Mi újság a vírusfronton ?

2005. március 29.

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

Tartalom

- Vírusok a spamküldés szolgálatában
- Kéretlen levelek antivírusoktól
- Elnevezések problémája
  - > CheckVir Real-time AV test

Ki írta a Sobig-ot?

Who Wrote Sobig?

Version 1.0: 19-August-2003.
Version 1.1: 25-August-2003.
Version 1.2: 19-November-2003.
Version 1.3: 17-July-2004. This sanitized variation for public release.
Scheduled for release: 1-November-2004.

Ki írta a Sobig-ot?

Who Wrote Sobig?

Version 1.0:
Version 1.1:
Version 1.2:
Version 1.3:

This document is
The PGP key incl

Who Wrote Sobig? Copyright 2003-2004 Authors

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP

mQGiBEF5UyURBACZ9jsrBaowh4npI0ac84RVD9fzzR9oW9x4TkfPN1ddzzR4uhko
CsKUK9IfeEz7C6a6pMKbwB83xjBedhjRE5zMfgns4kSY33XJirGzRHWXWbD7n1zn
WFfq84VBCezDmUy6cy4+zipQDyPYs+u8YfCMUfS2XCHXwD8lqg5jvIzsiwCglpkp
z4+xlqvUrVNIkJlxeYzbDOsD/3Y/DHvNmNa8LGKTyF7KFgD5TTBSnPW5tpzdXkcp
+UVg09A6qHagx90LGOA610P8oOJYPGaCvuQV7Br2zqqAw5PUouwxPPJTsWrmU25N
lQ83jf8WaJTvU46/TXg8H+ctKeCLa4R6h4+dDkRjxSeKMuGbK8yZAVOv+VkANRci
sFumA/sHb/+owmRRn0rO6xSz0HDOzJNNCR3ghZ4M+hl3o7Ll4FCYVir2pWeoeWKH
```

Ki írta a Sobig-ot?

VESZPROG

2 Overview

