

SecurityFocus Microsoft Newsletter #73

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-02/0067.html>

From: Marc Fossi (mfossi@securityfocus.com)

Date: 02/11/02

Date: Mon, 11 Feb 2002 12:39:32 -0700 (MST)
From: Marc Fossi <mfossi@securityfocus.com>
To: Focus-MS <focus-ms@securityfocus.com>

SecurityFocus Microsoft Newsletter #73

This Issue is Sponsored By: GFI Ltd.

Intrusion detection through NT/2000 security logs: LANguard

Catch hackers red-handed with GFI's LANguard S.E.L.M.! Performs intrusion detection through network-wide monitoring of the security event logs of all NT/2000 servers & workstations. Enables you to respond quickly to important security events, without spending hours examining logs. Notifies you of critical security events in real time & more besides! Get your FREE evaluation from:

<http://www.gfi.com/securityfocus/>

I. FRONT AND CENTER

1. SecurityFocus is Hiring!
2. Event Announcement
3. The Devil You Know: Responding to Interface-based Insider Attacks
4. Heuristic Techniques in AV Solutions: An Overview

II. MICROSOFT VULNERABILITY SUMMARY

1. NetScreen ScreenOS Port Scan DoS Vulnerability
2. Oracle TNS Listener Arbitrary Library Call Execution Vulnerability
3. Internet Security Systems BlackICE and RealSecure DoS...
4. MIRC Nick Buffer Overflow Vulnerability
5. Microsoft MSN ActiveX Object Information Disclosure Vulnerability
6. Castelle Faxpress Plaintext Password Disclosure Vulnerability
7. Microsoft Site Server LDAP Plain Text Password Storage...
8. Microsoft MSDTC Service Denial of Service Vulnerability
9. MS Site Server Unauthorized SQL Command Injection Vulnerability

III. MICROSOFT FOCUS LIST SUMMARY

1. Secure Transactions over HTTPS???? (Thread)
2. Where would the changes be saved? (Thread)

3. Question regarding attack (Thread)
4. SYSTEM grabbing ports? (Thread)
5. Allowing users to change their password via the web (Thread)
6. Possible hack – Portable profile found in a Windows 2K Pro...
7. Local security policy Settings (Thread)
8. IM encryption (Thread)
9. TCP/IP Filtering problem on W2KAS (Thread)
10. Possible hack – Portable profile found in a Windows 2K Pro SP...
11. Windows 2000/.Net Group Policy Locker (Thread)
12. TCP/IP Filtering problem on (Thread)
13. SecurityFocus Microsoft Newsletter #72 (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Aventail ExtraNet Center
2. Luna XL
3. Cryptix EasyCrypt

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. NGSecureWeb v1.00
2. Typhon I
3. Securepoint Firewall and VPN Server SB v2.0.6.1
4. CIA Unerase Private v1.0

VI. SPONSORSHIP INFORMATION

I. FRONT AND CENTER

1. SecurityFocus is Hiring!

SecurityFocus is currently looking for a programmer/debugger for its Threat Analysis teams. This position requires skillsets which I have outlined below.

These positions require the staff members to be located in Calgary, Alberta, Canada. Relocation assistance is possible from within Canada. Skills will require verification by the way of an actual practical test before an in-person interview is secured.

Skills required:

- Expertise with SoftICE & IDA Pro (or similar tools).
- Expertise with x86 assembly language
- Programming ability in C & C++, targeting both the Unix and Windows platforms
- Strong report writing skills and ability to interface with customers.

Additional skills preferred:

- Working knowledge of computer viruses, worms, and trojans propagation techniques
- Working knowledge of honeypots.

Personal Skills Required:

Any applicant must be able to work in a team environment and deal with very tight deliverables. An outgoing pleasant personality is an absolute requirement. No rockstars, no primadonas.

About SecurityFocus

SecurityFocus, is the leading provider of security intelligence products and services for business. They include SIA (Security Intelligence Alert), which alerts subscribers to security vulnerabilities, and ARIS (Attack Registry & Intelligence Service), which predicts cyber assaults on customer networks, based on global attack data. SecurityFocus also licenses the world's largest and most comprehensive vulnerability information database, hosts the most popular security community mailing list on the Internet, Bugtraq, and publishes original security content on its Web site.

