virus BULLETIN

VIRUS BULLETIN PRODUCT REVIEW JUNE 2008: SUNBELT SOFTWARE VIPRE ANTIVIRUS + ANTISPYWARE

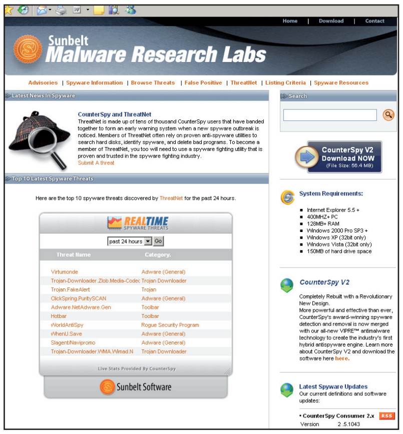
This month's review product is something quite exciting – a genuinely new anti-malware product emerging from the anti-spyware boom.

Many years ago, anti-virus developers opted to ignore malicious trojan programs, considering them to be outside their remit, and only later did they come to conclude that protection from such threats was a vital part of security. With spyware ignored by many established products, specialist anti-spyware products sprang up to fill the gap. When the wheel turned once again and spyware came to be understood as just another facet of the malware field, most of the leading players in the anti-virus market added anti-spyware functionality to their products. Similarly, players in the anti-spyware market adapted by either buying in or licensing anti-virus technology to complement their own.

Sunbelt Software, meanwhile, whose *CounterSpy* product remains one of the undoubted leaders in the anti-spyware arena, took the more arduous path of developing its own scanning engine to cover the wider range of malicious code. The long-awaited *VIPRE* (*Virus Intrusion Prevention and Recognition Engine*) is the fruit of the company's labours. Currently still in beta, with full release delayed somewhat longer than expected, the product has built up considerable expectations and I was excited to be able to take an early look at its capabilities.

WEB PRESENCE, INFORMATION AND SUPPORT

Sunbelt's online presence, and much of its brand recognition within the security industry, owes a lot to the company's renowned blog – which has become a regular recommendation in 'top 100 blogs' lists including those maintained by *PC World* and *CNET News.com*. The blog (at http://sunbeltblog.blogspot.com/) is run almost single-handedly by the firm's energetic CEO Alex Eckelberry, who keeps up a startlingly regular stream of updates on the latest developments in security, covering new scams and malware techniques, industry and market events, security-related news items (the blog was a pivotal campaign ground in the infamous Julie Amero case), with the occasional off-topic digression into humour and skateboarding pics.


Home | Download | Contact
Sunbelt
Malware Research Labs
Advisories | Spyware Information | Browse Threats | False Positive | ThreatNet | Listing Criteria | Spyware Resources
Latest News In Spyware
Search
CounterSpy V2 Download NOW (File Size: 56.4 MB)
Top 10 Latest Spyware Threats
REALTIME SPYWARE THREATS
past 24 hours
Go
Live Stats Provided By CounterSpy
Sunbelt Software
RSS

CounterSpy and ThreatNet

ThreatNet is made up of tens of thousand CounterSpy users that have banded together to form an early warning system when a new spyware outbreak is noticed. Members of ThreatNet often rely on proven anti-spyware utilities to search hard disks, identify spyware, and delete bad programs. To become a member of ThreatNet, you too will need to use a spyware fighting utility that is proven and trusted in the spyware fighting industry.

Submit A threat

Here are the top 10 spyware threats discovered by ThreatNet for the past 24 hours.

Threat Name	Category.
Virtumonde	Adware (General)
Trojan-Downloader.Zlob.Media-Codec	Trojan Downloader
Trojan.FakeAlert	Trojan
ClickSpring.PuritySCAN	Adware (General)
Adware.NetAdware.Gen	Toolbar
Hotbar	Toolbar
WorldAntiSpy	Rogue Security Program
WhenU.Save	Adware (General)
Slagent/Navipromo	Adware (General)
Trojan-Downloader.WMA.Wimad.N	Trojan Downloader

System Requirements:

- Internet Explorer 5.5 +
- 400MHZ+ PC
- 128MB+ RAM
- Windows 2000 Pro SP3 +
- Windows XP (32bit only)
- Windows Vista (32bit only)
- 150MB of hard drive space

CounterSpy V2

Completely Rebuilt with a Revolutionary New Design.
More powerful and effective than ever, CounterSpy's award-winning spyware detection and removal is now merged with our all-new VIPRE™ antimalware technology to create the industry's first hybrid antispyware engine. Learn more about CounterSpy V2 and download the software here here.

