Amenazas persistentes avanzadas, inteligencia y contrainteligencia en un contexto digital

Jeimy J. Cano

Recordar las escenas de agentes encubiertos, revelaciones de información secreta y comandos especializados de asalto, son evocaciones de un pasado, que ahora está presente alrededor del concepto de Amenazas Persistentes Avanzadas. Esta nueva realidad, concentrada en una labor de inteligencia avanzada para recabar información de los empleados de una empresa, establece una renovada estrategia de operaciones especiales, que busca lograr acceso a su infraestructura tecnológica a través del eslabón más débil de la cadena. Por tanto, este documento presenta un análisis sencillo y práctico de esta tendencia, revisando algunas lecciones aprendidas de casos particulares, sugiriendo marcos de acción para enfrentar sus impactos.

Introducción

Dice John Maxwell en su libro "El talento no es suficiente": "La perseverancia no es un asunto de talento. Tampoco de tiempo. Tiene que ver con acabar lo iniciado. El talento provee la esperanza para el logro, pero la perseverancia lo garantiza. (…)". Considerando esta motivadora afirmación, podemos advertir que, aplicada en el *lado oscuro de la fuerza* podemos asistir al escenario de esfuerzos perseverantes de los atacantes para doblegar nuestras defensas y convertirnos en un número más de las numerosas estadísticas de ataques y sistemas comprometidos a nivel global.

Recientemente, venimos observando un renovado interés de los "chicos malos" en el conocimiento de las nuevas tecnologías y tendencias emergentes (computación móvil, computación en la nube y cibercrimen en movimiento) (GROBAUER, B., WALLOSCHEK, T. y STOCKER, E. 2011, GOLDMANN, P. 2011), no para someterlas con la materialización de fallas técnicas, sino como plataformas de enlace para llegar cada vez más a los usuarios y hacerlos parte de sus estrategias de engaño, y así, encontrar nuevas formas de incursionar dentro de los dominios organizacionales y tener acceso a ese activo fundamental para mantenerse competitivo en su sector, como lo es la información.

En este sentido, se abre paso en la literatura técnica de seguridad la sigla APT, en inglés *Advanced Persistent Threat*, cuya traducción en español podría ser *Amenazas Persistentes Avanzadas* -APAv-, la cual no es otra cosa que las nuevas estrategias de los atacantes para tomar por sorpresa a los empleados de las empresas, para comprometer la infraestructura propia de sus organizaciones y tener acceso privilegiado a la información de éstas. Este renovado escenario de ataque, nos muestra que los intrusos mantienen un monitoreo vigilante de la inseguridad de la información, reconociendo en las personas el eslabón más débil de la cadena, para superar las barreras tecnológicas que las empresas puedan tener en su perímetro.

Por tanto, en este breve documento presentaremos algunos detalles de esta nueva tendencia de ataque coordinado y avanzado, para comprender la nueva dinámica emergente de amenazas, que aprovechándose de la movilidad de los usuarios y su marcada necesidad de ubicar sus recursos en la nube, son capaces de estudiar sus comportamientos y perfiles para hacerlos "víctimas útiles", para penetrar las defensas técnicas de las empresas y ganar acceso más allá de lo autorizado.

El ser humano: ¿eslabón más débil o más fuerte de la cadena? Ese es el reto. (CANO, J. 2010)

La información fluye a través de los diferentes medios informáticos que tenemos disponibles. Internet, es la autopista natural donde nos comunicamos y encontramos, para lo cual cada vez que enviamos un mensaje de texto, remitimos un correo electrónico o diligenciamos un formulario en la web, estamos abonando a nuestra sombra digital (LOHR, S. 2008) (lo que dicen los datos disponibles en internet sobre cada uno de nosotros), la cual es y podrá ser interpretada por los intrusos en cualquier momento.

En este contexto, 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 industriales de las empresas.