Please send resumes if interested to Alfred Huger ah@securityfocus.com

2. Event Announcement

THE PRACTITIONERS' FORUM ON MOBILE & WIRELESS SECURITY April 29 – 30, 2002, The American Management Training Association, Washington DC

Walk away with defensive tactics to protect your wireless networks – today!

Join wireless security leaders to discuss:

- * Various types of wireless attacks – and defense strategies for each
- * The pros and cons of WLAN security technologies: WAP, WEP, 802.11x, dynamic WEP, VPN's, bluetooth, 3G, dynamic IPsec, and PKI
- * Wireless security strategies: What the CIO should know
- * Corroborating with law enforcement after an attack occurs
- * Case studies presented by leading wireless security practitioners

Plus: A comprehensive post-conference workshop: "A How-To Guide to Implementing Wireless LAN Security Solutions" For more information please visit: <http://www.frallc.com>

3. The Devil You Know: Responding to Interface-based Insider Attacks by Ronald L. Mendell

It is estimated that up to eighty-five percent of intrusions are perpetrated by insiders. This article will examine how response teams can detect and investigate interface-based insider attacks. It is also hoped that the article will provide the basis of incident response policies for responding to and investigating insider attacks that exploit interface-based vulnerabilities.

<http://www.securityfocus.com/infocus/1543>

4. Heuristic Techniques in AV Solutions: An Overview
by Markus Schmall

Heuristic technologies can be found in nearly all current anti-virus (herein referred to as AV) solutions and also in other security-related areas like intrusion detection systems and attack analysis systems with correlating components. This article will offer a brief overview of generic heuristic approaches within AV solutions with a particular emphasis on heuristics for Visual Basic for Applications-based malware.

<http://www.securityfocus.com/infocus/1542>

II. BUGTRAQ SUMMARY

1. NetScreen ScreenOS Port Scan DoS Vulnerability

BugTraq ID: 4015

Remote: No

Date Published: Feb 01 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4015>

Summary:

NetScreen is a line of internet security appliances inetgrating firewall, VPN and traffic management features. ScreenOS is the software used to manage and configure the firewall. NeScreen supports Microsoft Windows 95, 98, ME, NT and 2000 clients.

An issue has been reported in NetScreen ScreenOS which could cause the system to stop responding.

If a user within the trusted network attempts to do a port scan on an external system, ScreenOS could fail requiring a restart. This is due to the number of concurrent sessions allowed per user. It is possible to exploit this issue with a port scanner that does not properly release sessions.

A restart of the service may be required in order to gain normal functionality.

2. Oracle TNS Listener Arbitrary Library Call Execution Vulnerability

BugTraq ID: 4033

Remote: Yes

Date Published: Feb 06 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4033>

Summary:

Oracle is a commercial relational database product. Oracle is available for the Unix, Linux, and Microsoft Windows platforms.

Oracle supports the PL/SQL programming language, used in part to create stored procedures and embed complicated operations within the database. PL/SQL includes the functionality to call arbitrary external functions through libraries or DLLs. PL/SQL accomplishes this through the Oracle Listener process.

When asked to make an external call, the PL/SQL function connects to the listener and causes a new process to be created. The Library call is then executed in this process, and results are communicated through named pipes.

As there is no authentication between the PL/SQL process and the Listener, it is possible for a malicious third party to emulate the conversation. Thus, any party able to connect to the Listener is able to request the execution of any library call. This may result in a system() call, and the execution of arbitrary shell commands.

Additionally, it is possible to force the process communication to occur through sockets instead of named pipes. This easily opens the potential for a full remote compromise of the Listener user.

Any code that an attacker executes would run with the privilege level of the listener. On Windows based systems, the library call is run within the local SYSTEM security context. On Unix systems, the Listener may run with user-level privileges.

3. Internet Security Systems BlackICE and RealSecure DoS Vulnerability BugTraq ID: 4025

Remote: Yes

Date Published: Feb 04 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4025>

Summary:

Internet Security Systems's BlackICE Defender, BlackICE Agent and RealSecure Server Sensor, are network intrusion detection systems which run in Microsoft Windows environments.

A denial of service condition has been reported in these products which can be exploited by a remote user. Exploitation is achievable via ping flood attack.