Latest Spyware Updates
Our current definitions and software updates:

• CounterSpy Consumer 2.x
Version 2 .5.1043

The firm's official website, www.sunbeltsoftware.com, is a slightly more sober place, but still bright and cheerful and adorned with the hot orange of the company's logo. The site's front pages are dedicated mostly to promoting the company's product range, which as well as various versions of *CounterSpy* includes a highly respected personal firewall (known as *Kerio* prior to its acquisition by *Sunbelt*), anti-spam and general email security products for home and enterprise users, and a selection of backup, compliance and vulnerability management tools.

Further into the site there is a research subsite offering a range of information and resources, including details of the latest threats, outbreak alerts and a threat database. The database is dominated by spyware but also includes a range of viruses, worms and other types of threat. Product updates and white papers are also provided here, along with access to another product, the *CWSandbox* malware analysis tool. This can be used as an online resource, quickly processing submitted files and providing detailed reports of their behaviours, and is also available as a standalone product for simple and effective analysis of suspect files.

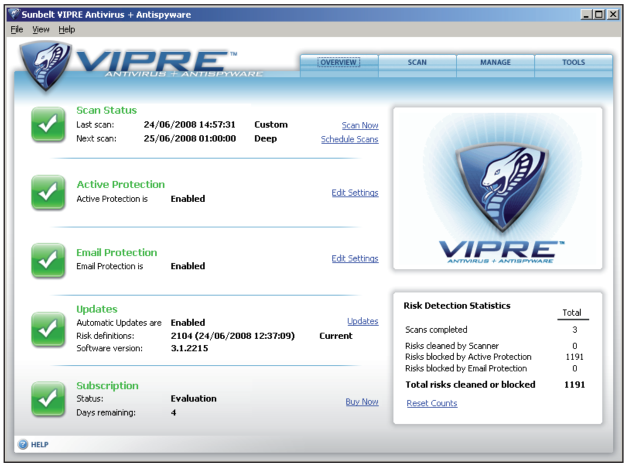
A support section provides a variety of methods for getting assistance, with the usual online form and generic email address complemented by an all-too-rare telephone number. A knowledgebase, which seems fairly well populated, is also provided to solve common issues, and the site hosts an impressive range of busy forums, discussing not only the company's own products but also a selection of other topics of interest to systems and security admins. These services are backed up by a series of news mini-sites providing top stories and comment on various versions of *Windows* as well as *CounterSpy*.

Documentation for the products was a little tricky to find, as I had assumed that the manuals etc. would be included in the support section. However, I eventually turned up a batch of user- and quick-start guides in the products section, which I found were well designed and written in informal, chatty language to minimise the fear factor. Instructions are given based on tasks rather than controls, allowing for easy mastering of important configuration and management jobs. A full user manual did not seem to be available, but this was more than made up for by the excellent inline help I discovered after installing, with the appropriate entry linked to from just about every area of the product, providing clear and simple guidance on the operation and use of the various functions.

INSTALLATION AND CONFIGURATION

Having prodded around enough, I finally sat down to try out the product itself. The installer package came in at a pretty reasonable 23.5 MB; this compactness, I later discovered, was helped by the product being provided with no detection data at all to begin with, relying instead on an initial update to get everything up to speed. The installation process began along pretty standard lines, with the usual warnings to ensure no other anti-virus software was running, a lengthy EULA, and the selection of install destination before the file-copying process got under way. This seemed reasonably speedy on most systems, taking less than a minute on even a few rather decrepit and underpowered ones. A reboot was required to finalise things.

After the reboot, the completion of a series of setup tasks was required, starting with providing details of any proxy that might be in use before defining the update settings. An initial update could be run manually from here, and options were available for allowing the product to initiate a web connection if required, and to pull down updates at will, with a default timing of every two hours. Next came the 'Active protection' module, the real-time scanner (for which a level of paranoia could be selected), and email scanning, which could be set to monitor particular ports for SMTP traffic if required.



