“Roadd, quiero ser anonymous. Enséñame a tirar servidores con DoS.”

Bienvenido, Manolo. Lamento decirte que aquí no estamos para temas **políticos activistas** pero de seguro vamos a ver de que trata el mundo del **DoS** en manera **teórica** (vimos la punta de la práctica en la bomba fork).

En resumen **DoS** son las siglas para **Denay of Service**, o en español: **Denegación de Servicio**. Es decir que vamos a dejar **inutilizable** algún **servicio** del **host** que hará de víctima así estemos hablando de su acceso a internet, o del sistema operativo entero. Parece un tema poco interesante y fácil pero verán lo **extenso** que se torna :).

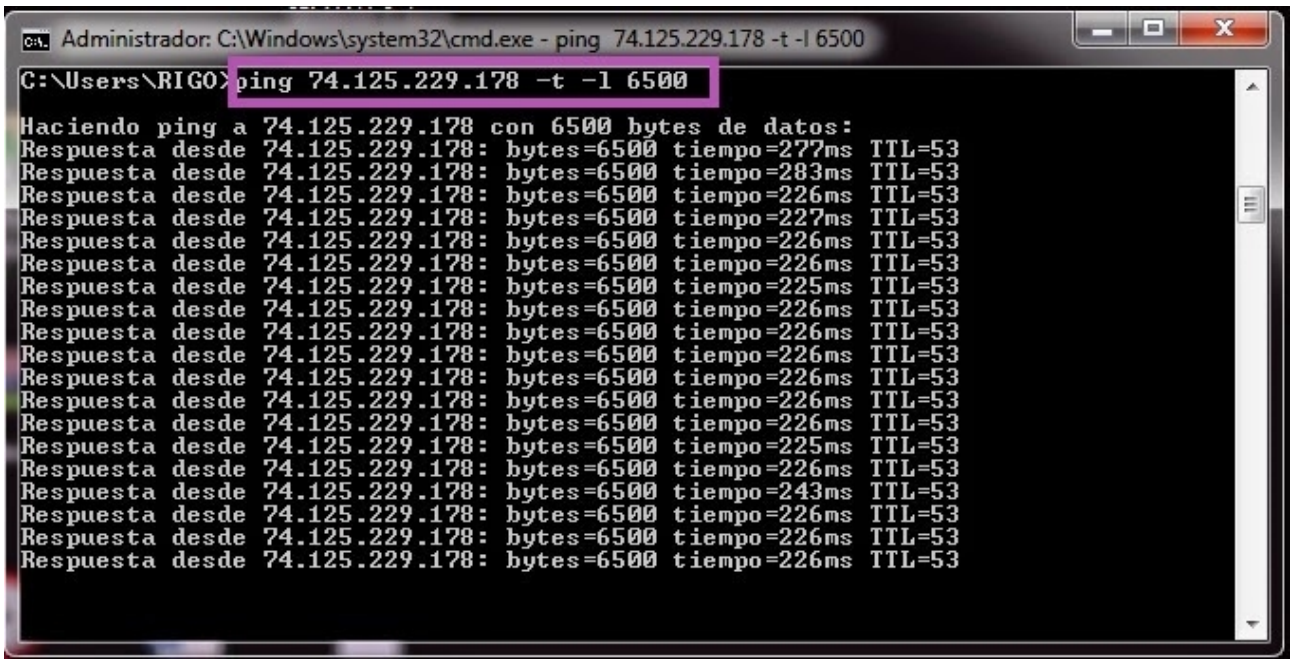
“Entonces no voy a ser un anonymous...”

No lo sé, lo único que conseguirás de este curso son **herramientas**, **conocimiento**. Nada de política. ¿Quieres el conocimiento?

“Vale. He oído sobre el ping de la muerte y la herramienta LOIC, pero no sé cómo funcionan.”

Genial. Importante que hayas escuchado de éso. El ***ping de la muerte*** se trata de mandar un sin límite de paquetes **ICMP** (el ping que usamos para saber si una computadora esta encendida y conectada a la red es un paquete ICMP) parecidos al **ping** pero **deformados**. Un sistema operativo de esa época -hablando de **1996**- no soportaba un paquete de tamaño mayor a unos **pocos Bytes**, y éste paquete malicioso tenía **64KB** o 65535 Bytes.

