



Mi újság a vírusfronton ?

Dr. Leitold Ferenc
Veszprog Kft.
fleitold@veszprog.hu

Tartalom



- **Virus Bulletin 2004 – Chicago**
- **JPEG biztonsági probléma**
- **CheckVir projekt**

VB 2004



- Gatekeeper – 80%-os ismeretlen vírus feleismerés
- Bagle vírusváltozatok evolúciója
- Internet wormok felismerési kérdései
- 10 Gbit/s vírusmonitor

vb 2004
CHICAGO

**VIRUS BULLETIN INTERNATIONAL
CONFERENCE & EXHIBITION**

THE FAIRMONT, CHICAGO, USA
SEPTEMBER 29 – OCTOBER 1, 2004

**AN ESSENTIAL
COMPONENT OF YOUR
ANTI-VIRUS STRATEGY**

- 30+ presentations by world-leading experts
- The latest anti-virus technologies
- Emerging malware threats
- User education
- Corporate policy
- Law enforcement
- Anti-spam techniques
- Real-world case studies
- Panel discussions
- Full social program for networking

Sponsored by:

REGISTER ONLINE AT WWW.VIRUSBTN.COM

The poster features a background image of a globe with a virus icon, overlaid with a stylized American flag and the word "CHICAGO" in large, semi-transparent letters.

JPEG biztonsági probléma



JPEG biztonsági probléma



2004. szept. 14.:

- Microsoft közzététele
- Észlelőeszköz

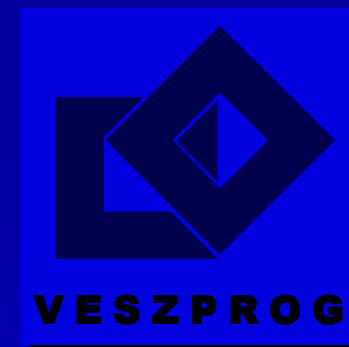
The screenshot shows a Microsoft Internet Explorer browser window displaying the download page for the Microsoft GDI+ észlelőeszköz (Microsoft GDI+ detector tool). The browser's address bar shows the URL: <http://www.microsoft.com/downloads/details.aspx?displaylang=hu&FamilyID=71CD9E74-7142-4780-83E5-CE54401DA1D1>. The page title is "Letöltés ismertetése: Microsoft GDI+ észlelőeszköz - Microsoft Internet Explorer". The page content includes a search bar, a navigation menu, and a main section titled "Microsoft GDI+ észlelőeszköz". The main section contains a description of the tool, a table of metadata, and a download button.

Összefoglaló	
Fájlnév:	gdidetool.exe
Letöltés mérete:	216 kB
Közzétéve:	2004. 09. 14.
Verzió:	1

Microsoft GDI+ észlelőeszköz
Magyar

Letöltés

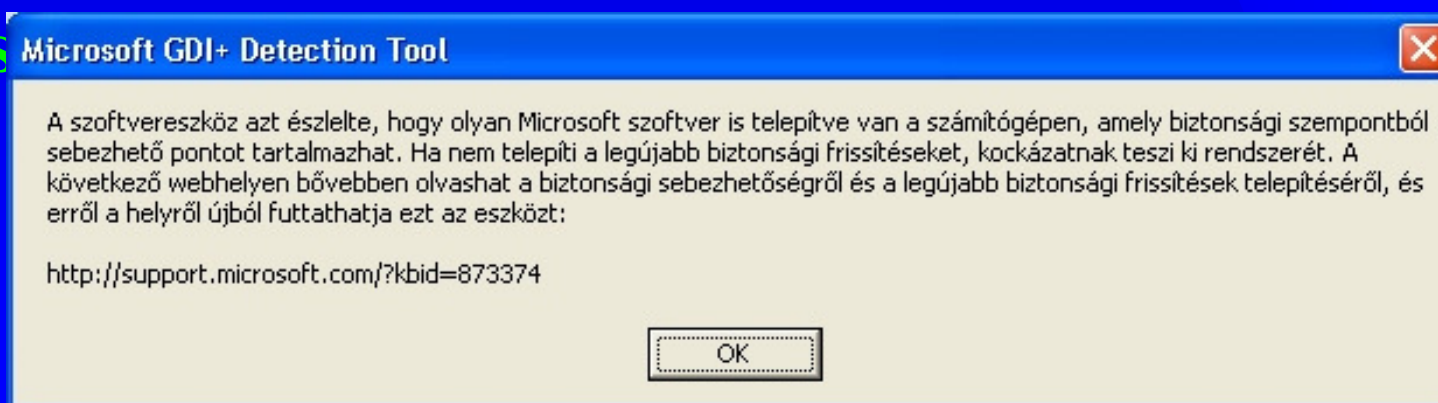
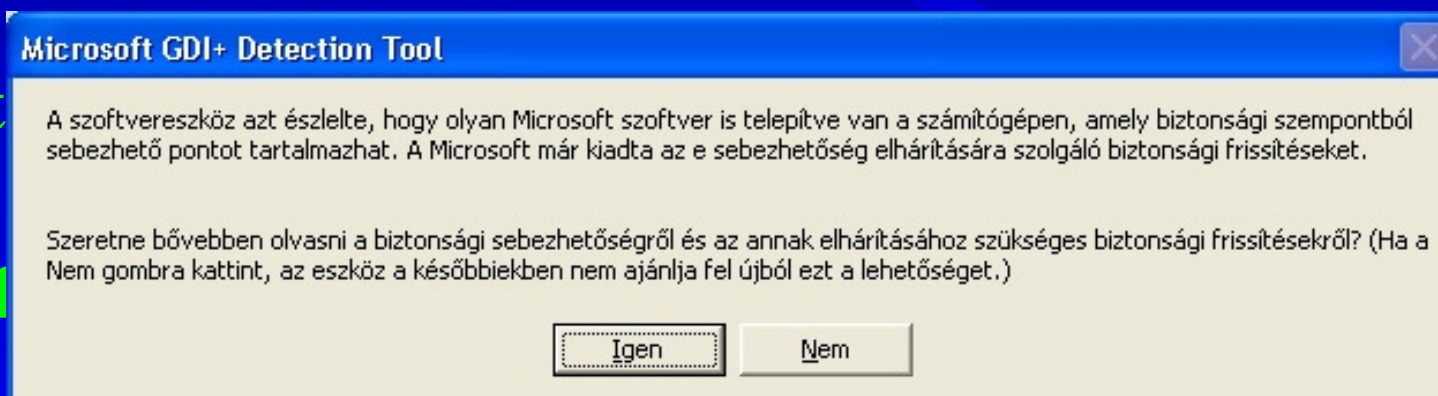
JPEG biztonsági probléma



