

# SecurityFocus Microsoft Newsletter #171

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-01/0020.html>

---

**From:** Marc Fossi ([mfossi\\_at\\_securityfocus.com](mailto:mfossi_at_securityfocus.com))

**Date:** 01/13/04

Date: Mon, 12 Jan 2004 18:07:20 -0700 (MST)

To: Focus-MS <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>

SecurityFocus Microsoft Newsletter #171

---

This issue sponsored by: SolSoft

FREE Webinar: Better Management for Network Security

Looking for a better way to manage your IP security? See a live demo to learn how Solsoft can help you:

- Ensure robust IP security through visual, policy-based management
- Make firewall, VPN, and NAT rules interoperable across heterogeneous networks
- Respond rapidly to network events from a central console
- Foster collaboration between network admins and security experts

Register for our FREE webinar at:

[http://www.securityfocus.com/sponsor/Solsoft\\_ms-secnews\\_040112](http://www.securityfocus.com/sponsor/Solsoft_ms-secnews_040112)

---

## I. FRONT AND CENTER

1. Digital Signatures And European Laws
2. IIS Lockdown and Urlscan
3. Locking your door in 2004

## II. MICROSOFT VULNERABILITY SUMMARY

1. Microsoft Internet Explorer Malicious Shortcut Self-Executin...
2. GoodTech Telnet Server Remote Denial Of Service Vulnerabilit...
3. EasyDynamicPages config\_page.php Remote PHP File Include Vul...
4. YaSoft Switch Off Large Packet Remote Denial Of Service Vuln...
5. YaSoft Switch Off swnet.dll Remote Buffer Overflow Vulnerabi...
6. Microsoft Word Form Protection Password Removal Weakness
7. Net2Soft Flash FTP Server Remote Directory Traversal Vulnera...
8. ASPApp PortalAPP Remote User Database Access Vulnerability
9. ASP-Nuke Remote User Database Access Vulnerability
10. Lotus Domino Initialization Files Weak Default Permissions V...
11. Open Text Corporation FirstClass Local File Reference Comman...
12. SnapStream PVS Lite Cross-Site Scripting Vulnerability
13. RealOne Player SMIL File Script Execution Variant Vulnerabil...
14. Kroum Grigorov KpyM Telnet Server Remote Buffer Overflow Vul...

15. Yahoo! Messenger File Transfer Buffer Overrun Variant Vulner...
16. HD Soft Windows FTP Server Username Format String Vulnerabil...

### III. MICROSOFT FOCUS LIST SUMMARY

1. Active Directory Question (Thread)
2. Accessing eventlogs remotely on W2K3 Server (Thread)
3. Article Announcement: IIS Lockdown and Urlscan (Thread)
4. SecurityFocus Microsoft Newsletter #170 (Thread)

### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. AccessMaster
2. KeyGhost SX
3. SafeKit
4. SecurDataStor
5. Proactive Windows Security Explorer
6. Outpost Personal Firewall Pro 2.0

### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. mrtg v2.10.12
2. Big Brother 1.9e
3. Fingerprint Verification System v0.1.0
4. Mod\_security v 1.8dev1
5. Stealth HTTP Security Scanner v2.0b47
6. IDA Pro – Freeware Edition

### VI. UNSUBSCRIBE INSTRUCTIONS

### VII. SPONSOR INFORMATION

#### I. FRONT AND CENTER

---

1. Digital Signatures And European Laws  
By Mirella Mazzeo

This article discusses the security requirements for electronic communications and commerce with European governments and many European-based businesses. It will also give an overview of the current trends for public key infrastructure in Europe, useful for any organization that does business with the EU.

<http://www.securityfocus.com/infocus/1756>

2. IIS Lockdown and Urlscan  
By Nishchal Bhalla and Rohyt Belani

This article discusses two important tools provided by Microsoft, IIS Lockdown and Urlscan, that target significant security-related configuration problems for IIS versions 6.0, 5.0, and earlier.

<http://www.securityfocus.com/infocus/1755>

3. Locking your door in 2004  
By Tim Mullen

Teach your users to think as you do... and other resolutions for the new year.

