ATAQUES HÍBRIDOS A INFRAESTRUCTURAS CRÍTICAS

El ciberespacio es el último campo de batalla para explotar las vulnerabilidades conocidas y, sobre todo, desconocidas de un supuesto enemigo o rival. Las ciberarmas son programas informáticos maliciosos diseñados para atacar a un sistema ciberfísico esencial, con el objetivo de alterar su funcionamiento normal o destruirlo. Estos tipos de ataques contra una infraestructura crítica no requieren inversiones multimillonarias como la fabricación de armas de guerra convencionales, y su capacidad de réplica es muy efectiva. Pero, ¿cómo se producen? ¿Quién los genera y cómo se distribuyen? ¿A quién sirven? Y, ¿cómo podemos defendernos?

Manel Medina Llinàs
Director del Máster en Cybersecurity Management, UPC-School; coordinador de la Oficina Técnica de Formación de la Agència de Ciberseguretat de Catalunya

CIDOB REPORT
08- 2022

A los tradicionales campos de batalla –tierra, mar y aire–, hace unos años se añadió el espacio orbital, y hace poco que se habla ya del ciberespacio. En los escenarios tradicionales, las armas pueden verse desde aviones o satélites, y los estados y las grandes coaliciones como la OTAN tienen bien controladas las del otro bando. Pero las ciberarmas son casi intangibles y pueden cruzar una frontera, no ya en un microchip de memoria, sino a través de las redes de datos. Esto hace que sea difícil saber qué capacidad destructiva tiene nuestro contrincante en caso de ciberguerra.

Pero empecemos por saber qué es una *ciberarma*. Hasta hace menos de una década, se consideraba ciberarma cualquier programa informático malicioso, capaz de atacar a nuestro enemigo en cualquier momento. Para no ser descubierta e inutilizada antes del ataque, normalmente, la ofensiva se basaba en uno o varios métodos de explotación de una vulnerabilidad de algún pro-

grama instalado en los sistemas informáticos de la víctima, lo que se conoce como *vulnerabilidad de día cero* (*zero-day*). Los más puristas dicen que para ser considerada ciberarma, esta debe ser «destructiva», es decir, causar daños materiales a infraestructuras críticas y/o personas. Por tanto, estas ciberarmas las tenemos que buscar, escondidas en los llamados *sistemas ciberfísicos* o *Internet de las cosas* (IoT), como sistemas de control industrial (ICS), ferroviarios, telecomunicaciones, suministros esenciales (agua, luz, gas), o sanitarios, entre otros. Esta particularidad, y el hecho de que muchos de estos sistemas no estén adecuadamente actualizados, hace que incluso puedan ser atacados con vulnerabilidades conocidas.

Una amenaza asequible y persistente

Muchas ciberarmas pretenden permanecer ocultas, imperceptibles, esperando la orden de destruir el objetivo. Se trata de la llamada «amenaza persistente avanzada» (APT, por sus siglas en inglés). En muchos casos, además, es difícil identificar al equipo desarrollador; pero, entre los más potentes, figuran divisiones o compañías del ejército o unidades de ciberinteligencia de gobiernos. Aunque, como ocurre con las armas físicas, también hay fabricantes de ciberarmas y organizaciones criminales que las venden en mercados más o menos ocultos. Recientemente ha irrumpido en el debate público y mediático la empresa israelí NSO, que vende sus ciberarmas a estados, como el *software* espía Pegasus, teóricamente diseñado para apoyar la lucha antiterrorista. Las ciberarmas no debemos buscarlas solo en la ciberguerra, sino también en herramientas de vigilancia, identificación biométrica, etc., con impacto en la cadena de suministro y, potencialmente, recopilando datos de usuarios y ciudadanos.

Las ciberamenazas son más «asequibles», no requieren inversiones multimillonarias como la fabricación de artefactos o armas de guerra. Descubrir nuevas vulnerabilidades y desarrollar nuevas herramientas de explotación de estas es mucho más barato y, sobre todo, es replicable centenares o millares de veces sin apenas coste adicional. Por lo tanto, las pueden desarrollar organizaciones «grises», que las comercializan tanto a gobiernos, de forma abierta, como a grupos criminales, de forma oculta.

