Pharming, nuevo fraude informático

Suxo Hinojosa JhovanaDoris
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
jhovi33@hotmail.com

RESUMEN

Cada vez se está haciendo más difícil memorizar los nombres de los nuevos fraudes cibernéticos, y es difícil detectar con algún antivirus o programa. A través de este artículo le explicamos esta nueva técnica de fraude que es el "PHARMING" que hace al usuario de Internet más vulnerable, ya que resulta muy difícil identificar cuando uno esta en la Red e ingresa a los sitios de su atacante. El fraude consiste en modificar el sistema de resolución de nombres de dominio, con lo que cada vez que introducimos una URL en nuestro ordenador para intentar acceder a una determinada página web, tienda on-line o un banco puede que estemos siendo víctimas de este fraude sin siquiera tratar de darnos cuenta.

Palabras clave

Código o lenguaje de virus, Dirección IP, DNS, Firewall, Malware, Troyano o Caballo de Troya.

1. INTRODUCCIÓN

A veces da la impresión, sobre todo en las empresas, que se cuenta con personal que desconoce sobre la parte informática que existe en nuestra empresa y no se toman medida de seguridad.

Se cae en el error de subestimar al trabajador sobre sus conocimientos de uso de los sistemas de información dando por hecho que su conocimiento informático no va a alcanzar para ingresar en la red y robar información o acceder a información que no debe y darle a otras personas información confidencial.

Así que la empresa ni se ha planteado la posibilidad de establecer barreras fiables para que eso no ocurra. Afortunadamente, esto ya no es muy habitual. Por otro lado, es frecuente que la dirección desconozca el uso que se está haciendo por parte de los trabajadores de los sistemas de información de la empresa. No es necesario que a un trabajador se le ocurra tratar de robar información relevante para la empresa para causarle un grave perjuicio o solamente por desconocer descargar programas que son nocivos para la organización y crear puntos de vulnerabilidad. Basta con que un usuario decida aprovechar la línea ADSL de la empresa e instalar un programa de intercambio de archivos Peer to Peer en el ordenador para bajarse música o películas (algo bastante frecuente, por otro lado). Su instalación puede causar un grave problema a la empresa y quitarle credibilidad, en este articulo enfocamos el problema para el lado del cliente que es usuario de un banco o quiera realizar alguna transacción vía on-line

Hoy en día el phishing sigue evolucionando y esta cada vez mas presente en los mensajes que recibimos y también cada vez en un mayor numero de países e idiomas. Ahora su evolución final ha culminado con la aparición del pharming, aun mas peligrosa y, en caso de llegar a realizarse, mucho mas efectiva que el phishing tradicional.

El articulo trata de prevenir a las personas que navegan por internet, explicando y, analizando en que consiste el pharming y como luchar ante este fraude.

2. CIBERDELINCUENCIA

Por ciberdelincuencia se entiende como las actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos.

Son tres tipos de actividades delictivas.

- El primero comprende formas tradicionales de delincuencia, como el fraude o la falsificación, aunque en el contexto cibernético se refiere específicamente a los delitos cometidos mediante las redes de comunicaciones y los sistemas de información electrónicos o redes electrónicas.
- El segundo se refiere a la publicación de contenidos ilegales a través de medios de comunicación electrónicos por ejemplo, imágenes de abuso sexual a menores o incitaciones al odio racial.
- El tercero incluye delitos específicos de las redes electrónicas, por ejemplo los ataques contra los sistemas informáticos, la denegación de servicio y la piratería.
- También con esto se produce los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

Acceso ilícito a sistemas informáticos. Interceptación ilícita de datos informáticos. Interferencia en el funcionamiento de un sistema informático. Abuso de dispositivos que faciliten la comisión de delitos. Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes noautorizadas y la utilización de spywarey de keylogger. Falsificación informática mediante la introducción, borrado o supresión de datos informáticos. Fraude informático mediante

la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos. El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

Delitos relacionados con el contenido, producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines: Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos.

3. PHARMING

En una conferencia organizada por el , Phillip Hallam-Baker definió este término como "un neologismo de mercadotecnia diseñado para convencer a banqueros y empresarios de comprar nuevos equipos o accesorios de seguridad".

Si buscamos en un diccionario de inglés el término pharming, lo encontraremos definido como "la producción de fármacos a partir de plantas y animales modificados genéticamente" ahora veremos como se relaciona con su concepto.

