



SLAC 2009

Ist AV tot?

Rainer Link • Senior Threat Researcher
Trend Micro Threat Research

Hinweis

Diese Präsentation wurde im Rahmen der Secure Linux Administration Conference 2009 in Berlin gehalten. Die Titelfrage „Ist AV tot?“ wurde bewusst provokativ gewählt und letztendlich ebenso die Beantwortung offengelassen.

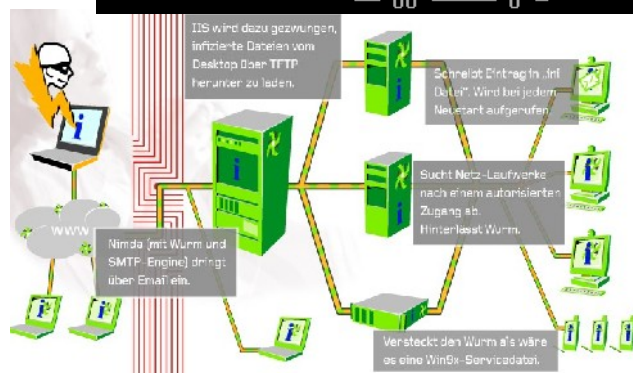
\$ whoami

- „Anfangszeit“ (~ 1991)
 - Entwickler CV-Info
- „Core Development“ (~ 1999)
 - Entwickler AMaViS
 - Entwickler samba-vscan
 - Werkstudent SuSE Labs
- „Research“ (~ 2003)
 - Trend Micro Deutschland GmbH
 - Threat Research
 - Pressesprecher Produkte & Technologien



Image courtesy F-Secure Image Archive

MOSAIC	BAK	10691	11.11.93	15.32
MOSAIC	INI	10683	20.01.94	19.50
APPLICA	GRP	4693	23.01.94	15.33



- TREND MICRO löst Yellow Alert aus: WORM_NETSKY.P...
- TREND MICRO löst Yellow Alert aus: BAGLE.Q...

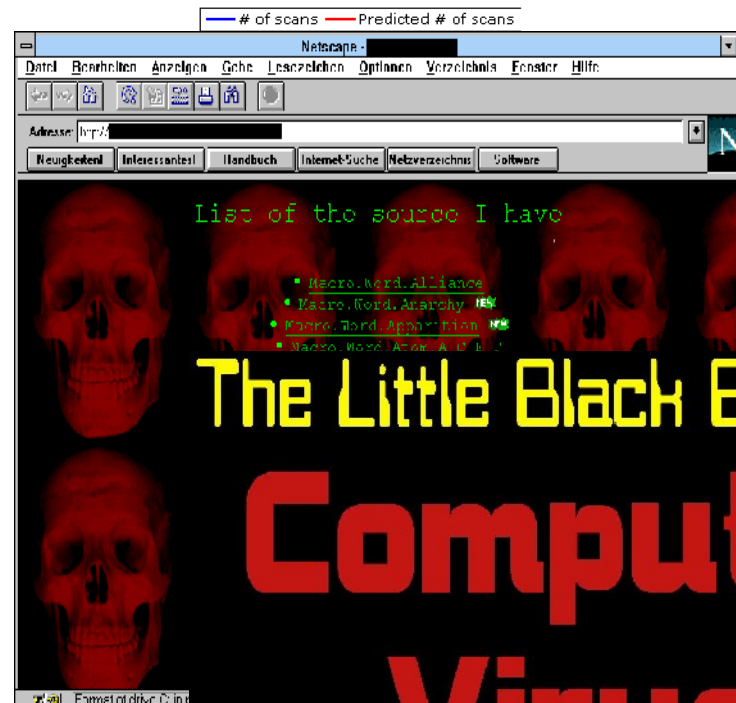
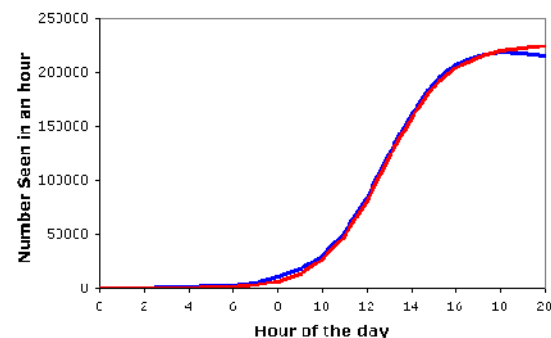
ENTERPRISE

