Siguiendo la evolución de las amenazas en internet

Durante el mes de Ciberseguridad de la UE, analizamos algunas de las principales amenazas en internet que hemos detectado en nuestra red a lo largo del año.

A medida que la forma en que los consumidores y las empresas utilizan Internet evoluciona, también lo hacen los riesgos que enfrentamos en el día a día. Entre septiembre de 2017 y marzo de 2018, observamos un aumento del 220% en el número total mensual de amenazas bloqueadas por Secure Net, el servicio de ciberseguridad desarrollado en la red de Vodafone.

Disponible en 10 países de Europa, Secure Net ha protegido desde hace más de 3 años a los clientes Vodafone; el servicio tiene actualmente más de 18 millones de clientes en Europa. Durante este tiempo, los intentos de malware, adware y phishing han sido una amenaza constante, pero la naturaleza del riesgo evoluciona, por lo que Secure Net ha evolucionado también para garantizar que la navegación segura de nuestros clientes.

Malware en evolución

Históricamente gran parte del malware (software malicioso oculto en sitios web y archivos descargados) tenía como objetivo el robo de información personal con el riesgo que supone de suplantación de identidad. Pero al inicio de este año, una de las mayores amenazas que hemos visto nuestra red es un pequeño código malicioso de JavaScript llamado Coinhive, que secuestra la potencia de procesamiento (CPU) de nuestros dispositivos llamado cryptojacking.

Cuando un usuario se conecta a un sitio web donde se esconde este script, a menudo oculto dentro de anuncios incrustados en la página, el código se apodera automáticamente de la CPU del dispositivo para "minar" criptomoneda, sin el conocimiento del usuario Este mayor uso de la CPU significa que los dispositivos van más lentos y las baterías se agotan más rápidamente. También pueden minar monedas programas que aparentemente prestan otros servicios, pero tienen un código oculto que se aprovecha de las capacidades de nuestro smartphone.

Cryptojacking es actualmente el malware más común en el mundo y la principal amenaza bloqueada por Secure Net: en marzo, alrededor del 38% del total de bloqueos a nivel europeo era por este motivo.

Cuidado con el todo gratis

Otro problema importante que vimos a principios de año provino de un programa publicitario (adware) llamado Leadzuaf. A menudo oculto en las descargas de software gratuitas, el adware redirige su navegador para mostrar anuncios no solicitados, a menudo en grandes cantidades y incluyendo otro tipo de virus; en febrero, hubo más de 110 millones de intentos de acceder a Leadzuaf solo en España.

Primer semestre del 2018

En Europa se han bloqueado más de 3.800 millones de amenazas durante la navegación y evitado la descarga de 38 millones de ficheros maliciosos.

Por países, Alemania y España se destaca por la gran incidencia del criptohacking a principio de año bajando su impacto en los siguientes meses; en España esta amenaza ha supuesto el 55% de

los ataques del semestre. En Alemania el adware ha tenido mucha actividad en enero y en febrero, representando el 38% de los bloqueos de seis meses.

En abril España sufrió una campaña de phishing muy agresiva a través de mensajes de chat, sin embardo en Turquía el repunte ha sido en Julio. Italia se destaca de los demás países en cuanto a intentos de descargas de ficheros infectados multiplicando por 10 los clientes afectados de cualquier otro país.

Siempre un paso por delante

Para enfrentar estas amenazas en constante cambio, es importante que los sistemas como Secure Net se adapten y evolucionen constantemente para mantenerse un paso adelante. La base de datos de identificación de virus de Secure Net es un organismo vivo que se adapta a las condiciones cambiantes de la web, por lo que siempre está alerta a las amenazas existentes y nuevas.

Estamos en el proceso de actualizar Vodafone Secure Net para que proteja nuestras redes fijas y móviles. Secure Net se convertirá en un servicio de red totalmente convergente, lo que significa que para el cliente gestionará un solo servicio independientemente se conecte a la línea fija de Vodafone, así como al servicio móvil, lo que contribuirá aún más a que nuestros clientes naveguen seguros por internet.

Para más información acerca de Secure Net:

Particulares: https://www.vodafone.es/c/particulares/es/mas-con-vodafone/servicios-para-tu-movil/secure-net/

Empresas: https://ayudacliente.vodafone.es/empresas/moviles-tablets-y-apps/aplicaciones-apps-servicios/secure-net/