Texto
Rufino Contreras

UN COLECTIVO ESENCIAL PARA AFRONTAR CON ÉXITO LA CIBERGUERRA

La mágica sombra del hacker

<< Son los cruzados de la cibercausa, imprescindibles aliados de las empresas en su lucha contra el malware. Les persigue una leyenda negra de la que se están sacudiendo a fuerza de formación, trabajo y evangelización. Representan nuestra esperanza blanca frente a las oscuras fuerzas del mal. Adentrémonos en el fascinante mundo de los hackers.

Hace un año el mundo quedaba conmocionado con el ransomware más dañino de la historia, Wannacry, que tuvo en suspenso a grandes empresas y organizaciones públicas. Tras varias horas de alerta e incertidumbre, salió a la luz un joven británico, Marcus Hutchins, que consiguió desactivarlo, infectando su propio equipo y comprando un dominio al que redireccionaba el virus. Solo necesitó 11 dólares. Pero su aureola de superhéroe global se fue al traste al conocerse sus actividades lucrativas como asaltador de tarjetas de crédito y cuentas bancarias. Fue arrestado por la policía en Los Angeles. Hutchins se une a un elenco de ciberdelincuentes notables como el mítico Kevin Mitnick que tras siete años de cárcel pasó del Black Hat al White Hat y fundó su propia compañía; o la joven Kristina Svechinskaya, apodada por los medios como la 'hacker más sexy del mundo'. Hay mucha leyenda en torno a este grupo de expertos del sombrero negro, capaces de hacer dinero fácil y con un talento especial, considerados como los Billy The Kid o Jesse James redivivos.

Pero los tiempos han cambiado y los ciberdelincuentes de ahora prefieren trabajar asociados y ampararse en el anonimato; nada de personalismos, eficacia e impunidad son sus señas de identidad. Esto ha hecho que la palabra hacker haya venido impregnada de connotaciones negativas y los white hats han tenido que lidiar con la mala prensa que todavía les persigue.

Enrique Serrano, hacker ético, reconoce en este punto la leyenda negra: "Cuando la gente escucha la palabra hacker se asusta. Pero nos gusta diferenciar entre hackers y cibercriminales. Los dos tienen grandes habilidades, pero los primeros las utilizamos para hacer el bien y

los segundos para hacer el mal. La línea entre ellos es muy fina y fácil de sobrepasar".

Yanko Kólev, ingeniero informático de Stackoverflow, narra al respecto una anécdota muy ilustrativa: "Durante un vuelo reciente, una señora me preguntó mi motivo del viaje. Le respondí que había estado trabajando en un proyecto del Gobierno para fomentar la igualdad laboral dando clases a un grupo de chicas que se denominaba Hacker Girls. Ella me contestó escandalizada: ¡Cómo es posible que el gobierno apoye la delincuencia!, y tuve que explicarle que lo que pensaba no era tal".

Para Carlos Lourero, otro ingeniero vinculado a Mundo Hacker Team, el concepto de hacking ético no está vinculado con la leyenda negra, "más bien surge del código ético que debe tener todo hacker, solo que parece que al hablar de hacker ético hacemos hincapié en que posee dicho código cuando realmente todo hacker debe tenerlo".

Kólev está convencido de que es un término inventado para poder hablar políticamente correcto y no escandalizar a los participantes en las reuniones de trabajo y el público en general. En cualquier caso, el adjetivo ético es aborrecido, como puntualiza Yago Hansen, un gran conocido de este mundillo, por la necesidad de justificar permanentemente una labor que es legal: "Un criminal es un criminal, sea hacker, carterista o de cualquier profesión".

Cualquiera no vale para ser hacker

Otra aserción que no tiene discusión es que cualquiera no puede ser hacker, pese a que siempre hay un 'lamer' sin fundamento que quiera llamar atención. La comparación de soldado o de médico es la que más se ajusta a su perfil, pero especialmente se pondera que tenga gran capacidad de aprendizaje y que adore su profesión. "Además de los skills personales mencionados, se necesitan importantes conocimientos técnicos, en lenguajes de programación, informática y electrónica. Muchos expertos de seguridad IT no deben ser considerados hackers, ya que solo se dedican a asesorar a empresas y organizaciones sobre políticas de cumplimiento de normativas y a utilizar herramientas desarrolladas por otros. Sin embargo, estos expertos en seguridad son totalmente necesarios en el esquema actual de seguridad", diferencia Hansen.

Lo que es evidente es que el hacker es el gran aliado actual de las empresas por su aproximación más creativa y conocimiento del terreno black hat; su labor va creciendo en importancia, de la misma manera que va a ser un rol muy demandado en los próximos años. Pero la carencia de talento en este ámbito empieza a preocupar. Lo cual no es óbice para que no sea una profesión tan bien pagada como se merece salvo casos rutilantes como el de Chema Alonso, CDO de Telefónica. Hackers consultados señalan una horquilla de entre 45.000 y 80.000 euros brutos al año en España, un sueldo bastante inferior al de otros países, donde su consideración es mayor.