Sending a continuous series of ICMP Echo Request (Ping) 10,000 byte packets to a target host, could cause the host to reboot. However, dial up users are not subject to this issue.

A continuous combination of such requests and replies could cause the systems functionality to diminish or crash. Results of this issue may slightly vary from system to system.

If an attacker is exploiting this issue on a host with the paranoid setting enabled, BlackICE could disable itself. In such a case where the BlackICE or RealSecure service becomes unresponsive, the host may become susceptible to attackers launching more "intelligent" attacks.

Reportedly, only Windows 2000 and XP hosts are susceptible to this issue.

* New information suggests that this may be an exploitable overflow condition, though this is unconfirmed.

4. MIRC Nick Buffer Overflow Vulnerability

BugTraq ID: 4027

Remote: Yes

Date Published: Feb 03 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4027>

Summary:

mIRC is a popular Internet Relay Chat client which runs on Microsoft Windows 9x/ME/NT/2000/XP operating systems.

A remote exploitable buffer overflow condition has been discovered in mIRC. This issue is due to improper bounds checking of nicknames sent by the server in the 001 numeric. Upon connection to an IRC server, most servers send a 001 numeric in response to a client connection to welcome the client. The 001 numeric looks like "Welcome to the Internet Relay Network \$nickname" where \$nickname represents the nickname of the user.

If the server sends an excessively long nickname to the client (200+ characters), it is possible to overwrite stack variables (including the return address). As a result, the malicious server can cause attacker-supplied instructions to be executed on the client host.

This issue is also exploitable via a webpage that can instruct the client to launch and to make a connection to the malicious server.

This may lead to a full compromise of the host running the client software on some Windows systems.

5. Microsoft MSN ActiveX Object Information Disclosure Vulnerability

BugTraq ID: 4028

Remote: Yes

Date Published: Feb 02 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4028>

Summary:

Microsoft's MSN Messenger is a popular instant messenger application for the Windows family of operating systems. It is based on the Passport system, and users are uniquely identified by an email address.

By default, some versions of MSN expose information through an ActiveX object. This object may be accessed through javascript or VBScript. Information available through this object includes the current user's display name, and the display name of all user's on their contact list. In the event that any party does not have a display name defined, their email address is available instead.

This may result in the disclosure of sensitive information, if the user has a meaningful display name and is under the impression that they are anonymously visiting a web page. This information may also be of some value in tracking usage across multiple domains, as a sort of "super cookie".

Additional information is available to a select group of Microsoft hosted sites, and to any trusted domain suffix listed in the registry. Malicious local software such as spyware or adware may modify this registry key, and expand the range of information available to a domain. It is possible to include a top level domain such as .com. The relevant key is:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MessengerService\Policies\Suffixes

6. Castelle Faxpress Plaintext Password Disclosure Vulnerability

BugTraq ID: 4030

Remote: Yes

Date Published: Feb 05 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4030>

Summary:

Castelle FaxPress is an integrated solution for a network fax environment. FaxPress is a hardware and software server providing fax functionality, and is designed to integrate with Microsoft Windows, Novell NetWare, and Linux based systems.

FaxPress includes support for printing, either directly or through a network printer queue. If a print job is submitted to the network queue with an incorrect password, an error message is reported to the client through the FaxPress notice system. This error message includes the submitted username and password in plain text.

Under some circumstances, this may result in the disclosure of sensitive information. For example, in a corporate environment, the FaxPress client may be configured by a central department, and the individual users unaware of the password used.

7. Microsoft Site Server LDAP Plain Text Password Storage Vulnerability

BugTraq ID: 4000

Remote: Yes

Date Published: Jan 31 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4000>

Summary:

Microsoft Site Server is designed to run on Microsoft Windows NT Server platforms. It provides a means for users on a corporate intranet to share, publish, and find information. Site Server Commerce Edition incorporates the same features as well as providing an interface for e-commerce sites to interact and conduct business with customers and suppliers.

Lightweight Directory Access Protocol (LDAP) is a protocol used to access the Active Directory service. The Active Directory maintains information about network resources and users. It organizes and controls user's privileges to various network resources.

An issue has been discovered in Site Server, which could allow a remote user to peruse sensitive data.