SMALL

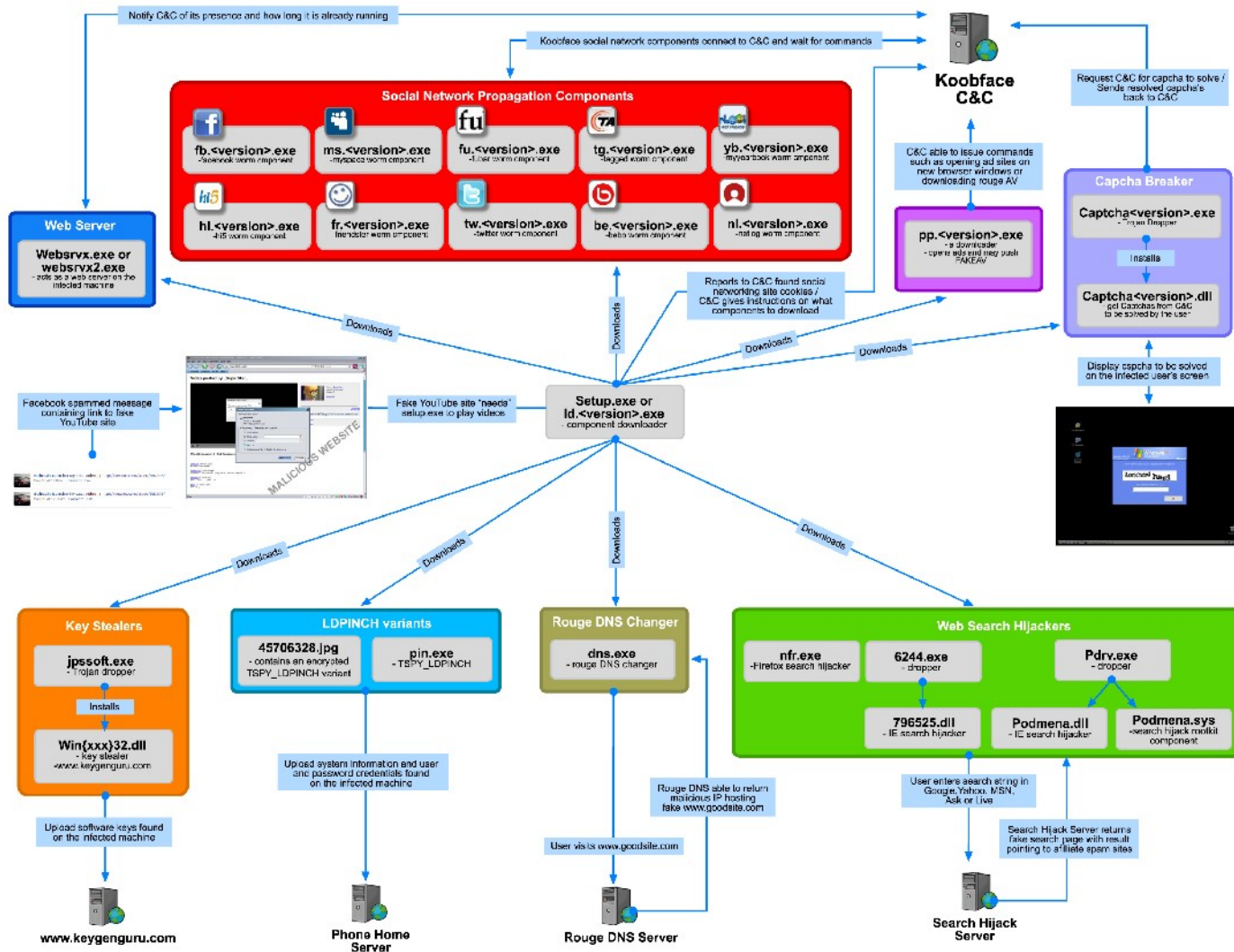
YELLOW ALERT

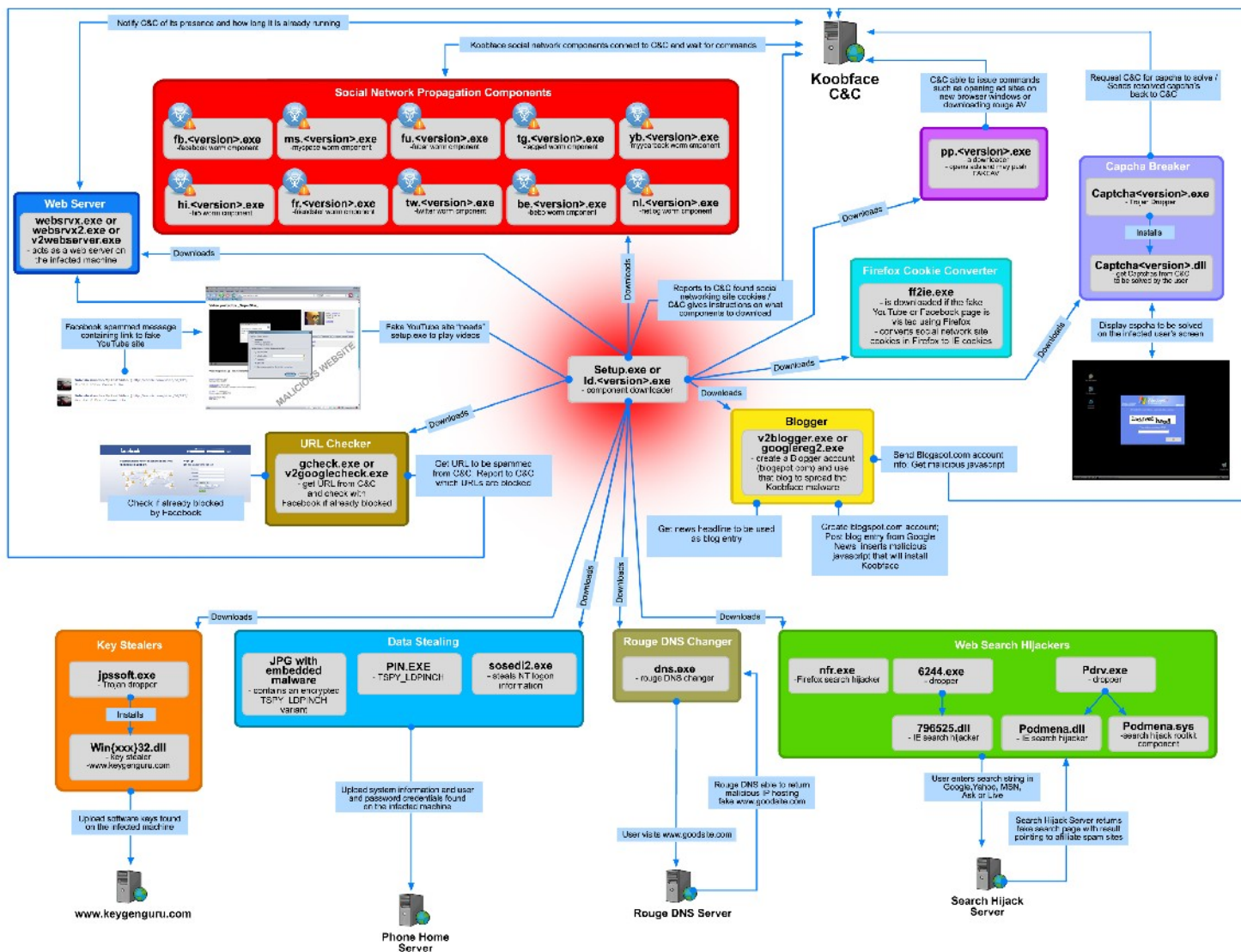
WORM_NETSKY.P is a medium risk alert

Probes Recorded During Code Red's Reoutbreak



The Little Black Book of Computer Viruses



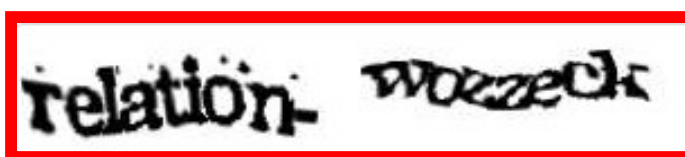


Join the C

Already use Twitter



☐ I want the inside scoop—please send me email updates!



Type the words above

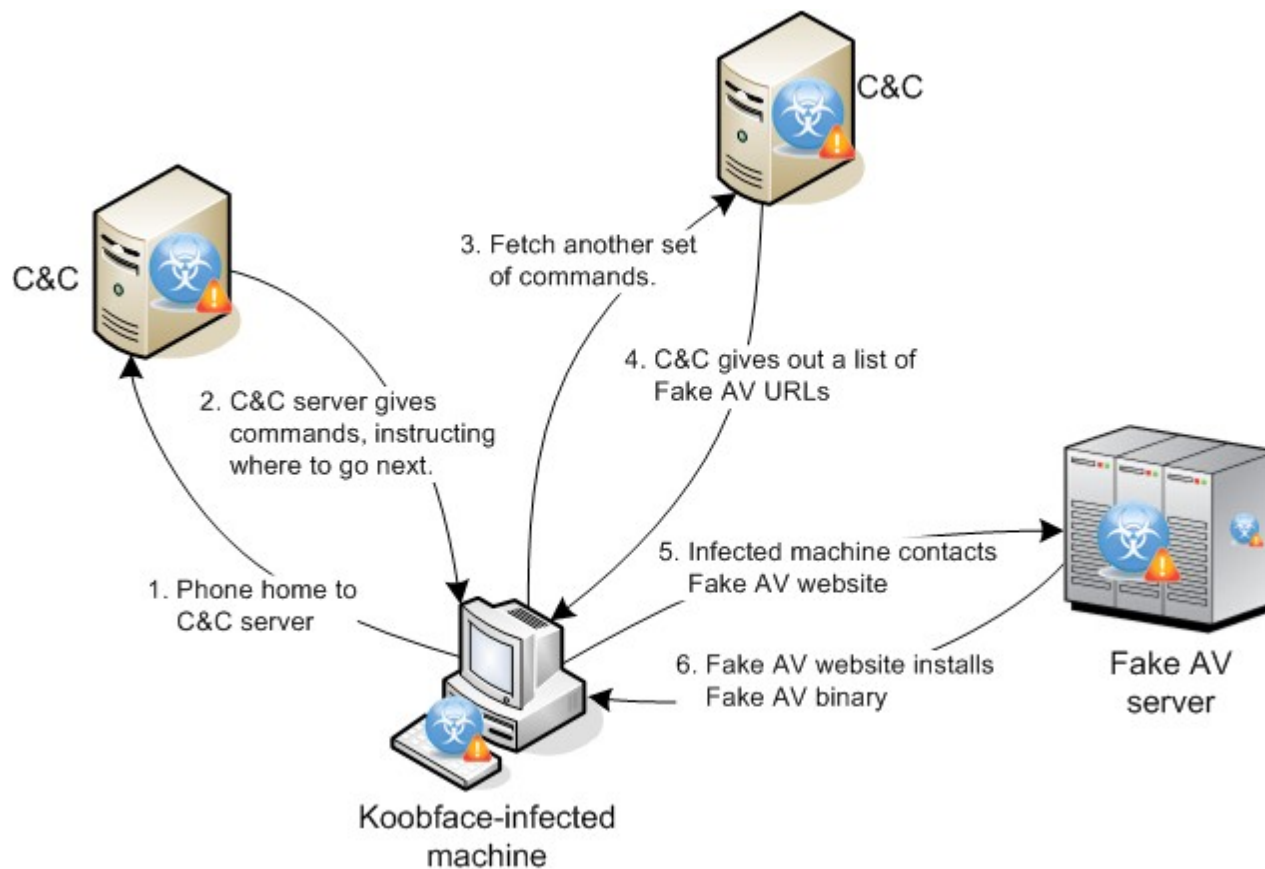
Create my account

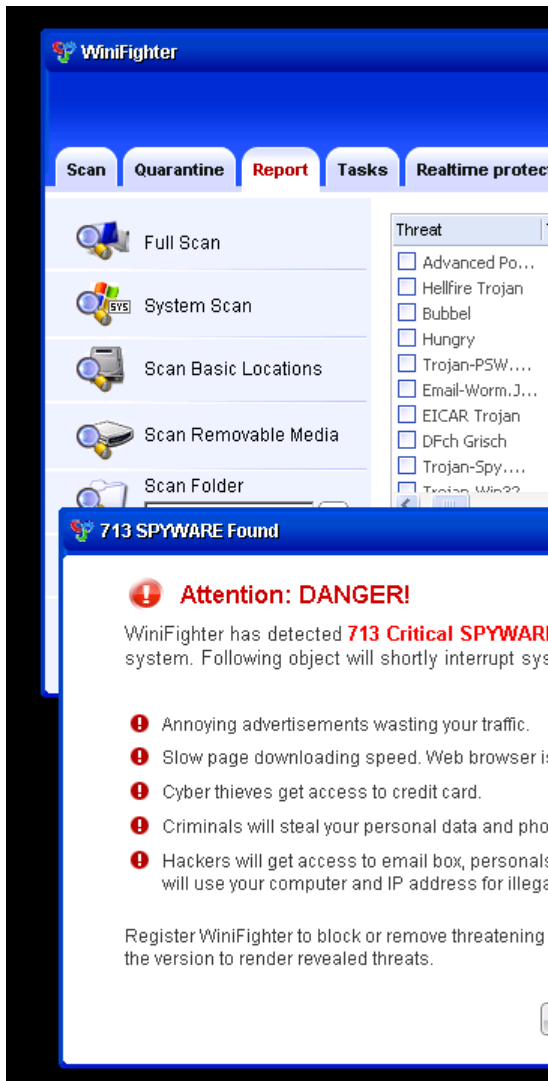
Can't read this?

[Get two new words](#)

[Hear a set of words](#)

Powered by reCAPTCHA.
[Help](#)





WiniFighter

The best Windows based system protection against viruses, worms and another malicious and unwanted software

We accept:

VISA MasterCard VISA Electron American Express Discover Mac OS

Your Payment Information

Price: \$49.95

Payment Type Credit Card

Card Number *

Card Expired *

CVV2 Number * [What is CWV2?](#)

Your Name and Address:

First Name *

Last Name *

Email *

Country *

City *

Street *

Phone

* - these fields are required. Information is needed for credit card verification even for download orders.
It is never shared with another companies.