<http://www.securityfocus.com/columnists/206>

## II. MICROSOFT VULNERABILITY SUMMARY

---

### 1. Microsoft Internet Explorer Malicious Shortcut Self-Executin...

BugTraq ID: 9335

Remote: Yes

Date Published: Jan 02 2004

Relevant URL: <http://www.securityfocus.com/bid/9335>

Summary:

A vulnerability has been reported that may permit remote attackers to execute arbitrary code on client systems running Microsoft Internet Explorer. A reliable source has created a proof-of-concept that causes a malicious self-executing HTML file to install and run an executable on the client system. This issue may be exploited from within a malicious web page.

The malicious self-executing HTML file includes embedded script code that abuses Shell Helper objects to obtain a shortcut file (.lnk), change its parameters, save it to disk and then execute the file pointed to by the shortcut. This will result in execution of arbitrary code.

In the proof-of-concept, a Shell Helper object is created and given the following namespace:

```
"C:\\Documents and Settings\\All Users\\Start Menu\\Programs\\Accessories"
```

The ParseName method will then be called on a shortcut (.lnk) file and the GetLink method is called on the shortcut with the link path pointing to the 'mshta.exe' executable (which is the Windows program used to parse HTML application files). This executable is used to run an external HTA file. A hostile shortcut will then be saved and opened on the client system. This shortcut will point to a malicious executable.

Shell Helper objects and use of the HTML Application interpreter present only one attack vector for exploitation of this issue. There may be other attack vectors, though none have been reported at this time.

This issue is similar to the vulnerability described in BID 8984.

Separate sources have reported conflicting details. One source claims that this issue only works if the self-executing file is run in the context of the Local Zone. The other source implies that this works from a remote site on some Windows platforms but on Windows 2003 it will not work remotely and would likely require another vulnerability to cause the self-executing HTML file to be interpreted in the context of the Local Zone. If the vulnerability does require exploitation of another issue to cause active content to be interpreted in the context of the Local Zone, there is still a slightly lessened security risk associated with this vulnerability. This BID will be updated as further details are made available.

2. GoodTech Telnet Server Remote Denial Of Service Vulnerabilit...

BugTraq ID: 9337

Remote: Yes

Date Published: Jan 02 2004

Relevant URL: <http://www.securityfocus.com/bid/9337>

Summary:

GoodTech Telnet Server is a commercial telnet daemon implementation that is available for Microsoft Windows operating systems.

GoodTech Telnet Server is reportedly prone to a denial of service vulnerability. This condition occurs prior to authentication when excessive data is received by the server. It is possible to reproduce this condition by sending 8245 bytes of data to the server while logging in. This will cause a server crash, requiring a restart for normal functionality to be restored. Exploitation could result in memory corruption, which could in turn be leveraged to execute arbitrary code, though this has not been confirmed by Symantec.

This vulnerability appears similar in nature to BID 862, though the amount of data required to trigger the issue is different. If this issue is indeed the same as BID 862, this BID will be retired and the earlier BID will be updated accordingly.

3. EasyDynamicPages config\_page.php Remote PHP File Include Vul...

BugTraq ID: 9338

Remote: Yes

Date Published: Jan 02 2004

Relevant URL: <http://www.securityfocus.com/bid/9338>

Summary:

EasyDynamicPages is a content management system that is written in PHP. It is available for Unix/Linux derivatives and Microsoft Windows operating systems.

EasyDynamicPages is prone to a remote file include vulnerability. The source of this vulnerability is that the 'config\_page.php' script includes an external file ('admin/site\_settings.php') in such a way that the attacker may influence the include path of the file. If the attacker specifies an include path to a malicious PHP script on an attacker-controlled server, this could result in execution of the malicious script in the context of the web server hosting the vulnerable software.

Exploitation will permit a remote attacker to gain interactive access to the vulnerable system.

4. YaSoft Switch Off Large Packet Remote Denial Of Service Vuln...

BugTraq ID: 9339

Remote: Yes

Date Published: Jan 02 2004

Relevant URL: <http://www.securityfocus.com/bid/9339>

Summary:

Switch Off is a freely available remote PC management suite. It is available for the Microsoft Windows platform.

