La evolución del espionaje casero: así de fácil fue para un profesor vigilar el ordenador de su alumna

Una gran variedad de programas permiten el acceso ilegal a dispositivos ajenos sin apenas conocimientos informáticos

JORDI PÉREZ COLOMÉ
27 DIC 2019

Era un sábado y el director de tesis encendió el ordenador que usaba su doctoranda en el Instituto de Biotecnología de la Universidad de Granada. Desde allí buscó un sencillo programa informático. Se tomó un tiempo para comparar la versión gratuita y la de pago. Entró en su cuenta de Paypal para comprarlo, lo descargó y lo instaló. Ese programa captura las teclas que el usuario pulsa, hace capturas de pantalla y lo manda a quien controla el programa.

Con ese método, el profesor obtuvo la contraseña de la cuenta de Facebook de su estudiante. Cuando accedió a la cuenta de ella, lo hizo desde su ordenador Apple y se buscó a sí mismo en el buscador de Facebook. Era un modo quizá de saber qué pensaba ella de él. Cuando la víctima volvió a usar Facebook vio sorprendida aquella búsqueda rara del nombre de su profesor, cuenta su abogada, Cristina Pasquau.

Entonces miró el historial de navegación del ordenador de la universidad y allí encontró todas las huellas de cómo le habían instalado el programa de espionaje en el equipo. El profesor no había borrado nada. Por si fuera poco Facebook distinguía accesos desde un móvil Android o Windows y Macintosh. Solo el profesor manejaba un Mac en la universidad.

Todo esto ocurrió entre el 27 y el 29 de junio de 2015. Más de cuatro años después —hace pocos días— se ha sabido la resolución del caso, que ha sido por acuerdo entre las partes: el profesor admite los hechos, ha pagado una sanción de 3.000 euros de responsabilidad civil y ha sido condenado a dos años de cárcel (en la que no ingresará) y dos años sin dirigir tesis.

Los hechos son una muestra casi perfecta de cómo ser un espía lamentable: dejó huellas digitales por todas partes. Fue una chapuza. Pero también indica que alguien más cuidadoso puede hacer esto bien si tiene acceso fácil al ordenador de la víctima. Hoy el programa cuesta 40 euros y tiene versión gratis. Su uso es de hecho legal en casos determinados. La primera excusa del profesor fue que había instalado el programa para controlar el uso de la impresora e información confidencial que había en el disco duro. Durante el proceso, sin embargo, optó por admitir los hechos y confesar que lo había hecho por interés personal.

A pesar de la denuncia, la universidad nunca cambió al director de la tesis, que finalmente fue presentada en otra universidad en Barcelona en diciembre de 2018. "Ante la inminencia de tener que presentarla sin posibilidad de cambiar de director, la alumna sufrió un trastorno ansioso depresivo y requirió de baja médica", dice Pasquau. Todo esto está confirmado porque el profesor lo ha admitido y la víctima hizo unas capturas de pantalla. Pero la policía científica no pudo analizar el disco duro porque estaba dañado. Durante su conservación en algún lugar de la Universidad de Granada ocurrió algo que perjudicó el disco duro.

Uno de cientos

El caso granadino es solo uno de entre cientos cada año. Según los datos de Interior, el acceso ilegal informático se multiplicó por dos entre 2011 y 2018, de 789 a 1.561 casos. La variación en casos esclarecidos y detenidos e investigados fue sin embargo mucho menor: de 114 casos esclarecidos en 2011 se pasó a 162 en 2018 y las personas detenidas o investigadas en realidad cayeron en esos años, de 52 a 41. "No es un ataque común si miramos la estadística de ciberdelitos, pero hay casos de revelación de secretos de todo tipo", dice el abogado David Maeztu, del bufete 451.Legal.

Los programas como el usado en este caso, del tipo ***keylogger***[1], son solo un tipo de herramienta de espionaje. Hay más. En noviembre la policía española colaboró en una operación coordinada por Europol contra una web que vendía un servicio llamado Imminent Monitor. Este servicio es un **RAT (*Remote Access Trojan)***. Sirve para controlar un móvil u ordenador a distancia.

Como los *keylogger*, los RAT también permiten espiar. Pero un RAT no necesita tener acceso físico al dispositivo (puede alcanzarlo mediante un *link*, archivos, *apps* maliciosas) y permite controlar el aparato en remoto (conectar micro, cámara, hacer capturas de pantalla), mientras que un *keylogger* debe instalarse y manda información puntual, sin posibilidad de más.

"Cualquiera con una inclinación perjudicial a espiar o robar podía usarlo por unos 22 euros"

"Imminent Monitor era considerado peligroso por sus características, facilidad de uso y bajo coste. Cualquiera con una inclinación perjudicial a espiar víctimas o robar datos personales podía usarlo por unos 22 euros", dice la nota de prensa de Europol. Las autoridades calculan que el *malware* fue comprado por 14.500 personas en 124 países. En la operación detuvieron a 13 de sus usuarios más prolíficos.

