Internet y nuevas tecnologías

Roberto Plá
Coronel del Ejército del Aire
http://robertopla.net/

CIBERGUERRA

ATAQUES A INFRAESTRUCTURAS CRÍTICAS DE ARABIA SAUDÍ

McAfee Strategic Intelligence es un equipo de investigación de ciberamenazas que se dedica solo a la ciberguerra y los incidentes de crimen cibernético más complejos. Uno de sus estudios más recientes, publicado en el *blog* corporativo, ha revelado que una serie de ataques cibernéticos en Arabia Saudí muestran un patrón que sugiere que no proceden de grupos pequeños de *hackers* o individuos aislados, sino que se trata de una organización que realiza sus ataques con un objetivo malicioso común.

Los ataques cibernéticos, dirigidos específicamente a Arabia Saudí, se produjeron entre el año 2012 y el presente y son el trabajo de grupos bien apoyados y coordinados de *hackers*, y no los esfuerzos al azar de diversos grupos de ciberdelincuentes regionales.

Shamoon, también conocido como Disttrack, es un virus informático modular descubierto por Seculert en 2012, dirigido a las recientes versiones basadas en *kernel* de NT de Microsoft Windows. El virus ha sido utilizado para el espionaje cibernético en el sector energético en Oriente Medio y las últimas campañas que han utilizado este software malicioso van más allá de algunos objetivos en plantas de energía, su objetivo inicial, para diversificar sus ataques hacia otros sectores críticos de Arabia Saudita.

Las anteriores campañas de ataques con Shamoon apuntaron a un número relativamente pequeño de organizaciones del sector energético, con el objetivo de interrumpir las operaciones de la industria crítica de la región. Los nuevos ataques se concentran en un mayor número de organizaciones

en los sectores de energía, gobierno, servicios financieros e infraestructura crítica con el evidente objetivo de perturbar el país entero.

La naturaleza de estas últimas campañas a gran escala, por su sofisticación y coordinación sugieren el liderazgo de un actor de tipo estado-nación. En conjunto, esta oleada de ataques de espionaje cibernético de Shamoon es significativamente más grande, bien planificada, bien dotada de recursos y coordinada a un nivel más allá de la limitada capacidad de pandillas de *hackers* independientes.

Los ataques se inician mediante el envío de correos electrónicos a objetivos cuidadosamente elegidos invitándoles a pulsar sobre un enlace que descarga un archivo de Microsoft Office con macros maliciosas que funcionan como una cabeza de puente del ataque, permitiendo el acceso de 'exploradores' que recorren la red en busca de información útil; finalizado el reconocimiento y extraída o no la información, el *malware* ataca el disco anfitrión destruyendo su registro central, el *Master Boot Record* (MBR) que comprende los primeros 512 bytes de un dispositivo de almacenamiento. El MBR no es una partición; está reservado al cargador de arranque del sistema.

DISPOSITIVOS MÓVILES

SAGITTARIUS

En el campo de batalla moderno no solo es necesario localizar con exactitud las coordenadas del objetivo, sino conocer con precisión la posición de nuestras fuerzas, al tiempo que estas reciben información de su entorno y transmiten la información captada por los sensores que transportan a la red de mando y control, en beneficio de la artillería, la aviación y los organismos de mando así como de los que deben generar inteligencia para apoyar las decisiones de este.

Por ello, los diferentes programas de desarrollo del equipo del combatiente del futuro han dotado al componente terrestre de sofisticados sistemas que realizan funciones de comunicaciones, transmisión de datos, geoposicionamiento y reconocimiento, así como de sistemas de apoyo a la precisión de las armas que les acompañan.

En el caso del programa Ratnik, de las fuerzas armadas de la federación rusa, el componente denominado Sagittarius proporciona los servicios de comunicaciones por voz y video, geoposionamiento mediante el sistema ruso basado en satélites GLONASS, tiene la forma de una tableta reforzada

y el tamaño de un libro y permite a los mandos de una fuerza terrestre comunicarse con los fusileros, que disponen de un equipo reducido, del tamaño de un radioteléfono. Producido por la empresa Radioavionika, dispone de periféricos y puede conectarse prácticamente a cualquier dispositivo.