A vulnerability has been identified in the YaSoft Switch Off software package when handling large packets. This may make it possible for a remote user to deny service to legitimate users of the service.

The problem is in the handling of traffic on the management port. The software launches a service that binds to TCP port 8000, allowing remote users to connect via a web browser. However, when a request of 10240 bytes followed by two Carriage-Return and Line-Feed sequences (CRLF) is sent to the service, the software enters a loop that stops only when the process is terminated. The issue reportedly exists in 'swnet.dll'. A manual restart of the service is required to resume normal functionality.

#### 5. YaSoft Switch Off swnet.dll Remote Buffer Overflow Vulnerabi...

BugTraq ID: 9340

Remote: Yes

Date Published: Jan 02 2004

Relevant URL: <http://www.securityfocus.com/bid/9340>

Summary:

Switch Off is a freely available remote PC management suite. It is available for the Microsoft Windows platform.

A vulnerability has been identified in the YaSoft Switch Off software package when handling message requests. This may make it possible for a remote user to execute arbitrary code through a vulnerable server.

Switch Off has a function for authenticated users that allows the user to send a message. The buffer overrun condition exists in the 'swnet.dll' module of the software due to insufficient bounds checking performed by the affected component. The overflow may be caused by sending an excessively long 'message' parameter to the application. Because of this, it is possible for a user to send a request to the service that overwrites sensitive process memory, and could result in the execution of code with SYSTEM privileges.

#### 6. Microsoft Word Form Protection Password Removal Weakness

BugTraq ID: 9342

Remote: No

Date Published: Jan 02 2004

Relevant URL: <http://www.securityfocus.com/bid/9342>

Summary:

A weakness in the handling of password protection of Microsoft Word documents has been identified. Because of this, the issue may make the defeat of password protection on forms more likely. This could create a false sense of security since the feature is often mistakenly used to protect documents from unauthorized modification.

When a Microsoft Word document has protection for forms turned on, the password for the protection feature is stored in the Word document. When

this document is saved into a HTML document, the password stored in the Word document is placed in hash form in the w:UnprotectPassword header field within the HTML document.

The attacker could circumvent this protection by locating the hash in the saved HTML version of the document and then use a utility such as a hex editor to locate and edit the stored password in the original Word document. Upon modifying the hash contained in the Word document to a string of 0x00000000, resulting in the password for the document being set to a blank string.

It should be noted that the vendor has stated that this feature is not intended to provide document security but instead is implemented to aid in collaborative situations where all parties are trusted. However, this issue still presents a security risk in scenarios where the feature is mistakenly used as a measure to prevent documents from being modified.

#### 7. Net2Soft Flash FTP Server Remote Directory Traversal Vulnera...

BugTraq ID: 9350

Remote: Yes

Date Published: Jan 03 2004

Relevant URL: <http://www.securityfocus.com/bid/9350>

Summary:

Flash FTP Server is a commercially–available FTP server software package for Microsoft Windows. It is distributed and maintained by Net2Soft.

A problem in the handling of directory traversal sequences has been discovered in Net2Soft Flash FTP Server. This may make it possible for an attacker to gain unauthorized access to sensitive information.

The problem is in the handling of slash–dot–dot (/..) sequences. The FTP server does not properly sanitize requests issued with commands. Because of this, an attacker has the ability to potentially execute commands outside of the FTP root directory, including but not limited to file access and file creation.

#### 8. ASPApp PortalAPP Remote User Database Access Vulnerability

BugTraq ID: 9354

Remote: Yes

Date Published: Jan 04 2004

Relevant URL: <http://www.securityfocus.com/bid/9354>

Summary:

PortalApp is a commercially available web application software package for the Microsoft Windows platform.

A problem has been identified in ASPApp PortalApp when user credentials are stored on a system. Because of this, an attacker may be able to gain unauthorized access to sensitive information.

The problem is in the handling of mdb files. User credentials such as usernames and passwords are stored in mdb files inside of the PortalApp

web hierarchy. Insufficient default access control is placed on these database files, making it possible for a remote user to gain unauthorized access to user credentials.