By default the LDAP service in Site Server listens on port 1002 and remote users can log in under anonymous. Logging in as anonymous will allow a user to have read access to network resources.

Due to a design flaw, the LDAP members passwords are stored in plain text. Any user, including unprivileged anonymous users, can gain knowledge of user passwords.

In addition, it has been reported that NT domain accounts can also gain access to this information.

Successful exploitation of this vulnerability could assist a user in gaining escalated privileges, which will facilitate in further attacks against the host.

8. Microsoft MSDTC Service Denial of Service Vulnerability

BugTraq ID: 4006

Remote: Yes

Date Published: Jan 31 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4006>

Summary:

The Microsoft Distributed Transaction Service Coordinator (MSDTC) allows for distributed transaction processing in a clustered or distributed environment. It is installed by default on Windows 2000, as well as with Microsoft SQL Server 6.5 and higher.

It has been reported that it is possible to cause this service to crash by sending 1024 bytes of random data to its listening port, by default port 3372. On some systems, this may cause the service to crash immediately, while on those that fail to crash, larger data packets and multiple connections will have no effect.

Restarting the service will reportedly allow it to resume normal operation.

The existence of this vulnerability has not been confirmed by Microsoft.

9. MS Site Server Unauthorized SQL Command Injection Vulnerability

BugTraq ID: 4009

Remote: Yes

Date Published: Jan 31 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4009>

Summary:

Microsoft Site Server is designed to run on Microsoft Windows NT Server platforms. It provides a means for users on a corporate intranet to share, publish, and find information. Site Server Commerce Edition incorporates the same features as well as providing an interface for e-commerce sites to interact and conduct business with customers and suppliers.

An issue exists in web applications that ship with Site Server that do not properly validate user input before passing it to an SQL query. The site applications contained within 'clocktower', 'vc30', 'mssql30' and 'market' allow for the injection of user specified SQL commands.

Successful exploitation of this issue will allow an attacker to modify queries, possibly resulting in data corruption or application subversion. Furthermore, it may be possible for an attacker to gain local access to the underlying host.

The existence of these vulnerabilities may be due to the issue discussed as BID 994. However this has not been confirmed.

III. MICROSOFT FOCUS LIST SUMMARY

1. Secure Transactions over HTTPS???? (Thread)

Relevant URL:

1013185372.2061.8.camel@tux.dogoodsoft.org//www.securityfocus.com/cgi-bin/archive.pl?id=88href="mailto:10131

2. Where would the changes be saved? (Thread)

Relevant URL:

AAEIJLOGDIINFKOLIPEMIEGOCOAA.ken.hoover@yale.edu//www.securityfocus.com/cgi-bin/archive.pl?id=88hr

3. Question regarding attack (Thread)

Relevant URL:

[http://www.securityfocus.com/cgi-bin/archive.pl?id=88\\$2a1f1880\\$0302a8c0@WorkGroup](http://www.securityfocus.com/cgi-bin/archive.pl?id=88$2a1f1880$0302a8c0@WorkGroup)

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #73

4. SYSTEM grabbing ports? (Thread)

Relevant URL:

[652ca8c0@FUSION.CO.UK//www.securityfocus.com/cgi-bin/archive.pl?id=88\\$950cd480\\$652ca8c0@FUSION.CO.UK](http://www.securityfocus.com/cgi-bin/archive.pl?id=88$950cd480$652ca8c0@FUSION.CO.UK//www.securityfocus.com/cgi-bin/archive.pl?id=88$950cd480$652ca8c0@FUSION.CO.UK)

5. Allowing users to change their password via the web (Thread)

Relevant URL:

[NEEPLCMFPIEOEDGJJIGGEIKCAA.bryan_allerdice@yahoo.com//www.securityfocus.com/cgi-bin/archive.pl?id=88\\$950cd480\\$652ca8c0@FUSION.CO.UK](http://www.securityfocus.com/cgi-bin/archive.pl?id=88$950cd480$652ca8c0@FUSION.CO.UK//www.securityfocus.com/cgi-bin/archive.pl?id=88$950cd480$652ca8c0@FUSION.CO.UK)

6. Possible hack – Portable profile found in a Windows 2K Pro SP1 station.. (Thread)

Relevant URL:

[F114g5wlSe9F6EBSotw00003374@hotmail.com//www.securityfocus.com/cgi-bin/archive.pl?id=88href="mailto:F114g5wlSe9F6EBSotw00003374@hotmail.com](http://www.securityfocus.com/cgi-bin/archive.pl?id=88href=)

7. Local security policy Settings (Thread)

Relevant URL:

[NEEPLCMFPIEOEDGJJIGMEHJCAA.bryan_allerdice@yahoo.com//www.securityfocus.com/cgi-bin/archive.pl?id=88\\$950cd480\\$652ca8c0@FUSION.CO.UK](http://www.securityfocus.com/cgi-bin/archive.pl?id=88$950cd480$652ca8c0@FUSION.CO.UK//www.securityfocus.com/cgi-bin/archive.pl?id=88$950cd480$652ca8c0@FUSION.CO.UK)

8. IM encryption (Thread)

Relevant URL:

[HMEIJMEKHLHGNJPCDCEBOCEHMCLAA.jrodriguez@intellinet-tech.com//www.securityfocus.com/cgi-bin/archive.pl?id=88\\$950cd480\\$652ca8c0@FUSION.CO.UK](http://www.securityfocus.com/cgi-bin/archive.pl?id=88$950cd480$652ca8c0@FUSION.CO.UK//www.securityfocus.com/cgi-bin/archive.pl?id=88$950cd480$652ca8c0@FUSION.CO.UK)

9. TCP/IP Filtering problem on W2KAS (Thread)

Relevant URL:

[20020205164653.A14288@garbarek.hsc.fr//www.securityfocus.com/cgi-bin/archive.pl?id=88href="mailto:20020205164653.A14288@garbarek.hsc.fr](http://www.securityfocus.com/cgi-bin/archive.pl?id=88href=)

10. Possible hack – Portable profile found in a Windows 2K Pro SP 1 station.. (Thread)

Relevant URL:

<http://www.securityfocus.com/cgi-bin/archive.pl?id=88D411A45200D0B73C4DE12127A1@ThisAddressDoesNotExist>

11. Windows 2000/.Net Group Policy Locker (Thread)

Relevant URL:

[20020204173152.28883.qmail@web10907.mail.yahoo.com//www.securityfocus.com/cgi-bin/archive.pl?id=88href="mailto:20020204173152.28883.qmail@web10907.mail.yahoo.com](http://www.securityfocus.com/cgi-bin/archive.pl?id=88href=)

12. TCP/IP Filtering problem on (Thread)

Relevant URL:

[180349117824.20020204172944@rubikon.pl//www.securityfocus.com/cgi-bin/archive.pl?id=88href="mailto:180349117824.20020204172944@rubikon.pl](http://www.securityfocus.com/cgi-bin/archive.pl?id=88href=)

13. SecurityFocus Microsoft Newsletter #72 (Thread)

Relevant URL:

[Pine.LNX.4.43.0202041517560.7331-100000@mail.securityfocus.com//www.securityfocus.com/cgi-bin/archive.pl?id=88\\$950cd480\\$652ca8c0@FUSION.CO.UK](http://www.securityfocus.com/cgi-bin/archive.pl?id=88$950cd480$652ca8c0@FUSION.CO.UK//www.securityfocus.com/cgi-bin/archive.pl?id=88$950cd480$652ca8c0@FUSION.CO.UK)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Aventail ExtraNet Center

by Aventail

Platforms: Linux, Solaris, Windows NT, AIX, HP-UX, DG-UX

Relevant URL:

<http://www.aventail.com/managed/extranet.asp>

Summary:

Aventail ExtraNet Center is simple to deploy and requires no changes to your partner's network, applications, or firewall configuration. This simplifies the political challenges of the extranet, speeds deployment times to days not months, thus increasing your competitive advantage. Customer Service: By their very nature, extranets bring key partners and customers to valuable resources. Aventail ExtraNet Center's client runs transparently in the background and requires no contact with the user beyond authentication. This increases the value of the partner extranet while lowering corporations' support costs. And, it's not just HTTP, Aventail ExtraNet Center provides security and management for any IP application.

