Mit is mondott? Hogy is hívják? Eligazodás a kártevők világában

Dr. Leitold Ferenc

Veszprémi Egyetem
Veszprog Kft.

fleitold@veszprog.hu

Mit is mondott? Hogy is hívják? Eligazodás a kártevők világában

Dr. Leitold Ferenc

Pannon

~~**Veszprémi**~~ **Egyetem**

Veszprog Kft.

fleitold@veszprog.hu

Tartalom

- Problémák
- Eddigi tevékenységek
- Elméleti vonatkozások
- Használható eszközök
- CheckVir Real-time AV teszt

A fő probléma …

Az antivírus fejlesztők különböző elnevezéseket használnak a kártevők azonosítására.

A felhasználók nem tudják, hogy melyik vírusról, féregről van szó.

A fő cél …

Azonos neveket kellene használni a vírusvédelmekben.

Definicíós probléma

Mit nevezünk “azonos kártevőnek” ?

Nehéz definiálni!

Speciális esetek:

- **makró vírusok**
  - **VBA konverzió újabb vírusokat hoz létre**
- **jelszóval tömörített férgek**
  - **felhasználói beavatkozás szükséges**

Eddigi tevékenységek

EICAR

http://www.eicar.org/camdier/index.html

The CAMDIER project is made up of firms and academic institutions from various countries, as well as non-profit organizations. The Consortium represents a public-private initiative (e.g., public is represented during beta tests through such groups as Cyberworld Awareness and Security Enhancement Structure [CASES]).

CAMDIER brings together people from various disciplines, organisations and countries within the EU to move a step forward in anti-virus research and defence efforts. The consortium firmly believes that in order to achieve progress in this area, a major project bringing together people from various disciplines, organisations and countries within the EU is imperative.

2. What are the Major Objectives of CAMDIER?

CAMDIER has the following strategic objectives:

- develop a Framework for the Classification and Categorization of various types of attacks;
- develop a Unified Naming Convention;
- develop tools using heuristics and other technologies to automatically, or at least, semi-automatically classify and categorize known and yet unknown viruses and malicious code;
- to use knowledge management techniques for diffusing information to various stakeholder groups and networks such as CASES (Cyberworld Awareness and Security Enhancement Structure). It also intends to reach out to users and vendors (e.g. EICAR's members and working groups), home users (e.g. Internet Society- ECC), students and academia (TERENA), as well as Telecities and Global Cities in order to increase citizens' trust and confidence in local e-government efforts;
- to reduce the time lag between discovery of a malicious code attack on an organization's system and the possible measures that can be used to limit potential damages; and,
- to achieve research synergies with CAMDIER that support system architectures envisioned by CASES, Telecities and the Nordic security network group (established by IT/telecom ministers) and which work towards greater collaboration amongst Member and Baltic states with respect to improving information technology (IT) security.

Graphically, CAMDIER, a STREP project of 36 month duration, can be depicted as follows:

figure 1 (6 kBytes)

Figure 1. Simplified research process, results and deliverables/outcomes from CAMDIER.

Eddigi tevékenységek

US CERT

november 24, 2004 (1:37 DU EST)

Order To Come To Virus Naming Chaos

By TechWeb News

US-CERT, the federally-funded security clearinghouse, will try to put some order to the often-chaotic naming of worms and viruses in early 2005, the organization wrote in a letter sent to a security research group Tuesday.

Virus and worm nomenclature is typically left up to the security vendor which first discovers the malware. Until 2004 the process worked, more or less.

But the large scale and rapid release of multiple variants of worms in the Netsky and Bagle and MyDoom families this year led to confusion, with firms out of sync in their naming. One vendor would tag a new Bagle as Bagle.w, for instance, while others would call it Bagle.u or Bagle.t.

Most recently, confusion reigned when some security firms gave a worm an entirely new name -- "Bofra" -- while others claimed that it was only a variation of the long-running MyDoom.

"As a 'neutral third party' in the marketplace, US-CERT will coordinate with security vendors to implement a CME [Common Malware Enumeration] malware identification scheme," members of US-CERT's CEM initiative wrote in a letter to the SANS Institute's Internet Storm Center. "Limited operational capability is expected first quarter, 2005; this phase will concentrate on the most important threats, including the recent Beagle/Bagle variants."

Although there are obstacles to a common naming process -- including time constraints as anti-virus vendors rush to identify a worm and produce a defense against it -- US-CERT believes it's for the common good.