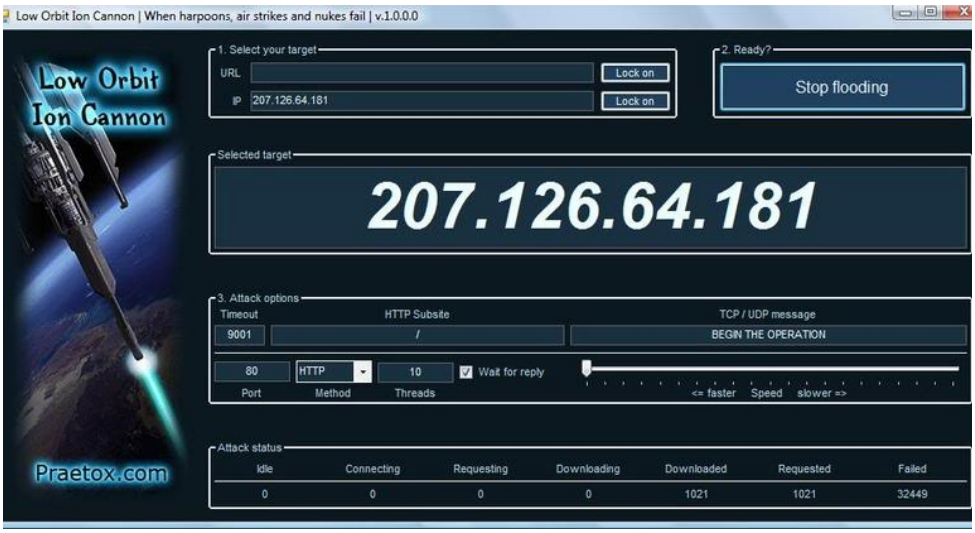
Todo genial hasta aquí, pero ¿por qué se satura? Bueno un paquete de este tamaño no es posible envíarlo de una vez. Como vimos, **los paquetes se fragmentan** y se envían con un número que indica el **órden**. Luego el **receptor** del mensaje **reconstruye** el paquete en memoria. Lo que en ese entonces significaba el acabose del sistema remoto. La **vulnerabilidad** fue **corregida** al año siguiente, pero hubieron trabajos posteriores. Al fin y al cabo es simplemente mandar un ping.



Ejemplo del comando envíado con 6500 bytes.

LOIC -Low Orbit Ion Cannon- es una **herramienta** que manda paquetes **TCP**, **UDP** o peticiones **HTTP** para realizar un **DoS** en el objetivo. Un desarrollador hizo un cambio a esta herramienta y permitía que alguien pudiese aceptar unirse a una **botnet** (red zombie de computadoras) **voluntariamente para ceder recursos y atacar organizadamente a un objetivo.**

Adivina quién usó ésta herramienta. Claro, **Anonymous**. Lo bueno de que hayan usado LOIC es que sólo podían hacer que una web caiga con la aceptación de una cantidad mínima de personas. Es decir que es de apoyo comunitario y no por puro capricho de una sola persona ya que una sola no iba a dar una cantidad de recursos óptima para el ataque, convirtiendose en una ***sentada virtual*** en la puerta de acceso para que nadie pueda entrar, una **protesta pacífica** (aunque obviamente las empresas no lo vean así).



