

SecurityFocus Microsoft Newsletter #124

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-02/0039.html>

From: Marc Fossi (mfossi@securityfocus.com)

Date: 02/10/03

Date: Mon, 10 Feb 2003 12:15:17 -0700 (MST)

From: Marc Fossi <mfossi@securityfocus.com>

To: Focus-MS <focus-ms@securityfocus.com>

SecurityFocus Microsoft Newsletter #124

This Issue is Sponsored by: NetIQ

Security Webcast Featuring Kevin Mitnick Do you need cost-effective methods to create and implement information security policies to gain control of your enterprises? Join former hacker turned consultant Kevin Mitnick for NetIQ's free webcast—"People & Policies: Turning Your Weakest Security Link into a First Line of Defense."

Register now at:

<http://www.netiq.com/f/form/form.asp?id=1696&origin=NSecFocusMSFTNL021103>

I. FRONT AND CENTER

1. The Great IDS Debate : Signature Analysis Versus Protocol Analysis
2. Smallpot: Tracking the Slapper and Scalper Unix Worms
3. Lessons From the Slammer
4. Something Needs to Change
5. SecurityFocus DPP Program
6. InfoSec World Conference and Expo/2003(March10-12,2003,Orlando,FL)

II. MICROSOFT VULNERABILITY SUMMARY

1. Macromedia ColdFusion MX Windows User File Authorization...
2. WinSCP SSH2 Authentication Password Persistence Weakness
3. Bladeenc Signed Integer Memory Corruption Vulnerability
4. Microsoft Internet Explorer dragDrop Method Local File Reading...
5. PHP-Nuke Avatar HTML Injection Vulnerability
6. Opera JavaScript Console Attribute Injection Vulnerability
9. Majordomo Default Configuration Remote List Subscriber...
10. Microsoft Windows 2000 NetBIOS Continuation Packets Kernel...
11. Microsoft Windows 2000 RPC Service Privilege Escalation...
12. KaZaA Advertisement Response Denial of Service Vulnerability
14. Opera Cross Domain Scripting Vulnerability
15. Opera Image Rendering HTML Injection Vulnerability
16. ByteCatcher FTP Client Long Server Banner Buffer Overflow...

III. MICROSOFT FOCUS LIST SUMMARY

1. L0phtCrack and Windows 2000 LM Hashes (Thread)
2. Customising user rights on win2k Pro (Thread)
3. Unknown Windows Process (Thread)
4. Unknown Windows 2000 files? (Thread)
5. Secure Ldap call not working due to IUSR/IWAM permissions?...
6. Dynamic Entries in IP Routing Table (Thread)
7. SecurityFocus Microsoft Newsletter #123 (Thread)
8. IIS Security using Integrated Windows Authentication (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. SAM
2. SoftClan e-cryptor
3. CryptoForge

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. proDETECT v0.1b
2. WaveLock v1.0
3. NtDump v1

VI. SPONSOR INFORMATION

I. FRONT AND CENTER

1. The Great IDS Debate : Signature Analysis Versus Protocol Analysis by Matt Tanase

Intrusion detection systems (IDS) have rapidly become a crucial component of any network defense strategy. Over the past few years, their popularity has soared as vendors have refined their results and increased performance capabilities. At the heart of intrusion detection systems lies the analysis engine. It reviews each packet, determines if it is malicious, and logs an alert if necessary – the core tasks of an IDS. Two different IDS techniques, each favored by separate and loyal camps, have emerged as the preferred engine behind the software. Despite the copious marketing material and fiery online debates, each method has distinct strengths and weaknesses. In this article, we'll examine and compare the two different techniques: signature analysis and protocol analysis.

<http://online.securityfocus.com/infocus/1663>

2. Smallpot: Tracking the Slapper and Scalper Unix Worms by Costin Raiu

Fueled by the old myth that "you can't get a virus in Unix" and by the increasing popularity of Linux and FreeBSD, Unix viruses passed an important milestone in 2001 and continued by receiving even more attention during 2002.

