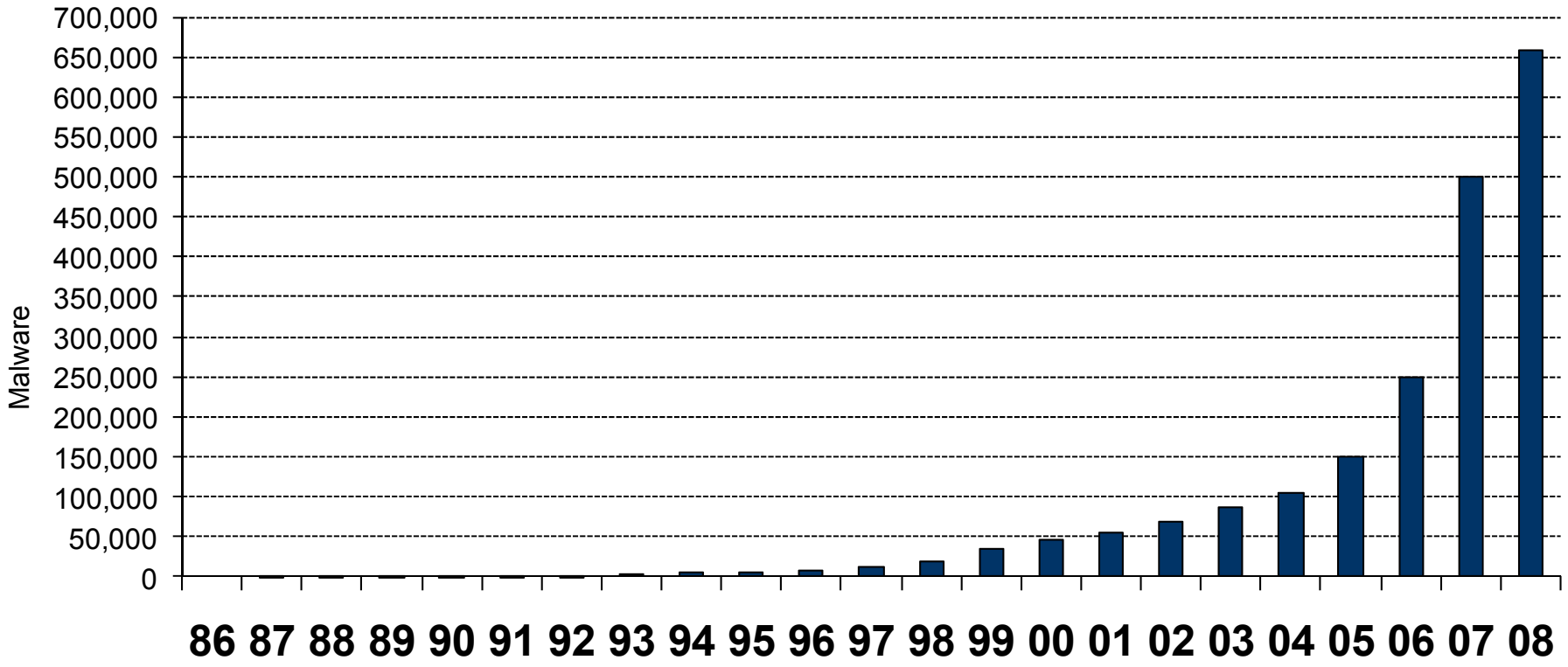
Anti-Virus Testing and AMTSO

Patrik Runald, Security Response Manager

Helsinki ● Kuala Lumpur ● San Jose ● Tokyo ● London ● Paris ● Milan ● Hong Kong
Mumbay ● Warsaw ● Munich ● Copenhagen ● Brussels ● Oulu ● Utrecht ● Oslo ● Stockholm