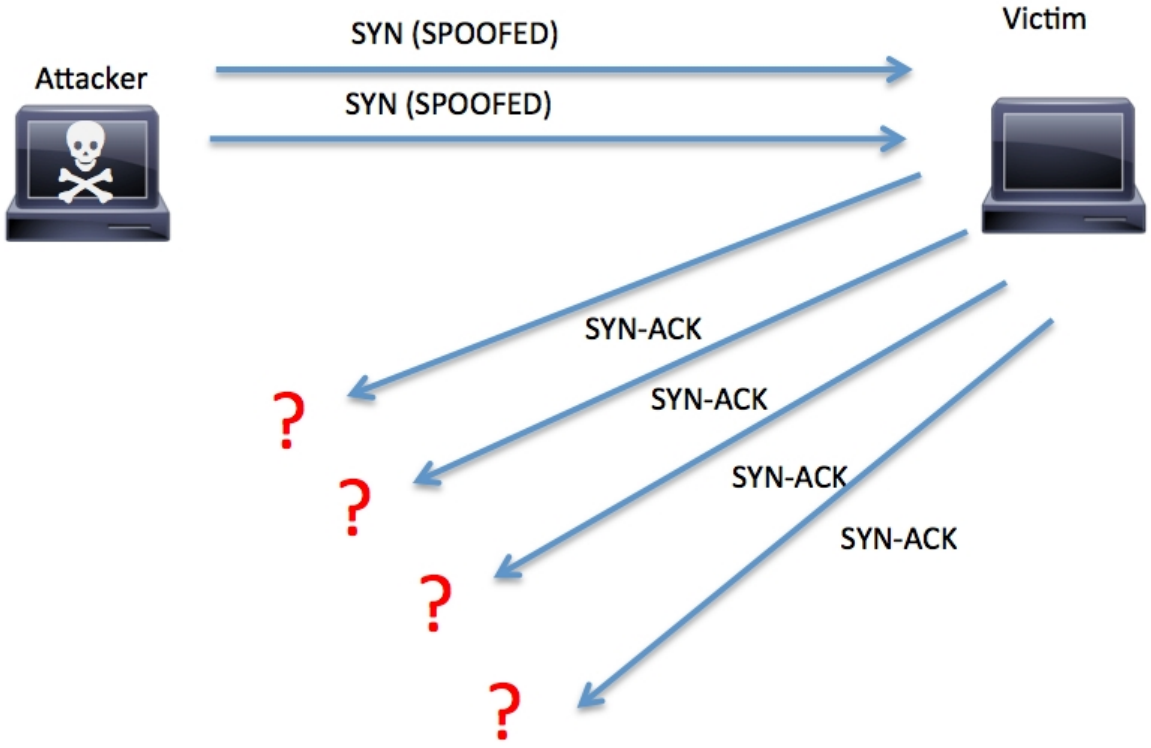
Pantallazo de LOIC

Pero hay muchos tipos de ataques, veamos como hacer un desastre para los administradores:

- **Ping flood:** A diferencia del ping de la muerte, éste no es un paquete malformado (se pueden usar paquetes malformados también). En el escenario de un ping normal, se envía una vez el request y se espera la respuesta del otro dispositivo. Aquí, se envían

deliveradamente todos los paquetes **sin esperar respuesta** alguna. El host víctima tiene que resolver peticiones sin parar y encima su **ancho de banda** se consumirá entre todos los **paquetes entrantes** y las **respuestas salientes**.

- **SYN flood:** Este ataque realiza la **petición TCP** para abrir la comunicación numerosas veces (recordar la clase 18), mandando paquetees **SYN**. El servidor responde con un **SYN+ACK** esperando que el atacante le envíe un paquete diciendo si acepta la comunicación o la rechaza. Pero el atacante **cambia de IP** rápidamente para envíar otro paquete SYN esperando abrir otra conexión. Obviamente el servidor acepta muchas conexiones simultáneas, y mientras responde esta segunda petición desde otra dirección, la otra comunicación sigue esperando respuesta (hasta que caiga porque tienen un tiempo límite para responder). Es decir que quedan varias **comunicaciones abiertas** por la **mitad** hasta que el sistema no puede resolver tantas peticiones, se satura y los usuarios (legítimos o no) son denegados de conexión por el sistema.