Teniendo en cuenta lo anterior, con la sobrecarga incremental de información que circula en la red y fuera de ella, establecemos un escenario ideal para ser objeto de engaños y manipulaciones, que vulneren los principios básicos de nuestra privacidad, de la esfera personal, que antes de ser propia de una sociedad dominada por la necesidad de información instantánea, era custodiada y resguarda por la poca movilidad de la misma. Así las cosas, se hace necesario renovar nuestros hábitos y estrategias para proteger nuestra información y aquella que se nos delega 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, que conquiste y alcance su objetivo.

Revisando la etimología de la palabra fuga, encontramos que viene de la palabra *fugare* (en latín espantar, hacer huir), deriva de *fugere* (huir), por esta razón en latín fuga significa las dos cosas: persecución y huída. (Tomado de: http://etimologias.dechile.net/?fugar)

Considerando el origen de la palabra en español y su origen latino, la fuga es un acto en el cual se da una huída y a la vez una persecución. Podría decirse que no existe la huída sin una persecución. Necesariamente el acto de huir, exige una causa que anima a una de las partes a desaparecer del escenario para tratar de evitar ser visto o identificado y hacer más exigente la persecución por la otra parte interesada.

Con los recientes acontecimientos relacionados con la fuga de información (en inglés *information leakage*) se revelan muchos de los secretos mejor guardados de las naciones y la agenda paralela que se mantiene entre los gobiernos para conservar los lazos diplomáticos y acuerdos estratégicos. Si revisamos con cuidado lo que ha ocurrido podemos tener diferentes lecturas y motivaciones para calificar los hechos, bien como la mayor brecha de seguridad que se haya realizado o un acto de real libertad de información.

En cualquiera de los dos casos tenemos una fuga de información, que necesariamente genera una persecución, bien por haber expuesto información clasificada como secreta o altamente secreta, o bien por publicar y mancillar la privacidad natural y propia, tanto de las personas naturales como jurídicas. En este contexto, todos tenemos cosas que sabemos son restringidas y propias de nuestra intimidad, que estamos dispuestos a preservar de la mirada de otros, no porque sean ilegales o prohibidas, sino porque hacen parte de nuestra realidad y personalidad propia. Por tanto, todas las acciones que emprendamos para defendernos ante esta situación estarán justificadas frente a la magnitud de los hechos, sabiendo que las consecuencias de estas acciones tendrán efectos a corto, mediano y largo plazo e impactos en la reputación y buen nombre de los involucrados.

Amenazas persistentes avanzadas -APAv-: una tendencia orientada a los empleados de las empresas

Considerando los impactos que puede tener una fuga de información a nivel corporativo y los constantes intentos de los intrusos por alcanzar las infraestructuras tecnológicas de las empresas, vía la práctica del engaño y manipulación de información disponible en internet, se hace evidente una tendencia o vector de ataque, que busca como objetivo contar con un grado de control de la infraestructura vulnerada, actuando persistentemente para retener el acceso y las posibilidades que éste brinda.

En este sentido, Richard Betjlich, detalla los elementos básicos del adversario que actúa siguiendo los elementos de una APAv, con el fin de comprender mejor su motivaciones y movimientos que nos permitan, más adelante, establecer algunas contramedidas para limitar el accionar de este tipo de amenazas, que buscan comprometer la esencia misma de la ventaja competitiva de las empresas, como lo es su información: (BEJTLICH, R. 2010)

Amenaza significa que el adversario no es una pieza de código sin sentido, al contrario, es una persona motivada, financiada y organizada, que busca un objetivo particular, para lo cual estará bien rodeada y asistida para lograr la misión designada.

Persistente significa que el adversario tiene una tarea que cumplir y que insistirá en ella hasta lograrla. En este sentido, persistente no significa necesariamente que buscará ejecutar un código malicioso en el computador víctima, sino mantener el nivel de interacción necesario para alcanzar sus objetivos.

