (or are modified) in some way at run-time e.g because they are packed or encrypted. Such files cannot be efficiently "fingerprinted", since their in transit or on-disk appearance is largely irrelevant to their functioning.

5 Months later – the first results (PC Magazine, USA, Aug 2005)

However, no more than 5 months passed by, and some parts of the technology were in field trials, when a new independent test showed that the new technology actually worked, and it did a very good job:

Proactive Detection of Malware Based On MS05-039 Vulnerability As Measured By AV-Test

AV-Test *(http://av-test.org/)* is an anti-virus research project at the Institute of Technical and Business Information Systems at the Otto-von-Guericke University Magdeburg (Germany).

They measured the detection times for six of the malware programs released last week utilizing the MS05-039 Plug and Play vulnerability under 36 different anti-virus products. Eleven of the products were able to detect one or more of the attacks proactively, without any special pattern update to identify it specifically. Here are the numbers for each of the eleven:

Product	Score
BitDefender	6 of 6
Fortinet	6 of 6
Nod32	5 of 6
eSafe	3 of 6
F-Prot	3 of 6
Panda	3 of 6
QuickHeal	3 of 6
McAfee	2 of 6
Norman	2 of 6
AntiVir	1 of 6
ClamAV	1 of 6

"Clearly BitDefender and Fortinet did an admirable job in this test, and some of the others weren't too shabby either. AV-Test notes that eSafe, Fortinet and QuickHeal use heuristic detection rules that generate a high number of false positives as well, if scanned files are simply runtime-compressed."
Source: *http://www.pcmag.com/article2/0,1895,1850851,00.asp* (Aug 2005)

In short, BitDefender was the only company to proactively detect all six variants of the Zotob worm without generating false positives. The future of B-HAVE (patent pending technology) looked bright.

5 more months later – Malware detection: Top-Notch (PC World, USA, Jan 2006)

Five more months later, PC World, USA published yet another test, which showed conclusively that B-HAVE lived up to everyone's expectations:
The stated goal of "60% detection with B-HAVE" was pretty close to the actual figures, and looks set on improving in the following months, as the technology would be refined even more. The successful deployment of B-HAVE placed BitDefender in an enviable position:

Product	Proactive Detection	
	Heuristic detection with one-month-old signatures	Heuristic detection with two-month-old signatures
BitDefender 9 Standard	56.00%	38.00%
McAfee VirusScan 2006	53.00%	34.00%
Kaspersky Anti-Virus Personal 5.0	51.00%	26.00%
F-Secure Anti-Virus 2006	52.00%	27.00%
Symantec Norton AntiVirus 2006	22.00%	8.00%
Panda Titanium 2006 Antivirus + Antispyware	21.00%	16.00%
AntiVir Personal Edition Classic 6.32	11.00%	6.00%
Alwil Software Avast Home Edition 4.6	9.00%	5.00%
Trend Micro PC-cillin Internet Security Security 2006	6.00%	3.00%
Grisoft AVG Free Edition 7.1	8.00%	4.00%

"This low-cost antivirus tool performed the best in our heuristics tests and caught the widest range of malware. BitDefender 9 Standard is inexpensive, easy to use, and effective at detecting malware threats; as a result, it earned PC World's Best Buy distinction in "The New Virus Fighters" roundup of ten antivirus products."

Advanced+ Proactive Detection (May 2006)

The independent testing authority AV-Comparatives.org showed in May 2006 that the pro-active detection rate of BitDefender engines was higher than that of all its major competitors (namely F-Secure, Kaspersky, McAfee, Symantec and Panda) outperforming the closest competitor's detection rate by 15% and that of Symantec by a solid 29%. Detailed results are available on the AV-Comparatives.org website.

http://www.av-comparatives.org/seiten/ergebnisse_2006_05.php

All BitDefender workstation and server products embody the B-HAVE technology, the latest and most successful pro-active software defense.

B-HAVE advantages over other existing technologies:

- generic unpacking methods which provide 0-day unpacking support for new packers.
- visual basic runtime engine for proactive detection of visual basic viruses.
- faster because most functions implemented in our windows subsystem are not emulated but rather natively run, thus dramatically increasing the scanning speed.
- enabled by default on-demand and on-access.
- COM support in order to fully emulate VB viruses.
- good against viruses and backdoors, but also against Trojans.
- very good static unpacker support.
- platform independent: it runs on Windows as well as on all Linux and FreeBSD flavors
- BAT/CMD emulation embedded in the virtual machine

About BitDefender®

BitDefender is a leading global provider of security solutions that satisfy the protection requirements of today's computing environment. The company offers one of the industry's fastest and most effective lines of security software, setting new standards for threat prevention, timely detection and mitigation. BitDefender delivers products and services to over 41 million home and corporate users in more than 100 countries. BitDefender has offices in the United States, the United Kingdom, Germany, Spain and Romania. Further information about BitDefender can be obtained by visiting: *www.bitdefender.com*

Contact Info

Efficient communication is the key to a successful business. For the past 10 years SOFTWIN has established an indisputable reputation in exceeding the expectations of clients and partners, by constantly striving for better communications. Please do not hesitate to contact us regarding any issues or questions you might have.

Country: **U.S.A**
Contact: Eric D Lewis
Function: General Manager
Company: **BitDefender LLC**
Address: 6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Phone: 954 776 62 62
Fax: 954 776 64 62
Email: *sales@bitdefender.us*

Country: **Romania**
Contact: Oliviu Talianu
Function: Country Manager
Company: **SOFTWIN SRL**
Address: 5th Fabrica de Glucoza St. Bucharest
Phone: +40 21 2330780
Fax: +40 21 2330763
Email: *sales@bitdefender.ro*

Country: **Germany**
Contact: Martin Siemens
Function: Geschäftsführer
Company: **Softwin GmbH**
Address: Karlsdorfer Straße 56 88069 Tettnang
Phone: 07542/94 44 44
Fax: 07542/94 44 99
Email: *msiemens@bitdefender.de*

Country: **Spain**
Contact: Florin Baras
Function: General Manager
Company: **Constelación Negocial, S.L**
Address: C/ Balmes 195, 2ª planta, 08006 Barcelona, España
Phone: +34 932189615
Fax: +34 932179128
Email: *fbaras@bitdefender-es.com*