Biztonsági aktualitások, a felhasználók felelőssége

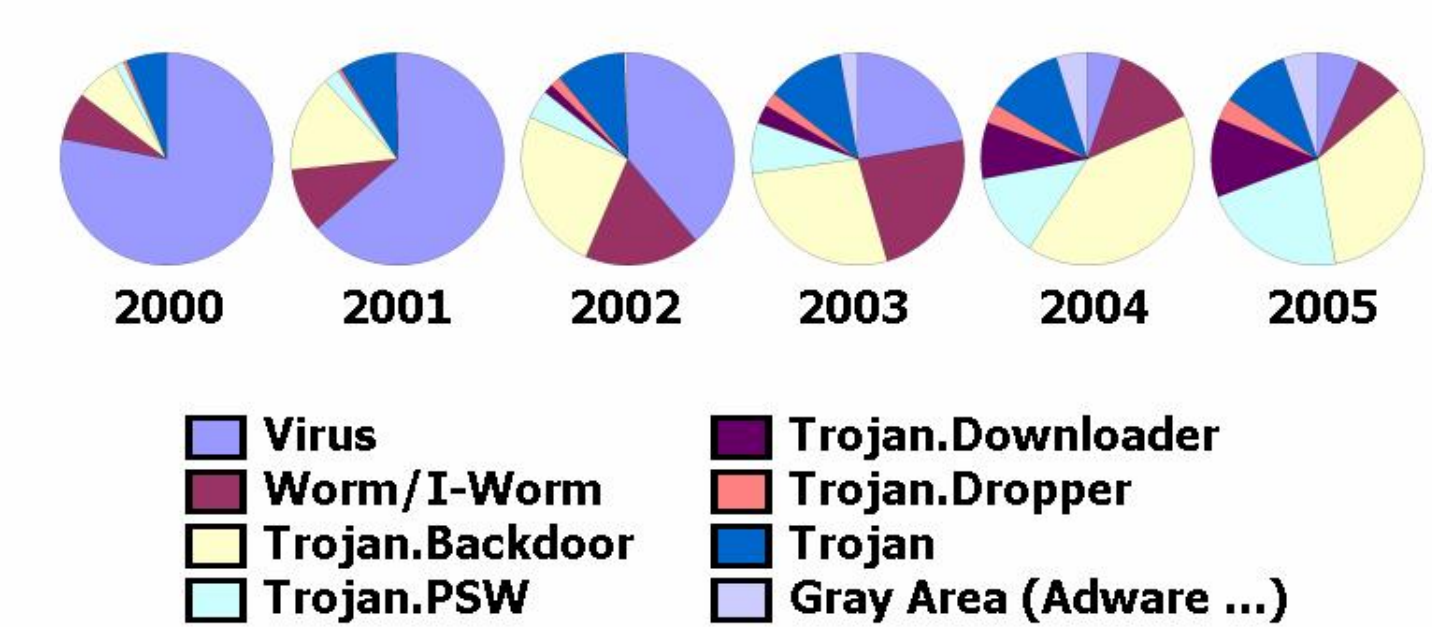
Fulajtár Pál

FOOLY Stúdió Kft.

FOOLY

www.avg.hu

A világ megváltozott



Az elmúlt egy év

Egyre több 0. napi támadás

c|net NEWS.com

Today on CNET | News | Reviews | Compare prices | Tips & Tricks | Downloads | CNET TV beta

Today on News | Business Tech | Cutting Edge | Access | Threats | Media 2.0 | Markets | Digital Life | My News | Most

Search: Go! Options

Zero-day Word flaw used in attack

By Joris Evers
Staff Writer, CNET News.com
Published: May 19, 2006, 11:32 AM PDT

TalkBack E-mail Print del.icio.us Digg this

A new, yet-to-be-fixed security hole in Microsoft Word exposes computer users to cyberattack, Symantec warned Friday.

Would-be intruders already have attempted to compromise PCs at a Japanese government entity by exploiting the flaw, Vincent Weafer, the senior director at Symantec Security Response, said in an interview. In response, Symantec has raised its ThreatCon to Level 2, which means an outbreak is expected.

"What we're seeing is a continuation of the targeted threat using zero-day vulnerabilities," Weafer said. (Zero-day flaws are ones for which no patch exists.) "We got it from a single large customer inside Japan. We have not seen anyone else get it."

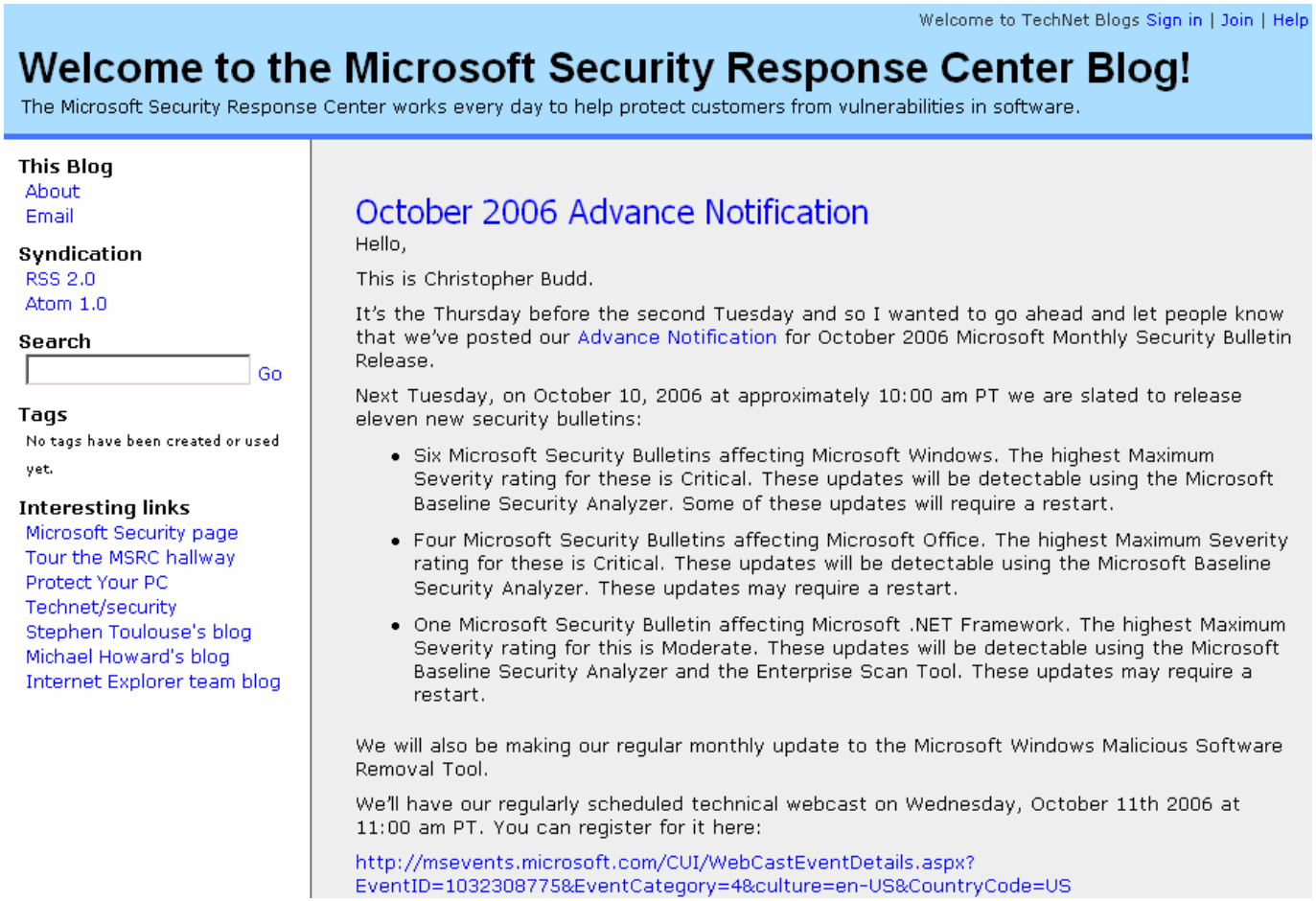
Microsoft is readying a security update for Word that repairs this vulnerability, a company representative said in an e-mailed statement. The fix is scheduled to be released as part of the June 13 security updates, or sooner, if warranted, the representative said.

