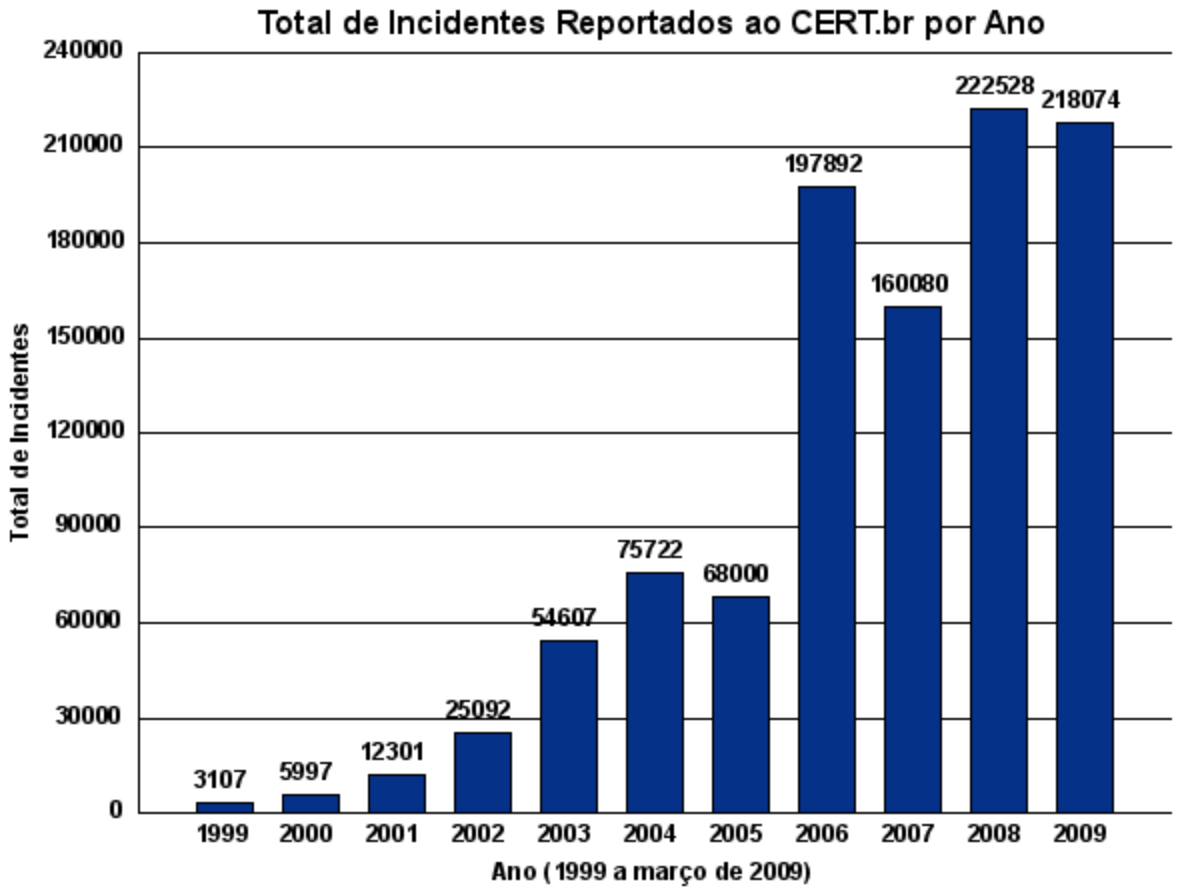
Ataques Complexos

Quando as ameaças tornam-se realmente híbridas!

TODAS AS INFORMAÇÕES, TEORIAS, DEMONSTRAÇÕES, FERRAMENTAS E CÓDIGOS CONTIDOS NESTA APRESENTAÇÃO SÃO APENAS PARA ALERTAR A AUDICÊNCIA / PLATÉIA SOBRE A POSSIBILIDADE DE UTILIZAR-SE ATAQUES COMPLEXOS PARA CRIAÇÃO DE UM CENÁRIO ONDE A MOTIVAÇÃO PODERÁ SER: FRAUDE, EXTORSÃO E GANHO FINANCEIRO.

