

# Tendinte. Provocari. Oportunitati

Mircea MITU – IT Assist

# Agenda

- Tendinte
  - Browser / Email / Retele sociale & IM
  - SEO poisoning / Exploit-uri
  - Mobile / Mac / Atacuri directionate
- Provocari & Oportunitati

# Tendinte / Browser



# Tendinte / Browser



## Secunia Advisories

### Highlighted



[Internet Explorer iepeers.dll Use-After-Free Vulnerability](#)

2 weeks ago // 10,768 views



[Google Chrome Multiple Vulnerabilities](#)

1 week ago // 3,288 views



[Microsoft Windows "MsgBox\(\)" HLP File Execution Vulnerability](#)

4 weeks ago // 4,772 views

### Most popular - 3 hours

[Mozilla Firefox Multiple Vulnerabilities](#)



Issued 1 month ago // 104 views

[Adobe Flash Player Domain Sandbox Bypass Vulnerability](#)



Issued 1 month ago // 48 views

[Microsoft Internet Explorer Local File Disclosure Vulnerabilities](#)



Issued 2 months ago // 36 views

# Tendinte / Browser



# Tendinte / Browser



CanSecWest  
PWN2OWN

# Tendinte / Browser



# Tendinte / Browser



Interesting, PWN2OWN contestants all did homework. All successful. iPhone, Safari/OSX, IE8/Win7, Mozilla all fell. [#cansecwest](#)  
about 22 hours ago via web

# Tendinte / Browser

- Tinta multiplatforma:
  - Windows / Linux / Mac / Android / iPhone
- Exploatabil (browser, plugins, web apps)
- Phishing
- Inginerie sociala

# Tendinte / Email

- Al 2lea vector de atac
- Cel mai utilizat mijloc de comunicare pentru afaceri
- Spam personalizat:
  - Profil “tinta”
  - Bazat pe comunicate de presa

# Tendinte / Retele sociale & IM

- Tehnici: social engineering, exploits
- CAPTCHA poate fi decodată, ceea ce duce la crearea automată de conturi noi, utilizate apoi pentru spam, ID theft, botnets



# Tendinte / SEO poisoning

- Cuvinte cheie populare detectate prin Google si Twitter trends
- Site-uri si landing pages create utilizand aceste expresii populare
- Botnets utilizati pentru trafic => page rank mare
- In cateva ore => top 5 results
- Alte tehnici SEO poisoning: PDF/Flash redirection



security patch before pwn2own

Căutați

Căutare:  pe Web  pagini scrise în limba română  pagini din Români

Web [+ Afișați opțiunile...](#)

Rezultatele 1 - 10 din aproximativ 68.600 p

[Pwn2Own trifecta: Hacker exploits IE8, Firefox, Safari | Zero Day ...](#) - [ [Tradu această pagină](#) ]

[ ALSO SEE: **Pwn2Own** 2009: Safari/MacBook falls in seconds ]. A **security** researcher named "Nils" (he declined to provide his full name) performed a clean ...

[blogs.zdnet.com/security/?p=2934](http://blogs.zdnet.com/security/?p=2934) - [În Cache](#) - [Pagini similare](#)

[Pwn2Own Interview with Charlie Miller – Security Threat Research News](#) - [ [Tradu această pagină](#) ]

17 Mar 2010 ... For real-time updates: Twitter: @TheZDI Hash tag: #pwn2ownThe TippingPoint Zero Day Initiative (ZDI) is ... As always, we will not discuss a vulnerability **before** the ... Keep Systems Safe: **Patch** Alternative Browsers ...

[www.thesecurityblog.com/2010/03/pwn2own-interview-with-charlie-miller/](http://www.thesecurityblog.com/2010/03/pwn2own-interview-with-charlie-miller/)

[Pwn2own Safari](#) - [ [Tradu această pagină](#) ]

25 Mar 2010 ... Youtube.com Movies Two weeks **before** a browser hacking contest is to kick off ... Miller wasn't the only one hacking Safari at **PWN2OWN**, a **security** ... Apple **patches** Safari vulnerabilities ahead of **Pwn2Own** - forum topic. ...

[frogshrine.com/znkmk.php?on=pwn2own%20safari](http://frogshrine.com/znkmk.php?on=pwn2own%20safari) - [În urmă cu 6 ore](#)



security patch before pwn2own

Căutați

Căutare:  pe Web  pagini scrise în limba română  pagini din Români

Web [+ Afișați opțiunile...](#)

Rezultatele 1 - 10 din aproximativ 68.600 p

[Pwn2Own trifecta: Hacker exploits IE8, Firefox, Safari | Zero Day ...](#) - [ [Tradu această pagină](#) ]

[ ALSO SEE: **Pwn2Own** 2009: Safari/MacBook falls in seconds ]. A **security** researcher named "Nils" (he declined to provide his full name) performed a clean ...

