CAPÍTULO 45

ARQUITECTURA DEL CICLO DE VIDA DE ACCIONES DE MONITORIZACIÓN EN REMOTO DE EQUIPOS INFORMÁTICOS

Pablo Luis Gómez Sierra
Universidad de Alcalá

1. Introducción

Los sistemas informáticos y de comunicación conviven en una misma sinergia al estar íntimamente conectados, debido en parte al impacto que tienen en la sociedad, permiten las acciones cotidianas y actividades que los seres humanos realizan en cualquier momento y lugar creando una dependencia directa de ese procesamiento de datos sin contar las posibles transferencias y almacenamiento consciente o no de la información.
En este contexto, y siguiendo en cuenta el párrafo anterior esa tecnodependencia humana genera multitud de amenazas a los sistemas y a la información que almacenan en ellos, evolucionando constantemente esa inseguridad tecnológica por medio de herramientas creadas para realizar acciones de cibercrimen, siendo cada vez más peligrosas por su gran impacto cuando son lanzadas contra sectores orientados a las infraestructuras críticas logrando en algunos casos crear caos.
Esas conductas de los cibercriminales en el ámbito digital se podrían dividir en cuatro grandes grupos de ciberdelitos. Como son: los cibereconómicos-patrimoniales, contra la intimidad y privacidad en el espacio red, el ciberespionaje y el ciberterrorismo. De todos los grupos de ciberdelitos mencionados, los ataques más graves que se pueden producir son los que van en contra de los intereses grupales o colectivos como son el ciberespionaje y ciberterrorismo.
En este mismo sentido el autor VELASCO (2010) en su obra Delitos cometidos a través de Internet comenta que estos ciberdelitos “afectan indiscriminadamente a intereses generales de la población, con la intención de crear pánico y terror, para subvertir el sistema político o de convivencia generalmente aceptado. Apenas tiene incidencia estadística, pero su realización, por afectar a la masa, genera mucha intranquilidad y desasosiego”.
Esta delincuencia de técnica avanzada se encuentra unida directamente con las nuevas tecnologías, usando el “Espacio Red” para crear estructuras de crimen organizado, ciberterrorismo o campañas de difusión de noticias falsas, persuasión o influencia manipulando los medios.
Estas operaciones artificiales de cibercrimen en algunas ocasiones se desarrollan con herramientas simples y sin embargo otras pueden ser orquestadas por procedimientos muy complejos y duraderos en el tiempo logrando poner en riesgo a la sociedad en su conjunto, estás técnicas tan complicadas pueden ser realizadas mediante las “amenazas persistentes avanzadas” (APT,s), estos ataques informáticos tienen diferentes tipologías que hacen que sus efectos puedan ser trasladadas desde el mundo digital al mundo físico.
Pero, ¿cómo se realiza el ciclo de vida en estas acciones “Ciber”?, a lo largo de este artículo se intentará dar respuesta a esta pregunta planteada.

2. Objetivos

La pretensión fundamental de este artículo es mostrar como con unas herramientas digitales y con una metodología de ciclo de vida se pueden obtener datos de dispositivos sin que su propietario tenga conocimiento de ello.
En primer lugar, darán las pautas generales sobre la arquitectura de un ataque de APT" mediante una descripción general.
Seguidamente y por último, se profundizará en la metodología de ciclo de vida de las acciones de monitorización en remoto de equipos informáticos.

3. Metodología

La metodología utilizada es la exposición de resultados a través de un estudio descriptivo de la evaluación de 19 artículos de diferentes soportes, realizados entre los años 2006 y 2022, relacionados todos ellos con las amenazas persistentes avanzadas y las arquitecturas de ciclo de vida de un ataque a dispositivos informáticos.

