Cyber-security update

Sebastian Lopienski

CERN Computer Security Team

Acknowledgements

Thanks to the following people (all CERN/IT) for their contributions and suggestions:

- Lionel Cons
- Sebastien Dellabella
- Jan Iven
- Wojciech Lapka
- Stefan Lueders
- Djilali Mamouzi
- David Myers
- Giacomo Tenaglia
- Romain Wartel

Overview

A small selection of highlights
in computer/ software/ network security
for the last several months:

- vulnerabilities
- attack vectors
- malware (and scareware)
- mobile security
- Linux vulnerabilities
- at CERN (in the HEP community)
- general trends

Vulnerabilities

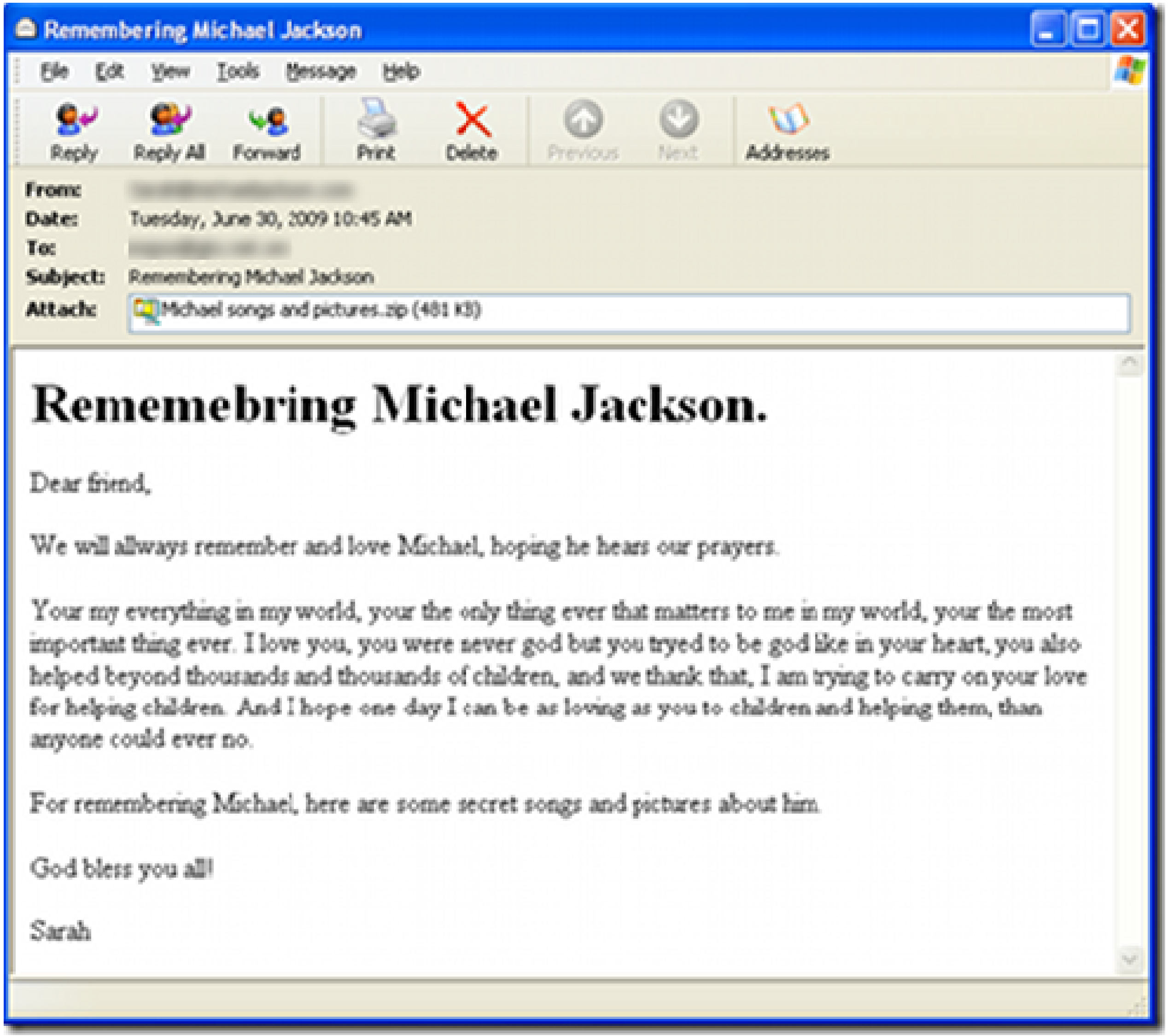
- Adobe Reader, Flash (Windows, Mac, Linux), Acrobat
- Windows
  - ActiveX Video Controls, spreadsheet ActiveX, DirectShow
  - TCP/IP stack processing (from 2008, now patched)
  - SMB2 (Server Message Block protocol) on Vista and 2008
  - 2 critical flaws in Windows 7 (before its official release)
- Mac OS X, iTunes, Java for Apple
  - Snow Leopard initially included outdated Flash player
- Web browsers:
  - Firefox (Just-in-time JS compiler, URL bar spoofing etc.)
  - IE (out-of-cycle patch in July)
  - Google Chrome; Safari
- XML libraries in products of Sun, Apache and Python
- Oracle DB, Application Suite