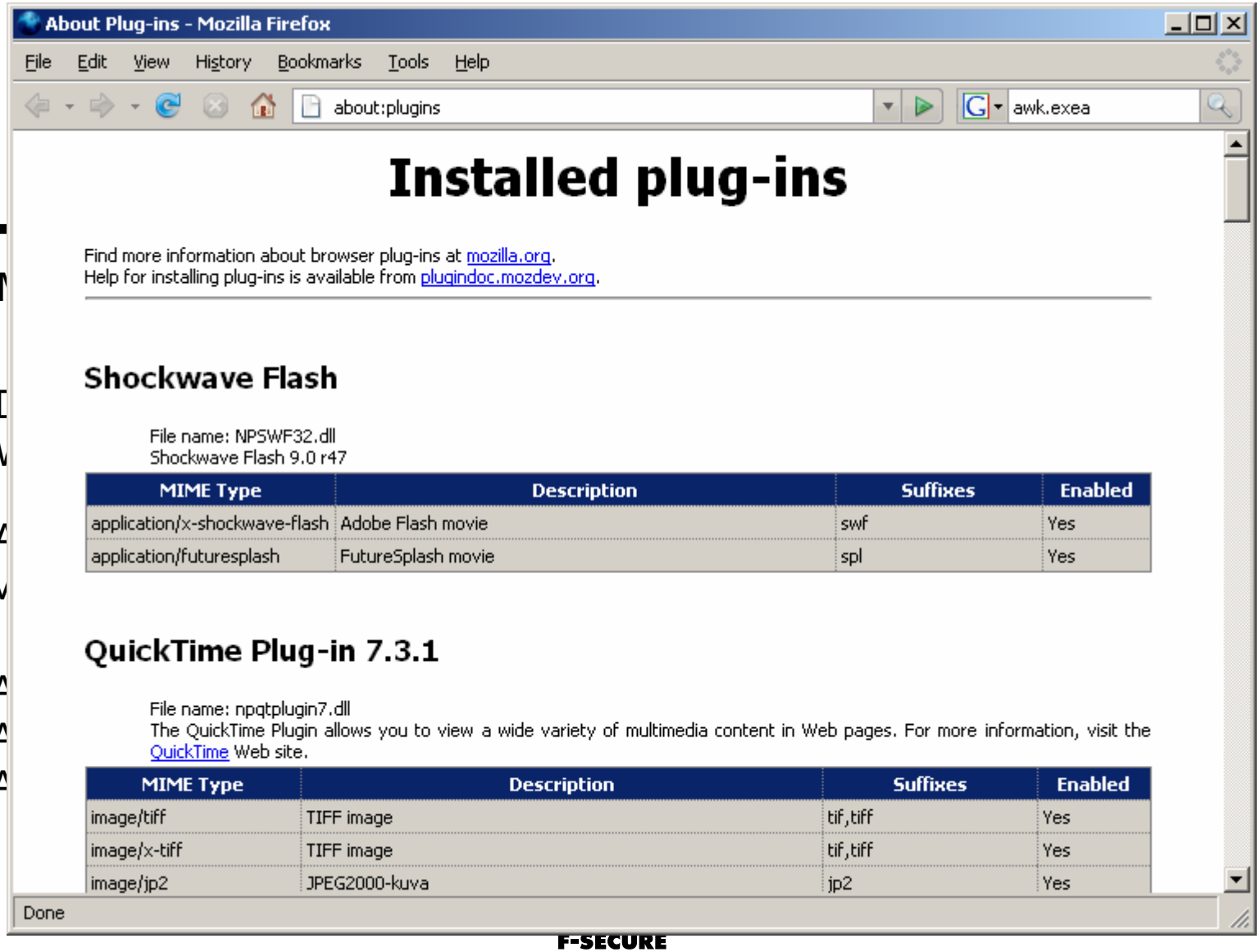

F-SECURE
F-SECURE

Growth of malware



Data source: F-Secure


F-SECURE®


About Plug-ins - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:plugins
awk.exea
Installed plug-ins
Find more information about browser plug-ins at mozilla.org.
Help for installing plug-ins is available from plugindoc.mozdev.org.
Shockwave Flash
File name: NPSWF32.dll
Shockwave Flash 9.0 r47
MIME Type | Description | Suffixes | Enabled
application/x-shockwave-flash | Adobe Flash movie | swf | Yes
application/futuresplash | FutureSplash movie | spl | Yes
QuickTime Plug-in 7.3.1
File name: npqtplugin7.dll
The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the QuickTime Web site.
MIME Type | Description | Suffixes | Enabled
image/tiff | TIFF image | tif,tiff | Yes
image/x-tiff | TIFF image | tif,tiff | Yes
image/jp2 | JPEG2000-kuva | jp2 | Yes
Done

Disclaimer

Material and comments in this presentation doesn't necessarily represent the actions or methods used by F-Secure Corporation.

Problem with AV testing

Doesn’t always state testing methodology

Requires deep knowledge about antivirus technologies

Requires extensive collection or malware

Doesn’t test all parts of an antivirus solution

Engines can be modified/tweaked to do well in tests

Heavily biased toward static file scanning

Testing same as 10 years ago

Testing today

On-demand testing

- WildList/WildCore
- Large (zoo)

Retrospective

- Test product after x amount of time

On-access

- Barely happens, too difficult

Reaction tests

- How long did it take for vendor x to detect sample y

WildList/WildCore

- A collection of malware samples in-the-wild

  “WildCore is a set of replicated virus samples that represents the real threat to computer users”

  “When a virus is reported by two or more reporters it goes into the WildCore”

- Easy to pass as the list is known

Zoo collections

Large collection of samples

Shouldn’t contain trash but often does

Can be tricked by setting paranoid settings/heuristics

Could mean detection based on another vendor

False positives is a problem but can be whitelisted

