Asociación de Internautas

Troyanos en mi ordenador, ¿Posible? ¿Y que?

La publicación en medios del borrador de anteproyecto de Código Procesal Penal del Ministerio de Justicia encargado por el departamento que dirige Alberto Ruiz-Gallardón, ha levantado todas las alarmas en la red. Y no es para menos. Voy a intentar explicar de una manera sencilla, mi visión sobre el alcance de este borrador y las consecuencias que, a mi modo de ver, podrían tener sobre los usuarios de la red.

La ley, permitiría, en caso de aprobarse este borrador tal y como se ha presentado, instalar software (programas) que dan acceso a los ordenadores investigados, con autorización judicial expresa, en los casos que se concretan en el mismo borrador.

Permite la intrusión en los ordenadores, mediante herramientas informáticas, las que sean. Podrían ser, entre otras, lo que conocemos como troyanos (permiten el acceso y control de un ordenador infectado) , keyloggers (registran cualquier pulsación que realice el usuario), virus, etc.

Es decir, este borrador también abre la puerta a entrar de cualquier manera en un ordenador. Porque se considera programa informático, a una serie de instrucciones. Y unas líneas de comandos, contenidas en un archivo, entraría dentro de la acepción de programa informático . De manera general, como intrusión, entenderemos el colarnos en un ordenador ajeno sin permiso.

Un programa informático, puede hacer muchas cosas más que espiar, activar la webcam, grabar nuestras claves de acceso y robarnos el video erótico con la parienta o el pariente Hará lo que el programador haya querido que haga. Y ahí está el problema. En el borrador no se dice que única, exclusiva, y explícitamente se puedan espiar o intervenir las comunicaciones.

Por ejemplo, pueden hacer un programa que espíe, y que a la vez, descargue un archivo en el ordenador de la persona investigada. O que borre datos, o cualquier acción prevista por el programador.

¿Y dónde está el problema?

Pues como según dicho borrador, la ley, no lo prohibiría, podrían dejarnos en nuestros ordenadores, cualquier archivo. Y cualquier archivo, es cualquiera. Desde imágenes de menores, hasta una película protegida por derechos de autor, o la prueba que quieran dejar. Hasta enviar correos en nuestro nombre, o llenar las redes sociales de mensajes incitando al racismo, violencia, homofobia lo que se les ocurra, que después, puede ser utilizado en nuestra contra.

Simplemente manipulando fechas, metadatos, etc. Pueden fingir que ese archivo siempre estuvo ahí. Y podrían contar, y sería de obligado cumplimiento, con la colaboración de todo tipo de personal experto en seguridad (hackers, para entendernos), con los ISP, con cualquiera!

¿Tan fácil resulta hacerlo?

En condiciones normales, no es tan sencillo, entre otra razones, porque no conocemos la IP de la

persona a hackear y esta puede cambiar con bastante frecuencia y se han de poseer conocimientos de seguridad para hacerlo.

Habitualmente, somos nosotros mismos los que nos infectamos con estos programas, bien en la red, abriendo archivos enviados por personas de nuestra confianza, es decir, la infección la solemos provocar nosotros mismos, porque somos confiados por naturaleza y tenemos un dedo muy rápido con el ratón, visitando alguna web que nos introduzca el código malicioso, abriendo un archivo infectado (esto es muy fácil, con enviar un archivo calentito de alguna celebridad, caen la mayoría de usuarios). Hay muchas maneras de infectar a la víctima. Los archivos maliciosos, normalmente se esconden detrás de algún archivo que parece inocuo , pero con gancho.

Y una vez infectada la víctima, como su IP cambia, ese programa malicioso, se encarga de avisar al atacante de nuestra nueva dirección IP, enviándosela al correo, dejando un archivo con la IP en algún servidor, o de cualquier otra manera accesible al atacante. De esta manera, mientras no se elimine el dichoso programa del ordenador infectado, el atacante siempre tendrá acceso a él.

