PRÓXIMAS RESERVAS VOLUNTARIAS CON EL 150 POR 100 DEL SUELDO

Jesús A. LORENZO RODRÍGUEZ

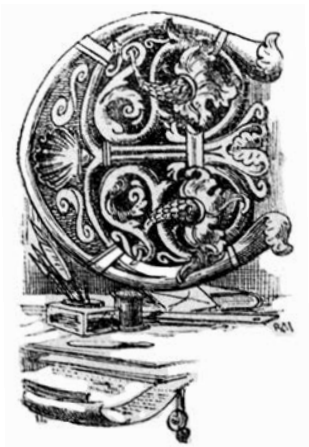
Cuando repeles un ataque sabes que tu enemigo volverá mañana. Tú tienes que ganarle todos los días, mientras que a él le basta un mal día tuyo para vencer.

José Selvi, investigador de Seguridad Senior de Kaspersky.

Yo no he tocado nada.

Anónimo.

Introducción



En esta misma REVISTA, José M.ª Molina Mateos nos expuso cómo integrar la ciberseguridad en la Estrategia de Seguridad Nacional (ESN) de 2013 (RGM enero-feb. 2014). El alférez de fragata (RV) Antonio Moreno-Torres Gálvez analizó la ciberseguridad, la seguridad marítima y la energética como ámbitos de actuación dentro de la misma ESN (RGM nov. 2015). El hoy capitán de fragata Carlos Garau Pérez-Crespo planteó la posibilidad de ataques a infraestructuras críticas (RGM enero-feb. 2015). Manuel Gálvez Reina, alférez de navío, explicaba el nuevo reto que suponía la ciberdefensa para las FF. AA. (RGM abril 2015). De nuevo, José M. ª Molina Mateos hizo una aproximación al problema de la ciberdefensa en el ámbito naval (RGM junio 2015). El capitán de navío Enrique Cubeiro Cabello, en su artículo «¿Dónde se ubica el lugar más peligroso del ciberespacio?» (RGM enero-feb. 2014), expresaba que de todos los cometidos del MCCD (Mando Conjunto de Ciberdefensa) ninguno resultará tan decisivo para potenciar nuestra capacidad

«Santiago». (Fuente: *Flickr* de Katy Levinson).

de ciberdefensa como la concienciación. Concienciación que, en el fondo, no supone otra cosa que inculcar, profundamente y en cada miembro de la organización, el convencimiento de que ciberdefensa somos todos. Concluyendo, de forma ingeniosa, que el lugar de más peligro en esta guerra se encuentra entre el teclado y la silla: los usuarios, que sin duda somos el eslabón más débil de la cadena y el objetivo de la mayor parte de los ataques.

En cuanto nos mencionan la palabra ciberdefensa, enseguida pensamos en un ciberdelincuente, como un lobo solitario, en la mayoría de las ocasiones gordo y sin vida social, metido en un oscuro sótano rodeado de ordenadores, con vasos de café o cola y bolsas de patatas fritas repartidas por la mesa y sin salir a ver la luz del sol durante días. En ese ambiente, lo imaginamos tecleando frenéticamente en lenguaje hexadecimal para intentar acceder a los servidores centrales del FBI, la CIA o del mayor banco del mundo. Por supuesto, en escasos minutos, consigue la contraseña y accede sin más a la mayor base de datos de los espías en el mundo, se cambia la identidad o realiza transacciones millonarias después de varios saltos acrobáticos por distintas cuentas en bancos de paraísos fiscales.

Sin embargo, nada más lejos de la realidad; independientemente de su lugar de «trabajo», son personas normales con los suficientes conocimientos informáticos como para crear o saber dónde conseguir programas maliciosos,

tanto si trabajan por su cuenta como si pertenecen a los numerosos grupos de ciberdelincuentes que, organizados y en equipo, planean y ejecutan los ataques. Con el paso de los años, se han dado cuenta de que sus ataques contra las grandes empresas y organizaciones se hacen cada vez más inútiles o costosísimos, lo que les ha llevado a buscar otras vías más sencillas, con menor esfuerzo y que les proporcionen los mismos beneficios.

Esa otra vía, como apuntaba el capitán de navío Cubeiro, somos los usuarios, bien en nuestro hogar o bien como integrantes de una organización o una empresa.

No se preocupen, aún no he entrado en el asunto del pase a la reserva con el 150 por 100 del sueldo. Será en los próximos apartados.