WiniFighter 24H Premium support **highly recommended** ☒ \$49.95

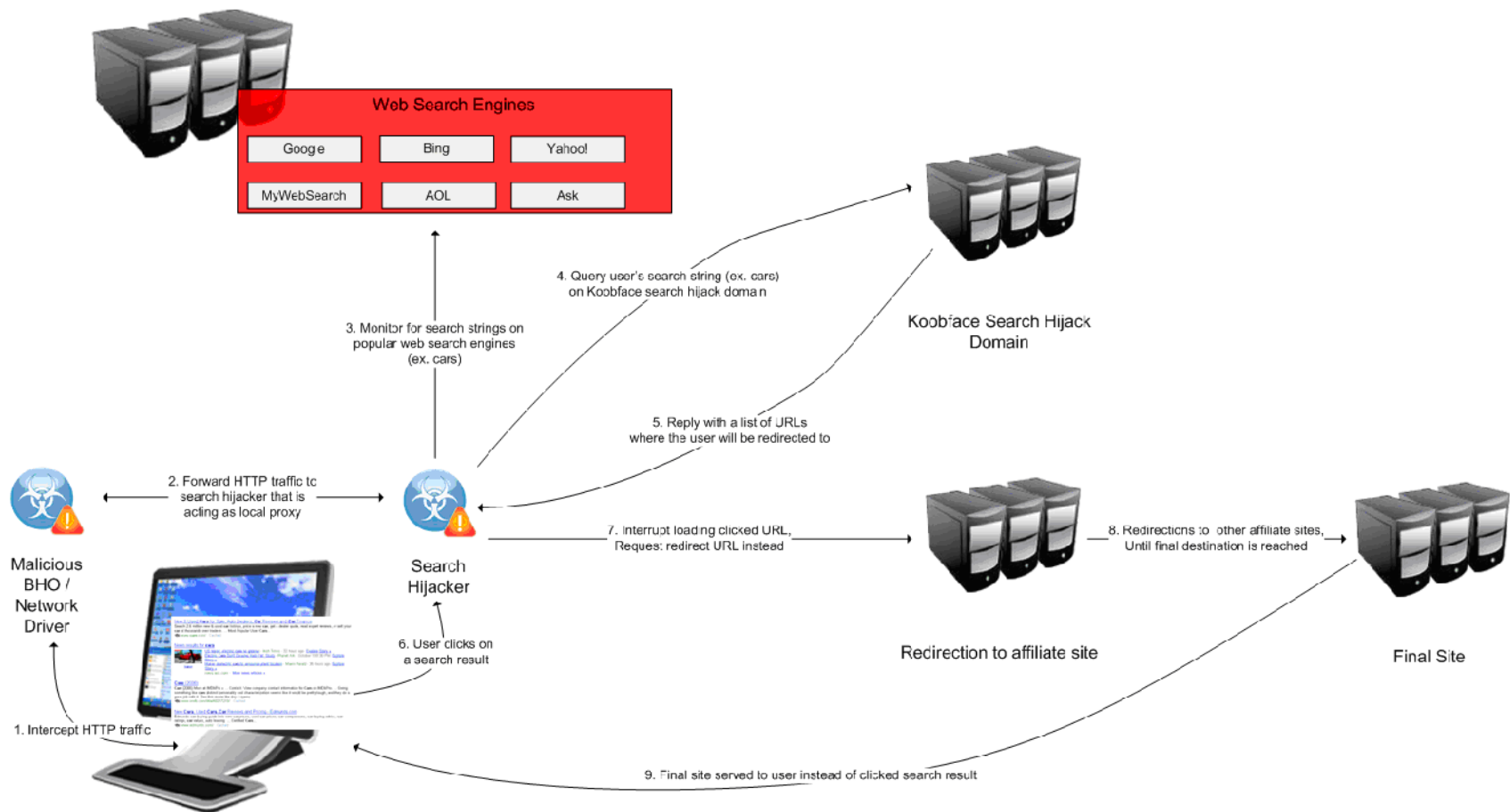
IMPORTANT: Please allow up to **two minutes** for live processing of Your order.
Don't click **BACK** or **CANCEL** while waiting.

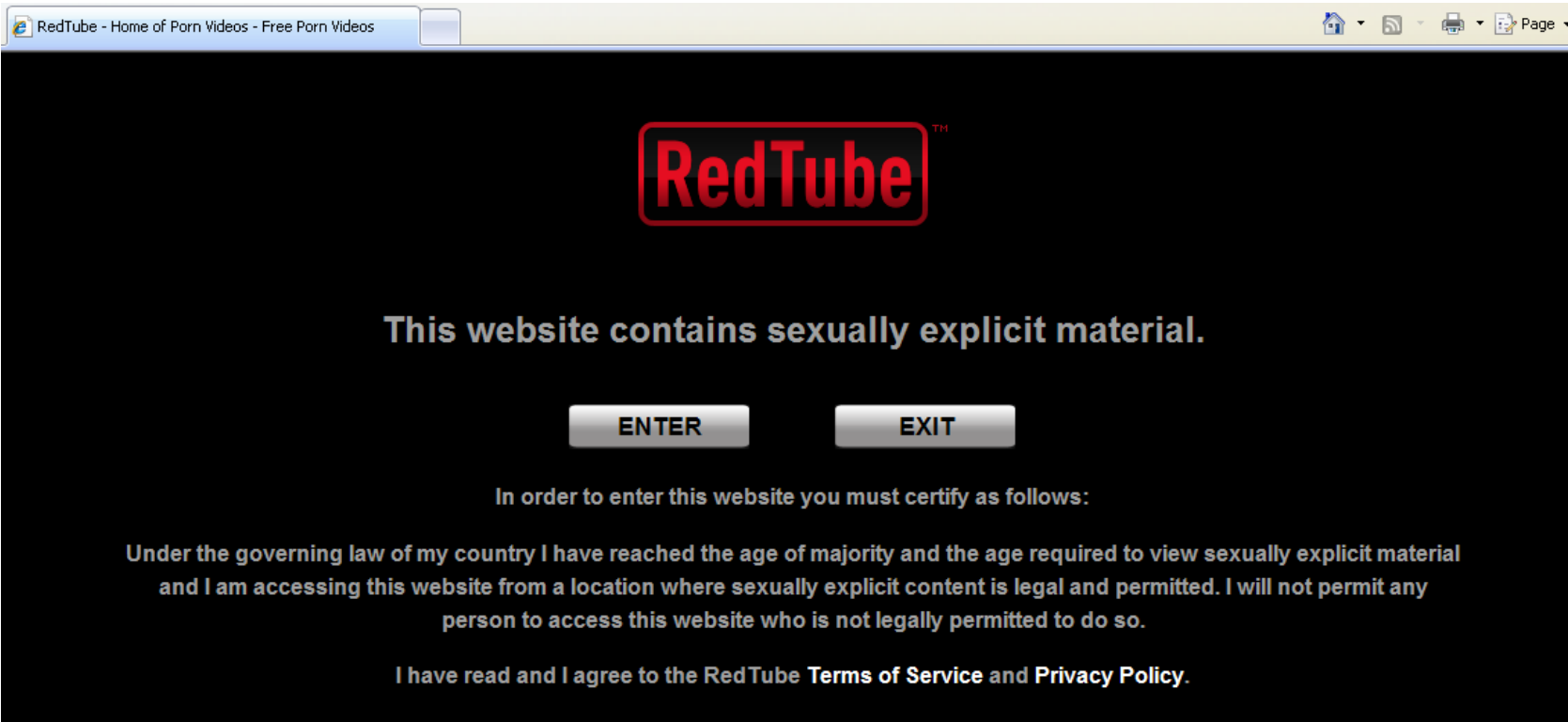
Certified:

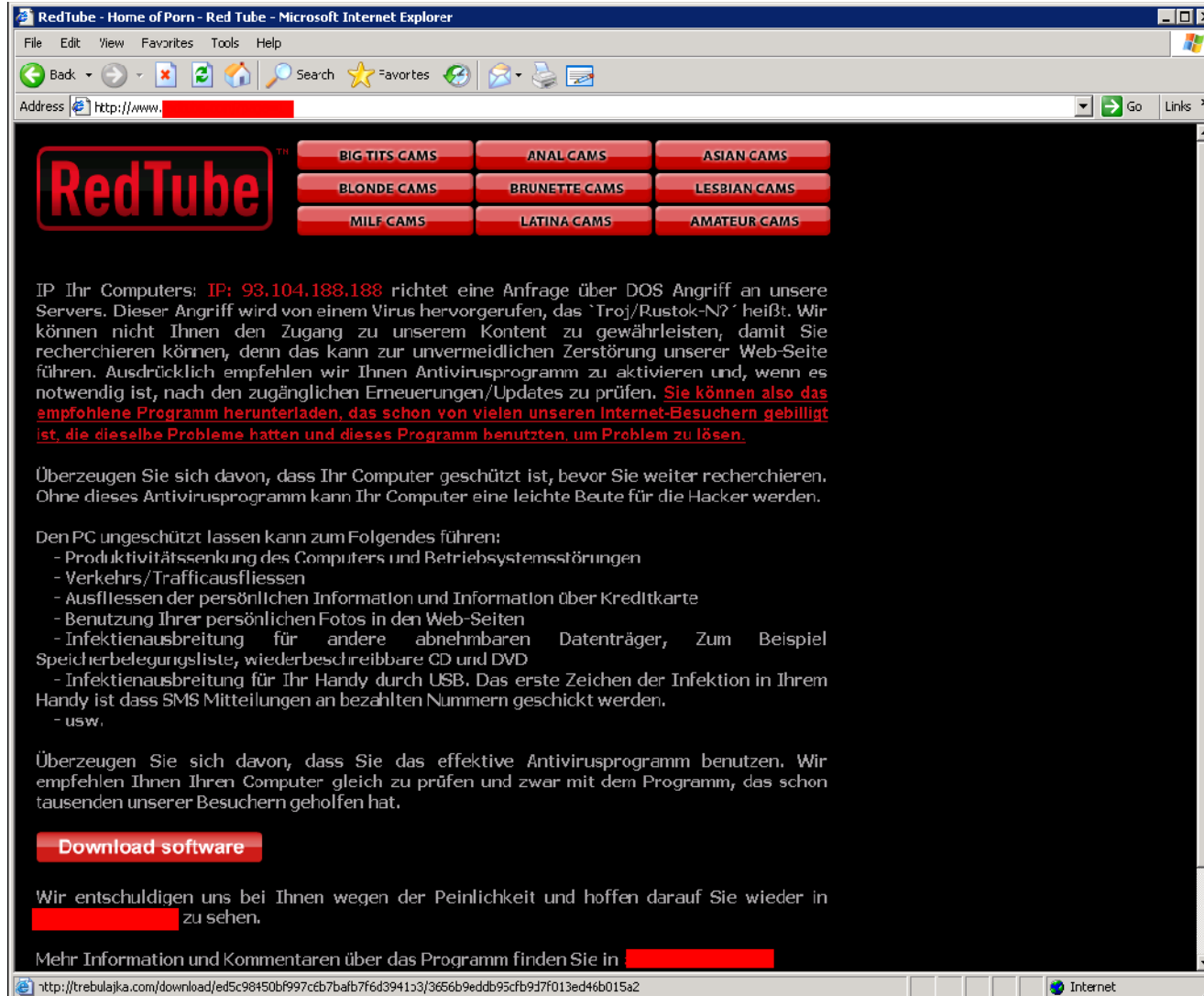
Verified by VISA MasterCard SecureCode ETA