#### 9. ASP–Nuke Remote User Database Access Vulnerability

BugTraq ID: 9355

Remote: Yes

Date Published: Jan 04 2004

Relevant URL: <http://www.securityfocus.com/bid/9355>

Summary:

ASP–Nuke is a freely available web application software package for the Microsoft Windows platform.

A problem has been identified in ASP–Nuke when user credentials are stored on a system. Because of this, an attacker may be able to gain unauthorized access to sensitive information.

The problem is in the handling of mdb files. User credentials such as usernames and passwords are stored in mdb files inside of the ASP–Nuke web hierarchy. Insufficient default access control is placed on these database files, making it possible for a remote user to gain unauthorized access to user credentials.

#### 10. Lotus Domino Initialization Files Weak Default Permissions V...

BugTraq ID: 9366

Remote: No

Date Published: Jan 06 2004

Relevant URL: <http://www.securityfocus.com/bid/9366>

Summary:

Domino is the e–mail server distributed by Lotus. It is available for the Unix, Linux, and Microsoft operating systems.

A vulnerability has been identified in Lotus Domino for the Linux operating system. Due to an issue with installation permissions, it may be possible to modify sensitive configuration files.

The problem is in the default permissions of initialization files. By default, the /local/notesdata/notes.ini and /opt/lotus/LPSilent.ini initialization files are installed with world read–write UNIX file permissions. Because of this, an attacker can modify these files to force Domino to perform potentially dangerous actions.

#### 11. Open Text Corporation FirstClass Local File Reference Comman...

BugTraq ID: 9370

Remote: Yes

Date Published: Jan 06 2004

Relevant URL: <http://www.securityfocus.com/bid/9370>

Summary:

FirstClass is a mail user agent distributed and maintained by the Open Text Corporation. It is available for the Microsoft Windows platform.

A vulnerability has been identified in the handling of URIs that reference local content by Open Text Corporation FirstClass software. An attacker can create a HTML link using one of these URIs (such as file://) that when clicked on by a target user results in the execution of system commands. Commands executed through this means would be carried out with the privileges of the user logged into the system.

This vulnerability can be exploited by sending a malicious e-mail with the hostile link to a victim user.

#### 12. SnapStream PVS Lite Cross-Site Scripting Vulnerability

BugTraq ID: 9375

Remote: Yes

Date Published: Jan 06 2004

Relevant URL: <http://www.securityfocus.com/bid/9375>

Summary:

SnapStream Personal Video Station (PVS) Lite is multimedia software for Microsoft Windows platforms.

SnapStream PVS Lite is prone to a cross-site scripting vulnerability. The vulnerability is due to insufficient input validation of user-supplied input, that will be included in web pages that are generated by the software. In particular, certain variations of embedded HTML tags are not filtered.

An attacker could exploit this issue by enticing a victim user to follow a malicious link to a system hosting the software that contains embedded HTML and script code. The embedded code may be rendered in the web browser of the victim user.

This could be exploited to steal cookie-based authentication credentials from legitimate users. Other attacks are also possible since the attacker can influence how the site will be rendered to the victim user.

#### 13. RealOne Player SMIL File Script Execution Variant Vulnerabil...

BugTraq ID: 9378

Remote: Yes

Date Published: Jan 07 2004

Relevant URL: <http://www.securityfocus.com/bid/9378>

Summary:

RealOne Player is a media player that is available for a number of platforms including Microsoft Windows and MacOS systems.

RealOne Player includes support for Synchronized Multimedia Integration Language (SMIL) presentations.

A vulnerability has been reported in RealOne Player. Script embedded in SMIL presentations may be executed in the context of a domain that is specified by an attacker. In particular, if a URI is opened from within a SMIL file, embedded script code may access the properties of the URI's domain.

This could allow for theft of cookie-based authentication credentials, but more seriously, could also cause embedded script code to be executed in the context of the My Computer Zone. Given the ability to execute script code in the My Computer Zone, it is possible to exploit other security flaws to cause malicious executables to be installed and executed on client systems.