"Once all parties adopt a neutral, shared identification method, effective information sharing can happen faster and with more accuracy, making it easier to distinguish between very similar threats," the group wrote.

VESZPROG

Eddigi tevékenységek

CME – Common Malware Enumeration

CME Editorial Board

The CME Editorial Board includes members from the international anti-virus community, including product vendors, testing organizations, and government. The Board approves which threats are assigned CME identifiers for publication on the CME Web site and oversees all content updates on the CME List. Many Board members also act as members of the CME Sample Redistribution Group, discovering and submitting possible threats for inclusion on the list.

The MITRE Corporation and US-CERT created the CME Editorial Board, moderate Board discussions, and provide guidance throughout the process to ensure that CME serves the public interest. Other anti-virus and information security experts will be invited to participate on the Board on an as-needed basis based upon recommendations from Board members.

CME Editorial Board Members

Arbor Networks
Computer Associates International, Inc.
F-Secure Corporation
ICSA Labs
Kaspersky Lab
McAfee, Inc.
MessageLabs Ltd.
Microsoft Corporation
Norman ASA
Panda Software International S.L.
Sophos, Plc
Symantec Corporation
Trend Micro, Inc.

MITRE (Moderator)

US-CERT (Sponsor)

Eddigi tevékenységek

CME – Common Malware Enumeration

CME Editorial Board

The CME Editorial Board includes members from the international anti-virus community, including product vendors, testing organizations, and government. The Board approves which threats are assigned CME identifiers for publication on the CME Web site and oversees all content updates on the CME List. Many Board members also act as members of the CME Sample Redistribution Group, discovering and submitting possible threats for inclusion on the list.

The MITRE Co
provide guidar
and informatic
upon recomme

CME Editori

Arbor Networ
Computer Ass
F-Secure Corp
ICSA Labs
Kaspersky La
McAfee, Inc.
MessageLabs
Microsoft Cor
Norman ASA
Panda Softwa
Sophos, Plc
Symantec Co
Trend Micro,

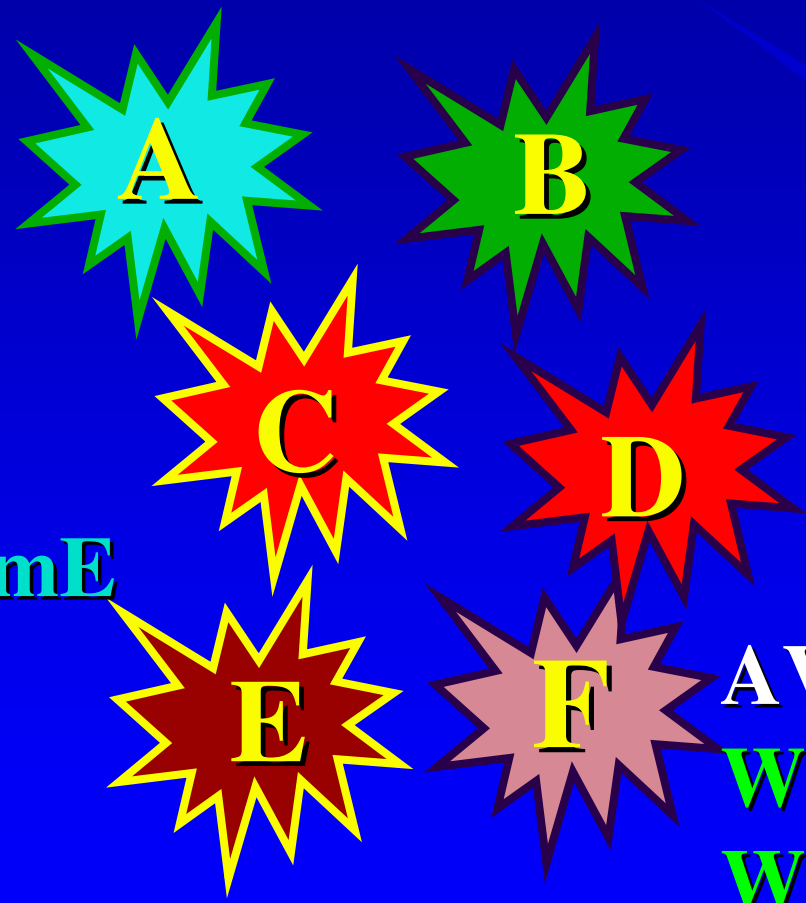
CME-ID	Aliases	Description	Date Assigned
CME-934	*Aladdin Knowledge Systems*: Win32.Agent.adu *Authentium*: W32/Downloader.SEL@dl *Avira*: TR/Dldr.Small.NIH *CA*: Win32/Clagger.Q *ClamAV*: Trojan.Downloader.Small-1133 *ESET*: Win32/TrojanDownloader.Small.NIH *Fortinet*: W32/Small.NIJ!dldr *Grisoft*: Generic.QYK *H+BEDV*: TR/Dldr.Small.NIH *iDefense*: Agent.ACX *Kaspersky*: Trojan-Downloader:Win32.Agent.adu *McAfee*: Downloader-ATM!CME-934 *Microsoft*: TrojanDownloader:Win32/Clagger.C!CME-934 *Norman*: W32/Clagger.C *Panda*: Trj/Nabload.CC!CME-934 *Sophos*: Troj/Clagger-K *Symantec*: PWSteal.Tarno.T *Trend Micro*: TROJ_CLAGGER.D	This is small Trojan downloader that downloads files and lowers security settings. It is spreading as an email attachment.	2006-03-20

