>> Jorge Dávila

Hackers: estuvo bien mientras duró

Los escenarios "Ciber" empiezan a moverse más deprisa. Las empresas y el ciudadano van tomando conciencia del peligro al que están expuestos y cómo esos ataques reducen su porción de la riqueza generada. La demanda de profesionales en la defensa y quizás en el ataque está despertando una nueva profesión, un nuevo gremio que unos quieren encauzar como a todos los anteriores, y para el que otros preconizan algo distinto. La Rooted CON levantó la liebre y es bueno que hablemos aquí de ello.

En la pasada sesión de Rooted CON la Comunidad nacional *Hacker* hizo una revisión de sus más recientes logros en multitud de temas. Lo tratado fue desde cómo ampliar el arsenal de ataque WiFi, hasta cómo encontrar "*stegomalware*" en los millones de *apps* que nutren las ciber-kasbas de Android y Apple, pasando por las infecciones de las BIOS (algo así como el envenenamiento esencial y ontológico del alma de un PC), la Ingeniería inversa de circuitos integrados y el desarrollo y operaciones de la APT conocida como Turla, entre muchas otras.

Al final del primer día se celebró una mesa redonda en la que sus organizadores intentaron establecer qué es eso de ser un *hacker* y si había que darles un carnet como tales. Los puntos de vista de la tertulia fueron muy variados; desde el enfoque de un socio de una importante consultora *big four*, al del fundador de la Rooted COM, pasando por el del Servicio de Criminalidad Informática de la Fiscalía General del Estado, el del Grupo de Delitos Telemáticos de la Unidad Central Operativa de la Guardia Civil, el de varios representantes de empresas de seguridad de nuestro país y el mío. La mesa redonda fue un tanto caótica y no se centró necesariamente en las preguntas de los moderadores (Revista SIC), lo que hizo que la temática tratada fuera más extensa y variopinta.

En Rooted CON se identificaron dos propuestas esencialmente distintas; la de una visión romántica del hacker individual, que con pensamiento lateral y apasionado por la tecnología busca el modo de hacer con ella cosas distintas o hacerlas mejor. Y la otra, más moderna, que es la del Consultor de Seguridad en la que su definición profesional uniformiza a todos ellos y los prepara para actuar coordinada y cooperativamente dentro de un mercado como el actual.

Dos visiones del *hacker*

Empezando por el *mea culpa* o auto-identificación como *hacker* o no de cada uno de los miembros de la mesa, pronto saltó la frecuente y reiterada cuestión de qué es "ser *hacker*" y qué no lo es. En este punto se identificaron dos propuestas esencialmente distintas; la de una visión romántica del *hacker* individual, que con pensamiento lateral[1] y apasionado por la tecnología busca el modo de hacer con ella cosas distintas o simplemente hacerlas mejor. Y la otra visión, más moderna, que es la del Consultor de Seguridad en la que su definición profesional uniformiza a todos ellos y los prepara para actuar coordinada y cooperativamente dentro de un mercado como el actual.

Frente al individualismo del *hacker* creado por la cinematografía, el periodismo generalista y sensacionalista y por algunos personajes a título particular, se planteó si lo que la sociedad va a necesitar son héroes o villanos individuales, o grupos bien entrenados de profesionales capaces de moverse con soltura y naturalidad en los "escenarios Ciber" (-crimen, -defensa, -guerra, -delincuencia, -activismo, etc.).

El "miedo Ciber" y su reiteración en los medios generadores de opinión en las masas permite augurar un dulce futuro, más que a los hackers, a los profesionales del hacking que sepan trabajar en grupo, estandarizar sus modos de actuación, comunicar adecuadamente sus resultados y demostrar incluso más lealtad y compromiso con un fin colectivo que en otras profesiones.

Dado el grado de dependencia de la sociedad moderna en los sistemas de comunicación de información y de almacenamiento digital, cualquier ataque a esa médula espinal de Occidente es un ataque a toda la sociedad, y sus efectos pueden llegar a ser muy extensos. El "miedo Ciber" y su reiteración en los medios generadores de opinión en las masas permite augurar un dulce futuro, más que a los *hackers*, a los profesionales del *hacking* que sepan trabajar en grupo, estandarizar sus modos de actuación, comunicar adecuadamente sus resultados, y demostrar incluso más lealtad y compromiso con un fin colectivo que en otras profesiones.

