Nadie está a salvo de los ataques de los ciberdelincuentes

# ANTONIO SALAS

## LOS HOMBRES QUE SUSURRAN A LAS MÁQUINAS

Hackers, espías e intrusos en tu ordenador


ESPASA

Antonio Salas

# Los hombres que susurran a las máquinas

ESPASA



Depósito Legal: B. 23.963-2015
ISBN: 978-84-670-4621-2



Espasa, en su deseo de mejorar sus publicaciones, agradecerá cualquier sugerencia que los lectores hagan al departamento editorial por correo electrónico: sugerencias@espasa.es.

www.espasa.com
www.planetadeloslibros.com
Impreso en España/*Printed in Spain*
Impresión: Unigraf, S. L.

El papel utilizado para la impresión de este libro es cien por cien libre de cloro y está calificado como **papel ecológico.**

Espasa Libros, S. L. U.
Avda. Diagonal, 662-664
08034 Barcelona

Índice

Prefacio. Ladrones de vidas ..... 15

*Octubre de 2014. Matar a Antonio Salas* ..... 19

PARTE I

Capítulo 1. Los secretos están en el aire ..... 25
Después de *Operación Princesa*. Octubre de 2013 ..... 25
Una nube de secretos en el aire ..... 28
Juan vs. David: un hacker en el CNI ..... 31

Capítulo 2. Red de mentiras ..... 41
Solo por que mil voces lo repitan, no necesariamente es verdad ..... 41
Un altavoz de mentiras ..... 45
Chávez muere en la red: un golpe digital a la credibilidad de los medios ..... 47
Del *hoax* de SM la reina, a la Wiki War: la información como propaganda ..... 50

PARTE II

*5 de marzo de 2014. Objetivo Tiger88* ..... 59

Capítulo 3. Internet: el invento que revolucionó la historia ..... 63
La rueda del siglo xxi ..... 63
Un gran poder implica una gran responsabilidad ..... 66

Policías 2.0 ..... 70
*Hackstory* ..... 73
Ya estamos en Matrix ..... 75

*Marzo de 2014. El cachorro de UltraSSur* ..... 85

Capítulo 4. Inmigrantes digitales en una red más segura ..... 92
El mejor antivirus eres tú. Tu mayor vulnerabilidad, también .. 92
X1Red+Segura ..... 96

*Abril-Agosto de 2014. Propaganda fascista en la red* ..... 102

Capítulo 5. El yihad informático ..... 110
El día que Boko Haram descubrió internet ..... 110
Ramadán de 1435 en El Príncipe ..... 112
El Diablo en tu teléfono móvil ..... 119

*Octubre de 2014. Desaparecido* ..... 124

Capítulo 6. Los guardianes de la reputación *online* ..... 126
El Celebgate ..... 126
OnBranding, guardianes de tu reputación digital ..... 129
Cuando los casos reales superan a la ficción ..... 138

*Octubre de 2014. La confesión* ..... 144

Capítulo 7. Los *whitehats* de la Guardia Civil ..... 151
En el GDT del capitán Lorenzana ..... 151
Operaciones contra el cibercrimen ..... 156
Cómo usa tu ordenador la industria del cibercrimen y cómo puedes ponérselo difícil ..... 160

*Octubre-Noviembre de 2014. MarkoSS88: un preso político* ..... 168

Capítulo 8. Los hackers de ETA ..... 177
Terrorismo vasco en la red ..... 177
Ertzaintza 2.0. ..... 182

*Noviembre de 2014. Silvia, la novia de MarkoSS88* ..... 187

Capítulo 9. Estafados en internet ..... 190
Estafas en serie en la red ..... 190
*Ransomware*: el cibertimo de Correos ..... 192

Roi, un estafador en serie ..... 195
Los falsos Antonio Salas ..... 198

*Finales de noviembre de 2014. La pista okupa* ..... 203

Capítulo 10. Esteganografía, hacking wifi y espionaje ..... 209
CyberCamp: «Buscamos talentos» ..... 209
Hacking wifi ..... 212
Esteganografía: hacking para espías ..... 214
«¡Antonio Salas! ¿Qué haces aquí?» ..... 216