Retrospective

- Scan a sample collection (WildCore or Zoo) after x amount of time
- Define a date and freeze the updates at that time
- Check detection rates on new samples
- Doesn’t take into account generics on new families
- Unless correlated with false positive testing will benefit high paranoid heuristics

On-access

- Every file would have to be executed. Enough said…

Reaction testing

- How long does it take for a vendor to detect a specific sample
- Less interesting today as there are so many new samples
- Not only that, they are polymorphing

Bias toward file scanning

- Why? Because it’s easy and fast
- Today's products are multi-layered (firewall, HIPS, buffer overflow, IDS etc)

Let's look at some tests

F-SECURE®

	Windows XP Jun 2007	Windows Vista x64 Aug 2007	Netware 6.5 Oct 2007	Windows 2000 Dec 2007	Windows Server 2003 Feb 2008
AEC (Trustport)	VIRUS 100	-	-	X	X
Agnitum	X	-	-	VIRUS 100	X
AhnLab	X	-	-	-	VIRUS 100
Alwil	VIRUS 100	VIRUS 100	-	X	VIRUS 100
Authentium	VIRUS 100	-	-	-	-
Avira	VIRUS 100	-	-	X	VIRUS 100
BitDefender (SOFTWIN)	VIRUS 100	-	-	VIRUS 100	VIRUS 100
Bullguard	VIRUS 100	VIRUS 100	-	VIRUS 100	-
CA eTrust	VIRUS 100	X	VIRUS 100	VIRUS 100	VIRUS 100
CA Home	VIRUS 100	-	-	X	-
CAT QuickHeal	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100	X
Doctor Web	X	-	X	X	X
eEye	VIRUS 100	-	-	-	-

AV-Test March 2008

Vendor	detected 3/2008	% detected
AVK (G Data)	1129521	99.9%
WebWasher (CW	1128800	99.9%
TrustPort	1126425	99.6%
AnyVir (Anvir)	1126370	99.6%
Avast! (Alwil)	1117099	98.8%
Trend Micro	1116139	98.7%
Sophos	1109030	98.1%
Ikarus	1107753	98.0%
Nod32 (Eset)	1106286	97.8%
Microsoft	1105564	97.8%
BitDefender	1105397	97.8%
Kaspersky	1098533	97.2%
F-Secure	1094188	96.8%
F-Prot (Frisk)	1093516	96.7%
eScan	1093247	96.7%
ZoneAlarm	1089191	96.4%
AVG	1088422	96.3%
Norton (Symantec)	1084078	95.9%
Panda	1080986	95.6%
McAfee	1080580	95.6%
Rising	1063960	94.1%
Norman	1049019	92.8%

"A comprehensive review should not only concentrate on detection scores of the on-demand scanner, as this would give a user only a very misleading and limited view of the product's capabilities."