Avanzada quiere decir que el adversario puede operar un amplio espectro de posibles intrusiones informáticas; es decir, puede utilizar desde las más evidentes y publicitadas vulnerabilidades o elevar el nivel del juego, para investigar o desarrollar nuevas debilidades o fallas, dependiendo de las prácticas de seguridad y control de la empresa objetivo.

Como quiera que este tipo emergente de amenazas no es nuevo, en cuanto se basa en un componente eminentemente humano y asociado con comportamientos de las personas frente al tratamiento de la información, sí representa una importante novedad, cuando se trata de operaciones digitales asistidas con propósitos de espionaje y desinformación, aplicados sobre objetivos gubernamentales, militares o privados.

Casos recientemente publicados y ampliamente difundidos dan cuenta de que este tipo de amenazas han cobrado importantes organizaciones, poniendo en tela de juicio sus posturas frente a la seguridad de la información. A continuación se detallan algunos de ellos, como fuente de documentación y lecciones aprendidas: (SAVAGE, M. 2011)

- El ataque a la firma RSA inició con dos correos phishing con asunto: "2011 Recruitment Plan", enviado a dos pequeños grupos de empleados. Un empleado dio *click* en una de las hojas electrónicas adjuntas en el correo, el cual contenía un *exploit* de día cero, lo cual abrió una brecha de seguridad dentro de la empresa, lo que permitió que los atacantes tuviesen acceso a los sistemas de información críticos de la empresa y paso a la información relacionada con los productos SecureID, del cual son líderes en la industria de seguridad informática.

- Así mismo, tenemos el ataque del grupo "Anonymous" a la firma de seguridad HBGary Federal a comienzos de este año. El ataque consistió en efectuar un engaño a un administrador de red, para que se diese acceso al sitio Rootkit.org, sitio web de investigaciones en seguridad informática mantenido por el fundador de la empresa *Greg Hoglund*, ocasionando desde allí un ingreso no autorizado a la empresa, ganando acceso a los sistemas interno de correo electrónico con datos sensibles y otra información crítica de la misma.

- Finalmente, el ataque a Google efectuado el año anterior, donde los atacantes recolectaron información publicada por los empleados de la firma en redes sociales como *facebook* y *linkedid*. 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, la personas hacía *click* 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.

APAv, lecciones aprendidas y algunas por aprender

El foco fundamental de una APAv es atacar a los usuarios y no a las máquinas. Es un movimiento psicológico y de comportamiento basado en la información misma de las víctimas, que genera una falsa sensación de seguridad que permite al atacante tener acceso a la infraestructura interna de las organizaciones. En este sentido, es necesario establecer iniciativas de monitoreo de

cruce de información, balancear la necesidad natural de los empleados por descargar información, permitir dispositivos móviles en las redes internas y el acceso a redes sociales; un mundo de intereses cruzados que enfrenta los derechos fundamentales de los individuos y la exposición a los riesgos propia de las empresas con presencia en internet.

¿Qué hemos aprendido de los múltiples casos de uso efectivo de las APAv? Hagamos una mirada crítica sobre tres elementos fundamentales:

1. Nuestra naturaleza orientada a confiar en los demás. Esta condición sana y generosa que dentro de las empresas se genera por un ambiente de camaradería y motivación al trabajo en equipo, se ve mancillada y desvirtuada, frente a las APAv, toda vez que la información expuesta de las personas de la empresa en internet, opera como estrategia de inteligencia para abrazar la confianza de una comunidad, que de manera inadvertida acepta y entiende, que de personas conocidas podemos aceptar mensajes o comunicaciones, generando graves brechas de seguridad que comprometen el buen nombre y los activos intangibles de la empresa.

