«Cuando las barbas de tu vecinx veas cortar…» Francia quiere convertir los objetos conectados en chivatos de la policía

En el blog hemos ido publicando algunos textos en relación con la (in)seguridad informática, como la introducción de la 6ª ed. de la guide d'autodefense numerique *(donde entre otras cosas se advierte del uso de vulnerabilidades "zero day" por parte de los Gobiernos para llevar a cabo ataques informáticos dirigidos); un comunicado de Ivan Alocco en el que contaba que la policía obtuvo acceso a sus discos cifrados, y algunas respuestas (1,2) que brindan información tratando de arrojar luz sobre el asunto: si los algoritmos de cifrado considerados seguros habían sido crackeados y otras posibles técnicas por las que podrían haber obtenido las claves de cifrado o las contraseñas (passphrase) que las protegen, si bien ninguna contemplaba la posibilidad de se hayan usado puertas traseras o vulnerabilidades "zero day", que pueden afectar tanto a nivel software (sistema operativo, aplicaciones) como a nivel hardware.*
Detengámonos un momento para recordar que la policía debe demostrar las técnicas con las que ha obtenido las pruebas para poder usarlas en la acusación. En el caso de Ivan, dicen no haber encontrado ninguna prueba en los discos que lo relacione con los delitos contestados. En el dossier policial tampoco indican la técnica por la que obtuvieron acceso.
Estas sospechas del uso de vulnerabilidades, que ya nos surgían al leer el comunicado de Ivan, vuelven al enterarnos de que se acaba de presentar un proyecto de ley en Francia para permitir tomar el control de todo tipo de dispositivos conectados de forma remota usando vulnerabilidades en estos (lo que también permitiría usar en sede judicial interceptaciones que hasta ahora sólo servían a nivel policial e investigativo por no haber sido obtenidas de forma legal).

A continuación extractos de un reciente comunicado del Observatoire des libertés et du numérique *en relación con el nuevo proyecto de ley:*

Francia quiere convertir los objetos conectados en chivatos de la policía

El proyecto de ley «Orientación y Programación del Ministerio de Justicia 2023-2027» ha comenzado a debatirse en el Senado, y su artículo 3 ya está causando polémica. Y con razón.

Entre disposiciones encaminadas a ratificar, sin ningún orden en particular, la intervención a distancia de médicos en caso de prolongación de la custodia policial y de intérpretes desde el inicio de la misma, o la ampliación de las posibilidades de registros nocturnos a los delitos comunes, **se ha creado una nueva herramienta de investigación que permite la activación a distancia de los dispositivos electrónicos de una persona sin su conocimiento para obtener su geolocalización en tiempo real o captar imágenes y sonidos**. Art. 3, puntos 12°, 13° y 17° a 19°.

Para decirlo claramente, los investigadores forenses podrán, por ejemplo, geolocalizar un coche en tiempo real utilizando su sistema informático, escuchar y grabar todo lo que se dice por el micrófono de

un teléfono aunque no haya ninguna llamada en curso, o activar la cámara de un ordenador para filmar lo que está en el campo de visión, aunque el propietario no la encienda. **Técnicamente, la policía aprovechará los fallos de seguridad de estos dispositivos para instalar un software que les permita tomar el control y convertir en chivatos tus herramientas, las de tus seres queridos o las de diversos lugares**.

Para justificar estas graves invasiones de la vida privada, el Ministerio de Justicia invoca el «temor de atraer la atención de los delincuentes investigados por delincuencia organizada, de revelar la estrategia o simplemente porque expondría la vida de los agentes encargados de esta misión» al instalar herramientas de vigilancia. En resumen, sería demasiado arriesgado o complicado para los agentes instalar micrófonos y balizas «físicas», así que más les vale utilizar todos los objetos conectados. Sin embargo, ese supuesto riesgo no está respaldado por ninguna información seria ni por ejemplos concretos. Sobre todo, hay que tener en cuenta que el pirateo de los dispositivos seguirá realizándose en gran medida mediante el acceso físico a los mismos (que es técnicamente más sencillo), por lo que los agentes seguirán expuestos a este supuesto riesgo vinculado al terreno. (…)

La medida establecida en el art. 3 es **especialmente problemática para los teléfonos móviles y los ordenadores,** ya que son una parte muy importante de nuestras vidas. **Pero el peligro no acaba ahí, ya que el ámbito de aplicación de la medida en realidad abarca todos los «dispositivos electrónicos», es decir, todos los objetos digitales con micrófono, cámara o sensor de localización.** Por tanto, esta medida de investigación permitiría:

– «sonorizar», es decir, escuchar espacios desde un televisor conectado, un vigilabebés, un asistente de voz (como Google Home o Alexa) o un micrófono integrado en un coche;
– retransmitir imágenes y vídeos desde una cámara portátil, un smartphone o una cámara de seguridad con detección de movimiento;
– obtener la ubicación de una persona mediante el posicionamiento GPS de un coche, un patinete conectado o un reloj conectado. Muchos otros dispositivos equipados con estos sensores también podrían ser pirateados.