THE BIG PICTURE | RELATED STORIES

Related news

- Bounty for Vista coders who squish b
  May 12, 2006
- Microsoft probes Outlook Express pat

blogs.technet.com / msrc



Welcome to TechNet Blogs Sign in | Join | Help

Welcome to the Microsoft Security Response Center Blog!

The Microsoft Security Response Center works every day to help protect customers from vulnerabilities in software.

This Blog
About
Email

Syndication
RSS 2.0
Atom 1.0

Search
Go

Tags
No tags have been created or used yet.

Interesting links
Microsoft Security page
Tour the MSRC hallway
Protect Your PC
Technet/security
Stephen Toulouse's blog
Michael Howard's blog
Internet Explorer team blog

October 2006 Advance Notification

Hello,

This is Christopher Budd.

It's the Thursday before the second Tuesday and so I wanted to go ahead and let people know that we've posted our Advance Notification for October 2006 Microsoft Monthly Security Bulletin Release.

Next Tuesday, on October 10, 2006 at approximately 10:00 am PT we are slated to release eleven new security bulletins:

- Six Microsoft Security Bulletins affecting Microsoft Windows. The highest Maximum Severity rating for these is Critical. These updates will be detectable using the Microsoft Baseline Security Analyzer. Some of these updates will require a restart.
- Four Microsoft Security Bulletins affecting Microsoft Office. The highest Maximum Severity rating for these is Critical. These updates will be detectable using the Microsoft Baseline Security Analyzer. These updates may require a restart.
- One Microsoft Security Bulletin affecting Microsoft .NET Framework. The highest Maximum Severity rating for this is Moderate. These updates will be detectable using the Microsoft Baseline Security Analyzer and the Enterprise Scan Tool. These updates may require a restart.

We will also be making our regular monthly update to the Microsoft Windows Malicious Software Removal Tool.

We'll have our regularly scheduled technical webcast on Wednesday, October 11th 2006 at 11:00 am PT. You can register for it here:

http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032308775&EventCategory=4&culture=en-US&CountryCode=US

Menedzselt frissítés

- Gyors reakció, gyorsan kiadott frissítések
- Frissítéssek minél gyorsabb eljuttatása a felhasználókhoz
- Frissítések szétosztása a munkaállomások számára
- Visszacsatolás, a frissítés sikerességének mérése