Getting infected

- Main infection vector: surfing the Web
  - compromised legitimate Web sites, or
  - newly registered malware domains
    - hot topics: Michael Jackson’s death, Samoa tsunami, swine flu…
    - domains quickly (automatically) registered,
      with names based on Google trends analysis
    - traffic attracted by SEO poisoning, e-mails, tweets etc.
  - drive-by download getting more sophisticated
    - malicious JavaScript checks visitor’s system for vulnerabilities in OS, browser, plug-ins
      (PDF reader, Java, Flash)

DI

Getting infected



Remembering Michael Jackson
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses

From: [redacted]
Date: Tuesday, June 30, 2009 10:45 AM
To: [redacted]
Subject: Remembering Michael Jackson
Attach: Michael songs and pictures.zip (481 KB)

Rememebring Michael Jackson.

Dear friend,

We will allways remember and love Michael, hoping he hears our prayers.

Your my everything in my world, your the only thing ever that matters to me in my world, your the most important thing ever. I love you, you were never god but you tryed to be god like in your heart, you also helped beyond thousands and thousands of children, and we thank that, I am trying to carry on your love for helping children. And I hope one day I can be as loving as you to children and helping them, than anyone could ever no.

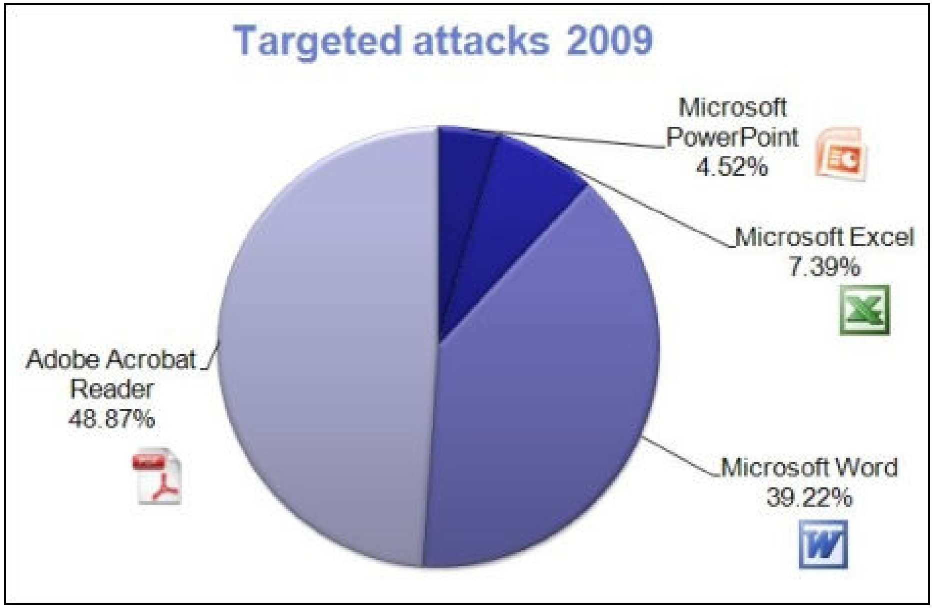
For remembering Michael, here are some secret songs and pictures about him.

God bless you all!