Official Partner MRC

Spyware Alert!







Adobe - Adobe Flash Player - Windows Internet Explorer

http://adobe.com

File Edit View Favorites Tools Help

Adobe - Adobe Flash Player

Your account | Contact | United States (Change)

Solutions Products Support Communities Company Downloads Store

Home Downloads Flash Player

Adobe Flash Player



Install Adobe Flash Player

Adobe Flash Player version 9.0.159.0
Windows | 1.4MB
[Different operating system or browser?](#)

Browser: Firefox, Safari, Opera, Mozilla, Netscape, AOL
Download time estimate: 2 minutes @ 56K modem

[Learn more](#) | [System requirements](#) | [Distribute Flash Player](#) | [Installation instructions](#)

You must close all other browser windows before installing.

[Agree and install now](#)

By clicking the "Agree and install now" button,
you agree to the [Software License Agreement](#).

[Careers](#) | [Online Privacy Policy](#) | [Terms of Use](#) | [Contact us](#) | [Accessibility](#) | [Report piracy](#) | [Permissions and trademarks](#)
| [Product license agreements](#) | [Send feedback](#)

Copyright © 2009 Adobe Systems Incorporated. All rights reserved.
Use of this website signifies your agreement to the [Terms of Use](#) and [Online Privacy Policy](#) (updated 07-08-2008).
Search powered by Google™



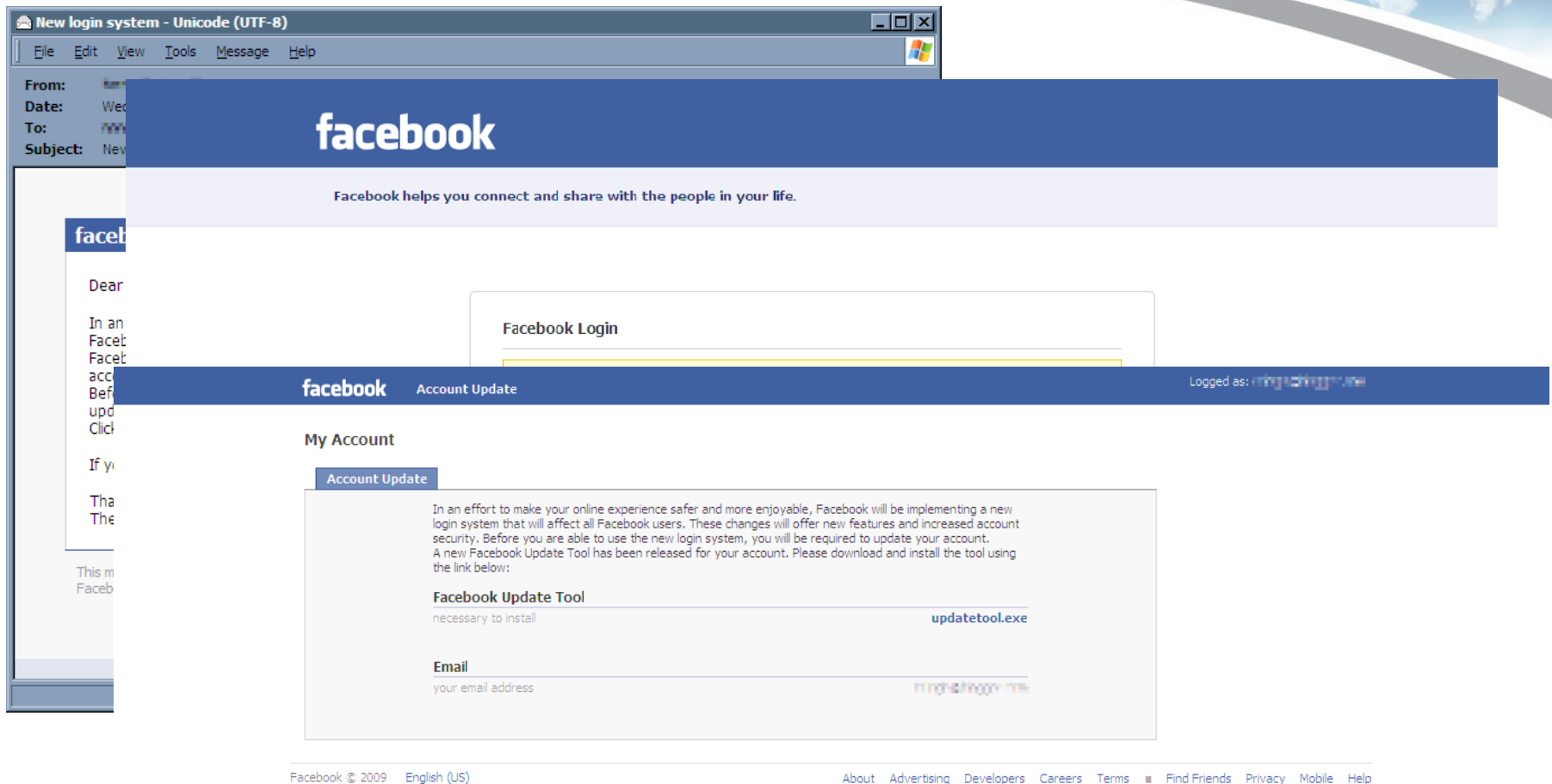
Adobe – Erkennung des Installationsprogramm als Schadsoftware