Pero Es que la ley, además tiene prevista la colaboración de los ISP (telefónica, Orange, etc.), que mediante orden judicial, también estarán obligados a facilitar todos los datos de que dispongan. Es decir, podría ser nuestra IP, los datos de nuestro router (recordar que telefónica, ó orange, tienen la contraseña de la wifi en la parte inferior, y la guardan en su base de datos), o cualquier otra información que facilite el acceso a nuestro ordenador.

En resumen, que tienen prácticamente la puerta abierta a nuestro ordenador. Imaginar que con la IP conseguida mediante orden judicial, alguien experto, puede hackearnos , aprovechándose de las vulnerabilidades de Windows (porque la gente normal, usa Windows) y nos cuela el susodicho troyano .

O más fácil, con cualquier técnica de intrusión, simulando la IP del servidor de Windows, nos cuelan una actualización de Windows, que además, viene con regalito, el troyano . O nos envían un enlace, cuya página nos infecta (las páginas con nombres porno no fallan).

También, con la clave de la wifi obtenida de las bases de datos del ISP, podrían plantarse debajo de nuestra ventana, con un portátil, conectarse a nuestra red local, y una vez dentro de la red, mirar si tenemos carpetas compartidas, para dejar el troyano . Estando en nuestra red, pueden hacer muchas cosas Y para ellos, no sería delito.

¿Y ya está? ¿El antivirus no lo detecta?

Ahí está la parte complicada del proceso. Los antivirus incluyen los programas maliciosos en sus listas una vez tienen constancia de que existen, También pueden sospechar de su existencia utilizando diferentes técnicas, como la heurística (fechas raras en nuestros archivos), pero no son adivinos.

Si alguien crea un código malicioso del que no hay patrón, y no hace cosas raras, como inflarnos a publicidad o imagenes porno de repente, abrir determinados puertos (las vías de comunicación de nuestro ordenador con el resto de la red), o nuestro ordenador empieza a desvariar, ir lento, o hacer cosas raras, probablemente, no sea detectado.Y es que además, el código inicial del troyano, puede ir cambiando (mutando) para evitar ser descubierto y lo mas probable, es que el usuario no experto ni se entere.

El código para el troyano policía , lo normal es que sea escrito por empresas o usuarios con conocimientos avanzados de los mismos, para evitar repetir patrones, y conductas detectables.

Un Juez, ¿Da la autorización tan fácilmente?

Pues depende de lo que se entienda por fácil. Está previsto, que se autoricen estas actuaciones policiales cuando haya indicios razonables de que se están cometiendo delitos intencionados castigados con pena con límite máximo superior a los tres años de prisión-. Junto a este presupuesto se añaden otros dos: a) que estemos en presencia de delitos cometidos en el seno de un grupo u organización criminal; b) que se trate de delitos cometidos por medio de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación (si, hasta tu movil ese tan guay puede llevarte a la carcel)

Si sumamos que, con la ya conocida como Ley Lasalle Alguien de quien se sospeche que está copiando a un coleguita el mp3 comprado en itunes, podría resultar afectado. Ya no quiero ni pensar, por descargarse una película bajo derechos de autor.

¿Y si no me bajo nada de internet, o poseo algún archivo sujeto de autor?

Pues tampoco estás tan a salvo! Con lo que comentaba al principio, de que por lo que veo , no se limita la acción policial a espiar , sería posible colarnos un archivo indebido en nuestro ordenador.

Con técnicas conocidas como Spoofing es posible falsear la dirección IP. Alguien puede simular que se está bajando un archivo como si fueramos nosotros, falseando la IP, y suplantandola con la nuestra. Un archivo con contenido de menores, por ejemplo. Con esta falsa prueba, el Juez podría facilitar la intervención de las comunicaciones, y abrir la puerta a que nos introduzcan un troyano . Y con ese troyano en nuestro equipo, bajar a su vez, archivos indebidos a nuestro ordenador. Y ya tendrían las pruebas (Pruebas falsificadas) para condenarnos por un delito que no hemos cometido.

