El Salvaje Oeste Digital

Michael Crichton escribió y dirigió en 1973 una pieza cinematográfica en la que definía con bastante acierto los límites éticos y morales de la humanidad, ejemplificados en el parque temático Westworld.

Llevada a la pequeña pantalla en dos ocasiones, y seguramente conocida por muchos de los aquí presentes por la reinterpretación que han hecho recientemente Jonathan Nolan y Lisa Joy para la HBO, en Westworld se da rienda suelta, en un entorno controlado, a lo que en el Salvaje Oeste fue el día a día de millones de personas.

Un paraje artificial ocupado por anfitriones, androides indistinguibles de los humanos, para disfrute de los clientes del parque. En el parque un funcionario puede transformarse en un atractivo ladrón de bancos, en un asesino, en un putero, y en definitiva, hacer lo que le venga en gana. Él no puede morir y los anfitriones, como máquinas que son, pueden ser reemplazados cuando la diversión se ha ido de madre.

Un escenario amparado por la Ley del Salvaje Oeste. Si algo no te gusta, eres libre de cambiarlo, utilizando para ello las herramientas que veas oportunas. Con la salvedad de que al menos en este entorno controlado no habrá represalias de las que debas preocuparte.

En estos últimos meses en EEUU, cuna en su momento de este movimiento libertario y hasta cierto punto aún presente en algunas enmiendas de su Constitución, algunas voces se han levantado para reclamar un poquito de Salvaje Oeste en el tercer entorno, que permitiría a particulares y empresas ejercer de jueces y verdugos a la hora de defenderse y contraatacar a cibercriminales.

Y quizá sea que a un servidor la cosa le queda un poco lejos. Que quizá estoy muy influido por el sistema garantista europeo. O que lo mismo le veo más puntos débiles que fuertes. El caso es que me ha parecido interesante que dediquemos esta pieza a hablar de la propuesta, y sobre todo, de todo lo que supondría si al final sale adelante.

Pablo F. Iglesias, Analista de información en PabloYglesias.com y CTO en la consultora SocialBrains @PYDotCom

El principal problema de los ataques digitales es que la fuente de origen no siempre se corresponde con el origen del atacante.

Entendiendo el ACDC

El Proyecto de Ley de Seguridad Cibernética Activa (ACDC por sus siglas) viene a ofrecer a las víctimas de un ataque informático la potestad de acceder a ordenadores ajenos para rastrear a los atacantes y proteger los posibles datos que hayan sido robados en el mismo. Fue presentado por el republicano Tom Graves, aunque encuentra también apoyo en algunos representantes demócratas, como es el caso de Kyrsten Sinema.

En la práctica, hablamos de una suerte de excepción a la Ley de Abusos y Fraudes Informáticos (CFAA), que prohíbe el acceso a ordenadores de terceros sin autorización expresa de sus dueños o del poder judicial. Y antes de que se lleve las manos a la cabeza, es cierto que tiene algunas limitaciones a considerar:

- Has de ser un "defensor cualificado": es decir, solo se aplicaría el ACDC en caso de que hayas sido víctima de un ataque, y además, conozcas la identidad de los atacantes. Algo profundamente complejo de asegurar en un entorno como el digital, pero voy a contenerme un poquito más antes de criticar la medida.
- No se puede usar ninguna técnica que "cause imprudentemente daños físicos o pérdidas financieras": seguramente, con la idea en mente de evitar hacer daño a los que al final van a ser las víctimas reales del contrahackeo (otras víctimas utilizadas como vectores de ataque por los cibercriminales), pero sigamos ☺.
- Queda terminantemente prohibido "excederse intencionalmente" en el ámbito del contrahackeo: vaya, que la excepción solo nos cubre la identificación del atacante, el borrado y protección de los datos que nos hayan sido robados, y si eso el desmantelamiento (que a ver cómo se hace sin "causar imprudentemente daños físicos o pérdidas financieras") de los sistemas y herramientas utilizados por los atacantes. Nada de hacer de justiciero y liarnos a tiros (binarios) por el Salvaje Oeste Digital.
- El FBI debe estar al tanto: para terminar, es necesario que antes de empezar con ello, alertemos a los cuerpos del orden de la situación. Eso sí, no hace falta esperar respuesta alguna por su parte.

Entendiendo cómo funciona el tercer entorno

Todo suena genial hasta que comprendes un poco cómo funciona el mundo digital.

Primero de todo, querría que me explicara usted cómo diantres vamos a saber de antemano quién es el atacante. O ya puestos, cómo vamos a identificarlo en un ecosistema basado cada vez más en el Crime As A Service. El principal problema de los ataques digitales es que la fuente de origen no siempre se corresponde con el origen del atacante. Que, de hecho, esta es la principal razón de por qué resulta tan complicado declarar la guerra a un país por un hackeo, pese a que todo apunte aparentemente a un país "enemigo".