Scan report of: install_flash_player(2).ex2

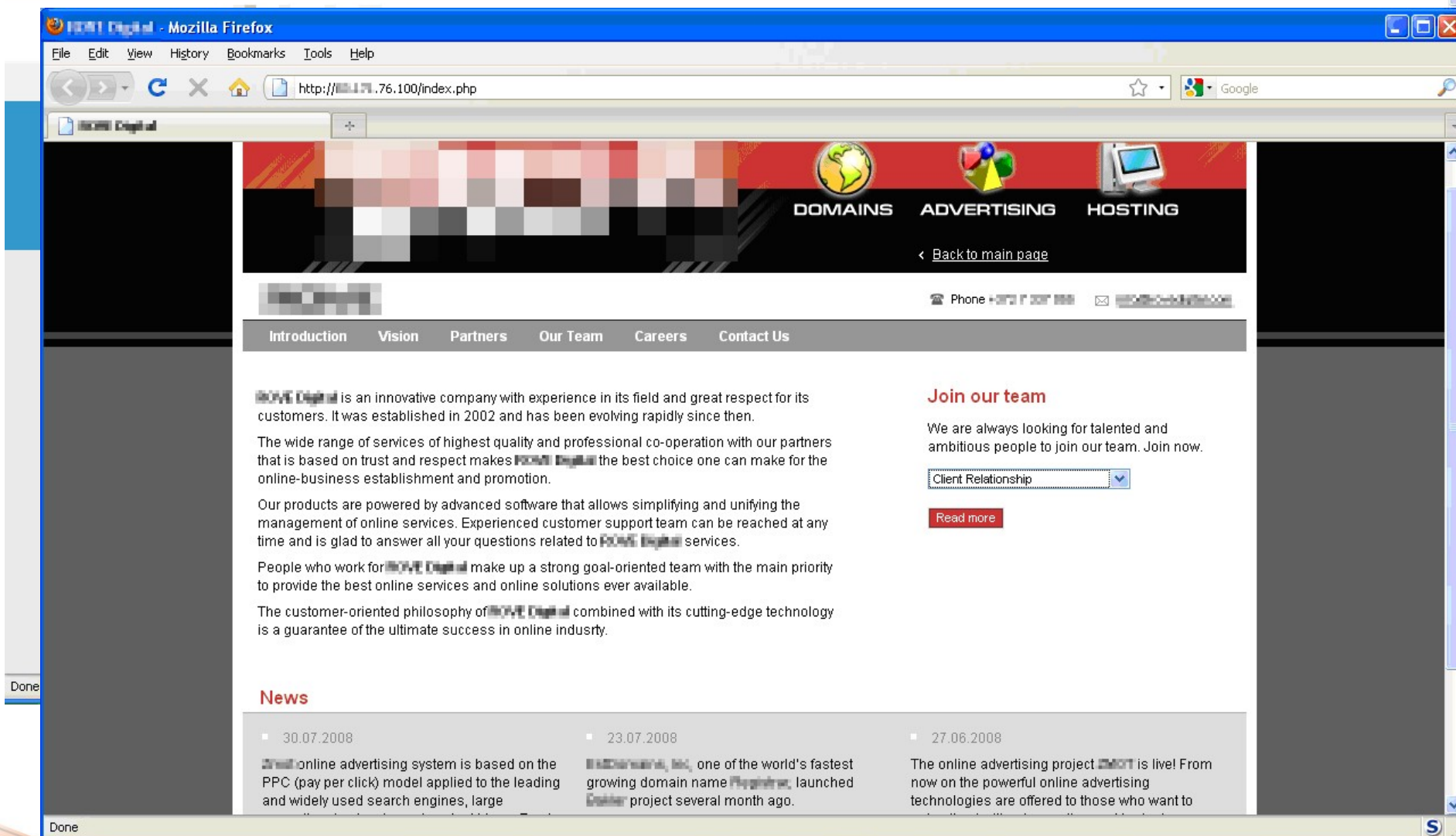
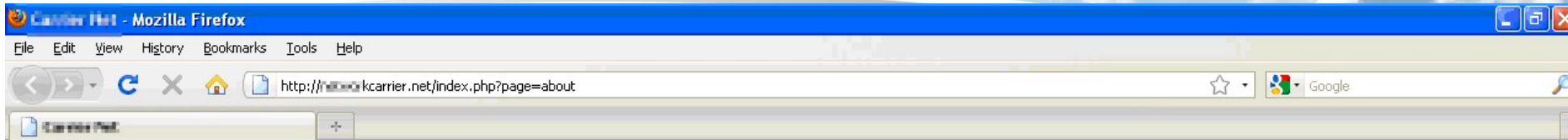
AntiVir	-	Panda	-
Authentium	-	Panda (BETA)-	
Avast	-	Panda (Online)	-
AVG	-	QuickHeal	-
BitDefender	-	Rising	-
CA-AV	-	Sophos	-
CA-AV (BETA)	-	Spybot S&D	-
ClamAV	-	Sunbelt	-
Dr Web	-	Symantec	-
Eset Nod32	-	Symantec (BETA)	-
Fortinet	-	Trend Micro	-
Fortinet (BETA)	-	Trend Micro (Cons.)	-
F-Prot	-	Trend Micro (CPR)	-
F-Secure 2009	-	VBA32	-
F-Secure 2010	-	VirusBuster	-
Ikarus	-		
ISS VPS	-		
K7 Computing-			
Kaspersky	-		
Kaspersky (Cons.)	-		
McAfee	-		
McAfee (BETA)	-		
McAfee (Online)	-		
McAfee GW Edition	-		
Microsoft	-		
Norman	-		



Figure 1. Sample malware software license agreement



Falls der Exploit Pack einen nicht gleich infiziert hat, der fällt ggf. auf Social Engineering rein ...



CNN.com

Web CNN News CNN Videos

SEARCH

POWERED BY Google

[HOME](#)
[WORLD](#)
[U.S.](#)
[POLITICS](#)
[CRIME](#)
[ENTERTAINMENT](#)
[HEALTH](#)
[TECH](#)
[TRAVEL](#)
[LIVING](#)
[BUSINESS](#)
[SPORTS](#)
[TIME.COM](#)

[Topics](#) »
[Hamas](#) •
[Bill Richardson](#) •
[John Travolta](#) •
[Gaza Crisis](#) •
[Year in Review](#) • more topics »

Weather Forecast

Edition: [International](#) | [Set Pre](#)

Set your CNN.com Edition ☒ CNN U.S. ☐ CNN International

SET EDITION

updated 9:17 p.m. EST, Mon January 5, 2009

Make CNN Your Home Page



updated 52 minutes ago

'Friendly fire' kills three Israeli soldiers

The Israeli military surrounded densely populated Gaza City late Monday as the death toll continued to mount in the war-torn territory and both sides showed little interest in

Other News

- [Franken claims victory as lawsuit looms](#) 50 min
- [Dem senator unhappy with Obama CIA pick](#) 22 min
- [CNNMoney: Obama pushes huge tax cuts](#)
- [Obama, Spears Twitter accounts hacked](#)
- [CNNMoney: Sales plummet for U.S. automakers](#)
- [German battlefield yields Roman surprises](#)
- [Sheriff: Boy not reported missing for 10 years](#)
- [Richard Simmons kisses anchor's foot](#)
- [Pictures of Obama girls' first day of school](#)
- [Old ladies bowl better than Obama](#)
- [Ticker: Candidates for RNC chair knock Bush](#)
- [Boy, 4, at rest stop says mom was shot](#)
- [People: Source says seizure killed Travolta son](#)
- [Parents share heartbreak of children's deaths](#)
- [Sex, violence common topics for MySpace teens](#)
- [Apple's Steve Jobs explains weight loss](#)
- ['Batman' character actor Pat Hingle dies](#)
- [SUV goes airborne, flies toward gas pump](#)
- [CNN Wire: Asia, Pacific stocks up early](#)

Video »



Simmons kisses anchor's foot 2:14



Four-year-old: Mom was shot 2:16



Madoff hearing 3:38

LIVE: CNN International's global perspective



CONSUMERGUIDE
2009 BEST BUY

AWARD WINNER



[Topics](#) » [Hamas](#) • [Bill Richardson](#) • [John Travolta](#) • [Gaza Crisis](#) • [Year in Review](#) • more topics »

Weather Forecast

Edition: [International](#) | [Set Pre](#)

updated 9:17 p.m. EST, Mon January 5, 2009

[Make CNN Your Home Page](#)



updated 55 minutes ago

'Friendly fire' kills three Israeli soldiers

The Israeli military surrounded densely populated Gaza City late Monday as the death toll continued to mount in the war-torn territory and both sides showed little interest in international calls for a truce. Military officials also said "friendly fire" killed three Israeli troops in an explosion in northern Gaza. full story

Other News

- [Franken claims victory as lawsuit looms](#) 54 min
- [Dem senator unhappy with Obama CIA pick](#) 26 min
- [CNNMoney: Obama pushes huge tax cuts](#)
- [Obama, Spears Twitter accounts hacked](#)
- [CNNMoney: Sales plummet for U.S. automakers](#)
- [German battlefield yields Roman surprises](#)
- [Sheriff: Boy not reported missing for 10 years](#)
- [Richard Simmons kisses anchor's foot](#)
- [Pictures of Obama girls' first day of school](#)
- [Old ladies bowl better than Obama](#)
- [Ticker: Candidates for RNC chair knock Bush](#)
- [Boy, 4, at rest stop says mom was shot](#)
- [People: Source says seizure killed Travolta son](#)
- [Parents share heartbreak of children's deaths](#)
- [Sex, violence common topics for MySpace teens](#)
- [Apple's Steve Jobs explains weight loss](#)
- ['Batman' character actor Pat Hingle dies](#)
- [SUV goes airborne, flies toward gas pump](#)
- [CNN Wire: Asia, Pacific stocks up early](#)

[all news from the past 24hrs »](#)

Popular News

[SEE TOP 10](#)

Video »



Simmons kisses anchor's foot 2:14



Four-year-old: Mom was shot 2:16



Madoff hearing 3:38

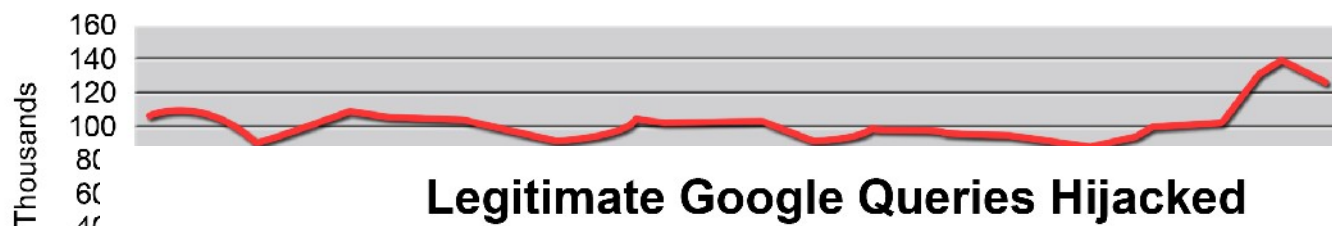
[LIVE: CNN International's global perspective](#)