Sobig was a virus specifically designed to aid the anonymity of spammers. Sobig opened up services that enabled spammers to relay their emails anonymously. Although publicly the motivation and author of the Sobig virus is unknown, through the use of forensics and profiling, we have identified a very likely suspect and motive.

Our research indicates that Ruslan Ibragimov of Moscow, Russia, and/or Ibragimov's development team, authored the Sobig virus. Ibragimov himself is the author of Send-Safe, a bulk mailing tool product that was explicitly designed for sending unsolicited email (spam).

Send-Safe/SSSG és Sobig verziók

		own proxies. Major registration charge if Send-Safe provides proxies.
Send-Safe 2.13	5/18/2003	Compiled on May 18, 2003. **Supports more proxy types**. (HTTP, HTTPS, Socks, etc.)
Sobig-B	5/18/2003	Compiled on May 16, 2003. Deactivates May 31, 2003. Executable packaged with UPX. Believe to be the first non-proof-of-concept release. Release correlates with Send-Safe 2.13 release. Provides **many types of proxies**, most (all?) are supported by Send-Safe 2.13, but not supported by Send-Safe 2.09.
Send-Safe 2.14	5/30/2003	Compiled on May 30, 2003. New registration system. All proxies found by Send-Safe proxy scanner are now sent to a central Send-Safe server for all users. **More complex encryption system** for transferring the proxy list.
