Impacto De APTs Sobre El Mundo Moderno

Giovanni Dueck
giodueck@gmail.com

Universidad Católica Nuestra Señora de Asunción

Octubre, 2023

Resumen

Las amenazas cibernéticas que enfrenta el mundo de la informática hoy en día tienen una trayectoria de unos 30 años. Las amenazas relacionadas a gobiernos más antiguas datan a los años 90, y sus acciones influenciaron profundamente la forma en que funcionan las redes y computadoras hoy en día.

Esta investigación busca recopilar algunos de los grupos y eventos más significativos en el mundo de las Amenazas Persistentes Avanzadas, abreviadas *APT*, y cuales fueron los efectos que tuvieron sobre la tecnología moderna, el espionaje y el dominio de la guerra cibernética.

1. Definiciones

1.1. APT

Una Amenaza Persistente Avanzada, o APT (*Advanced Persistent Threat* en inglés) es un actor sigiloso, típicamente un grupo perteneciente a o apoyado por un gobierno, que gana acceso no autorizado a una red de computadoras y permanece sin detectarse por un tiempo extendido. No se limitan a grupos apoyados por estados. [27]

Una entidad se clasifica como APT si es:

- **Avanzada (Advanced)**: Los operadores detras del grupo poseen un espectro completo de herramientas de recolección de inteligencia. Incluyen herramientas propias y open-source, pero pueden también incluir a la organización de inteligencia del estado.
- **Persistente (Persistent)**: Los operadores poseen objetivos a largo plazo, y no buscan información oportunísticamente por motivos de ganancia financiera u otros. Este tipo de objetivo sugiere que el atacante es guiado por una entidad externa. Los objetivos del atacante necesitan de un acceso permanente al objetivo, y al ser expulsados típicamente reintentan ganar acceso, y lo logran.

- **Amenaza (Threat)**: Los atacantes son una amenaza porque tienen tanto capacidad como intención. Son manejados por acciones humanas y no simplemente por código automatizado. Son operadores capacitados, organizados y bien financiados. [16]

1.2. Arma Cibernética

Comúnmente se refiere a malware empleado por parte de agencias militares, paramilitares o de inteligencia en un ataque cibernético. Esto incluye, entre otros, virus, trotanos, spyware y gusanos.

A diferencia de malware desarrollado para el crimen cibernético, como adware o ransomware, las armas cibernéticas típicamente son creadas por un APT o actor apoyado por un gobierno y pueden ser altamente selectivas en su objetivo. [47]

1.3. Ciberdelito

Delito cibernético, o ciberdelito, es todo crimen o delito que involucra una computadora o redes de computadoras. Existen varias clases de crimen cibernético, desde fraude y lavado de dinero hasta crímenes financieros, estafas, extorsión, tráfico de drogas y materiales de abuso sexual de niños.

En la mayoría de los casos, el delito se comete con el fin de lucrar. Por lo tanto, en muchos casos, operaciones ejecutadas por APTs son especiales en el mundo del ciberdelito y son más similares al espionaje.

Se hará esta distinción en el resto del documento: una acción es claramente un ciberdelito si busca lucrar o ataca a la sociedad civil sin objetivos militares, de lo contrario típicamente se puede hablar de una guerra o arma cibernética. Aun así, veremos más adelante que esta distinción no siempre se puede hacer claramente. [7]

1.4. Malware

Malware ("malicious software", o software malicioso) es cualquier software diseñado para causar disrupción en una computadora, servidor, cliente o red, filtrar información privada, ganar acceso no autorizado, privar de acceso a información, o de otra forma irrumpe en la seguridad o privacidad informática de un usuario. [49]

1.5. Zero-day

Un Zero-day (también escrito "0day") es una vulnerabilidad en un sistema informático desconocida por el proveedor y el público general. El nombre se refiere al tiempo que un proveedor conoce la vulnerabilidad.