Scan Status
Last scan: 24/06/2008 14:57:31 Custom Scan Now
Next scan: 25/06/2008 01:00:00 Deep Schedule Scans

Active Protection
Active Protection is Enabled Edit Settings

Email Protection
Email Protection is Enabled Edit Settings

Updates
Automatic Updates are Enabled Updates
Risk definitions: 2104 (24/06/2008 12:37:09) Current
Software version: 3.1.2215

Subscription
Status: Evaluation Buy Now
Days remaining: 4

Risk Detection Statistics	Total
Scans completed	3
Risks cleaned by Scanner	0
Risks blocked by Active Protection	1191
Risks blocked by Email Protection	0
Total risks cleaned or blocked	**1191**

Reset Counts

This was followed by the 'ThreatNet' settings, a herd immunity scheme to which users can contribute suspect files if desired, and then the scheduling of scans. This seemed to lack a little granularity and could either be off or running nightly at 1 a.m. – finer tuning of this setting (to allow night hawks to carry on gaming uninterrupted into the small hours) turned out to be available in the interface proper. Then there were some options to integrate with the *Windows Security Center*, and to disable *Windows Defender* if running, then activation and registration options, and finally everything was good to go. Keen users can celebrate the end of this rather lengthy process by viewing an online demonstration video, in which a smooth voice guides the viewer through the basics of the product's layout.

I decided to explore the product for myself however, and got my first look at the interface itself. It presented a pretty attractive face to the world, adorned with a snazzy snake-on-a-shield logo. The front page is clean and clear, with a list of the major components marked with the standard green tick/red cross to indicate their status, and some simple statistics in one corner. Each section has a link to the appropriate controls page, and a row of tabs along the top provides access to further functions. Even the most inexperienced software user would have no trouble finding their way around.

Most of the settings options lead to the appropriate tab of a unified configuration window, where many of the settings defined during the initial setup process can be adjusted, along with some more in-depth controls for some areas. Granularity in the controls for both on-demand and on-access scanning is fairly reasonable; checking of certain locations, file types and threat types can be switched on or off and response to threats can be either automated or interactive. The on-access scanner can be set to monitor custom file types by extension and even includes a limited intrusion prevention system, which can be set to monitor a range of system areas for signs of unauthorised interference. These monitors ‘allow all’ by default but can be set to prompt for permission before allowing changes to things like the hosts file, pivotal registry settings and *Internet Explorer* settings.

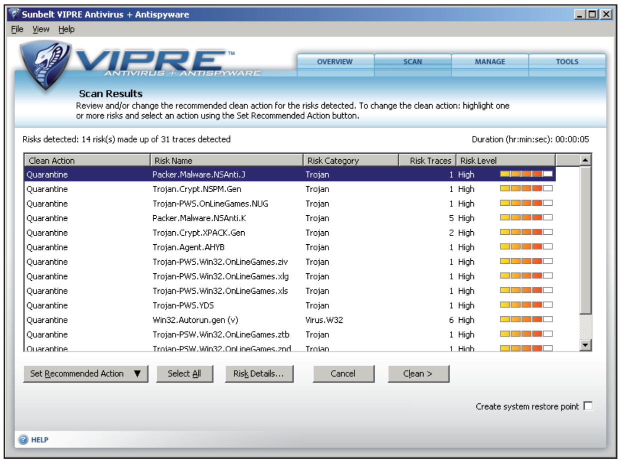
The tabs along the top give access to a range of extra tools, some management tasks including scheduling jobs, perusing the quarantine and scan and detection histories (detailed logging is available), and the lists of ‘always allowed’ and ‘always blocked’ items. The on-demand scanner has its own tab, offering a quick mode and a ‘deep’ mode, as well as a custom option, and of course can also be operated via a right-click menu entry.

The full set of updates were downloaded fairly speedily but expanded to an impressive 55 MB once installed. After transferring these to my test systems I put the various options to use running some scans over the *VB* sample collections.

SYSTEM PROTECTION AND MALWARE DETECTION

Some initial scans of our clean test sets provided an idea of the scanning speed of the product, which was pretty impressive across the board – perhaps not quite up with the very fastest products measured over the same test sets in recent VB100 comparatives, but some way ahead of most. With the product getting its first glimpse of these large and diverse test sets – which have a habit of tripping up even the most respected products on a regular basis – I expected to see quite a large number of false alarms, but was surprised to find only a tiny number of fairly obscure items flagged as suspicious.

Moving on to the malware sets, scanning across the full range of items produced fewer surprises. Detection rates over the more recent sets of widespread worms and bots were excellent, as was coverage of the collections of trojans and spyware that are currently being compiled from recent reports. File-infecting malware was always going to be more difficult, and detection of some of the older samples was understandably limited, but some of the macro sets were handled impressively. Detection of polymorphic items, including some of the W32/Virut strains riding high in our prevalence reports in recent months, was somewhat patchy, but this is something that *Sunbelt* is working to improve as the product nears its final release, collaborating with certification agencies to ensure more complete coverage. Although the product was not quite ready for entry in the latest VB100, it looks like a strong contender for achieving certification once it is fully released.