Frissítési séma

Hagyományos ütemezett frissítés

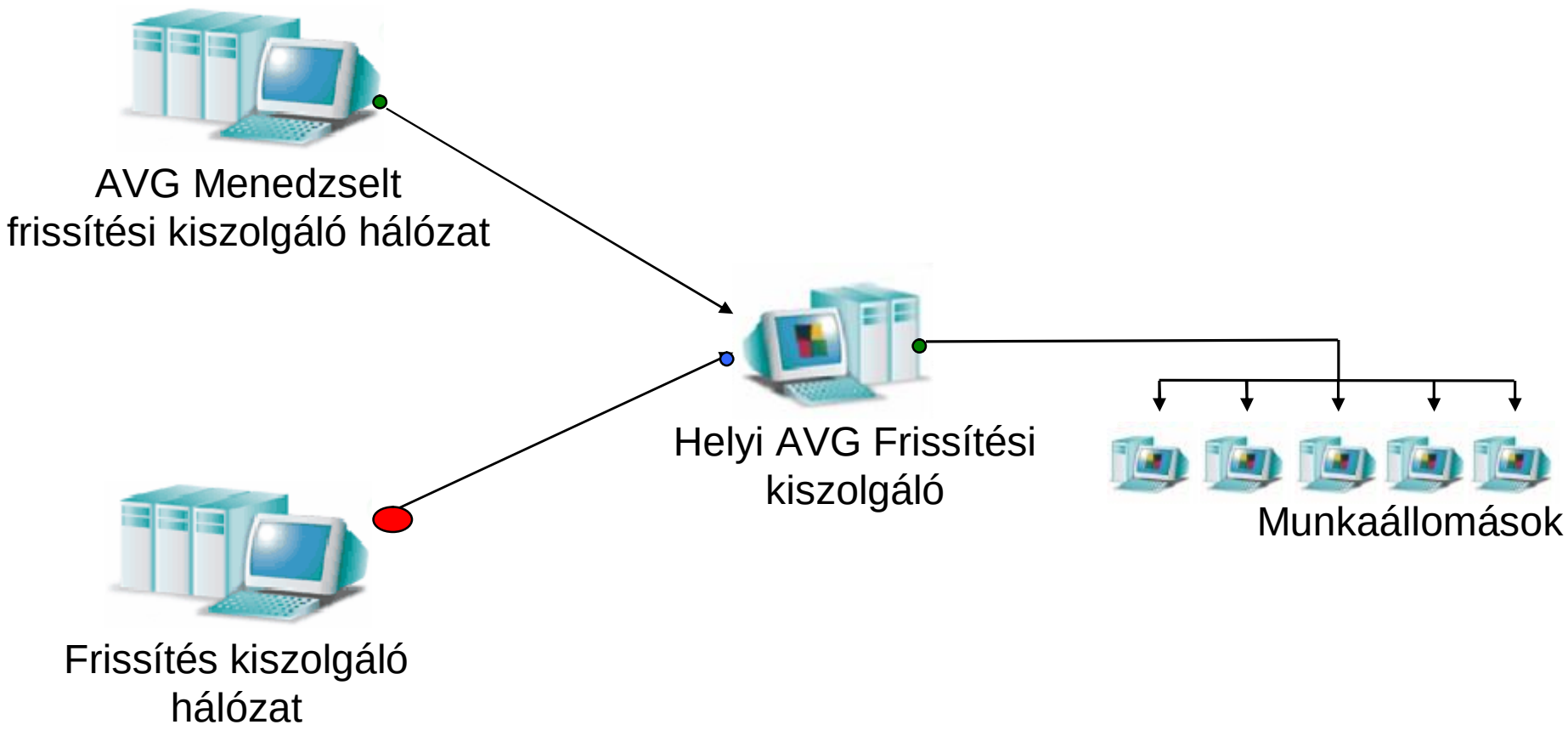
AVG Menedzselt frissítés

- Telik az idő…
- Új „vírus” megjelenése
- Frissítés megjelenése
- A kliensek időzítése
- Védelem nélkül eltelt idő