Elméleti vonatkozások

VESZPROG

AV1:

W32/virA
W32/virB
W32/virC
W32/virD
Worm/wormE
W32/virF



AV2:

Win32.blue
Win32.green
Win32.red
I-Worm.brown
Win32.pink

AV3:

Win32.greenoutline
Win32.blackoutline
Win32.yellowoutline

Következmények

1. Az elnevezések puszta cseréje LEHETETLEN!

2. A neveket lehetne szinkronizálni, azonban ez azt is jelenti, hogy a felismerési algoritmusokat is szinkronizálni kellene.

3. Az elérhető megoldás egy megfelelő névazonosítási szolgáltatás.

Használható eszközök

Virus Bulletin - VGREP

Terms: Netsky.X Match **Whole String**: ☐

Search by **Vendor**: Any Search

Results

Results: 1-5, 6-10, 11-14

ALWIL	[undetected]	*H+BEDV*	[undetected]
GRISoft	[undetected]	*Kaspersky Lab*	Email-Worm.Win32.NetSky.x
SOFTWIN	Win32.Netsky.W@mm.Damaged	*Doctor Web*	Win32.HLLM.Netsky.based
Frisk Software	W32/Netsky.W@mm	*McAfee*	W32/Netsky.w@MM
IKARUS	Email-Worm.Win32.Netsky.X	*MKS*	[undetected]
Symantec	[undetected]	*ESET*	[undetected]
Norman	Netsky.W@mm	*Panda*	W32/Netsky.W.worm
Trend Micro	WORM_NETSKY.W	*GeCAD RAV*	Win32/Netsky.W@mm
Sophos	W32/Netsky-N	*CA VET*	[undetected]
CA InoculateIT	Win32/NetSky.W.ZIP!Worm	*VirusBuster*	[undetected]