*Mallorca. Navidad de 2014. Compasión por un neonazi* ..... 219

Capítulo 11. La Comunidad hacker ..... 223
Hack&Beers ..... 223
«En local funciona» ..... 227
«No todo el hacking es software»: el pensamiento lateral ..... 230

PARTE III

*Enero de 2015. Soraya, la nueva novia de MarkoSS88* ..... 239

Capítulo 12. Operación Charlie Hebdo ..... 243
El ISIS ataca en el París del Chacal ..... 243
Geografía del terror ..... 247
Anónymous y su #OpCharlieHebdo ..... 250
«Je Suis Charlie» vs. «Je Suis Ahmed» ..... 256
La conexión española ..... 262

*Enero de 2015. El arrepentimiento de MarkoSS88* ..... 267

Capítulo 13. Perfiles falsos para ligar en la red ..... 268
La estrategia del miedo ..... 268
Hackeando las mentiras de Roi en FITUR ..... 271
La red creó el problema, y también la solución ..... 277

*Febrero de 2015. Geolocalizando a MarkoSS88* ..... 283

Capítulo 14. Los hackers del Estado Islámico ..... 288
La caída del Temible Pirata Roberts ..... 288
Historia del espionaje ..... 292
ISIS: terrorismo en línea ..... 294

Yihad 2.0 ..... 299
No en mi nombre ..... 301

*Febrero - Marzo de 2015. La pista policial* ..... 303

Capítulo 15. Espionaje y Ciberdefensa ..... 307
Mauro, el pequeño espía ..... 307
Ciberdefensa ..... 309
Defensa del ciberespacio nacional ..... 316

*Marzo de 2015. El skin que borra los metadatos* ..... 322

Capítulo 16. Viaje a la Deep Web ..... 324
Hacker antes que guardia civil ..... 324
TOR: el pasaporte a una ciudad sin ley ..... 326
Policías en la red profunda ..... 332
Operación Cool Daddy: cazar a un monstruo en ocho días .... 345

*Abril de 2015. Silvia Hierro no existe* ..... 350

Capítulo 17. RootedCON y las vulnerabilidades de la banca ..... 353
RootedCON ..... 353
Vulnerabilidades ..... 357
Falciani, o cómo hackear la banca suiza ..... 362
A solas con Falciani ..... 366

*Mayo de 2015. La pista penal* ..... 375

Capítulo 18. Hacktivismo ..... 378
El hombre que lanza piedras a la luna ..... 378
El encantador de códigos ..... 384
Cómo hackear un satélite ..... 401

*Mayo de 2015. La pista telefónica* ..... 405

Capítulo 19. El oscuro futuro que nos espera ..... 408
Biografía de un hacker ..... 408
El gueto hacker de Varsovia ..... 418

*Mayo de 2015. La vulnerabilidad del Firewall de MarkoSS88* ..... 423

Capítulo 20. Acoso en la red ..... 429
El ventilador de miserias ..... 429

«Estoy cansada de vivir» ..... 431
Morir en la red ..... 435
La responsabilidad parental ..... 438
Cuando el menor es culpable... y el padre también ..... 443

*Junio de 2015. El ladrón de vidas* ..... 449

Capítulo 21. El hacking y la ley ..... 453
Ciberjusticia ..... 453
Zero Day ..... 458
Falciani y el servicio secreto de Ada Colau y Manuela Carmena ..... 467

*Junio de 2015. Markos no es Jordi* ..... 471

Capítulo 22. Juegos de espías ..... 473
De Stuxnet al Hacking Team ..... 473
El Maligno ..... 483
El internet de las cosas ..... 487
El hacking en el siglo XXI ..... 489

*Julio de 2015. Markos es Pedro* ..... 500

Epílogo ..... 506
Cuando algo es gratis, el producto eres tú ..... 509
La verdad está ahí dentro... pero hay que saber buscarla ..... 512

Glosario hacker básico ..... 514

Bibliografía ..... 520

Agradecimientos ..... 523

Índice onomástico ..... 525

«Internet es una gigantesca máquina de espionaje al servicio del poder. Debemos luchar contra esta tendencia y convertirla en un motor de transparencia para el público, no solo para los poderosos.»