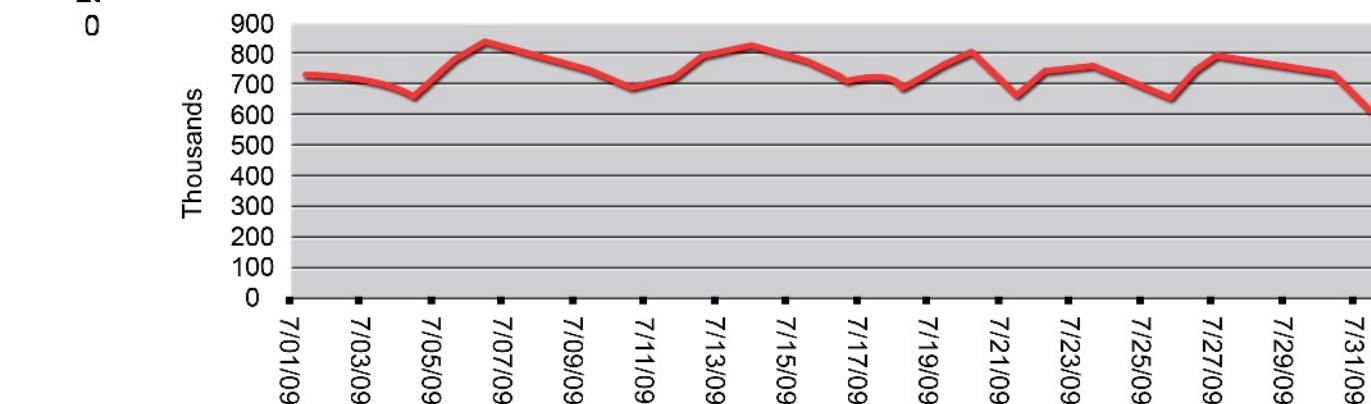
Legitimate Ads Replaced by Vimax Ads



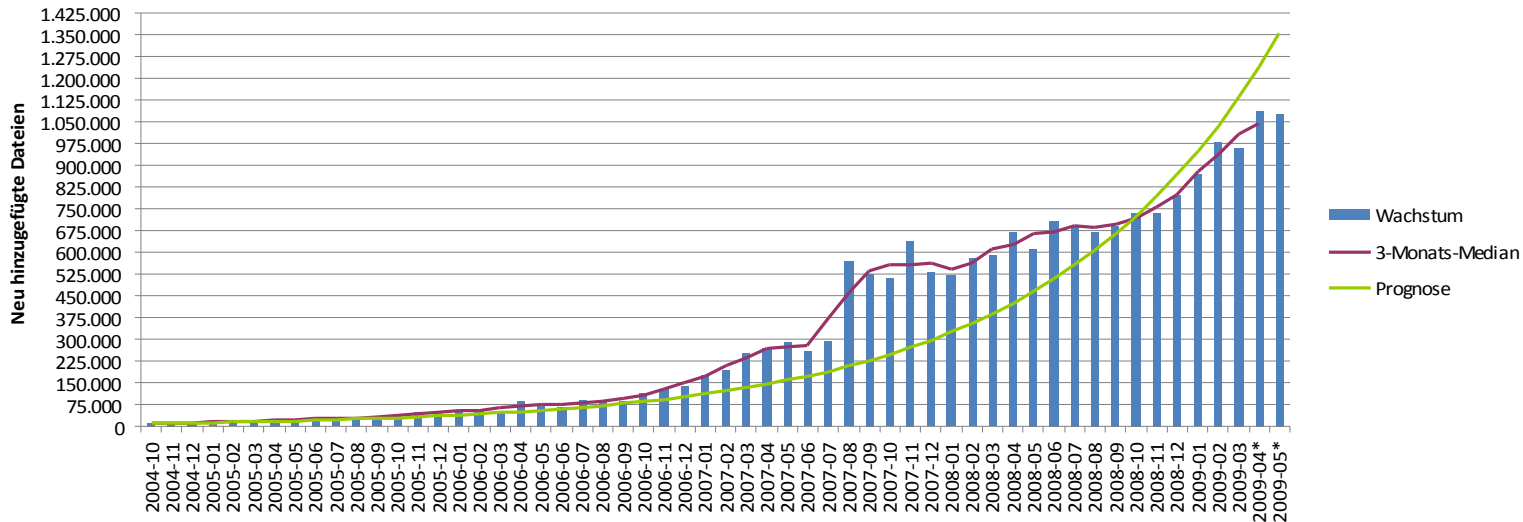
Unique IPs Exposed to Fake Antivirus Instead of Porn



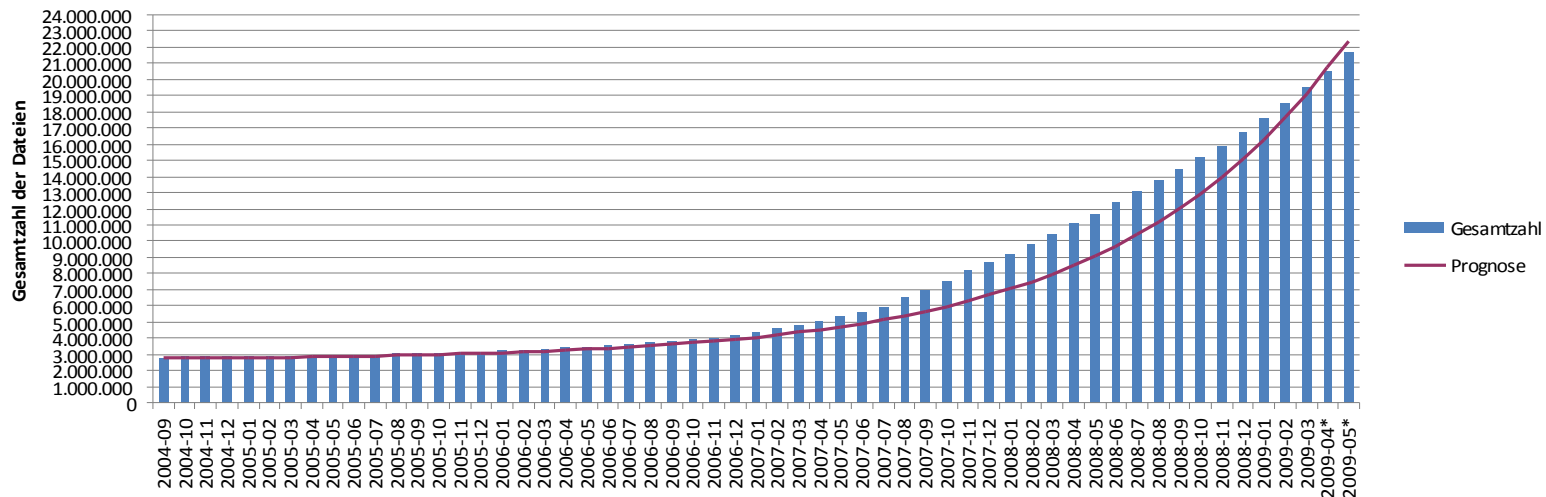
Legitimate Google Queries Hijacked



Neu hinzugefügte Dateien in der Malware-Sammlung von AV-Test.o

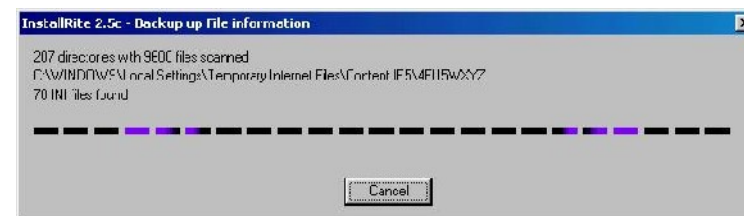


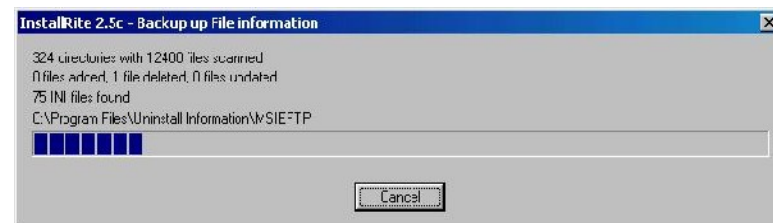
Gesamtzahl der Dateien in der Malware-Sammlung von AV-Test.o