Pero no nos limitamos a archivos, hay más: También se considera delito ya la agitación en la red.(http://tecnologia.elpais.com/tecnologia/2012/04/11/actualidad/1334142744_604523.html): "delito de integración en organización criminal" por alterar "gravemente el orden público". Y así, otras actuaciones, que podrían encuadrar como actos delictivos (que superen los 3 años de pena máxima), para solicitar la instalación de troyanos en nuestro ordenador.

¿Qué es lo raro que veo en este borrador, lo que más me ha chocado nada más leer las primeras noticias?

Si se quiere perseguir (además de presuntos terroristas) también a cyberdelincuentes avanzados, o hackers , hay que tener en cuenta que estas personas están acostumbradas a proteger sus acciones. El bien más preciado de un experto en seguridad, es el anonimato. No resulta sencillo colarles un troyano, porque de entrada, no suelen usar windows, más bien, suelen usar Linux, unix, y cualquier variante de este sistema operativo.

Sus equipos, suelen estar bien protegidos. Además, suelen conectar de forma anónima, utilizando equipos por medio que oculten su IP (proxys, equipos remotos atacados previamente con esa finalidad, etc), y suelen sus encriptar datos y borrar pistas y registros de actividad. Sus correos, apenas aportan datos útiles. Las redes sociales, salvo casos de elevado egocentrismo ú otra razón no muy común, es poco probable que las utilicen.

El hecho de usar troyanos , ya delata que el perseguidor, no es muy buen "hacker". Está mal visto utilizar herramientas ajenas! El verdadero hacker, explora vulnerabilidades, crea sus herramientas,

etc. De lo contrario, se le llama Lammer. (leim) en el argot.

Quizás tengan pensado utilizan hackers de verdad obligados por este borrador, porque de lo contrario, me temo que tendremos usuarios policías , sin demasiados conocimientos, utilizando un programita cualquiera, diseñado por una empresa, para captar datos, que después, pueden ser interpretados de muchas maneras, o resultar inexactos. Y tampoco una dirección IP identifica a una persona. Solo al propietario de la línea. Que puede que no tenga nada que ver. No es complicado romper hoy en dia una WIFI, sobre todo, las de los usuarios poco técnicos. Quizás, no pretendan cazar hackers o cyberdelincuentes expertos, más bien .. al usuario normal y corriente, usando Windows.

¿Y esto, a quien puede beneficiar?

Con la situación actual, no es difícil imaginarse muchas cosas. Personas que lideran grupos contra el gobierno, líderes de opinión en redes sociales, gente que no interesa tener en la calle No creo que permitan otro 15M. Esto les carta blanca para ir a por cualquiera que no les interese que esté en la calle.

En Alemania, ya se ha hecho (aunque limitado a presuntos terroristas). El Partido Pirata alemán lo denunció en su día (http://www.larepublica.pe/26-03-2013/alemania-partido-pirata-acusa-al-gobierno-de-espiar-con-un-troyano)

En España, también se han espiado las comunicaciones, vía SITEL, un sistema de la compañía Ericsson (http://www.internautas.org/html/5741.html).

Y nadie nos garantiza que no lo estén haciendo ya. Si lo están haciendo, las pruebas obtenidas, no serían probablemente válidas. Quizás, lo que necesiten vaya más allá de controlar la red, el aseguramiento de pruebas válidas.

Vivimos en una situación de mucha tensión y mucho descontento. Es una manera fácil y limpia de librarse de los que molestan. Si no han hecho nada, se hace que parezca. A esto podríamos llegar, si se utiliza de manera inadecuada el borrador propuesto.

No olvidemos, que en dos años habrá elecciones. El PP y el PSOE, bajan cada vez más en intención de voto. Esto deja de ser un riesgo si no quedan muchos más partidos por abajo o no hay gente que proteste.

Teniendo en cuenta que Rajoy puede llegar a quemarse y ser necesario sustituirlo en el partido y que otro tome el relevo, y que Aznar está prácticamente fuera de juego, por ahora, no hay demasiadas quinielas de quien puede ser el sustituto de Rajoy Pero, los juegos de estrategia, que se los monte cada uno a su gusto.