2. Manejo de las expectativas de las personas. Esta situación propia de los seres humanos se ve oscurecida, cuando un tercero es capaz de conocer o inferir este tipo de deseos o anhelos, en los cuales encuentra el mejor motivador y motor para capturar la atención de sus víctimas. En este sentido, información sobre ascensos, ingresos, nuevos beneficios o incluso retiros de personas de las empresas, se vuelve sensible y clave a la hora de lanzar estratégicamente engaños electrónicos, relacionados con las esperanzas e intereses de las personas en las organizaciones.

3. El afán de compartir información: si no estás en las redes sociales, no existes. Estamos en un mundo donde la información fluye todo el tiempo. Es nuestro deber, saber qué debe circular y qué no, qué información voy a compartir y cuáles serán sus implicaciones al hacerlo. Debemos tomar mejores decisiones informadas sobre los riesgos derivados de ubicar información en los medios electrónicos, sabiendo que al hacerlo estamos minando nuestro propio derecho a la privacidad y control de la misma. Así, mientras más conscientes seamos de la información que tenemos y compartimos, mejores experiencias tendremos al interactuar en la red.

Todo esto nos lleva indefectiblemente a cuestionarnos sobre el contexto futuro y emergente que nos traen las nuevas tendencias tecnológicas y propuestas de servicios, que no hacen otra cosa que motivarnos a mantener información en otros dominios, compartir información con otras personas y movilizarnos todo el tiempo sin restricciones de cables o lugares. Por tanto, se requiere hacer un pare en el camino y comenzar a desaprender nuestros comportamientos actuales y concretar algunas recomendaciones para disfrutar de manera responsable este nuevo entorno abierto, móvil y dinámico que nos proponen los nuevos desarrollos.

En este contexto, a continuación detallamos algunas lecciones que tenemos por aprender frente a los avances de las APAv, que prometen continuar sorprendiendo ahora en un universo personalizado en la nube y con empoderamiento permanente de los usuarios frente al uso de las tecnologías de información y comunicaciones.

1. *Insistir en el valor de la información como activo crítico empresarial.* ¿Por qué no le duele a las personas la información de la empresa? ¿Por qué sólo hasta cuando algo ocurre nos interesamos en el tratamiento de la información? La respuesta es sencilla, no existe un vínculo formal que permita valorar la información, como las cosas propias que afectan la vida de cada individuo. La información es algo externo a su realidad, que sólo es considerada importante, cuando la misma te afecta como persona en cualquier contexto de la vida.

2. *Clasificar la información como práctica natural del tratamiento de la información*. Todos sabemos que manejamos información privada y pública. Nadie quiere que se conozca parte de su vida y obra, a menos que cada uno lo autorice formalmente. De igual forma debería funcionar con la información empresarial, toda ella representa la vida y obra de la firma, mucha de ella habla de cosas que sólo le pertenece a la empresa, mientras otra está diseñada para ser compartida con el entorno. Así, mientras este ejercicio intuitivo que hacemos de manera personal no sea una práctica natural en el entorno corporativo, continuaremos escuchando historias que nunca se debieron contar.

3. *Promover sistemas de inteligencia y monitoreo preventivo sobre el flujo de información empresarial*. Esta consideración advierte a las organizaciones que deben avanzar en el desarrollo de nuevas capacidades de detección de patrones competitivos y de amenazas informáticas en el contexto de sus relaciones de negocio, para establecer acciones preventivas que permitan anticiparse a futuros ataques o amenazas. Esto significa, que la información no será solamente un activo crítico, sino la fuente misma de las acciones de la organización, frente a los retos de seguridad de la información que le sugiera su entorno, teniendo la capacidad de cambiarlo si es necesario.

Reflexiones finales

Cuando hablamos de Amenazas Persistentes Avanzadas –APAv-, no estamos caminando por terrenos tecnológicos o de propuestas de investigación y desarrollo novedosas; estamos recorriendo los senderos de la mente humana, sus motivaciones y sus condiciones en un escenario corporativo. De hecho, estamos caminando por los pasillos de importantes empresas comerciales, con intereses económicos fundados en información crítica como pueden ser patentes, estrategias empresariales o eventos internos que pueden desequilibrar el buen momento de una compañía.

