

BITDEFENDER ANTIVIRUS TECHNOLOGY

White paper

Introduction

This is an executive summary of the architecture, design and general structure of the BitDefender Antivirus.

The BitDefender Antivirus System presents a pluggable and distributed architecture that is based on distinct scanning engines for different types of files and malware. Its distinct plug-ins can be loaded on-the-fly, one for each kind of malware, without reconfiguring the whole system or restarting it.

Each type of malware is dealt with by a plug-in which can detect and possibly disinfect/clean the given malware type. As an example, the Antispyware modules were integrated into BitDefender 9 Internet Security right alongside the antivirus-specific ones. Plugins function sequentially (i.e. they take turns at checking each file), to detect malware like viruses, worms, trojans, exploits and also spyware. The plugin architecture is such that the plugins can pass messages between themselves.

The modularized architecture used to build BitDefender has contributed to its ability to be used in a variety of environments ranging from embedded systems to workstations and high-end servers, in desktop, dedicated or generic server solutions.

BitDefender antivirus technology is integrated in a diverse range of products from: Data Becker, G Data, GFI, Hauri, Ipswitch, Laplink, Software 602, Bullguard, and others.

BitDefender Antivirus is portable and platform independent, presenting compatibility at binary level for any IA32 based Operating Systems (such as: Windows, Linux, FreeBSD) and at the source code level for other OS's.

An added side-benefit of having portable binaries is that the BitDefender Antivirus is effectively isolated and largely independent from the host OS, which makes the adding of detection routines a relatively straightforward process, which does not have to be repeated for each OS to deal with compatibility issues.

BitDefender Antivirus is differentiated into two main components:

- **The Scanning Engines**
- **The Archive Logic**

The Scanning Engines

The scanning engines are comprised of modules which are continually being developed to offer full protection against all types of malware including, but not limited to: executable viruses, script viruses, macro viruses, backdoors, trojans, spyware, dialers, etc. Every virus family benefits from a dedicated scan engine which was designed in accordance with the class characteristics.

- High speed. Multi - threading architecture
- Low memory consumption.
- 100% disinfection for In The Wild viruses as certified by ICSA Labs and Checkmark
- Proactive detection of viruses including various versions of very well known viruses such as Bagle, Zafi, Sober, Zotob
- Using this technology BitDefender can detect suspicious activity common to P2P worms, E-mail worms, Antivirus Killer programs and many other
- The optimized emulation procedure enables BitDefender to analyze the behavior of all files types in a virtual machine without significant performance impact.

BitDefender Antivirus System

The scanning engines benefit from a number of technologies which have been implemented over time:

Classic antivirus scanning (pattern matching)

In February 2006, BitDefender had in its database over 270 thousand malware signatures (of which “only” 256 thousand were viruses and worms, and the rest as spyware. This is not to say, however, that BitDefender can detect 270 thousand pieces of malware – the addition of generic signatures means that many “related” virus or spyware threats are described with one signature, so the actual number is much higher. The generic signatures can also help to protect against new variants of old malware.

Heuristic Scanning

B-HAVE [2]: combines a lot of different techniques to proactively detect malware.
B-HAVE is the basis for:

- Behavior-based heuristics
- Generic detection routines,

- Virtual Machine for VB scripts
- Virtual Machine for BAT/CMD scripts
- VB script emulator
- Virtual Machine for executable files (PE, MZ, COM, SYS, Boot Images)

B-HAVE is by now thoroughly proven technology and is responsible for some spectacular results:

- According to independent German testing outfit AV-Test, BitDefender antivirus was capable to detect six out of six variants of the Zotob virus without the need for a signature update.
- The PC World test held in January current nominated BitDefender as the best antivirus where detection of new/unknown viruses is concerned.

The B-HAVE technology also acts as a “force multiplier” for other, more traditional forms of defense. For example, files which emerge from the B-HAVE environment (OLE components, dropped executables, etc) are then filtered by the other modules, possibly even in a recursive manner (where they are afterwards returned to the B-HAVE component for a “second opinion”, or go straight into the more classical heuristic filters.

In addition to content-based heuristics, which is now in wide use even among our competitors, B-HAVE implements behavior-based heuristics, which reduces false positives enormously and increases detection rates for new malware.

Exploit detection code

Special detection routines can (and have been) added to the BitDefender Antivirus to root out exploit code, such as the recent unpatched WMF exploit. Thus sometimes detection is available for worms using a new exploit long before the actual worms are written.