Pero el catálogo de las ciberarmas incluye, además, un instrumento, en apariencia, menos belicoso: la desinformación, que puede ser empleada también para atacar a infraestructuras críticas. Llegando a través de los canales de información convencionales (redes sociales, medios de comunicación, etc.), la desinformación se dirige, de manera selectiva, a las personas que tienen capacidad de gestión de la infraestructura, y puede ser complementada con el ciber(contra)espionaje. Los *softwares* espía empleados por los

departamentos de inteligencia también pueden ser atacados, y generar informaciones falsas al enemigo que nos espía, incitándole a tomar decisiones que le pueden llevar a una trampa de difícil salida, bloqueando la infraestructura o perdiendo su control. Sin embargo, la desinformación más habitual en entornos ciberfísicos, como forma de ataque, consiste en alterar los datos que proporcionan los sensores de sistemas físicos. La intención es provocar decisiones de reacción equivocadas por los propios sistemas de gestión de la infraestructura, intentando, por ejemplo, corregir un problema inexistente, con lo que se estará creando otro en sentido contrario, que no será detectado. Esto sucedió en el ataque Stuxnet, en el que un virus (ciberarma) destruyó las centrifugadoras de uranio iraníes, modificando los datos de las revoluciones por minuto registrados por unos que mostrasen normalidad, para evitar ser detectado. Esta modificación de los datos de los sensores se puede realizar de diversas formas: a) reemplazando un sensor por otro engañoso, o introduciendo uno fraudulento, b) modificando su *software* para que proporcione lecturas falsas, o c) modificando los datos en el servicio de almacenamiento de estos (en un servidor o en la nube). Si la transmisión, el almacenamiento o el procesado de los datos no están adecuadamente protegidos, es muy fácil alterarlos sin ser advertidos, hasta que el daño sea irreparable o inevitable.

LAS CIBERARMAS PUEDEN ESTAR ESCONDIDAS EN CUALQUIER SITIO: UN CHIP, UN PROGRAMA, UNA TARJETA DE MEMORIA, O ALMACENADAS EN LA NUBE. UNA CIBERARMA ESTÁ FORMADA POR BITS, QUE SE PUEDEN OCULTAR DE CUALQUIER MANERA Y SON INDETECTABLES; PUEDEN ESTAR LATENTES DURANTE AÑOS EN UNA CENTRAL DE PRODUCCIÓN DE ENERGÍA O EN UN CENTRO DE CONTROL DE TRÁFICO FERROVIARIO O AÉREO, O EN EL DESPACHO DE UN GOBERNANTE O DIRECTIVO, SIN QUE NADIE SE DÉ CUENTA.

Las ciberarmas pueden estar escondidas en cualquier sitio: un chip, un programa, una tarjeta de memoria, o almacenadas en la nube. Una ciberarma está formada por bits, que se pueden ocultar de cualquier manera y, por lo tanto, son indetectables; pueden estar latentes durante años en una central de producción de energía o en un centro de control de tráfico ferroviario o aéreo, o en el despacho de un gobernante o directivo, sin que nadie se dé cuenta, como de hecho ya denunció el informe Mandiant en 2014. Esta investigación desveló decenas de organizaciones que habían sido infiltradas por el equipo de desarrollo de programas informáticos de ciberespionaje chino APT1 y en las que estas ciberarmas se habían mantenido ocultas una media de 229 días, llegando en algunos casos a estar instaladas varios años.

En una ciberguerra, se invaden los ordenadores o dispositivos de control de las infraestructuras de un país, pero ello no se sabrá hasta que alguien «pulse un botón» y despierte a los agentes (programas maliciosos) dormidos en sus madrigueras, y estos empiecen a actuar, deteniendo las infraestructuras que permitan el funcionamiento del país.