[blogs.zdnet.com/security/?p=2934](http://blogs.zdnet.com/security/?p=2934) - [În Cache](#) - [Pagini similare](#)

[Pwn2Own Interview with Charlie Miller – Security Threat Research News](#) - [ [Tradu această pagină](#) ]

17 Mar 2010 ... For real-time updates: Twitter: @TheZDI Hash tag: #pwn2ownThe TippingPoint Zero Day Initiative (ZDI) is ... As always, we will not discuss a vulnerability **before** the ... Keep Systems Safe: **Patch** Alternative Browsers ...

[www.thesecondityblog.com/2010/03/pwn2own-interview-with-charlie-miller/](http://www.thesecondityblog.com/2010/03/pwn2own-interview-with-charlie-miller/)

[Pwn2own Safari](#) - [ [Tradu această pagină](#) ]

25 Mar 2010 ... Youtube.com Movies Two weeks **before** a browser hacking contest is to kick off ... Miller wasn't the only one hacking Safari at **PWN2OWN**, a **security** ... Apple **patches** Safari vulnerabilities ahead of **Pwn2Own** - forum topic. ...

[frogshrine.com/znmk.php?on=pwn2own%20safari](http://frogshrine.com/znmk.php?on=pwn2own%20safari) - În urmă cu 6 ore



Warning! Your computer is vulnerable to malware attacks.

We recommend you to check your system immediately.  
Press OK to start the process now



The screenshot shows the Windows Security interface. At the top, it displays 'Computer > Virus Scanner'. Below this, there are navigation options: 'Organize', 'Views', 'System properties', 'Uninstall or change a program', and 'Open Control Panel'. On the left, there are 'Favorite Links' including Documents, Pictures, Music, Recently Changed, Searches, and Public.

### Hard Drive Antivirus scanner

Local Disk (C:) 100% **6 infected files**

Local Disk (D:) 100% **4 infected files**

### Windows Security

**Antivirus Protection Disabled**

Threat Name	Threat type	Threat Level
Backdoor.Tidserv	Virus	High
W32.Daprosy	Virus	Critical
W32.Fujacks.CE!inf	Virus	Medium
Suspicious.MLApp	Virus	Medium
Trojan.Bankpatch.D	Virus	Medium

**Recommended:** Click "Erase infected" to erase all infected and suspicious files and make your system protected.

**Erase infected**

Status: **Windows Infected, 10 threats detected.**  
Browser: IE 7.0  
Operation system: Windows Vista

1024 bit **100% SECURE SITE**

puter. Are you sure you  
...exe?

This type of file can harm your computer. Are you sure you  
want to download packupdate\_buil....exe?



# Tendinte / Atacuri directionate

- Global:
  - Operation Aurora (MS10-002)
- Local:
  - Banking Trojans (phishing)
  - IRC bots (felicitari)
  - Scurgeri de informatii (inginerie sociala, exploatarea vulnerabilitatilor)

# Tendinte / Exploit-uri

- **Vuln: Microsoft Security Advisory (979352)**
  - Vulnerability in Internet Explorer Could Allow Remote Code Execution
  - Published: January 14, 2010 | Updated: January 21, 2010
  - Also known as MS10-002
- **Exploit: Operation Aurora (Google vs China)**

# Tendinte / Exploit-uri

- PDF
- Documente Office
- MS Internet Explorer
- Flash
- Imagini
- ~~Aplicatii regionale populare~~

# Tendinte/ Mobile & Mac

- Mobile (Symbian, iPhone, Android, BlackBerry):
  - Smartphone-urile devin foarte populare
  - Oferă oportunități noi distributiei de malware și spionajului economic
- Mac:
  - +5% market share
  - Exploit-uri (PDF, Flash, WebKit)

# Tendinte / Mobile & Mac



**dragosr**

iPhone sploit used Safari and downloaded contacts from phone to attacker. [#pwn2own](#) [#cansecwest](#)

about 22 hours ago via web

# Provocari

- Security awareness
- Solutii orientate nevoilor SMB
- Piraterie
- Comunitate InfoSec (experti in securitate IT)

# Oportunitati

- Campanii educationale:
  - Security awareness
  - Solutii si servicii de securitate
  - Formarea unui nucleu de experti InfoSec

# Oportunitati

- Masuri antipiraterie:
  - Licentiere flexibila (SaaS)
  - Structura de preturi orientata pietii romanesti
- Solutii si servicii de securitate adaptate nevoilor SMB si VARs

**it** Assist    Departamentul tau IT

Servicii IT **sigure** pentru companii



**Red Bull**<sup>®</sup>

**SIEMENS**

**xerox**



**L'ORÉAL**<sup>®</sup>



**UNIVERSAL MUSIC GROUP**

# Multumesc

## Mircea Mitu – IT Assist

Twitter: @mirceamitu  
Company twitter: @itassist  
[www.itassist.ro](http://www.itassist.ro)