

Preparación de la Inteligencia del Entorno de Información y Comunicaciones

JEFFREY CARR

MIENTRAS QUE LA Preparación de Inteligencia Conjunta del Entorno de Operación (JIPOE) es para fines ofensivos, este artículo propone una función que el autor ha llamado Preparación de Inteligencia del Entorno de Información y Comunicaciones (IPICE) que, si se implementa, mejorará la táctica defensiva por medio de entidades comerciales así como gubernamentales. Los componentes de IPICE pueden invertirse y aplicarse de manera ofensiva contra un objetivo extranjero, sin embargo ese es un tema para un artículo diferente.

La tendencia actual entre compañías de seguridad de información es “seguridad impulsada por la inteligencia”. Lockheed Martin puede haber iniciado el concepto gracias al trabajo de sus empleados como Eric M. Hutchins, Michael J. Cloppert y Rohan M. Amin que escribieron el artículo “Defensa de redes de computadoras impulsadas por inteligencia informada por análisis de campañas del adversario y cadenas de aniquilamiento de intrusión”¹. Cloppert creó más adelante un modelo muy detallado para ataques de APT² que condujeron al artículo al que se hace referencia arriba y del que RSA tomó prestada amplia información de su artículo “Adelantarse a las amenazas avanzadas: logro de seguridad de información impulsada por la inteligencia”³.

Hoy en día, el modelo de Lockheed Martin es utilizado ampliamente entre los miembros de la Base Industrial de Defensa (DIB) y el Centro de Delitos Cibernéticos de Defensa del Departamento de Defensa que envía inteligencia de amenazas a la DIB. De hecho, Lockheed recientemente ganó un contrato⁴ de más de 400 millones para proporcionar investigaciones digitales y soporte de análisis a DC3. Aunque este sistema da buen resultado para la finalidad prevista, representa un punto de vista inadecuado del conjunto de amenazas en general. Esto se debe en gran parte a los vendedores de seguridad que apoyan a la DIB y a la mayor parte de las compañías Fortune 500 con sus soluciones de ciberseguridad; soluciones que tienen una eficacia limitada contra objetivos deseados y un alcance muy limitado del entorno operacional de una compañía.

Antes de que una corporación privada o el gobierno federal puedan evaluar la eficacia de cualquier proceso de ciberseguridad, especialmente algo llamado “impulsado por la inteligencia”, es necesario ver por completo el conjunto de amenazas u entorno medioambiental de la organización. La cadena de aniquilamiento de intrusión de Lockheed Martin solamente se fija en ataques típicos estilo APT que se basan en “spear phishing” con anexos de correos electrónicos, que alienta al lector a hacer clic en un enlace malicioso, y cargas útiles maliciosas suministradas a través de medios removibles. Los defensores de este método dicen que representa la mayoría de los ataques que observan. El objetivo de este artículo es dar una imagen más completa del conjunto de amenazas usando la Preparación de Inteligencia Conjunta del Entorno Operacional (JIPOE) del Departamento de Defensa.⁵ La JIPOE puede servir como modelo efectivo para crear un plan de seguridad completo de Tecnología de Información y Comunicación (ICT) basado no en el conjunto de amenazas limitadamente definidas en la actualidad (es decir, Lockheed Martin y la cadena de aniquilamientos de intrusión de RSA) sino en una imagen operacional más completa. A continuación indicamos un resumen de la JIPOE según se describe en la Publicación Conjunta 2-01.3:

Primer paso de la JIPOE: Definición de un entorno operacional

- Identificar el área operacional

- Determinar las características significativas del entorno operacional
- Determinar las lagunas de inteligencia e información

Segundo paso de la JIPOE: Describir el impacto del OE

- Desarrollar una perspectiva geoespacial del OE
- Desarrollar una perspectiva del sistema del OE

Tercer paso de la JIPOE: Evaluación del adversario

- Actualizar o crear modelos de adversario
- Determinar la situación del adversario actual
- Identificar las capacidades y vulnerabilidades del adversario

Cuarto paso de la JIPOE: Determinación de los cursos de acción de adversario

- Identificar los objetivos probables del adversario y el estado final deseado
- Identificar el conjunto completo de COA del adversario

He simplificado los pasos anteriores de cuatro a tres, a saber:

1. Definir la superficie de ataque (es decir, entorno operacional)
2. Evaluar al adversario
3. Determinar los cursos de acción del adversario

¿Qué es “Inteligencia”?