Sobig-C	5/31/2003	Compiled on May 30, 2003. Deactivates June 8, 2003. Executable packaged with UPX. **More complex encryption system**. Release correlates with Send-Safe 2.14 release.
Sobig-D	6/18/2003	Deactivates July 2, 2003. Believed to be a premature release or a test due to limited spread and overlapping expiration date with Sobig-E. Sobig-D used the same ports as the previous Sobig releases.
SSSG	6/18/2003	SSSG observed relaying through a system with ports **2280-2285** open.
Sobig-E	6/25/2003	Compiled on June 24, 2003. Deactivates July 14, 2003. Executable packaged with tElock. Proxy ports changed to 1555, 2001, and **2280-2285**.
Send-Safe 2.14	6/28/2003	Web page updated. Re-release of the same code; no code change.
SSSG	7/1/2003	SSSG is observed using a new, unreleased version of Send-Safe. This version is believed to be a pre-release of Send-Safe 2.16, possibly 2.15.
SSSG	8/9/2003	SSSG observed relaying through a system with ports **3380-3385** open. The open services match Sobig-F.
Sobig-F	8/18/2003	Compiled August 17, 2003, public announcements 2 days later. Deactivates September 10, 2003. Executable packaged with tElock. Includes encrypted command structure and remote control. The proxy ports changed to 2555, 3001, and **3380-3385**.