<http://online.securityfocus.com/infocus/1662>

3. Lessons From the Slammer By Richard Forno

January's Slammer infection held valuable lessons for all security stakeholders.

<http://online.securityfocus.com/columnists/140>

4. Something Needs to Change By Tim Mullen

That's all there was to "Slammer," 376 bytes. When you think about it, it's amazing that a piece of code could have wreaked such havoc on the Internet and caused such widespread system failure — at about the size of two paragraphs of this column.

<http://online.securityfocus.com/columnists/139>

5. SecurityFocus DPP Program

Attention Universities!! Sign-up now for preferred pricing on the only global early-warning system for cyber attacks – SecurityFocus DeepSight Threat Management System.

Click here for more information:

<http://www.securityfocus.com/corporate/products/dpsection.shtml>

6. InfoSec World Conference and Expo/2003 (March 10–12, 2003, Orlando, FL)

Optional Workshops March 8, 9, 12, 13, & 14 Vendor Expo March 10 & 11

Solutions to today's security concerns; hands-on experts; blockbuster vendor expo; the CISO Executive Summit; invaluable networking opportunities. InfoSec World has it all!

Go to: <http://www.misti.com/10/os03n137inf.html>

II. BUGTRAQ SUMMARY

1. Macromedia ColdFusion MX Windows User File Authorization Vulnerability

BugTraq ID: 6737

Remote: Yes

Date Published: Jan 30 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6737>

Summary:

ColdFusion MX Enterprise Edition is the application server for developing and hosting infrastructure distributed by Macromedia. It is available as a standalone product for Unix, Linux, and Microsoft Operating Systems.

When ColdFusion MX is used in conjunction with Microsoft IIS, Windows NT authentication, and NTFS file permissions, it may be possible for a user to access files and templates they do not have permission to access.

This is due to a configuration error. IIS is not configured by default to determine if files associated with ColdFusion MX are accessible or not by the authenticated user. Consequently, user supplied file names are passed directly to ColdFusion MX which apparently does not check NTFS permissions against the user itself.

2. WinSCP SSH2 Authentication Password Persistence Weakness

BugTraq ID: 6732

Remote: No

Date Published: Jan 30 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6732>

Summary:

WinSCP is a freely available secure file transfer client for Microsoft Windows operating systems.

A problem with WinSCP may allow the recovery of sensitive information.

It has been reported that WinSCP does not safely handle password information. As a result, a local user may be able to recover authentication passwords.

The problem is in the handling of authentication passwords after authentication has been negotiated. Correct behavior of such applications is to remove passwords from memory immediately after authentication has occurred. However, WinSCP retains password information in memory, which may result in recovery by another user with sufficient privileges. In addition to being present in process memory space, this information may also be retrieved from memory dumps of processes.

3. Bladeenc Signed Integer Memory Corruption Vulnerability

BugTraq ID: 6745

Remote: No

Date Published: Feb 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6745>

Summary:

Bladeenc is an open-source MP3 encoder and is available for a variety of platforms including Microsoft Windows and Linux and Unix variant operating systems.

A memory corruption vulnerability has been reported for Bladeenc. Bladeenc encodes WAV files in 'chunks' of data. The vulnerability exists when Bladeenc is seeking a WAV file chunk. Specifically, in the function `__myfseek()` in the `samplein.c` source file, an integer value is not properly verified. When this function is given a negative value, it will result in the corruption of sensitive areas of memory with attacker-supplied values.

An attacker can exploit this vulnerability by creating a malicious WAV file with carefully crafted headers that will cause Bladeenc to execute malicious attacker-supplied code.

This vulnerability was reported for Bladeenc 0.94.2 and earlier.

4. Microsoft Internet Explorer dragDrop Method Local File Reading Vulnerability

BugTraq ID: 6749

Remote: Yes

Date Published: Feb 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6749>

Summary:

Microsoft Internet Explorer 5.5 and higher contain the ActiveX method dragDrop() that allows HTML elements to be dragged and dropped on a web page.