La palabra inteligencia en la frase “ciberinteligencia” es utilizada de forma confusa por la industria de seguridad de información y los medios de comunicación. A veces se usa de forma intercambiable con datos de “malware”. Otras veces, se usa para describir investigaciones de código abierto de Anonymous y otros piratas. La palabra “ciber” tiene sus propios problemas de definición, por lo que para las intenciones de este artículo, el autor recomienda la de Nicolas Eftimiades, autor de la definición de “Operaciones de inteligencia china”⁶ que en realidad es más una descripción informal del proceso de inteligencia tradicional:

“Las agencias de inteligencia mundiales comparten el mismo objetivo general: proporcionar inteligencia precisa y oportuna a sus consumidores. Para ello reúnen información sin procesar de una variedad de fuentes humanas y técnicas. Después deben cotejar y analizar estos datos para separar la realidad de la ficción y opinar sobre una variedad de sucesos pasados, actuales y futuros. El producto analítico completo, inteligencia, se disemina después al consumidor, cuyo requisito de información empezó el proceso. Esa persona o ese grupo está entonces en una posición para pedir un análisis adicional o implementar una política basada en la inteligencia recibida. Todo el proceso se denomina ciclo de inteligencia”.

La superficie de ataque

Una Corporación Multinacional (MNC) tiene una vasta superficie de ataque. Antes de poder construir una estructura de seguridad eficaz, se necesita establecer la superficie de ataque. El entorno de información de una corporación, un gobierno o una organización militar incluye amenazas internas y externas. La amenaza interna, lo que significa una acción hostil contra la compañía por parte de un empleado, es un problema activo y a menudo sin reportar para muchas compañías y una que normalmente cuesta más que los incumplimientos por parte de agentes externos.⁷ Otra forma de amenaza interna es lo que ocurre cuando una compañía contrata a ingenieros extranjeros para dotar a sus oficinas de investigación y desarrollo en China, Rusia, Francia y otros países. Mientras estén empleados en la compañía, estos ingenieros adquieren

información propietaria que se llevan cuando dejan de trabajar para empezar a trabajar en una compañía dirigida por el estado con intereses similares en uno o dos años. A esto se le denomina “transferencia de tecnología”.

Entre las amenazas externas se incluyen muchos más vectores de ataque que los usados por ataques de estilo APT. Se incluye lo siguiente entre otras cosas:

- A las oficinas de las compañías de fuera de Estados Unidos que están sujetas a leyes de ICT extranjeras sobre recopilación de información se les puede interceptar y monitorear legalmente todas sus comunicaciones. Esto incluye correo electrónico, VOiP, móvil, terrestres, satélite y VPN.
- Es posible que se requiera a las corporaciones multinacionales proporcionar su código a servicios de inteligencia extranjeros para la inspección a fin de asegurar que no plantee ninguna amenaza a su seguridad nacional. De no cumplir con esto, significaría ser detenido y no poder realizar actividades comerciales dentro de las fronteras de ese país.
- Empleados de la compañía, particularmente ejecutivos, que ponen en riesgo sus dispositivos al irse de viaje al extranjero.
- Los vendedores extranjeros a los que la compañía contrata pueden estar afiliados con su gobierno autóctono y pasar secretos comerciales a ese gobierno a petición gracias a su acceso autorizado a la red de compañías de EE.UU.
- Los subcontratistas, las subsidiarias y los socios estratégicos de los vendedores pueden tener afiliaciones con su gobierno autóctono y hacer lo mismo de arriba.