Sarah

Getting infected

- Also via e-mail attachments with exploits
  - mainly PDFs, and MS Office files
  - more common for targeted (*spear*) attacks

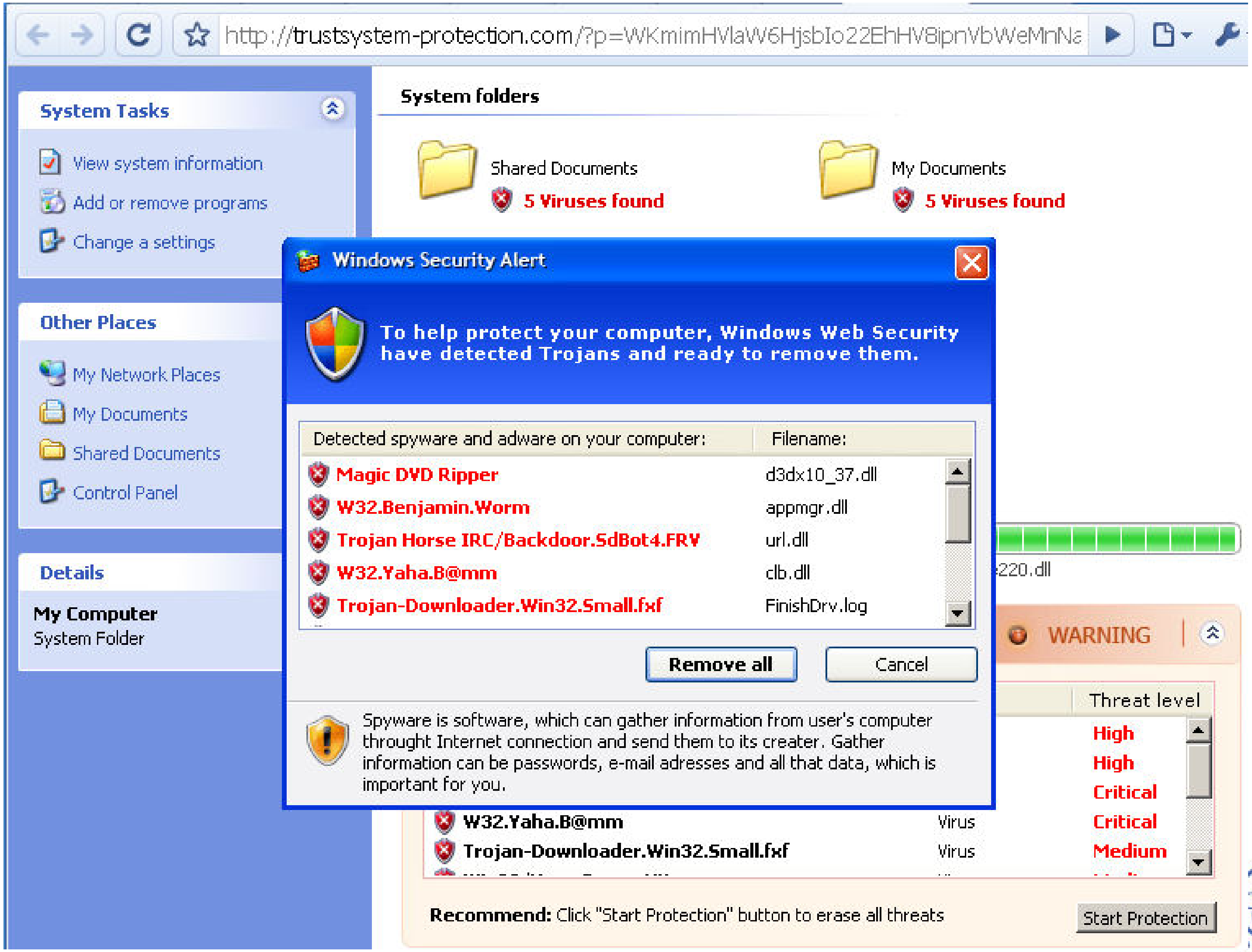


From F-Secure: http://www.f-secure.com/weblog/archives/00001676.html

- More exotic: a virus infecting Delphi compiler
  - then all compiled code also gets infected