The dragDrop() method can be used by a maliciously crafted web page to read local files from an Internet Explorer user's local drive.

If a web page is constructed containing a script element utilizing the dragDrop() method and properly obfuscated, users can be tricked into uploading a local file to the malicious webserver.

This can typically be achieved by constructing a Javascript element appearing to be a hyperlink that actually contains elements to drop text, such as a file name, into an HTML upload control using the dragDrop() method. The local file name must be known in order for the attack to succeed, however, relative paths may be used. The user must also perform another action, such as clicking on a button, in order to trigger the file upload.

5. PHP-Nuke Avatar HTML Injection Vulnerability

BugTraq ID: 6750

Remote: Yes

Date Published: Feb 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6750>

Summary:

PHP-Nuke is a web-based portal system. Implemented in PHP, it is available for a range of systems, including Unix, Linux, and Microsoft Windows.

A vulnerability has been reported in PHP-Nuke that may result in HTML injection. The vulnerability occurs because PHP-Nuke does not sanitize some user-supplied input submitted to a site when selecting 'avatar' images. Due to this condition, a malicious user may be able to insert malicious HTML code which will then be displayed to unsuspecting users of PHP-Nuke forums. Any attacker-supplied code will be interpreted in a victim user's web browser in the security context of the site hosting the

software.

It may be possible to steal the unsuspecting user's cookie-based authentication credentials, as well as other sensitive information. It is also possible to modify or corrupt other user's Avatars. Other attacks are also possible.

This vulnerability was reported for PHP-Nuke 6.0 and earlier.

6. Opera JavaScript Console Attribute Injection Vulnerability

BugTraq ID: 6755

Remote: Yes

Date Published: Feb 04 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6755>

Summary:

Opera is a web client available for a number of platforms, including Microsoft Windows, Linux and Unix variants and Apple MacOS.

A vulnerability has been reported for Opera 7 browsers for Microsoft Windows operating systems. The vulnerability exists in Opera's JavaScript console program. The console program consists of three HTML files, one of which is 'console.html'. Any unhandled exceptions thrown by any JavaScript are listed in the console and are converted into clickable links.

The vulnerability exists in the regular expressions used by 'console.html' to format exception messages. Specifically, exception messages are not parsed for quote characters. It is possible, by inserting quote (") characters, to add additional attributes to URLs that may make it possible to execute arbitrary attacker-supplied script code in the file:// protocol context. This may lead to disclosure of local file contents to remote attackers.

This vulnerability was reported for Opera 7 browser for Microsoft Windows.

7. IBM WebSphere Exported XML Password Encoding Weakness

BugTraq ID: 6758

Remote: No

Date Published: Feb 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6758>

Summary:

IBM WebSphere is a commercial web application server which runs on a number of platforms including Linux and Unix variants and Microsoft Windows operating environments.

IBM WebSphere allows administrators to export configuration files to XML. When the WebSphere configuration file is exported in this manner, passwords are obfuscated using an easily reversible algorithm.

The algorithm used to obfuscate the password is as follows:

$$\text{CHARobfuscated}(n) = \text{CHARpassword}(n) \text{ XOR } \text{CHAR}(_ _)$$

where n is the position of the character.

The obfuscated password is then Base64 encoded.

If an attacker gains access to an exported XML configuration file, it is a trivial task to decode the password.

To exploit this weakness, an administrator must first export the configuration to XML and then the attacker may gain unauthorized access to the exported file.

The WebSphere documentation states that exported configurations will contain encoded (and not encrypted) passwords. Administrators should be cautious when exporting configuration files.

This issue was reported in IBM WebSphere Advanced Server Edition 4.0.4. It is not known if the same encoding is used in other versions. Though the core weakness is that passwords are encoded and may be easier to reverse than if encrypted using a strong algorithm, so all current versions should be considered prone to this weakness to some degree.