Evaluar el adversario

Hay 28 naciones estado⁸ que tienen capacidades de guerra/espionaje cibernéticos. Muchas de ellas tienen conocidas relaciones con grupos de piratas y un número creciente dispone de milicias de voluntarios adiestrados para operar en el ciberespacio. Mientras que las capacidades rusas⁹ y chinas¹⁰ se han documentado ampliamente, el Consejo Nacional de Autoridad de India dispone de autoridades para ciberoperaciones ofensivas asignadas a la Agencia de Inteligencia de Defensa y a la Organización Nacional de Investigación Técnica¹¹. La Unidad 8200 de Inteligencia Militar de Israel y su Directorado C4I han anunciado una operación de reclutamiento entre los piratas de élite de Israel¹². Actualmente los siguientes países disponen de comandos equivalentes o basados en el Cibercomando de EE.UU.: Australia, Brasil, Bulgaria, Canadá, China, Chequia, Estonia, Finlandia, Francia, Georgia, Alemania, India, Irán, Israel, Italia, Myanmar, Países Bajos, Corea del Norte, Pakistán, Polonia, Rumania, Rusia, Singapur, Sudáfrica, Corea del Sur, Suecia, Taiwán, Ucrania y Zimbabue. De éstos, los estados más activos que participan en ataques de ciberespionaje por medio de actores estatales y no estatales son Brasil, Bulgaria, China, Francia, Georgia, India, Irán, Israel, Países Bajos, Corea del Norte, Rumania, Rusia, Corea del Sur, Taiwán y Ucrania. Las compañías multinacionales de EE.UU. que tienen oficinas en estos estados deben considerar que sus redes están ya intervenidas y tomar las medidas apropiadas para mitigar los efectos de ese estado.

Autoridades legales de servicios de inteligencia extranjeros

Tanto Rusia como China han promulgado leyes que dan a sus servicios de seguridad respectivos mucha libertad para recopilar información de corporaciones extranjeras que disponen de oficinas dentro de sus fronteras. A continuación se indica una encuesta de lo que significan esas leyes para las compañías extranjeras, sin embargo eso no se aplica solamente a Rusia y China. India ha estado utilizando agresivamente tácticas similares y otros países disponen de sus propias

políticas y procedimientos. El Centro de Operaciones de Seguridad y el Consejo Principal de cada MNC debe ser consciente del impacto que estas autoridades tienen en su compañía y sus datos sensibles.

Ley de Seguridad del Estado de la República Popular China

La Ley de Seguridad del Estado de la República Popular China (RPC) gobierna la forma en que pueden operar los servicios de seguridad de China y obliga a la participación de su población si se le pide. En otras palabras, si usted es un visitante que se hospeda en un hotel de Shanghai, el personal de ese hotel debe cooperar con cualquier solicitud del servicio de seguridad para darle acceso a su habitación sin su conocimiento o consentimiento si se presenta como un asunto de seguridad estatal. Aquí hay algunas partes relevantes de las leyes, que pueden encontrarse completas en china.org.cn:

Artículo 8. Cualquier funcionario de un órgano de seguridad del Estado, al ejecutar una tarea de seguridad del Estado, puede entrar en cualquier sitio interesado después de presentar un certificado apropiado, y puede, según las estipulaciones pertinentes del Estado, con aprobación y después de producir un certificado apropiado, entrar en áreas, sitios o unidades restringidas interesadas; y puede tener acceso a archivos, materiales y artículos relacionados para su examen.

Artículo 10. Donde el reconocimiento de una acción que pone en peligro la seguridad del Estado, un órgano de seguridad del Estado puede emplear, según las disposiciones pertinentes del Estado y después de pasar estrictos procedimientos de aprobación, medios de reconocimiento tecnológicos.

Artículo 11. Donde la seguridad del Estado lo requiera, un órgano de seguridad del estado puede inspeccionar los instrumentos y aparatos de comunicación electrónicos y otros equipos e instalaciones similares que pertenezcan a cualquier organización o individuo.

Artículo 16. Los ciudadanos y las organizaciones deben proporcionar comodidades u otra asistencia para el trabajo de seguridad del Estado.

Artículo 18. Cuando el órgano de seguridad del Estado investiga y averigua cualquier circunstancia que pone en peligro la seguridad del Estado y reúne evidencia relacionada, los ciudadanos y las organizaciones interesados deben suministrar lealmente la información pertinente y no pueden rechazar hacerlo.

Ley Federal de la Federación Rusa No. 40

La versión rusa de la ley china anterior se denomina Ley Federal No. 40 "Sobre el Servicio de Seguridad Federal (FSB)". La ley original se promulgó en 1995 y la última enmienda se promulgó en 2008. Capítulo II Artículo 8 establece las actividades autorizadas principales del FSB. Son, a saber:

- actividades de contrainteligencia;
- combate del terrorismo;
- combate de la delincuencia;
- actividades de inteligencia;
- actividades en la frontera;
- garantizar la seguridad de información.