Scareware

- Fake Windows folder „scanner” (= an image)



http://trustsystem-protection.com/?p=WKmimHVlaW6HjsbIo22EhHV8ipnVbWeMnNa

System Tasks

View system information

Add or remove programs

Change a settings

Other Places

My Network Places

My Documents

Shared Documents

Control Panel

Details

My Computer
System Folder

System folders

Shared Documents
5 Viruses found

My Documents
5 Viruses found

Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
Magic DVD Ripper	d3dx10_37.dll
W32.Benjamin.Worm	appmgr.dll
Trojan Horse IRC/Backdoor.SdBot4.FRV	url.dll
W32.Yaha.B@mm	clb.dll
Trojan-Downloader.Win32.Small.fxf	FinishDrv.log

Spyware is software, which can gather information from user's computer throught Internet connection and send them to its creater. Gather information can be passwords, e-mail adresses and all that data, which is important for you.

220.dll

WARNING

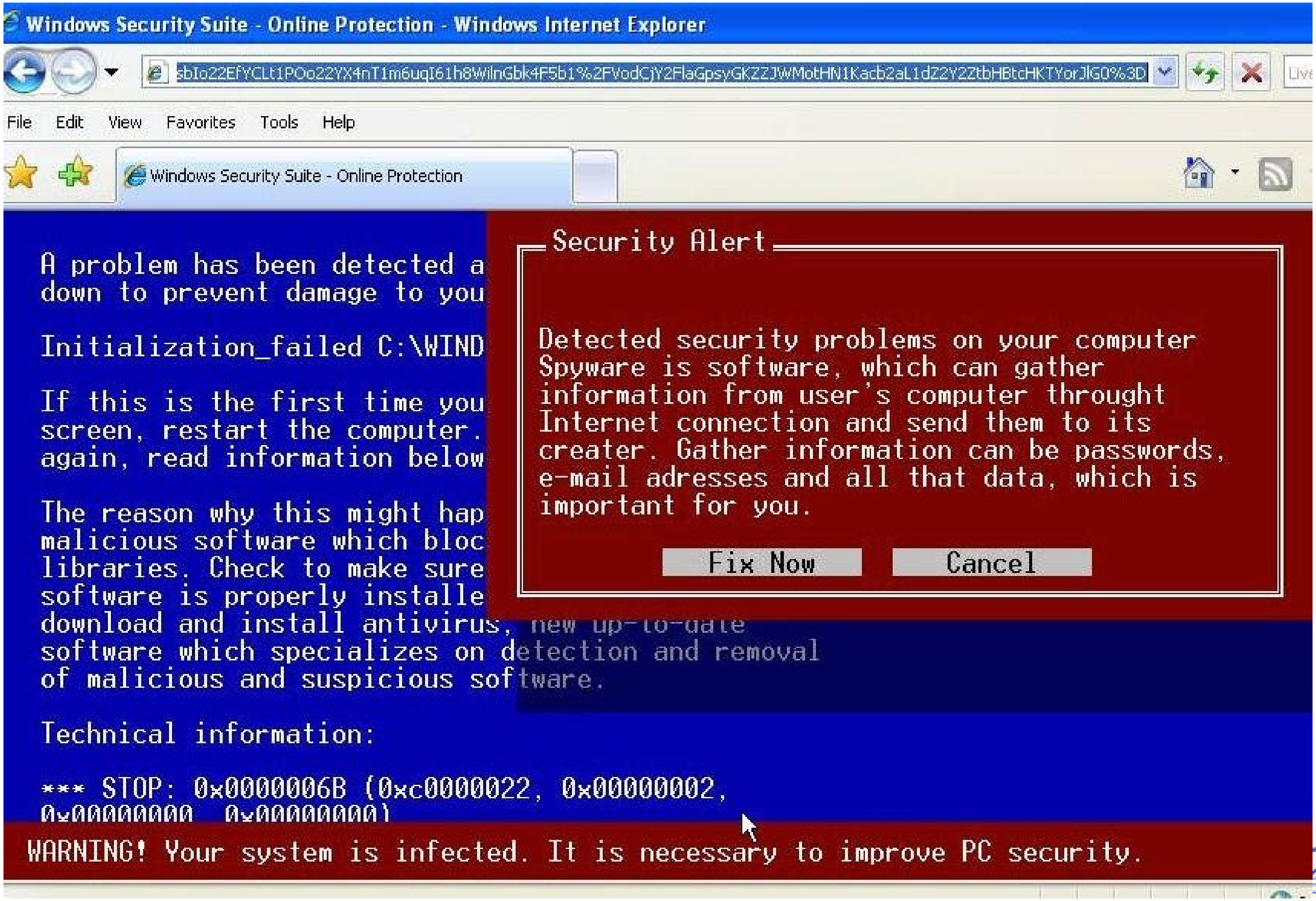
		Threat level
		High
		High
		Critical
W32.Yaha.B@mm	Virus	Critical
Trojan-Downloader.Win32.Small.fxf	Virus	Medium