Como siempre, Jaj haciendo amigos. No me gustan los troyanos, espero no tener que pelearme con ninguno.

ANEXO

Párrafos extractados del borrador de anteproyecto de Código Procesal Penal del Ministerio de Justicia como complemento.

VI.- LIBRO IV. PROCESO ORDINARIO

A) LA INVESTIGACIÓN

La reforma opta, frente a otros modelos comparados que acogen una enumeración casuística de los delitos que autorizan este medio de investigación, por exigir la concurrencia, no cumulativa, de cualquiera de los tres requisitos que define el art. 295 de este Código. El primero de ellos, opera como una limitación genérica, de carácter cuantitativo, ligada a la gravedad de la pena delitos dolosos castigados con pena con límite máximo superior a los tres años de prisión-. Junto a este presupuesto se añaden otros dos: a) que estemos en presencia de delitos cometidos en el seno de un grupo u organización criminal; b) que se trate de delitos cometidos por medio de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación.

Unas líneas mas abajo:

El Código pretende completar las perturbadoras lagunas del actual art. 579 de la Ley de de Enjuiciamiento Criminal. En la nueva regulación se confiere sustantividad propia a otras formas de comunicación telemática que han carecido de tratamiento normativo en la ley procesal. Las dificultades asociadas a ese vacío se han visto multiplicadas en la práctica por una interpretación jurisprudencial de la legislación llamada a reglar la obligación de las operadoras de conservar los datos generados por las comunicaciones electrónicas, que ha degradado algunos de los extendidísimos instrumentos de comunicación telemática por ejemplo, los mensajes de SMS o el correo electrónico- a la condición de aspectos accesorios, de obligado sacrificio siempre que se adopte una decisión jurisdiccional de intervención telefónica. Frente a esta concepción, el nuevo texto autoriza la intervención y registro de las comunicaciones de cualquier clase que se realicen a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual. Pero somete la interceptación de todas ellas en su propia y diferenciada instrumentalidad- a los principios generales que el texto proclama. Se pretende con ello que sea el propio Tribunal, ponderando la gravedad del hecho que está siendo objeto de investigación, el que determine el alcance de la injerencia del Estado en las comunicaciones particulares. La resolución habilitante, por tanto, deberá precisar el ámbito objetivo y subjetivo de la medida. Es decir, tendrá que motivar, a la luz de aquellos principios, si el sacrificio de las comunicaciones telefónicas no es suficiente y si la investigación exige, además, la interceptación de los SMS, MMS o cualquier otra forma de comunicación telemática de carácter bidireccional.

Artículo 81.- Obligación de colaboración con la Policía Judicial

Los funcionarios integrantes de la Policía Judicial tendrán el carácter de comisionados del Ministerio Fiscal y podrán requerir el auxilio necesario de las autoridades y de los particulares.

CAPÍTULO XI.- REGISTROS REMOTOS SOBRE EQUIPOS INFORMÁTICOS

Artículo 350.- Presupuestos

1.- El Tribunal de Garantías podrá autorizar, a petición razonada del Ministerio Fiscal, la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma

remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que la medida resulte proporcionada para la investigación de un delito de especial gravedad y sea además idónea y necesaria para el esclarecimiento del hecho investigado, la averiguación de su autor o la localización de su paradero.

2.- La resolución judicial que autorice el registro, además de motivar la idoneidad, necesidad y proporcionalidad, deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios de almacenamiento de datos informáticos o bases de datos y datos informáticos almacenados objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

d) Los agentes autorizados para la ejecución de la medida.

e) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

f) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

Artículo 351.- Deber de colaboración

1.- Los proveedores de acceso o servicios telemáticos y los titulares o responsables del sistema informático o base de datos objeto del registro están obligado a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización.

2.- Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia.

Publicado por jaj en P2Pedia