8. Opera Error Message History Disclosure Weakness

BugTraq ID: 6759

Remote: Yes

Date Published: Feb 04 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6759>

Summary:

Opera is a web client available for a number of platforms, including Microsoft Windows, Linux, Unix variants and Apple MacOS.

The Opera console is used to keep a track of any JavaScript error messages that may have occurred when browsing a Web site.

It has been reported that Opera fails to ensure that a remote site has proper authorization before executing some methods used to access error messages stored in the Opera console. Specifically, Opera does not validate any requests for the `opera.errorIndex()` and `opera.errorMessage(i)` methods.

This issue is further exacerbated by the fact that error messages also contain the URL of the site that caused the issue. This can be exploited by a malicious attacker to obtain a listing of the victim user's Web browsing habits for, potentially, malicious purposes.

This vulnerability was reported for Opera 7 browser for Microsoft Windows.

9. Majordomo Default Configuration Remote List Subscriber Disclosure Vulnerability

BugTraq ID: 6761

Remote: Yes

Date Published: Feb 04 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6761>

Summary:

Majordomo is a freely available, open source mailing list management software package. It is available for Unix, Linux, and Microsoft Windows platforms.

A problem with Majordomo may allow remote users to gain access to sensitive information.

It has been reported that Majordomo does not sufficiently guard list subscriber information. By sending specific commands to a default implementation, a remote user may be able to gain access to the list of mailing list subscribers. This issue is documented in the Majordomo documentation.

The problem is in the default configuration of the mailing list manager. The software does not place sufficient access controls on the ability of users to execute the which command. By sending the command "which @", remote users may be able to list the entire member base of the list, resulting in a loss of privacy.

It should be noted that in the Majordomo 2 branch, this vulnerability is limited to gaining access to one address per submission per list.

10. Microsoft Windows 2000 NetBIOS Continuation Packets Kernel Memory Leak Vulnerability

BugTraq ID: 6766

Remote: Yes

Date Published: Feb 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6766>

Summary:

Microsoft Windows 2000 is reported to be prone to a denial of service when handling NetBIOS continuation packets.

NetBIOS continuation packets are normally generated when a SMB message is split across a number of packets. Under some circumstances, when these packets are handled by the server, a kernel memory leak will occur.

This may result in a failure to service SMB requests, which will cause a denial of service.

11. Microsoft Windows 2000 RPC Service Privilege Escalation Vulnerability

BugTraq ID: 6769

Remote: No

Date Published: Feb 04 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6769>

Summary:

Microsoft Windows 2000 uses Remote Procedure Calls (RPC) for client-server communications in a distributed computing environment (DCE). TCP Port 135 is typically used for DCE endpoint resolution.

A vulnerability was previously reported which causes a denial of service against the DCE-RPC endpoint mapper (BID 6005). If a system service crashes as a result of this denial of service, there is a possibility that it will orphan a named pipe.

This named pipe could then be hijacked by a malicious user in order to escalate their privilege level on the system when a privileged process attempts to connect to the orphaned pipe. This could result in a complete system level compromise.

12. KaZaA Advertisement Response Denial of Service Vulnerability

BugTraq ID: 6747

Remote: Yes

Date Published: Feb 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6747>

Summary:

KaZaA Media Desktop is a peer to peer file sharing utility. KaZaA is available for the Microsoft Windows operating system.

When KaZaA clients make a connection to a file sharing server, a request is made for an advertisement (*ad*) download. A vulnerability has been discovered in KaZaA clients when receiving unexpected responses to *ad* requests. When the susceptible KaZaA client attempts to process the response, the client will crash. This condition likely occurs due to client assuming various attributes of the response. Computing values assumed to exist in a response, which may not be in an expected format, may cause the client to behave in an unpredictable manner.

This issue could be exploited by an attacker to cause a denial of service against KaZaA clients. The denial of service may also be triggered by a filter configured to reject various web requests.

Although not yet confirmed, it has been reported that this issue may be exploited to execute arbitrary instructions within the context of the target client process.

