Análisis forense en MSN Messenger

Cuenca Sarzuri Rudy
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
rudymoon111@hotmail.com

RESUMEN

Hoy en día muchos tenemos miedo a que se nos dañe nuestro correo electrónico o que nos quiten el pasword de nuestra cuenta , lo cual conoceríamos como el secuestro de email. El presente trabajo elaborado describe alguna de las maneras en que se pueden usurpar el correo, también veremos que herramienta forense se debe utilizar para verificar si es que se presenta un secuestro de cuentas de MSN, en especial.

Palabras Clave

MSN, SPAM, Multitraking, HOAX, POP3,

1. INTRODUCCIÓN

Hoy en día quien no tiene un correo electrónico, para poder entregar y recibir información. Cualquiera diría en una empresa el MSN es innecesario, pero no, en una empresa donde los empleados tienen su propia cuenta de correo electrónico podemos mencionar que mediante Chat, el jefe de la empresa puede llamar a todos los empleados a una reunión no estando en el mismo edificio, también se hace uso del chat para la entrega de documentos, por la transferencia de datos más directa, facilitando la entrega de la información electrónica hacia otras oficinas.

En cuanto a errores, hay momentos en el cual el Messenger tiene errores no solo por el tráfico de cuentas sino también por el daño que sufren los archivos del MSN por algún virus, o gusano que dañan los archivos de ejecución, para ello también hay herramientas de corrección, de los cuales el MSN E-Fix 2.0.exe es el más utilizado para la restauración, la cual posee una variedad de tipo de errores, para dar la respectiva reparación.

2. SEGURIDAD EN CORREOS ELECTRÓNICOS

HOAXES, los cuales son mensajes que da una noticia de alarma como de un virus filtrado en el MSN o noticia que requiera de su apoyo, etc. Generalmente son enviados a personas que, una vez que reciben el mensaje ellos envían a todos sus contactos.

Un buen artículo introductorio sobre las técnicas filtrado de SPAM es “. Normalmente, realizado por un robot, que recoge direcciones de una base de datos o recogidas de analizar las existentes en un hoax previamente lanzado, también es posible. Microsoft publicó un truco para añadir simultáneamente a varios remitentes en la lista de no deseados en . () es un puerto para Windows del SpamAssasing, un proxy local (127.0.0.1) de POP3 que filtra los mensajes y los marca como SPAM. utiliza filtros bayesianos para autoaprender del SPAM anterior. Se integra perfectamente con el cliente de correo Bloomba ().

3. MAILTRACKING

es un sistema de seguimiento de emails mediante la confirmación manual de recepción del destinatario. es una utilidad para extraer ficheros de un archivo Winmail.dat de Outlook. permite extraer varios ficheros multipartes de emails en crudo en formato codificado MIME-Base64, etc. Respecto al MSN Messenger, el protocolo utilizado está ampliamente documentado en la web del ; además de ser utilizado también por una versión de software libre, .

4. ANALISIS EN MESSENGER

4.1. MSN Shadow

Es una herramienta de análisis forense orientada a MSN Messenger (recientemente rebautizado como Windows Live Messenger), ya que puede realizar operaciones específicas de análisis basadas en el Microsoft Notification Protocol, el protocolo de mensajería instantánea desarrollado por Redmond del que se abastece el popular Messenger.

MSN Shadow permite capturar el tráfico de texto y de vídeo de las sesiones Messenger, pudiendo exportarlas a HTML y AVI respectivamente. Adicionamente, permite la realización de pruebas de concepto relacionadas con el spoofing de autoría de mensajes (reenviando los números ACK de las conversaciones mediante paquetes reset RST) y el secuestro de sesiones (igual que el método anterior, pero creando dos reglas específicas iptables para gestionar los paquetes, lo que hará que se abra una nueva ventana para continuar la conversación como si fuéramos la persona cuya sesión ha sido secuestrada)

Este software está pensado para analizar el tráfico de Messenger y para poder verificar si es factible la suplantación y el secuestro de sesiones, lo que podría tener utilidad como prueba pericial en un caso donde se presenten evidencias en la forma de logs de mensajería instantánea. Bajo ningún concepto se entiende que esté orientado a