"When comparing the security of cars, we would not only focus on the safety belts, but also check the ABS system (anti-lock braking system), one or more airbags, crush zones, the ESP (electronic stabilization program) as well as constructional changes and many other features which make a car secure."

In order to get a more comprehensive impression of the products, one should not only look at this test, but also compare the results of various tests and the products' performance over time and their on-going development.

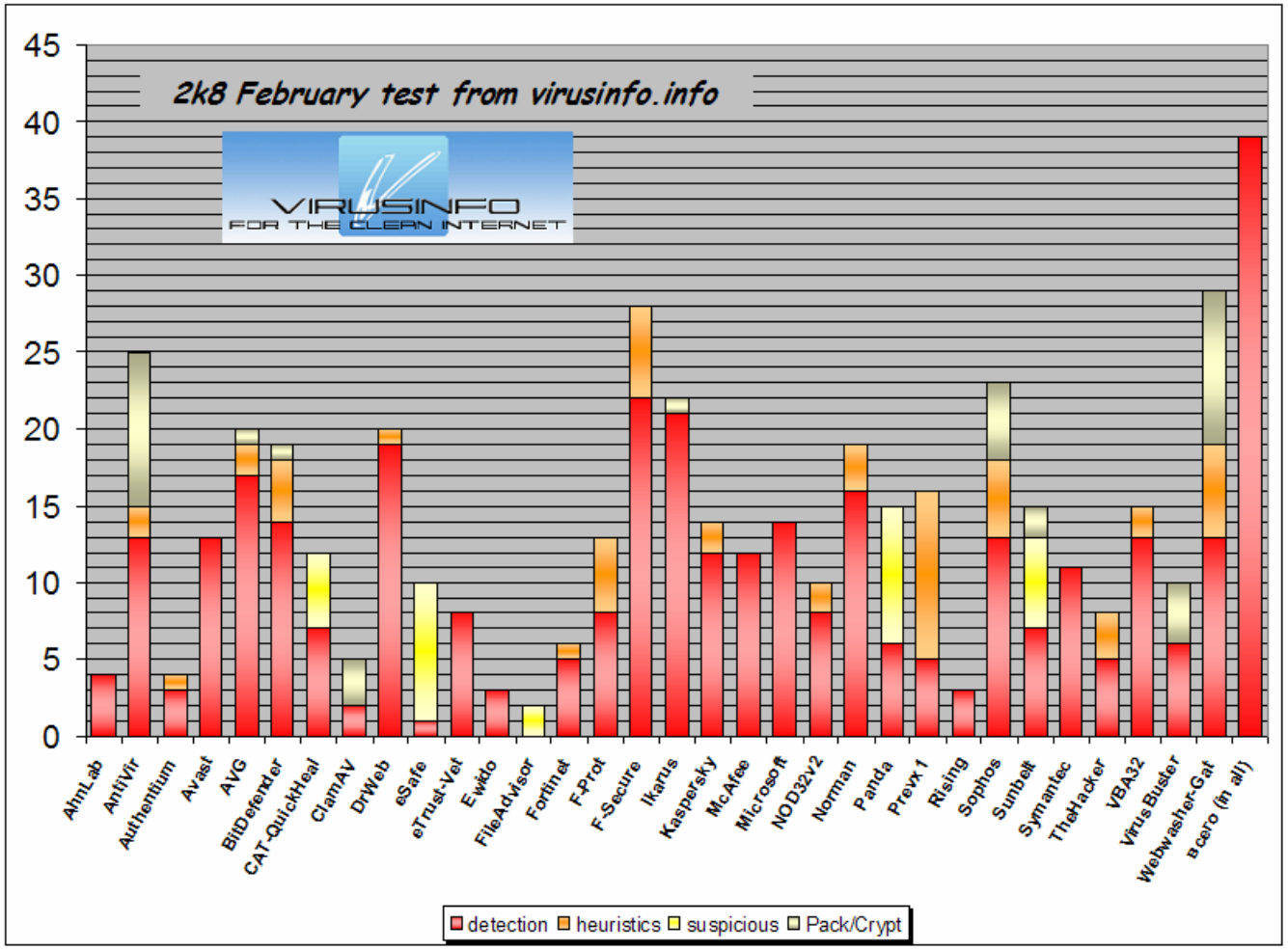
AV-Comparatives Feb 2008

Company		AVIRA		G DATA Security		Alwil Software		AVG Technologies		BitDefender		MicroWorld		F-Secure	
Product		**AntiVir PE Premium**		**AntiVirusKit (AVK)**		**avast! Professional**		**AVG Anti-Malware**		**BitDefender Prof.+**		**eScan Anti-Virus**		**F-Secure Anti-Virus**	
Program version		7.06.00.308		18.0.7227.533		4.7.1098		7.5.516		11.0.15		9.0.768.1		8.00.101	
Engine / signature version		7.06.00.62 / 7.00.02.90		18.2654 / 18.123		080203-0		269.19.19 / 1258		7.17325		*N/A*		7.30.13161	
Number of virus records		*1.092.160*		*unknown*		*unknown*		*unknown*		*978.896*		*unknown*		*unknown*	