En este escenario, estamos recreando condiciones históricas de espionaje y filtración de información del pasado, donde agentes encubiertos podían establecer importantes contactos y crear redes de manejo de datos, que permitían generar posiciones privilegiadas a empresas o naciones, las cuales eran transportadas o manejadas en sistemas rudimentarios de almacenamiento como microfilms, discos magnéticos o en sencillas cintas magnetofónicas. Así las cosas, ahora en un mundo interconectado, no es necesario estar en los sitios físicos para lograr el objetivo, basta una operación digital planeada para revelar aquello que se había cuidado y poner en aprietos a las empresas más grandes, a través de los más pequeños en la cadena: sus empleados. (BEJTLICH, R. 2010)

Conocer y advertir este tipo de estrategias de inteligencia informática, exige de cada una de las organizaciones, afianzar sus esfuerzos de entrenamiento y prácticas asociadas con el tratamiento de la información, porque cada vez más habrá "comandos especializados" que adelanten operaciones focalizadas para tener información sensible que requiere un tercero, utilizando como puente a alguno de los empleados. Por tanto, mientras más conciencia se tenga del nivel de exposición frente al manejo de la información, mejor será el "mínimo de paranoia administrable" que cada una de las personas debe tener.

En consecuencia y sabiendo que la situación no habrá de mejorar en el corto plazo, desarrolle una función de contrainteligencia informática sustentada en la formación y desarrollo de "firewalls" humanos, que compartiendo información y advirtiendo situaciones fuera de lo establecido, pueda distinguir la asimetría de la inseguridad de la información, a través de patrones de comportamiento emergentes y divergentes.

Finalmente y sabiendo que el adversario será persistente en su misión para lograr el acceso no autorizado, debemos advertirle, que aunque no conocemos qué nuevo movimiento estará planeando, sí estaremos vigilantes y perseverantes para hacerles la vida más difícil, aprendiendo de nuestra maestra la inseguridad de la información.

Referencias

[1] BEJTLICH, R. (2010) Understanding the advanced persistent threat. Information Security Magazine. July. Disponible en: http://searchsecurity.techtarget.com/magazineContent/Understanding-the-advanced-persistent-threat (Consultado: 6-06-2011)

[2] SAVAGE, M. (2011) Gaining awareness to prevent social engineering techniques attacks. Information Security Magazine. May. Disponible en: http://searchsecurity.techtarget.com/magazineContent/Gaining-awareness-to-prevent-social-engineering-techniques-attacks (Consultado: 6-06-2011)

[3] GOLDMANN, P. (2011) Cyber fraud: Why are we still being victimized. Report. White-Collar 101 LLC.

[4] GROBAUER, B., WALLOSCHEK, T. y STOCKER, E. (2011) Understanding cloud computing vulnerabilities. IEEE Security & Privacy. March/april.

[5] CANO, J. (2010) Fuga de la información: Revelando la inseguridad de la información en el factor humano. Diciembre. Publicación en blog. Disponible en: http://insecurityit.blogspot.com/2010/12/fuga-de-la-informacion-revelando-la.html (Consultado: 6-06-2011)

[6] LOHR, S. (2008) Measuring the size of your digital shadow. New York Times. Disponible en: http://bits.blogs.nytimes.com/2008/03/11/measuring-the-size-of-your-digital-shadow/ (Consultado: 6-06-2011)

Jeimy J. Cano, Ph.D, CFE. *Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Ph.D en Administración de Negocios de Newport University, CA. USA. Executive Certificate in Leadership and Management del MIT Sloan School of Management. Profesor Distinguido y miembro del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática de la Facultad de Derecho de la Universidad de los Andes. Examinador Certificado de Fraude – CFE por la ACFE y Cobit Foundation Certificate por ISACA.*