La palabra “pharming”, según Wikipedia, deriva del término ingles “FARM” que en castellano significa granja. El origen de la palabra se halla en que una vez que el atacante ha conseguido acceso a un servidor DNS y tomado control de este, es como si poseyera una "granja" donde puede hacer uso a conveniencia de los recursos que allí se encuentran. Sin embargo, si buscamos esta palabra en el diccionario inglés, aparecerá como: "la producción de fármacos desde plantas y animales genéticamente alterados". Pharming es un fraude informático que consiste en manipular las direcciones DNS (Domain Name Server) que utiliza el usuario.

Cuando un usuario teclea una dirección en su navegador, ésta debe ser convertida a una dirección IP numérica. Los servidores DNS son los encargados de este proceso que se llama resolución de nombres. En ellos se almacenan las direcciones IP de cada nombre de dominio. En cada computador conectado a Internet hay un archivo en el que se almacena una pequeña tabla con nombres de servidores y direcciones IP al que se denomina Hosts, de manera que no haga falta acceder a los DNS para conectarse con las páginas usadas frecuentemente. Así, que cuando el usuario intenta acceder a una página específica, realmente esta accediendo a una página Web falsa.

La modificación del archivo Hosts puede hacerse empleando un código malicioso (virus) o directamente por el hacker (accediendo remotamente al sistema). El virus puede entrar al sistema a través de múltiples vías: e-mail (la más frecuente), descargas por Internet, etc. Entre estos virus esta, Banker o Bambra que son malwares disfrazados que suelen esconderse en ficheros adjuntos, o se descargan al acceder a páginas falsas creadas con este objetivo.

Simplificando un poco todo el proceso antes descrito, el pharming consiste: estando nuestro ordenador infectado por un troyano o programa que permita realizar los cambios en las DNS, nosotros intentaremos acceder a una página web introduciendo para ello la URL y, estando nosotros confiados de que esa es la web deseada, realizaríamos las compras o accesos a nuestras cuentas bancarias en una página falsa, con lo que finalmente los atacantes obtienen nuestros códigos secretos y por ende la puerta abierta para cometer el fraude.

Otro tipo de Pharming, aun mas peligroso y efectivo es el que se realiza a nivel local, es decir en cada equipo individualmente. Tan sólo es necesario modificar un archivo denominado HOSTS, que tiene cualquier ordenador que funciona bajo sistema operativo Windows y que utilice Internet Explorer para navegar por internet.

El fichero hosts actúa de tal forma que no es necesario acceder al servidor DNS para reconducir a la web deseada. Esta almacena una pequeña tabla con las direcciones de servidores y direcciones IP que mas suele utilizar el usuario. Al modificar este fichero, por ejemplo, con falsas direcciones de bancos online sucederá que en el navegador se escribirá el nombre, pero nos enviara a una página que no corresponde con la real.

Proxies. Existe un peligro añadido a esta nueva técnica de pharming, que reside en los servidores proxies anónimos. Muchos usuarios desean ocultar su dirección IP a la hora de navegar, por lo que utilizan servidores proxy instalados en Internet que llevan a cabo la conexión con la IP del servidor en lugar de la IP del cliente. En el peor de los casos, uno de estos servidores proxy puede tener la resolución de nombres alterada, de manera que los usuarios que intenten entrar en su página bancaria, a pesar de que su sistema local está perfectamente asegurado, sean redirigidos por el proxy a una página con el mismo diseño y apariencia de su banco, pero falsa. También se podría pensar que el servidor proxy ha sufrido algún tipo de ataque que altere su sistema de resolución de nombres de dominio.

4. DETECCIÓN Y PREVENCIÓN CONTRA PHARMING

Los consumidores y las empresas pueden tomar varias medidas para prevenir los ataques del tipo pharming utilizando:

Certificados digitales. Sirven para diferenciar a los servidores web legítimos de los sitios ilegítimos; los sitios web que utilizan autenticación mediante certificados son más difíciles

de falsificar. Los consumidores pueden utilizar el certificado como una herramienta para determinar si un sitio es confiable.

Administración de nombres de dominio: Las empresas deben administrar cuidadosamente los nombres de dominio asegurándose de que éstos se renueven en forma oportuna. Las instituciones también deben investigar el riesgo que implica registrar nombres de dominio similares. Además, muchos registradores ofrecen bloqueadores de dominio para evitar el cambio no autorizado de un dominio.

