

ESTUDIO DE LA SEGURIDAD EN LOS SERVICIOS DE VIDEOCONFERENCIA POR MEDIO DEL TELEVISOR.

EVOPHONE VS *SET-TOP BOX* GENÉRICO

Cada día son más las empresas que descubren las ventajas de la videoconferencia como un medio rápido, efectivo y económico de comunicación interna y externa. La comunicación a través de este sistema, que combina la transmisión de imagen y voz ha pasado de ser un lujo tan sólo al alcance de directivos de alto nivel, a un servicio asequible incluso para la pequeña y mediana empresa.

No obstante y dada la proliferación de equipos que se vienen comercializando para prestar este servicio y la importancia de las comunicaciones que a través de ellos se realizan, conviene tener claras cuales son las garantías de seguridad que dichos sistemas nos ofrecen.

El presente estudio pretende clarificar cuales son las debilidades de las diferentes modalidades de videoconferencia presentes en el mercado.

Los actuales sistemas de videoconferencia modulares (los que no requieren PC) pueden clasificarse en dos grandes grupos:

- Sistemas que envían la información directamente a través de Internet (típicos *Set-Top Box Plug & Play*).
- Sistemas que envían la información a través de “túneles seguros” (redes VPN).

Existe una diferencia sustancial en el precio de ambos tipos de sistemas, de forma que los más sencillos, que son los del primer grupo, son bastante más económicos. Sin embargo, este ahorro se produce a costa de reducir la seguridad de la comunicación y por ese motivo, a largo plazo pueden ser la causa de graves problemas, incluyendo posibles responsabilidades legales derivadas de la prestación de un servicio inseguro y de los daños acarreados a los clientes finales.

Para clarificar esta situación, a continuación se exponen las diferencias entre el sistema de videoconferencia basado en VPN EVOPHONE, comercializado en exclusiva para España por PROINSSA y los demás sistemas de *Set-Top Box* convencionales y de bajo precio.

TABLA COMPARATIVA		
	EVOPHONE	SET-TOP BOX
TIPO DE RED	VPN / ETHERNET	INTERNET / ETHERNET
SEGURIDAD	●●●●	●
VELOCIDAD	16 FPS	30 FPS
FACILIDAD DE USO	●●●●	●●
DISPONIBILIDAD DE CONEXIÓN	●●●●	SUPEDITADO A LA CONGESTIÓN DE INTERNET
CONTROL DE LA CALIDAD DE COMUNICACIÓN	SI	NO
PERSONALIZACIÓN DE LA INTERFAZ	SI	NO
TELEMEDICINA	SI	NO
NECESITA PC	NO	NO
VISUALIZACIÓN	TV	TV
MANDO A DISTANCIA	SI	SI
ACTUALIZACIÓN	AUTOMÁTICA	AUTOMÁTICA

| ● = MUY MALO | ●● = MALO | ●●● = BUENO | ●●●● = MUY BUENO |

ACLARACIONES:

➤ SEGURIDAD:

- EVOPHONE: Establece la comunicación por una conexión segura VPN, dicha comunicación se realiza con las máximas condiciones de seguridad. **No hay peligro de que los piratas informáticos puedan acceder al contenido de la transmisión.**
- SET-TOP BOX: Realiza la transmisión directamente por Internet, por lo que **las comunicaciones no son seguras**, pudiendo ser objeto de sabotaje, acceso y uso indebido de la información contenida en las comunicaciones. Un hacker podría acceder a la comunicación entre dos puntos y disponer de la información obtenida a su capricho, o incluso vender/ceder los datos de los usuarios a terceros delincuentes que podrán llevar a cabo actos delictivos con la mayor vulnerabilidad para la víctima (robos,).

➤ COSTE:

- EVOPHONE: Proporciona una comunicación en un entorno de seguridad por medio de VPN, por lo que el precio final del producto se incrementa.
- SET-TOP BOX: Este tipo de videoconferencia resulta más económica, al realizarse la comunicación a través de Internet. No obstante resulta muy vulnerable frente a las agresiones propias de este canal de comunicación.