Agenda

- ✓ O que são ataques complexos?
- ✓ Alguns vetores de ataque
- ✓ Utilizando-se de um *Framework* para Fraude
- ✓ Demonstrações
- ✓ *Botnets (Conficker)*
- ✓ Perguntas e Respostas


Total de Incidentes Reportados ao CERT.br por Ano
Total de Incidentes
240000
210000
180000
150000
120000
90000
60000
30000
0
3107
5997
12301
25092
54607
75722
68000
197892
160080
222528
218074
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
Ano (1999 a março de 2009)

O que são ataques complexos?

Definição

- ✓ Um “Ataque Complexo” é uma seqüência de ações comuns / ordinárias e ataques híbridos direcionados à vetores[1] diferenciados os quais, uma vez combinados, resultarão em uma ação de proporções maiores.
  - Exemplo:
    - *SYN Flood* → Criando uma situação de indisponibilidade do DNS Server;
    - *DNS Cache Poisoning* → Envenenando o DNS Server com uma entrada maliciosa;
    - *Drive-by-Download* → Comprometendo a máquina do usuário.

Construindo um Ataque Complexo

- ✓ Muitos dos cenários teorizados utilizam-se de dois principais grupos:
  - Infra-estrutura;
  - Serviços;
  - *Client-Side.*

Ataques Complexos: Exemplos Reais (?)

"Ataques de hackers causam problemas no Speedy, diz Telefônica" (9 de Abril de 2009)

(http://g1.globo.com/)

"Atenção! Não acessem o site do banco Bradesco se estiver utilizando Net Virtua." (12 de Abril de 2009)

(http://stoa.usp.br/walrus/weblog/)

"Entenda como funciona o ataque que derrubou o Speedy" (9 de Abril de 2009)

(http://g1.globo.com/)

"Ataque leva clientes do Virtua a site clonado de banco" (17 de Abril de 2009)

(http://g1.globo.com/)

Alguns vetores de ataque

Exemplo de vetores de ataques (Infra-estrutura)

✓*SYN Flood*[1]:
- Centenas de códigos.

✓*UDP Bomber*:
- Centenas de códigos.

✓*BGP Router Attack Tool*:
- `brat.c`

✓*BGP Test Tools & BGP Password Cracker:*
- `ciag-bgp-tools-1.00.tar.gz`

✓*MPLS Label Brute-forcer*:
- `mpls-lbf.c`

✓*MPLS Sniffer and Packet Forwarder*:
- `mpls-fwd.c`

✓*DNS Cache Poisoning*[1]:
- `baliwicked_host.rb`
- `h0dns_spoof.c`
- `dns_mre-v1.0.tar.gz`

Exemplo de vetores de ataques (Infra-estrutura)

✓Cisco:

- IOS FTP Server Multiple Vulnerabilities (Buffer Overflow);
- CVE-2004-0230;
- CVE-2006-3906;
- CVE-2008-0960;
- CVE-2008-1447;
- Etc.

✓Juniper:

- CVE-2004-0230;
- CVE-2007-6372;
- CVE-2008-0960;
- CVE-2008-1447;
- Etc.

✓Nortel:

- CVE-2008-0960;
- CVE-2008-1447;
- Etc.

✓Lucent:

- Multiple Router UDP Port 9 Information Disclosure;
- Brick Spoofed Address Communication Denial Of Service;
- CVE-2008-1447;
- Etc.

✓Outros:

- Vulnerabilidade não é privilégio apenas da:
  - Cisco, Juniper, Nortel e Lucent.

Exemplo de vetores de ataques (*Client-Side*)

✓Microsoft:

- MS08-078[1]
- MS09-002[1]
- MS09-014

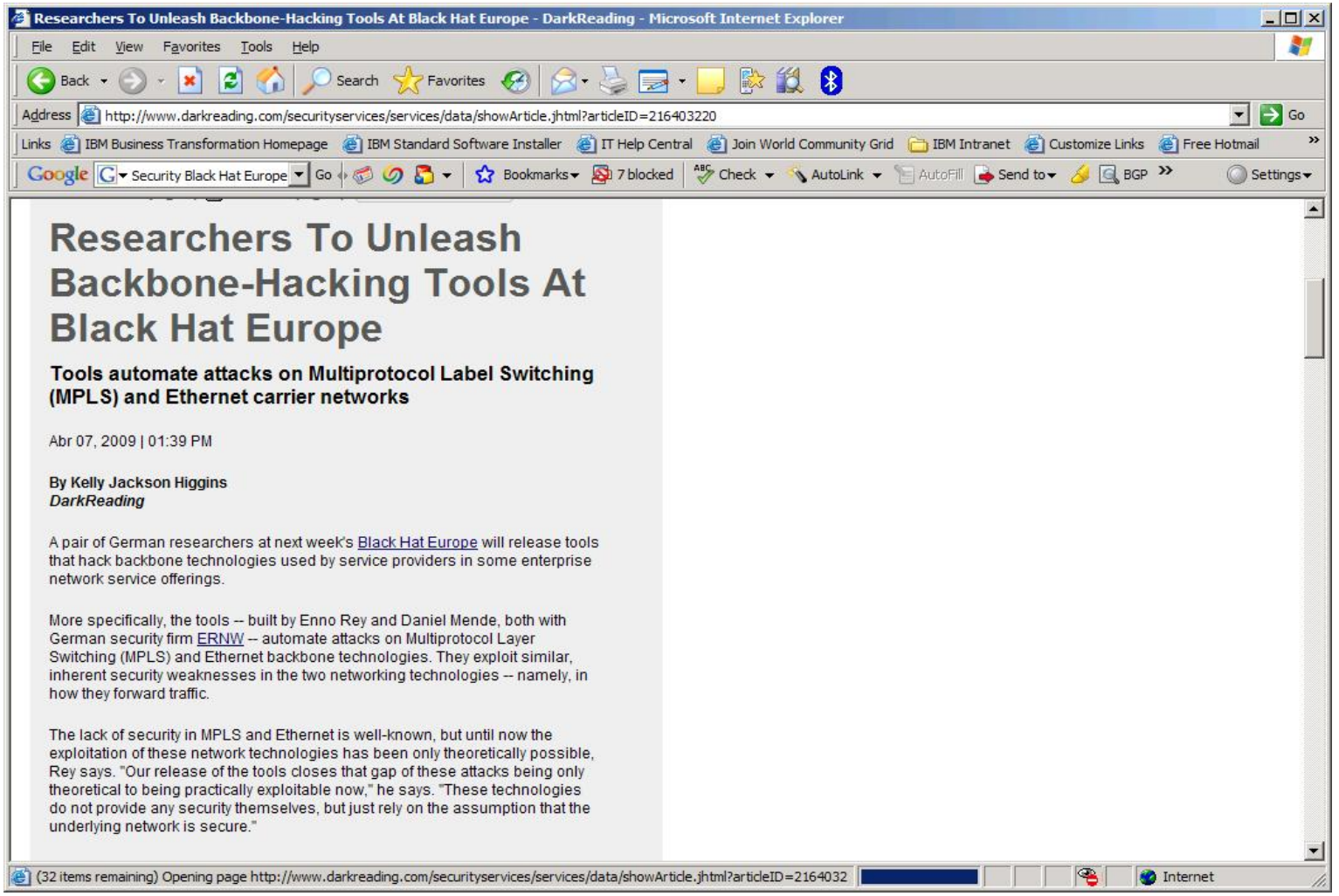
✓Mozilla:

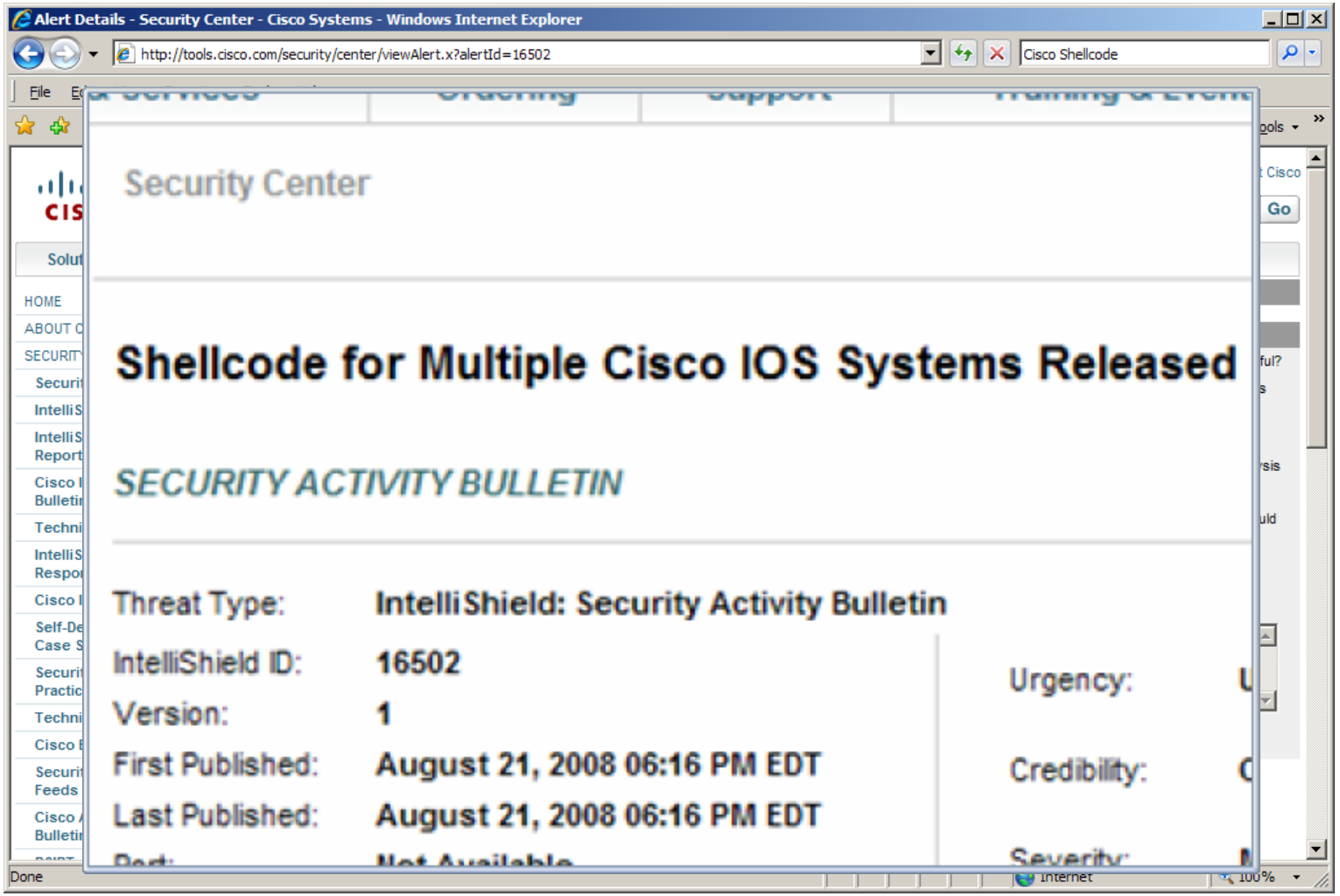
- MFSA 2009-12
- MFSA 2009-13

✓Adobe:

- APSA09-01

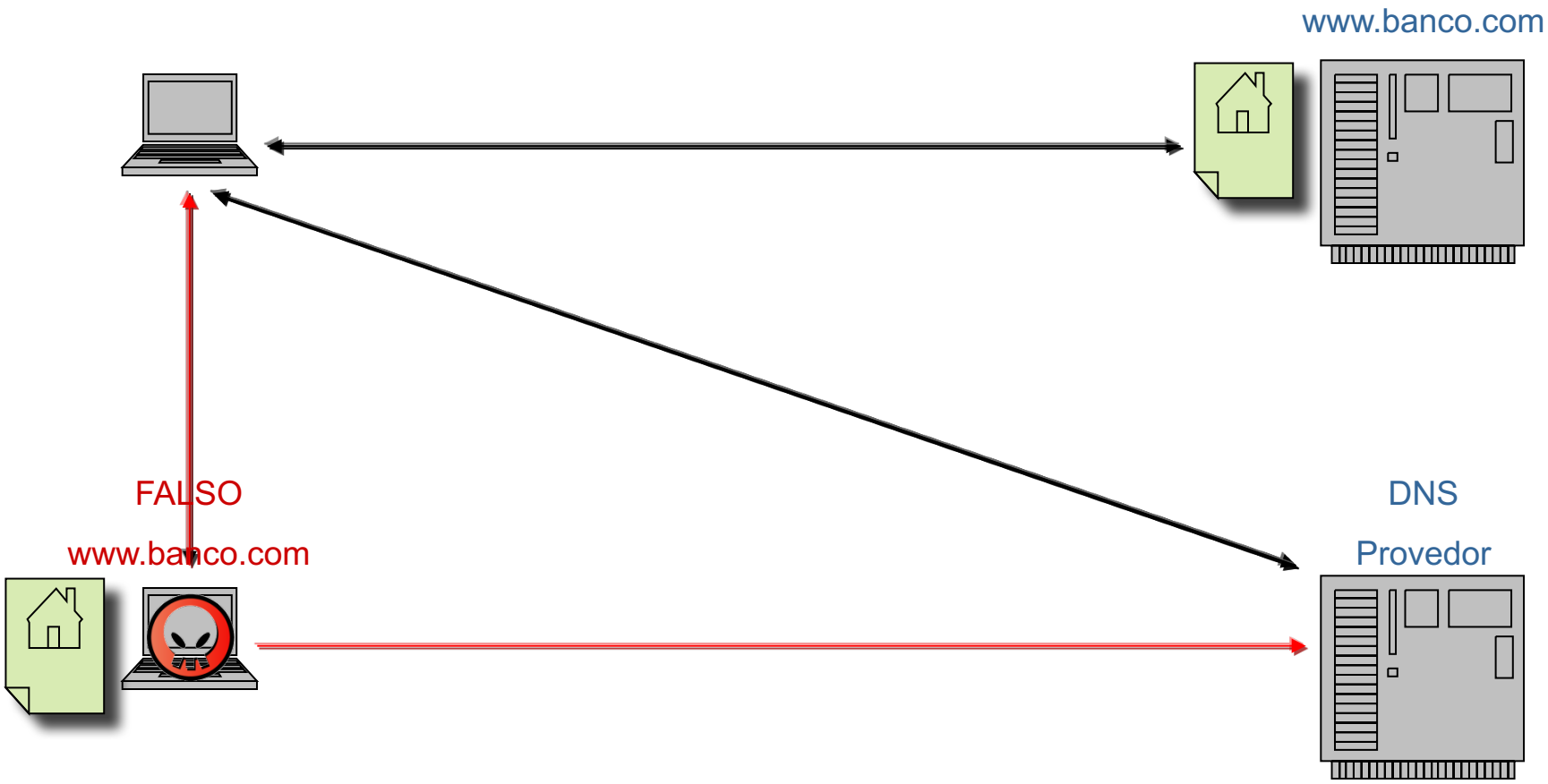
✓Existem vários outros exemplos, porém nesta apresentação ficaremos apenas com seis exemplos de *Client-Side*.


Researchers To Unleash Backbone-Hacking Tools At Black Hat Europe - DarkReading - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.darkreading.com/securityservices/services/data/showArticle.jhtml?articleID=216403220
Go
Links IBM Business Transformation Homepage IBM Standard Software Installer IT Help Central Join World Community Grid IBM Intranet Customize Links Free Hotmail
Google Security Black Hat Europe Go Bookmarks 7 blocked Check AutoLink AutoFill Send to BGP Settings
Researchers To Unleash Backbone-Hacking Tools At Black Hat Europe
Tools automate attacks on Multiprotocol Label Switching (MPLS) and Ethernet carrier networks
Abr 07, 2009 | 01:39 PM
By Kelly Jackson Higgins
DarkReading
A pair of German researchers at next week's Black Hat Europe will release tools that hack backbone technologies used by service providers in some enterprise network service offerings.
More specifically, the tools -- built by Enno Rey and Daniel Mende, both with German security firm ERNW -- automate attacks on Multiprotocol Layer Switching (MPLS) and Ethernet backbone technologies. They exploit similar, inherent security weaknesses in the two networking technologies -- namely, in how they forward traffic.
The lack of security in MPLS and Ethernet is well-known, but until now the exploitation of these network technologies has been only theoretically possible, Rey says. "Our release of the tools closes that gap of these attacks being only theoretical to being practically exploitable now," he says. "These technologies do not provide any security themselves, but just rely on the assumption that the underlying network is secure."
(32 items remaining) Opening page http://www.darkreading.com/securityservices/services/data/showArticle.jhtml?articleID=2164032
Internet