Certification level reached in this test		**ADVANCED+**		**ADVANCED+**		**ADVANCED+**		**ADVANCED+**		**ADVANCED**		**ADVANCED+**		**ADVANCED+**	
On-demand detection of virus/malware															
Windows viruses	149.202	148.903	99,8%	149.119	99,9%	148.387	99,5%	143.393	96,1%	147.022	98,5%	148.683	99,7%	148.684	99,7%
Macro viruses	95.059	95.034	~100%	95.059	100%	94.631	99,5%	94.823	99,8%	94.736	99,7%	95.054	~100%	95.055	~100%
Script viruses	14.284	13.916	97,4%	14.165	99,2%	13.010	91,1%	12.055	84,4%	13.372	93,6%	13.949	97,7%	14.102	98,7%
Worms	190.952	190.530	99,8%	190.564	99,8%	188.006	98,5%	188.821	98,9%	189.084	99,0%	189.484	99,2%	189.515	99,2%
Backdoors/Bots	400.986	399.900	99,7%	399.536	99,6%	391.432	97,6%	395.103	98,5%	382.706	95,4%	390.205	97,3%	390.239	97,3%
Trojans	817.043	813.233	99,5%	811.200	99,3%	793.223	97,1%	803.376	98,3%	782.493	95,8%	788.147	96,5%	788.288	96,5%
other malware	15.838	15.447	97,5%	15.715	99,2%	14.402	90,9%	14.078	88,9%	14.710	92,9%	15.299	96,6%	15.345	96,9%
TOTAL	**1.683.364**	1.676.963	**99,6%**	1.675.358	**99,5%**	1.643.091	**97,6%**	1.651.649	**98,1%**	1.624.123	**96,5%**	1.640.821	**97,5%**	1.641.228	**97,5%**