Descripción de la víctima

Víctimas potenciales somos todos aquellos que, en un momento determinado, no tenemos precaución con algún suceso anómalo en nuestro equipo bien por visitar paginas no confiables, bien por recibir correos de dudosa procedencia.

Usuarios que van desde el más incauto o desidioso, que deja las sesiones abiertas, hasta el traidor que por dinero o por despecho roba, facilita el robo de información o la instalación de un *software* malicioso que permita acciones contra el sistema. Un alto porcentaje de incidentes es debido a los usuarios, involuntariamente por no tener cuidado o voluntariamente por traiciones o coacciones de todo tipo, amenazas físicas o de sacar a la luz alguna información sensible sobre su persona.

No vale de nada hacer una gran inversión en sistemas de última generación y en los mejores técnicos informáticos en seguridad si luego los usuarios, que nos convertimos en un elemento más de la seguridad del sistema, no estamos concienciados del riesgo y cometemos dos errores principales:

1. Creer que como la red o el equipo están aislados y no conectados a internet están seguros.

Es posible que muchos de ustedes hayan oído hablar del virus *Stuxnet*, que muy resumidamente se basa en que, como decía el gran Gila, «… alguien ha hecho algo… alguien ha dejado algo…»; pues bien, ese «alguien» dejó suelto por internet un virus, *Stuxnet*, que no hacía absolutamente nada, excepto infectar los PC y los USB que se ponían a su alcance. ¿Cuál era entonces su objetivo? Esperar muy pacientemente a que algún trabajador de una central nuclear iraní cometiese el enorme error de conectar un USB infectado con ese virus en algún PC de la red de la central nuclear. Y sucedió; un individuo, sin ninguna precaución, insertó un USB particular infectado en la red. El resulta-

do fue que el virus, una vez detectó que había llegado a su objetivo, empezó a variar el funcionamiento de la central, impidiendo que se pudiese producir el uranio enriquecido que se intentaba obtener. Este comportamiento imprudente permitió salvar las barreras de aislamiento de la red e incluso las físicas de la instalación. Imagínese el lector las medidas físicas que habría que sobrepasar para producir un daño similar.

2. Creer que no tenemos ninguna información que sea útil para ningún atacante.

Nuestras claves del banco, del correo personal y del PC de nuestro puesto de trabajo permitirían al atacante disponer de la información suficiente para cometer delitos directamente contra nosotros o, a partir de ella, contra terceros. Por cierto, la contraseña «123456» fue en 2016 y por enésimo año consecutivo la más utilizada en el todo el mundo.

A través de nosotros pueden conseguir entrar en el resto de equipos de la red hasta llegar a tener el control total para robar información, mantener una vigilancia en busca de información más relevante o dañar la red para impedir su uso borrando toda la información o incluso cifrándola para pedir un «rescate».

También pueden, indirectamente, obtener la de otros miembros o de la propia organización para realizar ataques más selectivos sobre personas de alta responsabilidad. Permítame el lector un ejemplo: el AJEMA pretende asistir a la conferencia habitual de los martes en el CGA y se lo comunica al 2.º AJEMA, que considera promover más afluencia de oficiales y redirecciona el correo a los almirantes de las divisiones y de otras jefaturas; el AJESACIS se lo reenvía al ayudante mayor para que supervise el estado de la sala; éste al segundo ayudante mayor, quien se lo remite a un suboficial que finalmente se lo reenvía al marinero que comprobará las luces y limpieza general del salón de conferencias.

Estamos acostumbrados a estas cadenas de correos. El marinero en cuestión siempre ha pensado que no tiene ninguna información que cuidar, que no es «nadie» en la organización. Sin embargo, fíjense qué información contiene en esa cadena. Aparte de las direcciones de correo, da una idea de cómo estamos organizados y quién es quién. A partir de aquí se pueden realizar ataques a personas que sí pueden tener información importante simplemente con un correo suplantando a alguien de confianza dentro de la organización. Una vez obtenidas las direcciones, fácilmente se puede suplantar el correo de uno de ellos para entrar en el PC de otro y así sucesivamente.

Al 2.º AJEMA no le extrañará recibir un correo de un «falso» AJEMA en el que le pide que revise un documento adjunto, infectado; a sus almirantes tampoco, y así sucesivamente. Un simple correo que anunciaba una situación totalmente inofensiva da la suficiente información como para iniciar un ataque selectivo.