FOOLY

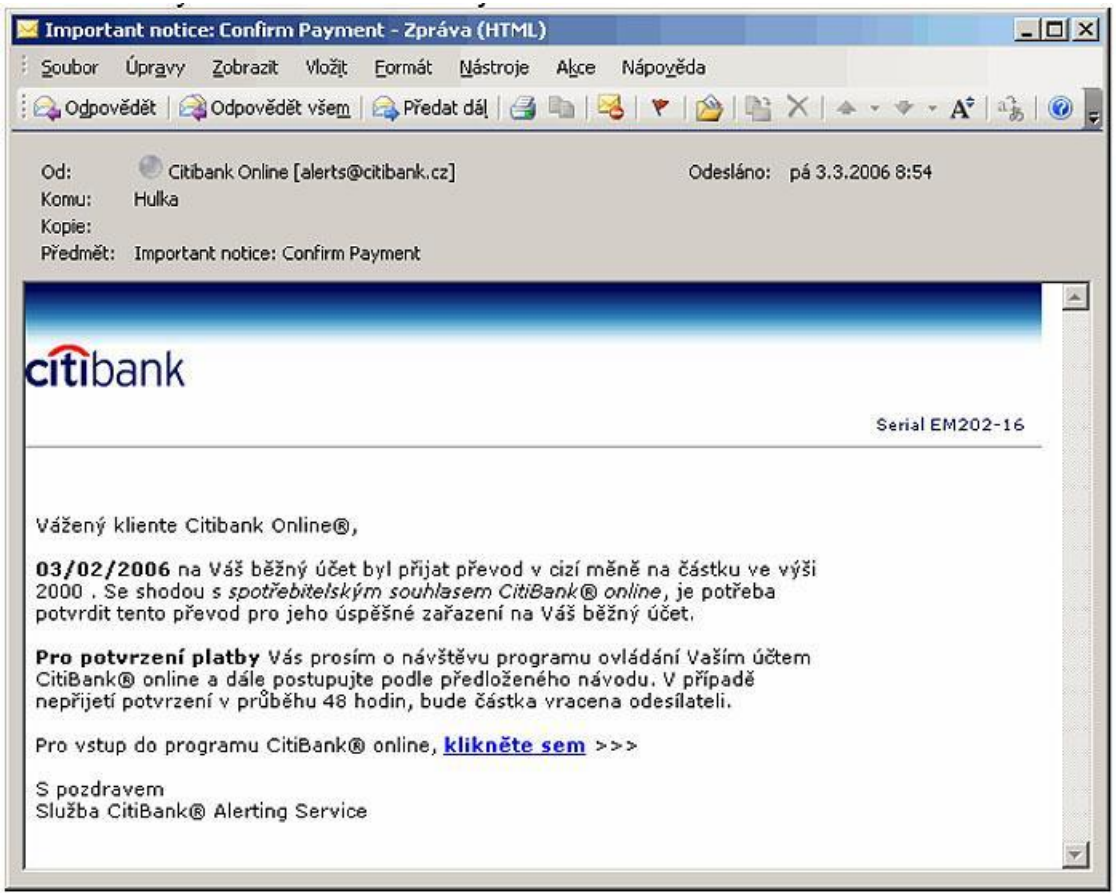
www.avg.hu

Menedzselt frissítési hálózat

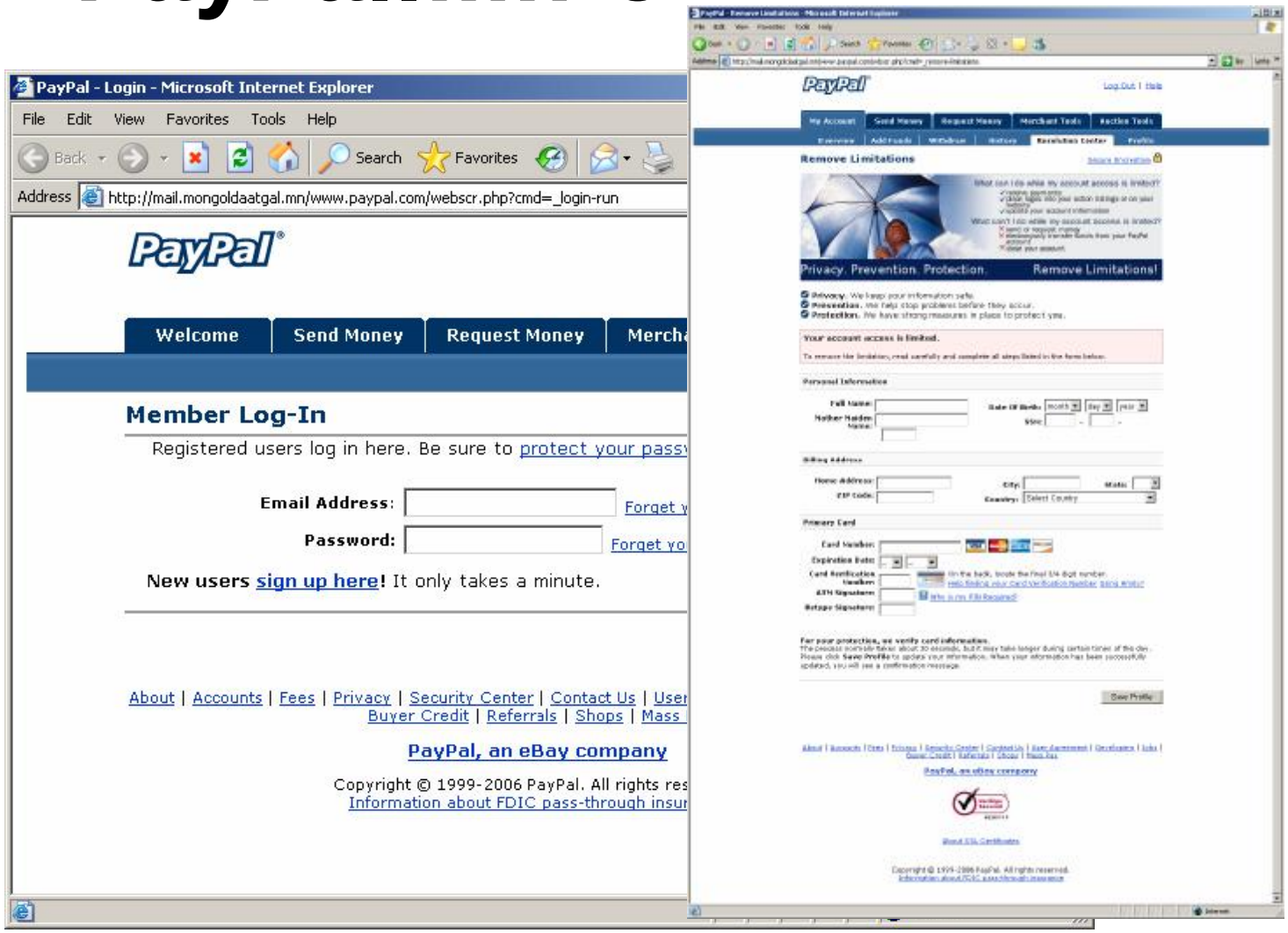


Adathalászat

Adathalászat

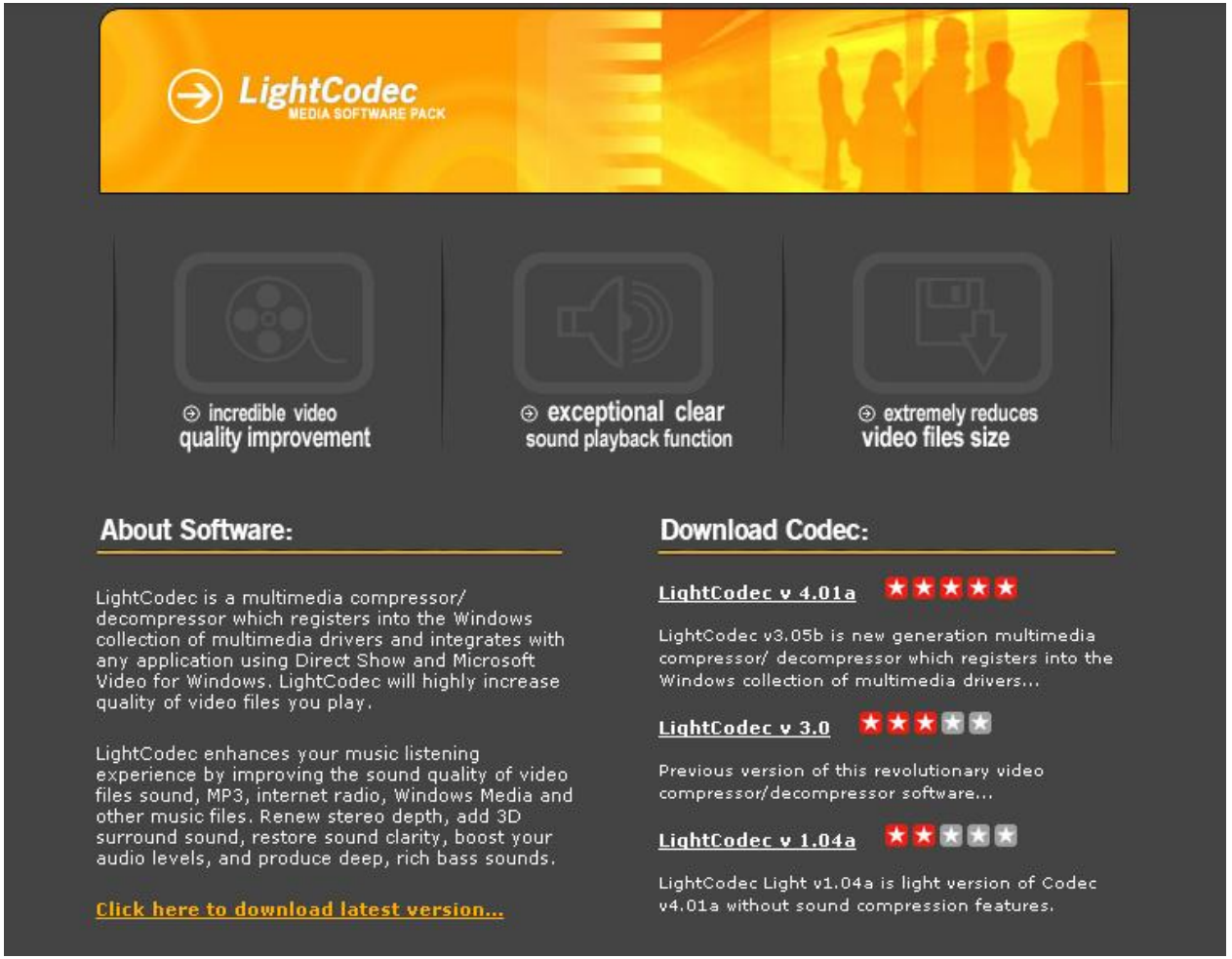


PayPal.mn J

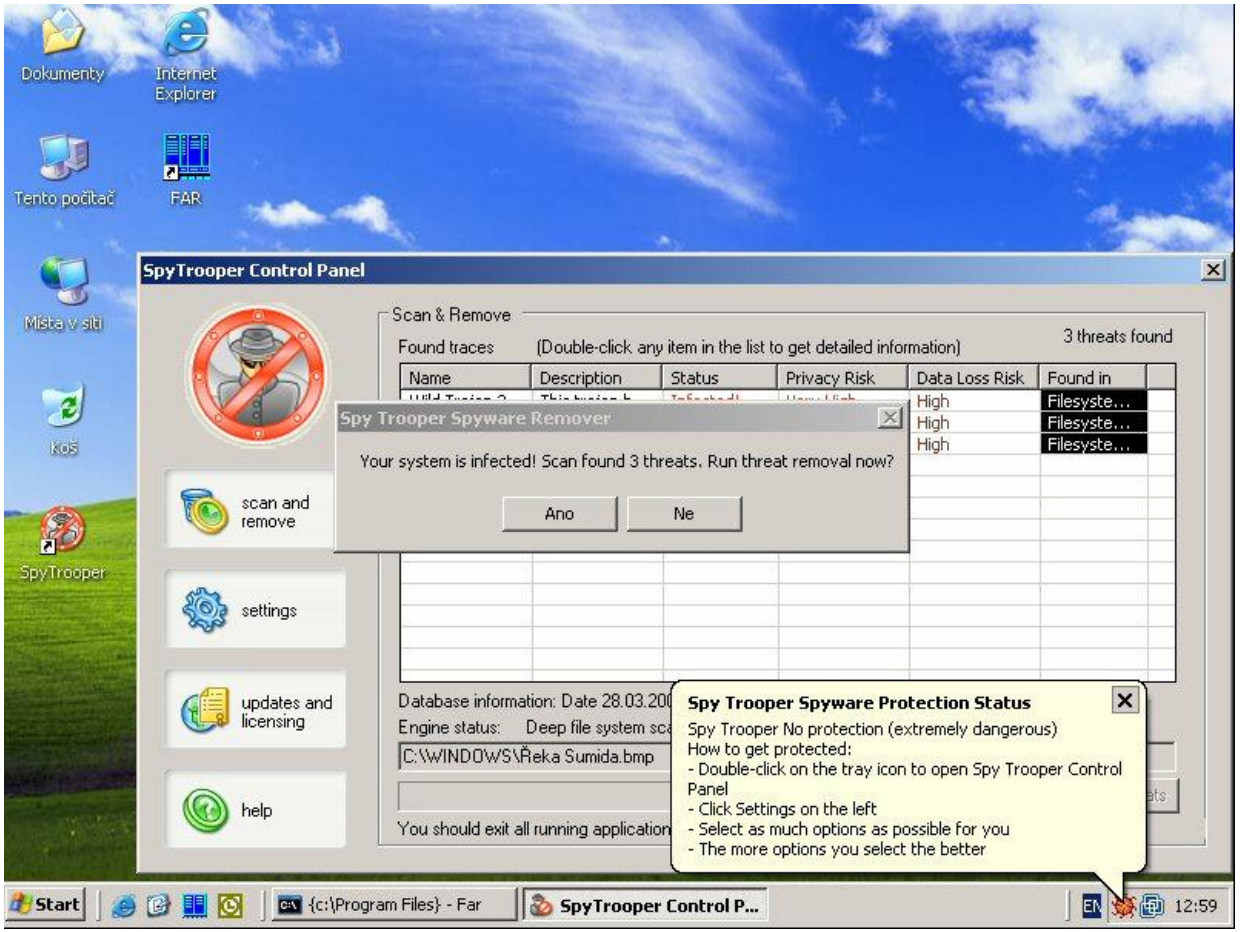

PayPal - Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://mail.mongoldaatgal.mn/www.paypal.com/webscr.php?cmd=_login-run
PayPal
Welcome
Send Money
Request Money
Member Log-In
Registered users log in here. Be sure to protect your pass
Email Address:
Password:
New users sign up here! It only takes a minute.
About | Accounts | Fees | Privacy | Security Center | Contact Us
Buyer Credit | Referrals | Shops | Mass
PayPal, an eBay company
Copyright © 1999-2006 PayPal. All rights res
Information about FDIC pass-through insu
PayPal
Remove Limitations
Privacy. Prevention. Protection. Remove Limitations!