Los problemas que ya se nos han planteado y que desde luego nos asaltarán mañana, no son la obra de un atacante individual tímido, un poco inadaptado, ligeramente ciclotímico, a veces genial, muy creativo, y para sí mismo "único". Lo que ya se está viendo es la obra de grupos bien organizados, con pautas casi funcionariales y disciplinas militares, por lo que no es de extrañar que la respuesta deba y vaya a ser de esa misma naturaleza.

La evolución de la Ciberdefensa

Si vemos cómo ha evolucionado en estos últimos diez o quince años lo que ahora llamamos abiertamente Ci-

[1] Ver http://es.wikipedia.org/wiki/Pensamiento_lateral

berdefensa, nos llevaremos la sorpresa de que han sido las empresas y no los Estados nacionales los que colman el escenario real de los ciber campos de batalla.

Cuando el general de tres estrellas **Keith B. Alexander** asumió el cargo de Director de la NSA puso todos los recursos de esa supersecreta agencia al servicio del control cibernético. Durante su mandato, el mayor comprador planetario de Zero-Days fue la NSA, el mayor arsenal de defectos desconocidos de programación de todo el mundo lo tenía y atesoraba la NSA, y ello incluso aunque todos ellos supusiesen un peligro inconmensurable para el país que había hecho de Internet su cualidad económica diferencial respecto al resto del mundo.

En sus años de mando, el general Alexander actualizó el masivo sistema de escuchas e intercepciones que desde siempre ha tenido esa agencia, para convertirlo en un sistema de sondas que vigilasen todo el tráfico digital y que diesen la alarma cuando hubiese actividades telemáticas consideradas por ellos "amenazadoras". La NSA llegó a presumir de ese secretísimo *know-how* plasmado en sus reglas de IDS y llego a considerarlo su más preciado tesoro. Sin embargo, cuando llegó la hora de la verdad, la mayoría de esas reglas estaban obsoletas y eran mucho menos precisas/eficaces de lo que sus creadores y propietarios creían. Por si eso fuera poco, en esos mismos escenarios que hoy llamamos APTs, los mejores resultados lo conseguían compañías privadas (Kaspersky Lab, Mandiant, FireEye, Symantec, Check Point, etc.) y no entidades gubernamentales.

Para los Estados Unidos de Norteamérica su defensa, su capacidad de fabricación de armas, siempre ha estado en poder de un complejo industrial privado liderado y alimentado por los masivos fondos y recursos financieros que la Administración norteamericana dedicaba a ello. Sin embargo, el escenario Ciber no requiere de tan espectaculares cantidades de dinero para poder jugar y jugar fuerte. Por ello, la iniciativa privada ha entrado en escena desde el principio y se ha movido con una libertad que Lockheed Martin, Northrop Grumman, Raytheon y Booz Allen Hamilton nunca han tenido a la hora de diseñar misiles, tanques, bombas y multitud de artefactos creados para matar y matar mucho.

El liderazgo en el ciberespacio no está en las manos de Estados nacionales, al menos en las sociedades occidentales, y han sido las empresas las que han tenido que aprender sobre la marcha cómo defenderse de los diferentes y múltiples ataques que durante estos años han sufrido. La mayor parte del conocimiento ciberdefensivo se encuentra almacenado, cristalizado en las experiencias de esos trabajadores de seguridad IT que han visto crecer la amenaza en sus propias carnes.

El liderazgo en el ciberespacio no está en las manos de Estados nacionales, al menos en las sociedades occidentales, y han sido las empresas las que han tenido que aprender sobre la marcha cómo defenderse de los diferentes y múltiples ataques que durante estos años han sufrido. La mayor parte del conocimiento ciberdefensivo se encuentra almacenado, cristalizado en las experiencias de esos trabajadores de seguridad IT que han visto crecer la amenaza en sus propias carnes.

Tomemos como ejemplo sencillo de ello los famosos CERTs, que empezaron 1988 en la Universidad Carnegy Mellon para combatir el famoso Gusano de Morris[2]. Las primeras líneas de defensa se establecieron, mano a mano, entre Universidades e instituciones del Ministerio de Defensa como el DARPA[3]. Más tarde, cuando las compañías privadas aterrizaron en Internet, a esta corriente se unieron los departamentos de seguridad IT de algunas grandes empresas.