Tanto esas direcciones de correo como los enlaces a páginas *web* son fácilmente falseados para que lo que creemos estar viendo no sea realmente lo que vemos.

Un habitual en los ataques mediante correo electrónico es el Banco de Sabadell. En dicho correo nos envían un enlace, un hipervínculo que va en el texto del propio correo electrónico, al que nos piden que accedamos para actualizar nuestras credenciales. En ese hipervínculo creemos estar leyendo *sabadell.com,* y al acceder, creemos estar viendo la *web* legítima, pero es posible que en realidad lo que esté escrito sea *sabade11.com* y acabemos accediendo a una página falsa, pero idéntica a la «buena»; en el tipo de letra *Birch Std* las «eles» se confunden con los «unos», permitiendo fácilmente el engaño. Hay otros muchos tipos que nos permiten camuflar algún dígito o letra de esta manera.

Todos hemos visto en alguna ocasión el típico párrafo con numerosos caracteres erróneos que, sin embargo, somos capaces de leer perfectamente: «Sgeun un stsduio de una uivenrsdiad ignlsea, no ipmotra el odren en el que las ltears etsan ersciats, la uicna csoa ipormtnate es que la pmrirea y la utlima ltera esten ecsritas en la psiocion cocrrtea». Pues bien, esa capacidad de nuestro portentoso cerebro nos puede jugar malas pasadas y llevarnos a un error de consecuencias lamentables. Podemos, por ejemplo, creer leer *universidadcomplutense* cuando en realidad está escrito *universdadcomplutense* y este enlace nos llevará, irremediablemente, a un *web* indeseable.

Cualquiera de los métodos anteriores puede ser aplicable a las direcciones de correo, tanto las de remitentes como a las que vienen insertadas en los mensajes que recibimos. Este es un aspecto que debemos tener siempre presente cuando recibamos correos que no sean habituales; pero existen otros que deben hacernos, como mínimo, dudar y tratarlo con precaución: un correo directo de una alta autoridad de nuestra organización que no está previsto que se dirija directamente a nosotros; otros con factura anexa de una determinada compañía cuando el servicio lo tenemos contratado con otra; algunos regalándonos premios de sorteos en los que nunca hemos participado o restituyendo un dinero que nunca hemos reclamado, etcétera.

A estas alturas, el lector ya está convencido de que en este artículo no encontrará nada referente al pase a la reserva con el 150 por 100 del sueldo, es más, ya sabe que es una tomadura de pelo que de forma engañosa le han llevado a leer (era mi humilde intención) acerca de un asunto que quizás no le interese lo más mínimo. Ha caído exactamente en la misma trampa a la que se verá sometido en multitud de ocasiones en los correos recibidos, tanto en el particular como en el oficial, con tan solo la diferencia de que en ese caso las consecuencias podrían haber sido dolorosas: un robo bancario, la pérdida de todos los archivos del destino, todas las fotos familiares en formato digital, la pérdida del control del PC, que podría usarse para cometer otro delito más grave, etc. Sin embargo, en «mi trampa» el mayor de los efectos que puede

	Decálogo de seguridad del correo electrónico
1	No abra ningún enlace ni descargue ningún fichero adjunto procedente de un correo electrónico que presente cualquier síntoma o patrón fuera de lo considerado normal o habitual.
2	No confíe únicamente en el nombre del remitente. El usuario deberá comprobar que el propio dominio del correo recibido es de confianza. Si un correo procedente de un contacto conocido solicita información inusual contacte con el mismo por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.
3	Antes de abrir cualquier fichero descargado desde el correo asegúrese de la extensión y no se fíe por el icono asociado al mismo.
4	No habilite las macros de los documentos ofimáticos incluso si el propio fichero así lo solicita.
5	No debe hacerse clic en ningún enlace que solicite datos personales ni bancarios.
6	Tenga siempre actualizado el sistema operativo, las aplicaciones ofimáticas y el navegador (incluyendo los plugins/extensiones instalados).
7	Utilice herramientas de seguridad para mitigar exploits de manera complementaria al software antivirus.
8	Evite hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.
9	Utilice contraseñas robustas para el acceso al correo electrónico. Las contraseñas deberán ser periódicamente renovadas. Si es posible utilice doble autenticación.
10	Cifre los mensajes de correo que contengan información sensible.

