¿Leer? o ¿Leer y Escribir? Dos Nociones sobre el Hacking.

Extracto

Podríamos decir que un sistema organizacional es un conjunto funcional que resuelve una serie de problemas, mediante decisiones lógicas a lo largo de un proceso que va ejerciendo control de una dinámica interna, cerrándose después en el análisis continuo de sus múltiples posibilidades, el cierre de sus posibilidades y la predicción de estos procesos internos; es el primer síntoma que empujará a la modificación funcional del sistema organizacional originario. Si esta modificación no es realizada desde el interior, lo que comúnmente pasa, se ejercerá presión desde el exterior del territorio, demarcado por el sistema, chocando de forma continua e impredecible sobre él hasta penetrarlo; modificando sus límites, densidad y trayectoria. Una vez que esta operación ha sido realizada, la deriva aparece, y un sistema desmembrado tanto en su nivel organizacional como en su nivel informacional, se desplaza golpeándose interna y externamente. Avanzando y retrocediendo, sin una dirección determinada, fijando ruidos que lo desestabilizarán. Para prevenir el colapso, o una entropía, se despliegan al interior del sistema organizacional una serie estrategias, para redireccionar o disminuir al intruso hasta lograr neutralizarlo. Pero algunas veces, existe la posibilidad de que el sistema que contiene al intruso no lo detecte, o se retracte de realizar estrategias para anularlo, y en vez de eso, lo asimile y, paradójicamente, tras esa acción, se pueda crear un otro paralelo, que sea tan o más complejo que el originario. Este texto pretende analizar y dar un ejemplo de las posibilidades anteriormente descritas, es decir, las que modifican un sistema organizacional para desestabilizarlo, o los que lo intervienen para crear otro, pero no desde un punto de vista biológico, sino que a partir de las posibilidades que nos dan los protocolos que configuran las redes y computadoras en el espacio informacional.

1

En la primavera del hemisferio sur del año 2006, la noticia se expandió en los medios chilenos: un colectivo organizado para irrumpir mediante diferentes técnicas y herramientas, autodenominado Byond Crew, conformado por c0diux ; phnx ; SSH-2 ; NETTOXIC, fue puesto a disposición de los tribunales chilenos luego de haber atacado cientos de sitios de Internet(1) en EEUU, Israel, Chile, Colombia, Venezuela, Argentina, Bolivia, Perú y Turquía. Entre ellos, el de la NASA. La intervención consistió en un ataque a gran escala, mediante la inyección de código SQL, que les permitió alterar la imagen corporativa por mensajes en contra de la guerra, generalmente correspondiente al rostro de un niño herido y un texto que decía: “No más Guerra: Esta es una Cyber Protesta”(2), refiriéndose explícitamente a la guerra Israelí-Libanesa que en ese momento había estallado. Este tipo de intromisión política, en un espacio privado pero de acceso público, se podría asociar a una serie de acciones realizadas por grupos de activistas, que se caracterizan por desactivar el carácter semántico de un símbolo para cuestionarlo o subvertir su significado(3). Un ejemplo reciente, son las poleras (remeras) que circulan actualmente por la ciudad de Santiago de Chile, que tienen impresa la palabra *Cuma* en vez de Puma. Cuma, es una palabra proveniente del Coa (jerga de los delincuentes chilenos), que denota a una persona que posee escaso o nulo grado normalizado de educación, lo cual lo demuestra comportándose de forma “grosera” e “inhóspita” con los que “sí la poseen”.

Pero, que diferencias entre estos dos tipos de acciones (sin considerar del formato que se esta usando en la accion) existan entre ambas intromisiones que subvierten los signos?¿Qué punto en común los une, además del fin político que persiguen?