13. Opera History Object Information Disclosure Weakness

BugTraq ID: 6757

Remote: Yes

Date Published: Feb 04 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6757>

Summary:

Opera is a web client available for a number of platforms, including Microsoft Windows, Linux and Unix variants and Apple MacOS.

An information disclosure weakness has been reported for Opera 7 browsers on the Microsoft Windows platform.

The weakness is due to the way the history object exposes some properties. Specifically, the properties history.next and history.previous are exposed.

A vulnerable user, when navigating to a malicious website, may have some information pertaining to browser history logged by the site. This information can be used by Web masters for, potentially, malicious purposes.

This vulnerability was reported for Opera 7 browser for Microsoft Windows.

14. Opera Cross Domain Scripting Vulnerability

BugTraq ID: 6754

Remote: Yes

Date Published: Feb 04 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6754>

Summary:

Opera is a web client available for a number of platforms, including Microsoft Windows, Linux and Unix variants and Apple MacOS.

A vulnerability has been reported reported for Opera 7 browsers for Microsoft Windows operating systems.

Due to flaws in Opera, it is possible for functions in different domains to be accessed and executed by an attacker with the credentials of the victim user. This vulnerability is also exacerbated by the fact that an attacker may also be able to override properties and methods in other windows to create malicious methods that can be accessed by a victim user.

Exploitation of this vulnerability will allow an attacker to obtain access to local resources on a vulnerable system.

This issue may be similar to the ones described in BID 6184.

These vulnerabilities were reported for Opera 7 browser for Microsoft Windows.

15. Opera Image Rendering HTML Injection Vulnerability

BugTraq ID: 6756

Remote: Yes

Date Published: Feb 04 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6756>

Summary:

Opera is a web client available for a number of platforms, including Microsoft Windows, Linux, Unix variants and Apple MacOS.

Problems with Opera could make it possible to execute arbitrary HTML code in a vulnerable client.

It has been reported that, when generating HTML to display images or embedded media, Opera does not correctly format the provided URL or sufficiently encode local URLs. Specifically, URLs that use the 'file://' protocol to access local files are not sufficiently sanitized of malicious HTML code.

This vulnerability could allow an attacker to inject malicious HTML code to an unsuspecting user of Opera, through a malformed link. Any code will be executed in the security context of the local Opera User.

Successful exploitation of this vulnerability may result in the disclosure of local file contents to remote attackers. Other attacks are possible.

This vulnerability was reported for Opera 7 browser for Microsoft Windows.

16. ByteCatcher FTP Client Long Server Banner Buffer Overflow Vulnerability

BugTraq ID: 6762

Remote: Yes

Date Published: Feb 04 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6762>

Summary:

Save-It Softwares ByteCatcher is an FTP client for Microsoft Windows that lets you resume downloads.

It has been reported that a memory corruption bug exists in ByteCatcher FTP client. Under some circumstances, when the client connects to a malicious FTP server, it may be possible for the server to trigger a boundary condition error.

This issue is due to insufficient bounds check of FTP banners. When the FTP client receives an FTP banner that contains an excessive amount of data it becomes unstable. It has been reported that this vulnerability can be reproduced by sending an FTP banner of 4096 bytes or more to a vulnerable client, which may cause sensitive regions of memory to be corrupted with attacker-supplied values.

It is possible that this vulnerability is an exploitable buffer overflow, and could result in the execution of attacker-supplied code. Any code executed would be in the security context of the FTP client process.

III. MICROSOFT FOCUS LIST SUMMARY

1. L0phtCrack and Windows 2000 LM Hashes (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/310916>

2. Customising user rights on win2k Pro (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/310826>

3. Unknown Windows Process (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/310818>

4. Unknown Windows 2000 files? (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/310741>

5. Secure Ldap call not working due to IUSR/IWAM permissions? (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/310763>

6. Dynamic Entries in IP Routing Table (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/310213>

7. SecurityFocus Microsoft Newsletter #123 (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/310002>

8. IIS Security using Integrated Windows Authentication (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/310013>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. SAM

by SYSTOR Security Solutions GmbH

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

Relevant uRL:

http://www.systor.com/en/index/core/core_sam_home/core_sam_prod_home.htm

Summary:

With the SAM product line, Systor offers integrative and integrated software for quick and comprehensive control of enterprise-wide security management. SAM products set worldwide standards in the fields of role-based access control, access rights management, and security workflow. With the integration of password synchronisation, single sign-on and network security, Systor covers all relevant areas for optimally protecting business processes.