SSSG	9/30/2003	SSSG is observed using a new, unreleased version of Send-Safe. This version is later

E-mail fejlécek

Send-Safe 2.14 email header	Sobig-F email header
Message-ID: <036a55d03c4c$8127a7d8$6bc21ae1@hhutma> From: <alastairbaileymf787@flash.net> To: <*user@domain*> Subject: **You're ~Approved~* Date: Wed, 26 Mar 2003 13:21:50 -0000 MIME-Version: 1.0 Content-Type: multipart/mixed; boundary="----=_NextPart_000_00B0_40A21C5D.D8133A18" X-Priority: 3 (Normal) X-MSMail-Priority: Normal X-Mailer: QUALCOMM Windows Eudora Version 5.1 Importance: Normal	From: <info@nofear.ch> To: <*user@domain*> Subject: Thank you! Date: Tue, 26 Aug 2003 14:29:47 --0400 X-MailScanner: Found to be clean Importance: Normal X-Mailer: Microsoft Outlook Express 6.00.2600.0000 X-MSMail-Priority: Normal X-Priority: 3 (Normal) MIME-Version: 1.0 Content-Type: multipart/mixed; boundary="_NextPart_000_0661EBB9"

Programozási stílus

5.3.2 Similar: Coding Conventions

The Sobig malware has a significant number of coding conventions that are very similar to Send-Safe:

- **String concatenations**. The Sobig virus uses static email header values, i.e. the string "X-Mailer: Microsoft Outlook Express 6.00.2600.0000" does not vary. Although the string is static, the code that generates it concatenates two independent strings: "X-Mailer: " and "Microsoft Outlook Express 6.00.2600.0000". The concatenation suggests that the developer reused code with a static value ("Microsoft...") rather than simply encoding the entire static string.

  The majority of bulk mailing tools concatenate the field and value pairs like Sobig. Send-Safe uses a concatenation function to combine the header information with the dynamic value strings. This suggests that Sobig used existing code for generating an email header, and then modified it to concatenate static strings rather than simply hard-coding the static header values.

- **Use of "%s"**. When concatenating strings, there are many different approaches that can be used, i.e. a C++ programmer can use "." or "+" for concatenation, or the old-style C notation "%s". There are also string concatenation functions such as 'strcat()'.
  - When generating the email header, both Send-Safe and Sobig do not use "%s" to concatenate strings. But, when establishing a connection to an email server (SMTP connection), both Send-

Motiváció

5.4 Motive to Write Sobig

Senders of spam typically relay their email messages through open proxy servers in a continuing effort to obscure the true sending host. With the proliferation of blacklists and other anti-spam systems, spam senders are finding it more and more difficult to locate available open proxy servers. By opening multiple proxy services on millions of compromised systems, a spam sender could very quickly and anonymously relay messages without the fear of being identified.

Sobig provides the following two benefits for spam senders:

1. Sobig opens multiple proxy servers on systems that are not blacklisted;
2. Sobig spreads very quickly, infecting and re-infecting millions of systems in under a week.

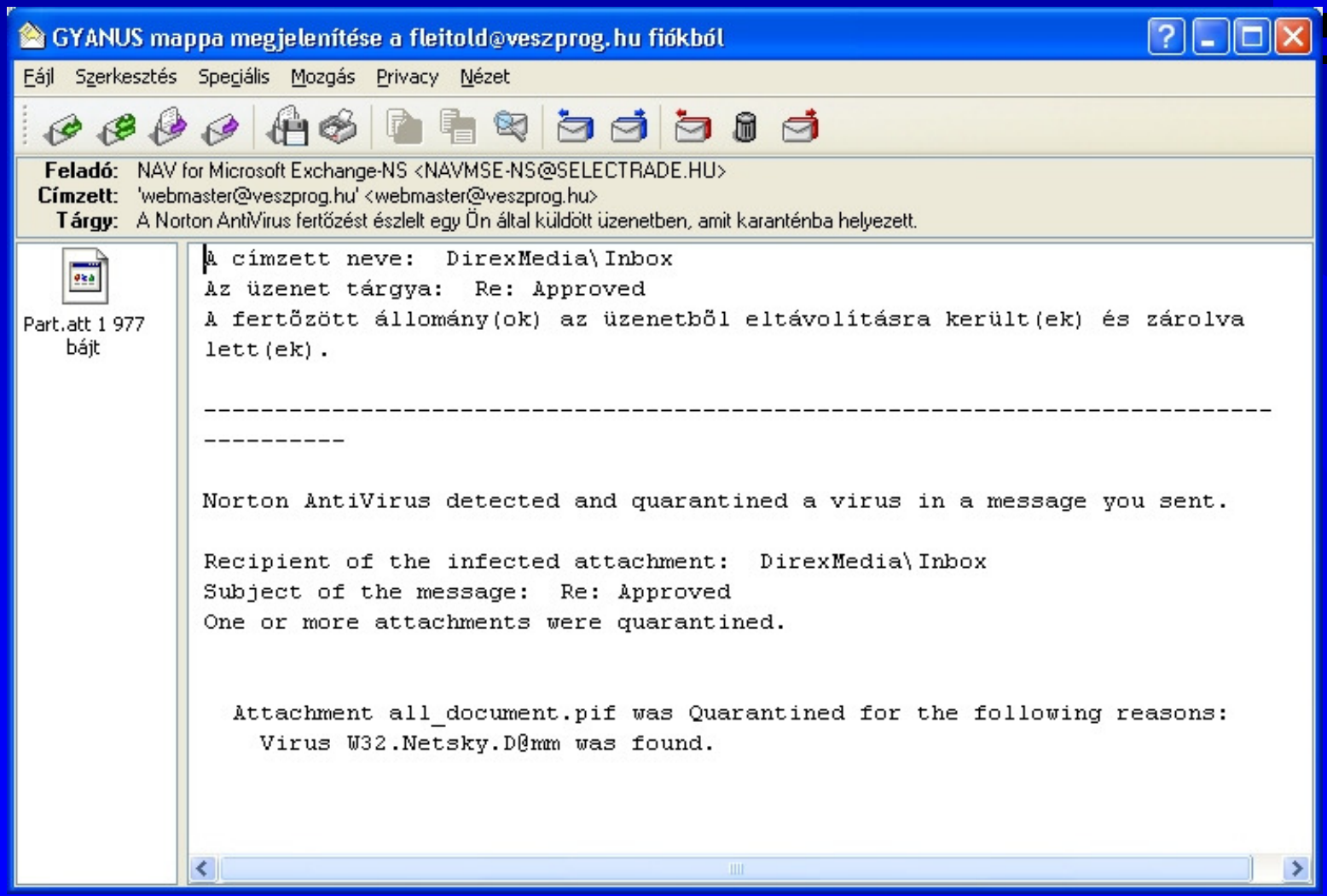
These benefits provide spam senders with a very large base of open proxy servers. Even though most of the infected systems will be cleaned within a week, there will be some systems that will remain infected to continually provide open proxies for weeks or even months.

We believe that Sobig was most likely written to support spam software. Any user or developer of spam mailing software, including Ruslan Ibragimov and Send-Safe, would be financially eager to leverage malware such as Sobig.

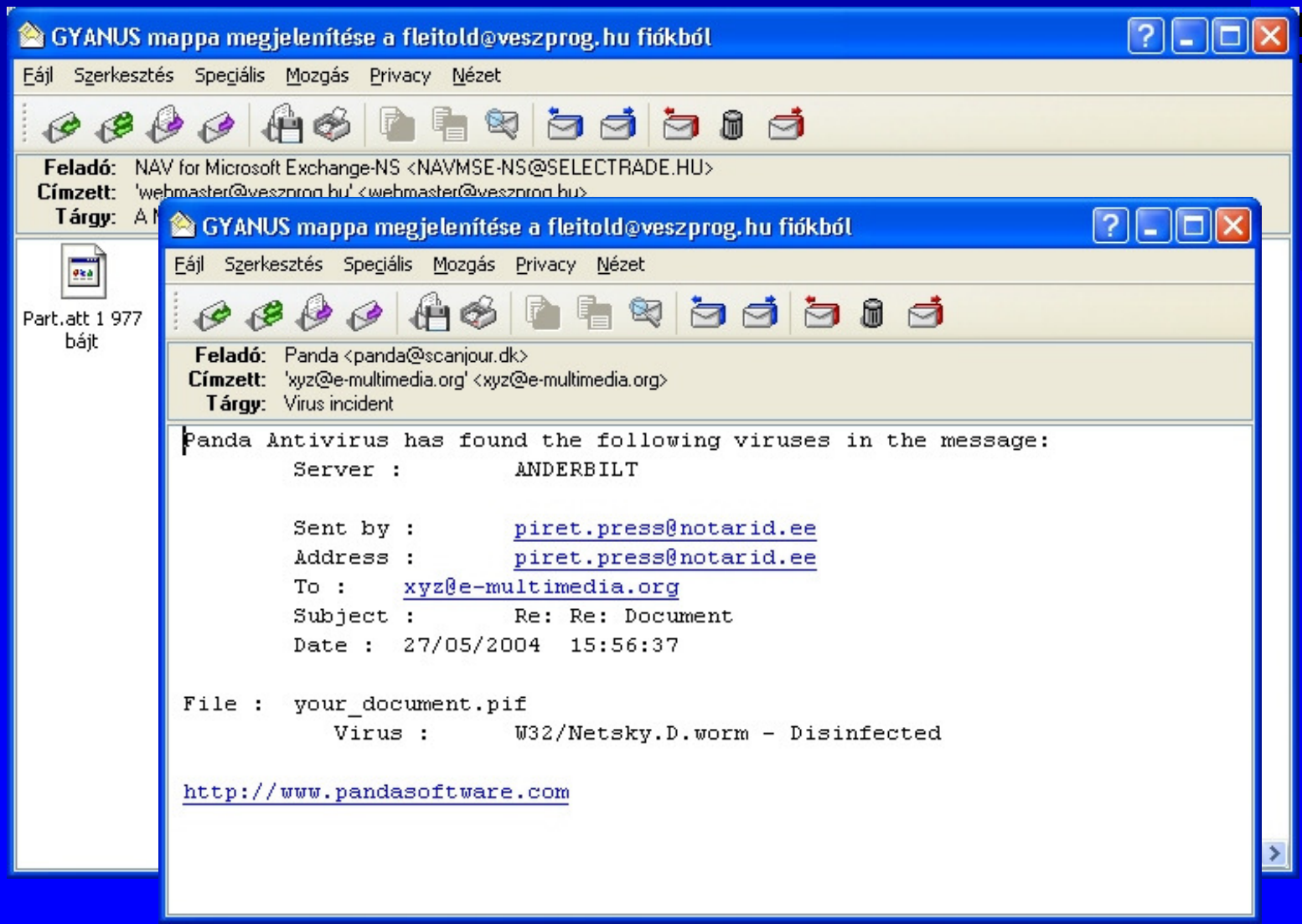
Kód-összehasonlítás

Kéretlen levelek antivírusoktól

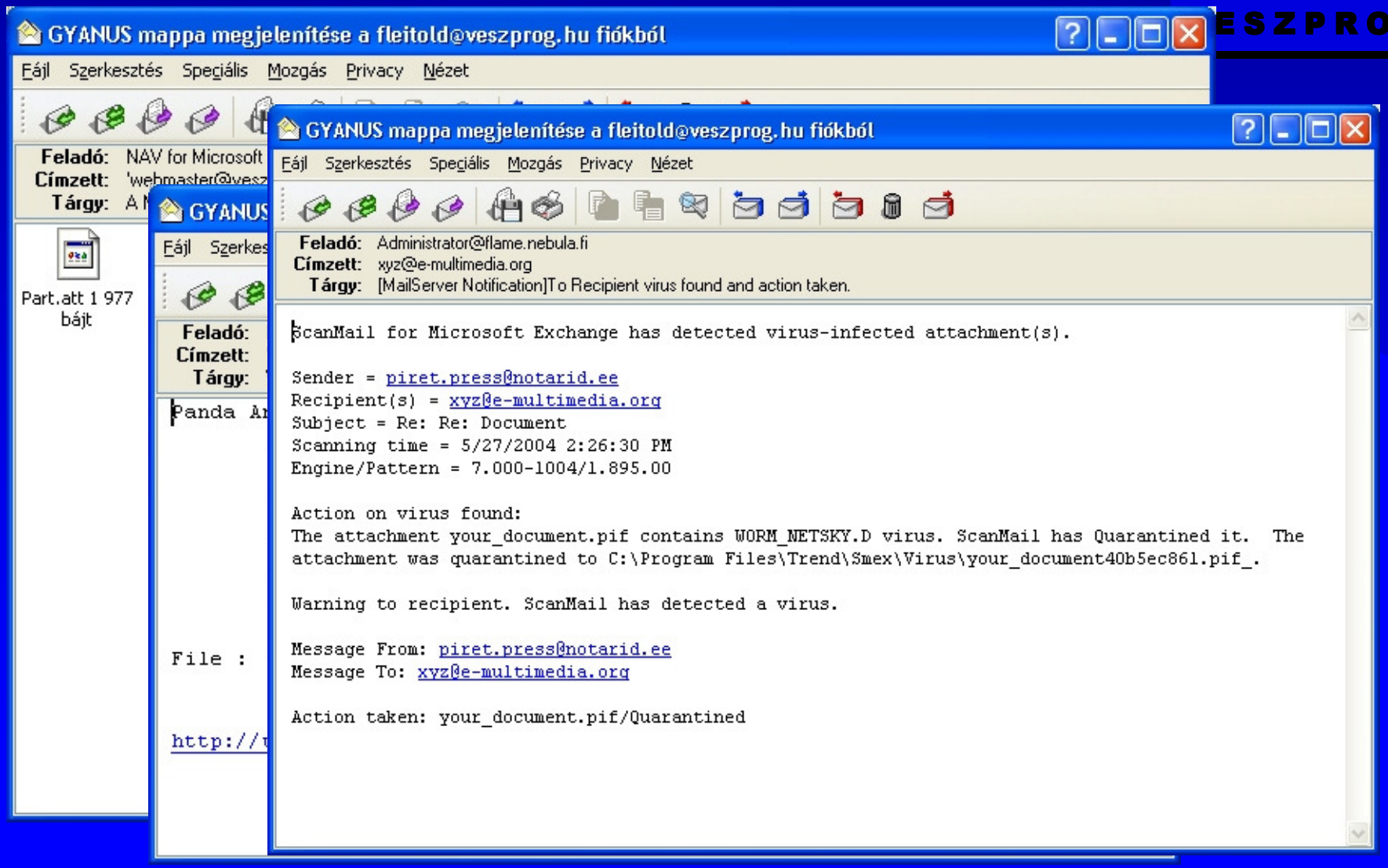