La primera pregunta arrojaría como respuesta; el período económico donde estas herramientas y las técnicas fueron pensadas y producidas, y esto sirve para responder la segunda pregunta; ambas acciones necesitan de una estrategia económica para que la acción sea realizada. En este sentido, la segunda acción descrita (las poleras con la palabra impresa Cuma) está basada en una economía de la fabricación y la industria, y la primera realizada por Byond Crew, está basada en la economía del conocimiento y la información. Esto es sumamente importante de mencionar, ya que el activismo, y sobre todo el activismo latinoamericano, por lo general desecha la idea de ocupar las herramientas y las técnicas provenientes de la economía de la información y el conocimiento para realizar sus acciones, desaprovechando o ignorando los alcances que puedan tener(4) al interior del modelo económico reinante, que querámoslo o no, directa o indirectamente, todos tenemos un grado de compromiso con él(5). Volviendo atrás y profundizando la primera respuesta que eh dado, si consideramos la técnica como uno o varios procedimientos para lograr un resultado(6), y la herramienta un dispositivo artificial cuya función es facilitar la aplicación de energía a una pieza o material durante la realización de una tarea(7), nos daremos cuenta que la técnica que permite dibujar la palabra en el bastidor de serigrafía proviene de una economía basada en la industria, y la técnica ocupada en vincular la imagen desde otro sitio proviene de una economía basada en la información y el conocimiento. A su vez, las herramientas que permiten imprimir la palabra en la polera son pertenecientes a las era industrial, y la herramienta que provoca la inyección de datos pertenece a la era digital, período donde han surgido nuevas formas de relacionarse con el mundo que nos rodea y donde han surgido términos como: base de datos, redes distributivas, o virus informáticos, que no tienen nada que ver con la noción de la era digital instalada por la publicidad, donde un computador es sólo un símbolo de status y de la eterna juventud.

Pero vayamos por parte: ¿cómo opera la técnica que vincula una imagen que no está en la carpeta del código HTML que la contiene? Muy simple, poniendo la dirección donde la imagen está guardada. Por ejemplo, si la imagen estuviese almacenada en el siguiente directorio:

```
http://www.elmercurio.com/guerra/libano-israel/imagen-niño.jpg
```

El código HTML de la página intervenida quedaría escrito de la siguiente manera:

```
<body>
<p>No mas Guerra: Esta es una Cyber Protesta ! </p>
<p><img src="http://www.elmercurio.com/guerra/libano-israel/imagen-
niño.jpg"
width="130" height="200" /></p>
</body>
```

Ahora, con respecto a lo que la inyección de datos se refiere esta vendría siendo un proceso generalmente realizado por una herramienta automatizada donde el atacante logra entrar a la base de datos SQL, y le agrega parámetros no deseados que le permitirán acceder a datos a los que de otro modo no tendría acceso.

Lo primero que hace el atacante es escanear el sitio, con herramientas como SPI Dynamics WebInspect o Wikto, para detectar si existe una entrada por donde inyectar los datos, y luego realizar el proceso de inyección del código SQL con otro tipo de herramienta, como podría ser SPI Dynamics' SQL Inyector, Pero también existen procedimientos manuales donde el atacante puede ocupar diferentes técnicas. Por ejemplo, si una persona accede a una página donde haya una tabla con dos campos, y donde dos campos te permitan acceder mediante una clave y un nombre a un sitio, se puede inyectar sentencias SQL en los campos que servirán para pedir registros o

cambiar sentencias:

```
Login: hi' or 1=1--
Pass: hi' or 1=1—

'; exec master..xp_cmdshell 'ping 10.10.1.2'--
```

2

Como vimos, el primer ejemplo descrito pertenece a la categoría donde hackear es visto como sinónimo de desestabilizar intermitentemente o parcialmente un dominio, irrumpir en un sistema para desestablizarlo. El ejemplo que viene a continuación, posee otra noción de hackear, que se diferenciará de la primera descrita, ya que no se realizará de forma anónima; cumplirá una función práctica y no necesitará del lector clásico que entiende que leer es sólo un ejercicio cognitivo receptivo, sino que necesitará de un lector que entienda que la interpretación del significado dependerá de sus propias acciones, transformando al lector en un agente activo en vez de uno pasivo que se remite solamente a realizar la lectura desde fuera para poder completar la interpretación. Al contrario, el hack que describiré a continuación, el lector debe completar un proceso que le permitirá interpretar el significado, pero dicha interpretación, como veremos mas adelante no es el fin del hack.