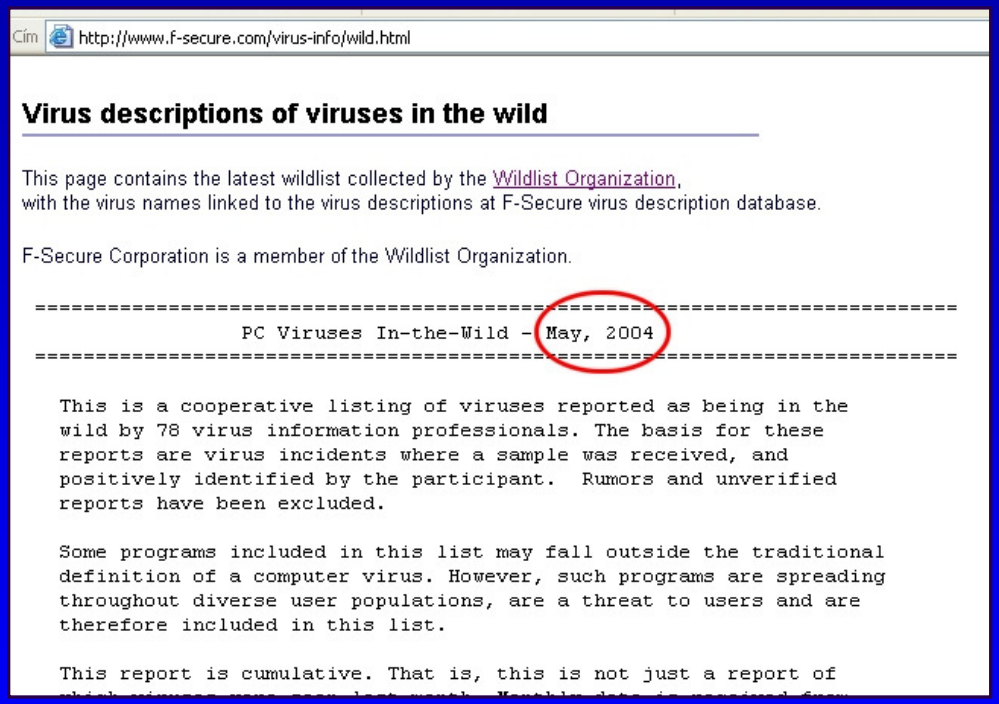
ALWIL	[undetected]	*H+BEDV*	[undetected]
GRISoft	I-Worm/Netsky.X	*Kaspersky Lab*	Email-Worm.Win32.NetSky.y
SOFTWIN	Win32.Netsky.Y@mm	*Doctor Web*	Win32.HLLM.Netsky.based
Frisk Software	[undetected]	*McAfee*	W32/Netsky.x@MM
IKARUS	Email-Worm.Win32.Netsky.Y	*MKS*	[undetected]
Symantec	W32.Netsky.gen@mm	*ESET*	Win32/Netsky.X
Norman	[undetected]	*Panda*	W32/Netsky.X.worm
Trend Micro	WORM_NETSKY.GEN	*GeCAD RAV*	Win32/Netsky.X@mm
Sophos	W32/Netsky-Y	*CA VET*	Win32.Netsky.gen
CA InoculateIT	Win32/Bagle.Variant!Worm	*VirusBuster*	[undetected]

Használható eszközök

Wildlist

Használható eszközök

Wildlist


Cím http://www.f-secure.com/virus-info/wild.html