Kéretlen levelek antivírusoktól



Kéretlen levelek antivírusoktól



Kéretlen levelek antivírusoktól



Elnevezések problémája

- “Ahány ház, annyi szokás!”
- Azonos nevek használata megoldhatatlan
  - Több, mint 100.000 kártevő
  - Felismerési és azonosítási algoritmusok nem minden esetben felelnek meg egymásnak
- Probálkozások:
  - EICAR
  - CERT USA
- Cross-reference
  - VGREP project (Virus Bulletin)
  - CheckVir Real-time AV test

Real-time AV test

- Folyamatos AV tesztelés (minden verzió)
  - új vírus megjelenésekor
  - új antivírus megjelenésekor
- Elterjedt vírusokkal szemben
  - > folyamatosan bővül
- Felismeri-e? Ha igen, milyen néven?

Real-time AV test

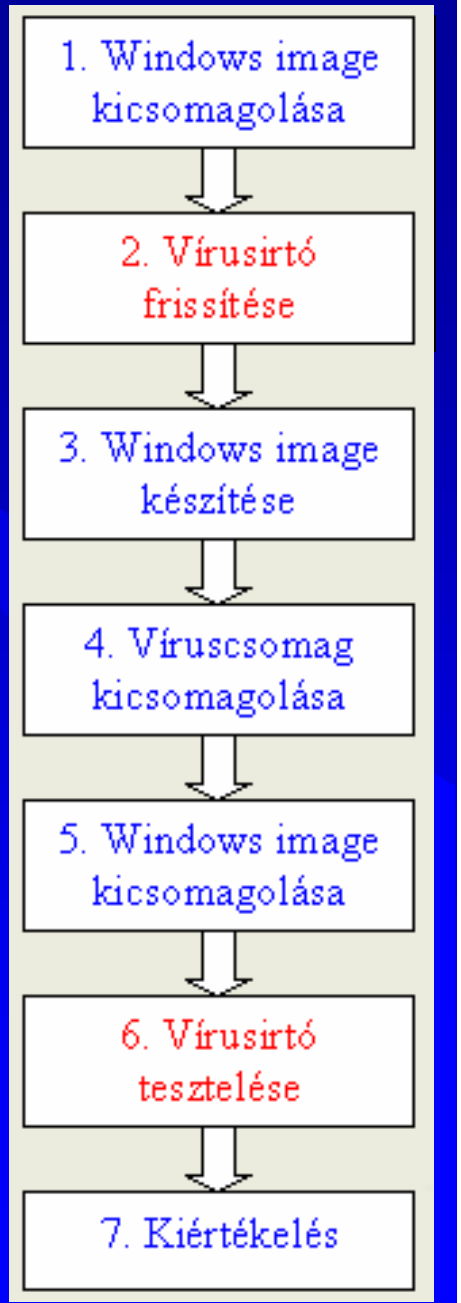
W32/Zafi.A

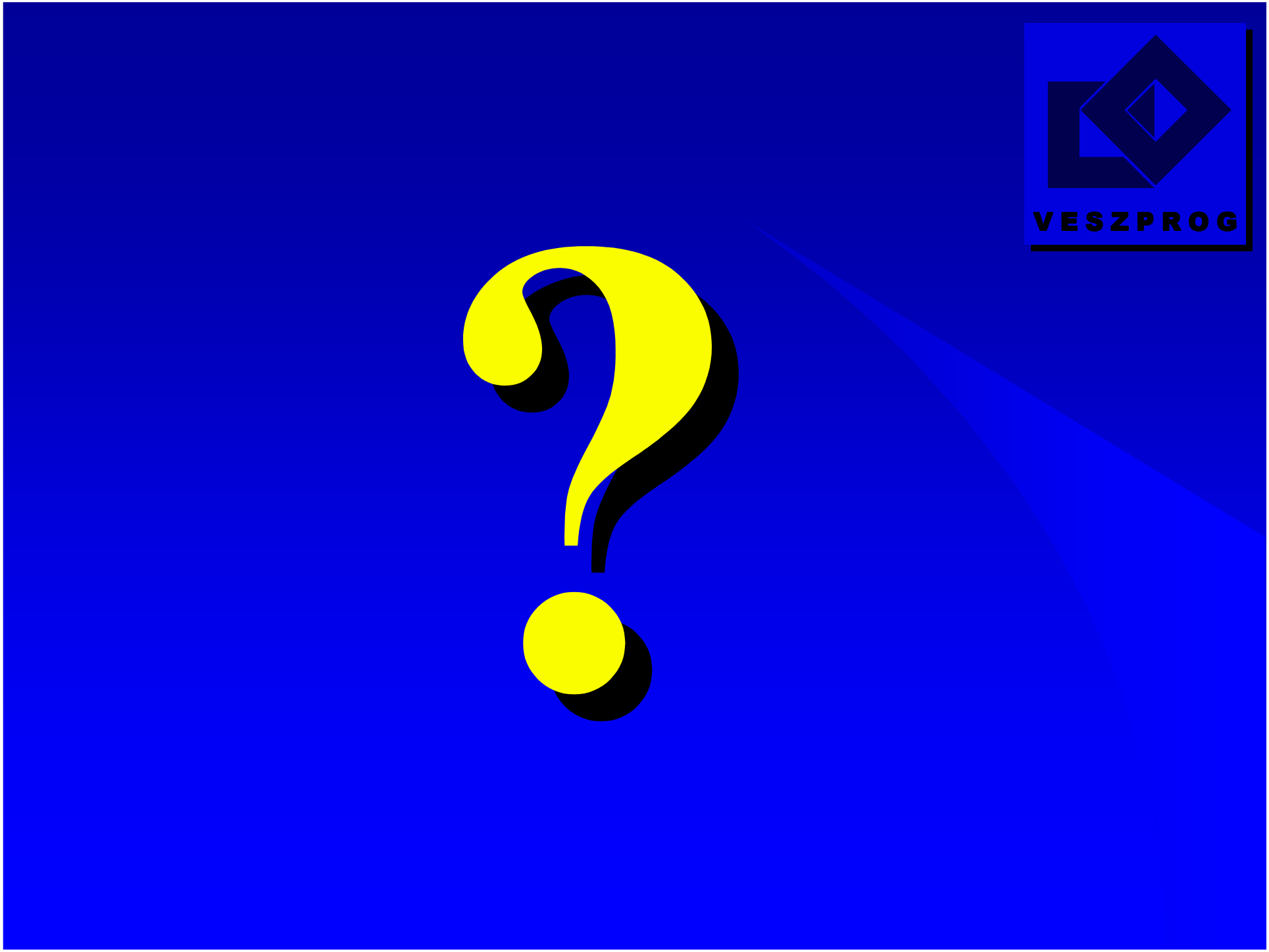
Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus	4.5.0.95, 87139 (known viruses)	I-Worm.Zafi
Kaspersky Anti-Virus	4.5.0.95, 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

A tesztelés menete

1. **Windows visszaállítása (antivírussal)**
2. **Vírusirtó frissítése**
3. **Frissített Windows mentése**
4. **Víruscsomag másolása**
5. **Frissített Windows visszaállítása**
6. **Vírusirtó tesztelése**
7. **Kiértékelés a *naplófájlok*, *eredmény-könyvtárak* alapján.**




VESZPROG