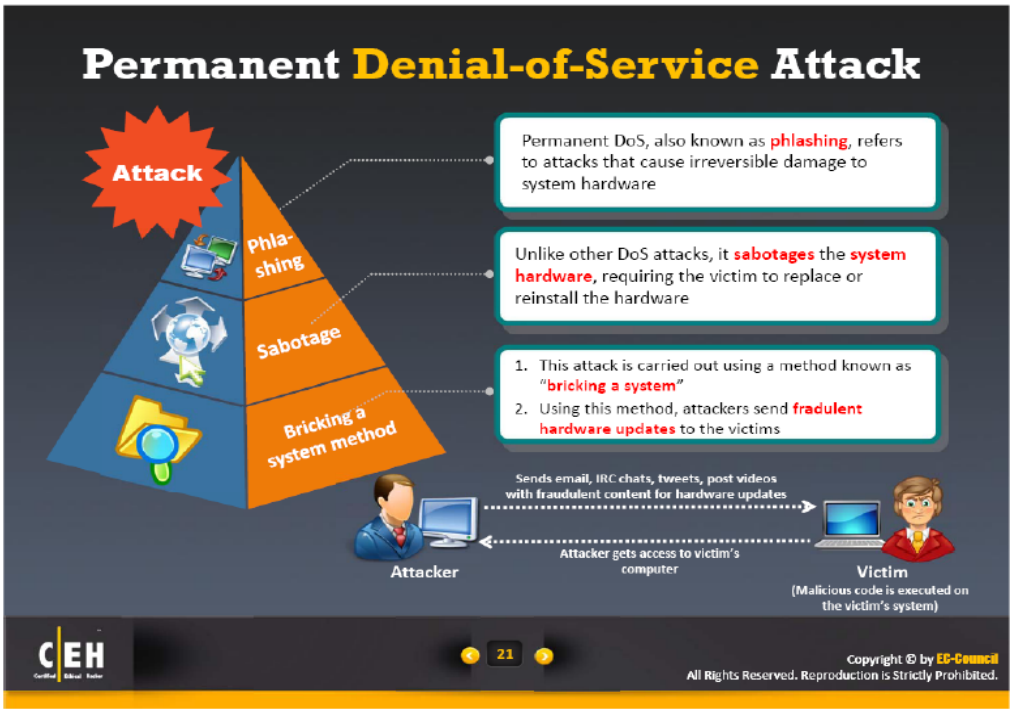


Gráfica de un ataque de inundación de SYN.

- **Smurf Attack:** básicamente es otro ataque utilizando el protocolo **ICMP**, pero esta vez se usa dentro de una **red interna**, haciendo una petición por **broadcast** (ver clase 15) y **falsificando** la **IP** de origen de estos paquetes **duplicando** la del objetivo. Así la víctima y, sobretodo, la **red** se inundan con respuestas de los todos los hosts.

- **P2P Attack:** Lo que se logra aquí es aprovechar una **vulnerabilidad** en **clientes P2P**, que son programas para el intercambio de archivos como Kazaa, Emule, Ares. Se desconectan a los grandes clientes de este tipo de conexiones para que se conecten juntos a una web específica objetivo, llegando a las **varias decenas de miles** y saturando los servidores. Se puede prevenir haciendo que este protocolo (P2P) no pueda usar el puerto 80 (donde generalmente se accede al servicio de la página web).

- **DoS permanentes (PDoS):** También conocido como **phlashing**, es uno de los más interesantes. Ataca directo al **hardware**, aprovechando **vulnerabilidades** para cambiar **firmewares** y haciendo del dispositivo físico inusable, se "***brickea***" (jerga apuntando a que se convierte en un ladrillo). Para resolver el problema, se debe cambiar el hardware o reparar el firmware que no es nada divertido para un administrador.