AV-Comparatives Feb 2008

Kaspersky Labs **Kaspersky AV** 7.0.1.321a *N/A* *574.209*		McAfee **McAfee VirusScan+** 12.0.176 5200.2160 / 5222 *371.817*		Microsoft **Microsoft OneCare** 2.0.2500.22 1.27.6270.0 / 1.3204 723.778		ESET **NOD32 Antivirus** 3.0.621.0 2847 *unknown*		Norman ASA **Norman ISS AV+AS** 7.0 5.91.10 *1.310.735*		Symantec **Norton Anti-Virus** 15.0.0.58 100204 / 78215 *73.845*		Sophos **Sophos Anti-Virus** 7.0.7 2.70.1 / 4.26E+132 *345.615*		AEC **TrustPort AV WS** 2.8.0.1629 2.8.0.1630 *unknown*		VirusBlokAda **VBA32 Anti-Virus** 3.12.6.0 *unknown* *unknown*	
ADVANCED+		**ADVANCED**		**ADVANCED**		**ADVANCED+**		**ADVANCED**		**ADVANCED+**		**ADVANCED**		**ADVANCED+**		**STANDARD**	
148.909	99,8%	147.115	98,6%	146.690	98,3%	148.453	99,5%	140.874	94,4%	149.128	~100%	145.076	97,2%	149.037	99,9%	132.863	89,0%
95.054	~100%	95.056	~100%	94.624	99,5%	95.044	~100%	94.869	99,8%	95.059	100%	94.810	99,7%	95.053	~100%	92.909	97,7%
13.949	97,7%	12.855	90,0%	11.963	83,8%	13.338	93,4%	10.753	75,3%	14.049	98,4%	10.730	75,1%	13.979	97,9%	7.200	50,4%
189.893	99,4%	188.318	98,6%	185.743	97,3%	189.659	99,3%	185.448	97,1%	190.551	99,8%	185.065	96,9%	190.781	99,9%	171.497	89,8%
392.713	97,9%	383.059	95,5%	376.054	93,8%	391.015	97,5%	380.204	94,8%	384.939	96,0%	394.944	98,5%	400.503	99,9%	351.683	87,7%
798.083	97,7%	757.305	92,7%	753.863	92,3%	792.222	97,0%	761.830	93,2%	794.816	97,3%	783.006	95,8%	815.262	99,8%	708.649	86,7%
15.390	97,2%	14.370	90,7%	12.044	76,0%	14.226	89,8%	12.272	77,5%	15.464	97,6%	12.135	76,6%	15.458	97,6%	11.498	72,6%
1.653.991	**98,3%**	1.598.078	**94,9%**	1.580.981	**93,9%**	1.643.957	**97,7%**	1.586.250	**94,2%**	1.644.006	**97,7%**	1.625.766	**96,6%**	1.680.073	**99,8%**	1.476.299	**87,7%**

VirusInfo


2k8 February test from virusinfo.info
VIRUSINFO
FOR THE CLEAN INTERNET
45
40
35
30
25
20
15
10
5
0
AhnLab
AntiVir
Authentium
Avast
AVG
BitDefender
CAT-QuickHeal
ClamAV
DrWeb
eSafe
eTrust-Vet
Ewido
FileAdvisor
Fortinet
F-Prot
F-Secure
Ikarus
Kaspersky
McAfee
Microsoft
NOD32v2
Norman
Panda
Prevx1
Rising
Sophos
Sunbelt
Symantec
TheHacker
VBA32
VirusBuster
Webwasher-Gat
zcero (in all)
detection
heuristics
suspicious
Pack/Crypt

VirusTotal

So what can be done?

FRISK
software international

Order | Products | Download | Support | Virus Information | Partners | About | News | Forum | Fee

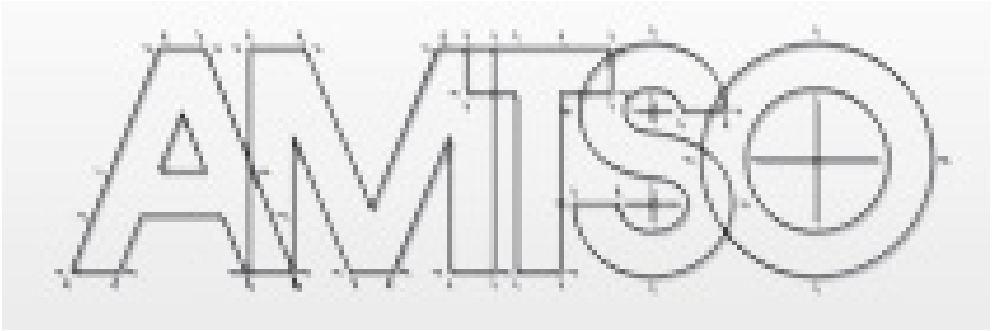
International Antivirus Testing Workshop