La guerra híbrida es una guerra con una capa adicional de operaciones remotas. A diferencia de las guerras convencionales, en las que el ejército invasor puede verse en las calles, los preparativos de un ciberataque son imperceptibles, porque no hay movimientos de tropas en la frontera. En el ciberespacio no hay fronteras.

El peligro de la proliferación de ciberarmas

Una vez vistos el escenario y las armas, vamos a ver los peligros a los que nos enfrentan estas nuevas amenazas cibernéticas y los factores que las hacen atractivas y peligrosas.

La ciberguerra «está servida»: las ciberarmas están siendo desplegadas por Internet frente a nuestros ojos, aunque estos no puedan verlas. Armas más potentes que un lanzamisiles o un tanque se comercializan inadvertidamente para la mayoría de los ciudadanos y también de los países, porque son tan solo «bits de datos». Como con las armas tradicionales, existen compras «legales», realizadas por gobiernos, y otras «ilegales», llevadas a cabo por particulares o grupos criminales con interés en espiar a un enemigo comercial o estratégico, para suplantarle y tomar el control de la infraestructura, o destruirla, como hizo BlackEnergy, que desconectó y destruyó los programas de control de las plantas de producción de energía eléctrica ucranianas el 23 de diciembre de 2015.

Las ciberarmas pueden ser producidas por cibermafias, por unidades cibernéticas de ejércitos convencionales, o por empresas al servicio de gobiernos. Lo que preocupa a los gobernantes es que diseñar y construir una ciberarma está al alcance de cualquier pequeño país u organización, ya que su producción no requiere materias primas, disponibles en los mercados, pero que son más caras. La guerra híbrida es preferible a la tradicional porque es más rentable. Rusia y otros países europeos distribuyen este tipo de ciberarmas, muchas veces producidas en proyectos de colaboración público-privada. Los gobiernos y las grandes organizaciones multinacionales generan las herramientas, y la cadena de suministro no ha sido analizada todavía.

Cuando se produzca un ciberataque híbrido, no sabremos quién lo ha ordenado, quién lo ha perpetrado o cuándo empezó su preparación. En al-

gunos casos, su autoría puede ser muy evidente; por ejemplo, a raíz de la presentación en la Berlinale de 2016 del documental Zero Days, sobre el ataque Stuxnet, se denunció la coordinación entre Estados Unidos e Israel –aunque ellos no lo han reconocido– del ciberataque (mencionado anteriormente) para destruir las centrifugadoras de enriquecimiento de uranio iraníes. En otros casos, la determinación de la autoría es más difícil. Recientemente, la guerra de Ucrania también se está librando en el ciberespacio, y Moscú y Kíev se han acusado mutuamente de ataques de falsa bandera. Por ejemplo, en los ataques a servicios web gubernamentales ucranianos en enero de 2022, los atacantes dejaron pistas falsas incriminando a disidentes ucranianos y polacos, para desviar la atención de Rusia como atacante. Por ello, establecer el origen del ataque es esencial.

Para identificar el autor de un ciberataque, hay que analizar el código de la ciberarma en busca de comentarios o nombres que puedan indicar el país o el idioma empleado por el desarrollador. Pero este puede conocer dicha técnica y dejar pistas falsas en el idioma del contrincante al que pretende suplantar con un ataque de falsa bandera. Para complicarlo aún más, aunque el desarrollador no haya intentado ocultar su identidad o ideología, el atacante real puede ser diferente de quien ha desarrollado la herramienta de explotación, si esta se distribuye en el mercado soterrado. Otra técnica de detección es mirar la procedencia del ataque, aunque los indicios tampoco son concluyentes, ya que se pueden usar servidores intermedios que oculten el origen de la agresión como los de la red Tor[1]. Todo lo comentado hasta ahora abre multitud de posibilidades de injerencia a varios niveles, y requiere el despliegue de estrategias de defensa basadas en «desconfiar de todo».

LAS CIBERARMAS PUEDEN SER PRODUCIDAS POR CIBERMAFIAS, POR UNIDADES CIBERNÉTICAS DE EJÉRCITOS CONVENCIONALES, O POR EMPRESAS AL SERVICIO DE GOBIERNOS.

