Botnet como arma de control total

Lic. Cristian Borghello, CISSP – CCSK – MVP

www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo
@CursosSeguInfo

SEGU-INFO SEGURIDAD DE LA INFORMACION AGASSI

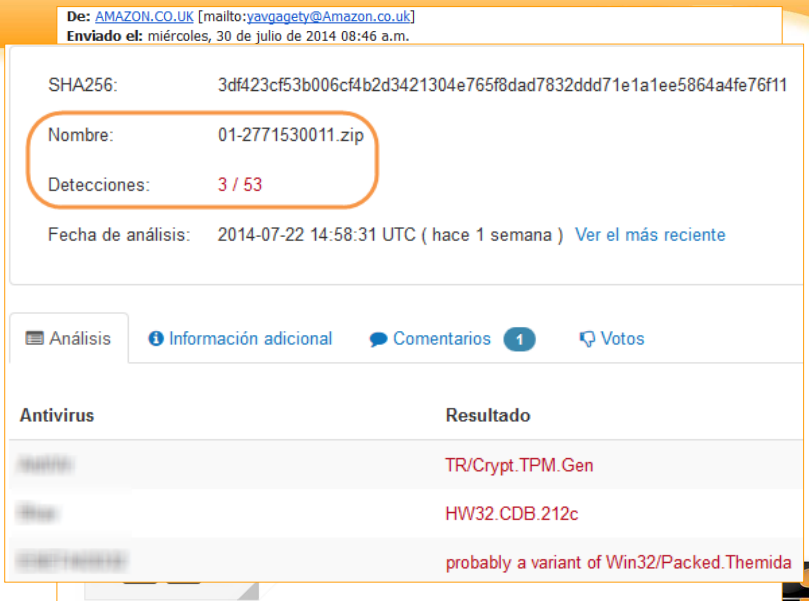
Sobre Cristian Borghello

- Licenciado en Sistemas UTN desde 2000
- Desarrollador desde los 8 años
- CISSP (Certified Information Systems Security Professional) desde 2008
- Microsoft MVP Security (Most Valuable Professional) desde 2010
- CCSK (Certificate of Cloud Security Knowledge) desde 2014
- Creador y Director de Segu-Info
- Consultor independiente en Seguridad de la Información

Relación Spam y Malware

- El spam es un medio eficaz, eficiente y barato para propagar malware
- Gran parte del spam actual se difunde a través de botnet
- Ofrece anonimicidad al delincuente
- El malware actual instala un servidor SMTP propio para enviar correos desde los equipos infectados
- Es parte fundamental del circuito delictivo

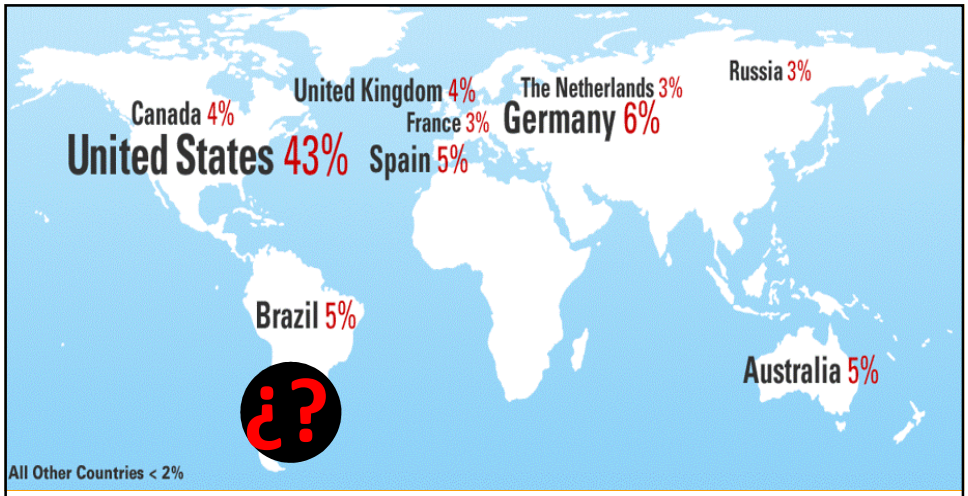
Spam → Malware



Phishing

Phishing: acrónimo de *Password Harvesting Fishing* (recolección y pesca de contraseñas)

- Actividad que intenta obtener de forma fraudulenta, información personal sensible (datos personales, contraseñas, PIN, tarjetas de crédito, etc.) a través de la simulación de identidad de un entidad conocida por la víctima (*spoofing*)
- El método principal utilizado es el engaño a través de técnicas de Ingeniería Social



no hay números (estadísticas) por eso "no hay casos"

Fuente: www.phishtank.com

Pasos del Phishing

1. **El delincuente** crea el sitio web falso
2. Lo aloja en servidores vulnerados o gratuitos
3. Envía spam a usuarios al azar (según su BD)
4. **El usuario** recibe el correo electrónico
5. Hace clic en el enlace del correo electrónico y es direccionado al sitio web falso
6. Ingresa su información en el formulario
7. Recibe un mensaje de error, o es direccionado al sitio web real
8. La información está en poder del delincuente

Características de un correo falso

Asunto con gravedad

Spoofing de Remitente

Imagen de la entidad afectada

Ausencia del nombre del receptor

Errores gramaticales
Errores de ortografía

Supuesto enlace a la entidad

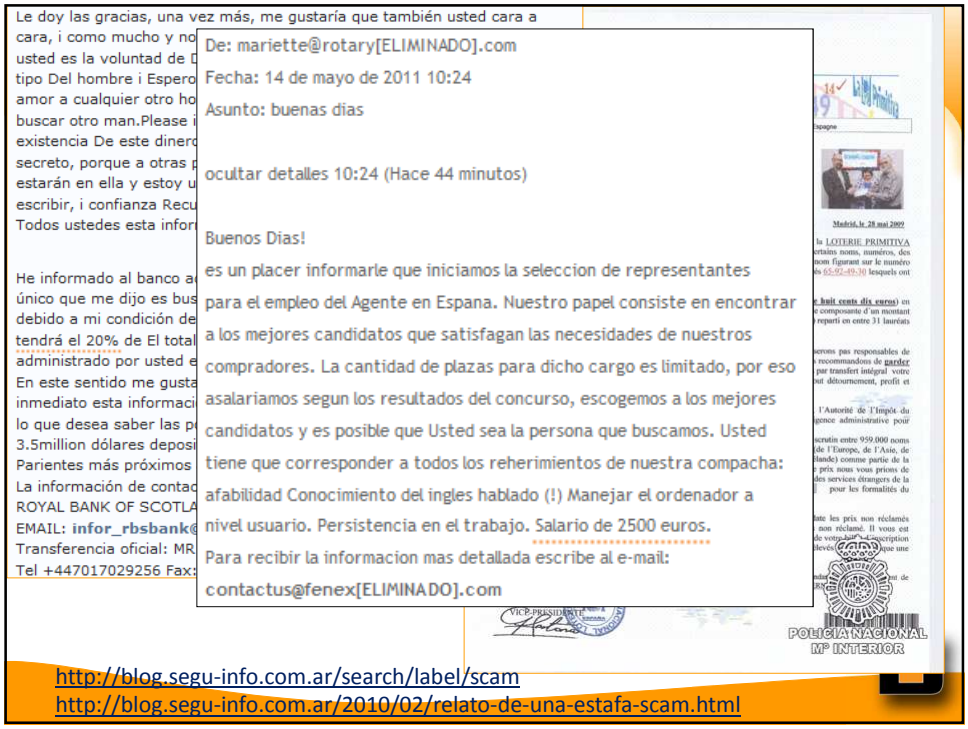
Enlace al sitio falso

Scam

Scam: engaño que busca provocar algún perjuicio patrimonial a través de transacciones financieras con la víctima

- El atacante lucra de forma directa con la víctima a través de dichas transacciones
- La víctima generalmente cree que ganará algo de las acciones realizadas
- También se los conoce como “Carta nigeriana”, “el cuento del tío” y “estafas 419”

Tipos de scam: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-754.pdf
Casos reales: http://www.bobbear.co.uk/



http://blog.segu-info.com.ar/search/label/scam
http://blog.segu-info.com.ar/2010/02/relato-de-una-estafa-scam.html

Reclutamiento de mulas

- Mulas o muleros: personas que blanquean o lavan dinero fraudulento, habitualmente sin saberlo

1. El estafador recluta a la mula mediante oferta *"gana mucho y trabaja poco"*
2. La víctima proporciona sus datos bancarios
3. El estafador deposita en la cuenta dinero que procede de actividades delictivas (virtuales o físicas)
4. El estafado es autorizado por el estafador a retener una comisión de ese dinero ingresado (10%) y mueve el resto otra cuenta/medio que le proporciona el estafador
5. La sucesión de cuentas hacen irrastreable la procedencia del dinero y del estafador

Botnet

Conjunto de sistemas infectados y que son controlados por un sistema central y que generalmente tiene un objetivo financiero y económico

"La supercomputadora más potente del mundo está en línea"

Ph.D. Peter Guttmann

Bot proviene de "robot", programa o agente que realiza una tarea simulando acciones humanas

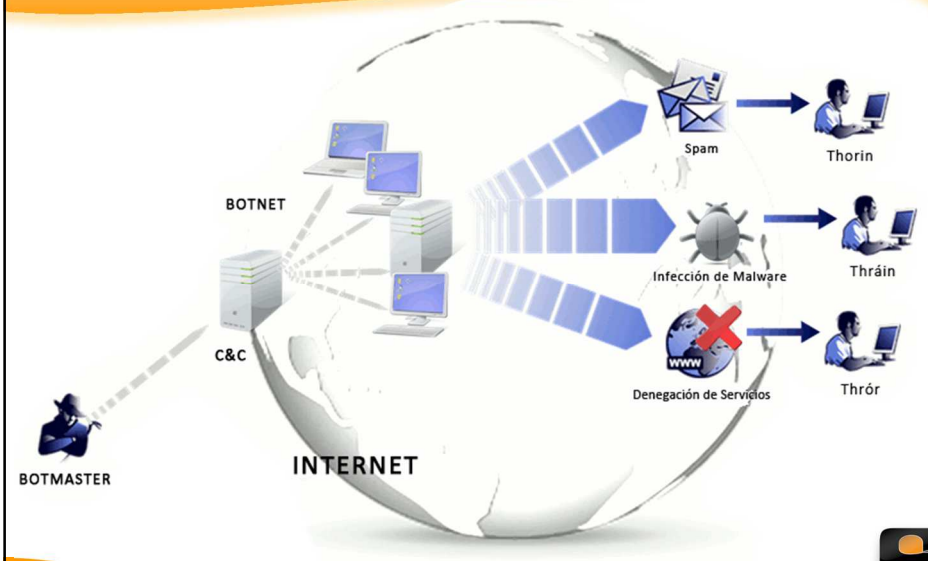
Otras definiciones

- **Bot/Zombie:** nombre que recibe cada sistema controlado
- **Botmaster/Botherder:** persona que controla y/o es dueño y responsable de la botnet
- **C&C (Comando & Control):** punto central de control desde donde el botmaster opera la botnet
- Se utiliza el principio del poder del cómputo distribuido para efectuar tareas dañinas

Objetivos de una Botnet

- Robar credenciales financieras/bancarias
- Enviar de spam
- Realizar ataques de denegación de servicio distribuido (DDoS)
- Construir servidores web para alojar material pornográfico y pedofílico
- Construir servidores web para ataques de phishing
- Redes privadas de intercambio de material ilegal (warez, cracks, seriales, etc)
- Distribución e instalación de nuevo malware
- Abuso de publicidad online como Adsense
- Manipulación de juegos online
- Imaginación!!

Capas de una Botnet



http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence/at_download/fullReport

Negocios, solo eso

- Las botnets se convirtieron en una **economía virtual** con clientes finales, revendedores, distribuidores, etc.
- El creador de malware vende su “producto o servicio” al creador de la botnet
- El botmaster alquila o vende la red
- El spammer distribuye más correo con publicidad
- Cualquier delincuente puede almacenar su información en equipos de usuarios infectados
- Cualquiera puede utilizar la red para realizar DDoS
- Las empresas venden los productos publicitados
- Cualquiera de ellos distribuye más malware infectando más equipos y retroalimentando el sistema

Nuevos servicios

- Malware as a Service (MaaS): modelo para difundir e instalar malware a medida a través de Internet, generalmente mediante inyección de código en sitios web
- Criminal to Criminal (CtC): servicios y negocios criminales realizados virtualmente
- CyberCrime as a Service (CaaS): modelo de negocio para recolectar, comprar y vender información obtenida en forma fraudulenta en Internet

Modelo de organizaciones criminales centradas en el malware y distribuidas en Internet para generar ingresos rápidos

Un robo masivo

- CyberVor acumuló 4,5 mil millones de registros de credenciales robadas
- 1.200 millones de credenciales únicas
- Robaron más de 420.000 sitios web y FTP

afirma que un grupo ruso se apoderó de alrededor de 1,2 mil millones de contraseñas y direcciones de correo electrónico en el mundo. De confirmarse, este robo de contraseñas, constituiría el mayor robo informático llevado a cabo hasta ahora, indicaron expertos ayer, recalcando el método poco común usado en esta oportunidad.

Después de más de siete meses de investigación, Hold Seguridad identificó un grupo ruso que se encuentra actualmente en posesión de la mayor cantidad de datos robados. Si bien la banda no tenía nombre, se la apodó *"CyberVor"* ("vor", significa "ladrón" en ruso).

http://blog.segu-info.com.ar/2014/08/cybervor-roban-12-mil-millones-de.html

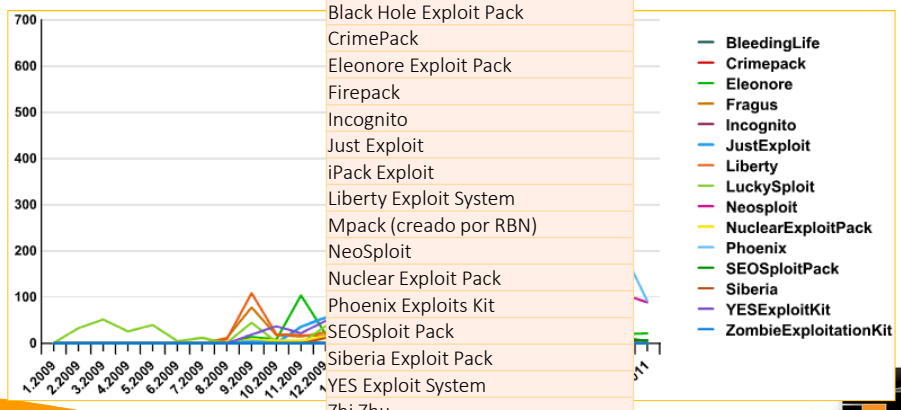
Malware y *exploits*

- **Conficker:** aprovecha un 0-Day en un servicio de Windows. Fue solucionado con la actualización MS08-067
- **Stuxnet:** utiliza cuatro vulnerabilidades 0-Day
- **Duqu:** aprovecha de un 0-Day en el Kernel
- **Slapper:** familia de gusanos de Linux que aprovechan una vulnerabilidad en OpenSSL
- **Cada día aparecen vulnerabilidades y 0-Day para cualquier plataforma y aplicación**

Exploit Packs (I)

Exploit Packs: paquetes comerciales con gran cantidad de *exploits* funcionales y utilizados para infectar

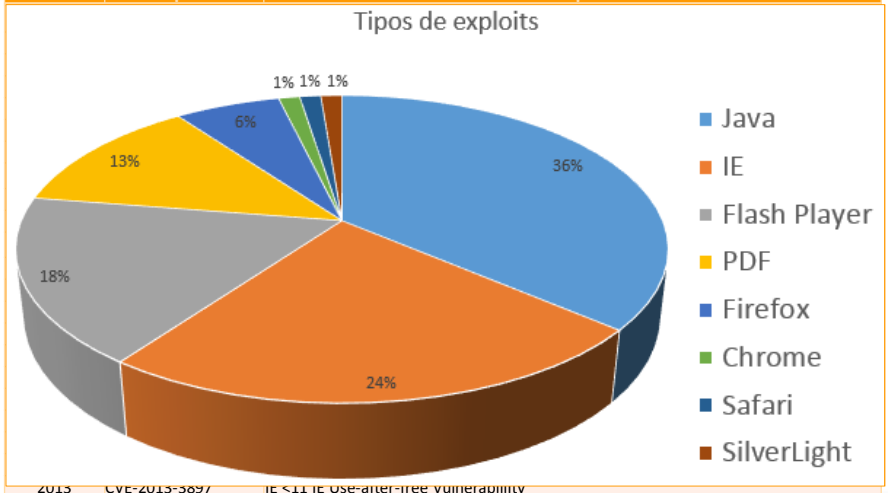
Exploit Packs
Adrenalin
Black Hole Exploit Pack
CrimePack
Eleonore Exploit Pack
Firepack
Incognito
Just Exploit
iPack Exploit
Liberty Exploit System
Mpack (creado por RBN)
NeoSploit
Nuclear Exploit Pack
Phoenix Exploits Kit
SEOSploit Pack
Siberia Exploit Pack
YES Exploit System
Zhi Zhu



http://contagiodump.blogspot.com.ar/2010/06/overview-of-exploit-packs-update.html

Exploit Packs (II)

Año	Exploit	Descripción
2013	CVE-2013-3897	IE <11 IE Use-after-free Vulnerability
2013	CVE-2013-5329	Flash 11.9.900.117 Memory Corruption
2010	CVE-2010-3971	Internet Explorer Recursive CSS Import Vulnerability



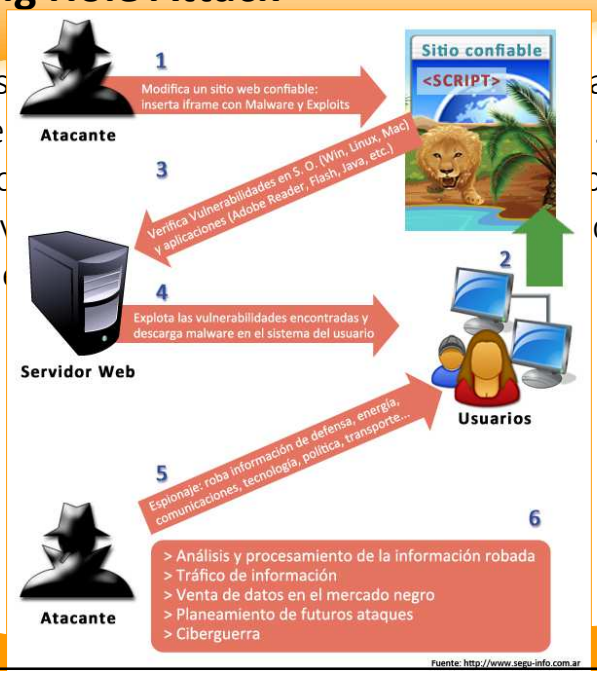
Vendo, vendo...

Drive-by-Download

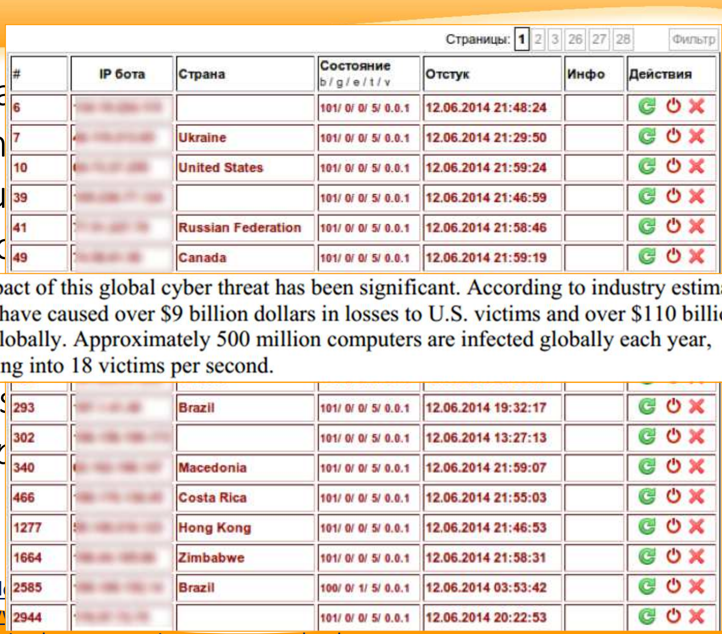
Proceso por el cual se explotan vulnerabilidades, se descarga y/o ejecuta malware a través de *scripts* inyectados en páginas web

Watering Hole Attack

A través a, se redirige .
El sitio c bolín" para lle dando a la esp



BrutPOS



Страницы: 1 2 3 26 27 28 Фильтр

#	IP бота	Страна	Состояние b / g / e / t / v	Отстук	Инфо	Действия
6			101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:48:24		
7		Ukraine	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:29:50		
10		United States	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:59:24		
39			101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:46:59		
41		Russian Federation	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:58:46		
49		Canada	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:59:19		
293		Brazil	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 19:32:17		
302			101/ 0/ 0/ 5/ 0.0.1	12.06.2014 13:27:13		
340		Macedonia	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:59:07		
466		Costa Rica	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:55:03		
1277		Hong Kong	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:46:53		
1664		Zimbabwe	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:58:31		
2585		Brazil	100/ 0/ 1/ 5/ 0.0.1	12.06.2014 03:53:42		
2944			101/ 0/ 0/ 5/ 0.0.1	12.06.2014 20:22:53		

The impact of this global cyber threat has been significant. According to industry estimates, botnets have caused over $9 billion dollars in losses to U.S. victims and over $110 billion in losses globally. Approximately 500 million computers are infected globally each year, translating into 18 victims per second.

- La … r
  in … s
  lu
- Lo
  us … o
  “p

http://bl…
http://w…
bruteforcing-botnet-targeting-pos-systems.html

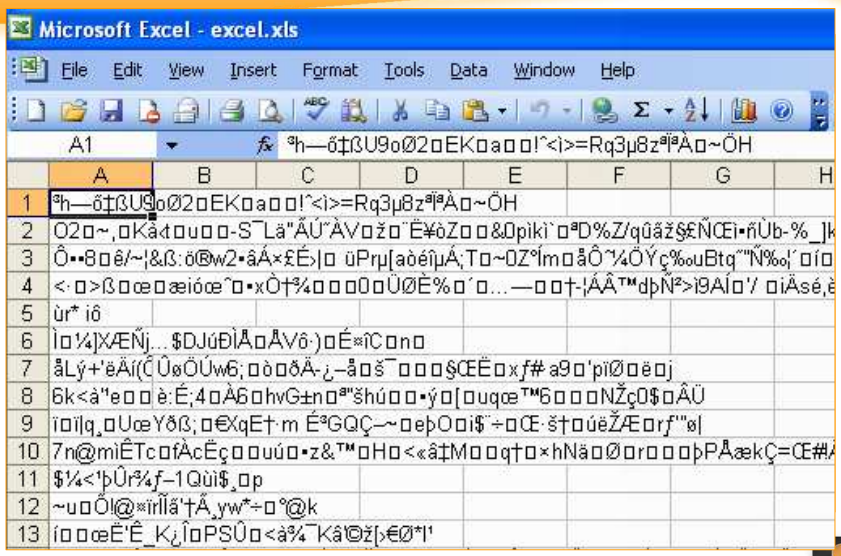
GameOver Zeus y Cryptolocker

- A diferencia de versiones anteriores de Zeus, con un C&C, la versión GameOver Zeus posee una infraestructura descentralizada mediante una red Peer-to-Peer
- Los comandos pueden provenir de cualquier sistema infectado, dificultando su localización
- Uno de los objetivos es propagar CryptoLocker, un *ramsonware* que cifra archivos y luego pide un rescate en dinero para entregar las claves

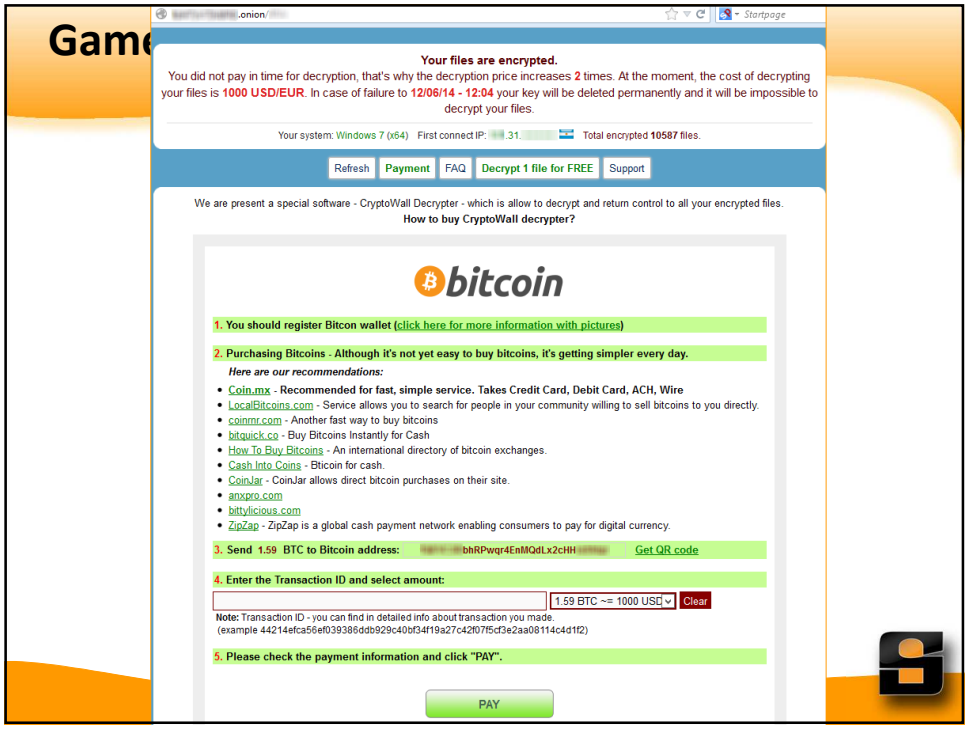
http://blog.segu-info.com.ar/2014/06/fbi-desbarata-botnet-game-over-zeus-goz.html

GameOver Zeus y Cryptolocker

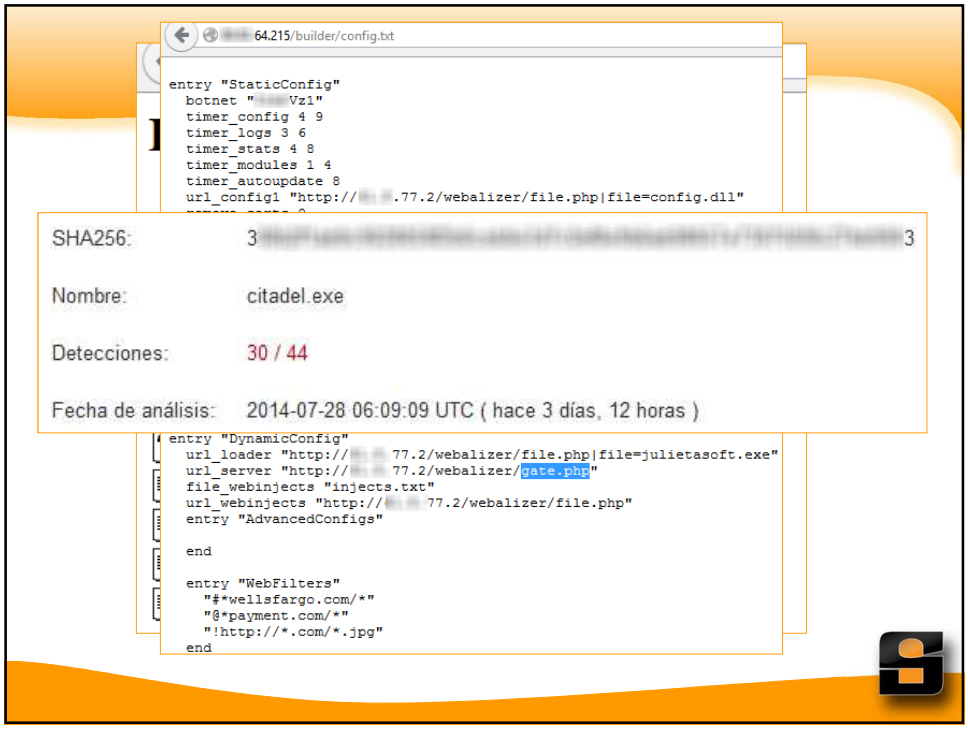
GameOver Zeus y Cryptolocker



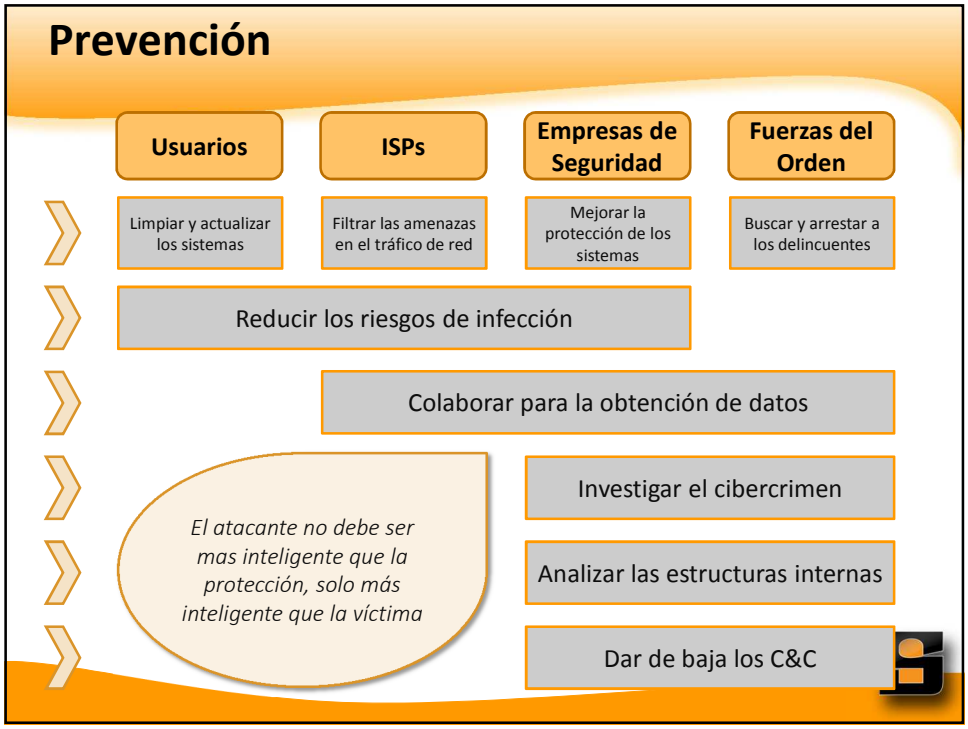
http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/documents/gameover-zeus-and-cryptolocker-poster-pdf


Game
.onion/
Startpage
Your files are encrypted.
You did not pay in time for decryption, that's why the decryption price increases 2 times. At the moment, the cost of decrypting your files is 1000 USD/EUR. In case of failure to 12/06/14 - 12:04 your key will be deleted permanently and it will be impossible to decrypt your files.
Your system: Windows 7 (x64) First connect IP: .31. Total encrypted 10587 files.
Refresh
Payment
FAQ
Decrypt 1 file for FREE
Support
We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?
bitcoin
1. You should register Bitcon wallet (click here for more information with pictures)
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
Coin.mx - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
coinmr.com - Another fast way to buy bitcoins
bitquick.co - Buy Bitcoins Instantly for Cash
How To Buy Bitcoins - An international directory of bitcoin exchanges.
Cash Into Coins - Bticoin for cash.
CoinJar - CoinJar allows direct bitcoin purchases on their site.
anxpro.com
bittylicious.com
ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. Send 1.59 BTC to Bitcoin address: bhRPwqr4EnMQdLx2cHH Get QR code
4. Enter the Transaction ID and select amount:
1.59 BTC ~= 1000 USD
Clear
Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)
5. Please check the payment information and click "PAY".
PAY


SHOWTIME


64.215/builder/config.txt
entry "StaticConfig"
botnet "Vz1"
timer_config 4 9
timer_logs 3 6
timer_stats 4 8
timer_modules 1 4
timer_autoupdate 8
url_config1 "http://.77.2/webalizer/file.php|file=config.dll"
SHA256:
Nombre: citadel.exe
Detecciones: 30 / 44
Fecha de análisis: 2014-07-28 06:09:09 UTC (hace 3 días, 12 horas)
entry "DynamicConfig"
url_loader "http://77.2/webalizer/file.php|file=julietasoft.exe"
url_server "http://77.2/webalizer/gate.php"
file_webinjects "injects.txt"
url_webinjects "http://77.2/webalizer/file.php"
entry "AdvancedConfigs"
end
entry "WebFilters"
"#*wellsfargo.com/*"
"@*payment.com/*"
"!http://*.com/*.jpg"
end


https://www.dropbox.com/sh/
julio
Nombre
Tamaño
Modificado
Hace 14 días
Hace 14 días
Hace 14 días
Hace 14 días
5.txt
2,74 MB
Hace 14 días
¡PLOP!


Prevención
Usuarios
ISPs
Empresas de Seguridad
Fuerzas del Orden
Limpiar y actualizar los sistemas
Filtrar las amenazas en el tráfico de red
Mejorar la protección de los sistemas
Buscar y arrestar a los delincuentes
Reducir los riesgos de infección
Colaborar para la obtención de datos
El atacante no debe ser mas inteligente que la protección, solo más inteligente que la víctima
Investigar el cibercrimen
Analizar las estructuras internas
Dar de baja los C&C


En Internet no pasa todo lo que debería sólo porque…
No hay suficientes delincuentes y ganas ☺

Agradecimientos

A la Comunidad de Segu-Info que todos los días [nos] aporta conocimiento a través de los distintos grupos de discusión

¡GRACIAS!

Lic. Cristian Borghello, CISSP – CCSK – MVP

www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo
@CursosSeguInfo

SEGU·INFO
SEGURIDAD DE LA INFORMACION

AGASSI