El uso principal de Imminent Monitor era probablemente el **cibercrimen**, según fuentes de la policía. Pero el tipo de material encontrado por las fuerzas de seguridad incluye "fotos privadas, detalles personales y vídeos", según Europol. La dedicación personal que requiere el control de un RAT hace pensar que su uso es más específico: "El atacante controla cada dispositivo infectado manualmente. Esto lleva tiempo y dedicación, lo que hace que las infecciones de RAT sean menos

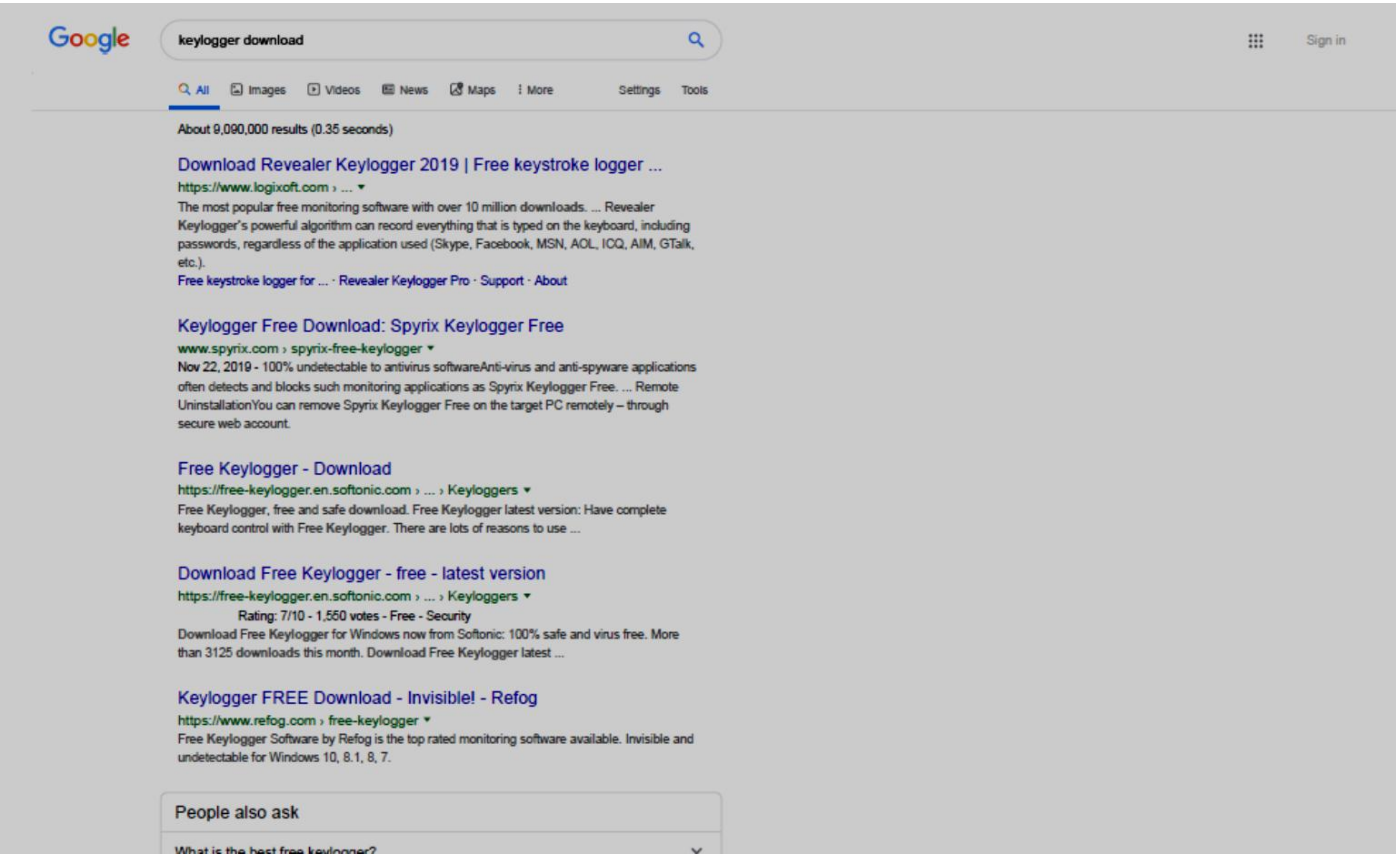
[1] Un **keylogger (regitrador de teclas**) es un programa o un hardware que se encarga de registrar todo lo que escribimos al utilizar el teclado, es decir, puede registrar todo lo que tecleamos en cualquier plataforma, ya sea dentro y fuera de Internet. Estos programas pueden ser instalados teniendo o no acceso a la computadora de la víctima.

numerosas que las de otros *malware* como Zeus, FakeSpy, Retadup", dice Verónica Valeros, investigadora de la Czech Technical University de Praga.

Valeros lleva años estudiando los RAT. No cree que su uso esté mucho más extendido: "Los años entre 2010 y 2014 o 2015 fueron los años más activos según mi investigación. Quizás ahora se les presta un poco más de atención y por eso se percibe ese aumento", explica.

**Veronica**@verovaleros

Third iteration of my study of RATs. Timeline of the 300 most 'well known' RATs investigated, according to their time of appearance. Blog post here: https://www.veronicavaleros.com/blog/2018/3/12/a-study-of-rats-third-timeline-iteration …



Como con los *keylogger*, los RAT también tienen un uso legítimo: "Se emplean mucho para poder proveer control y asistencia remota a dispositivos. Pero hay muchos cuyo código se ha filtrado y esto hace que cualquiera pueda agarrar ese código, cambiarlo, y convertirlo en su propio RAT", explica la investigadora.

También como los *keyloggers*, un RAT no requiere de *hackers* profesionales: "Los RAT son fáciles de operar y ofrecen un rango de funcionalidades muy amplio", añade Valeros.

La actuación policial tiene probablemente que ver con la facilidad de distribución del *malware* Imminent Monitor: "Muchas de estas herramientas no solo las explota quien las diseña. Es *malware* para alquilar o vender, que no es tan complicado de usar", dice Eusebio Nieva, director técnico de Check Point.