

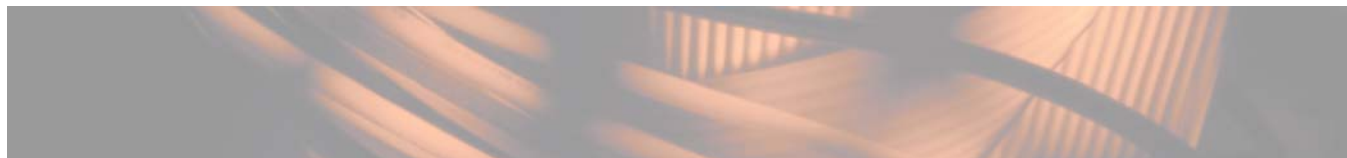
**ANTI-SPYWARE SOLUTIONS
TECHNOLOGY REPORT**

FEBRUARY 2006

ESET NOD32



Contents



Eset NOD 32



Introduction	3
Spyware - More than an emerging threat	4
Test specifications	6
The product	8
Test results	10
West Coast Labs conclusion	13
Security features buyers guide	14
Appendix 1 – Checkmark spyware certifications	16
Appendix 2 – Glossary of malware	17



Introduction

When discussing and evaluating anti-spyware products, the most immediate difficulty is that there is little agreed definition of spyware, and little agreement as to whether a given sample is or is not spyware. Compared with the firmly established classifications in fields such as macro and boot sector viruses, this does tend to make our work very difficult. How can detection be measured if the items to be detected cannot be agreed?

Groups such as the Anti-Spyware Coalition are now attempting to define the various spyware classifications, looking not just at how the malware in question works but also at the methods used to analyse it. West Coast Labs supports the efforts of the ASC and for our testing purposes, the products fighting spyware are divided into three groups: gateway products, desktop products and products aiming to remove installed spyware. Each group requires a different approach to carry out its anti-spyware functions.

As for defining their opponents, we have established some base standard definitions, in which we consider that the most important facts are unauthorised usage of an Internet connection, the gathering of information (often financial or commercial) about the user and transmission of that data to external destinations. We do not include adware in these definitions, as that produces a rather different level of problem.

Spyware - More than just an emerging threat

Over recent years the history of malware can be seen as a series of waves, each cresting then fading as new waves arrive. Recently there have also been two main trends; the decline of traditional viruses and the change in the nature of malware writers. Comparatively few new pieces of malware now match the traditional definition of viruses as a parasitical infection of files and/or boot sectors. Worms remain frequent, but more and more of the new samples that continue to emerge so steadily are now loosely termed 'spyware'.

There is little universally agreed definition of what this term means, but two things are generally agreed; the facts that most infections are now produced for commercial purposes, and that most of these are now written by a new breed of malware writers. Previously virus writers may have acted from malice but generally did not try to steal from those they infected. Now, malware is becoming a very profitable business.

Infection by spyware can prove very expensive. Think beyond the loss of computer service caused by old-style infections; think even beyond the theft of credit card and online banking details. What if competitors received your customer database, your forthcoming plans, your accounts and your staff salaries? Or what if the information was stolen and you had to pay for its return?

No reliable statistics exist as to how much damage malware causes each year, because many companies who have found themselves compromised prefer to keep that fact hidden. Losses are estimated to be somewhere between \$50 and \$100 billion each year, with a steady increase from year to year. These include harm ascribed to viruses and worms, but increasingly are caused by spyware.

Spyware - More than just an emerging threat

Under the definitions that we have established, spyware includes backdoors, downloaders, exploits, crackers, hijackers, password stealers, key loggers and proxys as well as financials - programs designed to steal financial information. Our full definitions of these terms can be found in Appendix 2 of this White Paper.

As to what comes next, no-one can be sure. One thing that seems likely is a rise in targeted attacks, where malware is not released generally but is tailored to assault a particular company for a particular purpose. These succeed partly by not being widespread enough to attract the attention of the antispymware industry before the attack occurs, and thus not providing the target with any advance protection. Companies and individuals will need all the assistance they can get against spyware; the following products can help.