Hamisított alkalmazások

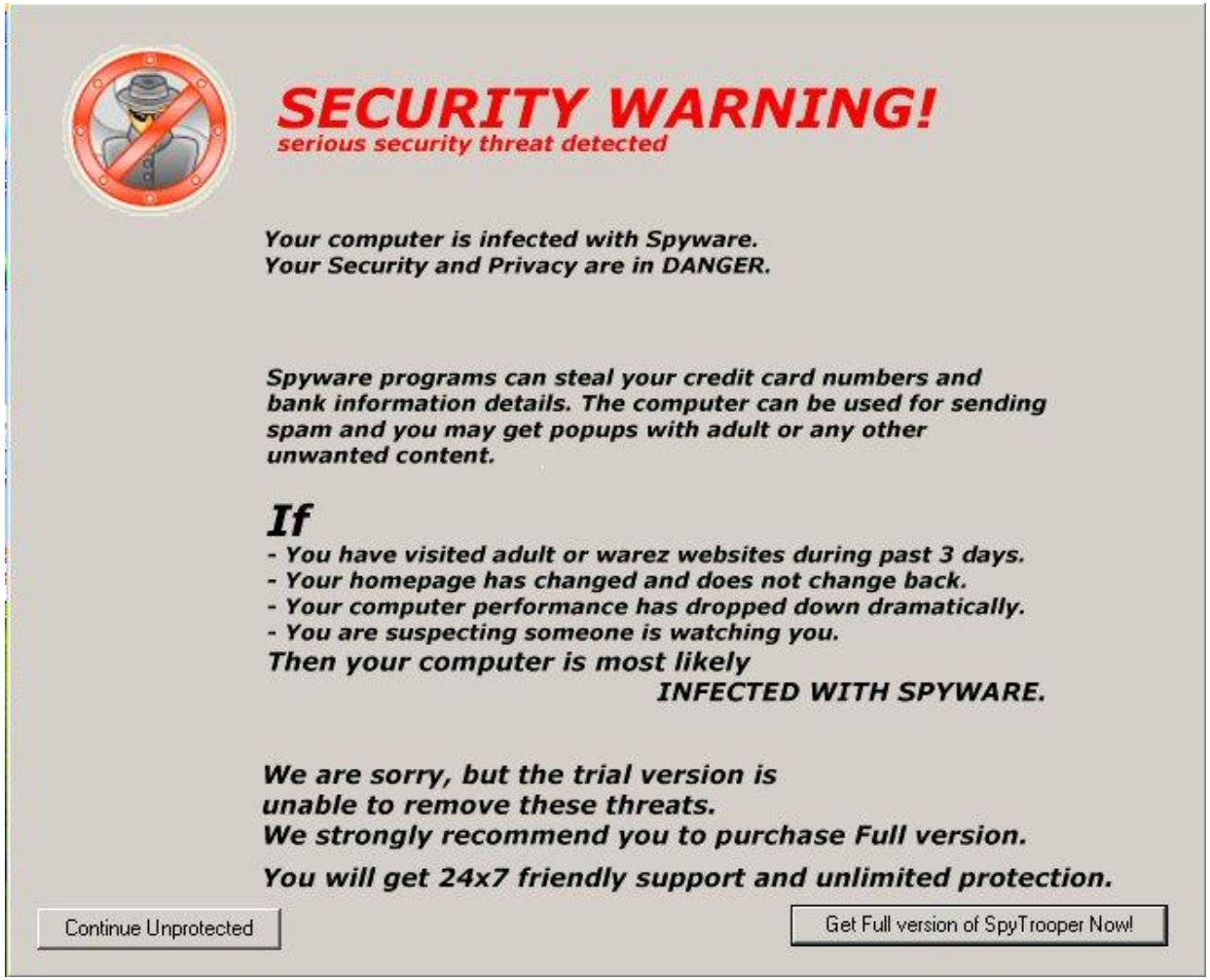
LightCodec


LightCodec
MEDIA SOFTWARE PACK
incredible video quality improvement
exceptional clear sound playback function
extremely reduces video files size
About Software:
LightCodec is a multimedia compressor/ decompressor which registers into the Windows collection of multimedia drivers and integrates with any application using Direct Show and Microsoft Video for Windows. LightCodec will highly increase quality of video files you play.
LightCodec enhances your music listening experience by improving the sound quality of video files sound, MP3, internet radio, Windows Media and other music files. Renew stereo depth, add 3D surround sound, restore sound clarity, boost your audio levels, and produce deep, rich bass sounds.
Click here to download latest version...
Download Codec:
LightCodec v 4.01a
LightCodec v3.05b is new generation multimedia compressor/ decompressor which registers into the Windows collection of multimedia drivers...
LightCodec v 3.0
Previous version of this revolutionary video compressor/decompressor software...
LightCodec v 1.04a
LightCodec Light v1.04a is light version of Codec v4.01a without sound compression features.