4. CICLO DE VIDA

El ciclo de vida de una amenaza persistente avanzada viene justamente después de desplegar los medios informáticos necesarios para llevar a cabo la acción, es decir, tras crear la infraestructura necesaria, tiene lugar el ataque propiamente dicho y es lo que se denomina ciclo de vida de la APT, teniendo las fases que se relatan a continuación:

- RECONOCIMIENTO DEL OBJETIVO A ATACAR: desde todos los puntos de vista posible. Se deben utilizar todas las herramientas disponibles para obtener toda la información sobre la víctima, para adecuar y personalizar el ataque. Un buen reconocimiento sobre el objetivo provocará un ataque eficaz y eficiente.
- PREPARACIÓN DEL ARCHIVO O MAIL CON UN ARCHIVO MALICIOSO PARA LA INFECCIÓN: esta fase consiste en tomar un objeto inocuo a simple vista, como puede ser una foto, mail, audio o un fichero ofimático, y armarlo con el malware que posteriormente será lanzado contra la víctima.
- ENTREGA DEL ARTEFACTO CON MALWARE A LA ORGANIZACIÓN QUE SE QUIERA COMPROMETER MEDIANTE CUALQUIER TÉCNICA DE INTRUSIÓN: dicha técnica vendrá determinada por la primera fase; tras un buen reconocimiento de la víctima se determinará cual es la mejor forma para introducirse en la organización, utilizando medios físicos como digitales.
- EXPLOTACIÓN DEL OBJETO CON MALWARE: cuando algún miembro de la organización visita una página web determinada o abre un archivo infectado, o cuando se han utilizado vulnerabilidades desconocidas para la seguridad de la organización.
- INSTALACIÓN DEL MALWARE EN EL DISPOSITIVO O DISPOSITIVOS ELECTRÓNICOS: completándose así la intrusión en la organización. Esta instalación puede ser en cuanto se produce la explotación, en la etapa anterior o posteriormente, pasado un tiempo, para no levantar sospechas en los sistemas de seguridad, haciendo más difícil su detección.
- ACCIONES SOBRE EL OBJETIVO: una vez se haya establecido la arquitectura en el seno de la organización a comprometer, se iniciarán las acciones, es decir, los movimientos tendentes a la consecución del objetivo. Dichas acciones podrán ser desde el robo de información hasta la utilización de la organización como plataforma para realizar ataques a mayor escala y a otras organizaciones superiores.

Este ciclo de vida de una APT, desde el diseño de la misma hasta que se consigue el objetivo por el que se creó, ya sea el robo de información o cualquier otro. Evidentemente no todas las APT,s son iguales debido a que ninguna organización es igual, ya que cada una de las APT creadas están diseñadas para un organización en particular, por lo que definir y establecer un procedimiento de actuación es altamente complicado, pudiendo aumentar o suprimir alguna de las fases.
De todas las fases del ciclo del ataque se puede simplificar aún más siendo necesario agruparse como mínimo en tres grandes acciones:

- RECONOCIMIENTO.
- INTRUSIÓN.
- EXPLOTACIÓN/PERSISTENCIA.

4.1. RECONOCIMIENTO

En la fase de reconocimiento, el atacante deberá recopilar toda la información disponible sobre el objetivo para diseñar y personalizar el ataque. Normalmente, en esta fase se puede trabajar con más tranquilidad que en el resto de las fases que se verán posteriormente debido a que en este momento será casi imposible ser detectado por los sistemas de seguridad porque no implica contacto con ningún sistema controlado por la organización. En esta fase se conseguirá toda la información que el atacante sea capaz de conseguir sobre la víctima a través de todos los medios que tenga a su disposición: arquitecturas tecnológicas, usuarios y contraseñas o, incluso, identificar el objetivo concreto y sensible dentro de la organización, la persona o dispositivo que contiene la información deseada, fin último del ataque. Aunque esta obtención de información se puede llevar a cabo mediante técnicas no intrusivas hacia la organización a comprometer, como es la utilización de fuentes abiertas, también existen técnicas más agresivas que requieren un contacto directo con los recursos humanos y técnicos de la organización. En este caso se deberá realizar una evaluación riesgo-resultado antes de utilizarlas y no sin antes haber extinguido todas las técnicas menos intrusivas.