Test specifications

The overall objective of this technology report is to evaluate each participating Anti-Spyware solution in a controlled environment, representing that of an SME. Throughout the test period each product had internet access and was configured as recommended to update online. Products were tested in accordance with the functionality and performance criteria of the levels of registration they hold in the Checkmark certification program.

www.check-mark.com

1. MANAGEMENT/ADMINISTRATION.

The testing reported on the following functions:-

- Installation
- Product update process
- Logging and reporting function

2. FUNCTIONALITY

The testing reported on the following spyware detection capabilities

- Products were tested in accordance with the relevant Checkmark spyware certification tests to determine the ability to detect malicious spyware.
- Under Desktop testing, the product was asked to detect all Spyware samples in the then current West Coast Labs test suite, with the spyware samples held on the file system but not installed prior to testing.
- Under Gateway testing, the product was asked to block all Spyware samples in the then current West Coast Labs test suite from passing through the product.
- Under Installed testing, the product was asked to detect and nullify a range of previously installed Spyware samples drawn from the then current West Coast Labs test suite.

Test specifications (continued)

3. TEST SUITE

The test suite includes a variety of backdoors, downloaders, exploits, proxys, RATs, password stealers, crackers, hijackers and financials. West Coast Labs has its own procedures for harvesting and analysing samples on a daily basis.

After analysis to determine the malicious activity of the sample, in particular the threat that it poses to a corporate network, it is then added where appropriate to the test suite.

The product

ESET has been a member of the Checkmark certification scheme since 2003.

NOD32 has been certified on Windows XP Professional since 2005, currently holding the Checkmark AntiVirus Level One and Level Two and the Trojan and Anti-Spyware Desktop certifications. NOD32 is also registered on Windows 2003 server, Exchange and Linux.

As part of the scheme, NOD32 is tested on Windows XP Professional on four occasions to both AV Level 1 and Level 2 to assess its virus detection and disinfection capabilities, on four occasions against the West Coast Labs Spyware collection, and on eight occasions against the West Coast Labs Trojan collection during each 12 month registration period. The complete test history for this product, including results that may postdate this report, can be found at www.westcoastlabs.org.

ESET has a long history in the antivirus industry, and has recently added antispyware functions to its products. NOD32 is marketed for both the home and corporate markets.

ESET says about the product...

ESET protects consumers and businesses from current and evolving threats. Its award-winning NOD32 Antivirus System offers the smallest, fastest and most advanced real-time protection against viruses, spyware and phishing attacks.

www.eset.com

ESET says about the product's business benefits...

Users of ESET's NOD32 Antivirus System will benefit from fewer malware infections, lower performance impact, easier manageability and lower cost.

The product (continued)

Proactive detection of current and future threats protects the integrity and confidentiality of business critical data also helping companies avoid bad press through breaches and disclosure requirements. It increases the productivity of employees and provides cost savings from acquisition, staff maintenance and cleanup.

The lower performance impact and easier manageability not only increase employee productivity, they also allow companies to deploy IT resources onto other projects providing cost savings.

www.eset.com

ESET says about the product's technical benefits...

ESET's, NOD32 Antivirus System offers the best detection and performance with powerful centralized management.

NOD32 hasn't missed a single, in-the-wild virus in seven years, and has the lowest false positive rate. Its unified anti-threat engine proactively stops current and future threats including variants of MyDoom, Netsky, Bagle, Mytob and Zotob.

NOD32 uses approximately 20MB of memory and has a 19MB/second throughput scanning rate. It has a minimal performance impact of 6% for on-access scanning.

NOD32 is easy to use and allows for sophisticated control, logging and reporting. It usually installs in under a minute (under five minutes on typical networks).

www.eset.com

Test results

1. Functionality & Performance Testing

The tests carried out were as follows:

The West Coast Labs collection of spyware files was scanned.

Using the database 1.1316, NOD32 detected all the files without any difficulty.

Test Engineers performed some simple benchmarking tests for each solution. After the solution was installed, a selection of malware from the West Coast Labs test suite was scanned to see how each solution impacted CPU performance.

Scanning this selection took NOD32 59 seconds. Scanning the full disk took 5 minutes 18 seconds.

2. Using NOD32

Installation of NOD32 always has been a straightforward process and remains so. The only point deserving attention is that, to avoid a clash between two real time scanners, NOD32 does not automatically start its AMON scanner. Instead, it alerts the user to this and requests that they select automatic deployment of AMON after they have ensured that no other real time scanner is running, a very reasonable approach to resolving this problem. NOD32 has one engine, ESET's own, which can scan for both viruses and spyware.