Virus descriptions of viruses in the wild

This page contains the latest wildlist collected by the Wildlist Organization,
with the virus names linked to the virus descriptions at F-Secure virus description database.

F-Secure Corporation is a member of the Wildlist Organization.

==========

PC Viruses In-the-Wild - May, 2004

==========

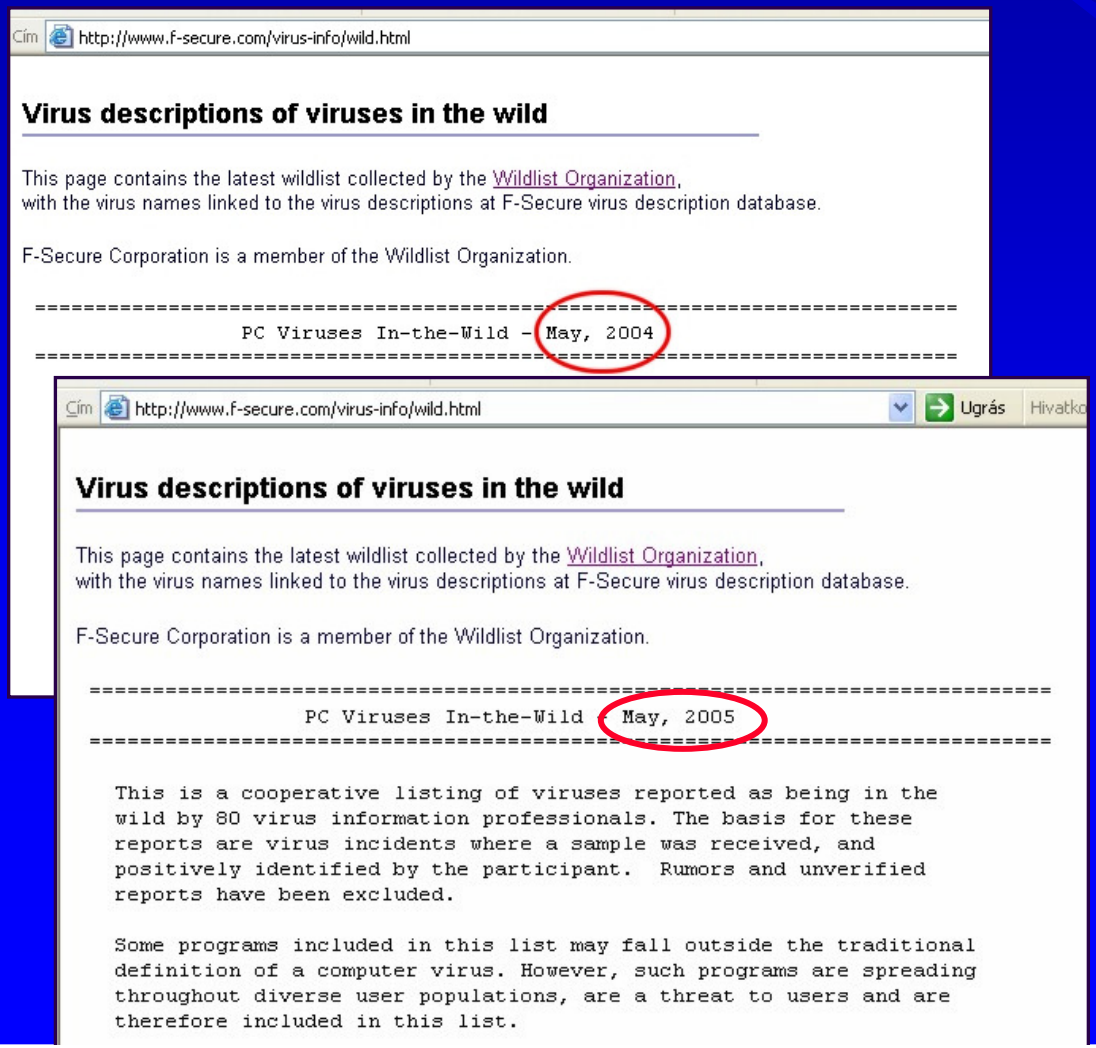
This is a cooperative listing of viruses reported as being in the wild by 78 virus information professionals. The basis for these reports are virus incidents where a sample was received, and positively identified by the participant. Rumors and unverified reports have been excluded.