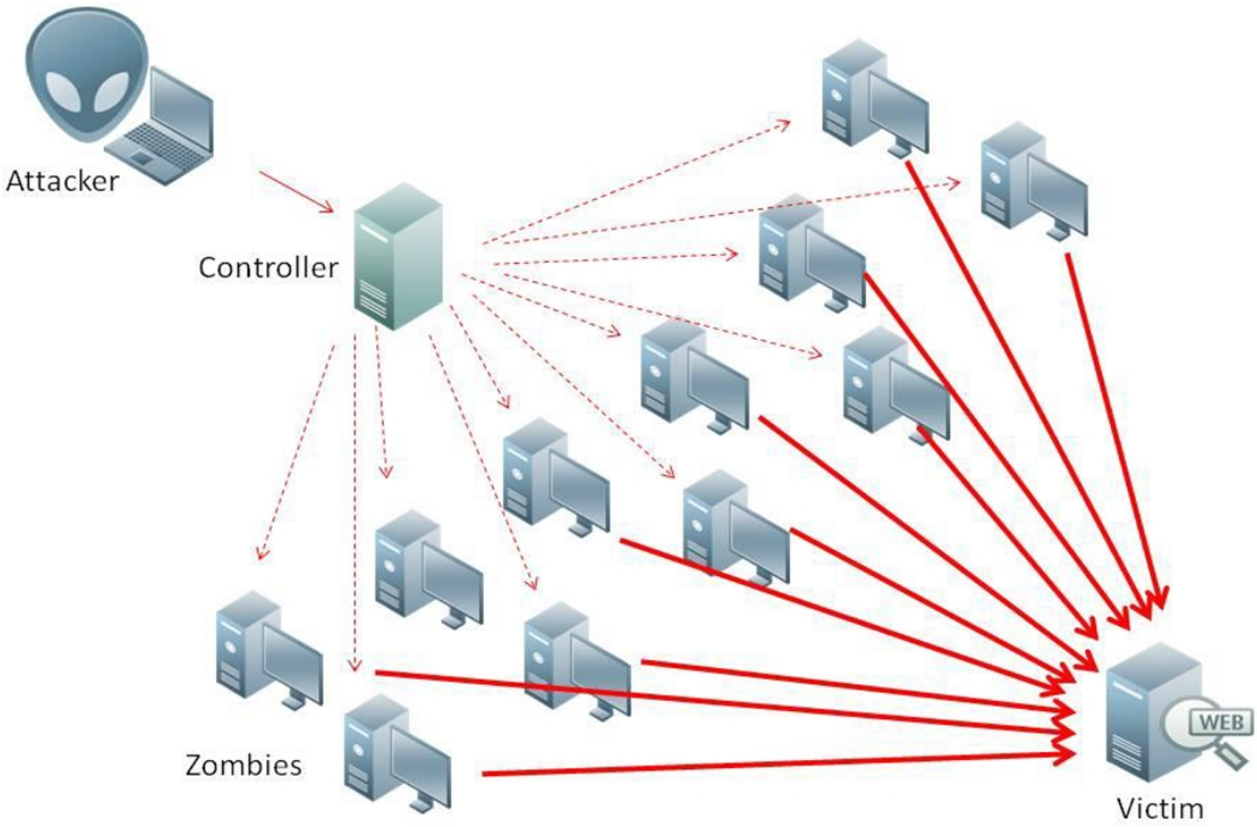


No es de vago, no recorto la imagen para que vean de dónde viene. xD

- **HTTP POST DoS attack:** en síntesis es un pedido legítimo al servidor a través de la web, donde se especifica que la **velocidad de transferencia** es muy **baja** y el **tamaño** es de **inmensas** cantidades. Imaginen el tiempo de transferencia de 1GB a 1Byte por segundo, es interminable (34 años aproximadamente). Obviamente para tirar un servidor la idea es hacer muchos ataques simultáneos.

- **RUDY:** (R U Death Yet?) es idéntico al anterior pero con la diferencia que sucede en **capa 7**, a nivel **aplicación** de la web.

- **Distributed attack:** Aunque en realidad merecería tener un apartado propio, así se le llama al **DDos**. La idea es aventajar la cantidad de **recursos** utilizados por muchas máquinas simultáneamente a comparación de usar una sola. Además es más complicado de bloquear ataques a muchas IP distintas, haciendo **casi imposible** lograr una **Black List** de direcciones **bloqueadas**. En los últimos años este tipo de ataques gano popularidad cuando se usó para temas **activistas** de parte de varios grupos cibernéticos quienes lograron dar de baja webs de empresas muy prestigiosas a nivel social.