Hace un par de años atrás, Mirko Petrovich hizo una modificación al código fuente de Pure Data, software de licencia libre similar a Max/MSP, que sirve para sintetizar y procesar señales de audio o video en tiempo real y construir aplicaciones interactivas. La intervención consistió en re-escribir el código fuente del programa con el fin práctico de poder pre-visualizar la amplitud de una señal en un sonograma(8) construido por él que media originalmente el tiempo y la frecuencia del sonido en Pure Data. Para hacer esto Mirko Petrovich transformo la paleta colores RGB que venia con Pure Data en una paleta de escala de grises, cambiando el siguiente codigo fuente del programa:

Codigo Original del Pure Data:

```
static int rangecolor( int n) /* 0 to 9 in 5 steps */
{
      int n2 = n/2;
      int ret = (n2 << 6);
      if (ret > 255) = 255
      return (ret);
}

static void numbercolor(int n, char *s)
{

      int red, blue, green;
      if (n < 0) n =0;
      red = n / 100;
      blue = ((n / 10) % 10);
      green = n % 10;
      sprintf(s, "#%2.2x%2.2x%2.2x", rangecolor(red), rangecolor(blue),
      rangecolor(green));
```

Codigo de Pure Data Hackeado

```
static int rangecolor( int n) /* 0 to 9 in 5 steps */
{
	int n2 = n/2;
	int ret = n2;
	if (ret > 255) = 255
	return (ret);
}

static viod numbercolor(int n, char *s)
{
	int red, blue, green;
	if (n < 0) n =0;
	red = n;
	blue = n;
	green = n;
	sprintf(s, "#%2.2x%2.2x%2.2x",rangecolor(red), rangecolor(blue),
		rangecolor(green));
```

El resultado final funciona tanto en su nivel auditivo como en su nivel visual, creando una nueva forma de visualización de datos, y porque de no decirlo, dando la posibilidad de cambia una herramienta para medir la frecuencia y el tiempo a una mas compleja, transformando el sonograma en una herramienta de composición, dando al lector de esta intervención, la posibilidad de realizar micro piezas sonoras.

Conclusión

Hemos visto dos posiciones frente al hack, que se diferencian entre sí. Con los datos expuestos anteriormente se podría realizar la siguiente tabla:

Autor	Intervencion	Propósito / Dominio	Tipo de Lector
Byond Crew	Sitios de organizaciones y compañías, mediante inyección de datos SQL	Guerrilla Semiótica Dominio Público	Receptivo / Pasivo
Mirko Petrovich	Pure Data mediante la re escritura de del código fuente del programa	Visualización de Datos Dominio Cultural	Productivo / Activo

Notas::

(1) http://www.zoneh.
org/component/option,com_attacks/Itemid,43/filter_defacer,byond%20hackers%20team/
(revisada el 5 de Abril 2007)

(2) http://www.zone-h.org/index2.php?option=com_mirrorwrp&Itemid=43&id=4402742
(revisada el 5 de Abril 2007)

(3) Este tipo de acciones son ampliamente tratadas en la revista canadiense Adbuster. Véase también la contra portada de la revista 2600, o el diario chileno The Clinic.

(4) Como contrapunto a esta mirada, se pueden revisar los vídeos producidos por la resistencia iraquí y subidos a Live Leak, donde francotiradores, mediante la técnica de cámara subjetiva, muestran cómo son eliminados soldados estadounidenses en Irak.
http://www.liveleak.com/browse?tag=sniper (revisada el 5 de Abril 2007)

(5) Léase. Nieto, Ignacio, Local: 0, Global: 1. Entrevista con Igor Stromajer (revisada el 7 de Abril 2007) http://newmediafix.net/daily/?p=820

(6) http://es.wikipedia.org/wiki/Herramientas (revisada el 5 de Abril 2007)

(7) http://es.wikipedia.org/wiki/T%C3%A9cnica (revisada el 5 de Abril 2007)

(8) Un Sonograma o Espectrograma, es una herramienta para calcular la frecuencia de una señal, en este caso una señal de audio. Al momento de importar la señal al sonograma esta queda fijada estableciendo la frecuencia y el tiempo que posee la señal; la cual se puede oír posteriormente. http://en.wikipedia.org/wiki/Spectrogram (revisada el 5 de Abril 2007)

Referencias:

- Woznicki, Kryztian. Retoric of Loss of Control. Páginas 41- 46. Camara Austria Nº 77, Graz Austria 2002

- Philippe Bootz. Die/Der Lesser. p0es1s. Ästhethik digitaler Poesie. Frederich W Bloch, Christiane Heibach y Karin Wenz editores. Hatje Cantz. Stuttgart, Alemania 2004

- Roads, Curtis. The Computer Music Tutorial. Cambridge EEUU.1996.

- Wark, McKenzie. A Hacker Manifesto. Harvard University Press. Cambridge EEUU. 2004

- SQL Injection Walkthroug. http://www.securiteam.com/securityreviews/5DP0N1P76E.html. Review March 23, 2008