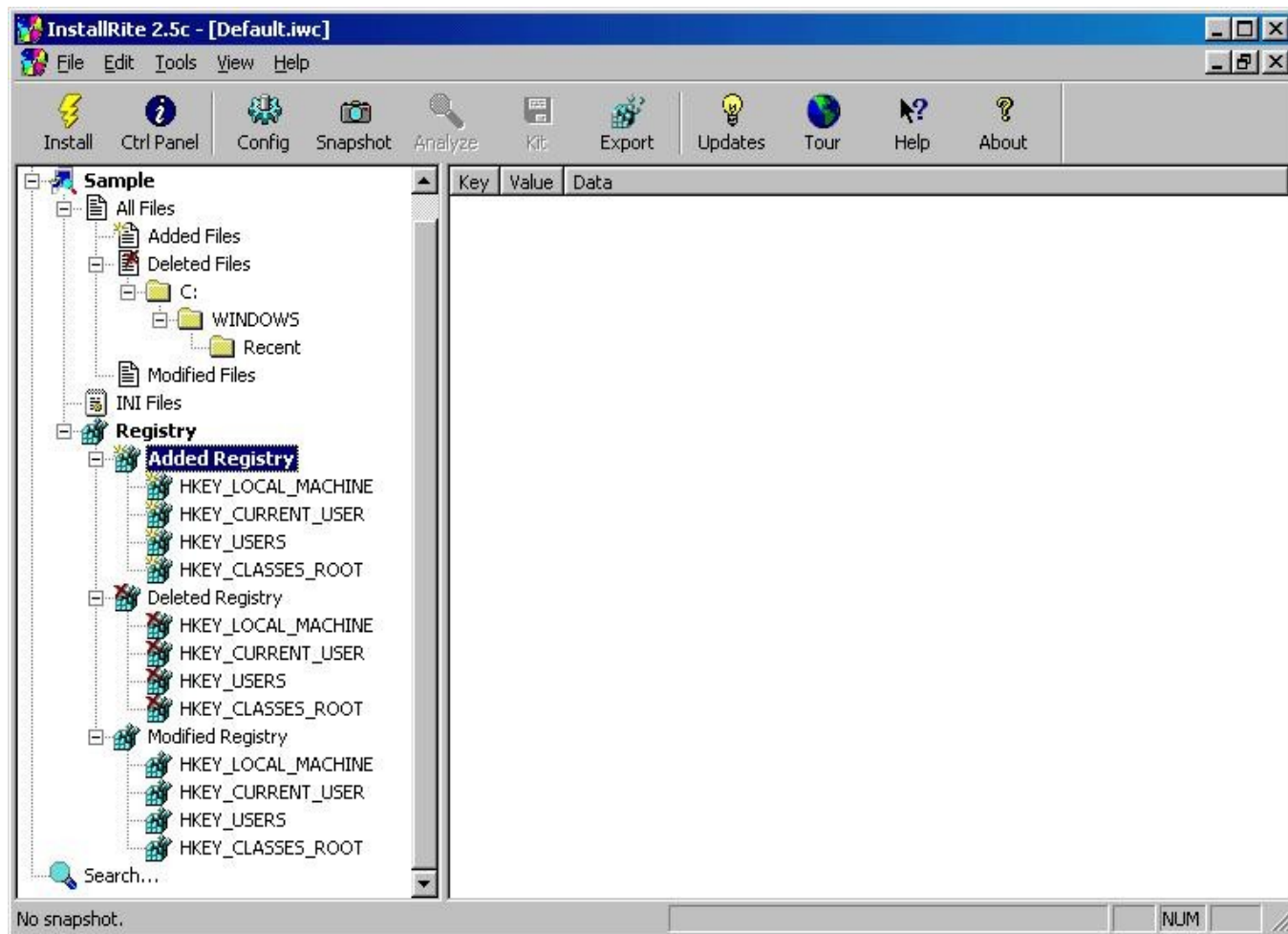


Stand 8.12.:
ca. 27 Mio
Samples

WWW








```
C:\D:\SunshineRelease\sunshineApp.exe

Sunshine 1.3.101, Copyright (c) 2006-2009 AU-Test GmbH, Magdeburg, Germany
~~~~~

Licensed to: #1203 AU-Test GmbH

Loading Database...

0 keys in the database
0 files in the database
0 processes in the database

Type command (help for a list of commands): aa
256523 keys inserted
10252 files inserted

Type command (help for a list of commands): cf
c:\WINDOWS\system32\evilmalware.exe

Type command (help for a list of commands): mf
c:\WINDOWS\system32\drivers\etc\hosts

Type command (help for a list of commands): ck
CreatedKey:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GoodApp
```

aa = add all

cf = created files

mf = modified files

ck = created keys

PackageGUI v0.3

7 of 8 samples processed

current sample: samples\unknown_malware

free disk space: 56,084,561,920 Bytes

Created files: 2 Created registry entries: 0

duration of infection: 0 min 11 sek network connection: internet

state: Malware executed. Awaiting creation of packages.

comment: unknown malware

Create snapshot Start Malware Create Package Re-Ghost

Package Manager 1.3.101 (AV-Test.org)

File Edit View Use Cases Help

Testset [C:\wildist (606)]

Package	Files	Mo...	Keys	Values
yahag.exe	7	0	0	0
yahak.exe	5	0	0	1
yahap.exe	4	0	3	7
yahaq.exe	4	0	3	7
yahat.exe	4	0	3	8
yahau.exe	4	0	3	7
zafia.exe	8	0	1	11
zafib.exe	18	0	1	25
zafic.exe	21	0	1	28
zafid.exe	13	0	1	15
zafif.exe	17	0	1	16
zindos.exe	1	0	0	1

Bagle

bagle111f.exe	5	0	0	3
bagle12cf.exe	2	0	0	1
bagle13ef8.exe	4	0	17	48
bagle1421f.exe	4	0	0	0
bagle1442c.exe	2	0	1	2
bagle16fa1.exe	4	0	17	48
bagle17349.exe	1	0	0	1
bagle17c00.exe	3	0	0	2
bagle17d26.exe	1	0	0	1
bagle1857c.exe	5	0	0	1
bagle18d5d.exe	4	0	0	0
bagle18e45.exe	6	0	0	3
bagle1a2ce.exe	5	0	0	0
bagle1b84d.exe	5	0	1	2
bagle1be57.exe	5	0	0	1

File name	Type	Size	Checksum (MD5)	Annotati
Created files				
c:\WINDOWS\system32\exeldr32.exe	PE Executable/Library	51424	121583934b15f82f6ae41230a6adad1d	
c:\WINDOWS\system32\taskmgr32.dll	PE Executable/Library	0		
c:\WINDOWS\system32\wintsk32.exe	PE Executable/Library	51424	121583934b15f82f6ae41230a6adad1d	Referenc
c:\yahat.exe	PE Executable/Library	51424	121583934b15f82f6ae41230a6adad1d	

Referenced files: 0 Referenced registry entries: 1

Key	Value	Data
Start keys		
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	MicrosoftServ...	C:\WINDOWS\system32\wintsk32.exe
Not classified		
HKLM\SOFTWARE\Microsoft\Snakes	Web	http://www.indiansnakes.cjb.net
HKLM\SOFTWARE\Microsoft\Snakes	Author	R0xx , C0bra , dEvIL inC4rn4Te
HKLM\SOFTWARE\Microsoft\Snakes	Version	2
HKLM\SOFTWARE\Microsoft\Snakes	Date	28.6.2003
HKLM\SOFTWARE\Microsoft\Snakes	Comments	This system belongs to the great indians...

Package information

Package name: yahat.exe

Additional information:

☐ Default Layer
 ☐ Marked for removal
 ☐ Bad packages
 ☐ Search results
 ☐ **Bagle**
 ☐ Layer 5

http://localhost:8080/classification_tree.php

SABRE Security VxClass - Home SABRE Security VxClass - Classifi... SABRE Security VxClass - Classificatio...

Classification Results

Search 466 Regular expression

yara-project
YARA: A malware identification and classification tool

Project Home Downloads Wiki Issues Source

Summary | Updates | People

YARA in a nutshell

YARA is a tool aimed at helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families based on textual or binary patterns contained on samples of those families. Each description consists of a set of strings and a Boolean expression which determines its logic. Let's see an example:

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example" /* NEW on version 1.3! */
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

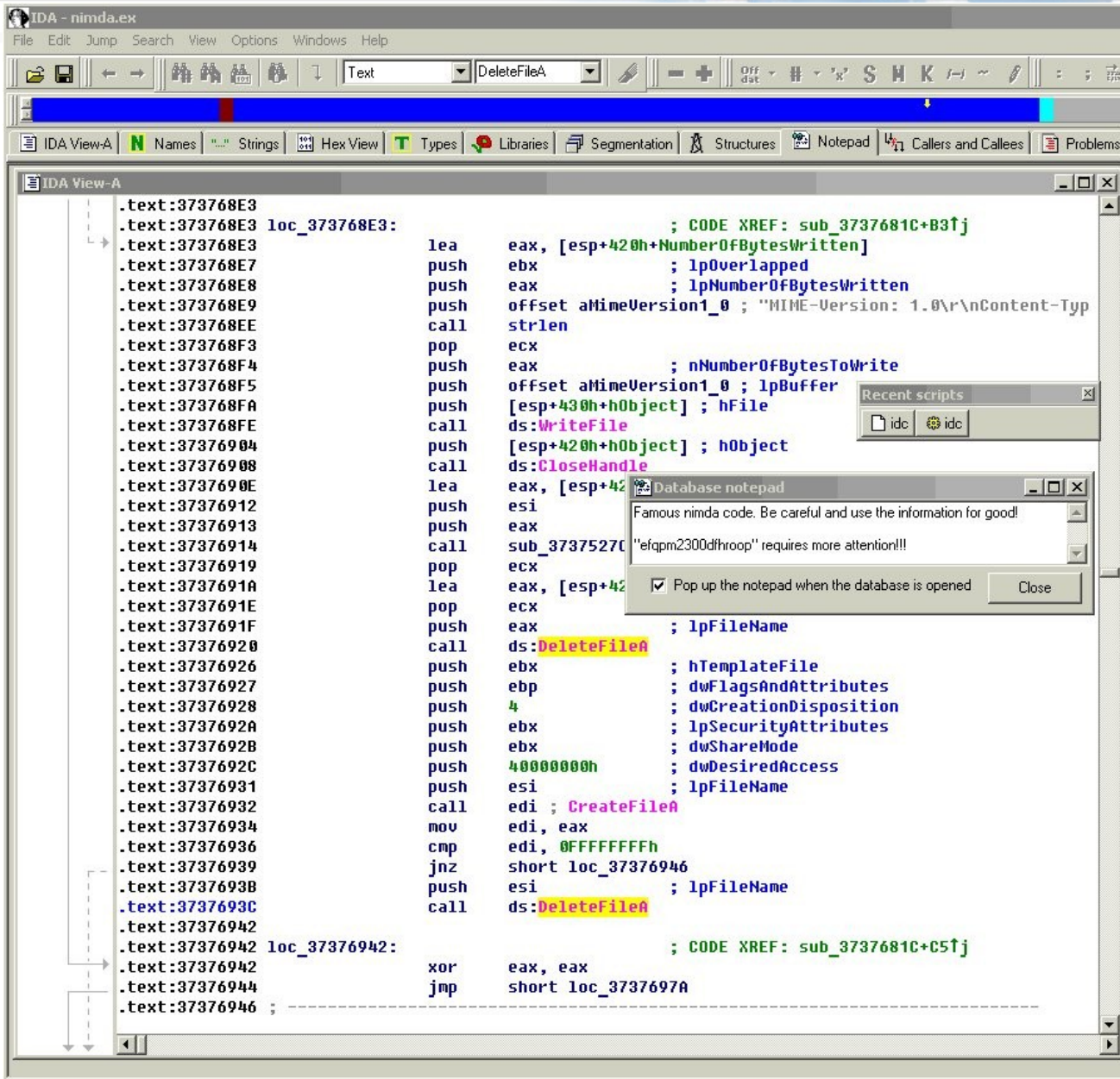
    condition:
        $a or $b or $c
}
```

Image

The rule above is telling YARA that any file containing one of the three strings must be reported as **silent_banker**.

