El uso de las redes sociales y la conciencia de contrainteligencia



Teniente Primero
GABRIEL DONAYRE MONTESINOS



Introducción

En la actualidad, el uso de las redes sociales se ha transformado en un fenómeno masivo que implica condiciones sociales, religiosas y generacionales. La Armada del Perú y su personal no son ajenos a este fenómeno.

Ante este suceso, si bien la nuestra Armada no prohíbe a su personal el uso de las redes sociales, entendiéndose que ello pertenece a su vida privada, no permite la publicación de información referida a la Fuerza Armada, "subir" fotos o comentar dónde alguien está destinado, puesto que se considera información que no le pertenece exclusivamente a la persona comprometida.

La información es naturalmente pública y libre, pero hay que tomar conciencia de que esta puede ser rastreada. Para ello, los analistas y el progresivo uso de programas informáticos monitorean las redes sociales, siendo los encargados de detectar la información selectiva de una forma temprana, analizarla, ponderarla, verificar su credibilidad, relacionarla con temáticas afines, tratarla, integrarla y hacerla circular entre su comunidad de interés.

En esa línea de pensamiento, se debe evitar la idea de que "a nadie le interesa lo que uno publica", o que "nadie va a estar buscando información" por este medio. Gran cantidad de casos han salido a la luz pública, relacionados con la obtención de información por medio del uso de las redes sociales, como para seguir desconociendo o negando este fenómeno.

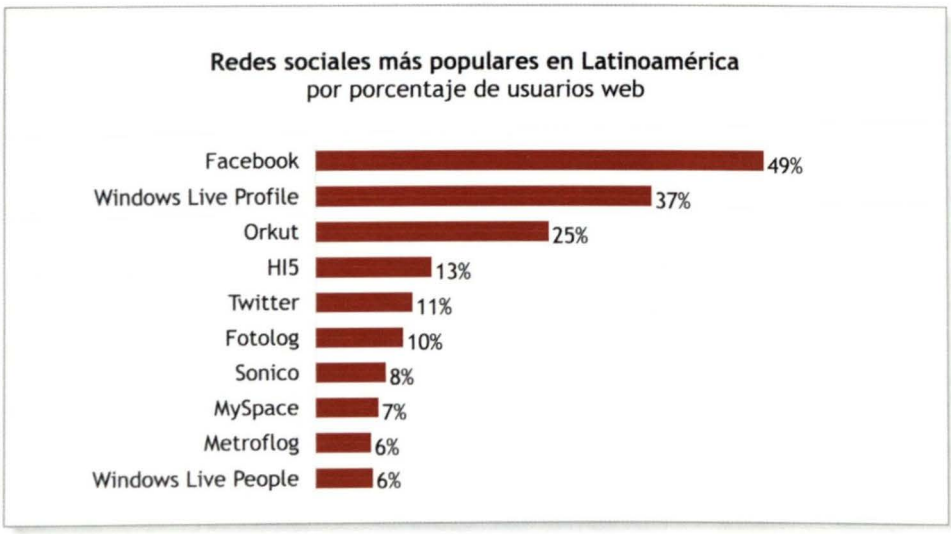
Bajo la perspectiva del profesor de Criminología en la Universidad de East London, Andrew Silke, "el hecho de que las agencias de inteligencia prohíban a su propio personal el uso de las redes como *Twitter o Facebook* debería decirnos algo acerca de su valor potencial".

Las redes sociales

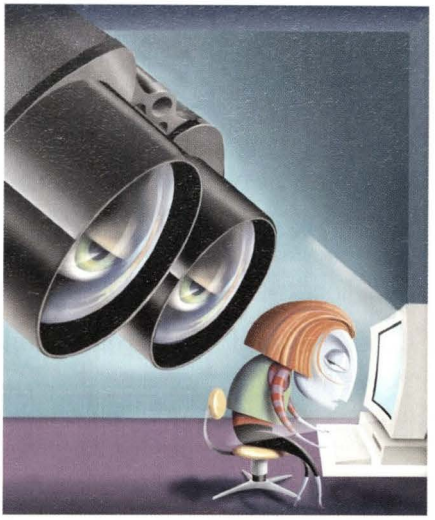
Son estructuras compuestas por grupos de personas que se encuentran conectadas por uno o varios tipos de relaciones, sean estas de amistad, parentesco, intereses comunes o intercambio de conocimientos.