2. Luna XL

by Chrysalis-ITS

Platforms: Linux, Solaris, Windows NT, Windows 2000

Relevant URL:

http://www.chrysalis-its.com/trusted_systems/luna_xl.htm

Summary:

Luna XL delivers high-performance hardware-based SSL acceleration for your secure web server, adding security to high value e-business transactions. Luna XL offers trench-tested key management for your SSL sessions without the performance penalty.

3. Cryptix EasyCrypt

by C&A Systems Security

Platforms: Solaris, Windows 95/98, OS/2, DOS

Relevant URL:

<http://www.ca-systems.zetnet.co.uk/crypto.htm#cryptixeasycrypt>

Summary:

EasyCrypt offers the DES algorithm or a proprietary algorithm and is invoked via a series of simple commands. The key management mechanism enables total flexibility of approach, allowing central or devolved control and use. The whole system is designed for ease of use and versatility. Full message authentication (MAC'ing) is provided, as are several levels of key control for direct mapping onto complex environments. EasyCrypt is of use to any enterprise that requires flexible and simple file security with minimal overhead. It will provide a high level of cryptographic security and a consistent platform independent approach.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. NGSecureWeb v1.00

by NGSEC Research Team labs@ngsec.com

Relevant URL:

<http://www.ngsec.com/download.html>

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

Summary:

NGSecureWeb is a security module for Web Servers. It acts as an application IDS/firewall, preventing security bugs from being exploited. It has the ability to check for shellcodes (even polymorphic ones), buffer overflows, forbidden words, long URLs, long GET arguments, long POST arguments, long HEADERS, etc., in the HTTP request. If the IDS engine detects a possible attack, the firewall engine stops the request. The Apache and Netscape Enterprise Web servers are supported.

2. Typhon

by Next Generation Security Software Ltd

Relevant URL:

<http://www.nextgenss.com/products/typhon.html>

Platforms: Windows 2000, Windows NT

Summary:

Typhon, an updated version of Cerberus Internet Scanner, is a vulnerability assessment tool. It will scan a given host for known security holes and vulnerabilities. It does this by looking at the services offered by a host and each of these are examined for holes. For example, Typhon will check for over 180 known vulnerabilities in the web service or daemon offered by a server. Once a scan has been completed a report in HTML is produced detailing what security holes were found, the impact of those holes and how to fix them. Once these holes have been removed then the host will be more secure against attacks. As new vulnerabilities are discovered almost on a daily basis it is necessary to ensure that the Typhon is kept upto date and hosts are scanned on a regular basis.

3. Securepoint Firewall and VPN Server SB v2.0.6.1

by Lutz Hausmann, lutz.hausmann@linkx.de

Relevant URL:

<http://www.securepoint.cc/download.htm>

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

Summary:

The Securepoint Firewall Server is a high-performance, commercial-grade application designed to offer full protection for network assets. The Securepoint is a complete software system with an operation system, based on a secure Linux. You can use the firewall on a standard PC with two or three network cards, and is easy to install and administer.

4. CIA Unerase Private v1.0

by Datapol GmbH

Relevant URL:

<http://www.ciaunerase.com>

Platforms: Windows 2000, Windows NT, Windows XP

Summary:

CIA Unerase is an easy to use unerase and data recovery tool for WinNT/2000/XP. It unerases files even without having to be installed before the disaster happened. Using the unique "CIS technology" it is capable to unerase up to 20 more files than any other solution. It supports FAT as well as NTFS and recovers files on physical, local logical, dynamic and RAID disks. Encrypted files, compressed files and files using streams are also supported. More then 95% of all deleted files are restored completely by CIA Unerase even if their status is "poor". The PRIVATE Edition works on all Workstation–Versions of Windows NT, Windows 2000 and Windows XP. A german version is offered on our German website <http://www.datapol.de>

VI. SPONSORSHIP INFORMATION

This Issue is Sponsored By: GFI Ltd.

Intrusion detection through NT/2000 security logs: LANguard

Catch hackers red–handed with GFI's LANguard S.E.L.M.! Performs intrusion detection through network–wide monitoring of the security event logs of all NT/2000 servers & workstations. Enables you to respond quickly to important security events, without spending hours examining logs. Notifies you of critical security events in real time & more besides! Get your FREE evaluation from:

<http://www.gfi.com/securityfocus/>

- **Previous message:** [Michael Dana–TM: "Windows 2000 log retention"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)