Recommend: Click "Start Protection" button to erase all threats

From http://f-secure.com/weblog/archives/00001773.html

Scareware

- Fake „Blue Screen of Death”


Windows Security Suite - Online Protection - Windows Internet Explorer
sbIo22EfYCLt1POo22YX4nT1m6uqI61h8WilnGbk4F5b1%2FVodCjY2FlaGpsyGKZZJWMotHN1Kacb2aL1dZ2Y2ZtbHBtcHKTYorJlG0%3D
File
Edit
View
Favorites
Tools
Help
Windows Security Suite - Online Protection

```
A problem has been detected a
down to prevent damage to you

Initialization_failed C:\WIND

If this is the first time you
screen, restart the computer.
again, read information below

The reason why this might hap
malicious software which bloc
libraries. Check to make sure
software is properly installe
download and install antivirus, new up-to-date
software which specializes on detection and removal
of malicious and suspicious software.

Technical information:

*** STOP: 0x0000006B (0xc0000022, 0x00000002,
0x00000000, 0x00000000)
```

Security Alert

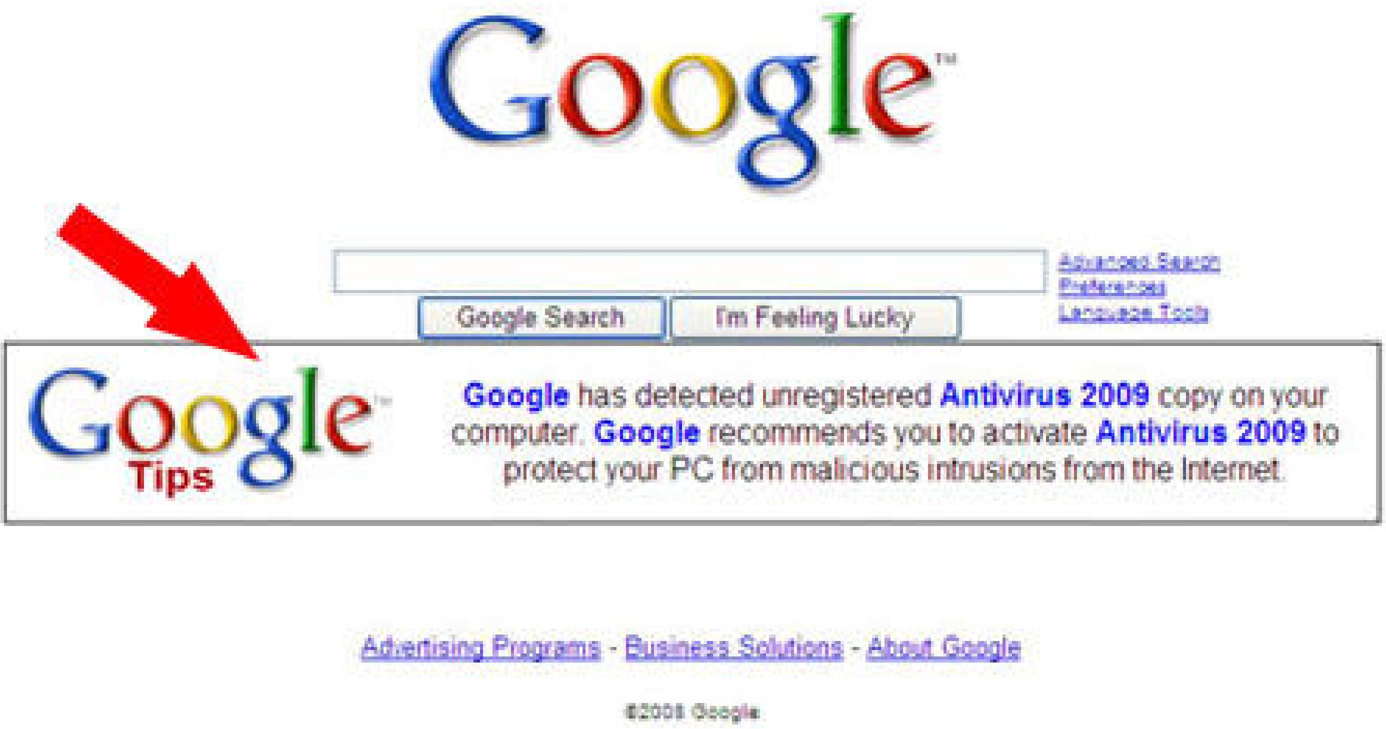
Detected security problems on your computer
Spyware is software, which can gather
information from user's computer throught
Internet connection and send them to its
creater. Gather information can be passwords,
e-mail adresses and all that data, which is
important for you.