A continuación, los puestos, ganados según su uso masivo a la fecha:

1. YouTube: "¡Ser famoso ya!".
2. Facebook: "Comunícate con las personas que más quieres".
3. Twitter: "Dilo en 140 caracteres".
4. Badoo: "Yo estoy aquí".
5. Google+.



Una característica intrínseca de las redes sociales es su capacidad de compartir abiertamente información personal; de esta manera, se expresa el estado de ánimo, se "suben" fotos, se "etiquetan" personas, se comentan fotos de amigos/conocidos, se generan nuevas amistades, y hasta se concretan negocios.



Monitoreo vigilante de la información.

El ser humano: ¿eslabón más fuerte o más débil de la cadena?

Como todos sabemos, una cadena es tan fuerte como su eslabón más débil. En este contexto, los intrusos mantienen un monitoreo vigilante de la información, reconociendo en *la persona* el eslabón más débil de la cadena, penetrando toda barrera tecnológica que la Institución pueda asentar en sus diferentes dependencias y ganando así acceso más allá de lo autorizado.

Los atacantes constantemente están haciendo reconocimiento de nuestros movimientos, utilizando para ello la información que dejamos en redes sociales, mensajes, registros y publicaciones, los cuales describen nuestros gustos, tendencias y motivaciones. Insumos básicos para desarrollar estrategias de ingeniería social, para motivar comportamientos deseados que dejen al descubierto formas de ingresar a infraestructuras tecnológicas o secretos de la Institución.

Se cita un ejemplo: el ataque a Google el 12 de enero de 2009, donde los atacantes recolectaron información publicada por los empleados de la firma en redes sociales como Facebook y Linkedin. Luego, configuraron un sitio *web* con fotos falsas, desde donde enviaban correos electrónicos que contenían enlaces al parecer confiables, dado que venían aparentemente de personas de confianza. Una vez las personas hacían clic sobre el enlace del correo, se descargaba un código malicioso que abrió una brecha de seguridad que dio acceso a los servidores corporativos de Google.

Se presume, además, que estos *hackers* habrían intentado obtener la información de acceso a las cuentas de importantes personas del Gobierno norteamericano antes de que el ataque fuera desbaratado.

Amenazas persistentes avanzadas

Una amenaza persistente avanzada *(Advanced Persistent Threat, APT)* es un tipo sofisticado de ciberataque, que constituye uno de los peligros más importantes y de rápido crecimiento que las organizaciones militares, políticas y del sector privado deben afrontar desde hace dos años aproximadamente. Es un hecho: la misma tecnología APT que usó China para atacar a Google, ahora está siendo utilizada por delincuentes informáticos para robar datos de organizaciones como la nuestra.

Sus ataques tradicionales empiezan mapeando las redes y realizando tareas de inteligencia para recolectar información acerca de vulnerabilidades técnicas. Sin embargo, un ataque APT empieza con un mapeo de la parte humana de la organización y recogiendo información de los empleados, más que por medio de las vulnerabilidades técnicas. Enfocarse en las personas, que, como hemos visto, son el eslabón más débil en la seguridad, es más fácil que tratar de evitar los componentes tecnológicos de seguridad como los firewalls y los sistemas de prevención de intrusos.

