Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Obteniendo el código utilizado en ataques de inyección de código en web

Hugo Francisco González Robledo
hugo.gonzalez@upslp.edu.mx

Agenda

- Antecedentes
- Tipos de ataques
- Trabajo relacionado
- Experiencia de trabajo
- Arania
- Resultados
- Conclusiones
- Trabajo a futuro

Antecedentes

- La aparición de virus, gusanos, troyanos y malware en general ha ido aumentando en los últimos años en Internet.
- Code Red, Nimda (2001)
- SQL Slammer (2003)
- Otros
- Es importante conocer al enemigo para poder luchar contra él.

Tipos de ataques

- Inyección de SQL
- Inyección de código
- XSS
- Inclusión de código remoto

Trabajo relacionado

- Honeypots
- PhpHoneypot
- Google hack honeypot

Experiencias de trabajo

- A finales del 2005, se reportaron varias vulnerabilidades relacionadas con Mambo, las cuales permitían ataques de tipo inclusión de código remoto. Los anuncios en formato original se muestran a continuación:
- El 17 de noviembre de 2005
- - Mambo "mosConfig_absolute_path" Remote File Inclusion Vulnerability
- http://www.frsirt.com/english/advisories/2005/2473
- - Mambo "mosConfig_absolute_path" Remote Command Execution Exploit Advisory ID : FrSIRT/ADV-2005-2473Rated as : High Risk
- http://www.frsirt.com/exploits/20051122.mambo45

- Se identificaron 42 nombres de herramientas diferentes, hospedadas en 220 sitios. La proliferación de sitios se debe principalmente que cuando identifican un archivo de este tipo es cancelado o borrado. La mayoría de los sitios son de alojamiento gratuito.
- Se identificaron durante los 3 meses de mayor actividad: 43656 intentos de explotación sobre un solo servidor. 973 ips únicas.

Direcciones con mayor cantidad de ataques

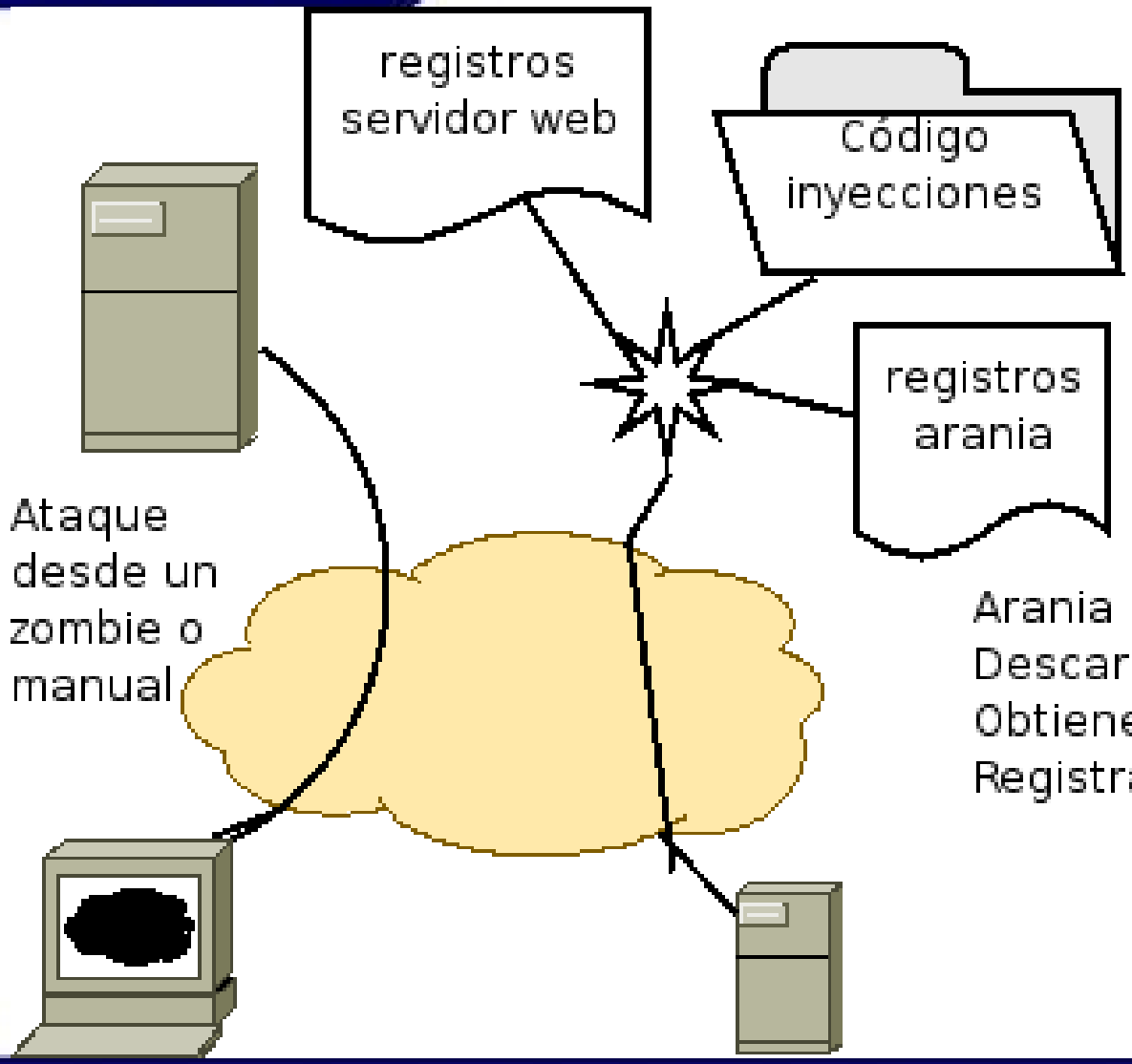
595	212.29.217.4
631	213.193.212.208
682	81.169.182.111
723	81.169.134.50
748	212.87.13.140
761	218.208.21.7
816	66.240.226.25
837	81.208.30.102
2032	193.255.143.5

Arania (Motivación)

- Luego de estar monitoreando el servidor, se intentaron descargar el código malicioso. Realizar esta tarea de forma manual fue ardua y no siempre se conseguía obtener la información, ya que algunos códigos ya habian sido eliminados. Y aunque las herramientas usadas que se obtuvieron tenían los mismo nombres, el código algunas veces variaba.
- Además de que algunas veces existia el “second include”

Arania (Diseño)

- El diseño de arania es simple y concreto, se cumplen varios objetivos:
  - Monitorea de forma automáticas/manual los registros del servidor web.
  - Es un modelo no-intrusivo, no afecta el funcionamiento del servidor web.
  - Obtiene el código malicioso que se trato de incluir.
  - Lo almacena marcándolo de acuerdo a su contenido.
  - Mantiene un registro detallado.
  - Se incorpora el “second include”, para descargar códigos incluidos en el primer ataque.



Arania monitorea registros
Descarga el código malicioso
Obtiene una firma y la almacena
Registra la actividad

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Arania (Descargas)

Aplicaciones Lugares Sistema vie 8 de jun, 13:30

arania - Google Code - Firefox

File Edit View History Bookmarks Tools Help

http://code.google.com/p/arania/downloads/list

Getting Started | Honeynet Project RS... | honeyblog | El Universal: Minuto... | OSNews | Barrapunto | La Cofradía ...

Programa | Shadowserver ... | Cyberbulling D... | DeepSec IDSC ... | arania - Goo... | PSC

hugo.glez@gmail.com | My Profile | Help | My Account | Sign out

Google Code

arania

Detect malicius remote code inyection.

Search Projects | Search the Web

Project Home | Downloads | Wiki | Issues | Source | Administer

New Download | Search Current Downloads for Search

1 - 2 of 2

Filename	Summary + Labels	Uploaded	Size	DownloadCount	...
arania1.0.2.tar.gz	Current version, some features included	Apr 12	2.4 KB	143	
araniav1.0.1.tar.gz	Some bugs fi	o 23	2.1 KB	26	

1 -

Uploaded	Size	DownloadCoun
Apr 12	2.4 KB	143
Feb 23	2.1 KB	26

©2007 ... cussion Group

Discusión

- Este código desarrollado en perl es muy similar, incluye funciones para conectarse a un servidor IRC, y esperar las ordenes del administrador de ese canal. Las ordenes que puede ejecutar son funciones dentro del programa, y están el escaneo de puertos, ataque de denegación de servicio “tcpflood” que es una inundación de peticiones, otra función es obtener la versión del bot, y tiene una función para buscar servidores mambo vulnerables y atacarlos, de echo esta es el mecanismo principal de dispersión.

Clasificación

- Shells php
  - c99shell
  - r57shell
- Deface tools
  - Revengans
- Pruebas
  - Morpheus Fucking Scanner

Aplicaciones Lugares Sistema vie 23 de mar, 20:39

localhost - c99shell - Firefox

File Edit View History Bookmarks Tools Help

http://localhost/inyection/fb50fb8dfcd38529492dfead930427f1

Getting Started Latest Headlines

!C99Shell v. 1.0 beta (21.05.2005)!

Software: Apache/2.0.55 (Ubuntu) mod_jk/1.2.18 PHP/5.1.6 mod_ruby/1.2.6 Ruby/1.8.4(2005-12-24)
uname -a: Linux Afrodita 2.6.15-26-686 #1 SMP PREEMPT Fri Sep 8 20:16:40 UTC 2006 i686
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: OFF (not secure)
/var/www/inyection/ drwxr-xr-x
Free 1.39 GB of 18.34 GB (7.59%)

Encoder Bind Proc. FTP brute Sec. SQL PHP-code Feedback Self remove Logout

Owned by hacker

Listing directory (14 files and 0 directories):

Name	Size	Modify	Owner/Group	Perms	Action
.	LINK	23.03.2007 21:38:03	hugo/hugo	drwxr-xr-x	
..	LINK	23.03.2007 21:26:28	root/root	drwxr-xr-x	
0c725f73e1b1ae33d03ce6c75e056571.php	13.44 KB	23.03.2007 21:29:39	hugo/hugo	-rw-r--r--	
01f3e68daeda9cb95d6820ea444334d3.php	20 B	27.02.2007 21:30:27	hugo/hugo	-rw-r--r--	
3b360e9bee7d458254a8c5dca632f4b7	21.16 KB	14.03.2007 21:39:39	hugo/hugo	-rw-r--r--	
4b75a81453bc84022f5480af069b409f	21.16 KB	12.02.2007 21:24:48	hugo/hugo	-rw-r--r--	
33d483fe302eab5eb1f0ea74cf929e45.php	186 B	21.03.2007 13:40:52	hugo/hugo	-rw-r--r--	
a89ede311c62db2a45a7aa908c8ce4d3.php	18.07 KB	23.03.2007 21:36:39	hugo/hugo	-rw-r--r--	
aa9a438c663c6e2728a94fbdf105e020.php	12.77 KB	16.02.2007 10:51:03	hugo/hugo	-rw-r--r--	
c6a9f127a925b03e9258950add07f026	593 B	15.03.2007 01:04:58	hugo/hugo	-rw-r--r--	
ce1bcf10a381bc729d93355fa2976bff	158.71 KB	12.03.2007 00:26:51	hugo/hugo	-rw-r--r--	
cmd2.txt	13.6 KB	19.03.2007 14:15:43	hugo/hugo	-rw-r--r--	
d7bbd74cf30203b8b608fec1d4754cf8	21.58 KB	12.02.2007 21:20:51	hugo/hugo	-rw-r--r--	
ed1fa8d084da09377857e06e07dd8346	18.07 KB	12.02.2007 21:20:36	hugo/hugo	-rw-r--r--	
fb50fb8dfcd38529492dfead930427f1.php	152.44 KB	12.02.2007 21:25:14	hugo/hugo	-rw-r--r--	
fea71881a0632685ff1e5cd6366580e2	16.56 KB	16.02.2007 20:37:20	hugo/hugo	-rw-r--r--	

Done

Aplicaciones Lugares Sistema vie 23 de mar, 20:30

Firefox

File Edit View History Bookmarks Tools Help

http://localhost/inyection/0c725f73e1b1ae33d03ce6c75e056571

Getting Started Latest Headlines

[CMD By #ShellFull] ?

by triton - maxsdr2@hotmail.com

sysname: Linux
nodename: Afrodita
release: 2.6.15-26-686
version: #1 SMP PREEMPT Fri Sep 8 20:16:40 UTC 2006
machine: i686
user: uid(33) euid(33) gid(33)
write permission: no
server info:
pro info: ip 127.0.0.1, *xterm* at /usr/X11R6/bin/xterm, *wget* at /usr/bin/wget, *lynx* at /usr/bin/lynx, *gcc* at /usr/bin/gcc, *cc* at /usr/bin/cc
***safe_mode*: NO**, *PHP* 5.1.6
current path: /var/www/inyection

command

send cmd | using shell_exec() | PHPget | PHPwriter | fileditor | list files on | safemode

stdOut from "", using *shell_exec()*

```
Comandos Exclusivos do DTool Pro

chdir <diretorio>; outros; cmds;
Muda o diretorio para aquele especificado e permanece nele. Eh como se fosse o 'cd' numa shell, mas precisa
ser o primeiro da linha. Os arquivos listados pelo filelist sao o do diretorio especificado ex: chdir
/diretorio/sub/;pwd;ls

PHPget, PHPwriter, Fileditor, File List e Overwrite
fale com o triton :P
```

Done

Aplicaciones Lugares Sistema vie 23 de mar, 20:40

By destructive > irc.gigachat.net > CMD > File List - Firefox

File Edit View History Bookmarks Tools Help

http://localhost/inyection/d7bbd74cf30203b8b608fec1d4754cf8

Google

Getting Started Latest Headlines

Informa►►es

Sistema: Linux
Uname: Linux Afrodita 2.6.15-26-686 #1 SMP PREEMPT Fri Sep 8 20:16:40 UTC 2006 i686
PHP: 5.1.6, **safe mode:** *OFF*
Methods: wget GET lynx
Ip: 127.0.0.1
Command: ls Send

Dir NO: /var/www/inyection/ - [New Dir] [New File] [BackTool]

Upload: Browse... Send

Entrance in the directory, OK!

Perms	File	Size	Commands
16877	../	4 KB	[Rename] [Del] [Chmod] [Copy]
33188	ed1fa8d084da09377857e06e07dd8346	18.07 KB	[Rename] [Del] [Chmod] [Copy]
33188	4b75a81453bc84022f5480af069b409f	21.15 KB	[Rename] [Del] [Chmod] [Copy]
33188	d7bbd74cf30203b8b608fec1d4754cf8.php	21.58 KB	[Rename] [Del] [Chmod] [Copy]
33188	fea71881a0632685ff1e5cd6366580e2	16.55 KB	[Rename] [Del] [Chmod] [Copy]
33188	ce1bcf10a381bc729d93355fa2976bff	158.70 KB	[Rename] [Del] [Chmod] [Copy]
33188	3b360e9bee7d458254a8c5dca632f4b7	21.16 KB	[Rename] [Del] [Chmod] [Copy]
33188	c6a9f127a925b03e9258950add07f026	0.57 KB	[Rename] [Del] [Chmod] [Copy]
33188	cmd2.txt	13.59 KB	[Rename] [Del] [Chmod] [Copy]
33188	01f3e68daeda9cb95d6820ea444334d3.php	0.01 KB	[Rename] [Del] [Chmod] [Copy]
33188	0c725f73e1b1ae33d03ce6c75e056571.php	13.43 KB	[Rename] [Del] [Chmod] [Copy]

Transferring data from localhost...

Conclusiones

- El problema de la inseguridad informática crece cada día, y los esfuerzos por mantenerse a salvo exígen cada vez más de las aplicaciones y del administrador de las mismas, es importante mantener contacto con anuncios para poder preparar nuestros sistemas y evitar ser víctimas de estos atacantes.
- Las herramientas nos simplifican la vida

Conclusiones (II)

- Los usos que se dan a los equipos comprometidos por lo general generan ganancias económicas a los atacantes.
  - Desde spam
  - Phishing scam
  - Control completa de la maquina.
- Un caso de un equipo comprometido, fue usado para generar spam relacionado con phishing scam.

Trabajo Futuro

- Se esta trabajando sobre una herramienta que permita clasificar automáticamente el malcode recolectado. “Chrysopa” es el nombre y será liberada proximante.
- Analiza el código recolectado por “arania”, obtiene el nombre de las funciones y las relaciona con los otros códigos ...