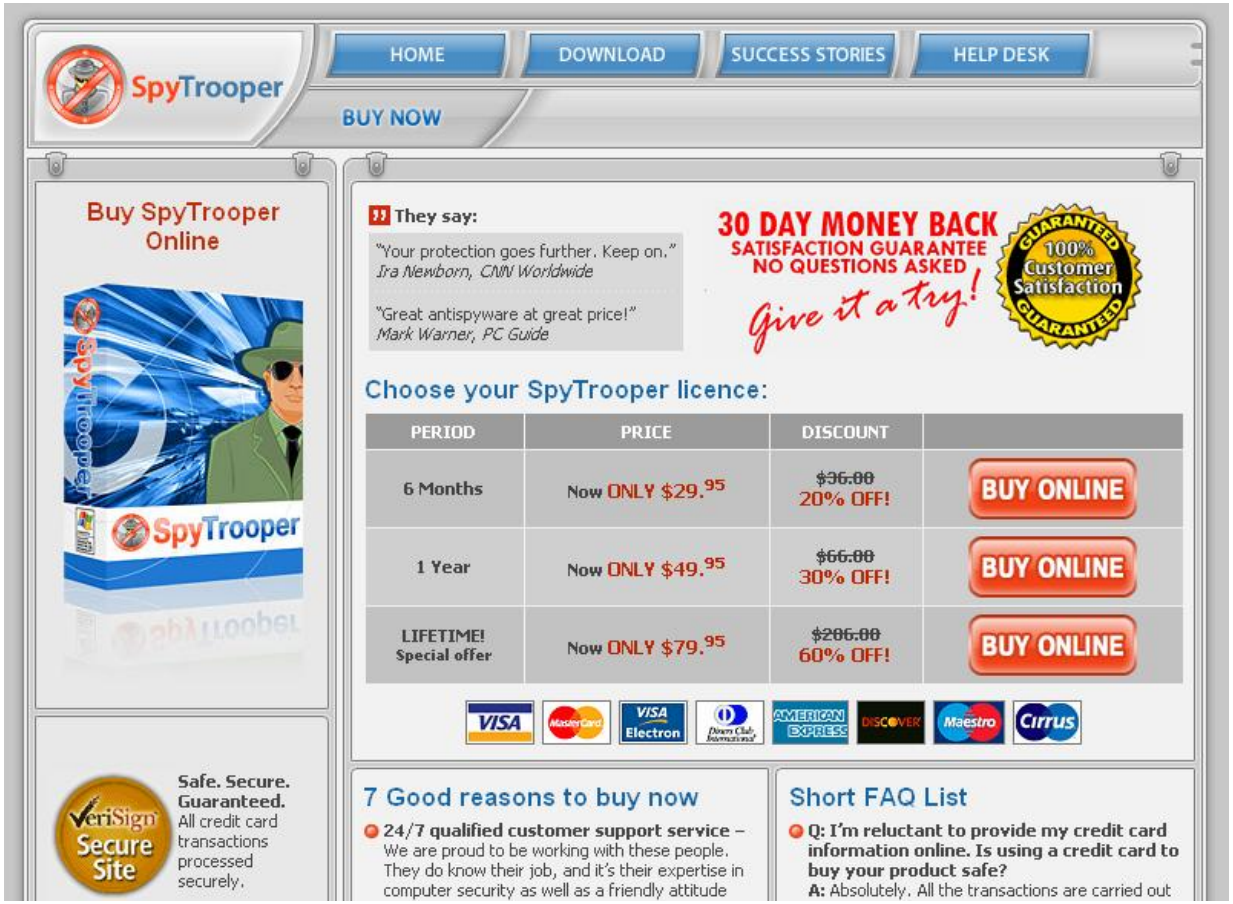
Hamis biztonsági alkalmazások



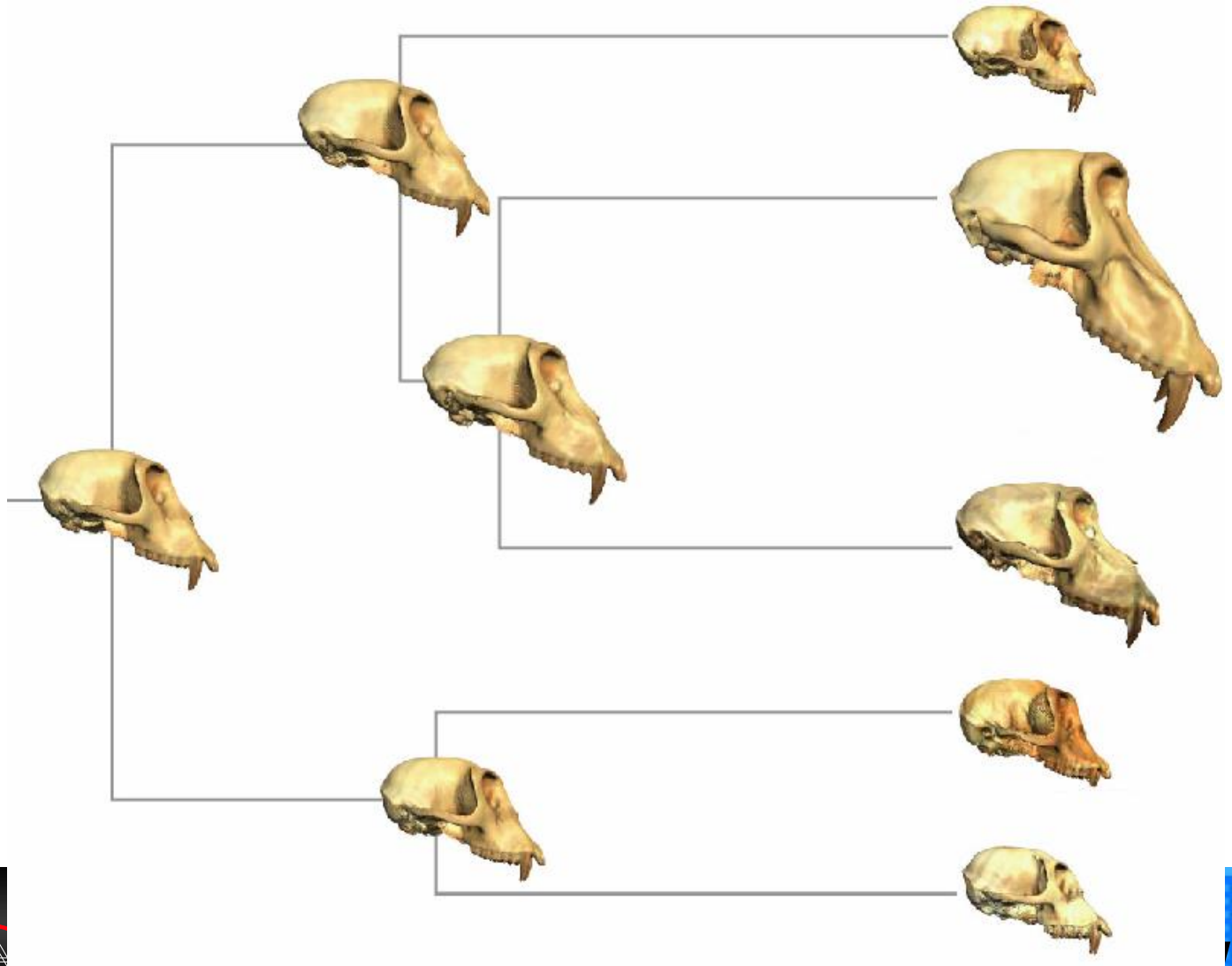
SpyTrooper


SECURITY WARNING!
serious security threat detected
Your computer is infected with Spyware.
Your Security and Privacy are in DANGER.
Spyware programs can steal your credit card numbers and bank information details. The computer can be used for sending spam and you may get popups with adult or any other unwanted content.
If
- You have visited adult or warez websites during past 3 days.
- Your homepage has changed and does not change back.
- Your computer performance has dropped down dramatically.
- You are suspecting someone is watching you.
Then your computer is most likely
INFECTED WITH SPYWARE.
We are sorry, but the trial version is unable to remove these threats.
We strongly recommend you to purchase Full version.
You will get 24x7 friendly support and unlimited protection.
Continue Unprotected
Get Full version of SpyTrooper Now!

SpyTrooper


SpyTrooper
HOME
DOWNLOAD
SUCCESS STORIES
HELP DESK
BUY NOW
Buy SpyTrooper Online
They say:
"Your protection goes further. Keep on."
Ira Newborn, CNN Worldwide
"Great antispyware at great price!"
Mark Warner, PC Guide
30 DAY MONEY BACK
SATISFACTION GUARANTEE
NO QUESTIONS ASKED
Give it a try!
100% Customer Satisfaction
Choose your SpyTrooper licence:
PERIOD
PRICE
DISCOUNT
6 Months
Now ONLY $29.95
$36.00
20% OFF!
BUY ONLINE
1 Year
Now ONLY $49.95
$66.00
30% OFF!
BUY ONLINE
LIFETIME!
Special offer
Now ONLY $79.95
$286.00
60% OFF!
BUY ONLINE
VISA
MasterCard
VISA Electron
Diners Club International
AMERICAN EXPRESS
DISCOVER
Maestro
Cirrus
VeriSign Secure Site
Safe. Secure. Guaranteed.
All credit card transactions processed securely.
7 Good reasons to buy now
24/7 qualified customer support service – We are proud to be working with these people. They do know their job, and it's their expertise in computer security as well as a friendly attitude
Short FAQ List
Q: I'm reluctant to provide my credit card information online. Is using a credit card to buy your product safe?
A: Absolutely. All the transactions are carried out

Morphing



I-Worm/Bagle (mutating)

