CÁPSULAS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA COORDINACIÓN DE SISTEMAS DE CÓMPUTO

POR CUAUHTÉMOC VÉLEZ MARTÍNEZ

Cápsula TI NO. 29

CREEPWARE

En la actualidad, hay una tendencia entre *hackers* y expertos en seguridad informática que consiste en cubrir las *webcams* y micrófonos de sus computadoras mediante el uso de etiquetas o adhesivos, aunque esto sugiere una obsesión de su parte, la realidad es que existen herramientas capaces de funcionar como auténticos *big brothers* recargados. Quien intenta acceder remotamente una computadora utiliza un programa denominado *RAT (Remote Administration Tools/Trojan*, según el propósito) que permite no solo tener a su disposición información de la víctima sino además, activar su micrófono y *webcam* sin que sepa lo que está sucediendo hasta que es demasiado tarde. Esta acción se denomina *creepware* (*creep*: moverse lenta y silenciosamente para pasar desapercibido; *ware*: sufijo de software)

Normalmente el *creepware* se instala de la misma manera que la mayoría del *malware* es decir, mediante clics presionados en ligas, chats o archivos adjuntos al correo electrónico. Una vez ejecutado el programa, el *hacker* tendrá acceso a la computadora objetivo como si estuviera sentado frente a ella. El control que tiene el atacante es casi ilimitado, programas como *Blackshades Adwind*, o *Darkcomet* permiten acceder remotamente a múltiples recursos: activar la cámara para videograbar o tomar fotografías, acceder y copiar archivos o carpetas, imprimir pantallas, prender el micrófono para grabar voz, robar contraseñas y nombres de usuarios, controlar el escritorio de la computadora e incluso encender la impresora conectada al equipo. Desafortunadamente, para realizar exitosamente estas acciones, no es necesario tener habilidades o conocimientos informáticos profundos, pues este *software* es relativamente sencillo de instalar y utilizar, además de estar disponible en la *web* para cualquier persona por algo más de 40 dólares. Una vez obtenida la información, el atacante la empleará para distintos propósitos según su intencionalidad: comprometer a la víctima, extorsionarla, robar su identidad, espiarla o incluso secuestrarla.

Los *smartphones* no se quedan afuera de esta amenaza. Desde 2012, existe un *malware* denominado *Nickispy* que actúa sobre sistemas operativos *Android*, capaz de reunir información del *GPS*, grabar llamadas telefónicas y robar mensajes recibidos y enviados; o bien, *AlienSpy* que según Kaspersky, entre 2013 y 2016 ha lanzado ataques a cerca de medio millón de usuarios alrededor del mundo y cuyas funciones incluyen recolectar información del dispositivo (nombre del equipo, versión del sistema operativo, memoria *RAM*, etc.), grabar video y tomar fotografías, almacenar datos tecleados (*keylogger*), entre otras.

Aunque en términos estadísticos el *creepware* no es una amenaza que figure entre las más importantes dada su frecuencia de ataques, las consecuencias para las víctimas pueden ser devastadoras; tal fue el caso de *Cassidy Wolf (Miss Teen America)* quien en 2013 denunció haber sido espiada a través de su computadora, tomando fotos en la intimidad de su cuarto y posteriormente extorsionándola para no publicarlas en redes sociales. James Abrahams, el *hacker* agresor, admitió ante el *FBI* haber realizado el mismo acto a más de 100 mujeres.

Por lo anterior, es muy importante seguir las siguientes recomendaciones para evitar la presencia de *creepware* en nuestros equipos:

Tener instalado y actualizado *software* de seguridad. La mayoría de las empresas dedicadas a la protección de datos y sistemas, tienen soluciones interesantes para proteger los equipos de cómputo tales como compras en línea, transacciones bancarias, resguardo de datos personales, detección y eliminación de *malware*.

Mantener actualizado el sistema operativo. Aunque llegan a ser molestos los avisos de actualización, tener un sistema operativo al día representa una disminución importante de riesgo por *malware* ya que las vulnerabilidades detectadas son corregidas mediante este proceso que indudablemente, por el incremento de amenazas que permean el ambiente, debe ser frecuente.

Instalar *software* de sitios legales y confiables. Buscar sitios que ofrecen *software* gratuito sin pensar en el peligro potencial que representa acceder a ellos, es un problema recurrente entre los usuarios. Los programas, si bien son productos intangibles, tienen un costo y muchos usuarios evitan pagarlo accediendo a páginas poco confiables con gran cantidad de anuncios (*adware*) o *links* que al presionar clic en ellos, pueden ejecutar programas malignos (*malware*) que dañen la información o recolecten datos confidenciales.

Ocultar la *webcam* y el micrófono. Una regla de la seguridad informática es que ningún sistema está 100% protegido, es decir, aun aplicando las debidas precauciones, cabe la posibilidad que nuestro equipo sea víctima de *creepware*, es por ello que como medida preventiva se colocan etiquetas sobre la cámara y el micrófono.

Aunque no podemos evitar la existencia de estas amenazas en internet, siendo preventivos y tomando las medidas adecuadas, disminuiremos la probabilidad de infectar nuestros equipos.

Referencias

-BBC. (2013). Miss Teen USA hacker pleads guilty to 'sextortion' threats. BBC News. Tomado de: http://www.bbc.com/news/technology-24929916

-Kamluk, V. (2016). Adwind a cross platform RAT. Kasperky Lab. Tomado de: https://securelist.com/securelist/files/2016/02/KL_AdwindPublicReport_2016.pdf

- Storm, D. (2012). Mobile RAT attack makes Android the ultimate spy tool. ComputerWorld. Tomado de: http://www.computerworld.com/article/2472441/cybercrime-hacking/mobile-rat-attack-makes-android-the-ultimate-spy-tool.html

- Symantec. (2013). Who's watching you? Symantec Security Response. Tomado de: http://www.symantec.com/connect/blogs/creepware-who-s-watching-you

Otras fuentes de información:

- https://www.fidelissecurity.com/sites/default/files/FTA_1018_looking_at_the_sky_for_a_dark_comet.pdf

- http://www.computerworld.com/article/2501964/security0/remote-access-tools-a-growing-threat-to-smartphones.html

- http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/DARKCOMET

- https://www.fidelissecurity.com/sites/default/files/FTA_1015_Alienspy_FINAL.pdf

- http://www.symantec.com/connect/blogs/truth-behind-shady-rat

- http://www.darkreading.com/attacks-and-breaches/shady-rat-hid-malware-in-digital-images/d/d-id/1099530?

- http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

- http://computerhoy.com/noticias/software/creepware-tu-webcam-te-espia-no-sabes-27023

- http://www.pcadvisor.co.uk/opinion/security/blackshades-how-police-cracked-down-on-hackers-3528675/

- http://www.symantec.com/connect/blogs/blackshades-coordinated-takedown-leads-multiple-arrests

- http://www.pcworld.com/article/3031736/security/java-based-trojan-was-used-to-attack-over-400000-systems.html

- http://blogs.cisco.com/security/talos/darkkomet-rat-spam

- http://www.zdnet.com/article/alienspy-rat-strikes-over-400000-victims-worldwide/