4.2. INTRUSIÓN

La fase de intrusión es junto a la anterior fase de reconocimiento, las que menor probabilidad tienen de ser detectadas por los sistemas de seguridad de la organización debido a la nula o escasa y puntual interacción atacante-víctima. Después de la anterior fase, el atacante habrá reconocido cuales son los objetivos más fáciles para atacar para conseguir la información deseada y la mejor forma de establecer contacto con ellos, ya sea directamente por medio de la ingeniería social, o indirectamente, por medio de saltos a través de objetivos secundarios, más fácilmente atacables y con menos medidas de seguridad.
Una de las conclusiones a las que tendrá que haber llegado el atacante después de la fase de reconocimiento será la de haber definido al objetivo, en función a las medidas de seguridad con las que cuenta, entre duro, bien protegido, o blando, con unas medidas de seguridad inexistentes o débiles. El coste económico de la APT vendrá determinado por esta circunstancia, habrá que invertir mayores cantidades de dinero contra un objetivo duro para tener unas altas probabilidades de éxito que si por el contrario el atacante se enfrenta a un objetivo blando, que con un ataque básico y barato se podrá conseguir el objetivo. La victima también podrá ser definida como de interés cuando representa realmente un objetivo prioritario para el atacante, contra las victimas definidas como de oportunidad, las cuales no poseen información muy sensible pero el atacante decide en un momento dado el robo de ésta por medio de técnicas más sencillas, pero igualmente dañinas o intrusivas.
Existen multitud de técnicas y procedimientos para penetrar en la víctima que se quiera comprometer, desde las más básicas y baratas, hasta las más sofisticadas y caras. Las primeras, como pueden ser la explotación remota de vulnerabilidades a través de Internet o por medio de la propia red wifi corporativa, no serán comúnmente utilizadas por una APT seria

porque su detección y posterior análisis es muy fácil y probable por los responsables de seguridad de la organización a atacar. El método lógico de ataque que desarrollará una APT será la infección utilizando la red, por medio de la descarga de un archivo dañino o un enlace malicioso, o a través de infecciones por un medio físico como pueden ser pen drives contaminados o utilizando la puerta trasera de algún dispositivo.
De entre todas las técnicas de intrusión, la más utilizada por la mayoría de las APT conocidas hasta el momento es el "spear phishing" utilizando el correo electrónico. Esta técnica, barata, sencilla y sin necesitad de comprometer la identidad del atacante, permite establecer contacto directo con la principal víctima u objetivos secundarios. A simple vista es un correo electrónico con cuya misión es que la víctima lo abra, por lo que deberá contener al menos un asunto con un tema atractivo para la víctima y con un remitente conocido. Dicho correo contendrá un anexo con forma de imagen, documento ofimático o enlace que al ser abierto por la víctima, infectará su dispositivo de una forma sigilosa y eficaz, pasando a ser controlado y monitorizado por el atacante.