DNS. Las empresas deben investigar las anomalías en sus sitios web para asegurarse de que los intentos de envenenamiento del DNS se contengan rápidamente. Por ejemplo, si el dominio de una empresa fue secuestrado, dejará de recibir solicitudes normales relacionadas con Internet de inmediato. La reducción del tráfico de Internet debería alertar al personal de tecnología de la empresa sobre el problema, que posteriormente debe ser investigado.

Educación del usuario. Se invita a los usuarios individuales a investigar y estudiar el problema de fraude y robo de identidad, a instalar versiones actuales de software de detección de virus, firewalls y herramientas de detección de spyware para disminuir las infecciones de su computadora, y comprender la importancia de actualizar con frecuencia estas herramientas para combatir nuevas amenazas.

En Windows Vista, tenemos la opción de Proteger el archivo host contra Escritura, para ello: Hacer clic con el botón derecho y darle en propiedades luego en seguridad, y luego en editar ahí, para cada uno de los usuarios, escoger que denegué la escritura del archivo, y con eso, ya no se podrá modificar pues cuando algún código lo intentara, se abrirá una ventana alertándonos de ello, y pidiéndonos si deseamos permitirlo en resumen, si tu host esta modificado, al teclear un nombre de una pagina web correcta podrías estar entrando a un servidor falso, y al ingresar tus claves, estarías enviándoselas a alguien mas, que después entraría al portal correcto del banco y haría movimientos a otras cuentas para robarse todo el dinero.

En julio de 2001, varios servidores de Irlanda fueron atacados mediante pharming, y no se resolvió hasta pasados más de 5 días. Muchas empresas irlandesas se vieron afectadas. El joven alicantino menor de edad que respondía al nick DragonKing fue detenido año y medio más tarde.

En enero de 2005, el nombre de dominio de un servidor de Nueva York, fue redirigido a un sitio web en Australia. Un proveedor de Secure e-mail, fue atacado mediante pharming el 24 de abril de 2005.

En marzo de 2005, el Senador Estadounidense Patrick Leahy introdujo un artículo de ley Anti-phishing, que proponía una condena de cinco años de prisión y una sanción económica a los individuos que realizasen ataques de phishing o utilizasen información obtenida mediante fraude online como phishing y pharming

5. ANTI-PHARMING

Anti-Pharming es el término usado para referirse a las técnicas utilizadas para combatir el pharming.

Algunos de los métodos tradicionales para combatir el pharming son la utilización de software especializado, la protección DNS y el uso de addons para los exploradores web, como por ejemplo toolbars.

El software especializado suele utilizarse en los servidores de grandes compañías para proteger a sus usuarios y empleados de posibles ataques de pharming y phishing, mientras que el uso de addons en los exploradores permite a los usuarios domésticos protegerse de esta técnica.

La protección permite evitar que los propios servidores DNS sean hackeados para realizar ataques pharming. Los filtros anti-spam normalmente no protegen a los usuarios contra esta técnica.

6. CONCLUSIONES

El malware ha adquirido una velocidad de propagación muy elevada, y los creadores son más y ofrecen al resto de la comunidad hacker, los códigos fuente para que introduzcan variaciones y puedan crear ataques nuevos. A pesar de los esfuerzos y la mejora de los laboratorios, es humanamente imposible que se elabore una solución adecuada y a tiempo para algunos códigos que se propagan en cuestión de minutos". La solución para este tipo de amenazas no debe ser, al menos en un primer frente de protección, una solución reactiva, sino que deben instalarse sistemas mediante los cuales se detecten no los ficheros en función de firmas víricas, sino las acciones que se llevan a cabo en el ordenador. De esta manera, cada vez que se intente realizar un ataque al sistema de DNS de la computadora, como es el caso de las aplicaciones para pharming, sea reconocido el ataque y detenido, así como el programa que lo ha llevado a cabo.

7. REFERENCIAS

[1] "Pharming, nuevamente en alerta", 2008.

[2] Depatamento de comunicación Technical Report "Fraude en internet: Del Phising al Pharming" 2004.

[3] IX Congreso Andino de Derecho Informático Organizado por www.NIC.BO Bolivia Universidad Católica.

[4] Osvaldo Callegari Analista de Sistemas. Seguridad de la información net report "Delitos informáticos: Pharming".