WARNING! Your system is infected. It is necessary to improve PC security.

From http://blogs.zdnet.com/security/?p=3912

Scareware

- Fake “Google tip”
  (added with a malicious Browser Helper Object)



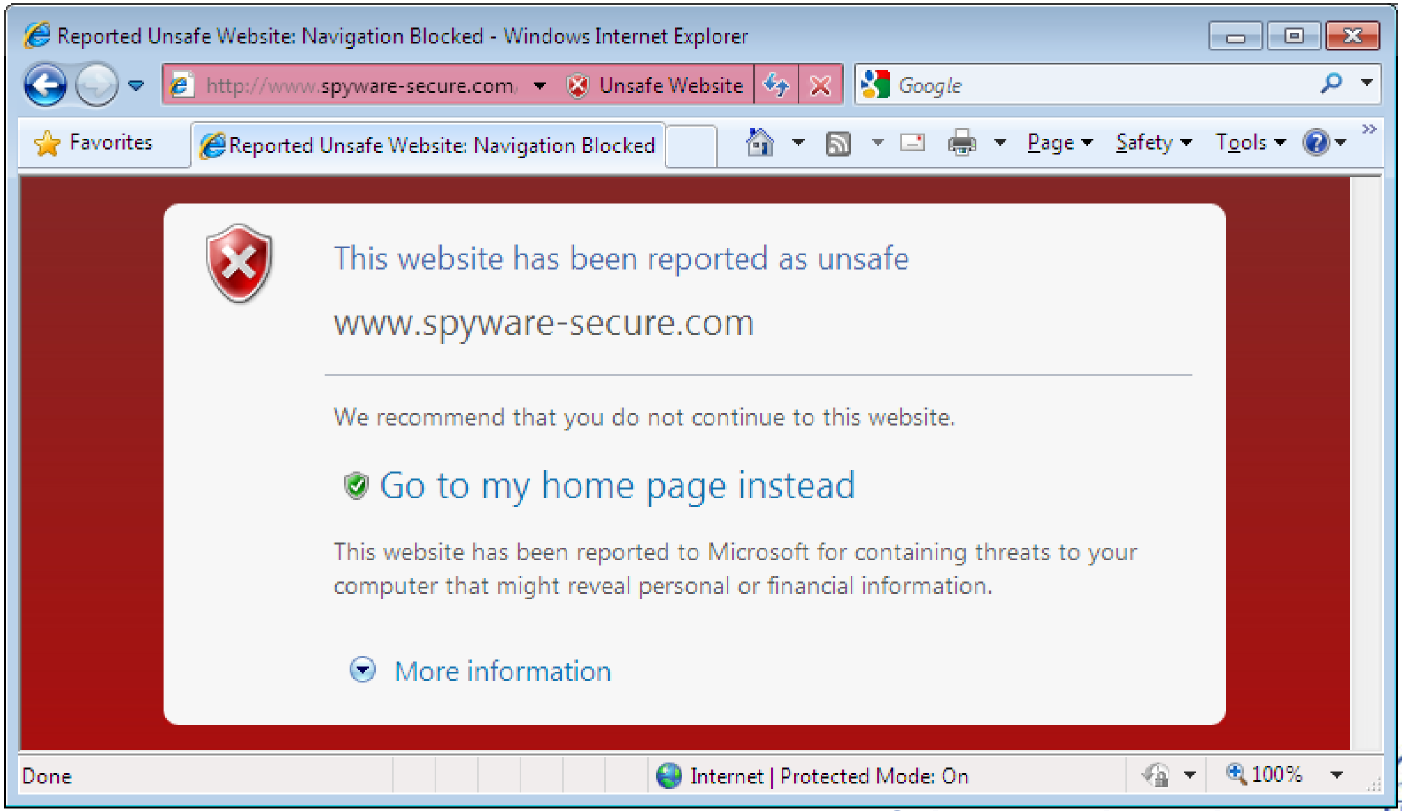
Google has detected unregistered Antivirus 2009 copy on your computer. Google recommends you to activate Antivirus 2009 to protect your PC from malicious intrusions from the Internet.

