Amenazas actuales a la seguridad TI

Cristian Venegas
Systems Engineer
Cisco Chile
Mayo 2009

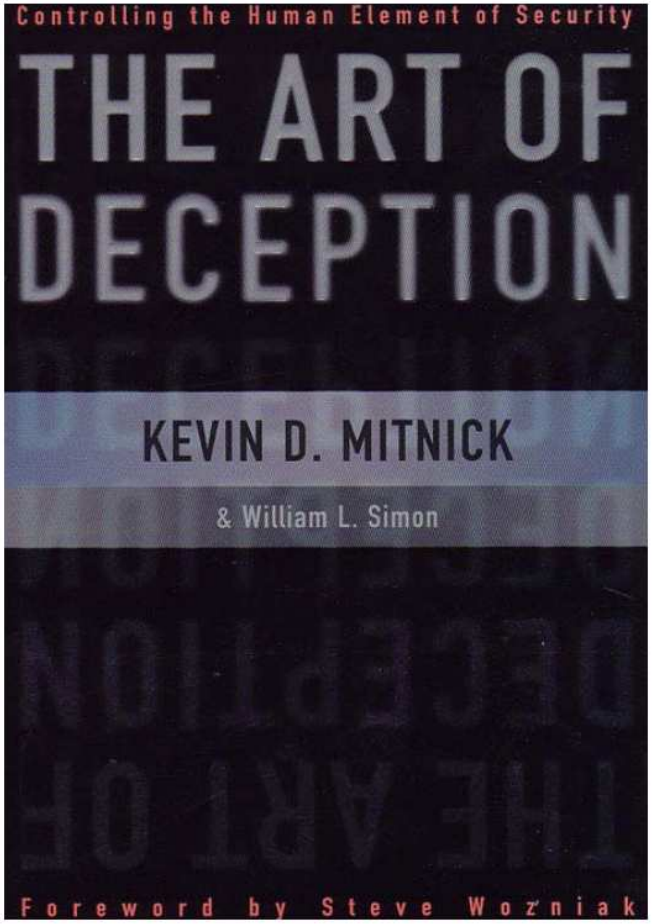
Agenda

- Introduccion
- Amenazas actuales
- Relevancia Cisco

Introducción

Amenazas del presente, pasado y futuro

- Ingeniería social
- Stanley Rifkin, 1978
- Security Pacific National Bank, Los Angeles, CA
- Mike Hansen, departamento internacional
- Record Guiness - fraude computacional más grande de la historia
- Seguridad trasciende a la tecnología



Amenazas de seguridad - tendencias

- Ganancias, colaboracion, innovacion
- Ataque en profundidad – multiples metodos para asegurar que la debilidad sera explotada
- Aumento en numero de vulnerabilidades (~ 6000 el 2008) y vectores de propagacion
- Malware y robo mas soterrado
- Fuga de informacion y bancos virtuales
- Vector web es el mas debil

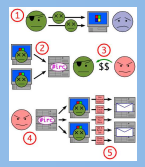
Amenazas actuales

▶ MALWARE

Gusanos, Virus, Troyanos, Spyware, Adware, Grayware, Ransomware,

▶ SPAM

Hit and run, pump and dump, 419, spamoetry, obfuscación …



▶ BOTNETS

Uso en DDoS/SPAM, peer-to-peer, encriptación uso de HTTP, polymorf, rootkits, honeypot

▶ PHISHING

Ingeniería social, aun efectivo, captura user/pass vía email/web.

▶ PHARMING

Abuso DNS, host files, home router para redirección a website suplantando original

▶ IP TELEPHONY

SPIT, fuzzing, DoS, carriers ($$), vishing, man-in-the-middle

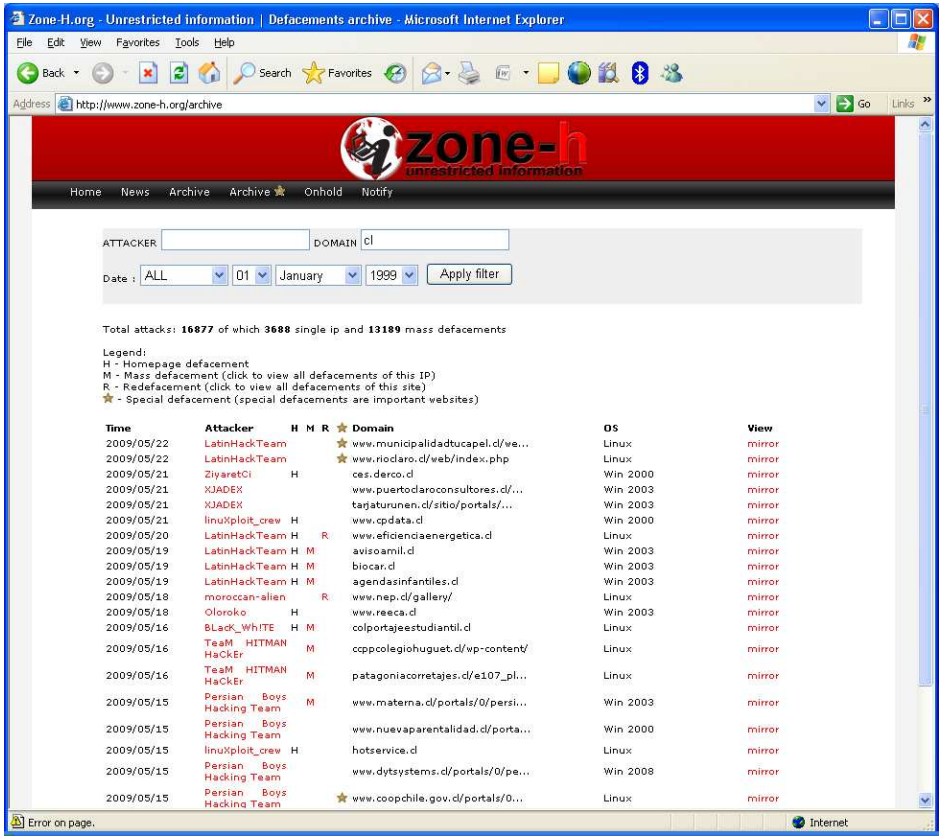
La economía underground

Current Rank	Previous Rank	Goods and Services	Current Percentage	Previous Percentage	Range of Prices
1	2	Bank accounts	22%	21%	$10–$1000
2	1	Credit cards	13%	22%	$0.40–$20
3	7	Full identities	9%	6%	$1–$15
4	N/A	eBay accounts	7%	N/A	$1–$8
5	8	Scams	7%	6%	$2.50/week–$50/week for hosting, $25 for design
6	4	Mailers	6%	8%	$1–$10
7	5	Email addresses	5%	6%	$0.83/MB–$10/MB
8	3	Email passwords	5%	8%	$4–$30
9	N/A	Drop (request or offer)	5%	N/A	10%–50% of total drop amount
10	6	Proxies	5%	6%	$1.50–$30

Table 4. Breakdown of goods and services available for sale on underground economy servers[55]
Source: Symantec Corporation

Fuente: Symantec

Estadísticas locales
Web defacement

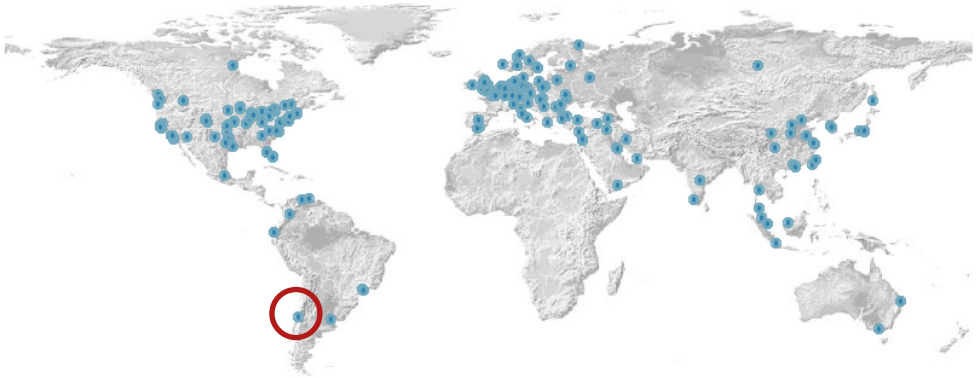


- Enero 1999 – Mayo 2009
- Ataques dominio .CL
  - **16877** ataques
  - 3688 single IP
  - 13169 masivos

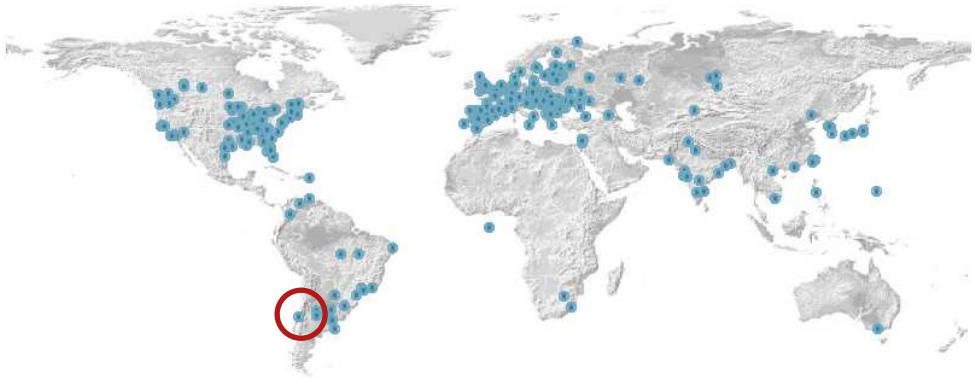
Fuente: http://www.zone-h.org

Botnets en Chile

- Botnet IRC servers

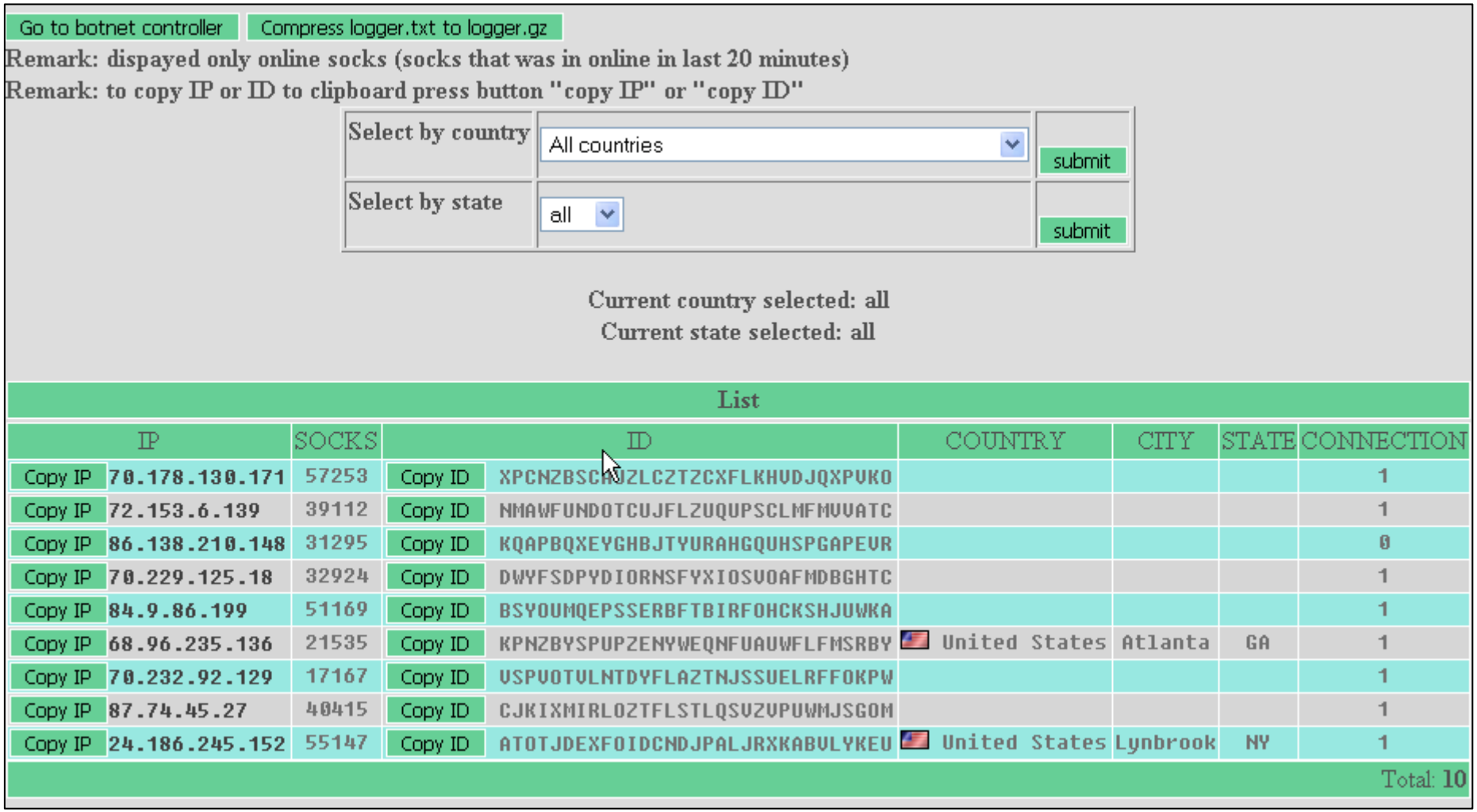


- Fast flux Bots



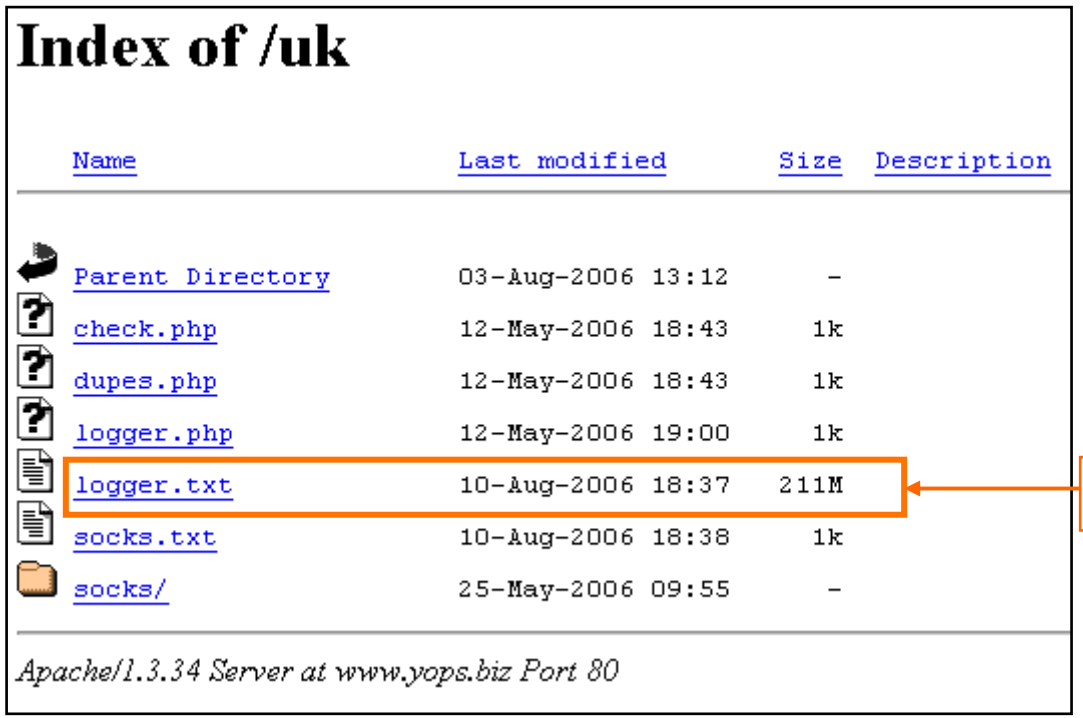
Fuente: ATLAS – Arbor Networks – Mayo 2009

Botnet Command and Control



IP	SOCKS	ID	COUNTRY	CITY	STATE	CONNECTION
Copy IP 70.178.130.171	57253	Copy ID XPCNZBSCHUZLCZTZCXFLKHVDJQXPVKO				1
Copy IP 72.153.6.139	39112	Copy ID NMAWFUNDOTCUJFLZUQUPSCLMFMVVATC				1
Copy IP 86.138.210.148	31295	Copy ID KQAPBQXEYGHBJTYURAHGQUHSPGAPEVR				0
Copy IP 70.229.125.18	32924	Copy ID DWYFSDPYDIORNSFYXIOSVOAFMDBGHTC				1
Copy IP 84.9.86.199	51169	Copy ID BSYOUMQEPSSERBFTBIRFOHCKSHJUWKA				1
Copy IP 68.96.235.136	21535	Copy ID KPNZBYSPUPZENYWEQNFUAUWFLFMSRBY	United States	Atlanta	GA	1
Copy IP 70.232.92.129	17167	Copy ID VSPVOTVLNTDYFLAZTNJSSUELRFFOKPW				1
Copy IP 87.74.45.27	40415	Copy ID CJKIXMIRLOZTFLSTLQSVZVPUWMJSGOM				1
Copy IP 24.186.245.152	55147	Copy ID ATOTJDEXFOIDCNDJPALJRXKABVLYKEU	United States	Lynbrook	NY	1
						Total: 10

Que se guarda en un nodo C&C?



Index of /uk

Name	Last modified	Size	Description
Parent Directory	03-Aug-2006 13:12	-	
check.php	12-May-2006 18:43	1k	
dupes.php	12-May-2006 18:43	1k	
logger.php	12-May-2006 19:00	1k	
logger.txt	10-Aug-2006 18:37	211M	
socks.txt	10-Aug-2006 18:38	1k	
socks/	25-May-2006 09:55	-	

Apache/1.3.34 Server at www.yops.biz Port 80

211 MB File…

Extracto de archivo de 211 MB

Malware envia lo tecleado al nodo C&C

botnet controller excerpt - Notepad

File Edit Format View Help

```
----------------------------------------------------------------------------
REMOTE ADDRESS: 172.189.109.174
ID: BPAQZLZBBLUWRYGVSXOTJHALUVNRBXS
TIMESTAMP: 25\5 14:0:51
Copyright By Smash and SARS
From: MATTHEW

Windows XP
Internet Explorer 6.0.2900.2180

**********
MAIL: POP383EE26C0
Chal89
PAUL
10.0.0.4
http://petiteteeniemania.join4free.com/_B64S_bm9kZWQvNjYvbW92aWVsYW5kL0FBQS9
TMxNDk3OTQ2L2ZBdi5UZGY5SEJscUU=_E/ Login: chal89@aol.com Pass: [redacted]
10.0.0.4 http://sib1.od2.com/common/Framework.aspx Login: chal89 Pass: [redacted]
10.0.0.4 http://uk.mcafee.com/root/login.asp
*** Protected Storage Data ends ***
----------------------------------------------------------------------------
----------------------------------------------------------------------------
REMOTE ADDRESS: 125.23.22.246
ID: KOBERVBOUKQIPXGITBBFSQWSGXJFUMO
TIMESTAMP: 31\12 19:47:37

......

**********
192.168.1.2 http://in.rediff.com/index.html Login: puneet.bhargava Pass:
**********
192.168.1.2 http://north.airtel-broadband.com/touchtelusernorth.html Login:
**********
192.168.1.2 http://sv2.freewh.com/index.php Login: udit_2001 Pass: [redacted]
**********
192.168.1.2 http://www.airtelworld.com/ Login: udit_2001 Pass: [redacted]
**********
192.168.1.2 http://www.airtelworld.com Login: 01152458021 Pass: [redacted]i
**********
192.168.1.2 http://www.cooltoad.com/go/login Login: udit_2001 Pass: [redacted]
**********
192.168.1.2 http://www.cooltoad.com/go/setup Login: udit_2001 Pass: [redacted]
**********
192.168.1.2 http://www.indianmoviesclub.com/board/forumdisplay.php Login: ud
**********
```

Website Passwords

Ecosistema de aplicaciones web vulnerables

SANS Top 20 Security Risks

http://www.sans.org/top20/#c1

- IE and Firefox vulnerables
  - "…**cientos de vulnerabilidades en controles ActiveX** instaladas por proveedores de software han sido descubiertas."
- Media Players y Browser Helper Objects (BHO)
  - RealPlayer, iTunes, Flash, Quicktime, Windows Media
  - Explosion de BHOs y plugins de terceras partes
  - Plug-ins son instalados de forma semi transparente por websites. Usuarios no tienen conciencia del riesgo asociado, introduciendo un nuevo vector de propagacion al visitar sitios web maliciosos.

Mpack: Infection Rate worldwide

Country	Traff	Loads	Efficiency
JP - Japan	93635	19875	21.23
DE - Germany	18702	4625	24.73
ES - Spain	13218	3947	29.86
US - United states	6954	926	13.32
RO - Romania	3070	1545	50.33
GB - United kingdom	1696	261	15.39
IT - Italy	1680	286	17.02
FR - France	1432	231	16.13
CN - China	1089	294	27

Malware vence a firmas de antivirus
Conferencia DefCon

- Criminales han desarrollado herramientas para mutar malware para vencer deteccion basada en firmas
- Investigadores en DefCon probaron su teoria nuevamente
- Seven virus y dos exploits, todos sumamente conocidos, fueron mutados para vencer firmas de antivirus
- Tiempo: 2 horas, 25 minutos

Seguridad en sistemas de control y automatizacion

- USSR pipeline explosion, 1982
- Bellingham pipeline rupture, 1999
- Queensland sewage release, 2000
- Davis Besse nuclear plant infection, 2003
- Northeast USA blackout, 2003
- Browns Ferry nuclear plant scram, 2006

Ejemplo 1 – Fuga de informacion
Heartland Payment Systems Data Breach

- Procesa 100 millones de transacciones mensuales de 175,000 mercantes
- Fuga en segunda mitad del 2008, se notifica a Visa en Octubre
- Malware roba tarjetas de credito/debito al pasar por la red
  - "Solo" numero de tarjetas, nombres y fechas de expiracion
- Vocero de Heartman:
- "Un bug extremadamente sofisticado ingreso a nuestro sistema. No fue causado por falta de atencion por parte de nadie. Nos estamos focalizando en actuar rapidamente para obtener la mejor seguridad en el futuro."
- 35% de baja en el precio de la accion, equivalente a reduccion de capitalizacion de mercado de $200M
- Tenian la certificacion PCI….

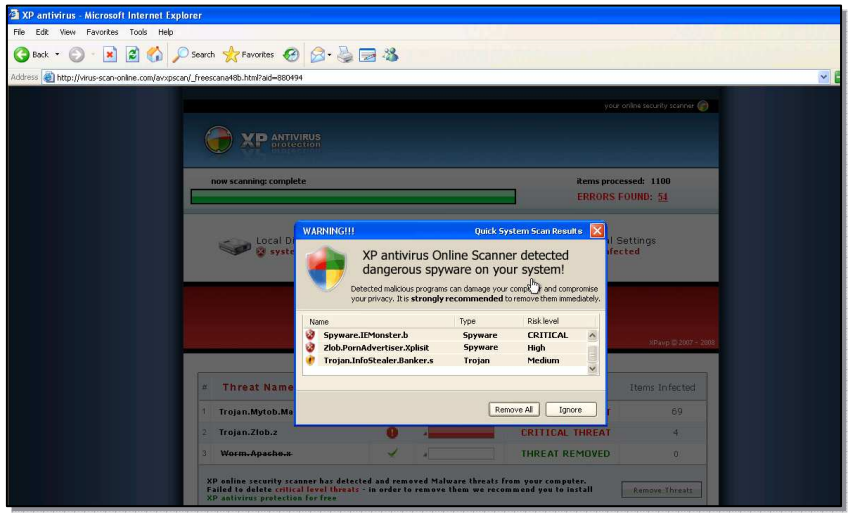
Ejemplo 2 - Gusano Conficker/Downadup

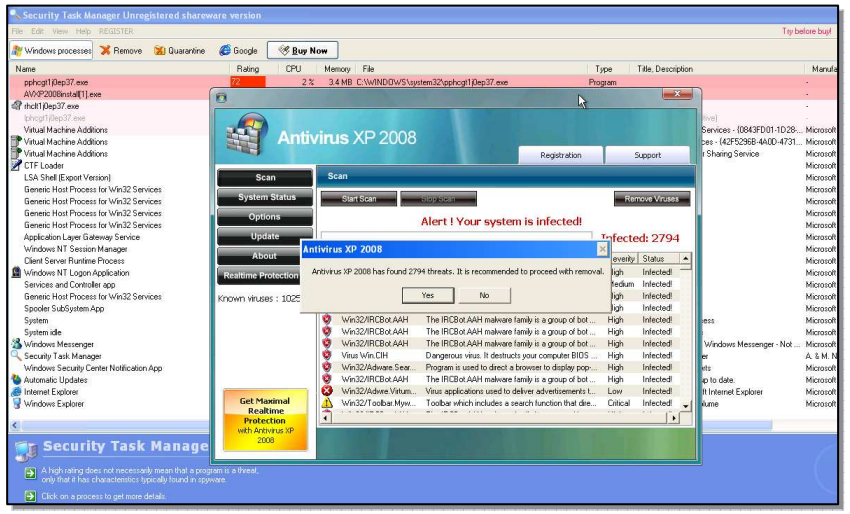
- Microsoft anuncia update de seguridad MS08-067 23 Oct 2008
- MS08-067 es una vulnerabilidad que permite ejecucion de codigo remota en puertos 139 o 445
  - 2000, XP, Windows Server 2003 sin autenticacion
  - Vista, Windows Server 2008 requiere autenticacion remota
- Conficker se transmite a traves de
  - Scanning de la red local buscando vulnerabilidad
  - Carpetas compartidas adivinando password de administrador
  - Dispositivos de almacenamiento externo como pendrives (autorun.inf)

- Deshabilita lookups DNS a sitios de seguridad
- Genera 250 nombres de dominio a traves de algoritmo y se conecta via HTTP
- Se estiman aproximadamente 9M de PCs infectados (F-Secure)
  - 1% in EEUU, mientras que China, Rusia y Brasil tienen el 41%
- Cisco tiene productos que entregan proteccion (IPS, CS-MARS, CSA, WSA)

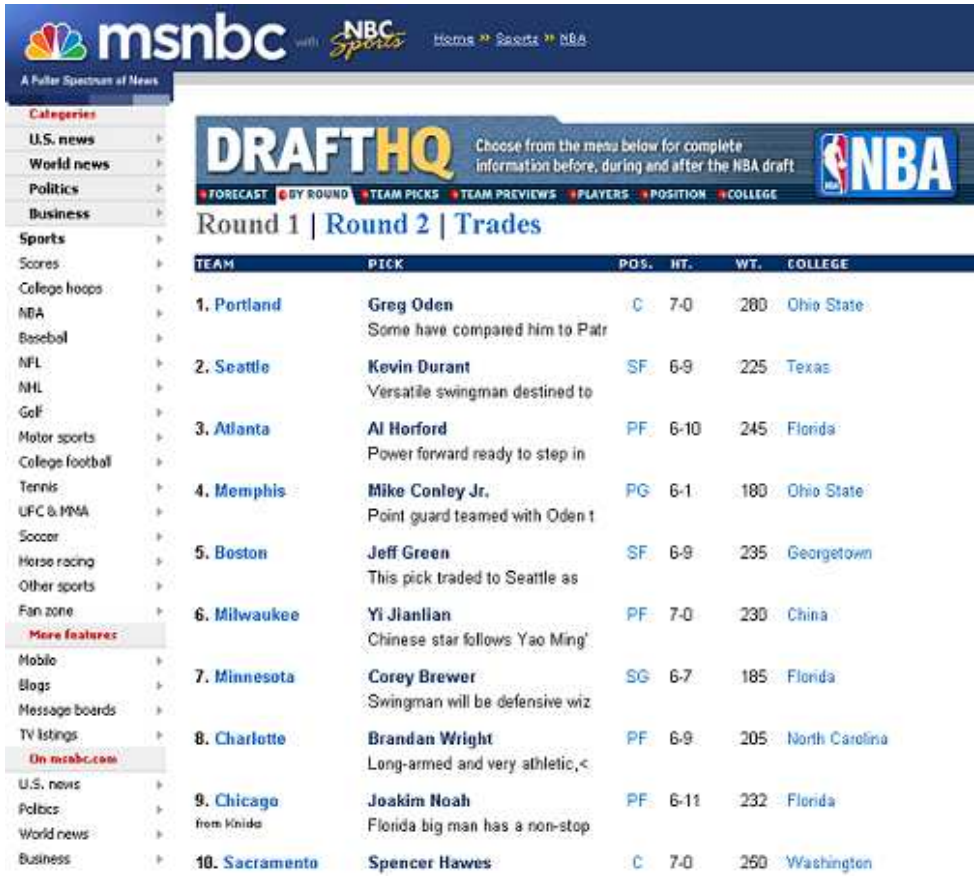
Ejemplo 3 - Scareware

- Malware que asusta al usuario para comprar antivirus falso
- Aumenta los ingresos de centavos a dolares
- Infecta a traves de sitio web con ingenieria social de antivirus, email y sitios web comprometidos
- Programa de afiliados disponible - bakasoftware.com
  - Un afiliado gano $147k en 10 dias basados en 155K infecciones generando 2772 compras a $50 cada una → 5M anuales





Ejemplo 4 – Web sites comprometidos



- El 18 de Marzo del 2008
  - ZDNet
  - history.com
  - wired.com
  - archive.org
- Visitas ejecutan un script que intenta ganar acceso al computador de la visita

Ejemplo 4 – Web sites comprometidos Ataque iFrame

- Minnesotahomefinance.com registrado en Godaddy en Junio 2005
- 209.51.132.218, Global Net Access en NY, con 312 domains

•Browser busca IFRAME y carga PHP de aarmrgdxrv.com

•85.255.121.195, Ukrtelegroup Ltd en Ucrania, con 15 dominios

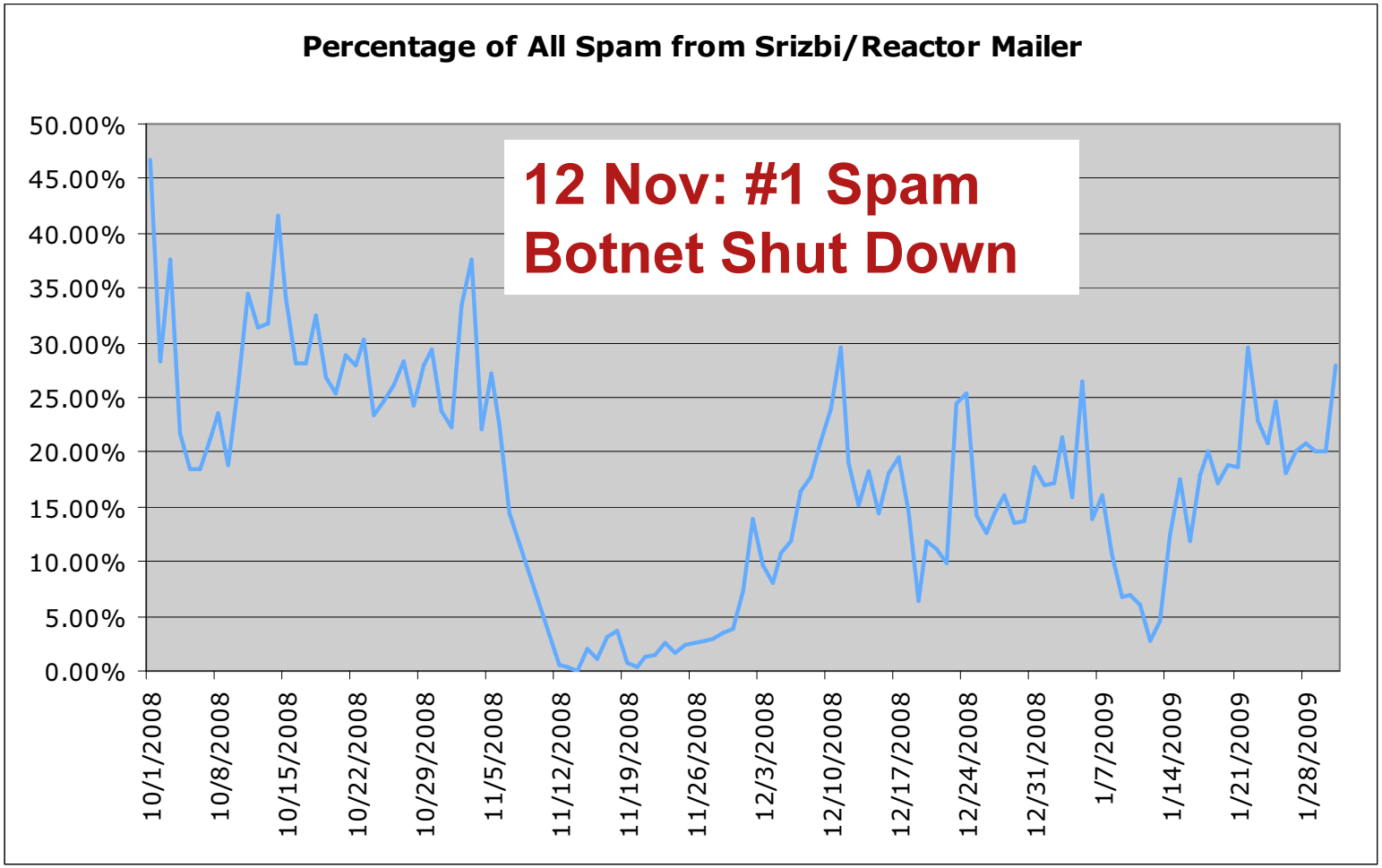
•Ukrtelegroup es parte de RBN (Russian Business Network)

Otros dominios siguen el patron, ej: adtctqypoa.com…

•aarmrgdxrv.com registrado en BIZCN.COM, INC.

Dominio spam con ranking existente: #18 en volumen, #11 por % malo

Buena noticia
Se elimina Botnet McColo

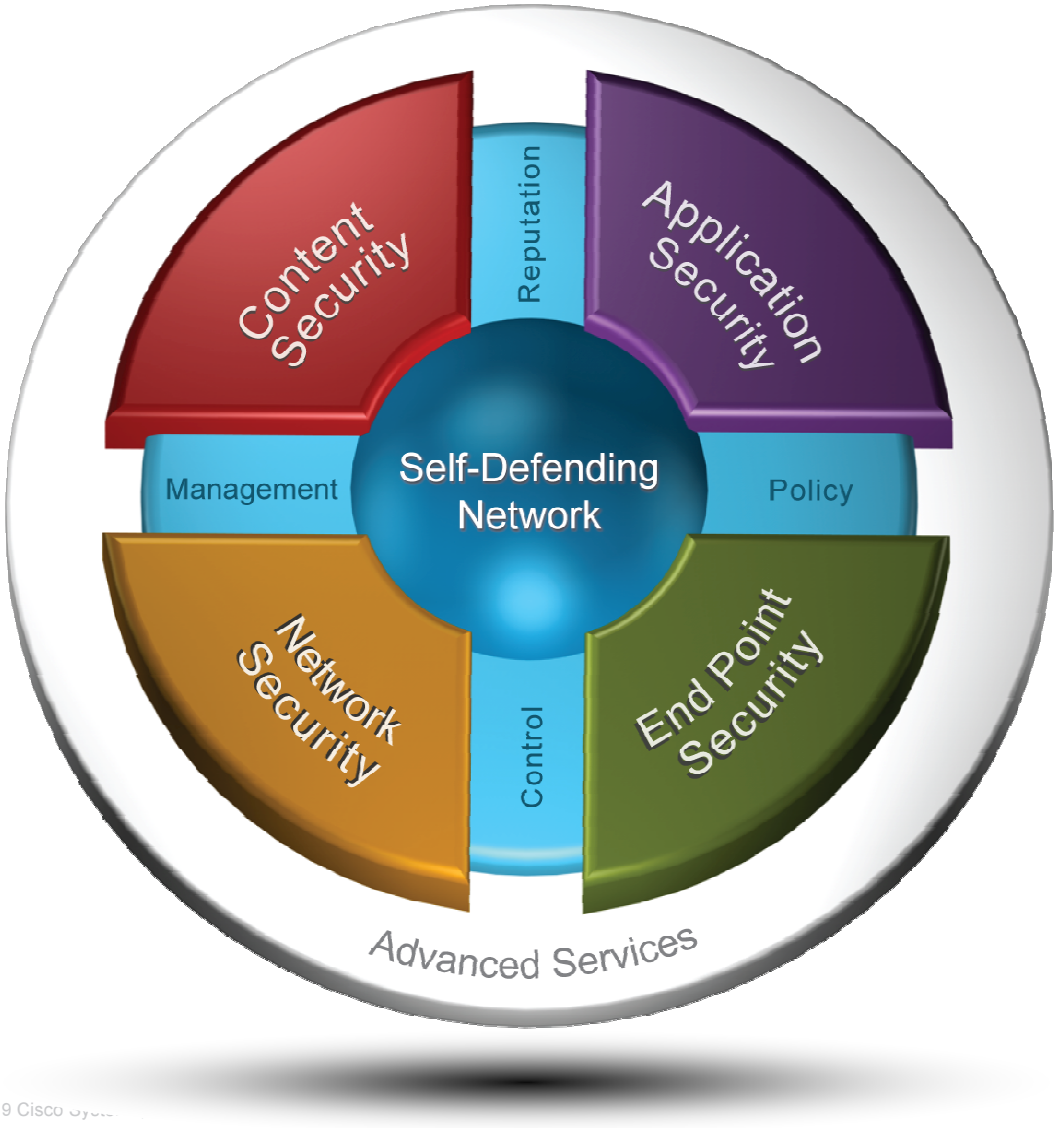


Buenas noticias 2008

- Intercage, un proveedor de hosting en EEUU asociado con el Russian Business Network es dado de baja
- Intercage, a US hosting provider associated with the Russian Business Network, was taken offline
  - Opero en EEUU por años de San Francisco dando apoyo a actividades criminales
- EstDomains desacreditado por ICANN
  - Registro de dominios haciendose pasar por compania estadounidense, controlada por criminales rusos
- Programa de afiliados de Spam SanCash/GenBucks dado de baja
  - Perseguidos por oficiales de EEUU y Nueva Zelanda
  - Afiliados de botnets enviaban spam de multiples productos

Relevancia Cisco

Cisco Self-Defending Network 3.0



Integración

Integra Advanced Network, Endpoint, Content, y Application Security para amenazas emergentes

Inspección del tráfico

Protege contra las últimas amenazas usando información obtenida de la red global

Solucion End-to-End

Provee una solución End-to-end con una amplia cobertura

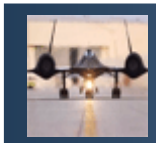
Infraestructura crítica

> “Critical infrastructures are physical or virtual systems and assests so vital that their incapacity or destruction would have a debilitating impact on national economic security, public heath or safety, or any combination of those matters.”
>
> Section 1016.e USA Patriot Act

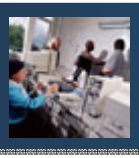
- Banca y Finanzas

- Químicos

- Comunicaciones



- Defensa



- Tecnologias de informacion

- Servicios postales

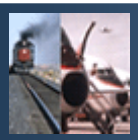
- Aguas

- Servicios de Emergencias

- Energia

- Agricultura y alimento

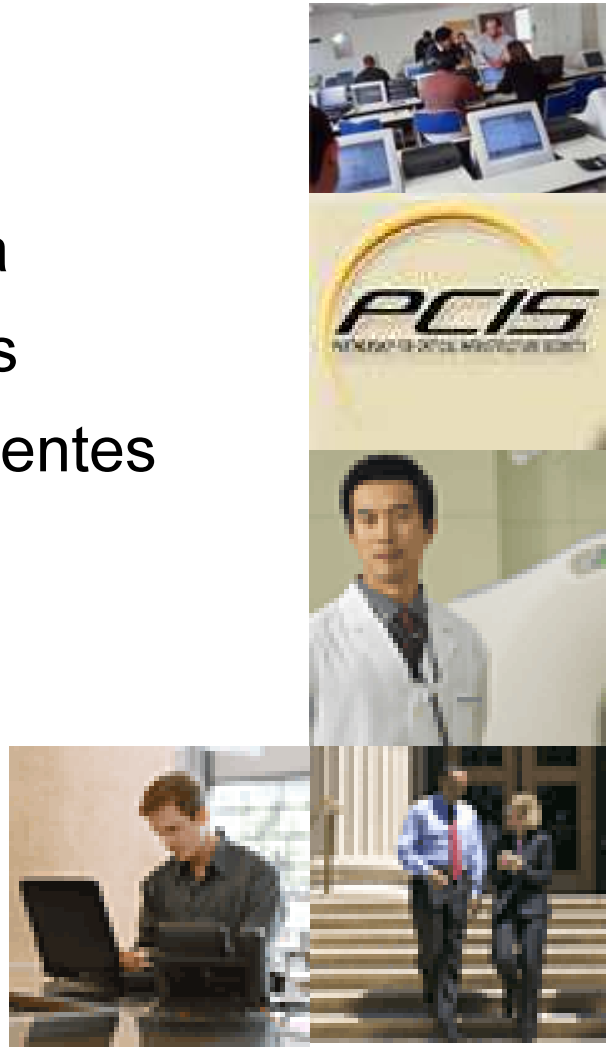
- Salud pública



- Transporte

Critical Infrastructure Assurance Group

- Educacion
- Entrenamiento
- I+D en seguridad de infraestructura
- Desarrollo de politicas y estandares
- Soporte de respuesta frente a incidentes



http://www.cisco.com/web/about/security/security_services/ciag/index.html

CIAG – Investigacion y desarrollo

ISRD Research Projects

Industrial Networking Security

- Honeynet for SCADA Environments
- Netfilter Extensions For Modbus/TCP
- SCADA Serial Link Protection
- Secure Administrative Access in SCADA Networks

Internet Infrastructures Security

- Internet DNS Scanning
- IPv6 Security
- Malware Impact on Network Devices

Internet Routing Protocols Security

- BGP Attack Tree Development and Testing
- Route Validation Graphs for Interdomain Routing

Legal, Financial, and Operational Security

- Common Vulnerability Scoring System

Physical Security

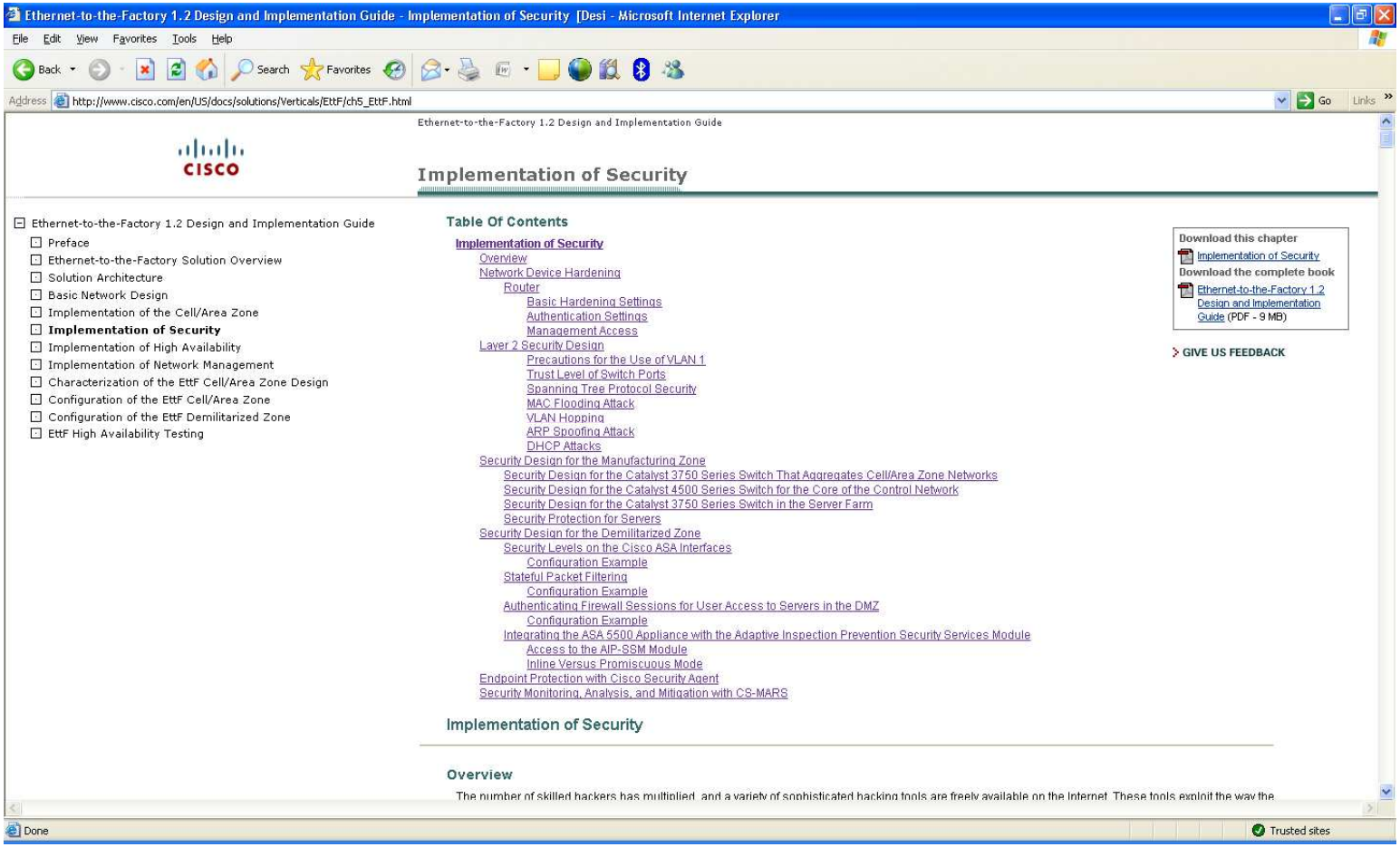
- Physical Security

Security Coding Practices

- eRFC
- Security Evaluation of an IP-Based Stack
- Software Engineering Best Practices

http://www.cisco.com/web/about/security/security_services/ciag/research/CIAG_research_projects.html

Securitización de redes industriales Infraestructura critica



http://www.cisco.com/en/US/docs/solutions/Verticals/EttF/ch5_EttF.html

Cisco: Apoyando a nuestros clientes a efectuar el viaje de soluciones aisladas a redes auto defensivas

- Self-Defending Network: integrado, colaborativo, adaptivo
- Habilita la práctica de seguridad en beneficio del negocio
- Reducción de riesgo, complejidad y costo total de propiedad más bajo
- Protege, optimiza y crece su negocio

cisco.com/go/security