Once installed, this product operates in two almost independent parts, NOD32 and NOD32 Control Center. Both can be opened from the menu, but clicking on the icon will open only NOD32 Control Center. There is a simple division of labour between the two parts; NOD32 is used for running manual scans while NOD32 Control Center is used to supervise the four monitors that run.

NOD32 contains everything you'd expect to find for running and configuring manual scans. Scans can be set to run against all files,

Test results (continued)


including those with no extension, although the default is to run against only a given (but modifiable) list of file extensions. Archives and self-extracting files are not included in default settings. Heuristics are automatically used, with three possible levels of sensitivity, and advanced heuristics can also be included; Adware/Spyware/Riskware is by default included in every scan, but potentially dangerous applications, though they can be included in scans, are not included by default. If malware is found, different responses can be set for malware found in files, in boot sectors and in memory.

Once the settings have been configured to the user's satisfaction, then they can be saved in a profile; each profile can then be allocated for use in various different types of scans, enabling a selective approach to scanning.

NOD32 Control Center controls the four monitors that can run, namely AMON (the file monitor), DMON (the MS Office document monitor), EMON (the MS Outlook email monitor) and IMON (the Internet monitor). (Icons turn red if the relevant monitor is not running, to alert the user to a possible problem.) It also provides a link to open NOD32, and entries for Update, Logs and System Tools. Each of the four monitors can be configured separately, and in contrast to the on-demand scanner, advanced heuristics and scanning of archives and self-extracting files are included in the default settings, although potentially dangerous applications are still excluded. Different settings are used when AMON scans newly-created or modified files.

The Update process updates all signatures together, including viruses and spyware. Updates run automatically but it is also possible to schedule updates for particular frequencies and times. Logging can be enabled or disabled, with output to a file specified by the user, that can be either appended to or overwritten. System Tools include the quarantine information, a scheduler for scans, information and system setup configuration, including the ability to password-protect scan settings.

Test results (continued)



ESET has incorporated detection of spyware into its product with a lack of ostentation. Signatures are incorporated into the main database and there is only one switch in each of the product's scans and monitors to enable or disable scanning for spyware.

NOD32 has been and remains a reliable and easy product to use. It has expanded into spyware with a minimum of fuss. Some default settings may need to be altered to suit the user's requirements but in general it continues to provide the level of service we expect of it.

3. Additional Features

The product was tested as a standalone product so that deployment and remote administration were not tested.

West Coast Labs conclusion

NOD32 has made its name in the antivirus and Trojan markets and has now successfully expanded into the anti-spyware field with minimal alteration.

Automatic use of heuristics in all scans helps proactive detection of future threats, but some other default settings may be unsuitable, mostly in the area of manual scans. In particular, check that AMON has been started. The ability to vary the configuration of settings in different areas and the use of profiles to save various combinations of settings are especially useful.

This notably small program combines ease of use with good results, and is suitable for both home and business users.

Having successfully detected all the spyware samples in the test suite, this product is formally certified for Checkmark Anti-Spyware Desktop, details of which can be found at www.check-mark.com.



West Coast Labs, William Knox House, Britannic Way, Llandarcy,
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.
www.westcoastlabs.org

Security features buyers guide as stated by Eset

PRODUCT

Is the product standalone or corporate? Both

UPDATES

Can the product be updated online? Yes

Are new updates produced daily? Yes

Can automatic updates be scheduled? Yes

Can updates be downloaded and installed manually? Yes

(If corporate) can updates be distributed? Yes

LOGS

Are logs produced? Yes

Can entire logs be printed off? Yes

Can selected entries be printed off? Yes

Can logs be saved in a file? Yes

Can selected/filtered entries be saved in a file? No

Can the format of the file be selected? No

Can the logs be sorted? Yes

Can the user select what information will appear in the log? No

(If corporate) can logs/notifications be sent to a remote user? Yes

Can user notifications be disabled? Yes

Security features buyers guide as stated by Eset

SCANNING

Is there a real-time scanner? Yes

(If corporate) If so, can the user be prevented from disabling it? NA

Can folders/files be selected for scanning? Yes

Can the product scan incoming mail? Yes

Does the product scan incoming mail by default? Yes

Can the product scan memory? Yes

Does the product scan memory by default? Yes

Can the product scan the registry? Yes

Does the product scan the registry by default? Yes

Can removable media be scanned? Yes

Can archives be scanned? Yes

Can scans be scheduled? Yes

Are unscannable files reported? Yes

Can infected incoming files be quarantined? Yes

Can infected incoming files be deleted? Yes

Can installed infections be nullified? Yes

Can users select the appropriate option when the infected file is found?
Yes

Does the product have system restore abilities? No

(If corporate) can scans be centrally controlled? Yes

(If corporate) can scan settings be changed by users? Yes (can be prevented)