Julian Assange, Wikileaks

«Aunque no esté haciendo usted nada malo, le están vigilando y le están grabando. Y la capacidad de almacenamiento de estos sistemas se incrementa año tras año y añade ceros a la derecha a un ritmo constante, hasta el punto en que, sin haber hecho necesariamente nada malo, bastará con que le resulte sospechoso a alguien, incluso por error, y podrán utilizar este sistema para retroceder en el tiempo y escrutar todas y cada una de las decisiones que hayamos tomado, a todos y cada uno de los amigos con los que hayamos comentado algo, y atacarnos valiéndose de ello con tal de levantar suspicacias a partir de una vida inocente y pintar a cualquiera dentro del contexto de un malhechor.»

Edward Snowden

«Dale a un hombre un arma y puede robar un banco. Dale a un hombre un banco y puede robar el mundo.»

Tyrell Wellick, *Mr. Robot,* cap. 1x02

Prefacio

# Ladrones de vidas

El último vídeo de gatitos en YouTube, que tu mejor amiga ha subido a su Facebook, te arranca una sonrisa. Pinchas en «Me gusta», y después lo compartes en tu muro añadiendo algún comentario ingenioso: «Ahora entiendo por qué mi perro cree que están para comérselos». Lo publicas también en tu perfil de Tuenti y tuiteas el enlace.

Ves que te han llegado seis nuevas solicitudes de amistad. Casi todo tíos. Ni siquiera te molestas en comprobar si realmente los conoces fuera de la red, o si tenéis amigos en común: los aceptas a todos. Con estos nuevos seis amigos, ya pasas de cien en Facebook y le ganas por tres a la presumida de tu amiga. Bien por ti. No serás la chica más popular del instituto, pero al menos en la red tendrás más «amigos» que ella...

Sospechas que probablemente alguno será un tío mayor, haciéndose pasar por alguien de tu edad. Recuerdas el incidente de aquella compañera. Descubrió que uno de los chicos que había agregado era en realidad un viejo verde que intentó quedar con ella. Pero ¿qué más da? Tú eres más lista y te sientes segura en la intimidad de tu cuarto, frente a la pantalla del ordenador. Incluso aunque algunos de esos perfiles fuesen falsos, ¿qué daño podrían hacerte desde el otro lado de la red? Terrible error.

A ti no te va a ocurrir lo que le pasó a tu hermano. Uno de los incautos que se bajaron la app The Adult Player, y que acabaron chantajeados con fotos comprometidas hechas desde su propia cámara. Lo has leído en las noticias: varios deportistas, actores y galanes famosos picaron el anzuelo. Pero crees que eso solo puede pasarle a un chico.

En casa estás a salvo, ¿verdad? Y la paranoia que te contagió aquella vecina que sufrió acoso hace unos meses ya está superada. Definitivamente, el ordenador te va mucho mejor desde que eliminaste el antivirus, que te ralentizaba unos incómodos segundos el equipo con tanta actualización

de software y tanta tontería. ¿Quién va a querer crackearte a ti? ¿Qué podrías tener tú que le interesase a un pirata informático? Nuevo error.

Chateas un rato con tu amiga, comentando el último disco que os habéis bajado del eMule; lo horrible que sale una de clase en las últimas fotos que subió a Instagram o lo interesante que está el libro que te has descargado en PDF, de una página pirata. Ella te pide el enlace para bajárselo también, y tú se lo das, porque no sabes que el PDF es el vector de ataque preferido por los piratas informáticos.

Si tuvieses que comprar el libro físicamente para regalárselo, te lo pensarías dos veces, pero es fácil ser generoso con lo que no te cuesta nada. Y todavía crees, ingenua, que todo en la red es gratis. Aún no sabes que cuando algo es gratis en la red, el producto eres tú.

