Menú principal

- Inicio

- Descargas
- Noticias
- Buscar
- Secciones
- Temas
- Enlaces Web
- Foros
- Análisis

Descargas

La descarga:
Manual MySQL 6 (Ingles) CHM
Manual MySQL 6 en Ingles, formato CHM
Hits: 24

Últimas descargas:
Java Version 6 Update 3 Linux
Ultima actualizacion de Java Version 6 Update 3 para sistemas Linux, archivo RPM.
Hits: 12

- Java Version 6 Update 3 Windows
- Windows Live Messenger 9.0 Beta
- Mozilla Firefox 3.0 Beta 2
- Messenger Plus! Live 4.23.276
- Webmin 1.38
- Net Tools © 2008
- Fedora Core 8 i386 Recue cd ISO
- Fedora Core 8 i386 ISO DVD
- CentOs 5 x86 ISO DVD

[Ir a Descargas] [Añadir]

Online

Actualmente hay 3 invitados y 0 usuarios registrados en línea.

Puedes loguearte o crear una cuenta nueva aqui.

Virus: Entrevista: Botnets... el lado oscuro

Enviado por: systemhalt en Sábado, 24 Noviembre, 2007 - 08:53 Imprimir Enviar

Botnets, redes Zombie, shellbots, winbots... quien no ha oído hablar de alguno de esos términos, muchos se preguntaran ¿quien los hace? ¿Por qué lo hacen? ¿Qué significa?, hoy gracias a una entrevista a fondo y en exclusiva a un conocido manipulador, programador, creador de inteligencia artificial (bots) podemos responder y aclarar el panorama acerca de este tema.
La siguiente entrevista se realizo con Morgan joven argentino que con solo unos años de edad ya es conocido personaje del ámbito under no solo en Argentina sino también en muchos países internacionales, incluso mas de una vez ha aparecido en listas de virus, seguridad, y por que no también decirlo en foros y otros lugares donde gente sin experiencia busca información acerca de este tema.

Morgan, ¿criminal?, ¿hacker?, ¿un dios?, en esta entrevista se hablo de muchas temáticas, incluyendo respuestas fuera de lo común, lo que nadie se atrevió a dar a conocer, la explicación que muchos buscan, el inicio de la información...

Damos gracias a el por habernos brindado esta entrevista, léanla atentamente ya que hay muchas cosas que deberían saber y nosotros gracias a el las hacemos publicas.

SA: Antes que nada, hace cuanto tiempo llevas metido en el tema de botnets y como se te ocurrió empezar en esto?

Morgan: Me interesó el tema en el año 2002/2003 no recuerdo bien. Un amigo, quien ya tenia su primer Bot formaba parte de un grupo que Hacían un bot llamado Prototype (pTy)
Me había mostrado un par de veces Sus canales con Botnets ...y las cosas que podía hacer, entonces decidí averiguar un poco del tema.

SA: Tenemos entendido que la gran mayoría de personas que tienen botnets lo usan para ataques de denegación de servicio, que otra utilidad les dan además de eso?

Morgan: La denegación de servicio fue un furor estos años para mucha gente, yo al principio los utilizaba para sacar claves... dejaba la función KeyLog de el bot encendida hacia algún canal ejemplo #Info y con algún script de mIRC grababa todo lo que había en #Info

(on *:text:*:#info:write c:/info.txt $1-)

Al día siguiente me pasaba un buen rato viendo que había capturado el KeyLog ...
Encontraba cuentas bancarias, paypals, servidores roots, Ftp's, correos,
sitios del gob. Luego de eso comencé a usarlos para la denegación de servicio
Me parecía divertido, todos temían de que yo les agarre la IP jaja...
en los servidores IRC tenia lo que quería con solo pedirlo (ips de usuarios, O:
lines etc.), la utilidad que prefiero darles ahora es Crear algunos programas por ejemplo para Hacer falsos clicks en AdSense o Testear otras cosas... la verdad ahora no uso (winbots) para atacar. Solo los uso para sacar información como hacia antes

SA: Winbots, hemos visto muchos códigos hablemos de shellbots (exp) es mas poderosa una botnet con shellbots que una con winbots?

Morgan: Los shellbots los conocí creo en el año 2004 o 2005. Antes era un simple script en perl que dejaba controlar la shell desde el IRC, con la opción de hacer un UdpFLood, Tcpflood.
En el 2005 con el error de PhpBB (viewtopic.php?t=) Era una locura que tantos sitios estén vulnerables a alguien se le ocurrió la idea de editar ese Shellbot para que Busque en google los foros PhpBB y los infecte automáticamente
Y decidimos Hacerlo... Me acuerdo muy bien esa noche cuando se probaba el código. Cuando comenzó a funcionar, nosotros teníamos un par de IRcd linkeados que soportábamos 3072 usuarios (nunca pensábamos en llenarlo) fue una cosa de locos, Lanzar el bot a buscar y ver como llovían... pero miles de Shellbots.

Era una cosa impresionante que hasta el día de hoy en los Winbots yo nunca he Visto En cuestión de un par de minutos, ya se habían llenado los 3 servidores. (3050 servidores WEB. los que equivalían a miles pero miles de maquinas de Windows "normales" infectadas) Me acuerdo que alguien que estaba con migo y otra gente en el Canal de pruebas Se fue porque tenia miedo de tener algún problema. Jaja...
La cosa es que ese código se hizo muy conocido y luego Google cambio el método de la búsqueda y el método de mostrar los resultados Ese shellbot todavía sigue por ahí en Internet, creo que había 40.000 sitios vulnerables.
Luego que paso todo eso, en el 2006 yo decido arreglar la Versión de ese Bot pero con otras funciones.
Por ejemplo este bot Buscaba lo que querías en google no solamente como antes (phpbb) sino que ahora podías aprovechar cualquier tipo de vulnerabilidad RFI
Para tener tu Botnet. Yo estaba en la red Gigachat donde toda la gente utilizaba mi código para infectar sitios y defacearlos o que se yo.
Cuando publique El código, que todavía lo tengo guardado:

```
#!/usr/bin/perl
# VulnScan v6 Stable By Morgan
#
# Note:
# DO NOT REMOVE COPYRIGHTS ...
# www.priv8.com.ar
#
# [Morgan]: http://priv8.com.ar/Zerocool.jpg
# [Morgan]: u got owned
# [ZEROCOOL]: bro
# [ZEROCOOL]: it's a rbot
# [ZEROCOOL]: i'm not fuckingstupid
# [ZEROCOOL]: uahuahuahuahua
#
#
# Greets to irc.gigachat.net :: #Morgan
#
#
# To work with auto-spread :
# Create a file named spread.txt with this :
#
#
#
# Change the url .. put ur bot url in that file
# then use the command :
#
# !morgan !eval @cmdstring='http://yoursite.com/spread.txt';
# or directly change it from the code..
#
# Enjoy the bot ....
# /Morgan
```

Bueno en fin. hoy en día los shellbots los usan casi todos, ya no prefieren usar winbots ya que rinden mucho menos ahora los utilizan para Buscar en google sitios vulnerables y defacearlos (A mi
criterio una estupidez)
Y claro el típico ddos... que ahora cualquiera se la da de Haxor con un par de bots :o)

SA: Si bien cada bot tiene cierta cantidad de fallos por los cuales escanear explotan y se reproducen (se denominan spreaders) es posible
darles comandos como por ejemplo: update?

Morgan: Si, yo tengo una versión con el comando !Update que lo que hacia era bajar el nuevo bot de alguna URL matar el proceso del bot actual y ejecutar el nuevo (Muy similar a los winbots)

SA: Los códigos llamados 0day o bots nuevos que no son públicos, generalmente se venden o intercambian, ahora en el caso de querer comprarlos se puede comprar con datos de alguna cuenta paypal o tarjeta de crédito digamos hacer una transferencia a esta X persona que tiene el código o generalmente es de otra forma?

Morgan: Yo nunca he vendido/comprado 0day's siempre los regalo (que buena persona) Pero alguna que otra vez he recibido un buen $$ por dar algunos 0day

SA: El tema de irc donde se alojan los bots... hay gente de empresas que realmente sepan que tienen alojado este tipo de irc y por temor o X motivo hacen "la vista a un lado"?

Morgan: Yo conozco empresas que el mismo dueño aloja botnets en ella, pero no deja que
sus clientes lo hagan. El problema de eso es cuando alguna Web de antivirus o lo que sea Desencriptan tu bot y denuncian la IP del botnet.

SA: A tu criterio que tan vulnerable son los sistemas Windows? en el caso de las botnets que sistema es mas propicio a infectar Windows o Linux?

Morgan: Prefiero infectar servidores en Linux, en Windows es como que ya me aburro no le
veo la gracia, salvo que encuentre alguna cosa nueva para hacer Son muchísimos mas vulnerables los sistemas en Windows.

SA: Los bots poseen algún tipo de identificación que te permita saber de que país provienen?

Morgan: Hay versiones de Winbots y Shellbots que detectan el país, lenguaje o sistema donde están ejecutados y hasta tienen de nick el país...
Por ejemplo:
[05|USA|XP|SP0]-7271

EL 05 es la cantidad de días, USA es su país, XP el sistema operativo y SP0 en
esa versión indica que service pack lleva

En shellbots:
[BR]-91827374
[USA]-12938582
[UK]-19237214
País - números y letras aleatorias.

SA: Podes comentarnos algunas funciones de ellos?

Morgan: Acá tenes algunas, http://www.darksun.ws/phatrxbot/rxbot.html :)
Y en los Shellbot... los mas usados son el !scan , !udpflood !tcpflood !synflood !httpflood y !portscan

SA: En tu caso principalmente que objetivo buscas al tener una botnet? ego propio, ataques de denegación, obtener datos...

Morgan: Yo los tengo porque son de utilidad muchas veces, ya sea para hacer algún pequeño ddos, sacar alguna info, entrar en algún servidor

SA: Denegación de servicio... alguna empresa te ha pagado alguna vez por este servicio?

Morgan (nos cita un documento en la Web que habla de el): En 9 días hemos recibido 6 ataques masivos a nuestro sitio Web, motivo
por el cual de manera constante nos han tirado abajo los servidores.
Algunos de los servers: que el joven: "MORGAN", se ha encargado de ATACAR FEROZMENTE, son:
1) http://www.freesevers.com
2) http://www.fortunecity.com
3) http://www.adwarspace.com
4) http://www.110mb.com
5) http://www.googlepages.com
También los servidores de nuestro Foro de Discusión están recibiendo ataques Masivos, y en estos momentos se está trabajando para ponerlo nuevamente ON LINE.

Por esta TAN NOBLE TAREA, "Morgan" (que algún día les contaré quien es, a que se dedica, y muchas otras cosas mas) cobra la nada despreciable suma de $ 3.000 mensuales, desde el mes de mayo de este año.

SA: Cuanto tardaría una persona en obtener digamos un par de cientos de bots a partir de uno solo?

Morgan: Depende... una persona con recursos y conocimientos... minutos, una persona que ha creado su primer botnet y es su primera experiencia y no tiene recursos puede tardar un poco

SA: La pregunta del millón: ¿es verdad que obtenes acceso a cuentas de banco papals datos de tarjeta de crédito y parecidos con ellos? y luego... es posible "retirar dinero" de esas cuentas para beneficio propio?

Morgan: O.o
Yo Prefiero vender los datos antes que arriesgarme como antes.
Claro que es posible, en algunas épocas se pone de moda algún llamado BUG en Western unión con el tema de las transferencias actualmente esta funcionando con Italia y Francia, hasta hace poco con Australia.
Después están los Cashiers, que son los que les pasas las cuentas o les haces las transferencias bancarias y ganas tu %.
Igualmente esta muy vulnerable la seguridad con el tema de compras online (Porque a las empresas les conviene) Así que no es tan difícil ir a Amazon.com comprarse algo con tarjeta, y crear una Suite en Skybox para recibir las cosas.

SA: Hemos tenido contacto con varias personas que mantienen botnets e incluso nos han invitado a su irc para ver funcionar sus bot, hemos visto algo que nos llamo la atención una especie de "mercado negro", la compra o venta de cuentas paypal e-gold datos de tarjetas de crédito etc... sin compromisos, podes explicar de que se trata?

Morgan: Claro, es la típica venta de garaje... se vende de todo... yo en eso que le llamas "mercado negro" he visto desde venta de tarjetas hasta trafico de personas.

SA: Se puede ganar dinero no solo con ataques sino por ejemplo: generando mas visitas en una Web realizando clicks en sistema que pagan por ello, etc.?

Morgan:
Ingresos de hoy: US$218,25
Responde eso tu pregunta? ^^

SA: Que tan seguros son los bots? es decir sabemos que alguien con pocos conocimientos puede "robarte" una botnet lo cual podría ser un gran desastre como se protegen ante este tipo de ataques?

Morgan: Uff no me hagas acordar, si abre perdido bots en el camino
Lo mejor es asegurarse de usar un servidor propio, con las contraseñas del ircd Encriptadas... y utilizar autentificacion por nick!ident@host en los bots.

SA: En argentina que tan conocido es el tema? hay mucha gente metido en esto? y realmente acá has hecho $$ a partir de algún "servicio de denegación"

Morgan: En argentina están de moda los winbots. También hay otros que tienen sus shellbots, pero solo porque tienen el código que los genera y listo. (Así cualquiera)
Yo sí, sinceramente he echo bastante dinero con el ddos y con los botnets. pero hay otras cosas para sacar más dinero.

SA: Tuviste problemas con la "ley?

Morgan: Siempre "safé", alguna vez tuve que parar. cambiar el disco. dns. emails etc.

SA: Cual fue a tu criterio el mejor ataque que cometiste?

Morgan: Fibertel argentina (Owned =) en la época Del Santy shellbot. con miles...

SA: Una vez cierta persona dijo en una entrevista (conocido portal hacker solo por el nombre) :Yo no tengo ninguna botnet. Esos son criminales. ¿Que pensas? realmente son criminales ustedes o es mas fácil juzgar a quien los contrata a ustedes para este tipo de ataques?

Morgan:
Criminales? no creo.
Criminales son esos hijos de puta que roban, secuestran, matan gente en nuestro país...
Criminales son esos políticos que nos gobiernan

SA: Palabras finales...

Hm, quisiera aclarar que hoy en día no realizo NINGUNA de las actividades estas,

Be safe.
/Morgan

#EOF

En el transcurso de los días crearemos un video documental donde veremos la "acción" por dentro de estos bots, como infectan realmente, donde buscarlos, el mercado negro, y mas para que ustedes puedan observar mas detenidamente este movimiento Ander que no tan conocido se lleva mucha ventaja de otros...

Nota: Security Adiction = SA

Entrevista: Botnets... el lado oscuro | Entrar/Crear una cuenta | 6 Comentarios

Mostrar Por Hilos de conversación Orden Los más viejos primero Refrescar

Pay attention to hardcord sex

por Invitado en 29 Dic, 2007 - 08:55

hardcord sex x men sportman nude x **naked teennagers** x entai ball dragon x ask ***** blacj x erect penis hard x made sxe home x twikn boys naked x **sex anla viedeos** x speis totallly x latexclubb x britne ***** x kobe sanua x celeberties free nude x cleebrities naked x **hhorny mamas** x diana russina x ***** sisster x fergie naked boobs x onterracial x rose mcgowan topless x "free movies bestiality" x boy masterbation teen x girl yuong

German Big Titts - I am serious !!

por Invitado en 29 Dic, 2007 - 08:56

German Big Titts . Pre-teen Hotties . Bbabes Nude . Jessica Alba Boobs . Orgazm Ladies . **Meg Naked Griffin** . **Coolio Babbes** . **Hot Horny Teachers** . Eroric Review . Housewife ***** . Nude Striptese . **Sexstories Post.com** . D Cup Girls . Shitting Gorls . **Black Free Ass Squriters** . **Musscle Gay** . Sex Movues . Sex Hardcore Lesbian . Summer Cummings . Cyberertoica . Tamned Teen

You must hear of Download Porn!

por Invitado en 10 Ene, 2008 - 07:02

Download Porn ? Groin Girls In The Kick ? Sucking Big Black ***** ? Public In Places Sex ? Teen Virgin ***** ? Swimming Topless ? **Latino Slut** ? Nude In Shower ? Tuner Girls Import ? Shemale Movies ? Sex Jungle ? Naked Carrie Fisher ? Punk Hairstyles ? **Voyuer** ? Jorja Fox A Lesbian ? Britney Spears Sucking Dick ? Shemale Panties ? **Sable Naked** ? ***** Head Up ? Lesbian Asian ? **Hardcore Black** ? Comic Bondage Fairies ? Kimpossible Porn ? Young Hot Guys ? **Dick Big** ? Girls Gone Wild Pictures ? With Girls Horses ? Job Blow Auditions ? Mom

Rachael Ray Nude - I am serious !!

por Invitado en 10 Ene, 2008 - 07:02

Rachael Ray Nude -- Apparel Dressage -- Xxx Celebs -- **Ass Ebony Black** -- Hot Cumshots -- First Time Virgins -- Ladies Village -- Eternal Nymphets -- Devon Sex -- Free Amateur Wife -- Nipples Hairy -- Heatherbbw -- Sex Bots -- Black Women Nude -- Dirty School Girl -- Old Lesbians -- Realmilfsex -- Gay Peeing -- Asian Pee -- **Christina Aguilera Nipple Slip** -- Gargoyles Hentai -- Sexy Sailor Moon -- Women Masterbation -- Gallery Anderson Pamela Nude -- **Family Orgies** -- Men Sucking Men -- **Gay Cartoon Sex** -- Sex Hilton Paris Having

Twstys.com - I am serious !!

por Imhoff33 en 11 Feb, 2008 - 11:36
(Información del usuario | Enviar un mensaje

Twstys.com x **Womens Errotica** x Penis Suking x PoornÂŽplus x Ttavestis x Erotic Lesbian x Hadcore Blowjob x Puffy Nipples Small Tits x Revealin Lingerie x Where Is The Love Black Eyed Peas x Marge Simpson ***** x Astrobooty x Hardore Pics Suze.net x Lesbiab Coeds x **Sex In The Water** x Girls Get Fukced In Car x Littlr Girls x **Nice Booobs** x Dirty Young Girls x Ejaulation Pictures x "brother+sister+*****" x **0ld Mature Sex** x Ideepthroat Download x Ftv Gils x **Mastervation For Women** x Gay Dik Free x Inbedwithashley Gallery x **Britney Spears Slipped Tit** x Sxe Viodes

Analvideos - I am serious !!

por Imhoff33 en 11 Feb, 2008 - 11:41

(Información del usuario | Enviar un mensaje

Analvideos : Guys Wearing Jock Straps : Extreme-tits : How To Get A Girl : Misty From Pokemn Nude : Adlt Sex Videos : **Exceptional Leaders** : Gay Poeno : Girl On Gril Pron : Laino Pron : **Preg Hentai** : Teen Amatur Preview : Mastetbation Technique : Sexy Dbz : Slave Cage : Fjiko Kano

Tu Web de Seguridad