Some programs included in this list may fall outside the traditional definition of a computer virus. However, such programs are spreading throughout diverse user populations, are a threat to users and are therefore included in this list.

This report is cumulative. That is, this is not just a report of

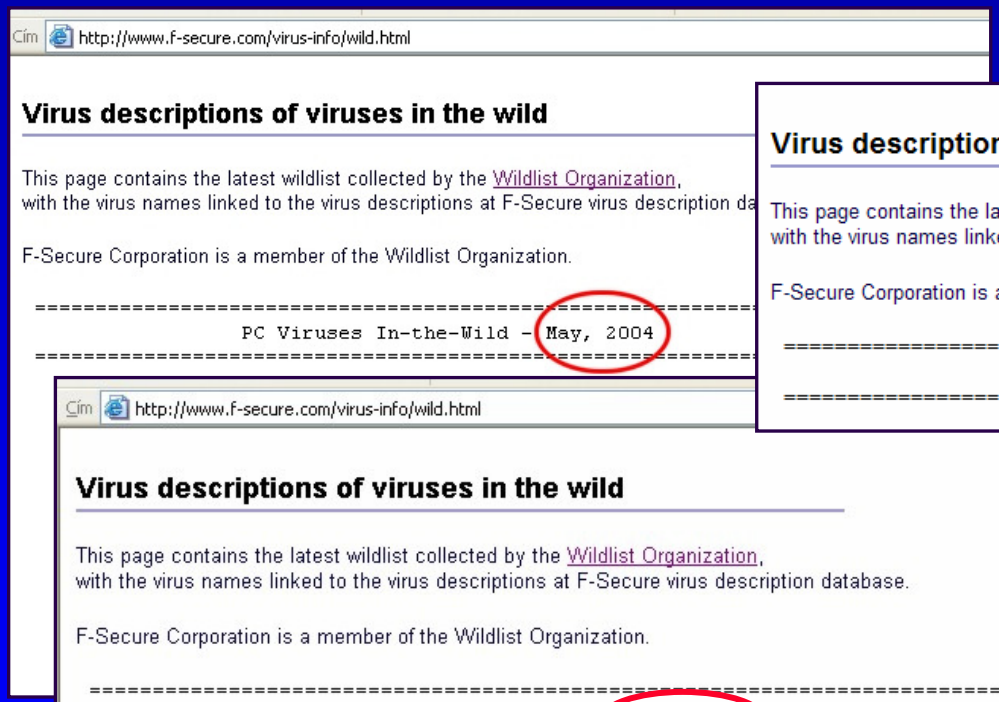
Használható eszközök

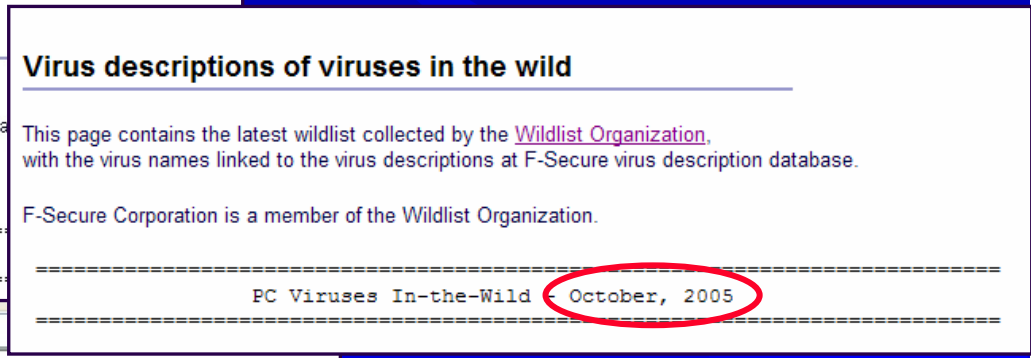
Wildlist



Használható eszközök

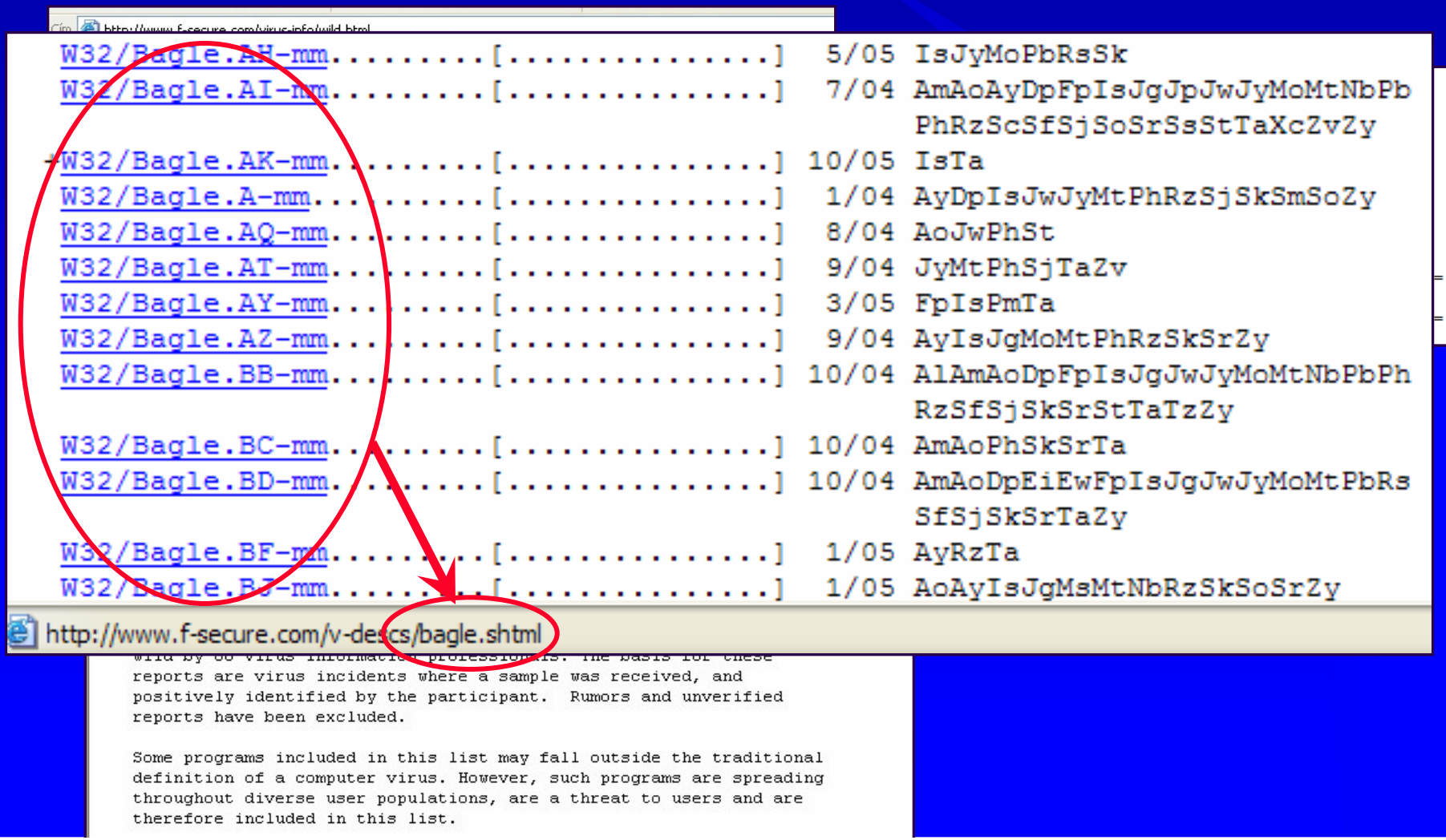
Wildlist





Használható eszközök

Wildlist



Eddigi tevékenységek

CME – Common Malware Enumeration

CME Editorial Board

The CME Editorial Board includes members from the international anti-virus community, including product vendors, testing organizations, and government. The Board approves which threats are assigned CME identifiers for publication on the CME Web site and oversees all content updates on the CME List. Many Board members also act as members of the CME Sample Redistribution Group, discovering and submitting possible threats for inclusion on the list.

The MITRE Co
provide guidar
and informatic
upon recomme

CME Editori

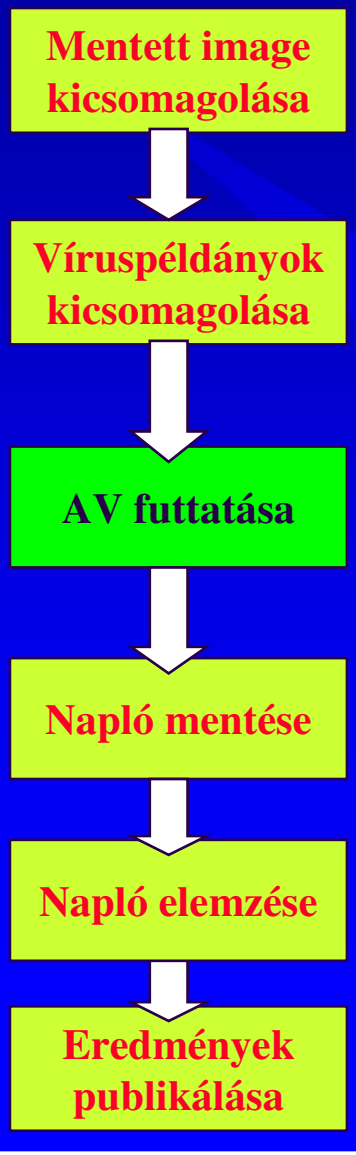