2004. szept

• Microsoft

• Észlelőes



JPEG biztonsági probléma



2004. szept. 27.:

Első JPEG trójai szétküldése (usenet newsgroup) – Troj.Moo

jpegheader - Jegyzettömb

Fájl Szerkesztés Formátum Nézet Súgó

```
Path: news.easynews.com!core-easynews!newsfeed2.easynews.com!newsfeed1.easynews.com!easynews
From: Power-Poster@power-post.org (Power-Post 2000)
Sender: Power-Poster@power-post.org
Newsgroups: alt.binaries.multimediaerotica.transsexuals,alt.binaries.pictureserotica.trans
Subject: (shemale-loves it up the ass.jpg (1/1)) [1/1] - shemale loves it up the ass
X-NewsPoster: NNTP POWER-POST 2000 (Build 24c) - net-toys.8k.com
Lines: 96
Message-ID:
Date: Mon, 27 Sep 2004 01:25:52 GMT
NNTP-Posting-Host: 82.1.163.241
X-Trace: newsfe3-win.ntli.net 1096248352 82.1.163.241 (Mon, 27 Sep 2004 02:25:52 BST)
NNTP-Posting-Date: Mon, 27 Sep 2004 02:25:52 BST
Organization: NTL
Xref: core-easynews alt.binaries.multimediaerotica.transsexuals:1756301 alt.binaries.pictur
X-Received-Date: Sun, 26 Sep 2004 19:19:51 MST (news.easynews.com)
```

JPEG biztonsági probléma



2004. szeptember 27.
Első

```
-rw-r--r-- 1 root root 90112 Sep 27 09:43 AdmDll.dll
-rw-r--r-- 1 root root 114688 Sep 27 09:43 Fport.exe
-rw-r--r-- 1 root root 663 Sep 27 09:43 ServUStartUpLog.txt
-rw-r--r-- 1 root root 32768 Sep 27 09:43 VNCHooks.dll
-rw-r--r-- 1 root root 1407 Sep 27 09:43 WinRun.dll
-rw-r--r-- 1 root root 811008 Sep 27 09:43 WinRun.exe
-rw-r--r-- 1 root root 1268 Sep 27 09:43 driver.log
-rw-r--r-- 1 root root 24576 Sep 27 09:43 drives.exe
-rw-r--r-- 1 root root 150 Sep 27 09:43 execute.bat
-rw-r--r-- 1 root root 0 Sep 27 09:43 filter3.ocx
-rw-r--r-- 1 root root 1052 Sep 27 09:43 irc-u.cfg
-rw-r--r-- 1 root root 0 Sep 27 09:43 irc-u.dat
-rw-r--r-- 1 root root 16802 Sep 27 09:43 irc-u.debug.log
-rw-r--r-- 1 root root 102400 Sep 27 09:43 irc-u.dll
-rw-r--r-- 1 root root 26624 Sep 27 09:43 kill.exe
-rw-r--r-- 1 root root 59392 Sep 27 09:43 nc.exe
-rw-r--r-- 1 root root 241664 Sep 27 09:43 nvsvc.exe
-rw-r--r-- 1 root root 36864 Sep 27 09:43 nvsvc32.dll
-rw-r--r-- 1 root root 45056 Sep 27 09:43 omnithread_rt.dll
-rw-r--r-- 1 root root 34304 Sep 27 09:43 peek.exe
-rw-r--r-- 1 root root 29408 Sep 27 09:43 raddrv.dll
-rw-r--r-- 1 root root 713 Sep 27 09:43 radmin.reg
-rw-r--r-- 1 root root 26112 Sep 27 09:43 rcrypt.exe
-rw-r--r-- 1 root root 40960 Sep 27 09:43 reg.exe
-rw-r--r-- 1 root root 6656 Sep 27 09:43 uptime.exe
-rw-r--r-- 1 root root 208896 Sep 27 09:43 vns.exe
```