Estrategias de defensa frente a ataques híbridos

Podemos distinguir dos grandes tipos de ataques híbridos: a) los que afectan a la (des)información, con el objetivo de provocar decisiones incorrectas, y b) los que afectan directamente a sistemas físicos.

1. La red Tor está formada por multitud de servidores en todo el mundo, que se pueden ir encadenando para evitar que se pueda detectar el origen real de una conexión.

Si empezamos a analizar las actividades de desinformación como las noticias falsas que circulan por la red e influyen en las percepciones y opiniones públicas, podemos concluir que su efectividad en la desestabilización social puede ser más eficaz incluso que los ataques a bases de datos de control de una infraestructura. La desinformación puede producir violencia, y es otra forma de iniciar conflictos o ataques a infraestructuras.

Las estrategias de ataques de desinformación se basan en la creación y posterior distribución de noticias a través de redes de usuarios influyentes o falsos (bot social), para aumentar su difusión entre burbujas de usuarios afines. La defensa frente a este tipo de ataques es la identificación y el bloqueo de los agentes distribuidores de noticias falsas, pero los administradores de las redes sociales no siempre están dispuestos a colaborar, dados los beneficios de publicidad que pueden proporcionar las campañas de difusión de este tipo de noticias. Por otro lado, los ataques híbridos más directos a infraestructuras críticas provenientes del ciberespacio plantean el problema de la falta de experiencia de los responsables de seguridad física, la falta de colaboración de los empleados, y la incredulidad de los directivos para concebir, planificar e implantar las medidas de ciberprotección adecuadas.

Los países de la OTAN, a pesar de haber declarado su predisposición a reaccionar a ciberataques en julio de 2021, no están tomando en consideración las actividades de Rusia respecto a ataques híbridos. Por ejemplo, la interrupción del servicio del gaseoducto más importante de Estados Unidos –Colonial Pipeline– o los ataques a través de suministradores de infraestructuras con el procedimiento SolarWinds, en 2020, o ataques de Ransomware generalizados a otros países de la OTAN, han sido orquestados por Rusia, directamente o a través de cibermercenarios, pero la Alianza Atlántica sigue sin reaccionar. Tal vez una de las razones sea la nueva Directiva NIS2 de la Unión Europea, donde se describe cómo enfrentarse a los ciberataques, aunque esta directiva diferencia claramente entre servicios críticos y esenciales[2], y se incide en que solo estos últimos se consideran objeto de defensa.

2. Los servicios críticos son aquellos que permiten un funcionamiento normal de la sociedad, pero cuya falta no paraliza totalmente sus actividades. Por ejemplo, el transporte público se podría sustituir por un sistema de vehículos compartidos, como sucedió en algunos países durante el confinamiento más duro de la pandemia, para trasladar a personal sanitario. Los servicios esenciales son aquellos sin los cuales la sociedad no funciona, como la electricidad o las telecomunicaciones.

En definitiva, los gobiernos están tomando medidas administrativas y legales para incentivar la ciberprotección, especialmente en sus infraestructuras esenciales y críticas, y no solo en estas, sino también en las de sus proveedores, y en toda su cadena de suministro de componentes fundamentales para el servicio. Los gestores de estas infraestructuras deberán identificar los servicios y activos más valiosos y los más vulnerables, para protegerlos de la forma más eficiente posible. Y, finalmente, también se tendrá que planificar el mantenimiento operativo de los mecanismos de protección instalados y formar adecuadamente a todo el personal implicado. De ello dependerá el funcionamiento de un país. Si la reconstrucción después de un ciberataque generalizado (ciberguerra) puede ser relativamente rápida, un ataque híbrido puede ser más complicado de recuperar, sobre todo si el daño causado a la infraestructura es irreparable y se debe reconstruir con componentes caros o difíciles de encontrar en el mercado.

Referencia

McWhorter, Dan. «APT1: Exposing One of China's Cyber Espionage Units». *The Mandiant Intelligence Center* (2021) (en línea) https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units