Scareware

- Scareware (rogue AV)
  - it’s only growing!
  - distribution: Web, e-mail (like malware)
  - scares user (*„Your computer is infected”*)
    to make them buy fake security/AntiVirus products
  - a „free scan” always reveals „infections”
  - “hybrid” version: with botnet “feature”
  - some even block all apps except IE browser
  - one license $50-80
  - total revenue estimated at $34M monthly

Avoiding infections - solutions

- Vigilance, as always… ☺
- Safe browsing - but which sites are safe?
  - using services like IE8's SmartScreen Filter



Reported Unsafe Website: Navigation Blocked - Windows Internet Explorer
http://www.spyware-secure.com/
Unsafe Website
Google
Favorites
Reported Unsafe Website: Navigation Blocked
Page
Safety
Tools

This website has been reported as unsafe

www.spyware-secure.com

We recommend that you do not continue to this website.

Go to my home page instead

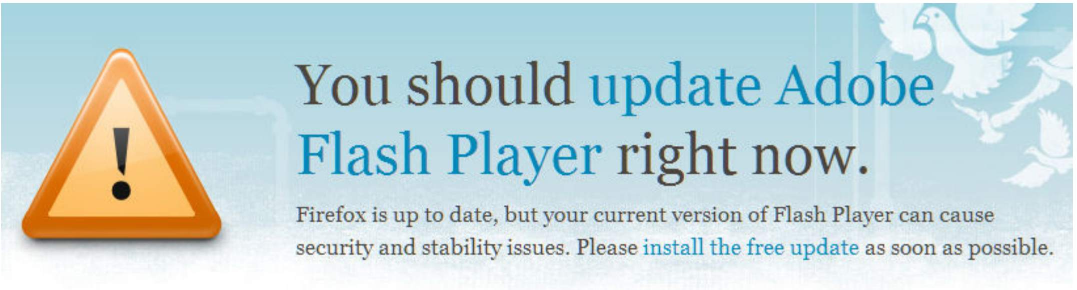
This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

More information

Done
Internet | Protected Mode: On
100%

Avoiding infections - solutions

- Keeping OS *and* software updated
  - using Secunia PSI/CSI
  - Firefox 3.5.3+ warns if Flash player plugin outdated



You should update Adobe Flash Player right now.

Firefox is up to date, but your current version of Flash Player can cause security and stability issues. Please install the free update as soon as possible.

- 10M people have followed a link to update Flash
- still, est. 75% of Firefox users have outdated Flash

  - Firefox 3.6 will check for newer versions of all plugins – as it already does for extensions
    - eventually: auto-update
    - (but 8% of Firefox users still on frozen Firefox 2.0)

Malware

- Long-living:
  - 80% remain infected after 1 month
  - 50% still infected after 10 months
- Stealth: not visible, some even hidden (rootkits)
- Secure ☺: some patch OS and applications, to avoid infections by other malware
- Botnets (infected machines) directed via:
  - fast-flux and/or short-living domains (e.g. ykqjm.sk)
  - legitimate services: Twitter, Google newsgroups
  - legitimate-looking domains: adobeupdating.com - owner in Zair, IP in S.Korea

Conficker

- Conficker worm (version C)
  - 50k malicious domains in 116 top-level domain, changing every day
  - didn't live up to its promise so far
  - a positive effect: collaboration between various players involved (Conficker Working Group)