La seguridad de información se considera una actividad principal, no subsidiaria. Los diversos artículos siguientes dan más detalles sobre cada actividad específica, a menudo con implicaciones de seguridad de información. Por ejemplo, las actividades de contrainteligencia incluyen la autoridad para monitorear comunicaciones. De hecho, las medidas para asegurar la información mediante actividades de monitoreo y recopilación aparecen de forma clara en los artículos.

Observe que el FSB está autorizado a llevar a cabo actividades de inteligencia, específicamente actividades de inteligencia extranjera, aun cuando Rusia mantiene un Servicio de Inteligencia Extranjero (SVR) separado. La ley indica que las operaciones de inteligencia extranjeras se hacen según acuerdos conjuntos con el SVR.

El Artículo 11.2 establece los detalles de actividad de seguridad de información. Son, a saber:

- la formación e implementación de una política pública y científico-técnica en el campo de la seguridad de información, incluido el uso de medios de ingeniería y criptográficos;
- proporcionar métodos criptográficos y de ingeniería de seguridad para sistemas de información y telecomunicación, y sistemas codificados, secretos y los otros tipos de comunicaciones especiales en Rusia y agencias rusas ubicadas fuera de Rusia.

En resumidas cuentas, la autoridad de seguridad de información del FSB es muy amplia. Establecen una política administrativa y técnica. El FSB está a cargo efectivamente de la infraestructura criptográfica de Rusia con autoridad sobre software y hardware. De hecho, el Artículo 3 pone a la Academia de Criptología de Rusia, nominalmente una institución académica, bajo la autoridad ejecutiva federal para seguridad, el FSB. Las regulaciones de implementación del FSB indican específicamente que el FSB opera la Academia de Criptología. La implementación de regulaciones, firmada por el entonces Presidente Putin, proporciona los detalles adicionales dando al FSB la autoridad de regular el desarrollo, la importación, la venta y la exportación de tecnologías criptográficas. Las regulaciones de implementación también permiten al FSB ayudar a organizaciones para proteger secretos comerciales.

Según el Artículo 15, las autoridades públicas así como las empresas, las instituciones y las organizaciones están obligadas a ayudar al Servicio de Seguridad Federal para llevar a cabo sus obligaciones asignadas.

Los individuos y las entidades legales en Rusia que proporcionan servicios postales y telecomunicaciones de todas clases, incluidos sistemas, comunicación de datos y comunicaciones confidenciales vía satélite, están obligados a petición del Servicio de Seguridad Federal a incluir hardware, equipos y software adicionales, así como a crear otras condiciones necesarias para las medidas operacionales y técnicas del Servicio de Seguridad Federal.

Para cumplir con los retos de RF, las fuerzas de seguridad del Servicio de Seguridad Federal pueden asignarse a autoridades, empresas, instituciones y organizaciones públicas sin que importe quienes sean los propietarios, con el consentimiento de sus gerentes en la manera prescrita por el presidente de Rusia, dejando su servicio militar. En otras palabras, si el FSB le pide su ayuda, usted debe ayudar. Si le piden modificar hardware o software para que puedan ejecutar una operación o monitorear una red, usted lo debe hacer. Y si desean poner a alguien en su organización para apoyar objetivos del FSB, puede hacerlo con el permiso de su gerencia.

Las regulaciones de implementación incluyen disposiciones no mencionadas específicamente en la ley. Por ejemplo, se permite al FSB establecer bancos y efectuar cambios de divisas. El FSB lleva a cabo operaciones de investigación y desarrollo, y fabrica tecnología independientemente y con "otras empresas, instituciones y organizaciones", incluido el campo de seguridad de información. Significativamente, estas disposiciones valen para todas las actividades del FSB, no solo para la seguridad de información. Por ejemplo, el FSB podría indicar a una compañía, incluido un exportador de software, que modifica ese software para ayudar a la operación de recopilación técnica del FSB. El FSB podría formar una compañía encubierta y vender software adaptado directamente por internet aceptando pagos en divisas extranjeras. De hecho, el uso agresivo del FSB de las disposiciones indicadas en la ley y las regulaciones del FSB presentan una amenaza considerable solamente limitada por los objetivos y la imaginación del FSB.