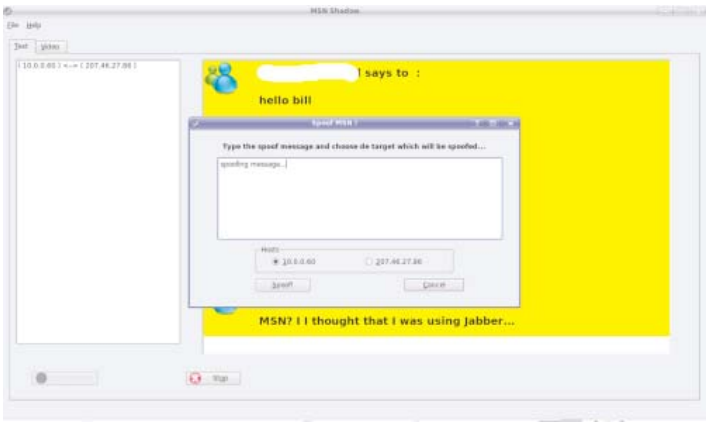

Figura 1. La interfaz de MSN Shadow

espiar/perjudicar/engañar/molestar a nadie

Para instalar MSN Shadow debe ejecutarse el tradicional ./configure & make & make install. Lamentablemente para los usuarios de Windows, no existe un binario ejecutable para esta plataforma en la actualidad.

5. ¿QUE ES EL ACK ?

ACKNOWLEDGEMENT (ACK) (en español acuse de recibo), en comunicaciones entre computadores, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado. Si la terminal de destino tiene capacidad para detectar errores, el significado de ACK es "ha llegado y además ha llegado correctamente".

Hay tipos más complejos de ACK cuyo significado podría traducirse como "reenvíame la trama 2" o "he recibido tu último mensaje, pero no puedo recibir más hasta que termine de procesar los anteriores".

La forma exacta del mensaje, es decir, la combinación de unos y ceros que lo caracterizan y su posición dentro de una trama, varía según el protocolo utilizado.

Según el protocolo que se utilice, puede existir una contrapartida de este mensaje denominada (Negative ACKnoledgement, o asentimiento negativo), que se suele enviar cuando se ha detectado un error en la trama recibida o cuando se ha perdido una trama.

La pérdida de una trama se detecta por su numeración en protocolos basados en (esto es, hay un error si la última trama recibida fue la número 3 y la recibida actualmente es la 6).

También pueden detectarse pérdidas por parte de la terminal emisor: si se envía una trama o grupo de tramas y el asentimiento no llega en un tiempo determinado, se asume que hay que volver a enviar los datos. Este tiempo se calcula en función de la velocidad de transmisión de las terminales y el tiempo que tarda una trama en viajar del origen al destino, de forma que no sea ni demasiado corto ni demasiado largo.

6. QUE ES UN SPOOFING?

Por spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque - al menos la idea - es muy sencilla: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Y como los anillos de confianza basados en estas características tan fácilmente falsificables son aún demasiado abundantes (no tenemos más que pensar en los comandos r-, los accesos NFS, o la protección de servicios de red mediante TCP Wrapper), el spoofing sigue siendo en la actualidad un ataque no trivial, pero factible contra cualquier tipo de organización. Como hemos visto, en el spoofing entran en juego tres máquinas: un atacante, un atacado, y un sistema suplantado que tiene cierta relación con el atacado; para que el pirata pueda conseguir su objetivo necesita por un lado establecer una comunicación falseada con su objetivo, y por otro evitar que el equipo suplantado interfiera en el ataque. Probablemente esto último no le sea muy difícil de conseguir, a pesar de que existen múltiples formas de dejar fuera de juego al sistema suplantado –al menos a los ojos del atacado– que no son triviales (modificar rutas de red, ubicar un filtrado de paquetes entre ambos sistemas...), lo más fácil en la mayoría de ocasiones es simplemente lanzar una negación de servicio contra el sistema en cuestión. Aunque más adelante, hablaremos con más detalle de estos ataques, no suele ser difícil de tumbar, o al menos bloquear parcialmente, un sistema medio; si a pesar de todo el atacante no lo consigue, simplemente puede esperar a que desconecten de la red a la máquina a la que desea suplantar (por ejemplo, por cuestiones de puro mantenimiento).