Scan Results

Review and/or change the recommended clean action for the risks detected. To change the clean action: highlight one or more risks and select an action using the Set Recommended Action button.

Risks detected: 14 risk(s) made up of 31 traces detected

Duration (hr:min:sec): 00:00:05

Clean Action	Risk Name	Risk Category	Risk Traces	Risk Level
Quarantine	Packer.Malware.NSAnti.J	Trojan	1	High
Quarantine	Trojan.Crypt.NSPM.Gen	Trojan	1	High
Quarantine	Trojan-PWS.OnLineGames.NUG	Trojan	1	High
Quarantine	Packer.Malware.NSAnti.K	Trojan	5	High
Quarantine	Trojan.Crypt.XPACK.Gen	Trojan	2	High
Quarantine	Trojan.Agent.AHYB	Trojan	1	High
Quarantine	Trojan-PWS.Win32.OnLineGames.ziv	Trojan	1	High
Quarantine	Trojan-PWS.Win32.OnLineGames.xlg	Trojan	1	High
Quarantine	Trojan-PWS.Win32.OnLineGames.xls	Trojan	1	High
Quarantine	Trojan-PWS.YDS	Trojan	1	High
Quarantine	Win32.Autorun.gen (v)	Virus.W32	6	High
Quarantine	Trojan-PSW.Win32.OnLineGames.ztb	Trojan	1	High
Quarantine	Trojan-PSW.Win32.OnLineGames.znd	Trojan	1	High

Create system restore point □

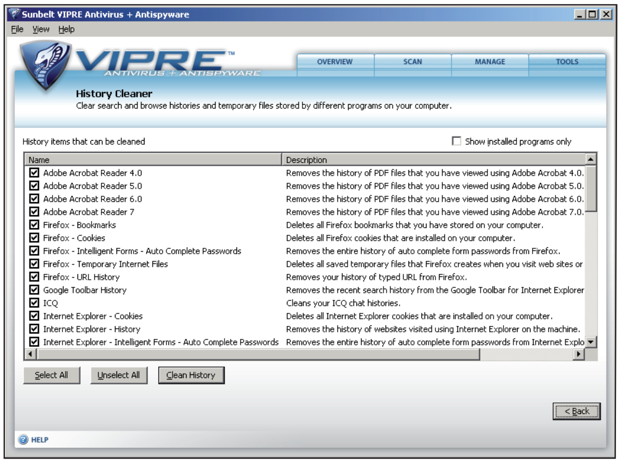
The on-access scanner showed similarly good scanning speeds, reflecting the low scanning overheads experienced during some general playing around on a protected system, and detection rates closely matched those of the on-demand side. A heavy bombardment (attempting to access tens of thousands of infected samples) did seem to overwhelm the product somewhat, bringing up some C++ runtime error messages and leaving the test system pretty crippled, but such an extreme situation is unlikely to be encountered in the real world, and once again the issue should be smoothed out in the final stages of pre-release testing. Turning up the paranoia levels sparked alerts on a wider range of items including the opener tool used for the on-access test, whose behaviour of accessing large numbers of files at once was rightly judged to be a little suspicious.

This led me to try out some of the intrusion-prevention monitors available in the advanced options of the ‘Active protection’ module, which once activated were able to spot and block many of the activities of a selection of new and unknown threats, including changes to the hosts file, installation as startup items, and other common steps in setting up an infection. With all options enabled it pretty much locked the system down, prompting for permission for just about any unexpected execution or action. With the product disabled a handful of other items were installed and, once re-enabled, *VIPRE* showed impressive abilities in the removal and cleanup of some tricky infections.

There was not enough time to carry out fully in-depth testing of the product’s various capabilities against a wider range of malware, but I hope to see it appearing in VB100 tests soon. I also hope to be able to review the product again at around the time the suite version emerges, when I will be able to give it a more thorough exercising.

OTHER FUNCTIONALITY

For the moment at least, *VIPRE* provides a bare bones anti-malware system rather than a full suite; integration with



History Cleaner
Clear search and browse histories and temporary files stored by different programs on your computer.