➤ PELIGROS Y AMENAZAS DE LOS “SISTEMAS BARATOS”

- Las conversaciones mantenidas, **audio y vídeo**, pueden ser accesibles a determinados delincuentes informáticos, porque no existe un sistema de seguridad en la comunicación cuando se emplean sistemas baratos.

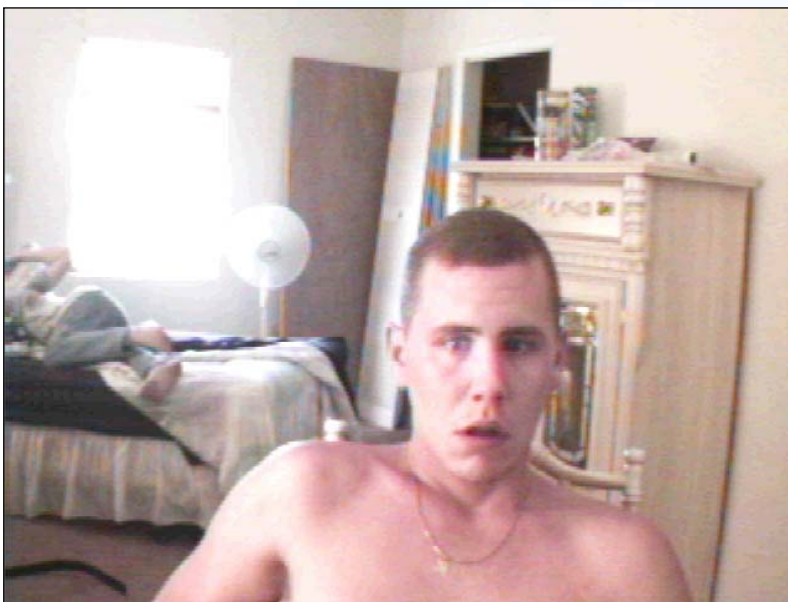
- Si un delincuente puede acceder a la comunicación audio-visual, obtendrá información muy sensible:
 - Datos personales confidenciales, como datos médicos, datos profesionales, números de teléfono personales, números de tarjetas de crédito, de cuentas bancarias, etc.
 - Status social: Los delincuentes pueden deducir cual es el nivel socio-económico del habitante, ya que pueden ver el salón de la casa, donde está habitualmente el televisor, y también ven el aspecto del habitante.
 - Hábitos y costumbres del usuario, como por ejemplo, cuándo está en casa o en qué horas está solo, es decir, información sobre vulnerabilidad del individuo.

➤ **EL ESPIONAJE REMOTO POR LA WEBCAM YA ES UNA REALIDAD.**

Por medio de los “virus y troyanos” de última generación, especialmente diseñados para espiar *webcams*, ya se están dando casos de videoconferencias interceptadas en Internet y que luego son mostradas de forma indiscriminada en la red, **para escarnio de la víctima.**

• **CASO REAL:**

Esta es una imagen obtenida de Internet donde se observa a un usuario de videoconferencia que no utiliza un sistema seguro, en el momento en el que el *hacker* le informa de que está siendo espiado a través de su *webcam*.



Este es el mensaje que el usuario está leyendo en el momento en que se tomó la imagen.

Traducción del mensaje: “Hola. Sé que no hemos hablado antes. Éste es tu ordenador. Puesto que puedo ver todo lo que hay en tu habitación, te daré un par de consejos. En primer lugar ponte una camiseta por favor. En segundo lugar, veo que hay una linda muchacha acostada en tu cama y que tú estas ahí sentado delante del ordenador con cara de tonto. Vamos. No seas gay.”



➤ **NOTICIAS SOBRE LA APARICIÓN DE NUEVOS VIRUS ESPECIALIZADOS EN SISTEMAS DE VIDEOCONFERENCIA**

- ***“El virus Rbot-GR asume el control de las cámaras web conectadas a sistemas intervenidos para luego usarlas, vía Internet, para observar las imágenes que éstas captan en hogares y lugares de trabajo.***

Rbot-GR aprovecha vulnerabilidades conocidas que algunas aplicaciones de Microsoft, para así instalar un troyano en las máquinas intervenidas. Asumiendo el control de cámaras web y micrófonos conectados a las máquinas infectadas, el troyano comienza a enviar a los intrusos que controlan el troyano las imágenes y audio captados por las cámaras.