Arbor Networ
Computer Ass
F-Secure Corp
ICSA Labs
Kaspersky La
McAfee, Inc.
MessageLabs
Microsoft Cor
Norman ASA
Panda Softwa
Sophos, Plc
Symantec Co
Trend Micro,

CME-ID	Aliases	Description	Date Assigned
CME-934	*Aladdin Knowledge Systems*: Win32.Agent.adu *Authentium*: W32/Downloader.SEL@dl *Avira*: TR/Dldr.Small.NIH *CA*: Win32/Clagger.Q *ClamAV*: Trojan.Downloader.Small-1133 *ESET*: Win32/TrojanDownloader.Small.NIH *Fortinet*: W32/Small.NIJ!dldr *Grisoft*: Generic.QYK *H+BEDV*: TR/Dldr.Small.NIH *iDefense*: Agent.ACX *Kaspersky*: Trojan-Downloader:Win32.Agent.adu *McAfee*: Downloader-ATM!CME-934 *Microsoft*: TrojanDownloader:Win32/Clagger.C!CME-934 *Norman*: W32/Clagger.C *Panda*: Trj/Nabload.CC!CME-934 *Sophos*: Troj/Clagger-K *Symantec*: PWSteal.Tarno.T *Trend Micro*: TROJ_CLAGGER.D	This is small Trojan downloader that downloads files and lowers security settings. It is spreading as an email attachment.	2006-03-20

Real-time AV teszt

- Folyamatos AV teszt (majdnem minden verzió)
  - új kártevő megjelenésekor
  - új AV verzió megjelenésekor
- Az elterjedt kártevők vizsgálata
  - > folyamatos bővítés
- Felismeri? Gyanúsítja? Milyen néven/neveken?