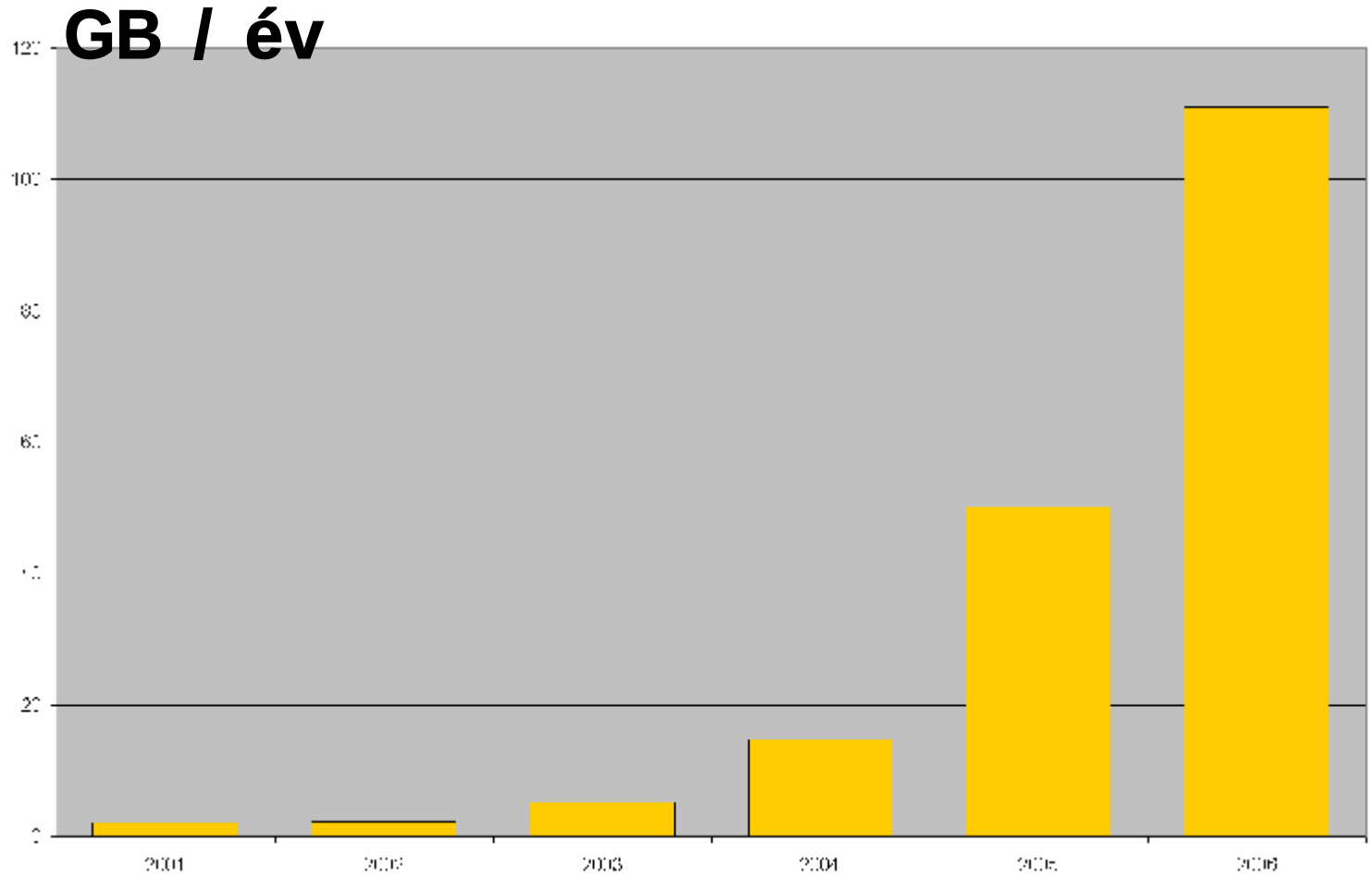
http://ala-bg.net/666.jpg
http://alevibirligi.ch/666.jpg
http://alfaclassic.sk/666.jpg
http://allanconi.it/666.jpg
http://allinfo.com.au/666.jpg
http://eleceltek.com/666.jpg
http://www.bbrealservis.sk/666.jpg
http://www.befag.ru/666.jpg
http://www.benininfo.com/666.jpg
http://www.bennylife.com/666.jpg
http://www.bestcheapdomainregistration.info/666.jpg
http://www.bidsforbaby.com/666.jpg
http://www.binhaigolf.com/666.jpg
http://www.bitsolution.ro/666.jpg
http://www.boldrussell.com/666.jpg
http://www.bronko-m.ru/666.jpg
http://www.bulkemaildirectmarketing.com/666.jpg
http://www.bulkemailservicenow.com/666.jpg
http://www.calidad.biz/666.jpg

Common Malware Enumeration

I-Worm/Generic.FX

ALWIL AVAST!	: Win32:VB-CD [Wrm]
H+BEDV AntiVir	: Worm/KillAV.GR
GRISoft AVG	: Worm/Generic.FX
Kaspersky Lab Kav	: Email-Worm.Win32.Nyxem.e
SOFTWIN BDC	: Win32.Worm.Tearec.A
Doctor Web DrWebWCL	: Win32.HLLM.Generic.391
Frisk FPCMD	: W32/Kapser.A@mm
McAfee Scan	: W32/MyWife.d@MM!M24
Fortinet Vscanner	: W32/Grew.A!worm
IKARUS PSCAN	: Email-Worm.Win32.VB.BI
Microsoft MP CL	: Win32/Mywife.E@mm!CME-24
Symantec SAVCLS	: W32.Blackmal.E@mm
ESET NOD32	: Win32/VB.NEI
Norman NVCC	: W32/Small.KI@mm
Panda	: W32/Tearec.A.worm!CME-24
Trend Micro VSCANTM	: WORM_NYXEM.E
Sophos SAV32CLI	: W32/Nyxem-D
CA VET RESCUE	: Win32/Blackmal.F!CME24
CA InoculateIT	: Win32/Blackmal.F!Worm
VirusBuster	: Worm.P2P.VB.CIL!CME-24

Összegyűjtött malware mennyiség



FOOLY

www.avg.hu

A felhasználók felelőssége

A felhasználók összetétele megváltozott

- **Mindenki számára elérhető Internet használat**
  - **Próbálkozások, tanulás - jó dolog!**
  - **kellő tudás és védelem nélkül**
- **Védelmi szoftverek vásárlása segíthet?**
  - **Tudatos felhasználói viselkedés nélkül nem nyújt magas szintű védelmet**

Téves beidegződések és elvárások

- **A tűzfal (személyi!) fontosságának túlhangsúlyozása**
  - **Az alap felhasználóinál magasabb szintű ismeretek szükségesek, ha nem csak varázslót szeretne használni**

- **Szerverekhez tervezett funkciók elvárása munkaállomásoknál**
  - **pld. öntanuló SPAM szűrő rendszer manuális taníthatósága**
  - **TERMÉSZETESEN MEGOLDOTT!! De gyakorlati jelentőssége csak a felhasználók töredékénél van, mivel több ezer spam és ham minta szükséges az eredményes tanításhoz.**

Hogyan választ a „laikus” felhasználó?


Vegyük meg a legolcsóbbat! Mint szükséges rossz…

Esetleg egy mindenható tűzfal…


Vegyük meg a legdrágább „mindent tudó” megoldást, mert az biztosan megvéd!

Milyen kérdéseket vet fel?

- **Kellő védelmet nyújt-e?**
- **Szükséges-e az adott esetre a vásárolt megoldás?**
- **Tudja-e majd kezelni a felhasználó?**

Kinek jó a nem átgondolt megoldás?

Van-e fontosabb, mint a vírusvédelem? J

- Jogtiszta termékek használata
- Biztonsági rések befoltozása
- Alapvető számítástechnikai ismeretek
- Alapvető biztonsági ismeretek
- Vírusok, rosszindulatú programok, kém és hirdetési programok, adathalászat és spam elleni védelem

Köszönöm a figyelmet!

Kérdések?