The archive Logic

BitDefender Antivirus archive logic component is built around the concept of “in-depth scanning”, which means that it can be configured to scan embedded archives down to any depth, while still being relatively impregnable against zip bombs or other forms of DoS attack against itself.

- Generic unpacking for executables packed with new packers 80% of new viruses appearing in the wild use some form of packing, but packing apps are legion, and more are created every day. Generic unpacking routines allow for variations in packing format, and so can unpack new/unknown types of packed files.
- Scanning support for over 18 types of archivers and more than 100 packers (including UPX, Neo-Lite, ASPack, PECrypt, pklite and self extractable files SFX) as well as the majority of installation packers and mail archive types.

BitDefender Antivirus has cleaning support for .zip, some mail databases, .gzip and other types of archives. The archives are unpacked, files are checked, cleaned and then repacked.

BitDefender scans inside the most common type of archives and packed files, including, but not limited to the following:

Supported archive types

Ace	Arc	Arj	Bzip2
Cab	Cpio (clean + delete)	Gzip (clean + delete)	Ha
Imp	Jar	MS Compress	Lha (lzx)
Rar (including 3.0)	Rpm (clean + delete)	Tar (clean + delete)	Z
Zip (clean + delete)	Zoo		

Mail archives

Dbx (Outlook Express 5, 6 mailboxes)	Mbx (Outlook Express 4 mailbox)	Pst (Outlook mailboxes - supports clean and delete)	Mime (base64, quoted - printable, plain) - supports clean and delete
Mbox (plain mailbox - Linux and Netscape)	Hqx (HQX is a format used for mail attachments on Mac)	Uudecode	Tnef (a Microsoft format in which some properties of the attachments are encoded, it can contain scripts).

Installation packers

Inno (Inno Installer)	Instyler	WISE (viza.xmd)
InstallShield (ishield.xmd)	Nullsoft Installer (NSIS)	Wise Installer

Supported packers

ACProtect/UltraProtect	ASPack (all versions)	Bat2exec (1.0, 1.2, 1.3, 1.4, 1.5, 2.0)	Yoda's Cryptor
CExe	Diet	DxPack	Dza Patcher
ECLIPSE	Exe32Pack (1.38)	ExePack	ExeStealth
Ezip 1.0	Fsg	Ice	JdPack
JdProtect	Lzexe	Mew	Molebox (2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.8)
Morphine	Neolite		PC/PE Shrinker 0.71
PCPEC	PE Crypt 32 (1.02 (a,b,c))	PE PACK\CRYPT	PeBundle
pecompact (up to 1.40 beta 3)	PeDiminisher	PELock NT	Pencrypt (3.1, 4.0a, 4.0b)
PePack (all versions)	Perplex	PeShield	PeSpin
Petite (all versions)	Pex	PhrozenCrew PE Shrinker (0.71)	PkLite
PKLITE32 (1.11)	Polyene	RelPack	Rjcrush (1.00, 1.10)
Shrinker (3.3, 3.4)	VgCrypt	Stpe	Telock (all versions)
T-pack	Ucexe	UPolyx	UPX (all versions)
WWPACK32 (1.0b9, 1.03, 1.12, 1.20)	Wwpack (3.01, 3.03, 3.04, 3.04PU, 3.05, 3.05PU)	Xcomor (0.99a, 0.99d, 0.99f (486), 0.99h, 0.99i)	

Others

Chm (contains html-s which can be infected)	Iso (CD images)	Pdf	Rtf
Mso (contains compressed OLE2 files, this way the macro's are saved in case a Doc is saved as html)	Swf (extracts certain fields that contain various commands; these are scanned by other plug-ins, for ex: SDX)	Bach (extracts debug.exe scripts on the basis of heuristic methods)	Omf (object file)

Notes:

[1] **malware:** "A program can be regarded as malware if it does at least one of the following:

- replicates through a network or a file system without users' consent
- allows an unauthorized person control over a remote system
- sends information or files to a remote system without user's consent
- sends data to a system in order to disrupt normal functioning."

[2] **B-HAVE:** Behavioral Heuristic Analyzer in Virtual Environment (patent pending technology)

Ref:

BitDefender Naming Conventions: <http://www.bitdefender.com/site/Naming-Conventions.html>

Malware on Wikipedia: <http://en.wikipedia.org/wiki/Malware>

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 Tetttnang
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