This is just a simple example, more complex and powerful rules can be created by using binary strings with wild-cards, case-insensitive text strings, special operators, regular expressions and many other features that you can find explained in [YARA's documentation](#).

YARA is multi-platform, running on Windows, Linux and Mac OS X, and can be used through its command-line interface or from your own Python scripts with the yara-python extension.



Command "JumpEnter" failed
Searching down CASE-SENSITIVELY for binary string ...
Search failed.
Command "JumpBinaryText" failed
Searching down CASE-INSENSITIVELY for binary string nimda...
Search failed.
Command "AskBinaryText" failed
Searching down CASE-INSENSITIVELY for binary string "nimda"...
Search completed. Found at 37379104.

AU: idle Down Disk: 54GB 0000693C 3737693C: sub_3737681C+120

Interne Tools ...



Is Desktop Antivirus Dead?

Analysts say signature-based checking can no longer keep up with flood of new viruses.

Ellen Messmer, Network World

Apr 6, 2007 5:00 pm

[News > Security](#)

Signature-based antivirus is dead: Get over it

By [Liam Tung, ZDNet.com.au](#)

29 April 2008 04:41 PM

Tags: [antivirus](#), [competition](#), [infection](#), [malware](#), [trojan](#), [heuristic](#), [signature](#), [race to zero](#)

A hacking competition will attempt to prove that signature-based antivirus is dead but security vendors say, apart from signatures, antivirus is alive and well.

Schneier on Security

A blog covering security and security technology.

[« John Mueller](#)

November 10, 2009

Is Antivirus Dead?

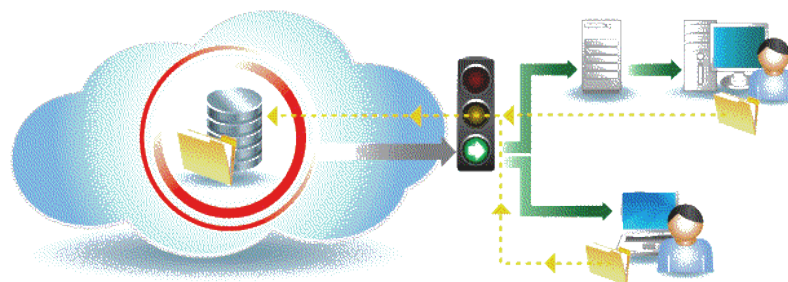
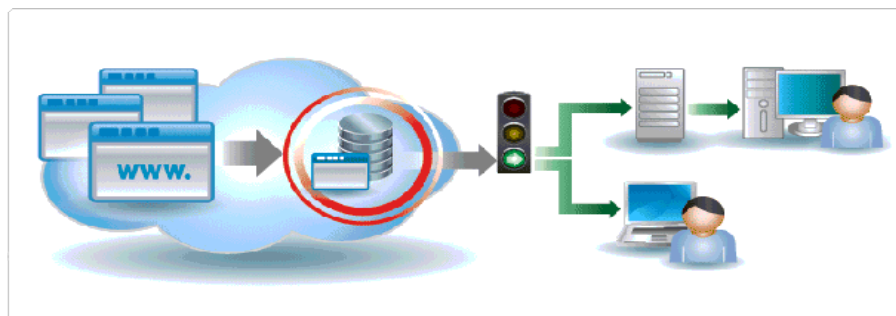
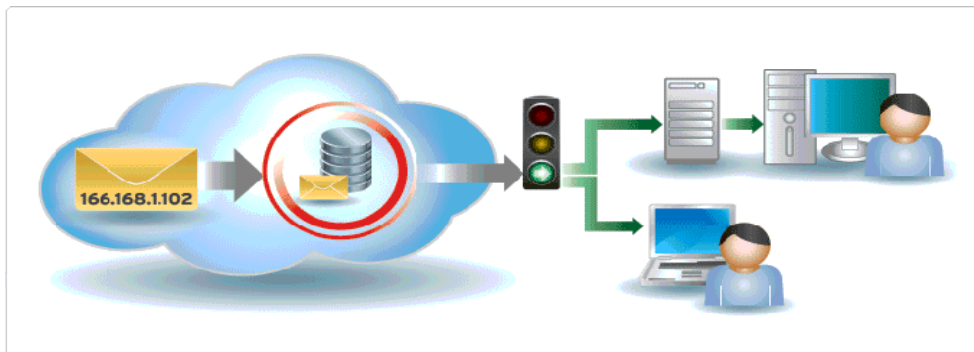
Ellen Messmer, Network World



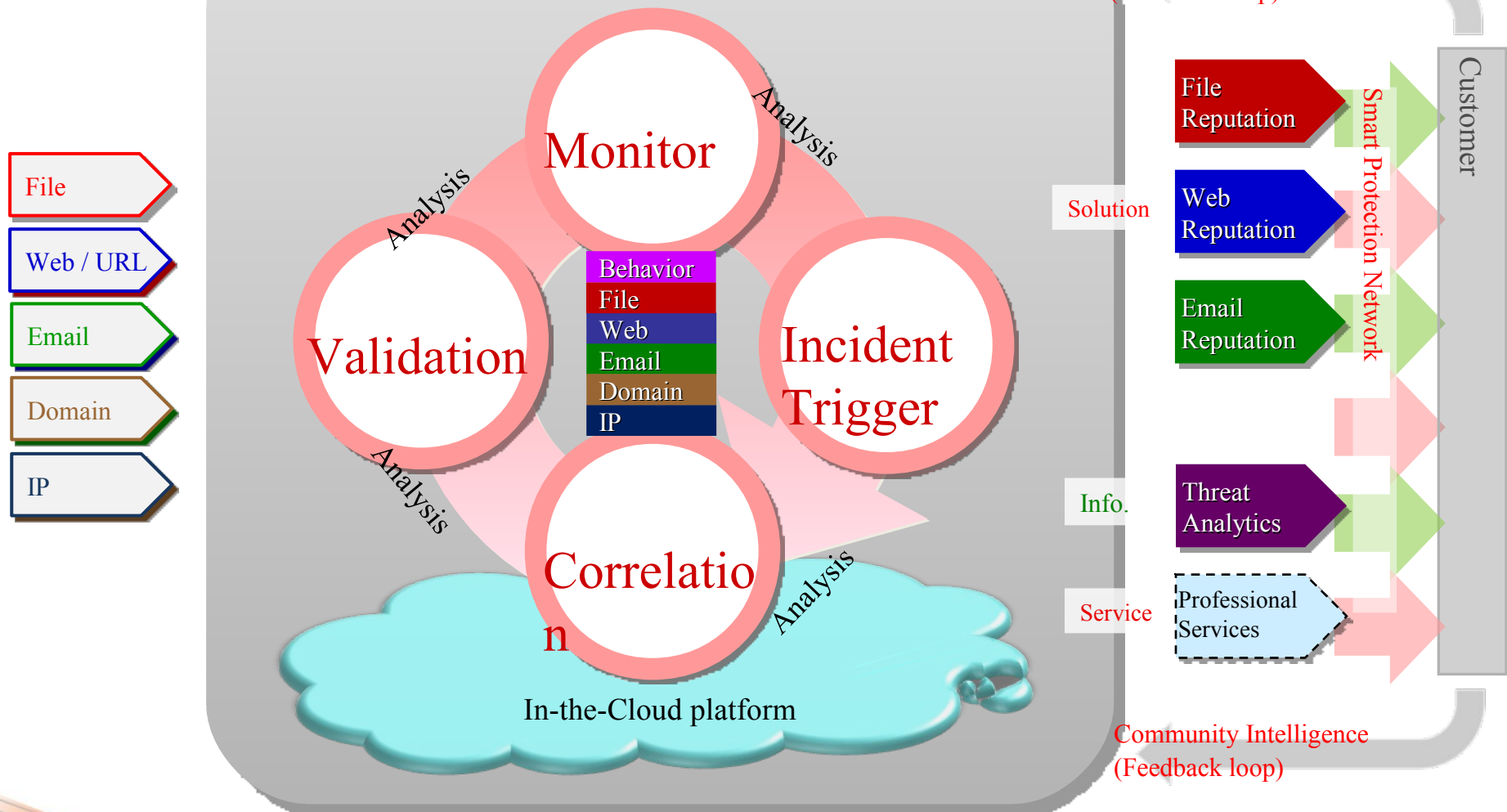
courtesy stock.xchng



Images courtesy de.wikipedia.org



Smart Protection Network



AV/AS/CS/FW/PM/IPS/DLP/TLM/B&R

User Education/Awareness

Noch nicht genug? ;-)

<http://blog.trendmicro.com>

<http://us.trendmicro.com/us/trendwatch/>

<http://www.smartprotectionnetwork.com>

Kontakt: [Rainer_Link AT trendmicro DOT de](mailto:Rainer_Link_AT_trendmicro_DOT_de)