This issue is a variant of the vulnerability described in BID 8453. The syntax used to embed script code is different than the previous vulnerability, and this new issue affects fixed versions of the player. This vulnerability may be exploited with "file:javascript:" syntax, where the previous issue just used a plain "javascript:" URI. Some other limitations are placed on the syntax that may be used in the embedded code, but it has been demonstrated that these restrictions may be bypassed by converting restricted characters to unicode.

As with the previous issue, there is also a likelihood that malicious script code could be embedded into other file types that are handled by the player.

#### 14. Kroum Grigorov KpyM Telnet Server Remote Buffer Overflow Vul...

BugTraq ID: 9379

Remote: Yes

Date Published: Jan 07 2004

Relevant URL: <http://www.securityfocus.com/bid/9379>

Summary:

Kroum Grigorov KpyM (KTS) is a telnet server that runs on Microsoft Windows platforms.

KpyM Telnet Server has been reported to be prone to a remote buffer overflow vulnerability. Because of this, it may be possible for a remote attacker to gain unauthorized access to a system running the vulnerable software. The condition is present due to insufficient boundary checking.

The issue presents itself when an attacker sends request with more than 10000 characters to the server. Immediate consequences of an attack may result in a denial of service condition.

An attacker may leverage the issue by exploiting an unbounded memory copy operation to overwrite the saved return address/base pointer, causing an affected procedure to return to an address of their choice. Successful exploitation of this issue may allow an attacker to execute arbitrary code in the context of the vulnerable software in order to gain unauthorized access, however, this has not been confirmed at the moment.

KpyM versions 1.05 and prior have been reported to be prone to this issue.

#### 15. Yahoo! Messenger File Transfer Buffer Overrun Variant Vulner...

BugTraq ID: 9383

Remote: Yes

Date Published: Jan 08 2004

Relevant URL: <http://www.securityfocus.com/bid/9383>

Summary:

Yahoo! Messenger is the instant message client distributed and maintained by Yahoo!. It is available for the Microsoft Windows operating system.

Yahoo! Messenger is vulnerable to a remotely exploitable buffer overrun issue. This vulnerability is due to insufficient bounds checking during user-initiated file transfer requests.

An attacker may trigger this condition by initiating file transfer using a file name of specific constructs, which the victim user must then accept. The file name must be in excess of 218 bytes. This will reportedly result in an exploitable buffer overflow condition. The condition exists in the ft.dll component, which handles file transfers for the client.

An attacker may theoretically exploit this condition to execute arbitrary code on a client system. Code executed on the target system would be with the privileges of the Yahoo! Messenger client.

16. HD Soft Windows FTP Server Username Format String Vulnerabil...

BugTraq ID: 9385

Remote: Yes

Date Published: Jan 08 2004

Relevant URL: <http://www.securityfocus.com/bid/9385>

Summary:

HD Soft Windows FTP Server is a FTP server application for Microsoft Windows platforms.

Windows FTP Server has been reported to be prone to a remote format string vulnerability when processing a malicious request from a client.

The vulnerability presents itself when the server receives a malicious request containing embedded format string specifiers from a remote client when supplying a username during FTP authentication. The source of the problem is incorrect use of a formatted printing function, which processes data supplied during FTP server authentication. As a result, format specifiers supplied in this manner will be interpreted literally and may result in attacker-specified memory being corrupted or disclosed.

Although it has been demonstrated that this could crash the server, the vulnerability could also theoretically allow for execution of arbitrary code on the system hosting the server. This would occur in the security context of the server process.

Windows FTP Server versions 1.6 and prior are reported to be prone to this issue.

### III. MICROSOFT FOCUS LIST SUMMARY

---

#### 1. Active Directory Question (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/349380>

2. Accessing eventlogs remotely on W2K3 Server (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/349292>

3. Article Announcement: IIS Lockdown and Urlscan (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/349218>

4. SecurityFocus Microsoft Newsletter #170 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/348921>

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. AccessMaster

By: Evidian Inc.

Platforms: IRIX, Solaris, Windows 2000, Windows 95/98, Windows NT

Relevant URL: <http://www.evidian.com/accessmaster/about/index.htm>

Summary:

Extending onto a networked world means embracing the unknown. Piracy, vandalism, industrial espionage... – attacks on companies are doubling each year. With uniquely integrated security software, AccessMaster manages and safeguards access to your data, end-to-end, from portals to legacy, and lets you enforce a single, unified security policy across the enterprise and beyond.