Suena un wasap. Es el grupo de las amigas del barrio. Te desnudas para meterte en la cama con el móvil mientras wasapeas con ellas, y durante un rato ríes despreocupada con sus ocurrencias. Tumbada sobre la cama, solo con una camiseta y las braguitas, pasas los siguientes minutos charlando con ellas a través del móvil, como si estuvieseis tomando cañas en el bar de la esquina. Solo que ahora puedes hacerlo en la intimidad y seguridad de tu habitación... ¿Intimidad?

Desde hace rato alguien te observa a través de la webcam del portátil que tienes sobre la mesa de tu escritorio. Justo frente a la cama. La activa por control remoto con un programa llamado Cammy, uno de los cientos de formas de *creepware* que existen para activar la cam o el micrófono de un contacto a distancia. Conoce tus rutinas, y lleva varios días grabándote mientras te desnudas en tu habitación. Tiene la esperanza de pillarte haciendo algo más fuerte, pero los vídeos de una joven de tu edad, desnudándose en su cuarto, ya valen dinero para algunas páginas de porno amateur. De hecho, todo vale dinero en la red.

También ha saqueado tus álbumes de fotos. Jamás sospecharías que tus fotografías veraniegas en la playa o bailando en la disco con tus amigas podrían valer dinero; hasta esas inocentes fotos de pies en la piscina que te gusta hacerte serán bien recibidas entre los fetichistas o pedófilos de Oriente Medio o Asia. Porque muchas de tus fotografías están ya en webs porno, para gusto y deleite de pajilleros japoneses, árabes o turcos, que podrían ser tus abuelos.

Incluso es posible que tu webcam esté directamente enlazada a una web especializada, como Insecam, una página donde se ofrecen miles de webcam pirateadas en todo el mundo, para que los *voyeurs* puedan contemplar cómo te desnudas en la «intimidad» de tu cuarto en tiempo real. Solo desde Insecam, en noviembre de 2014 se podía acceder a 4.591 cámaras pirateadas en los Estados Unidos, 2.059 de Francia, 1.576 de Holanda o 378 en España. Quizá la tuya sea una de ellas... Del Reino Unido se encontraron 500 enlaces, entre ellos algunos que filman, por ejemplo, la habita-

ción de un niño en Birmingham, un gimnasio en Manchester o un pub en Stratford.[1]

Pero tu imagen, vestida o desnuda, es lo que menos interesa al ciberdelincuente. Quiere mucho más. Lo quiere todo. Quiere robar tu vida.

Ha echado un vistazo a tu cuenta bancaria. ¡Bah!, no tienes mucho. Así que apenas te robará unos euros. Tan poco que jamás te darás cuenta. Como ocurre con los miles de ordenadores que ha infectado en su red zombi. Si fueses una empresaria de éxito, o una adinerada banquera, quizá habría caído en la tentación de vaciarte la cuenta, o de utilizar los códigos de tu tarjeta de crédito para hacer compras en eBay, Amazon o Alibaba. Pero robar un par de euros a miles de cuentas es tan rentable como robar miles de euros a una sola. Y mucho más seguro. Por eso tu ordenador pertenece a una *botnet*.

Sin embargo, que te roben dinero tampoco es el mayor de tus problemas. Lo que realmente quiere el pirata que infectó tu ordenador es utilizar tu identidad digital. Tu vida en la red. No eres una pieza de caza mayor, cuya captura requiriese una operación sofisticada de *malware* —software malicioso para infectar ordenadores y teléfonos móviles como el tuyo— dirigido, *pentesting* o ingeniería social. No. Eres una simple sardinilla anónima, en un banco de miles de peces, a la que capturó en su red de arrastre mientras navegaba por el inmenso océano de internet.

Le bastó diseñar un buen troyano. Esconderlo en un archivo «gratuito» —por ejemplo en una peli, una canción o un libro de moda— y subirlo a la red. Quizá, en la edición pirata del último libro de Antonio Salas... Tú te lo descargaste y con él te llevaste el virus a tu ordenador. A tu casa. No, nada es gratis en la red.