Si este texto se aprobara definitivamente, aumentaría peligrosamente las posibilidades de intrusión policial, convirtiendo todas nuestras herramientas informáticas en espías potenciales (…) Se consagra por ley el derecho del Estado a utilizar las fallas de seguridad de los programas o equipos informáticos (…)

La policía y los servicios de inteligencia ya disponen de herramientas altamente intrusivas: instalación de dispositivos ocultos en casas o coches (balizas GPS, cámaras de videovigilancia, micrófonos), extracción de información de ordenadores y teléfonos, por ejemplo, y el uso de grabadores de pantalla o de pulsaciones de teclas (keyloggers). Ya se está abusando de estas posibilidades tan amplias para vigilar a activistas como (en la lucha del Carnet, en la oposición a las megabalsas en locales militantes de Dijon, o en las fotocopiadoras de locales anarquistas, etc.).
(…)
En cuanto a la geolocalización de objetos conectados, **el espectro es aún más amplio, ya que la activación a distancia podría afectar a cualquier persona sospechosa de haber cometido un delito castigado con penas de cinco años de prisión** (…)

La historia nos ha demostrado que existe un «efecto carraca»: una vez adoptada una ley o un experimento de seguridad, ya no hay vuelta atrás. A la inversa, la creación de una medida intrusiva suele servir de base para futuras ampliaciones de la seguridad, legitimándolas por su mera existencia (…).

[Fuente: https://halteaucontrolenumerique.fr/?p=2937]

* * *

Algunas noticias recientes:

– El FSB (servicios secretos rusos) acusa a la NSA de utilizar una puerta trasera aún desconocida de los iPhone con el propósito de recopilar información.
– Una gran número de placas base Gigabyte incluyen puerta trasera en el *firmware* que permite instalar programa malicioso en la UEFI (o Bios), y tomar control de la computadora.
– El poco conocido proveedor israelí *QuaDream* fundado por un ex oficial militar israelí y veteranos del *Grupo NSO* (empresa que creó *Pegasus*), comercializa software espía llamado *Reign*, con funciones similares a *Pegasus.*

Respecto a los chips de código cerrado que gestionan el arranque del sistema operativo, un breve artículo de 2021 visto en internet:

Todos los ordenadores modernos tienen *puerta trasera*

Cada ordenador moderno con un procesador Intel o AMD tiene una puerta trasera (o backdoor) incorporada y no hay nada que puedas hacer al respecto. Puede acceder a todas las áreas de la memoria de su ordenador sin la CPU ni tu conocimiento e incluso más. ¿Quieres saber cómo se llama esta puerta trasera? Para Intel se llama Intel Management Engine. *Para AMD se llama* Platform Security Processor.

Estos son sistemas de código cerrado dentro de cada procesador Intel fabricado después de 2008 y en cada procesador AMD fabricado después de 2013. Pero, ¿qué pueden hacer? Bueno, esto da un poco de miedo.

Estos subsistemas pueden:

Acceder a todas las áreas de la memoria de tu computadora. Sólo eso ya permite “verlo” todo.

Ver todo lo que se muestra en pantalla.

Acceder a todos los dispositivos conectados al ordenador.

Configurar un servidor TCP/IP en tu interfaz de red sin importar si tu sistema operativo lo permite o no.

Ejecución remota, incluso cuando el ordenador está apagado: mientras esté enchufado a la pared o a la batería, el subsistema puede funcionar.

Encender o apagar el ordenador de forma remota.

Así que como puedes ver, si estas usando un procesador Intel o AMD, realmente no importa que sistema operativo estés ejecutando. Estas puertas traseras tienen acceso a todo. Incluso pueden abrir una conexión remota en la interfaz de red.

Vulnerabilidades y exploits conocidos

¿No te lo crees? Comprueba la lista de vulnerabilidades y exploits conocidos.
https://en.wikipedia.org/wiki/Intel_Active_Management_Technology#Known_vulnerabilities_and_exploits

y para AMD. https://arstechnica.com/gadgets/2018/03/amd-promises-firmware-fixes-for-security-processor-bugs/

¿Qué se puede hacer?

Lo único que se me ocurre es tener algún tipo de cortafuegos externo entre tu ordenador y la red que se pueda configurar para bloquear las peticiones entrantes o los intentos de llamar a casa.

Aparte de eso, no estoy seguro. No hay una manera segura de desactivar estos sistemas. Puedes usar un ordenador antiguo que no tenga estos sistemas. Algunas placas base y fabricantes como System76 ofrecen opciones para apagar o desactivar estos sistemas.

Pero más allá de eso, si quieres una CPU x86/x64 moderna, sólo te queda confiar en Intel y AMD. Al fin y al cabo, estos sistemas siguen siendo una caja negra. Mientras el código no sea abierto y no se pueda auditar, no podremos confiar plenamente en ellos.

Por eso me gustan proyectos como RISC-V. Están creando una CPU abierta. Están creando una CPU abierta, sin cajas negras secretas.

Aprende más

Hay mucho más que aprender sobre este tema, así que te animo a que investigues por tu cuenta. Voy a enumerar mis fuentes a continuación para que puedas ver lo que me llevó hasta la madriguera del conejo.
¿Me he equivocado o me he dejado algo importante? Házmelo saber en los comentarios.

Fuentes

https://proprivacy.com/privacy-news/intel-management-engine
https://lukesmith.xyz/articles/only-use-old-computers/
https://hackaday.com/2017/12/11/what-you-need-to-know-about-the-intel-management-engine/
https://news.softpedia.com/news/intel-x86-cpus-come-with-a-secret-backdoor-that-nobody-can-touch-or-disable-505347.shtml
https://en.wikipedia.org/wiki/Intel_Management_Engine
https://en.wikipedia.org/wiki/AMD_Platform_Security_Processor

[Fuente: https://www.sysjolt.com/2021/every-modern-computer-has-a-backdoor/]