

JATIMCOM: PHP BOTNETS IRC

Los ataques en forma de RFI son todavía muy comunes y efectivos, al igual que las Botnets controladas por IRC. Seguramente recibimos todo el tiempo múltiples de éstos ataques web que habitualmente pasan desapercibidos para nosotros, incluso una vez nuestras web y servidores actúan como Zombies de la Botnet.

1-Como nos percatamos del intento de RFI?

Si usamos un gestor de contenidos, un CMS como Drupal, Wordpress, Joomla o cualquier otro, y disponemos de un "log" de acceso, podemos ver como algunas URL como las siguientes:



The image shows three screenshots of web server logs. Each log entry shows a visitor (labeled 'Visitante') with an IP address, the last URL accessed, the user agent (Mozilla/5.0), and the host. The URLs are suspicious, containing keywords like 'vote', 'ask', 'password', 'poll', 'aip', 'id', 'txt', 'root', 'calendar', 'dategif', 'ipays', 'fid', 'txt', 'show_image', 'imgtag', 'php7mosConfig', 'absolute_path', 'http', 'www', 'protech', 'sa', 'Fimages', 'Fmcith', 'Fid', 'txt', 'F', 'govorit', 'mgsu', 'gic6', 'ch', 'govorit', 'ru'.

Podemos ver claramente el intento de RFI (Inclusión remota de archivos) desde una dirección web ya vulnerada, un servidor *zombie*, o bien una web creada para tal propósito.

Aunque la mayoría de las veces se utilizan escáneres automatizados como por ejemplo el explotado *FeeLCoMz* AI PHPBot, ahora una *moda* en países como Indonesia.

Algunos de los directorios donde se alojan los archivos maliciosos tienen permisos de lectura y escritura y podemos verlos directamente mediante el navegador web:

Index of /images/.ajim

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 ajim.txt	04-Oct-2009 05:02	186K	
 ajim1.txt	04-Oct-2009 04:59	76	
 ajim2.txt	04-Oct-2009 05:00	2.1K	
 asp-bot1.txt	22-Dec-2009 12:19	28K	
 edit.txt	18-Dec-2009 04:28	35K	
 idx.txt	27-Oct-2009 11:39	495	
 md5.txt	12-Sep-2009 14:49	15K	
 script.txt	08-Dec-2009 15:07	45K	
 yopcrew.txt	18-Dec-2009 04:23	35K	
 yopcrew.txt.1	18-Dec-2009 04:23	35K	
 wunderbar_emporium.tgz	14-Aug-2009 16:15	3.3M	

Apache/2.2.4 (Ubuntu) mod_jk/1.2.23 mod_mono/1.2.4 mod_python/3.3.1
Port 80

Una vez recopilamos alguna información, el tipo de herramientas usadas y alguna información sensible como direcciones de correo, nicks, imágenes...etc localizados los administradores de algunos sitios web que promueven públicamente estas herramientas y que en muchos casos disponen de botnet propia y son responsables de muchos intentos de RFI a nuestras webs.



En la imagen superior vemos una Shell modificada que se utiliza y distribuye actualmente.

Normalmente, los administradores de estas comunidades se escudan en que no pueden controlar lo que hacen algunos usuarios con sus códigos... o cualquier otra excusa del mismo tipo.

Cuando alguno de éstos escáneres nos realiza una prueba (archivo id1.txt, id.txt...etc):

```
<?php /* Fx29ID */ echo("Feel"."CoMz"); die("Feel"."CoMz"); /* Fx29ID */ ?>
```

Intenta comprobar si nuestra web es vulnerable a la inclusión remota de archivos(tienen listados amplios de "Dorks" predeterminados), si lo fuera y en la pantalla (navegador web) se mostrase simplemente el texto **Feel CoMz**, tendrían un directorio entero de nuestro servidor a su disposición para subir todo tipo de archivos, shells, escáneres, mailers, herramientas de DoS y archivos de todo tipo para seguir a su vez realizando éstos tipos de ataque en servers que actúan de "proxy" para ellos. Mientras ellos siguen desfigurando portadas, robando datos, eliminando archivos... y ampliando la red Zombie mantenida y controlada desde Mirc o paneles web como el siguiente:

<http://www.aminef.or.id/images/eusa/bot.php>



Visit <http://jatimcom.uni.cc/>

La comunidad Jatimcom, y muchas otras que operan desde Indonesia ahora mismo y que molestan a millones de webs en todo el mundo.

Jatimcrew, lumajangcrew, kamtiez.us, arianom.tk, hacker-newbie.org, inj3ct0r.com, fuck.vodork.co.cc, gang-dolly.co.cc, jerinxzone.co.cc, todas ellas situadas en Indonesia, mantienen, utilizan y amplían y difunden sus redes y herramientas BOT PHP, utilizadas para ganar dinero con la publicidad de sus sites ([Comprovar estadísticas Jatimcom](#)).

Aparentemente algunas webs propiedad de éstas comunidades tienen un aspecto normal e inofensivo:



Pero detrás de estos sitios aparentemente inofensivos se encuentran comunidades de (como ellos llaman) “hacking” de países como Brasil, Rusia, Indonesia, Italia, España, Turquía, Marruecos, o Argentina por citar a algunos, aunque podemos encontrar comunidades de éstas en casi todos los países.



Listado de sitios **zombie atacantes**:

<http://rdoug.sytes.net/on.txt???>
<http://goldenhelmets.fr/zip/test.txt??>
<http://rdoug.sytes.net/on.txt???>
<ftp://189.19.36.105/temp/pz.txt???>
<http://www.bci.unisel.edu.my/>
http://www.howtolisten.kr/sarangbi_bgm/id1.txt?
<http://bajuszbt.hu/language/byz9991.txt???>
http://www.miranda.gov.ve/modules/mod_sections/id1.txt???
<http://bajuszbt.hu/language/byz9991.txt???>
http://www.miranda.gov.ve/modules/mod_sections/id1.txt???
<http://www.verseoftheweek.com/id1?>
<http://www.boomong.com/bbs//data/1.txt???>
<http://daejin-env.co.kr/board/data/file/bbs7/id1.txt????>
http://www.p2700.pe.kr/bbs///skin/uks_gallery_v1090_10up/setup/dcom/au1.txt??
<http://nic.bupt.edu.cn/media/spread.txt?&modez=psybnc>
<http://daejin-env.co.kr/board/data/file/bbs7/id1.txt????>
<http://www.protech.su//images/zamki/id1.txt??>
<http://altogm.com/bbs/data/id1.txt?>
<http://www.jacksart.nl//administrator/templates/id1.txt?>
http://www.foodntop.com/bbs/data/notice_1/robot.txt????
<http://christmanandcompany.com/help/respon1.txt?>
<http://www.odysseygrp.co.uk/images/pickosikat.txt??&modez=psybnc>
<http://72.52.245.180/~sealques/x/id1.txt???>
<http://sparklygreeneyes.com/files/.data/id1.txt??>
[http://lclink.co.kr/bbs/icon/private_icon/templates/sken/id1\(pirates\).txt?](http://lclink.co.kr/bbs/icon/private_icon/templates/sken/id1(pirates).txt?)
http://www.kandeladesign.fr/administrator/components/com_tmp/ids1.txt??????
<http://networks.kpru.ac.th/list/respon1.txt??>
<http://www.kgbrico.xpg.com.br/bsp.txt?>
<http://www.stomatformula.com.ua/help/sh/id1.txt??>
<http://www.guianossacidade.com.br/logo/id1.txt??>
<http://www.knxshop.fr/>
http://www.isfparma.org/modules/mod_people/idlab1.txt??
<http://www.atb.gov.tr/portal/administrator/et/id2.txt?????>
<http://tailor.wen.ru/1.txt??>
<http://amedan-beaute-institut.fr/media/id1???>
http://bdkorea.org/zeroboard/data/bangla_notice/gh1.txt???
http://snia2009.com/components/com_jce/zfxidl.txt?
<http://www.cuccio.com/pdfs/eeng/respon1.txt?>
<ftp://vamo@akininguemtaska.info:vamo@akininguemtaska.info/yenor.php?>
<http://www.vinotecnia.es/files/ts????>
<http://ayasotel.com/media/ts????>
<http://www.hyonsvc.co.kr//bbs//icon/id1.txt???>
<http://arsip.rembangkab.go.id/modules/head??>
<ftp://alexandredasilva:12345@www.alexandredasilva.com/teste.php?>
<http://www.mendipcastors.co.uk/templates///id1.txt?>
http://snia2009.com/components/com_jce/zfxidl.txt?
<http://forum.c4evn.org/id1.txt?>
<http://kpaa.or.kr/int/skin/latest//dex/id1.txt????????????????????>
<http://www.maratechengineering.com/zen-cart/images/dvd/test.txt??>
http://jjang.oxwiz.co.kr/zboard//board/zero_vote/.cok/P1.txt?
<http://www.benibouayach.com/cache/1.txt??>
<http://www.telleriasnunez.com%2Fidl.txt%3F%3F>
<http://www.sly8.com/sly8//bbs/id1.txt?>
<http://dive2world.com/newdive/F1.txt>
<http://nic.bupt.edu.cn/media/j1.txt???>
<http://www.howtolisten.kr//parti/data/admin/id1.txt???>
<http://nic.bupt.edu.cn/media/j1.txt???>
http://www.miranda.gov.ve/modules/mod_sections/tmpl/main???

Podríamos ampliar muchísimo ésta lista, solo es cuestión de tiempo recibir éste tipo de ataques RFI.

-Más información de éste tipo de ataques y parecidos en la web luctus.es-



La conclusión que a groso modo extraemos de todo esto, es que actualmente operan millares, (por no decir millones) de comunidades similares a ésta.

Algunas más "*profesionalizadas*" y otras menos, pero más vale estar al día, tanto nosotros los usuarios comunes, como los servicios de web hosting.

Si tienes una web escrita en PHP eres un posible objetivo de éste tipo de escáneres que a veces detectan y explotan vulnerabilidades recientemente descubiertas, muchas de las veces con éxito. (Solo hay que mirar el log diariamente y ver que los ataques proceden de muchos sitios web diferentes). Si quiere saber que hacer frente a éste tipo de ataques y como protegerse contacte conmigo en la siguiente dirección de correo:

admin@luctus.com

Página Web: <http://luctus.es>

BOTNETS IRC © 2010 Fosul JATIMCOM: PHP