Troj.Moo

jpegl
Fájl Sze
Path:
From:
Sender
Newsgr
Subjec
X-News
Lines:
Messag
Date:
NNTP-P
X-Trac
NNTP-P
Organi
Xref:
X-Rece

ews.com!easynews
es.erotica.trans
the ass
5:52 BST)
.binaries.pictur

CheckVir projekt



- **Antivírus tesztelés fő célja**

- AV felhasználók informálása
- AV fejlesztők segítése munkájukban

- **AV tesztelés**

- 2000-től automatikus módszerek fejlesztése
- 2002 áprilisától nyilvános tesztek
- 2004 januártól minősítés
- *Oktatási Minisztérium Kutatás-fejlesztési Helyettes Államtitkársága, valamint az Informatikai és Hírközlési Minisztérium támogatásával*

Minősítés



- 2004 januárjától
 - Standard Level
 - Advanced Level
 - Mailscanner Level
- Víruskeresési eljárások
 - On-demand
 - On-access
 - In/out mail
- Víruskészlet
 - Elterjedt vírusokból
 - Min. 80% az elmúlt 3 hónapból

VIRUS BULLETIN www.virusbtn.com

NEWS

NEW KID ON THE CERTIFICATION BLOCK

At the start of this year, *CheckVir* became the latest independent organisation to offer certification for anti-virus products, when the *CheckVir* Anti-Virus Testing project became the *CheckVir* Anti-Virus Certification program.

Like a number of other testing bodies, *CheckVir* offers two levels of certification: Standard and Advanced. The Standard certification is awarded for a product's detection capability (the product must detect all virus samples in the test set both on access and on demand), while the Advanced level examines the product's ability to repair infected objects. The results, including descriptions and summaries, are published on the *CheckVir* website. More information can be found at <http://www.checkvir.com/>.



Minősítési szintek



- **Standard Level**

- Vírusok keresése
- Vírus minden példányát azonosítja



- **Advanced Level**

- Vírusok keresése és irtása
- Víruskód eltávolítása az objektumból
- Visszaállított objektum teljes értékűen használható
- Információvesztés megengedett, ha az AV a felhasználót tájékoztatja



Minősítési szintek



- **MailsScanner Level**

- Vírusok felismerése
- Vírus minden példányát azonosítja
- Vírusok blokkolása vagy eltávolítása
- Bejövő és kimenő levelek



Eredmények



- PC World, Számítástechnika
- www.checkvir.hu, www.checkvir.com

Eredmények



AV fejlesztő	Termékek száma	Standard	Advanced
Grisoft	7	7	-
Softwin SRL.	7	6	-
ID Anti-Virus Lab.	5	5	-
Computer Associates	7	2	5
F-Secure Ltd.	7	7	-
Kaspersky Lab.	7	7	-
Network Associates	7	7	-
ESET Software	7	7	-
Norman ASA	7	5	-
Panda Software	7	7	-
Trend Micro	7	1	6
VirusBuster Ltd.	7	5	2
MicroWorld Technologies Inc.	2	-	2

Real-time AV test



- **Folyamatos AV tesztelés (minden verzió)**
- **Elterjedt vírusokkal szemben**
- **Felismeri-e? Ha igen, milyen néven?**

Real-time AV test



W32/Zafi.A

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus	4.5.0.95, 87139 (known viruses)	I-Worm.Zafi
Kaspersky Anti-Virus	4.5.0.95, 89257 (known viruses)	I-Worm.Zafi
Kaspersky Anti-Virus Personal	5.0.121, 91566 (av database record count)	I-Worm.Zafi
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	I-Worm.Zafi.a
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	I-Worm.Zafi.a

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	New Malware.b (Virus)
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	New Malware.b (Virus)
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	New Malware.b (Virus)
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	New Malware.b (Virus)
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	W32/Zafi@MM
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Zafi.a@MM