Zero-days pueden ser explotados mientras no son conocidos por cualquier grupo para cualquier objetivo, incluyendo la infiltración de malware, spyware, o acceso indebido a información. Son mitigados mediante un parche por parte del

proveedor, y una vez descubiertos empieza una carrera por el proveedor para lanzarlo. [48]

2. Algunos APTs conocidos

2.1. China

2.1.1. APT1: Comment Crew

APT1 es un grupo vinculado al Ejército Popular de Liberación (PLA por sus siglas en inglés) de China. Es uno de los principales y más conocidos APTs chinos, y ha realizado campañas de ciberespionaje, robo de secretos y robo de propiedad intelectual principalmente en los Estados Unidos.

El nombre coloquial de *Comment Crew* se debe a la tendencia a vulnerar sistemas de comentarios en sitios web legítimos. [26]

2.1.2. APT10: Red Apollo

APT10 se vincula comúnmente al Ministerio de Seguridad del Estado de China, y es más conocido por la operación Cloud Hopper, una campaña extensa de ataque y robo de información en múltiples países de todos los continentes que tenía como objetivo a proveedores de servicios gerenciados (Managed Service Providers, MSP). [34]

2.1.3. APT41: Double Dragon

APT41 es único entre los APTs chinos en que su operación es dual, operan tanto en campañas apoyadas por el gobierno como en campañas de cibercrimen, es decir para lucro del grupo, de donde provee el nombre *Double Dragon*.

Fueron nombrados por el Departamento de Justicia de los EE.UU. por haber comprometido a más de 100 empresas. [5]

2.2. Corea del Norte

2.2.1. APT38: Lazarus Group

Lazarus Group es un grupo norcoreano designado tanto como APT como grupo criminal. Algunos investigadores reportan todos los casos de ataques provinientes de Corea del Norte bajo el nombre Lazarus Group, sin importar si provienen de algún subgrupo, como APT37 o Kimsuky. [21]

Sus ataques más infames incluyen el ataque destructivo a Sony, robo al Banco de Bangladesh y el ransomware WannaCry. Sus operaciones incluyen activismo digital, espionaje y exfiltración de información, y crímenes financieros. [46]

2.3. Estados Unidos

2.3.1. Equation Group

Equation Group es el grupo APT de la Agencia Nacional de Seguridad (NSA por sus siglas en inglés). Es actualmente considerado el APT más sofisticado, con operaciones que se adentran en el ciberespionaje, vigilancia masiva, y sabotaje por medio de armas cibernéticas capaces de causar daño en equipamiento industrial. [13]

La NSA fue objetivo de mucha crítica el ser descubierto su rol en la creación de Stuxnet, considerada por muchos la primera arma cibernética, por ende iniciando la era de las guerras cibernéticas, y por las tácticas y herramientas que tienen a su disposición, que fueron descubiertas por varios leaks. [29]

2.4. Iran

2.4.1. APT33: Elfin Team

APT33 es un grupo formado a más tardar en 2013, demostrando una gran capacidad de crecimiento en el área de seguridad por parte del gobierno iraní. Los objetivos de este grupo son principalmente los EE.UU. y Arabia Saudita, con el ataque más conocido deshabilitando las operaciones de la mayor empresa de petroquímicos de la zona, Saudi Aramco. [33]

2.5. Israel

2.5.1. Unit 8200

Unit 8200 es una unidad de los Cuerpos de Inteligencia de Israel cuya misión es la captación y descifrado de códigos. Frecuentemente son asociados con Stuxnet, ciberarma en cuya creación Israel colaboró con la NSA de los EE.UU. [29]

La unidad se compone principalmente de jóvenes de entre 18 y 21 años de edad, debido a, servicio militar obligatorio de no más de dos años. Esto significa que los reclutas elegidos deben tener la capacidad de aprender rápidamente y ser de utilidad a la unidad en el tiempo restante. Muchos ex miembros van al mundo empresario, con varios de estos fundando grandes empresas como Wix y NSO Group, y muchos otros trabajando en las mayores empresas tecnológicas del mundo. [53] [1]