Las cloacas de la red oscura

De lo que tampoco pueden desprenderse los hackers es de su etiqueta que genera 'cierta fascinación', por tratarse de profesionales que respiran las cloacas del Internet oscuro. Bajar a los sustratos de la dark net y la deep web "es una necesidad que surge en tanto en cuanto busca formarse y aprender", matiza Carlos Loureiro. Abunda documentación en ambos sitios, que no solo se inscribe dentro del ámbito de

GLOSARIO

BLACK HAT: Grupo de piratas informáticos dedicados a robar información y desarrollar malware. Se dividen en crackers y phreakers.

CRACKER: Dícese del ciberdelincuente dedicado a modificar el software y romper sistemas de seguridad.

DARK NET: Colección de tecnología para compartir información y contenidos digitales de forma anónima.

DATALEEK: Fuga de datos.

DEEP WEB: Es el contenido de Internet que no está indexado por los motores de búsqueda convencionales, debido a diversos factores.

LAMER: Se trata de una persona que presume de tener unos conocimientos de hacking y que carece de ellos.

PHREAKER: Manipula sistemas telefónicos para obtener algún tipo de beneficio como llamadas gratuitas.

RANSOMWARE: Malware que encripta los archivos de un equipo y pide un rescate para reponer la información original.

WHITE HAT: Hackers de sombrero blanco, se dedican a detectar vulnerabilidades para proteger los sistemas corporativos.

la formación técnica (programación), sino que también muchos ciberdelincuentes comparten piezas de código o bien se encuentran disponibles principalmente en la red oscura. Esto permite al hacker aproximarse a la forma de pensar de un cibercriminal con la finalidad de entender cómo realiza el ataque y, de esta manera, minimizar los ataques o incluso anticiparse a futuras evoluciones de código dañino.

Y el morbo se acentúa en aquellos casos cuyo celo profesional ha llevado a algún hacker a temer incluso por su vida o ser represaliado de alguna forma, por haber cruzado ciertas líneas rojas tras sacar a la luz información muy sensible. Es el caso de Edward Snowden y Assange, los cuales traspasaron dichos límites por medio de filtraciones de información o dataleaks, y se han consagrado como paradigmas de la rebelión individual contra los férreos centros del poder.

Por otro lado, el anonimato y la salvaguardia de estados como Rusia o China son las ventajas de los cibercriminales, lo cual hace desigual el combate. Y es que dichos ataques son muy rentables, como es el caso de las injerencias rusas a través de bots en Twitter y la difusión de las noticias falsas, por la confianza de los usuarios que siempre están con la guardia bajada. En general, en muchos países 'libres' se hace lo mismo con menor intensidad o de forma oculta. Yago Hansen opina que "la lucha contra el terrorismo, o contra el delito, no es suficiente razón como para violar el derecho universal a la privacidad personal de toda la ciudadanía. Los gobiernos utilizan cada vez más hackers o herramientas desarrolladas por hackers para realizar este tipo de vigilancia".

La sensación general de la población es que estamos indefensos, siempre a rebufo de los ataques de los malos. Los hackers consultados son conscientes de esta circunstancia, "dado que el factor beneficio de las compañías también fuerza a que no se invierta lo suficiente en el desarrollo seguro antes de vender un producto"; por tanto, saben que "el objetivo está en reducir al máximo posible el tiempo que separa un nuevo ciberataque de su solución". Pero claro, los hackers pueden pensar como black hats y eso les da un plus a la hora de entrever nuevas vías de ataque. Frente a un cierto fatalismo, Enrique Serrano apela a las nuevas herramientas de inteligencia artificial que "están haciendo auténticas maravillas, detectando comportamientos anómalos e incluso aprendiendo de los usuarios para reconocer malware y otros aspectos relacionados".

Pero en este punto, cabe preguntarse qué IA es mejor, la de los buenos o la de los malos. Yanko Kólev se decanta por la inteligencia artificial de la industria legal y que es la que más recursos invierte, "que para ello se necesita mucho tiempo de desarrollo y despliegue de infraestructuras grandes. Lo que no quita la posibilidad de que los malos sean infiltrados y tengan su capa ingeniosa de valor añadido".

En cualquier caso, la guerra no está perdida y aunque a los medios generalistas gustan de titulares apocalípticos, la seguridad es algo tan sencillo como educar y concienciar a las personas, tareas en las que este colectivo de hackers ético está muy implicado.

Explicando y enseñando a la población sobre los riesgos informáticos como páginas http versus https, contraseñas fuertes que se cambian regularmente, uso de antivirus y otras buenas prácticas, se puede mitigar el impacto del malware sobre las personas y la economía en general. A esto hay que añadir la gran cantidad de publicaciones, blogs, charlas y programas de TV que abundan en Youtube.

Los hackers no son omnipotentes pero son nuestros grandes paladines en la lucha contra el mal. Y las leyendas no hacen más que engrandecer su sombra. Una nueva anécdota de Yanko Kólev pone el broche en este sentido: "Un día, dando clase a unos alumnos de un país africano, me preguntaron si podía extraer información de un ordenador sin encenderlo. Les dije que era técnicamente imposible. Ellos afirmaron que su chamán sí podía hacerlo". ■

"El hacker es el gran aliado actual de las empresas por su aproximación más creativa y conocimiento del terreno black hat"