Ahora el tuyo es uno de sus ordenadores zombi. Como miles de ordenadores que se descargaron el mismo virus. El ciberdelincuente controla tu ancho de banda, tu disco duro, tu wifi, tus cuentas de correo o redes sociales. Tiene el poder total para utilizarlos como mejor le convenga. Y puede hacerlo él, o vender esa *botnet* al mejor postor en el mercado negro. Por ejemplo, en uno de los miles de mercados de vidas robadas en la Deep Web, la internet profunda, que no aparece en los buscadores.

¿Quién puede comprar tu vida? Alguien que necesite miles de ordenadores conectados entre sí a través de un mismo *malware,* para trabajar juntos por un objetivo más ambicioso... Como la red mundial del programa SETI, pero con intenciones mucho menos altruistas.

Tú no lo sabes, pero en la actualidad el negocio del *malware* supera con creces el tráfico de cocaína.

Utilizarán tu vida digital para abrir cuentas en casinos *online* a través de las que blanquear dinero. Para distribuir pornografía infantil en la Deep

1. http://www.elmundo.es/tecnologia/2014/11/20/546de362268e3ed7198b457f.html

Web. Para robar a tu banco a través de tu cuenta. Para atacar objetivos políticos o económicos con programas de DoS o para distribución de propaganda yihadista. No hay más límite que la imaginación del ciberdelincuente. Y su imaginación no tiene límite.

Dentro de unos días, quizá de unas semanas, recibirás la visita de la Policía o la Guardia Civil. Te detendrán por distribuir porno infantil, por blanqueo de capitales o por difusión de propaganda terrorista. Jurarás una y otra vez que eres inocente, que no sabes de qué te hablan, pero las pruebas serán irrefutables. La IP de tu ordenador o de tu teléfono móvil o de tu red wifi aparece asociada a esos delitos y solo tú, o eso creías, tenías acceso a ellas. Entonces pensarás que habría sido más barato haberte comprado el disco, la peli o el libro, que descargártelo «gratis» en la red...

La Policía está desbordada. De la misma forma en que la legislación contra nuevas drogas de diseño evoluciona al rebufo de la creatividad de los químicos, los cibercriminales crean nuevos delitos que aún no están definidos como tales.

A pesar de los ingentes esfuerzos, dedicación y recursos que las Fuerzas y Cuerpos de Seguridad del Estado están dedicando a la seguridad informática, los *blackhats* —hackers de sombrero negro o ciberdelincuentes— siempre van un paso por delante. Las nuevas leyes sobre seguridad informática tardan mucho en ser aprobadas, y para cuando se legisla sobre un nuevo tipo de ciberdelito, intrusión o *malware,* los *blackhats* ya han inventado mil nuevos virus, gusanos, troyanos y han descubierto nuevas vulnerabilidades en la red. Es una carrera perdida. Sobre todo si, como desveló hace un par de años Edward Snowden, el invasor de nuestra intimidad, el ladrón de nuestra vida, no es un cracker, ni una mafia organizada, ni un grupo terrorista... sino las agencias de Inteligencia más poderosas del mundo.

La buena noticia es que existen formas de ponérselo difícil. Existen maneras de protegerte. De evitar ser una sardinilla anónima en un inmenso banco de peces. Aunque solo ellos pueden ayudarnos a recuperar nuestras vidas robadas o evitar que nos las roben. Los hackers.

## Octubre de 2014
## Matar a Antonio Salas

«Más que por la fuerza, nos dominan por el engaño.»

Simón Bolívar

Quedamos en un discreto restaurante madrileño del norte de Madrid, donde nos reuníamos de cuando en cuando. Una decena de policías nacionales, municipales, guardias civiles... y un periodista encubierto. Yo era solo un invitado. Jamás tomé la iniciativa para convocar ninguna de aquellas tertulias, pero esta vez era distinto. Mis compañeros notaron que mi comportamiento era extraño. Me mantenía distante, preocupado, ensimismado... Y ante la insistencia de Pepe, saqué de mi mochila un puñado de papeles y se los pasé.