ACCESSORIES

Is there a spyware encyclopaedia on the hard disk? No

Security Features Buyers Guide...As Stated by Eset

Is there a spyware encyclopaedia online? Yes

Can samples be submitted to the vendor? Yes

Is the product dependent upon certain service packs being applied? No

(If corporate) Can the product be installed covertly? Yes with Remote Administrator

Security features buyers guide as stated by Eset

ADDITIONAL SECURITY FEATURES

- ThreatSense™ technology - a single optimized anti-threat engine for analyzing code to identify malicious behavior; such as viruses, spyware, adware, phishing and more
- Unprecedented heuristic analysis capable of discovering new malware threats as they emerge, including advanced code analysis
- Single unified engine for detection of all malware types, enhances speed and performance, reducing impact to the user
- Powerful virtual PC emulation technology enables examination of behaviours and improves protection.
- Advanced Predictive Profiling combined with traditional malware signatures
- Protects at multiple infiltration points - including HTTP, POP3, SMTP, and all local and removable media
- Prevents infected files from being opened, executed and warns on creation of infected files
- Excellent management software that allows complete visibility, configuration and management of remote clients on a network
- Can be configured to prevent user disablement
- Automatic execution on system startup
- Supports multiple Terminal Server environments
- Supports scanning of mapped network disks
- Advanced ThreatSense.Net sample submission system allows for automatic suspicious file submission, improving the reaction time.

www.eset.com

Appendix 1 – Checkmark Certifications

ANTI - SPYWARE DESKTOP CERTIFICATION

For a product to be certified to the Spyware Checkmark, the product must be able to detect all Spyware samples in the West Coast Labs test suite. Testing is performed against unpatched Windows workstations. The spyware samples are held on the filesystem but not installed prior to testing.

http://www.westcoastlabs.org/cm-av-list.asp?Cat_ID=8



SPYWARE GATEWAY CERTIFICATION

For a product to be certified to the Spyware Gateway Checkmark, the product must be able to block Spyware drawn from the West Coast Labs test suite from passing through the product. Network traffic tested will include HTTP, SMTP, POP3 and a variety of instant messenger programs.

http://www.westcoastlabs.org/cm-av-list.asp?Cat_ID=11



SPYWARE INSTALLED CERTIFICATION

For a product to be certified to the Installed Spyware Checkmark, it must be able to detect and nullify a range of installed Spyware samples drawn from the West Coast Labs test suite. Testing will be performed against unpatched Windows workstations, each of which will have been preinfected with up to 20 distinct items of different types of malicious spyware.

http://www.westcoastlabs.org/cm-av-list.asp?Cat_ID=12



West Coast Labs, William Knox House, Britannic Way, Llandarcy,
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.
www.westcoastlabs.org

Appendix 2 - Glossary of malware

MALWARE – The word Malware is short for malicious software, which is a program designed specifically to damage or disrupt a computer system or its usage, therefore creating a security risk. The term Malware includes Viruses, Worms, Trojans and Spyware.

VIRUS – A Virus is a program or piece of code attached to a file or diskette's boot sector; it is loaded onto a computer without the user's knowledge. Viruses are manmade (though they can be corrupted in use to form new variants of the virus) and replicate themselves by attaching themselves to files or diskettes, often soaking up memory or hard disk space and bringing networks to a halt. Most recent viruses are internet-borne and capable of transmitting themselves across and bypassing security systems. Minor variants of the same virus are classed as families of viruses.

TROJAN – Trojan Horses or Trojans are destructive programs that pretend to be benign applications. Unlike Viruses or Worms, Trojan Horses do not replicate themselves; they can be damaging to networks by delivering other types of Malware.