4.3. EXPLOTACIÓN/PERSISTENCIA

Después de que la APT se encuentra activa en el interior del objetivo, el objetivo será el de mantenerse activo en el seno de la organización durante el mayor tiempo posible. Es la fase más crítica de una APT ya que es cuando el sistema de seguridad tiene más probabilidades de detectar la amenaza, identificar el malware utilizado y analizarlo tranquilamente.
Cuando la amenaza esté en el interior del objetivo, se instalará en él y expandirá todas sus capacidades de ataque para obtener la información que satisfaga sus necesidades. Al inicio de la etapa de persistencia, se podrá completar el reconocimiento que se empezó anteriormente para determinar con absoluta certeza si la información con la que cuenta el objetivo es la que realmente se necesita; de no ser así abandonará rápidamente el objetivo, no dejando rastro, sin necesidad de gastar un exploit de día 0, por ejemplo, y ahorrando a la operación un recurso muy valioso.
Si al inicio de la etapa de persistencia, el atacante confirma la idoneidad de la víctima, la APT pondrá todas sus capacidades a trabajar para la consecución de dos objetivos principalmente a parte, como es obvio, de perdurar en el objetivo sin llamar la atención de la seguridad de la organización. Estos objetivos serán, conseguir la información deseada para posteriormente exfiltrarla y establecer una comunicación constante con los servidores externos de mando y control para conocer en todo momento el estado del malware que ha infectado el sistema. Para la consecución de estos dos objetivos, la APT realizará dos tipos de movimiento en el interior de la víctima, uno lateral encaminado a la obtención y tratamiento de la información obtenida, conteniendo actividades de fragmentación, compresión y encriptado de la información, y al sostenimiento de la persistencia, infectando un número determinado de dispositivos tal que la detección de uno no suponga peligro para el éxito de la operación; y el otro movimiento a realizar sería el externo, favoreciendo la comunicación con los servidores externos, ya sean para exfiltrar la información conseguida o para el mantenimiento de mando y control.

4.4. CONCLUSIONES

Estos ciberataques que pueden ser tan devastadores requiere el asegurar una adecuada defensa en el ciberespacio ante estas amenazas, aumentando las capacidades de defensa ante incidentes relacionados con las nuevas tecnologías, esa ciberseguridad se fundamenta en la protección del "Espacio Red" contra acciones que puedan poner en peligro las infraestructuras físicas, sus contenidos o servicios que proporcionan, impidiendo, detectando y mitigando cualquier acción ilegal organizada por grupos especializados en ejecutar delitos de alta tecnología, en este sentido la ciberseguridad tiene que ser un medio activo, en

constante evolución que pueda gestionar y analizar cualquier riesgo, la posición exclusiva de protección ha quedado obsoleta.
Los sistemas críticos son medios idóneos para ser atacados mediante APTs por organizaciones criminales, terroristas o de espionaje industrial que les permitan la ejecución de los objetivos que persiguen. Estos ataques son una realidad incluso en sistemas de redes independientes que no están conectadas a internet, debiendo ser una prioridad en las estrategias de seguridad de los sectores públicos y privados para crear protocolos de vigilancia, detección y mitigación de infecciones, incrementando medios y esfuerzos en la innovación, la investigación y el desarrollo de nuevas técnicas para alcanzar estos objetivos.

Se observa una continua evolución de las técnicas de infección y ataque a los sistemas, siendo así que cualquier estructura empresarial o gubernamental deberá orientar todo su esfuerzo en tener preparados equipos de respuesta ante situaciones de casos de detección de amenazas persistentes avanzadas, que permitan una neutralización, mitigación, interceptación e identificación de este tipo de ataques. Llegando a materializarse entre otras con medidas de monitorización persistente a través de programas de ciberseguridad automatizados que detecten comportamientos anómalos en las redes de comunicaciones propias, asumiendo que la red ha podido ser vulnerada en algún momento, intentando localizar vectores de exfiltración de información. Esta gestión de incidentes es necesario tener equipos de alta respuesta especializada para que una vez detectado cualquier comportamiento ilícito o anómalo se puedan hacer cargo de la situación comprobando si es una amenaza real o es un falso positivo. Si es una amenaza real tendrá que conocer dónde se dirige ese tráfico, que datos se envían o han sido enviados, a que máquinas de la organización están afectadas y en todo caso ver la posibilidad de aislar esas máquinas del resto del sistema, exponiendo todas estas informaciones en manos de los Cuerpos y Fuerzas de Seguridad del Estado o autoridades que las requieran.
El análisis de amenazas permanente es otra de las vías a desarrollar para proteger un sistema en el entorno de las nuevas tecnologías, la evolución de la tecnología y la constante conectividad de dispositivos hace más vulnerables los sistemas añadiendo nuevos vectores de ataque y riesgos, estos deben estudiarse y probarse ante la fortificación del sistema, ver su impacto y mitigación. Como norma general de protección no se implementarán nuevas tecnologías si no han sido auditadas y analizadas con los mayores estándares de seguridad.
La creación de planes de formación en ciberseguridad del personal que utilice cualquier medio tecnológico que pueda comprometer la seguridad de la organización, con programas de concienciación, prevención, gestión de incidentes y respuesta, basados en entrenamientos periódicos con actuaciones simuladas ante situaciones que puedan provocar una brecha de seguridad en la organización pública o privada.
Y por último, el fortalecimiento de las colaboraciones del sector público, privado y universitario, adaptar la legislación según las nuevas formas de criminalidad en el ciberespacio, la coordinación de todos los actores, el promover la cooperación internacional y suscribir acuerdos entre países son objetivos a desarrollar permanentemente, formando parte de la protección de la defensa nacional así como conseguir el logro de esta.

