Boletín de Seguridad

5 de septiembre 2011

Estimados clientes,

Con motivo de clarificar y evitar cualquier pánico innecesario dentro de sus organizaciones SEFISA envía este boletín explicando el funcionamiento de la red Anonymous y que es lo que estos utilizan como medio para organizar sus ataques.

Anonymous:

Anonymous nace en canales de comunicación públicos, en chats IRC, empieza como un movimiento de protesta contra la iglesia de la Cienciología en 2008. A raíz de un video de Tom Cruise una serie de usuarios de salas de chats comienzan espontáneamente a organizar sus críticas. El foro 4chan.org de la noche a la mañana se convierte en un improvisado cuartel general. Alguien propone una protesta, muchos usuarios se adhieren y ya está organizado.

Tal como ellos lo proclaman, "Anonymous es una idea y las ideas no se pueden arrestar". Al parecer, la posibilidad de dar un espacio y voz a los miembros es lo que más atrae a sus miembros. Defender una causa, detrás de la estela que provee Internet, que muchos no quieren o no pueden por miedo a ser descubiertos, bloqueados y detenidos.

Que utilizan?

¿Qué es LOIC?

LOIC (Low Orbit Ion Cannon / Cañón de Iones de órbita baja) es una aplicación desarrollada por hackers afiliados al 4Chan, diseñada para ser usada en masa por miles de usuarios anónimos con el objetivo lanzar ataques coordinados de DDoS (ataque de denegación de servicio). Como por ejemplo, el ataque Visa.com o Mastercard.com.

Es una aplicación de “pulsa-el-botón”…

La idea detrás de LOIC es que cualquier persona pueda participar en ataques incluso si no tiene idea de como hacerlo. Simplemente se descarga una copia del programa LOIC (que tiene versiones disponibles para Windows, Mac y Linux), coloca la información del objetivo (bien la URL o la IP), y ya está.

LOIC básicamente convierte la red en una manguera que dispara una cantidad de información inservible, dirigida a un servidor web. Por si sólo, una computadora raramente genera suficientes peticiones TCP, UDP o HTTP

para sobrecargar un servidor: incluso si las genera, los servidores pueden ignorar las peticiones ilegítimas y procesar las correctas.

Sin embargo, cuando miles de usuarios ejecutan el LOIC a la vez, la ola de peticiones es inmanejable, ocasionando el cierre del servidor web (o sus servicios asociados, como los servidores de bases de datos), bloqueando así cualquier acceso.

Que es DDoS?

En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le denomina "denegación", pues hace que el servidor no dé abasto a la cantidad de solicitudes. Esta técnica es usada por los llamados Crackers para dejar fuera de servicio a servidores objetivo.

Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS (de las siglas en inglés Distributed Denial of Service) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

La forma más común de realizar un DDoS es a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz por su sencillez tecnológica.

Como detener un DDoS?

Las recomendaciones básicas son las siguientes:

- No habilitar todos los registros ya que esto causara un mayor estrés en sus aplicaciones.
- Utilizar sitios alternos de publicación para sus sitios.
- Tener redundancia en proveedores de Internet.
- Utilizar redundancia en DNS.
- Utilizar un servicio de protección contra DDoS en la nube.

Hace unas semanas un famoso proveedor de servicios de seguridad de la información desarrollo una herramienta basada en Cloud Services. Con esto el proveedor recibe todos los ataques sin que estos lleguen a afectar a sus sitios web. Eliminando la capacidad que tienen los ataques de DDoS de impedir el acceso a ciertos sitios.

Este método es extremadamente sencillo de implementar y no requiere de la instalación de software, cambio de código o instalación de equipo. Se hace cambiando los registros de DNS del sitio.

Lo que lo hace también una herramienta forense muy poderosa es que tiene la capacidad de dar reportes de los ataques y ver los focos que los generaron.

Les dejo los links a los documentos de la solución que protege de los ataques de DDoS.

http://www.imperva.com/docs/DS_Imperva_Cloud_DDoS_Protection_Service.pdf

http://www.imperva.com/docs/DS_Imperva_Cloud_WAF.pdf

Aquí esta un reporte de demostración de los ataques.

http://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed1.pdf