WORM – A Worm is an insidious program or algorithm that replicates itself over a computer network or by email system and usually performs malicious actions, such as using up the computer's resources or distributing pornography and possibly shutting the system down. Unlike Viruses, Worms copy themselves as standalone programs and do not attach themselves to other objects.

SPYWARE – Spyware is a form of software that makes use of a user's internet connection without his or her knowledge, usually in order to covertly gather information about the user. Once installed, the Spyware may monitor user activity on the Internet and transmit that information in the background to someone else. Spyware can also gather information about addresses and even passwords and credit card numbers. Spyware is often unwittingly installed when users install another program, but can also be installed when a user simply visits a malicious website.

Appendix 2 - Glossary of malware (continued)

TYPES OF SPYWARE

1. BACKDOOR – A Backdoor is a secret or undocumented way of gaining access to a program, online service, computer or an entire computer network. Most Backdoors are designed to exploit a vulnerability in a system and open it to future access by an attacker. A Backdoor is a potential security risk in that it allows an attacker to gain unauthorised access to a computer and the files stored thereon.

2. KEY LOGGERS – A Key Logger is a type of surveillance software that has the capability to record every keystroke to a log file (usually encrypted). A Key Logger recorder can record instant messages, email and any information typed using the keyboard. The log file created by the Key Logger can then be sent to a specified receiver. Some Key Logger programs will also record any e-mail addresses used and Web Sites visited.

3. FINANCIALS – A Financial is a program that has the capability of scanning a PC or network for information relating to financial transactions and then transmitting the data to a remote user.

4. PROXIES – Proxies are designed to enable an external user to use a computer for their own purposes, for example, to launch DDoS attacks or send spam, so that the true originator of the attack cannot be traced.

5. PASSWORD STEALERS AND CRACKERS – A Password Stealer is a program resident on a computer which is designed to intercept and report to an external person any passwords held on that machine. A Password Cracker has the ability to decode any encrypted passwords.

6. DOWNLOADERS – A downloader is a file which when activated, downloads other files on to the system without the knowledge or consent of the user, those other files then carrying out malicious functions on the system.

Appendix 2 - Glossary of malware (continued)

EXPLOITS – An Exploit is a piece of code designed to attack a vulnerability on a computer system, or such an attack. Hackers and writers of Malware look for announcements of such vulnerabilities by manufacturers and other sources and then attack machines which have not been patched against the vulnerability. The code is designed to enable an activity that otherwise could not take place, or to avoid system restrictions preventing such an activity.

PHISHING – Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information, especially kfinancial information, which may be used for stealing from the user or for identity theft.

0/ZERO DAY MALWARE – A 0/zero day exploit is an exploit which uses vulnerabilities for which no patches are available. Either the vulnerability may not yet be known to the manufacturer, or a patch is not yet available.

0/Zero day malware is any malware for which signatures are not yet available, so that it will not be recognized by an antivirus program

VIRUS/TROJAN/WORM/SPYWARE SIGNATURES – A signature is like a fingerprint in that it can be used to detect and identify specific viruses. Generic signatures are used to detect and identify families of viruses. A signature can also be called a definition.

ZOO VIRUSES – A virus, which at the current time, is not causing a noticeable problem to computer users around the world and is not In the Wild. A zoo virus may have a limited and unimportant effect, or may never achieve release in the general computing world, and may only be found in a virus laboratory and be used for testing by researchers.

There is another category of zoo viruses - those which in the past may have caused a significant problem, but where the threat has now diminished, perhaps because the virus was written for old operating systems, or was contained on old media e.g. old diskettes, backup tapes etc.

Appendix 2 - Glossary of malware (continued)

WILDLIST – The WildList is a list produced each month of computer viruses found in the wild and reported by a diverse group of over 70 qualified volunteers around the world. The purpose of the WildList is to provide accurate, timely and comprehensive information about "In the Wild" computer viruses to both users and product developers. A virus is regarded as being in the wild if in any month it is reported as being seen by the customers of two or more reporters, those reporters being based in two or more countries. www.wildlist.org

ADWARE

Adware is software that brings targeted advertisements to the computer after the user provides initial informed consent. The advertisements may appear in a browser window. Some Adware collects information about the user, for example by tracking browsing habits, which may be reported to a central server. By definition, Adware is therefore not Malware as it does not perform a malicious act.