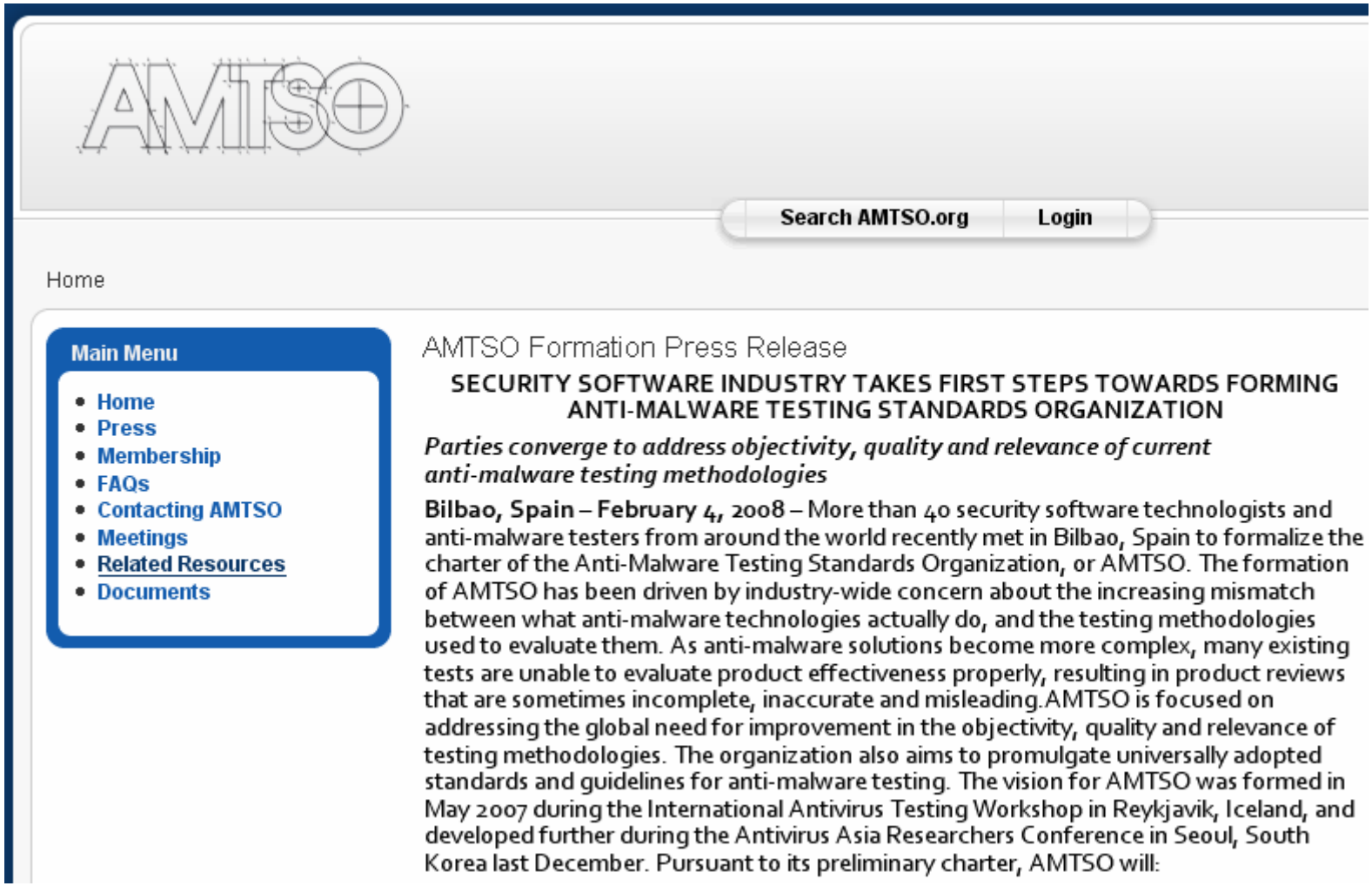
International Antivirus Testing Workshop