—Dime si te parece que es para preocuparse... Yo no sé qué hacer. —Supongo que mi voz delataba mi nerviosismo—. Seguramente será todo una paranoia, y este tío será un chalado que va de farol, pero he hablado con los organizadores del congreso y me confirman que es verdad. Se matriculó con nombre y DNI falso para asistir a mi conferencia y es verdad que alguien armó un follón en la entrada cuando se llenó la sala. Y si eso es cierto, quizá lo demás también lo sea.

A mi alrededor, en aquella mesa redonda, un grupo de veteranos policías se pasaban las hojas donde había impreso el email que acababa de recibir, en el que un conocido cibernazi, con una activa presencia en la red, me confesaba que en la mañana del 5 de marzo de 2014 había intentado degollarme con una navaja en el salón de actos del campus de Vicálvaro, de la Universidad Rey Juan Carlos de Madrid.

David Madrid, Pepe, Álex, Rubén, Toni, Rafa, Manu... se alcanzaban las hojas unos a otros. Era fácil reconocer cuándo llegaban al párrafo en cuestión, porque abrían mucho los ojos y dejaban escapar algún comentario... «Joder, qué fuerte.»

Casi todos habían oído ya hablar de MarkoSS88. El webmaster de una conocida página nazi es un veterano activista en la red. Sus Facebook, Telegram, Twitter y demás redes sociales han sido el campo de batalla de enconados debates entre los neonazis y los antifascistas. Intelectual e ideólogo, especialmente dedicado a la formación de las nuevas generaciones de jóvenes skinheads NS, MarkoSS88 es autor de muchos textos doctrinales sobre el movimiento nazi, su historia, política, filosofía y espiritualidad. Y en páginas de venta *online*, como lulu.com o dropbox.com, podía comprarse por 23 euros el libro que él firmaba: *¿Qué es el Nacional Socialismo? Un trabajo de dedicación y entrega.*

Pero MarkoSS88 no es solo un ideólogo. Al menos según su dilatada presencia en la red, también es un hombre de acción y un objetivo para los

grupos antifascistas, tras el asesinato de un joven latin king que tuvo cierta difusión en las redes y encabezó alguna plataforma en change.org. Según él, en defensa propia.

Mis compañeros de tertulia sabían también que MarkoSS88 llevaba un par de años absolutamente obsesionado conmigo. Era uno de mis acosadores más leales en la red. Cada vez que me entrevistaban en un medio y colgaban la entrevista, su nick aparecía entre los comentarios más agresivos. Sus insultos y amenazas de muerte llegaban con cierta frecuencia a mis cuentas de Twitter o email. No dejaba pasar la ocasión de difamarme, calumniarme y expresar su íntimo deseo de verme muerto. Como otros muchos nazis, antisistema, puteros, proxenetas o traficantes. Nada nuevo. No es la primera vez que me pasa. Poco antes de recibir ese email, me había encontrado con un mensaje de la Fiscalía de Protección de Testigos, al acudir a Intervención de Armas de la Guardia Civil para renovar mi licencia trianual. La fiscal quería reunirse conmigo para valorar la renovación de mi situación como testigo protegido.

Pilar y Gonza —dos agentes del Grupo VII de Información, que habían llevado la Operación Puñal contra Hammerskin en cuyo juicio declaré— me escoltaron de nuevo hasta la Fiscalía para mantener la reunión con la fiscal (María Antonia Sanz), y con la psicóloga responsable de los testigos protegidos (Marta de Prado). Uno de ellos fue quien me regaló el pasamontañas que utilizo en las entrevistas.

El día en que presté declaración en el juicio, y antes de bajarme del coche en el que me habían trasladado a la Audiencia Provincial, escondido en la parte de atrás, en un dispositivo que parecía salido de una película, me dijo que me pusiese el pasamontañas. «Por tu seguridad —exclamó mientras señalaba los edificios que rodeaban la Audiencia—. Podría haber alguien en alguna de esas ventanas.»