History items that can be cleaned

□ Show installed programs only

Name	Description
☑ Adobe Acrobat Reader 4.0	Removes the history of PDF files that you have viewed using Adobe Acrobat 4.0.
☑ Adobe Acrobat Reader 5.0	Removes the history of PDF files that you have viewed using Adobe Acrobat 5.0.
☑ Adobe Acrobat Reader 6.0	Removes the history of PDF files that you have viewed using Adobe Acrobat 6.0.
☑ Adobe Acrobat Reader 7	Removes the history of PDF files that you have viewed using Adobe Acrobat 7.0.
☑ Firefox - Bookmarks	Deletes all Firefox bookmarks that you have stored on your computer.
☑ Firefox - Cookies	Deletes all Firefox cookies that are installed on your computer.
☑ Firefox - Intelligent Forms - Auto Complete Passwords	Removes the entire history of auto complete form passwords from Firefox.
☑ Firefox - Temporary Internet Files	Deletes all saved temporary files that Firefox creates when you visit web sites or
☑ Firefox - URL History	Removes your history of typed URL from Firefox.
☑ Google Toolbar History	Removes the recent search history from the Google Toolbar for Internet Explorer
☑ ICQ	Cleans your ICQ chat histories.
☑ Internet Explorer - Cookies	Deletes all Internet Explorer cookies that are installed on your computer.
☑ Internet Explorer - History	Removes the history of websites visited using Internet Explorer on the machine.
☑ Internet Explorer - Intelligent Forms - Auto Complete Passwords	Removes the entire history of auto complete form passwords from Internet Explo

Sunbelt's personal firewall is expected soon, along with a corporate version of the product, and it seems likely that some of the company's anti-spam technology will eventually be added too. 'Bare bones' is perhaps a little misleading, as there is in fact considerably more on offer than simple malware detection, blocking and removal.

The first entry on the 'Tools' tab is a secure file eraser, which as far the interface is concerned only provides the chance to add an extra deletion option to the *Windows Explorer* context menu. This promises to shred files securely, beyond the reach of even specialist recovery tools, to ensure confidential data cannot fall into the hands of even the most determined thief. The exact method of deletion is not disclosed, but for most purposes a few levels of random overwriting are a pretty sure bet.

The history cleaner is a rather more complex tool, offering to remove temporary cache files, cookies, browsing history etc. from a pretty exhaustive range of browsers, media players, chat programs and much more besides. These can be configured to show only installed items, and also to leave some products alone, but new products cannot be added manually (presumably updates provided by the vendor can add coverage for extra items and the latest versions of those already included).

The third and last of the extra tools is 'PC Explorer', an even more sophisticated gizmo providing access to a range of low-level information, much of which is often concealed from users in the normal course of things. Lists of running processes, processes launched at startup, installed ActiveX objects and Browser Helper Objects and the contents of the hosts file, along with several other categories, can be perused, marked as safe if recognised, and more detail on most is available at the click of a button. In stark contrast to the idiot-proof simplicity of the main parts of the interface, this is seriously technical stuff that is likely to be beyond the understanding of the average user, but both fascinating and useful for the more computer-literate. The lack of simple buttons to fix unwanted items would mean that any problems discovered using this tool would require some technical knowledge in order to be corrected manually.

CONCLUSIONS

Having had high expectations of this long-awaited product, *VIPRE* did not disappoint. The design and layout is splendidly clear and useable, the range of features easily accessed and controlled. The protection capabilities are impressive, and will doubtless be even more so once a final release is available. In the area of virus detection, which is fairly new to the company, detection was rather impressive (if not yet up to the same level as the spyware handling), and this looks set to improve in leaps and bounds as the company dedicates more of its time and expertise to the problem.

There are several innovative items in this product, including the limited but potent intrusion prevention options and the string of useful and well-thought-out extra tools. The innovation carries on beyond the technical side of the product to include the availability of a 'home site licence', allowing home users with multiple computers – which is not uncommon these days – to protect all their systems for a single price.

If the next stage of the product's development – rolling in the company's full personal firewall technology to create a full-blown catch-all suite product – can maintain the high standards of design, solidity and usability seen here, it will surely be a force to be reckoned with.

Technical details

Sunbelt VIPRE was variously tested on:

AMD K7, 500 MHz, 512 MB RAM, running *Microsoft Windows XP Professional SP2*.

Intel Pentium 4 1.6 GHz, 512 MB RAM, running *Microsoft Windows XP Professional*.

AMD Athlon64 3800+ dual core, 1 GB RAM, running *Microsoft Windows XP Professional SP2* and *Windows Vista SP1* (32-bit).

AMD Duron 1 GHz laptop, 256 MB RAM, running *Microsoft Windows XP Professional SP2*.

Sunbelt Software

Sunbelt Software, 33 North Garden Avenue, Suite 1200,
Clearwater, Florida, USA 33755, Tel: + 1-727-562-0101,
Email: sales@sunbeltsoftware.com,
http://www.sunbeltsoftware.com/