Entre ellos, el uso de herramientas de redes sociales es el más común, para ganar la confianza de las víctimas y comprometer así los sistemas y las credenciales de acceso a los mismos. Es importante entender el elemento humano de una APT, pues es uno de los elementos que hacen sumamente efectivo este tipo de ataques, ya que utilizan *la tendencia de la gente a confiar en otros para así manipular a los empleados y terminar instalando 'malware' en los sistemas.*

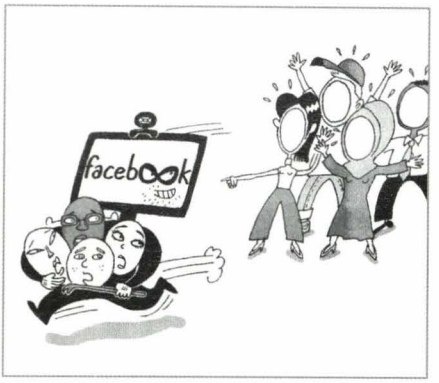
Anatomía de un ataque dirigido

Si bien no es nuestro caso, por no contar con acceso a las redes sociales a través de nuestro servicio de Intranet, los invito a ver un ejemplo citado por la empresa Websense para analizar el modus operandi de esta amenaza:

Avanzada: Los atacantes utilizan un espectro de tecnologías sofisticadas para reunir inteligencia. La acción generalmente comienza varios meses antes del ataque real de robo de datos de una organización:

- Los atacantes se infiltran y toman el control del servidor de otra compañía (no de la empresa elegida como blanco para el ataque). Esto se usará posteriormente como un buzón 'muerto' para los datos, y el seguimiento de los datos finalizará allí.

Una pieza de malware personalizada es enviada a la cuenta de *e-mail* personal de un empleado (sabiendo que dicho empleado revisa su e-mail personal en el trabajo). Ese malware luego comienza a viajar por la red, trazando un mapa de ella y examinando las medidas de seguridad instaladas.



Se debe procurar un máximo nivel de privacidad.

Nota: La vigilancia del blanco individual comenzó antes de la vigilancia de la red. Con frecuencia, el blanco de este *e-mail* se identifica a través de una búsqueda en la *Web* social o los perfiles de Linkedin o Facebook, simples búsquedas de ejecutivos en sitios corporativos, etc. En una sociedad "social", existe abundante información disponible sobre cualquier blanco, lo que hace que sea mucho más fácil para un ingeniero social elaborar un *e-mail* atractivo para el sujeto en su propio idioma, utilizando sus propios intereses e información para motivarlo a abrir el *e-mail*. Los atacantes pueden haberse hecho 'amigos' del sujeto con anterioridad y conversado con él en los sitios sociales para obtener información.

Persistente: Los atacantes están totalmente decididos a tener éxito. Realizarán un monitoreo paciente, constante y continuo para encontrar vulnerabilidades. Repiten intentos y cambian las tácticas si estas son detectadas:

- En nuestro ejemplo, el *malware* ahora ha trazado un mapa de la red y ha enviado información a los atacantes sobre los protocolos de seguridad instalados, incluida la dirección del *firewall proxy* existente. En este punto, los atacantes saben cómo ingresar y, más importante, dónde reside probablemente su premio.

Amenaza: Los atacantes también tienden a usar múltiples vectores de ataque, incluido malware específicamente elaborado y vulnerabilidades de día cero previamente desconocidas:

- En nuestro ejemplo, ya hemos visto una pieza de *malware* personalizada, utilizada para vigilancia. Ahora viene el código asesino.
- Se envía un nuevo *e-mail* a una cuenta personal de otro empleado que tenga acceso a los datos valiosos. Este *e-mail* lleva una carga de *malware* muy refinado que conoce qué sistemas evadir, dónde encontrar los datos

deseados y cómo robarlos sin ser detectado en forma inmediata. El código también es polimórfico y se actualiza con frecuencia para permanecer sin ser detectado por los AV y otras medidas de seguridad. Recuerden que no se trata simplemente de buscar credenciales bancarias en línea para liquidar una cuenta u obtener dinero. Estos atacantes piensan en grande. Van en busca de la propiedad intelectual, los secretos comerciales y otros datos confidenciales que pueden utilizar para avergonzarlo o aprovecharse de usted o su institución. [1]

La conciencia de contrainteligencia

Debemos considerar que este afán de compartir con nuestros amigos o conocidos debe ser compatible con nuestra conciencia de contrainteligencia. Al respecto, la conciencia de contrainteligencia se puede definir "como la actitud mental de todo personal militar, de estar preparado permanentemente para proteger a la Institución de las actividades de sabotaje y espionaje".