Making money with malware

- How criminals make money with malware:
  - sending spam
  - Denial of Service (DoS) attacks/extortion
  - stealing credit card numbers
  - capturing credentials or hijacking sessions of PayPal, eBay, online banks, poker sites, MMORPGs, stock broker sites, ad services etc.
    - to steal money: $40M from US SMEs since 2004
    - some malware (e.g. URLZone) alter online bank statements to hide fraudulent transactions
    - Clampi targets 4500 (!) different financial institutions
  - encrypting files on your disc (ransomware)
  - scareware

Protection and detection

- Host-level
  - signature-based approach (AV) won’t last long
  - move to OS and network behavior analysis and anomaly detection
- Network-level
  - monitoring access to malicious IPs, domains etc., event correlation
  - ISPs consider detecting and informing their clients
    - pilot program in US (Comcast)
    - proposed legislation in Australia requires this
  - but no incentives for home users to clean their machines – spam or DDoS affect others/everyone

Mobile security

- iPhone
  - SMS Remote Code Execution Vulnerability
- Symbian
  - A worm
- Blackberry
  - update pushed out by UAE telecom contained spyware (stealing e-mails and SMSes)
- Android
  - various vulnerabilities

Linux kernel – NULL pointer

- NULL pointer vulnerability
  - usually just programming error -> crash
  - in kernel, can be exploited for privilege escalation
- Exploit 1. (complex)
  - "pulseaudio" (SUID/root) loads shared library
  - SUID applications didn't properly clear MMAP_PAGE_ZERO, ADDR_COMPAT_LAYOUT when executing other programs (CVE-2009-1895)
  - kernel bug in net/tun.c (CVE-2009-1897):

```
struct sock *sk = tun->sk;
[…]
if (!tun)
  return POLLERR;
```

“optimized” (removed!) by compiler

Linux kernel – NULL pointer

- Exploit 2. – older kernels w/ SELinux (simpler)
  - various kernel drivers using sock_sendpage() had NULL pointer issues (bad macro didn't actually initialize struct) - CVE-2009-2692
  - exploits: *wunderbar_emporium, enlightenment*
  - workaround: blacklist vulnerable kernel modules.
- Exploit 3. (trivial)
  - udp_sendmsg NULL pointer (CVE-2009-2698)
  - *therebel* exploit
  - workaround: blacklisting UDP ???

Attacks

- Ongoing SSH-based attacks against the academic community
  - a compromised account (password, key) → root privilege escalation via a known vulnerability→ hiding with rootkit techniques → more compromised accounts
  - periodic rootkit update
  - traditional injection techniques (/dev/mem, LKM)
  - inexperienced sites or forgotten unpatched hosts are an easy target
  - user community more and more spread, making investigations slower

Attacks contd.

- Root escalation via known vulnerabilities
  - udev exploits in spring
  - CVE-2009-2692/2698 still very popular
  - are you *really* patched?
  - some sites still vulnerable, putting others at risk
  - EGEE suspended all its affected sites and is now CVE-2009-2692/2698 free

At CERN

- User training and awareness raising helps reduce the impact of phishing emails
  - making users think before clicking is the best security measure...
- External hosting and cloud computing = “cloud” support in case of incidents…
  - a compromised, externally hosted Web site, but no logs available, so forensics impossible
- Watch your Web for information disclosure
  - due to misconfiguration, lack of awareness etc.
- Projects: WAS, Snorts rules, source code tools

Various stories

- eBooks remotely removed from Kindle devices
  - Orwell's "Animal Farm" and "1984“
  - Amazon will pay $150k to a high school student who lost his annotations
- “ATM hacking” presentation cancelled at BlackHat 2009 conference:
  - it‘s an annual tradition, to cancel a talk ☺
  - but ATMs do really get infected with malware
  - $9m stolen from ~130 ATMs in 49 cities in Nov ’08
  - BTW, suspicious ATMs discovered at DEFCON ’09

Various stories

- Identity theft & co
  - a man from Seattle stole personal files from other people's PCs using LimeWire filesharing software
  - when arrested, he had 8 different driver's licenses in his wallet
  - hackers officially changed name of a Swedish man
  - reporter changed Empire State Building ownership
- Security researchers hijacking botnets

Thank you!

Questions?

Sebastian.Lopienski@cern.ch

National cyber-security