Bibliografía

ARQUILLA J. y RONDFELDT D. (2003). Redes y guerras en la red: El futuro del terrorismo, el crimen organizado y el activismo político. Madrid: Ed. Alianza Editorial.

CALTAGIRONE, S., PENDERGAST, A. y BETZ C. (Julio, 2013). Diamond Model of Intrusion Analysis. Center for Cyber Threat Intelligence and Threat Research. Hanover, MD, Technical Report ADA586960.

CAR, J. (2011). Inside Cyber Warfare: Mapping the Cyber Underworld. 2ª Ed.

CARO BEJARANO, M.J. (2011) Alcance y ámbito de la seguridad nacional en el ciberespacio. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. España: Ministerio de Defensa.

CROWLEY, D. (2010). Jack of all Formats. Trustwave SpiderLabs.

DE LEEUW, K. Y BERGSTRA, J. (2007). The history of Information Security. A Comprehensive Handbook. Elsevier.

DETECCIÓN de APTs, Centro de Seguridad TIC de la Comunidad Valenciana, acceso el 01 de junio de 2016, https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf

ELOY VELASCO, Delitos cometidos a través de internet cuestiones procesales (España: La Ley-Actualidad, 2010).

FERNANDEZ TERUELO J. G. (2007). Cibercrimen. Los delitos cometidos a través de Internet, Oviedo: Autor-editor.

FireEye (Octubre, 2014). APT28. A window into Russia´s Cyber Espionage operations? FireEye.

FLAME, EL CÓDIGO MALICIOSO MÁS COMPLEJO PARA CIBERESPIAR, Centro de Seguridad de las TIC de la Comunidad Valenciana, acceso el 03 de junio de 2016, https://www.csirtcv.gva.es/es/noticias/flame-el-código-malicioso-más-complejo-para-ciberespiar.html

GALÁN MUÑOZ A. (2006). Ataques contra sistemas informáticos, Boletín Información Ministerio de Justicia.

GARTNER SAYS BY 2020, MORE THAN HALF OF MAJOR NEW BUSINESS PROCESSES AND SYSTEMS WILL INCORPORATE SOME ELEMENT OF THE INTERNET OF THINGS, Empresa de tecnología Gartner, acceso el 03 de julio de 2016, http://www.gartner.com/newsroom/id/3185623

GONZÁLEZ RUS J.J. (2006). Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes, en El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales. Granada.

HEICKERÖ, R. (Marzo, 2010). Emerging Cyber Threats ans Russians View son Information Warfare and Information Operations. FOI. Swedish Defense Research Agency.

Observatorio INTECO (2016). ¿Qué son las amenazas persistentes avanzadas?, acceso 15 julio de 2016, http://www.egov.ufsc.br/portal/sites/default/files/cdn_apts.pdf

MARÍA JOSÉ CANO Alcance y ámbito de la seguridad nacional en el ciberespacio, Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio (España: Ministerio de Defensa, 2011).

MONTALVO LÓPEZ. M. Amenazas Persistentes Avanzadas. CCACES. Aranjuez. (2017)

W32.STUXNET DOSSIERR, EMPRESA DE SEGURIDAD SYMANTEC, acceso el 15 de mayo de 2016, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf