

Boletín de Seguridad UNAM-CERT-2012-003 Actividad DDoS

El US-CERT ha recibido información de múltiples fuentes acerca de ataques coordinados de negación de servicio distribuido (DDoS) con objetivos que incluyen agencias de gobierno de E.U.A. y sitios de la industria del entretenimiento. El colectivo afiliado de "Anonymous" supuestamente promovió los ataques en respuesta a la baja del sitio de hosting de archivos MegaUpload y en protesta a la propuesta de la legislación de E.U.A. concierne al tráfico en línea de derechos de propiedad intelectual y falsificación de bienes ("Stop Online Piracy Act", o SOPA y "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act", o PIPA).

- **Fecha de Liberación:** 24-Ene-2012
- **Última Revisión:** 20-Feb-2012
- **Fuente:** US-CERT
- **Riesgo** Importante
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Negación de servicio

1. Descripción

El US-CERT tiene evidencia de dos tipos de ataques DDoS: uno utilizando peticiones HTTP GET y otro utilizando un simple UDP flood.

La "Low Orbit Ion Cannon" (LOIC) es una herramienta de ataques de negación de servicio asociada con actividades previas de Anonymous. El US-CERT ha revisado al menos dos implementaciones de LOIC. Una variante está escrita en JavaScript y está diseñada para ser utilizada desde un navegador web. Un atacante puede acceder a esta variante de LOIC dentro de un sitio web, seleccionar objetivos, especificar mensajes opcionales, acelerar el tráfico de ataque y monitorear el progreso de dicho ataque. Una variante del binario de LOIC incluye la habilidad de unirse a una botnet para permitir a los nodos ser controlados mediante canales IRC o comandos RSS ("hiveMind").

Lo siguiente es una muestra del tráfico de LOIC capturado en una bitácora de un servidor web:

```
"GET /?id=1327014400570&msg=We%20Are%20Legion! HTTP/1.1" 200
99406 "hxxp://pastehtml.com/view/blafl1y1.html" "Mozilla/5.0
(Windows NT 6.1; WOW64; rv:9.0.1) Gecko/20100101 Firefox/9.0.1"
```

Los siguientes sitios han sido identificados en las cabeceras HTTP referrer con tráfico LOIC sospechoso. Esta lista podría no estar completa. Por favor no visite cualquiera de estos links ya que podría aún estar funcionando LOIC u otro código malicioso.

```
"hxxp://3g.bamatea.com/loic.html"
"hxxp://anonymouse.org/cgi-bin/anon-www.cgi/"
"hxxp://chatimpacto.org/Loic/"
"hxxp://cybercrime.hostzi.com/Ym90bmV0/loic/"
"hxxp://event.seeho.co.kr/loic.html"
"hxxp://pastehtml.com/view/bl3weewxq.html"
```

UNAM-CERT

```
"hxxp://pastehtml.com/view/bl7qh5c.html"
"hxxp://pastehtml.com/view/blafp1ly1.html"
"hxxp://pastehtml.com/view/blakyjwbi.html"
"hxxp://pastehtml.com/view/blal5t64j.html"
"hxxp://pastehtml.com/view/blaoyp0qs.html"
"hxxp://www.lcnongjipeijian.com/loic.html"
"hxxp://www.rotterproxy.info/browse.php/704521df/ccc21Oi8/
vY3liZXJ/jcmltZS5/ob3N0emk/uY29tL1l/tOTBibVY/wL2xvaWM/v/b5/
fnorefer"
"hxxp://www.tandycollection.co.kr/loic.html"
"hxxp://www.zgon.cn/loic.html"
"hxxp://zgon.cn/loic.html"
"hxxp://www.turbytoy.com.ar/admin/archivos/hive.html"
```

Lo siguiente son registros A de los sitios referentes al 20 de enero de 2012.

3g[.]bamatea[.]com	A	218[.]5[.]113[.]218
cybercrime[.]hostzi[.]com	A	31[.]170[.]161[.]36
event[.]seeho[.]co[.]kr	A	210[.]207[.]87[.]195
chatimacto[.]org	A	66[.]96[.]160[.]151
anonymouse[.]org	A	193[.]200[.]150[.]125
pastehtml[.]com	A	88[.]90[.]29[.]58
lcnonngjipeijian[.]com	A	49[.]247[.]252[.]105
www[.]rotterproxy[.]info	A	208[.]94[.]245[.]131
www[.]tandycollection[.]co[.]kr	A	121[.]254[.]168[.]87
www[.]zgon[.]cn	A	59[.]54[.]54[.]204
www[.]turbytoy[.]com[.]ar	A	190[.]228[.]29[.]84

Las peticiones HTTP contienen un valor "id" basado en un UNIX time y un mensaje definido por el usuario "msg", por ejemplo:

```
GET /?id=1327014189930&msg=%C2%A1%C2%A1NO%20NOS%20GUSTA%20LA%20
```

Otros ejemplos:

```
msg=%C2%A1%C2%A1NO%20NOS%20GUSTA%20LA%20
msg=:)
msg=:D
msg=Somos%20Legion!!!
msg=Somos%20legi%C3%B3n!
msg=Stop%20S.O.P.A%20:)%20%E2%99%AB%E2%99%AB HTTP/1.1" 200 99406
"http://pastehtml.com/view/bl7qh5c.html"
msg=We%20Are%20Legion!
msg=gh
msg=open%20megaupload
msg=que%20sepan%20los%20nacidos%20y%20los%20que%20van%20a%20nacer
%20que%20nacimos%20para%20vencer%20y%20no%20para%20ser%20vencidos
msg=stop%20SOPA!!
msg=We%20are%20Anonymous.%20We%20are%20Legion.%20We%20do%20not%20
forgive.%20We%20do%20not%20forget.%20Expect%20us!
```

El campo "msg" puede ser definido arbitrariamente por el atacante.

Al 20 de enero de 2012, el US-CERT ha observado otro ataque que consiste en paquetes UDP en el puerto 25 y el 80. Los paquetes contienen un mensaje seguido de una variable entre relleno, por ejemplo:

```
66:6c:6f:6f:64:00:00:00:00:00:00:00:00:00:00 | flood.....
```

La selección del objetivo, el tiempo y otra actividad es comúnmente coordinada a través de sitios de social media o foros en línea.

El US-CERT aún está investigando y proveerá información adicional cuando se encuentre disponible.

2. **Solución**

Hay varias estrategias de mitigación disponibles para hacer frente a ataques de DDoS, dependiendo del tipo de ataque así como la infraestructura de la red del objetivo. En general, la mejor práctica de defensa para mitigar ataques DDoS involucra preparación avanzada.

- * Desarrollar un checklist o procedimiento estándar de operaciones (SOP) para seguir en caso de un ataque DDoS. Un punto crítico en un checklist o SOP es tener información de contacto con su ISP y proveedores de hosting. Identificar quién debería ser contactado durante un DDoS, qué procesos se deberían de seguir, qué información es necesaria y qué acciones serán tomadas durante el ataque en cada entidad.

- * El ISP o proveedor de hosting podría proveer servicios de mitigación de DDoS. Asegúrese de que su equipo esté al tanto de los provisiones en su acuerdo de servicio (SLA).

- * Mantener información de contacto para equipos de firewall, IDS, redes y asegúrese de que está actualizada y fácilmente accesible.

- * Identificar servicios críticos que deben ser mantenidos durante un ataque así como su prioridad. Los servicios deben ser priorizados de antemano para identificar que recursos deben ser apagados o bloqueados para limitar los efectos del ataque. También, asegurarse que sistemas críticos tienen suficiente capacidad para soportar ataques DDoS.

- * Tener los diagramas actuales de red, detalles de la infraestructura de TI e inventarios. Esto ayudará en determinar acciones y prioridades en el progreso del ataque.

- * Entender el ambiente actual y tener una guía del volumen de tráfico al día, su tipo y el rendimiento. Esto permitirá al staff a identificar de una mejor manera el tipo, punto y vector de ataque utilizado. También, identificar cualquier cuello de botella existente y acciones de remediación requeridas.

- * Asegurar las opciones de configuración de la red, sistemas operativos y aplicaciones mediante la deshabilitación de servicios y aplicaciones no requeridas por el sistema para mejorar el rendimiento de sus funciones.

- * Implementar un bloque boggon en el borde de la red.

- * Emplear servicios de detección en routers de borde en la medida de lo posible para poder disminuir

la carga en dispositivos de estado como los firewalls.

- * Separar o dividir en compartimentos a los servicios críticos:
 - ** Separar servicios públicos y privados
 - ** Separar intranets, extranets, y servicios de Internet.
 - ** Crear servidores de propósito específico para cada servicio como HTTP, FTP, DNS.
 - ** Revisar las recomendaciones de seguridad del US-CERT sobre los ataques de negación de servicio.

3. Referencias

- * Cyber Security Tip ST04-015

<<http://www.us-cert.gov/cas/tips/ST04-015.html>>

- * Anonymous's response to the seizure of MegaUpload according to CNN -

<http://money.cnn.com/2012/01/19/technology/megaupload_shutdown/index.htm>

- * The Internet Strikes Back #OpMegaupload -

<<http://anonops.blogspot.com/2012/01/internet-strikes-back-opmegaupload.html>>

- * Twitter Post from the author of the JavaScript based LOIC code -

<http://www.twitter.com/#!/mendes_rs>

- * Anonymous Operations tweets on Twitter -

<<http://twitter.com/#!/anonops>>

- * @Megaupload Tweets on Twitter -

<<http://twitter.com/#!/search?q=%2523Megaupload>>

- * LOIC DDoS Analysis and Detection -

<<http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html>>

- * Impact of Operation Payback according to CNN -

<http://money.cnn.com/2010/12/08/news/companies/mastercard_wiki/index.htm>

- * OperationPayback messages on YouTube -

<http://www.youtube.com/results?search_query=operationpayback>

- * The Bogon Reference - Team Cymru -

<<http://www.team-cymru.org/Services/Bogons/>>

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

UNAM-CERT

- Javier Santillán Arenas (jsantillan at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT

Equipo de Respuesta a Incidentes UNAM

Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx

phishing at seguridad.unam.mx

<http://www.cert.org.mx>

<http://www.seguridad.unam.mx>

<ftp://ftp.seguridad.unam.mx>

Tel: 56 22 81 69

Fax: 56 22 80 47