AccessMaster ensures high security level by federating your existing security solutions, while ensuring at the same time user's convenience with Single Sign-On and security officer's ease of administration with centralized, Ldap-compliant, user and PKI management. In this way, AccessMaster reduces IT security cost of ownership, with rapid return on investment.

AccessMaster is recognized by analysts as a leading security suite for large enterprises today. It was awarded "best access control" software by Secure Computing Magazine three years running, in 2000, 2001, and 2002.

2. KeyGhost SX

By: KeyGhost Ltd

Platforms: BeOS, DOS, Linux, OS/2, Solaris, SunOS, Windows 2000, Windows 95/98, Windows NT, Windows XP

Relevant URL: <http://www.keyghost.com/SX/>

Summary:

KeyGhost SX discreetly captures and records all keystrokes typed, including chat conversations, email, word processor, or even activity within an accounting or specialist system. It is completely undetectable by software scanners and provides you with one of the most powerful stealth surveillance applications offered anywhere.

Because KeyGhost uses STRONG 128-Bit encryption to store the recorded data in its own internal memory (not on the hard drive), it is impossible for a network intruder to gain access to any sensitive data stored within the device.

### 3. SafeKit

By: Evidian Inc.

Platforms: AIX, HP-UX, Linux, Solaris, Windows 2000

Relevant URL: <http://www.evidian.com/safekit/index.htm>

Summary:

Evidian's SafeKit technology makes it possible to render any application available 24 hours per day. With no extra hardware: just use your existing servers and install this software-only solution.

This provides ultimate scalability. As your needs grow, all you need to do is add more standard servers into the cluster. With the load balancing features of SafeKit, you can distribute applications over multiple servers. If one system fails completely, the others will continue to serve your users.

### 4. SecurDataStor

By: encryptX Corporation

Platforms: Windows 2000, Windows 95/98, Windows NT, Windows XP

Relevant URL: <http://www.encryptx.com/products/securdatastor.asp>

Summary:

The SecurDataStor product line is designed to provide a comprehensive software security solution that manages and controls access to sensitive information that you need to share internally and externally. SecurDataStor is available in three versions: Basic, Premium, and Platinum. Depending on the level of security that you need, you can choose the SecurDataStor product that suits your needs.

With its end-to-end protection of sensitive business information, SecurDataStor products protect sensitive information when used by the originator, stored locally on a hard drive or file server, and when shared. Users can safely share sensitive information across different Microsoft Windows operating systems, over different network and firewall technologies, and across different forms of removable media.

### 5. Proactive Windows Security Explorer

By: Elcomsoft Co. Ltd.

Platforms: Windows 2000, Windows NT, Windows XP

Relevant URL: <http://www.elcomsoft.com/pwsex.html#>

Summary:

Proactive Windows Security Explorer (PWSEX) is a password security test tool that's designed to allow Windows NT, Windows 2000, and Windows XP-based systems administrators to identify and close security holes in their networks. Proactive Windows Security Explorer helps secure networks by executing an audit of account passwords, and exposing insecure account passwords. If it is possible to recover the password within a reasonable time, the password is considered insecure.

An administrator can also use it to recover any lost password and access a user's Windows account. Proactive Windows Security Explorer works by analyzing user password hashes and recovering plain-text passwords.

6. Outpost Personal Firewall Pro 2.0

By: Agnitum

Platforms: Windows 2000, Windows 95/98, Windows NT, Windows XP

Relevant URL: <http://www.outpost.uk.com>

Summary:

New Outpost Personal Firewall Pro 2.0 outdistances the award-winning Outpost Personal Firewall Pro 1.0 on multiple levels, from enhanced privacy features to ease-of-use. As the foremost security application for personal computers, Outpost Personal Firewall Pro 2.0 gives you the latest in personal firewall technology, making version 2.0 the clear security choice for your system.