Esta falta de protagonismo de los estados en el ciberespacio hace que proliferen compañías, también privadas, que **al más puro estilo mercenario lideran las capacidades ciberofensivas**[4] como es el caso de **Gamma International Group**[5] de Reino Unido y Alemania, la compañías francesas **Vupen** y **Amesys**, el **Hacking Team** de Italia, **Trovicor** en Alemania, **Blue Coat Systems**, **Endgame** y **CrowdStrike** en los EE.UU.; todas ellas venden productos que sólo pueden ser utilizados por gobiernos y grandes corporaciones, para violar los derechos humanos y la libertad de información.

Los estados defienden mal pero atacan muy bien, per se o gracias a los cibermercenarios que contratan al más puro estilo Blackwater; en ese caso, tanto ciudadanos como empresas, estamos tan solos como David delante de Goliat.

Guerras Cibernéticas y ejércitos privados

No sería de extrañar que un día de estos, algún equipo de ciberdefensa caiga en la tentación de lanzar un ataque como represalia y que con ello se inicie una era de **"Guerras Cibernéticas" desarrolladas por y entre ejércitos privados**, sin que haya una necesaria correlación o connotación nacional. En ese escenario, los Estados Nación habrán fracasado en su misión de proteger a sus ciudadanos y retornaremos a un modelo político en Internet más propio de la Italia renacentista, o incluso llegar a adoptar una organización medieval como es el caso de la Cosa Nostra[6].

Otra cosa muy distinta es si esos Estados Nación actúan como atacantes y sus Agencias de Inteligencia se convierten en recolectoras de Inteligencia Comercial o *Business Intelligence*. En ese caso, las capacidades económicas de los estados superan ampliamente a las del cibercrimen, y ellas seguirán adelante allí donde los criminales desistan de hacerlo. **Los estados defienden mal pero atacan muy bien, *per se* o gracias a los cibermercenarios que contratan** al más puro estilo **Blackwater**[7]; en ese caso, tanto ciudadanos como empresas, estamos tan solos como David delante de Goliat[8].

Un nuevo mercado profesional

Con este panorama es fácil entender que estemos ante un nuevo mercado profesional en el que la imagen de los

[2] Ver http://es.wikipedia.org/wiki/Gusano_Morris
[3] Ver http://www.darpa.mil
[4] Ver "Era of the digital mercenaries" http://surveillance.rsf.org/en/
[5] Ver http://surveillance.rsf.org/en/gamma-international/ y https://www.gammagroup.com/
[6] Ver http://es.wikipedia.org/wiki/Cosa_Nostra
[7] Ver http://en.wikipedia.org/wiki/Academi
[8] Ver http://blog.norsecorp.com/2015/03/10/enterprise-security-vs-nation-state-threat-actors/

hackers clásicos languidezca para dejar pasar a la visión de miles de consultores uniformizados intentado defender el patrimonio de sus contratantes y atacar los intereses de los enemigos o competidores de quién les paga.

El sistema educativo todavía debe evolucionar para poder atender a las necesidades Ciber. Las universidades, en general, no están sabiendo reconocer este nuevo ciberescenario y, por ello, no están dando soluciones nuevas y válidas para esta incipiente necesidad.

La pregunta es quién va a formar a estos profesionales. En principio, lo razonable será pensar que esos trabajadores los formaran las mismas instituciones que forman a todos los demás, esto es, las Universidades. Sin embargo, es cierto que las universidades, en general, no están sabiendo reconocer este nuevo ciberescenario y, por ello, no están dando soluciones nuevas y válidas para esta incipiente necesidad.

La formación de esos nuevos "Consultores" requiere de una inmediatez, y en cierto modo volatilidad, que no se llevan bien con las técnicas docentes a medio y largo plazo que dominan las instituciones académicas de todo el mundo. Esos futuros consultores de seguridad serán profesionales que requieran una frecuencia de reciclado, actualización o puesta al día en lo que a sus conocimientos y experiencias se refiere, mucho mayor que en otras profesiones ya que la dinámica en el ciberespacio así se lo exige. **La experiencia con fuego real es un componente muy importante en la ingeniería "Ciber"** y eso colisiona frontalmente con los sistemas educativos basados en clases magistrales e incluso con el paternalista modelo de Bolonia. El sistema educativo todavía debe evolucionar para poder atender a las necesidades Ciber.