El programa Ratnik entregó los primeros equipos en 2013 y su utilización en combate fue detectada a partir de 2016. El programa completo, similar al COMFUT desarrollado por las Fuerzas Armadas españolas, comprende todo el equipo del combatiente: desde el casco y los sensores más complejos hasta las protecciones que cubren el 90 % del cuerpo, auténtica armadura que permite la supervivencia a disparos del calibre 7,62, o las prendas textiles, atalajes y bolsas de transporte del equipo.

Sin embargo, la electrónica asociada al equipo no tendría ninguna utilidad si no fuera actualizada de forma constante; y en ese sentido, la infantería de marina rusa ha sido dotada recientemente del último modelo de este dispositivo, cuyo uso en las operaciones en Siria ha mostrado que es perfectamente capaz de obtener con precisión las coordenadas del objetivo y su transmisión oportuna no solo en beneficio de aviones y artillería, sino también de misiles contra superficie del tipo X-35 con un alcance de unos 300 km. y que pueden ser lanzados desde barcos, aviones o incluso vehículos no tripulados. Los analistas señalan la dificultad añadida de dirigir el fuego de la artillería naval, que se realiza por baterías que se hallan a su vez en movimiento y califican a los equipos Sagittarius como completamente efectivos en esta misión.

Las primeros tabletas de este tipo comenzaron a ser utilizados por unidades especiales en las fuerzas armadas de los países desarrollados hace varios años. Por ahora, el Commando Hubert francés, los Seals estadounidenses, el Sexto Comando de la Armada alemana y los buceadores del grupo de operaciones especiales de la Armada británica, el Special Boat Service, usan en gran medida este tipo de productos, pero su uso se está convirtiendo en un complemento imprescindible de cualquier combatiente.

HACKERS

HACKERS RUSOS DETENIDOS EN ESPAÑA

La Guardia Civil detuvo el pasado 13 de enero de 2017, en el aeropuerto de El Prat (Barcelona) al ciudadano ruso Stanislav Lisov. La detención se produjo como consecuencia de una orden de busca y captura emitida por el FBI a través de la Interpol. Lisov es informático de profesión y trabaja como especialista informático en la ciudad de Taganrog, a orillas del mar Negro. Se encontraba en la capital catalana acompañado de su mujer después de haber disfrutado de unas vacaciones en la costa de Tarragona.

Debido a que la detención se realizó en medio de la tormenta mediática sobre el supuesto ataque por *hackers* rusos de los ordenadores del Partido Demócrata durante la campaña presidencial, su detención fue relacionada por la prensa con estos hechos aunque desde Estados Unidos se le reclamaba por liderar una red de fraude financiero.

En el momento de su detención, el ciudadano ruso llevaba bajo vigilancia de las autoridades varios días. Lisov era investigado por Estados Unidos desde hace dos años por desarrollar y utilizar NeverQuest, un virus informático que se propaga a través de redes sociales, correo electrónico y transferencias de archivos que ha provocado pérdidas estimadas en millones de dólares.

En el mes de abril, fue la policía la que detuvo a otro *hacker* ruso, un conocido criminal tecnológico de origen ruso en su hotel de Barcelona donde había llegado recientemente con su esposa. La detención fue llevada a cabo tras una orden de detención internacional emitida por el FBI estadounidense.

Pyotr Levashov está acusado de diferentes delitos por infectar miles de ordenadores con *ransomware*, un tipo de software malicioso que sirve para secuestrar el sistema informático infectado y que pide dinero a sus usuarios a cambio de liberarlo.

Esa infección de *ransomware* la llevaba a cabo supuestamente Levashov a través de una red de ordenadores esclavos (*botnets*), llamada *Kelihos* y que controlaba desde 2016.

El Ministerio de Exteriores ruso criticó con dureza el arresto, acusando a Washington de organizar una "caza al hombre" de ciudadanos rusos alrededor del mundo. La agencia de noticias rusa RT, controlada por el gobierno, recogió las declaraciones del vicepresidente de la filial rusa del Comité Internacional de Derechos Humanos, Alexander Ionov, quien calificó el arresto de una violación del derecho internacional.

El director del FBI, James Comey, en su comparecencia ante el Comité Judicial del Senado el pasado 05 de mayo agradeció la colaboración de la policía española y se congratuló del hecho de que la detención del *hacker* hubiera permitido la liberación de numerosos ordenadores 'secuestrados'. •

Las páginas consultadas como fuentes para estas reseñas están recopiladas en la siguiente dirección: https://del.icio.us/rpla/raa864