Extracto del informe «Buenas Prácticas BP-02/16. Correo electrónico del CCN-CERT».

sufrir el lector es tomar conciencia de las amenazas que nos acechan, que no somos «nadie» como pensábamos y que nos vamos a proponer tener más cuidado y cambiar algunos hábitos con los que minimizar el riesgo.

No estamos solos

Por si todo este ambiente fuese ya poco respirable porque pareciera que tuviésemos la espada de Damocles permanentemente sobre nosotros, resulta que tampoco podemos confiar en nadie (o casi nadie): hace escasos meses el mundo tembló con un ataque masivo mediante un virus, *Wannacry*, que cifraba la información de los PC y servidores de numerosas empresas aprovechándose de incautos usuarios. Después se reclamaba una cantidad de dinero para dar la clave que permitiese recuperar esa información. Afortunadamente, Marcus Hutchins, un joven surfero, dio con una pista que permitió reducir sensiblemente los efectos de ese ataque. Pues bien, nuestro «héroe» fue detenido unas semanas después por vender un *software* malicioso utilizado para estafas bancarias. Pero siempre hay alguien en quien confiar:

— El CNI (Centro Nacional de Inteligencia), a través del CCN (Centro Criptológico Nacional), está en permanente vigilancia ante los constantes ataques y emite unos boletines de seguridad para advertirnos de estos y de cómo evitarlos. Además, publica unas guías de seguridad de configuración de sistemas operativos (Windows, Linux, Android) y *software* comúnmente usadas, proporcionando herramientas gratuitas para el análisis y protección de nuestros equipos o sistemas.
— El INCIBE (Instituto Nacional de Ciberseguridad) que, a través de su página *web*, proporciona gran cantidad de información, alertas sobre ataques, formación específica, guías, etc., dirigidas tanto a ciudadanos como a empresas.
— El MCCD (Mando Conjunto de Ciberdefensa) es el responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefen-

Imagen contenida en el «*kit* de concienciación» del INCIBE.

sa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa, así como de contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa nacional.

— El GRUCIBER (Grupo de Ciberdefensa de la Armada) que monitoriza sus redes específicas y, entre otros cometidos, colabora con el MCCD en la respuesta a incidentes que se hayan podido producir, tanto en redes clasificadas como en la WAN PG. Desde hace unas semanas, podemos ver un pequeño *banner* en la zona derecha de la página de inicio de intranet, en el que, mediante un sencillo código de colores, se pretende alertar a todos los usuarios sobre ataques que puedan estar llevándose a cabo o sobre cualquier incidente sobre el que convenga estar prevenido.

Una parte fundamental en esta lucha es conseguir concienciar a todos los usuarios de que ellos son el frente de batalla de esta guerra, para lo cual se ha creado recientemente, dentro del Plan de Concienciación de Ciberdefensa (CONCIBE) del MCCD, un aula virtual con el ambicioso objetivo de que la

efectúen 12.000 personas dentro de la estructura de la Armada, aunque está orientada a todo el personal de las Fuerzas Armadas, sin que sean necesarios conocimientos previos de ciberdefensa, y que consta de seis temas cuyo contenido no es técnico y se puede realizar en menos de tres horas.

Conclusiones

El ciberespacio se está constituyendo como el quinto dominio, después de tierra, mar, aire y espacio, pero contrariamente a los anteriores, que parecen ser exclusivos de profesionales de esos dominios, el dominio ciber no tiene fronteras y los participantes somos todos, tanto los profesionales como los usuarios, que constituimos la parte más débil del eslabón y donde se está centrando hoy en día la mayoría de los ataques, que en ocasiones solo necesitan que uno de nosotros cometa un error para afectar, en mayor o menor grado, a toda la organización.

Es fundamental, por tanto, conseguir que los usuarios estén concienciados de su papel y tomen las precauciones necesarias, tanto en su entorno de trabajo como en su vida privada, puesto que de la información que hagan pública (redes sociales principalmente) los atacantes pueden obtener datos que faciliten su objetivo.

BILIOGRAFÍA

Boletines de Concienciación del Mando Conjunto de Ciberdefensa.
Informes de Buenas Prácticas del Centro Criptológico Nacional: *https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp.html*.
Oficina de Seguridad del Internauta: *https://www.osi.es/es*.
Documentación de Concienciación del Grupo de Ciberdefensa de la Armada.