2.6. Rusia

2.6.1. APT28: Fancy Bear y APT29: Cozy Bear

APT28 y APT29 son dos grupos primariamente de ciberespionaje. Sus operaciones más conocidas son las interferencias en las elecciones de los EE.UU. en 2016, aunque también atacaron a varios países europeos y a la Agencia Mundial del Antidopaje. [32]

2.6.2. Sandworm

Este grupo realizó varias operaciones contra el ejército y el pueblo de Ucrania, con ataques a la red eléctrica y un wiper que arrazó con una gran mayoría de los sistemas informáticos del país, considerado el ataque cibernético más destructivo de la historia. También emplearon un malware destructivo para atacar a los juegos olímpicos de invierno de 2018, haciendo todo lo posible para evitar ser descubiertos. [18] [19]

3. Eventos y operaciones

3.1. Moonlight Maze (1996)

En 1996, uno de los primeros ataques cibernéticos masivos había comenzado. Un grupo de hackers exfiltró una cantidad monumental de documentos, que si fuesen impresos y apilados superarían los 160 metros de altura. [35]

Un equipo de investigación fue formado en 1999, y la investigación recibió el nombre de "Moonlight Maze". Se recolectó mucha evidencia, pero la mayoría fue clasificada o dejada fuera de las manos del público, pero una investigación reciente por parte de un equipo en Kaspersky reveló tácticas y herramientas que muestran conexiones con un grupo moderno: Turla.

Turla es un APT ruso cuya operación de ciberespionaje en 2014 fue descubierta por Kaspersky e investigada extensamente. Los ataques se aprovecharon de dos zero-days, además de varias vulnerabilidades ya resueltas, y el malware infectó a computadoras en más de 45 países mediante tácticas de ingeniería social y spear-phishing. [15]

Vincular a un grupo sofisticado como Turla con un ataque tan histórico como lo es Moonlight Maze, revela que el grupo es realmente uno de los más antiguos y experimentados APTs existentes. El único grupo de edad similar es Equation Group, el APT vinculado con la NSA. Este último ya estuvo activo en 2001, y tal vez hasta en 1996. [13]

Ataques de esta magnitud muestran que los APTs bien financiados y capaces no son un fenómeno nuevo, existen desde los comienzos del internet. Moonlight Maze estableció el estándar del arsenal de herramientas del atacante moderno.

3.2. Titan Rain (2000s)

En 2005 se revelaron una serie de ataques a varias instituciones de los gobiernos de los Estados Unidos y del Reino Unido, los cuales se sospechan que empezaron en 2003. El Reino Unido reportó que la campaña continuaba activa hasta 2007. [12]

Shawn Carpenter, un analista de seguridad informática en Sandia National Laboratories, laboratorio en el cual parte del arsenal nuclear americano es diseñado, descubre en 2003 una intrusión. En Lockheed Martin, una empresa de aeronáutica americana, el mismo actor logra infiltrarse y acceder a documentos sensibles relacionados a varios proyectos militares de la empresa.

Carpenter inicia una campaña propia para rastrear a los intrusos en su tiempo libre, actuando de informante para el gobierno. Increíblemente, Carpenter logra ubicar a los intrusores en la China. Según él, este grupo "nunca presionó una tecla equivocada."Sin duda, se trataba de un actor militar.[52] [4]

Como la operación de Carpenter no tenía una autorización, la FBI compartió los datos de su intervención en la investigación con Sandia, de la cual fue despedido. En respuesta, Carpenter lanza una demanda y gana US$ 4,3 millones, con el juez recalcando que este fue un acto patriótico por el cual no debió haber sido castigado.

El incidente recalcó la importancia de una actitud de la no ignorancia con respecto a la seguridad informática, y solidificó la noción de que el espionaje moderno cambió del dominio físico al digital. [54]

3.3. Operation Aurora (2010)

En enero de 2010, Google anunció que habían descubierto una intrusión en diciembre de 2009. Proviniendo de China, los ataques afectaron a 34 empresas de diversos sectores, desde internet a finanzas a fabricantes de químicos.