Sabíamos que las novias de algunos de los quince skins imputados habían hecho un fondo para contratar a un sicario que impidiese mi declaración ante el tribunal, y aquella era su última oportunidad de silenciarme antes de entrar en la sala. Ahora, cinco años después, ese mismo guardia me acompañaba a la reunión con la fiscal que debía tomar la decisión de cerrar mi expediente o mantenerme como testigo protegido a continuidad.

Cuando la fiscal me preguntó si continuaba recibiendo amenazas, sonreí con resignación: «Casi a diario, señora..., y no solo de los neonazis». Solo tuve que dejar sobre su mesa un montón de hojas impresas, con el torrente de amenazas que recibo, y la fiscal lo vio claro. Continuaría manteniendo el estatus de testigo protegido indefinidamente. Varias de aquellas amenazas venían firmadas por MarkoSS88.

Después de *El año que trafiqué con mujeres, El Palestino* y *Operación Princesa,* la lista de «damnificados» por mis infiltraciones había crecido de manera exponencial. Pero una cosa es que un puñado de cobardes te insul-

te, difame o amenace en la red, y otra muy distinta lo que aseguraba el email que mis amigos tenían ahora en sus manos, MarkoSS88 iba más allá. Mucho más allá.

No solo hablaba de cómo el 5 de marzo pasado había ido a buscarme armado con un cuchillo al Congreso de Inteligencia que se celebraba en la Universidad Rey Juan Carlos. No solo contaba con pelos y señales cómo había llegado hasta allí con la firme intención de rajarme el cuello, fuesen cuales fuesen las consecuencias. Incluso me explicaba que el día anterior había acudido al campus para estudiar los accesos al auditorio, las entradas y salidas, las rutas de escape...[2]

Sí, es verdad, he recibido amenazas antes. Pero es muy distinto cuando alguien te confiesa el día, la hora y cómo ha intentado matarte:

—Joder, Toni —dijo Álex, otro de los policías nacionales, al leer el correo—, tienes que averiguar quién es este tío. Podría volver a intentarlo.

—Lo sé. En realidad, si un imprevisto no hubiese complicado los planes de MarkoSS88, probablemente él estaría muerto y yo en la cárcel. Pero no me hace ni puta gracia que pueda ocurrírsele intentarlo otra vez...

Para cuando recibí la confesión de MarkoSS88 yo ya llevaba meses sumergido en la investigación sobre el hacking y la (in)seguridad informática. Así que estaba preparado para iniciar la «caza». Pero subestimé a MarkoSS88. Tras esa identidad no se ocultaba un simple neonazi vinculado a UltraSSur. El skinhead que había confesado cómo el 5 de marzo de 2014 intentó ejecutar a Tiger88 resultó ser alguien muy distinto al del perfil que yo imaginaba. Más poderoso. Más peligroso.

Durante los últimos años he conocido a hackers de sombrero blanco, gris y negro, a ciberactivistas, ciberdelincuentes y ciberpolicías. He asistido a sus congresos, talleres y seminarios. He conocido a los espías que utilizan las redes informáticas para obtener información y a los ciberterroristas que distribuyen en ella su propaganda. He convivido con los ciberacosadores y con sus víctimas, e incluso me he convertido yo mismo en víctima de alguno de ellos. Y me he convencido de que, en el siglo XXI, no existe nada más urgente que conocer cómo funciona nuestra vida en la red. Porque todos estamos ya en ella. Héroes y villanos, criminales y policías, nazis, proxenetas, traficantes, terroristas... El ordenador, y más aún los teléfonos móviles, son nuestro pasaporte al nuevo mundo. Si no usas internet y no tienes un teléfono móvil, no necesitas seguir leyendo. De lo contrario, prepárate para descubrir el lado oscuro, y también el más luminoso, de tu nueva vida. Una red en la que todos estamos atrapados. Una red llena de mentiras.

2. «Entrevista a mi asesino»: http://loshombresquesusurranalasmaquinas.blogspot.com.es/2015/09/entrevista-mi-asesino.html