Aparte de la invasión de la privacidad anteriormente descrita, el nuevo gusano actúa además como un troyano típico, al permitir a los intrusos acceso a la información almacenada en del ordenador. Asimismo, hace posible instalar código maligno y utilizar la máquina para realizar ataques de negación de servicio.

Desde Estados Unidos, Cluley, analista senior de Sophos, comentó al servicio de noticias CNet News, que el virus puede ser usado tanto para el espionaje industrial como para indagar en la vida privada de las personas. Cluley no estuvo en condiciones de señalar si, a su juicio, Rbot-GR fue diseñado para actividades “profesionales” o por simples voyeristas. Rbot-GR es una variante de la familia SDBot, consistente de un amplio grupo de troyanos, de los cuales hasta ahora se han detectado más de 200 variantes.”

Fuente: DiarioTi.com

- ***“Peeping Tom es nuevo troyano que se instala en la PC y controla las computadoras en forma remota. Una de las funciones específicas del virus es controlar la webcam y los micrófonos.***

La empresa de seguridad en Internet, Sophos, informó que el virus infecta la PC utilizando las vulnerabilidades de Windows e instala controladores en la webcam y los micrófonos, con el fin de grabar y espiar al usuario.

Peeping Tom también accede al disco duro en busca de claves o passwords. El troyano, cuyo nombre verdadero es W32/Rbot-GR, se distribuye a través de los programas de intercambio de datos (P2P).

Los directivos de Sophos consideran que este troyano es un ejemplo de una nueva generación de virus que espían las computadoras hogareñas y de pequeñas empresas.”

Fuente: reporterweb.com

➤ **LA OPINIÓN DE LOS ESPECIALISTAS:**

- *“Existe un comprensible rechazo a la utilización de aplicaciones de audio y vídeo basadas en IP, puesto que abrir en el cortafuegos puertos UDP que cambian dinámicamente el UDP no es una solución admisible si se quiere preservar la seguridad de la comunicación, o lo que es lo mismo, de la empresa.”*
- *“Publicaciones referentes a NAT, cortafuegos y acceso remoto recomiendan utilizar túneles VPN (en vez de H.323) para garantizar la seguridad en las comunicaciones por videoconferencia, puesto que estas soluciones no requieren abrir puertos TCP y UDP dinámicos a través del cortafuegos.”*
- *“En este panorama, las redes privadas virtuales proporcionan una manera de poner en ejecución usos de la videoconferencia con seguridad entre localizaciones múltiples dentro de una empresa.”*

Más información en:



➤ CONCLUSIONES

- 1. La comunicación a través de redes VPN proporciona la solución escalable y segura que permite a las empresas ofrecer servicios de videoconferencia de forma efectiva entre lugares distantes geográficamente.**
- 2. Las soluciones de videoconferencia basadas en tecnología IP, que no utilizan redes de comunicación VPN, requieren abrir los puertos TCP y UDP (H.323) del sistema, comprometiendo gravemente la seguridad y privacidad de las comunicaciones.**
- 3. Los sistemas *Set-Top Box* convencionales no son aptos para proporcionar servicios de videoconferencia con fines socio-sanitarios ya que no garantizan la privacidad de la información transmitida, por el contrario, para estos casos es preciso utilizar una infraestructura de comunicación segura, como es la que usa Evophone (VPN).**
- 4. Los graves riesgos de seguridad que son inherentes de los sistemas *Set-Top Box* convencionales pueden ser causa de graves problemas y perjuicios para los usuarios y sus consecuencias tendrán una extraordinaria repercusión legal y notoriedad en los medios.**

ANEXO: Noticias relacionadas

Detenido en Madrid un hacker que tenía acceso a las webcam de sus víctimas.
(Fuente: ABC, 17 de enero de 2005).

La Agencia Española de Protección de Datos ha impuesto dos multas, de 300.506 euros cada una, a dos clínicas que vulneraron la Ley de Protección de Datos y la obligación de custodia de la información sobre los pacientes.

El motivo de las multas fue la aparición de los expedientes médicos de pacientes en contenedores de basura, incluyendo el nombre, la dirección, el diagnóstico, etc.
(Fuente: El Mundo, 16 de marzo de 2005)