## V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

1. mrtg v2.10.12

By: Tobias Oetiker

Relevant URL: <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>

Platforms: POSIX, Windows 2000, Windows NT

Summary:

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing GIF/PNG images which provide a live visual representation of this traffic.

2. Big Brother 1.9e

By: Sean MacGuire, sean@iti.qc.ca

Relevant URL: <http://bb4.com/download.html>

Platforms: AIX, BSDI, DG-UX, Digital UNIX/Alpha, FreeBSD, HP-UX, IRIX, Linux, MacOS, NetBSD, Netware, SCO, SINIX, Solaris, SunOS, True64 UNIX, Ultrix, UNICOS, UNIX, Unixware, Windows NT

Summary:

Big Brother is a combination of monitoring methods. Unlike SNMP where information is just collected and devices polled, Big Brother is designed in such a way that each local system broadcasts its own information to a central location. Simultaneously, Big Brother also polls all networked

systems from a central location. This creates a highly efficient and redundant method for proactive network monitoring.

### 3. Fingerprint Verification System v0.1.0

By: Shivang Patel

Relevant URL: <http://fvs.sourceforge.net/>

Platforms: FreeBSD, Linux, UNIX, Windows 2000, Windows 95/98, Windows NT

Summary:

Fingerprint Verification System is an easy-to-use library that allows programmers to integrate fingerprint technology into their software without specific know-how. It is fast and small, and is great for embedded systems.

### 4. Mod\_security v 1.8dev1

By: Ivan Ristic

Relevant URL: <http://www.modsecurity.org>

Platforms: FreeBSD, Linux, Solaris, Windows 2000, Windows NT, Windows XP

Summary:

ModSecurity is an open source intrusion detection and prevention engine for web applications. It operates embedded into the web server, acting as a powerful umbrella – shielding applications from attacks. ModSecurity supports Apache (both branches) today, with support for Java-based servers coming soon.

### 5. Stealth HTTP Security Scanner v2.0b47

By: qw erty <qw@erty.net >

Relevant URL: [http://www.devhood.com/tools/tool\\_details.aspx?tool\\_id=353](http://www.devhood.com/tools/tool_details.aspx?tool_id=353)

Platforms: Linux, Windows 2000, Windows 95/98, Windows NT

Summary:

Stealth 1.0 scans for 2883 HTTP vulnerabilities. This tool is designed especially for the system administrators, security consultants and IT professionals to check the possible security holes and to confirm any present security vulnerabilities that hackers can exploit. Totally free for commercial and non-commercial use.

### 6. IDA Pro – Freeware Edition

By: DataRescue Inc.

Relevant URL: <http://www.datarescue.com/idabase>

Platforms: DOS, Windows 2000, Windows 95/98, Windows NT

Summary:

The freeware version of the Interactive Disassembler Pro. Supports 80x86 binaries and FLIRT, a unique Fast Library Identification and Recognition Technology that automagically recognizes standard compiler library calls. Widely used in COTS validation and hostile code analysis.

## VI. UNSUBSCRIBE INSTRUCTIONS

---

To unsubscribe send an e-mail message to [ms-secnews-unsubscribe@securityfocus.com](mailto:ms-secnews-unsubscribe@securityfocus.com) from the subscribed address. The contents of the subject or message body do not matter. You will receive a confirmation request message to which you will have to answer. Alternatively you can also visit <http://www.securityfocus.com/newsletters> and unsubscribe via the website.

If your email address has changed email [listadmin@securityfocus.com](mailto:listadmin@securityfocus.com) and ask to be manually removed.

## VII. SPONSOR INFORMATION

---

This issue sponsored by: SolSoft

FREE Webinar: Better Management for Network Security

Looking for a better way to manage your IP security? See a live demo to learn how Solsoft can help you:

- Ensure robust IP security through visual, policy-based management
- Make firewall, VPN, and NAT rules interoperable across heterogeneous networks
- Respond rapidly to network events from a central console
- Foster collaboration between network admins and security experts

Register for our FREE webinar at:

[http://www.securityfocus.com/sponsor/Solsoft\\_ms-secnews\\_040112](http://www.securityfocus.com/sponsor/Solsoft_ms-secnews_040112)

---

---

---