2. SoftClan e-cryptor

by CenturionSoft

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

Relevant URL:

<http://www.centurionsoft.com/SoftClan/ecryptor.htm>

Summary:

SoftClan e-cryptor is unique in that it offers both powerful AES encryption as well as ease-of-use. Encrypted files are self-decrypting. Your encrypted email recipients need nothing to decrypt the file except the password. E-cryptor is also perfect for encrypting files and folders because you never have to worry about having the software installed to decrypt them. This is particularly helpful if you want to encrypt files; including backup files – on removable media. You can decrypt them on any system, even a system that doesn't have e-cryptor installed.

3. CryptoForge

by Ranquel Technologies

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

Relevant URL:

<http://www.cryptoforge.com/>

Summary:

CryptoForge is the suite of encryption tools for professional and personal security. It allows you to protect the privacy of your sensitive files and messages by encrypting them with up to four strong cryptographic algorithms. Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network –like the Internet– and still remain secret. Later, the information can be decrypted into its original form. CryptoForge integrates the strongest cryptography available today into the Windows environment...

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. proDETECT v0.1b

by Egemen Tas egemen@ipipi.com or egemen@usaf.org

Relevant URL:

<http://www.cmpe.boun.edu.tr/~tas/>

Platforms: Windows 2000, Windows NT, Windows XP

Summary:

proDETECT is an open source promiscuous mode scanner with a GUI. It uses ARP packet analyzing technique to detect adapters in promiscuous mode. This tool can be used by security administrators to detect sniffers in a LAN. It can be scheduled for regular scanning over periods. It also has some advanced reporting capabilities such as SMTP reporting. Full source code is included.

2. WaveLock v1.0

by SecureWave <http://www.securewave.com>

Relevant URL:

http://www.securewave.com/products/free_utilities/wavelock.html

Platforms: Windows 2000, Windows NT, Windows XP

Summary:

Windows 2000 and Windows XP come with drivers for several wireless LAN ("WLAN") adapters; installation requires only insertion of one of those adapters. Administrative privileges are not required, as no new drivers must be registered with the operating system. WaveLock assists in enforcing security policies by blocking access to these adapters, making it harder to circumvent firewalls, filters, proxies, and other required safeguards.

To install WaveLock, download and uncompress wavelock.zip. Execute the resulting wavelock.msi file (a Windows Installer setup), which installs wavelock.sys. Reboot to load and activate WaveLock.

A list of the wireless network adapters supported out-of-the-box on Windows 2000 and Windows XP can be found below. Note that WaveLock cannot know about and will therefore not block additional drivers installed by administrators.

3. NtDump v1

by Ben Maurer bmaurer@users.sf.net

Relevant URL:

<http://ntdump.sourceforge.net/>

Platforms: Windows 2000, Windows NT

Summary:

NtDump allows the dumping of password hashes and LSA secrets on Windows NT computers. NtDump is small as so to reduce network traffic. It is also able to run in a batch-mode in which it can dump from multiple computers with maximum performance.

VI. SPONSOR INFORMATION

This Issue is Sponsored by: NetIQ

Security Webcast Featuring Kevin Mitnick Do you need cost-effective methods to create and implement information security policies to gain

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #124

control of your enterprises? Join former hacker turned consultant Kevin Mitnick for NetIQ's free webcast—"People & Policies: Turning Your Weakest Security Link into a First Line of Defense."

Register now at:

<http://www.netiq.com/f/form/form.asp?id=1696&origin=NSecFocusMSFTNL021103>