Real-time AV teszt folyamata



VESZPROG

Real-time AV teszt kimenete

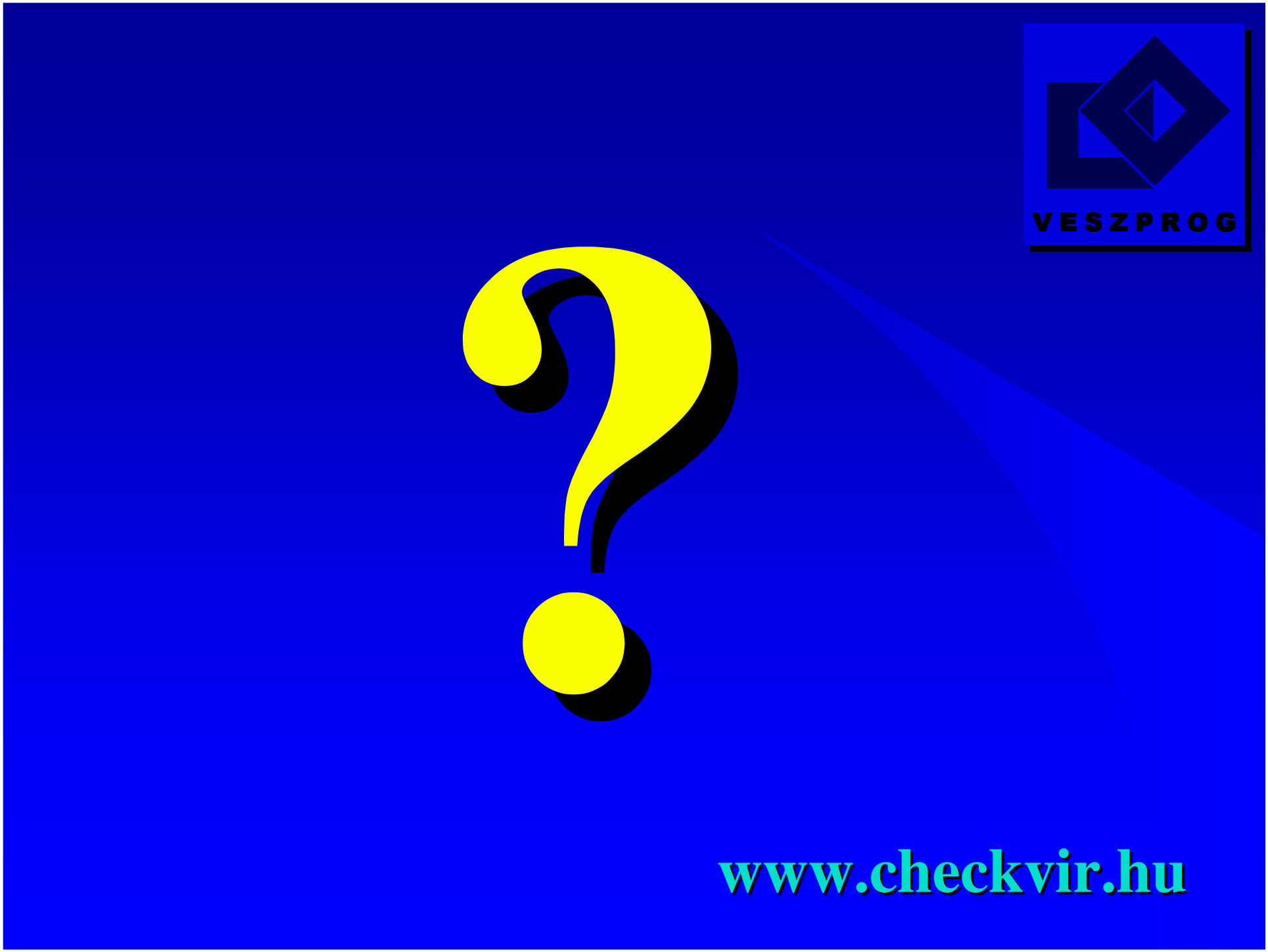
W32/Zafi.A

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

Real-time AV teszt kimenete

- **Kártevők nevei antivírus verziónként**
  - **> ki volt a gyorsabb ?**
- **Alapvető működési tulajdonságok**
  - **tömörítők, beágyazások, speciális formátumok ismerete**
  - **tárolómappák kezelése**
  - **eltávolítási eljárások (törlés, visszaállítás, …)**
  - **heurisztikus képesség**


VESZPROG
?
www.checkvir.hu