Determinación de los cursos de acción del adversario

Gracias a innovaciones globales continuas en tecnología de información y comunicaciones, no hay forma de identificar todos los posibles vectores de ataque pero los cursos de acción conocidos incluyen entre otros ingeniería social, "spear phishing", "exploits" de software, puertas traseras de hardware, intercepciones de ICT y amenazas internas. Todas las organizaciones comerciales, gubernamentales y militares necesitan ser conscientes de cada uno de estos vectores de ataque y tener un plan organizado para contrarrestarlos. □

Notas

1. Hutchins, Eric M., Cloppert, Michael J., Amin, Rohan M., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" (Defensa de redes de computadoras impulsadas por inteligencia informada por análisis de campañas del adversario y cadenas de aniquilamiento de intrusión), minutas del 6º Congreso Internacional sobre Guerra de Información, Verano de 2011.
2. "Security Intelligence: Defining APT Campaigns" (Inteligencia de seguridad: definición de las campañas de APT) <http://computer-forensics.sans.org/blog/2010/06/21/security-intelligence-knowing-enemy/>.
3. "Getting Ahead of Advanced Threats: Achieving Intelligence-Driven Information Security" (Adelantarse a las amenazas avanzadas: logro de seguridad de información impulsada por la inteligencia) por RSA, basados en conversaciones con el Consejo de Seguridad para la Innovación de Empresas.
4. Lockheed Martin To Assist Department Of Defense In Fight Against Growing Threat: Cyber Crime" (Lockheed Martín ayudará al Departamento de Defensa en la lucha contra una amenaza creciente; los cibercrimes): PR Newswire, 3 de mayo 2012.
5. Publicación conjunta 2-01.3, Estado Mayor Conjunto, Departamento de Defensa de EE.UU. <http://www.fas.org/irp/doddir/dod/jp2-01-3.pdf>.
6. Eftimiades, Nicholas (2011-02-19). Chinese Intelligence Operations (Operaciones de inteligencia chinas) (Kindle Locations 169-173). Naval Institute Press. Kindle Edition.
7. US-CERT "Interesting Insider Threat Statistics" (Estadísticas interesantes de amenazas internas), 25 de octubre de 2010: http://www.cert.org/blogs/insider_threat/2010/10/interesting_insider_threat_statistics.html.
8. Se hace un estudio de 28 Estados en el Capítulo 16 de Inside Cyber Warfare (Ciberguerra interna), 2ª edición (O'Reilly, 2011), no obstante hay Estados adicionales que han añadido esas capacidades en 2012. Con el tiempo cada nación con unas Fuerzas Armadas tendrá también algo similar al Cibercomando de EE.UU.
9. "Inside Cyber Warfare: Mapping the Cyber Underworld" (Ciberguerra interna: mapeo del submundo cibernético), 2ª edición, capítulo 15 "The Russian Federation: Information Warfare Framework" (La Federación Rusa: estructura de la guerra de información), 12/2011.
10. USCC, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage" (Ocupación del terreno elevado de la información: capacidades chinas para las operaciones de la red de computadoras y ciberespionaje), 2012: <http://www.uscc.gov/>.
11. http://www.theregister.co.uk/2012/06/11/india_state_sponsored_attacks/.
12. <http://www.jpost.com/Defense/Article.aspx?id=253487>.



Jeffrey Carr es el fundador y CEO de Taia Global, Inc. y es el autor de "Inside Cyber Warfare: Mapping the Cyber Underworld" (Ciberguerra interna: mapeo del submundo cibernético) (O'Reilly Media 2009 y 2011 (2ª edición)). Su libro ha sido recomendado por el General Chilton, antiguo Comandante de USSTRATCOM y el prefacio de la Segunda edición fue escrito por el antiguo Secretario de Seguridad Nacional Michael Chertoff. Jeffrey ha tenido el privilegio de dirigirse al US Army War College, Instituto de Tecnología de la Fuerza del Aire, el Grupo de Estudios Estratégicos de Jefe de Operaciones Navales, la Agencia de Inteligencia de Defensa, el Centro de Códigos Abiertos de la CIA y en más de 60 congresos y seminarios.