7. SOFTWARE IM HISTORY

IM History es una excelente aplicación que permite guardar las de diferentes clientes de mensajería instantánea en una

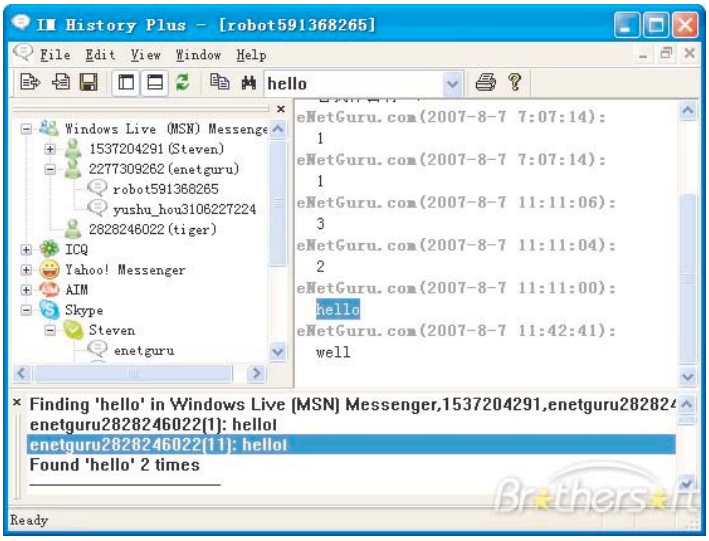

Figura 1. La interfaz de MSN Shadow

Tabla 1. La interfaz de MSN Shadow

	R	S	T
1	ilegible	apenas perceptible	nota muy ronca o chirriante
2	apenas legible	muy débil	nota CA muy grave, sin musicalidad
3	legible con dificultad	débil	nota CA grave, ligeramente musical
4	legible	aceptable	nota CA moderadamente musical
5	perfectamente legible	regularmente buena	señal musicalmente modulada
6		buena	nota modulada algo silbante
7		moderadamente fuerte	nota de CC con algo de zumbido
8		fuerte	con residuos de zumbido
9		extremadamente fuerte	nota de CC ideal y pura

sola aplicación de forma que todo nuestro log de charlas queden en un solo lugar.

Para utilizar el IM History solo tenemos que , descargar e instalar el programa, este detectara automáticamente los clientes de mensajería instantánea que tengas instalado y los configurara.

El IM History no se limita a guardar nuestras conversaciones en texto plano sino que además guarda imágenes, fotos además de guardar el texto con su tipo de fuente y color.

Los clientes de mensajería instantánea soportados de momento son: MSN , Yahoo! Messenger, ICQ, Trillian, Miranda, AIM, Skype, y pronto agregaran soporte para Gtalk, Kopete e iChat.

8. ¿QUE ES RST?

RST o código RST es un usado para describir la calidad de las transmisiones de, especialmente en escritos por el messenger. Cada letra del código representa un factor específico de la señal, y cada factor tiene diferentes escalas.

Explicación del código de tabla 1, donde:

R representa la CALIDAD DE RECEPCIÓN, que cubre 5 posibilidades.

S representa la INTENSIDA DE LA SEÑAL, que abarca las 9 posibilidades.

T representa la TONALIDAD (usada actualmente solo para telegrafía), que igual que la anterior, cubre las 9 posibilidades.

9. CONCLUSIÓN

El sistema MSN shadow es una herramienta forense aplicada a programas de mensajeria instantanea como el MSN messenger, esta diseñado para verificar si es posible el seuestro de emails. Pero es necesario preveer que así como un cuchillo es una herramienta para un panadero pero un arma para un asesino, es necesario evaluar hasta que punto esta aplicación es útil y para qué es útil.

10. REFERENCIAS

[1]http://tUDYFORENSE/showthread.php.html

[2]http://es.wikipedia.org/wiki/ACK

[3]http://foro.latinohack.com/showthread.php?t=13724

[4]http://es.wikipedia.org/wiki/RST

[5]http://foro.latinohack.com/showthread.php?t=10798

[6]http://msnshadow.blogspot.com/

[7]http://sourceforge.net/projects/msnshadow