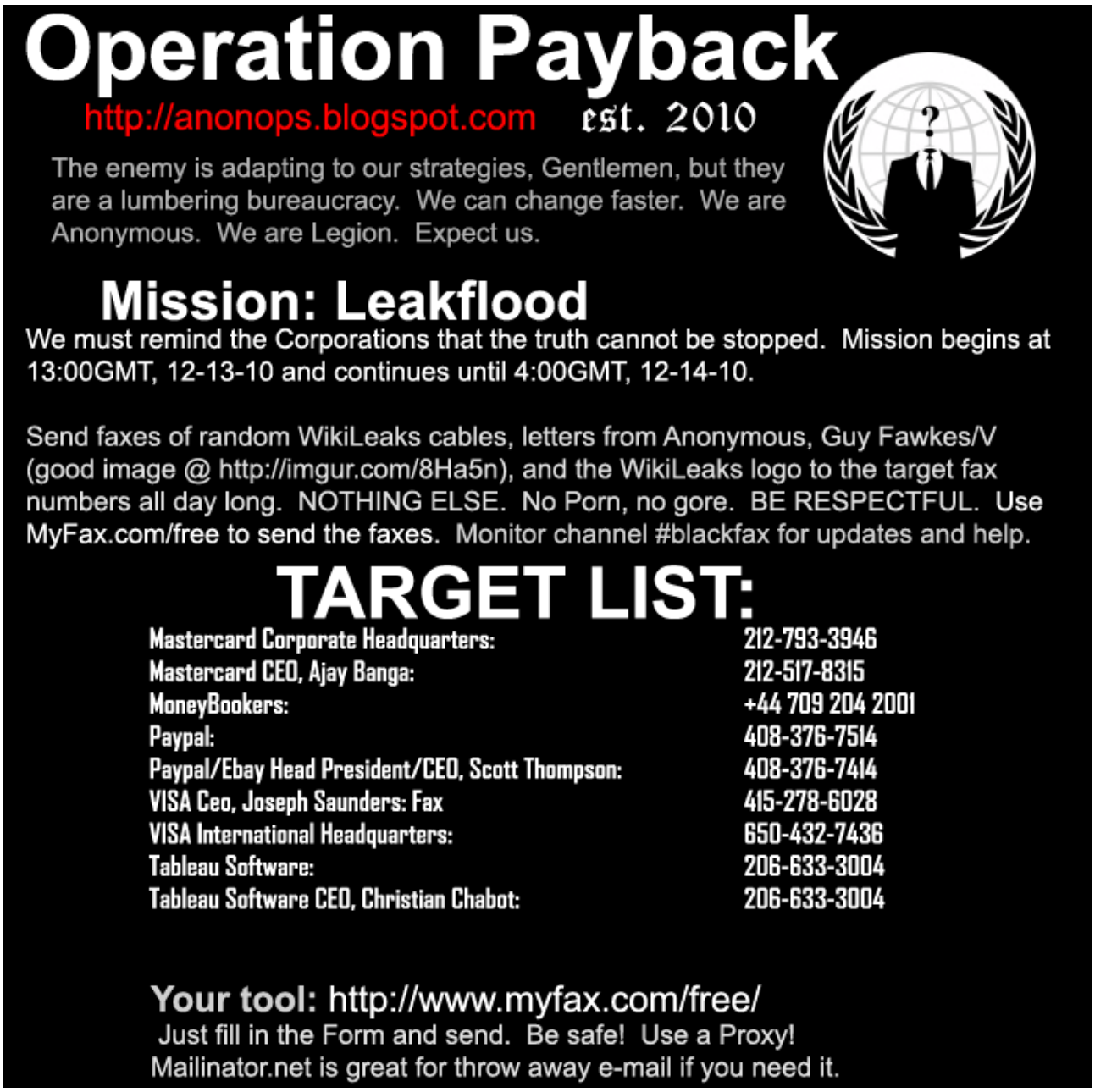


En esta imagen hace referencia a un controlador de una botnet.

- **Reflected/Spoofed attack:** De una manera parecida al Smurfing -que se considera un tipo de este ataque- pero de manera más generalizada, se intenta crear peticiones a distintos servers pero sustituyendo la IP a responder por la del equipo víctima, por lo que mientras un atacante hace peticiones, la víctima es quien recibe todas las respuestas de intento de conexión. Aunque a diferencia de Smurfing, este nombre es usado para conexiones UDP, que necesitan menos autenticaciones y problemas para mandar datos.

- **Jamming:** abstrayéndonos un poco del estándar que venimos hablando sobre computadoras, el Jamming hace una denegación de servicio contra las **redes inalámbricas** logrando que un dispositivo haga continuamente **señales de interferencia**. He visto casos donde se logra un Jamming si existen muchas (realmente excesivas cantidades) de **Access Points** en el mismo **canal de transferencia** en corta distancia.

- **Telephony DoS (TDoS):** No necesita mucha presentación porque no estamos profundizando y el nombre lo dice todo. Me es necesario aclarar que aquí se puede lograr una denegación aunque el equipo no sea un teléfono IP, aunque éstos son los que más ataques llevan. También se usa el **SMS flooding** (se darán una idea de lo que es) y **Black Fax** en el que básicamente se envían varias hojas rellenas de color negro matando al tintero.



Fíjense como se utiliza TDoS con fines políticos.

Los ataque de denegación de servicio **no** son algo **legal**. Incluso ejecutar una bomba fork que deje inutilizado el sistema de alguien más sin su consentimiento, nos dejaría en problemas en la mayoría de los países de América. En el año **2012**, dos miembros del grupo de **Anonymous** de America Latina fueron **encarcelados** por realizar este tipo de ataques a varios entes. Aquí la **Interpol** es uno de los organizadores más grandes contra el **ciberdelito** y ya verán que pueden traer problemas. Así que ustedes no hagan nada ~~si aún no saben como safarse.~~ :)

Les dejo el **link** del **LOIC** para descargar por si quieren jugar un rato: http://sourceforge.net/projects/loic/?source=typ_redirect **no ataquen sin permiso de la víctima**.

Pueden seguirme en Twitter: @RoaddHDC

Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente:

1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