Lo hemos visto estos últimos años con los continuos ataques (aparentes) entre EEUU, Europa, Rusia y China. Que si Rusia ha interferido con mecánicas de propaganda en las elecciones democráticas de EEUU y varios países europeos, que si China ha lanzado a sus "hackers" contra los servidores de grandes multinacionales occidentales...

La cuestión es que no hay certeza absoluta en el tercer entorno de que un atacante es Pepito o es Menganito. Lo que si podemos hacer es intentar seguir las migas de pan que los malos hayan ido dejando, y para ello, me temo que vamos a tener que entrar en dispositivos que presumiblemente serán de otras víctimas, haciéndoles por tanto daño también a ellas.

Lo que me lleva al segundo punto. ¿Qué consideramos un "defensor cualificado"? Habida cuenta de que la mayoría de ataques se ejecutan con la idea de que la víctima no sea consciente de ello, ¿es entonces un "defensor cualificado" aquel que intuye que podría haber sido víctima de un hackeo? Porque entonces ya le digo que usted, y un servidor, somos "defensores cualificados". Ni siquiera tengo la intuición, sino la certeza absoluta de que he sido víctima de algún ataque a lo largo de mi vida en Internet. Y no tengo ni idea de quién ha sido el beneficiario de tamaña empresa, pero lo que sé

El Proyecto de Ley de Seguridad Cibernética Activa (ACDC por sus siglas) viene a ofrecer a las víctimas de un ataque informático la potestad de acceder a ordenadores ajenos para rastrear a los atacantes y proteger los posibles datos que hayan sido robados en el mismo.

fijo es que por ahí hay unos “alguienes” que se han lucrado a mi favor.

Lo que en la práctica hace que cualquiera que quiera pueda ejercer una suerte de justicia limitada por su cuenta. Un pequeño Salvaje Oeste Digital, que comentaba en el título de esta columna.

Para colmo, me diga usted también qué consideramos “causar daños imprudentemente” de aquellos que podemos considerar accidentales. Si al entrar en una cámara IP exploto el protocolo de comunicación, y de paso me cargo el termostato de una casa que hace subir desproporcionadamente la factura de ese mes, ¿cómo demostramos que ha sido imprudentemente o con conocimiento de causa? ¿Y si al bloquear un puerto estoy activando una alerta que acaba por comprometer la seguridad física de una potabilizadora de agua? Lo mismo lo he hecho sin querer, o quizás mi intención era perjudicar a los supuestos cibercriminales para que aprendan, a sabiendas que habrá daños colaterales.

Pero si hay algo que me preocupa aún más, es que de sacarse adelante el Proyecto de Ley, el escenario se volvería más nocivo de lo que es a día de hoy. Porque dígame en qué país se ha reducido la delincuencia gracias al uso de las armas, qué tal le ha ido a cualquier Estado que ha decidido aplicar la mano dura para solucionar un problema armado, como puede ser el terrorismo o la industria de la droga.

Permitir justicieros en el tercer entorno es abrir la veda a que lo que ha sido un daño económico (robo de datos, secuestro de activos informáticos...) se pueda volver algo bastante más grave.

Que nunca ha sido buena idea seguir a los ladrones hasta su casa, más que nada porque vaya usted a saber con quién nos vamos a encontrar allí.

Recuerde que hablamos de personas sin escrúpulos, con un sentido de la ética y la moral que dista mucho de la del grueso de la sociedad.

Descontando, por supuesto, que en el tercer entorno el alcance de los ciberataques es global, entrando en juego por tanto diferentes jurisprudencias donde muy probablemente, de realizar un contraataque, sí estemos incumpliendo la ley.

En definitiva, con lo que quiero que se quede es que al menos como está planteado el ACDC actualmente, conlleva una serie de riesgos que claramente superan a las ventajas que tendría.

Hay, no obstante, algún punto fuerte que sí me parece interesante mencionar, como es el hecho de que las empresas y particulares estén obligadas a informar del ataque, y que los cuerpos del orden tengan también la obligación de elaborar un informe anual con el número de recursos e investigaciones abiertas que tienen sobre la mesa.

En definitiva, de ser más transparentes. Algo que ha demostrado por activa y por pasiva sí ser una gran herramienta para minimizar el impacto del cibercrimen.

Mayor coordinación entre jueces y policías. Mayor interoperatividad entre diferentes jurisprudencias. Mayor rapidez a la hora de dar caza a los malos. Pero todo por parte de aquellos que tienen las herramientas y el conocimiento necesario para hacerlo, además de las garantías adecuadas.

Permitir justicieros en el tercer entorno es abrir la veda a que lo que ha sido un daño económico (robo de datos, secuestro de activos informáticos...) se pueda volver algo bastante más grave.