El entrenamiento *hacker*

El entrenamiento *hacker* requiere de un esfuerzo y dedicación superior al de las formaciones generalistas que conocemos, por lo que tampoco es de esperar que sean muchos los alumnos que superen con éxito esos entrenamientos. De hecho, ya desde hace tiempo, la demanda de buenos "Consultores de Seguridad" es muy superior a la de informáticos de otras ramas, y sin embargo queda desierta porque la oferta con buena calidad es muy escasa. No sería de extrañar que en el siglo XXI sea más trabajoso hacerse buen Consultor de Seguridad, que Notario, Juez, Técnico de la Administración del Estado o Registrador de la propiedad.

El polémico futuro Reglamento de Desarrollo de la Ley de Seguridad Privada

Otro tema que se trató en la mesa redonda fue el del amenazante y futuro Reglamento de Desarrollo de la Ley de Seguridad Privada. Según parece, se pretendería que las empresas de "Seguridad Informática", voluntariamente, puedan darse de alta en un registro del Ministerio del Interior y, después de pagar las sempiternas tasas, se autoobligaran a remitir las alertas que conozcan al MIR de manera periódica y nada más.

Está claro que algo falla en estos rumores ya que no es lógico que una empresa o un profesional de la "seguridad informática" vaya voluntariamente a registrarse ante la Administración pública para obligarse a algo y no recibir nada a cambio. Otra cosa es que sea obligatorio o que se disfrace como carnet profesional y se hable de las un tanto antiguas competencias profesionales.

El sinsentido de los carnets

Aunque esto de dar carnets, licencias y patentes es un clásico de la seguridad física, no tiene sentido en el mundo informático. Tales credenciales son propias de aquella situación en la que un organismo ostenta en exclusiva una potestad y la administra mediante autorizaciones. Es ingenuo y a la vez preocupante que el Ministerio del Interior de cualquier país o países se crea con la potestad y la exclusiva de la seguridad en Internet porque en realidad no la tienen. La aceptación de esas credenciales sólo serviría para distinguir "***legales***" de "***ilegales***", lo cual **sumergiría a gran parte de la actual Comunidad *hacker* en *undergroud***. En esas circunstancias los resultados de esa comunidad ilegal sólo podrían tener salida a través de organizaciones criminales, lo cuál sería un desperdicio.

Las certificaciones y acreditaciones

Cuando el contratante sea la Administración pública, necesitará un baremo para evaluar a los candidatos y dentro de ese proceso estarán las certificaciones y acreditaciones públicas que la Administración fijará para ello. Sin embargo, en el mundo empresarial, será la demanda del mercado la que encontrará el modo de saber si un candidato está capacitado o no para lo que se postula o se le contrata. En ambos casos las acreditaciones serán completamente distintas y los encargados de darlas no tendrán nada en común. Cuál de ellas sea más importante y atractiva, al final dependerá de cual sea la que más contrate y en mejores condiciones.

Son tantas las cosas que hay que hacer, ver, entender, sufrir y arreglar en esto que llaman Ciberespacio, que lo más importante no es preocuparse por carnets gremiales o patentes de corso de uno u otro Ministerio, ni por posibles uniformes corporativos acompañados de un himno o de las fiestas patronales homologadas. Esto del Ciber o lo que sea se está poniendo cada vez más interesante. Los hechos van por delante de las capacidades de la sociedad que los sufre y el que no quiera verlo, ¡Allá él o ella! ■

La formación de esos nuevos "Consultores" requiere de una inmediatez, y en cierto modo volatilidad, que no se llevan bien con las técnicas docentes a medio y largo plazo que dominan las instituciones académicas de todo el mundo. Esos futuros consultores serán profesionales que requieran una frecuencia de reciclado, actualización o puesta al día en lo que a sus conocimientos y experiencias se refiere, mucho mayor que en otras profesiones ya que la dinámica en el ciberespacio así se lo exige.

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es