Hotel Saga, Reykjavik, Iceland

15th – 16th May 2007

F-SECURE®


AMTSO

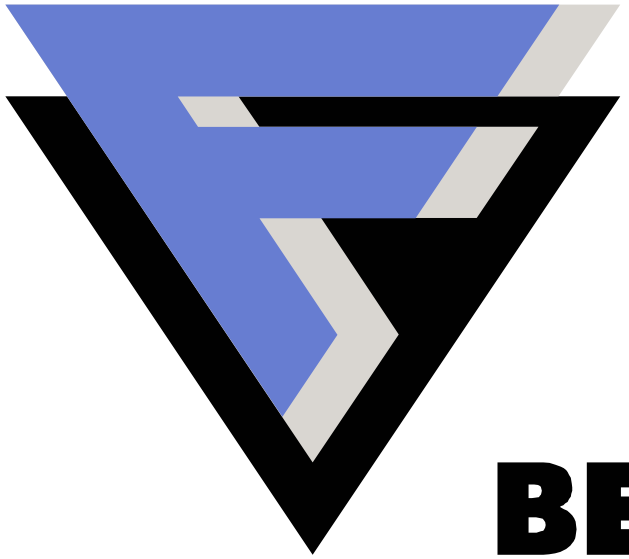

AMTSO
Search AMTSO.org
Login
Home
Main Menu
Home
Press
Membership
FAQs
Contacting AMTSO
Meetings
Related Resources
Documents
AMTSO Formation Press Release
SECURITY SOFTWARE INDUSTRY TAKES FIRST STEPS TOWARDS FORMING ANTI-MALWARE TESTING STANDARDS ORGANIZATION
Parties converge to address objectivity, quality and relevance of current anti-malware testing methodologies
Bilbao, Spain – February 4, 2008 – More than 40 security software technologists and anti-malware testers from around the world recently met in Bilbao, Spain to formalize the charter of the Anti-Malware Testing Standards Organization, or AMTSO. The formation of AMTSO has been driven by industry-wide concern about the increasing mismatch between what anti-malware technologies actually do, and the testing methodologies used to evaluate them. As anti-malware solutions become more complex, many existing tests are unable to evaluate product effectiveness properly, resulting in product reviews that are sometimes incomplete, inaccurate and misleading.AMTSO is focused on addressing the global need for improvement in the objectivity, quality and relevance of testing methodologies. The organization also aims to promulgate universally adopted standards and guidelines for anti-malware testing. The vision for AMTSO was formed in May 2007 during the International Antivirus Testing Workshop in Reykjavik, Iceland, and developed further during the Antivirus Asia Researchers Conference in Seoul, South Korea last December. Pursuant to its preliminary charter, AMTSO will:

AMTSO

ALWIL Software
AV-Comparatives
AV-Test.org
AVG Technologies
Avira GmbH
Bit9
BitDefender
Doctor Web, Ltd.
ESET
F-Secure Corporation
G DATA Software
Hispasec Sistemas
IBM
Kaspersky Lab
McAfee, Inc.
Microsoft Corp.
Norman ASA
Panda Security
PC Tools
Sana Security
Secure Computing
Sophos Plc
Symantec Corporation
Trend Micro Inc.
Virusbuster Ltd.

Finally we're making changes

F-SECURE®



BE SURE.

Patrik Runald

Security Response Manager

F-Secure Corporation

www.f-secure.com