Dos enfrentadas opiniones se disponen sobre las redes abiertas como fuentes de información. Aquellos que las tildan de poco fiables y dudosas y otros que, por el contrario, las incluyen entre su monto de investigación y análisis.

Algunos consejos que educan la conciencia de contrainteligencia podrían ser:

- No publicar fotos ni videos donde pueda apreciarse el estado de mantenimiento de nuestros equipos y sistemas.
- No publicar fotos ni videos de los interiores de las diferentes Unidades y Dependencias, así como interiores de oficinas y talleres.
- No "etiquetar" en las fotos, ni en los videos, al personal perteneciente a la Fuerza sin el consentimiento expreso de los involucrados.
- No comentar o hacer alusión a los lugares, momentos y duración de los diferentes despliegues, ejercicios y operativos.
- Tener la máxima restricción en la configuración de privacidad (por ejemplo: que el contenido del perfil solo pueda ser visto por "amigos" y que solo se puedan etiquetar fotos con la autorización correspondiente).
- Evitar las contraseñas obvias o repetidas.
- Formar grupos de amigos ("compañeros de la universidad", "camaradas", "familia") y restringir según corresponda el acceso a la información.
- Tener siempre presente la necesidad de saber.

- Nunca "subir" o publicar fotos, videos o comentarios que puedan ser interpretados como un delito o una falta disciplinaria. Recordar que como militar, uno es funcionario público; por lo tanto, uno tiene responsabilidades como tal.
- Si uno crea un grupo/página, procurar que este sea cerrado, con máximo nivel de privacidad y, principalmente, que las personas que no son parte del grupo no puedan ver a sus miembros.
- Evitar cualquier comentario, foto o video que dé un conocimiento detallado sobre la capacidad estratégica y táctica de un elemento.





Renovar hábitos y estratégias para proteger nuestra información.

Conclusiones

Las redes sociales son una herramienta de indiscutible utilidad, pero de fácil manipulación para quien la controle.

Dada la peligrosidad que representa, este tema merece seguir siendo investigado, puesto que cada vez quedan menos dudas de que las bases de datos de los que controlan las redes sociales podrían ser proporcionadas a centrales de espionaje o entidades interesadas.

Por otro lado, nadie nos garantiza que nuestros datos estén seguros en sus sistemas ni que podremos eliminarlos completamente, llegado el caso de haber publicado información clasificada por descuido.

Por lo tanto, se hace necesario renovar nuestros hábitos y estrategias para proteger nuestra información y aquella que nos delega la Institución para su aseguramiento, sabiendo que los atacantes tienen ahora mayores herramientas y trucos para interrogar nuestros modelos mentales y provocar el tan esperado premio: la fuga de información, y que el atacante conquiste y alcance su objetivo.

Finalmente, sabiendo que el adversario será persistente en su misión de lograr el acceso no autorizado, debemos estar vigilantes y perseverantes en nuestros actos y procedimientos.

Queda, en definitiva, en el criterio y la conciencia de contrainteligencia de cada uno, qué publicar, compartir o "subir" a la red.

Bibliografía

1. Según el ejemplo del Director Senior de Gestión de Productos, Patrick Murray, presentado en su Informe de Websense "Amenazas Persistentes Avanzadas: Del temor, la incertidumbre y la duda a los hechos".

Referencias

- Ing. Jeimy J. Cano. "Amenazas persistentes avanzadas, inteligencia y contrainteligencia en un contexto digital", (pdf).
- Carlos D. Tajer. Revista Argentina de Cardiología. "Las revistas científicas, la inteligencia colectiva y los prosumidores digitales" (2009), (pdf).

Web

- Cano, J. (Diciembre de 2010). "Fuga de la información: Revelando la inseguridad de la información en el factor humano". Publicación en blog. Disponible en: http://insecurityit. blogspot. com/2010/12/fuga-de-la-informacion-revelando-la.html (Consultado: 10-10- 2012).
- Magazicitum (2012). "El magazín de los profesionales de la seguridad para ti". Disponible en: http://www.magazcitum.com.mx/?p=1547 (Consultado: 06-10-2012)