Alert Details - Security Center - Cisco Systems - Windows Internet Explorer
http://tools.cisco.com/security/center/viewAlert.x?alertId=16502
Cisco Shellcode
Security Center
Shellcode for Multiple Cisco IOS Systems Released
SECURITY ACTIVITY BULLETIN
Threat Type: IntelliShield: Security Activity Bulletin
IntelliShield ID: 16502
Version: 1
First Published: August 21, 2008 06:16 PM EDT
Last Published: August 21, 2008 06:16 PM EDT
Urgency:
Credibility:
Severity:
Done

Utilizando-se de um Framework para Fraude.

Um cenário já conhecido

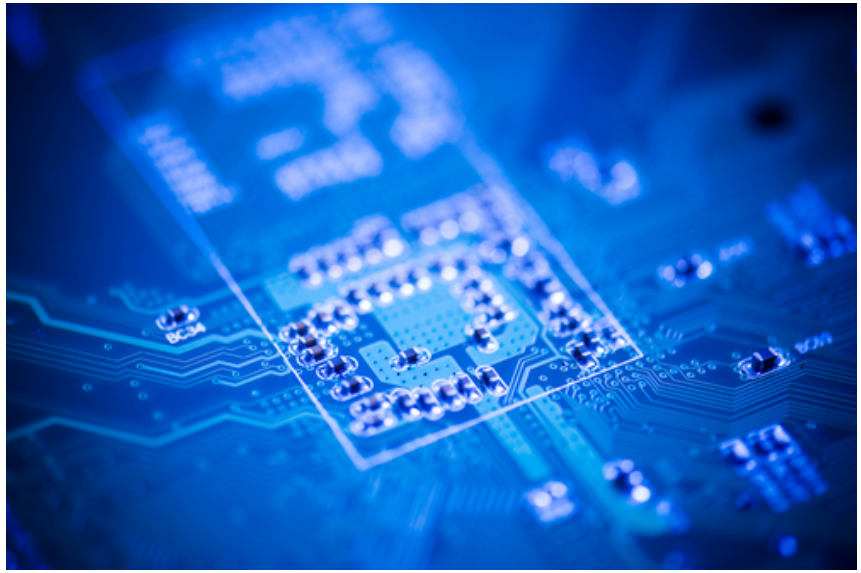


YES Crimeware – US$ 700,00 no Mercado Negro

Demonstrações

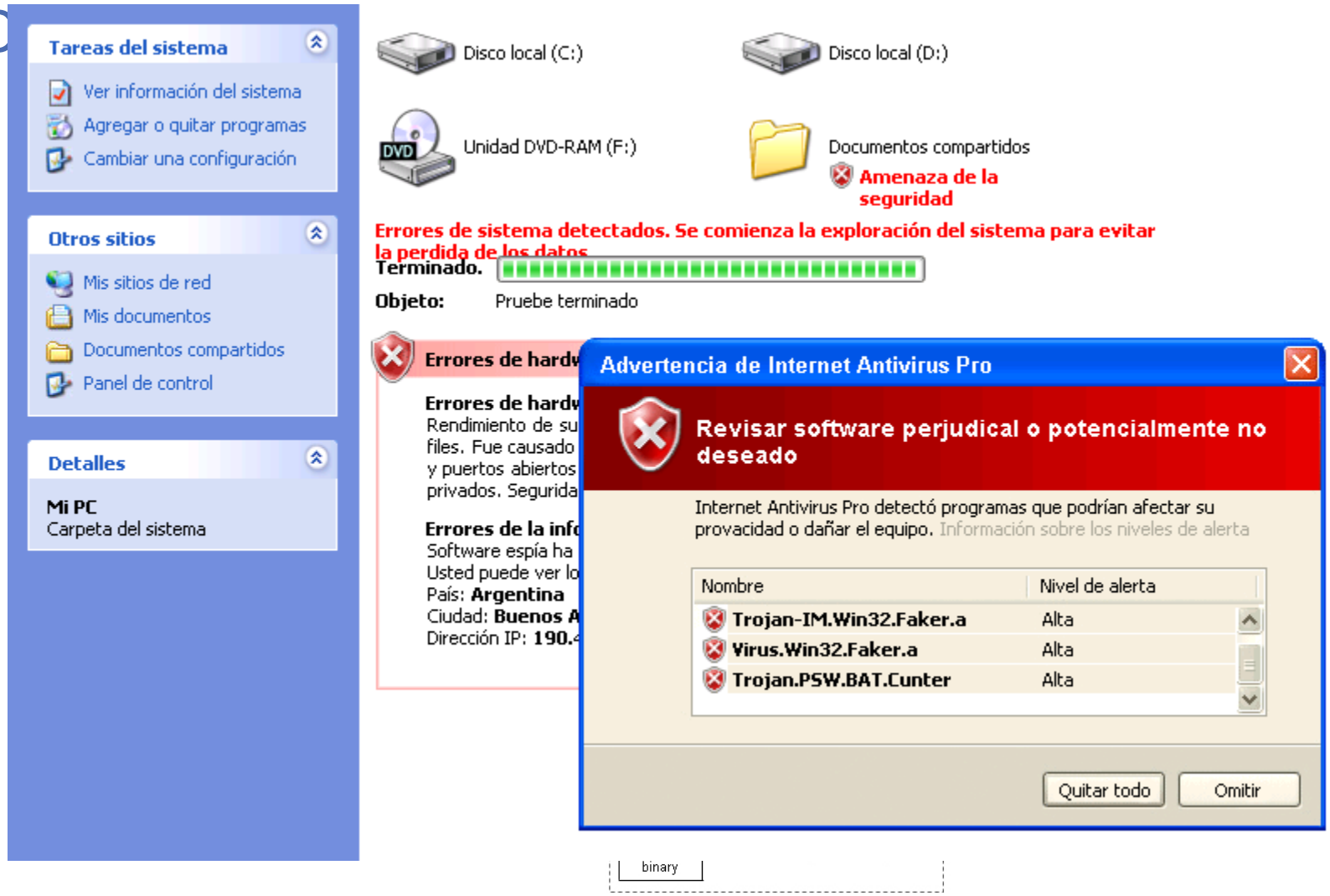
Demonstrações

- ✓ DEMO #01
  - *SYN Flood*
- ✓ DEMO #02
  - *DNS Cache Poisoning*
- ✓ DEMO #03
  - *Drive-by-Download 01*
  - *Drive-by-Download 02*
  - *Drive-by-Download 03*
  - *Drive-by-Download 04*



Botnets (Conficker)

Retrospectiva dos *Worms*


Tareas del sistema
Ver información del sistema
Agregar o quitar programas
Cambiar una configuración
Otros sitios
Mis sitios de red
Mis documentos
Documentos compartidos
Panel de control
Detalles
Mi PC
Carpeta del sistema
Disco local (C:)
Disco local (D:)
Unidad DVD-RAM (F:)
Documentos compartidos
Amenaza de la seguridad
Errores de sistema detectados. Se comienza la exploración del sistema para evitar la perdida de los datos
Terminado.
Objeto: Pruebe terminado
Errores de hardv
Errores de hardv
Rendimiento de su
files. Fue causado
y puertos abiertos
privados. Segurida
Errores de la info
Software espía ha
Usted puede ver lo
País: Argentina
Ciudad: Buenos A
Dirección IP: 190.
Advertencia de Internet Antivirus Pro
Revisar software perjudical o potencialmente no deseado
Internet Antivirus Pro detectó programas que podrían afectar su provacidad o dañar el equipo. Información sobre los niveles de alerta
Nombre
Nivel de alerta
Trojan-IM.Win32.Faker.a
Alta
Virus.Win32.Faker.a
Alta
Trojan.PSW.BAT.Cunter
Alta
Quitar todo
Omitir
binary

Perguntas e Respostas

Dúvidas?

Obrigado!