Los datos robados fueron principalmente propiedad intelectual, llevando a la especulación que el gobierno chino buscaba robar productos y tecnología americanos. Pero su objetivo en Google era principalmente el acceso a varias cuentas de Gmail pertenecientes a activistas de derechos humanos chinos. Además, Google descubrió que varias cuentas de activistas de alrededor del mundo sufrieron accesos no autorizados rutinarios en sus cuentas de Gmail. [8]

De acuerdo a McAfee, los atacantes tuvieron acceso al código fuente de varias empresas tecnológicas y del sector de defensa. En el centro del escándalo estaban los sistemas de gestión de configuración de software (SCM por sus siglas en inglés), que no tenían defensas. Esto significa que las vulnerabilidades en los productos de estas empresas pueden ser encontradas más facilmente al tener acceso al código fuente. [55]

3.4. Stuxnet (2010)

Stuxnet es el malware más sofisticado jamás encontrado. Según varios reportes, es la obra de las agencias de inteligencia de los Estados Unidos e Israel, y es generalmente considerada la primera arma cibernética y el incidente que inició la era de la guerra cibernética.

Inicialmente, expertos encontraron versiones que datan a junio de 2009, y más tarde se encontrarían versiones en uso desde 2007. Sin embargo, es la versión final descubierta en 2010 que hacía uso de varios *exploits* [1] críticos de Microsoft Windows y poseía capacidades impensables para la época. Con un total de cuatro zero-days, Stuxnet es de complejidad incomparable. Donde un malware común normalmente emplea tácticas de ingeniería social y no más de un zero-day, aquí se emplean cuatro en un solo ataque. [9] [10]

[1] Del inglés. Un *exploit* es un fragmento de software utilizado en la explotación de una vulnerabilidad de software

3.4.1. Historia

La misión de Stuxnet era una de sabotaje como alternativa a un conflicto tradicional. Los EE.UU. habían descubierto que Irán, por medio de un físico llamado A.Q. Khan en Pakistan, lanzó un programa de enriquecimiento nuclear entre 1998 y 1999 y comenzó a comprar diseños para una fábrica de centrífugas. La CIA y la inteligencia británica habían infiltrado la cadena de suministro de A.Q. Khan y lograron interceptar un envío de centrifugas a Libia. En 2004, la Agencia Internacional de Energía Atómica de las Naciones Unidas investigó al programa libio y la CIA adquirió los materiales del programa.

Las centrífugas se estudiaron extensivamente, lo que permitió crear un virus sigiloso que es capaz destruir equipamiento industrial físico, por primera vez en la historia. Con estos hallazgos, las administraciones del presidente Bush y más tarde la del presidente Obama aprobaron el programa, que fue nombrado Operación *Olympic Games* (Juegos Olímpicos).

La versión inicial, sin embargo, tenía una falta: no lograba alcanzar a todas las computadoras necesarias, las que controlaban al sistema de control industrial. Por este motivo se agregaron exploits agresivos que permitieron al virus (1) esparcirse por la red local de una máquina infectada, (2) obtener privilegios elevados y (3) esconder la presencia y acciones del sistema operativo. Esta clase de malware es llamada un *worm* (gusano), un programa que es capaz de replicarse de forma autónoma para moverse a huéspedes nuevos, y las herramientas que permiten esconderse del sistema operativo y obtener privilegios elevados son llamadas *rootkit*.

El ataque inició con una infiltración física del malware a la planta nuclear Natanz, que se encuentra en una zona remota y desconectada de internet. Una vez que Stuxnet logra infectar a la primera máquina, infecta rápidamente a toda computadora con Windows en la red en busca de instalaciones de software Siemens para el control de las centrífugas. Una vez encontradas estas computadoras críticas, monitorea el comportamiento normal de los sistemas de control antes de interferir en su operación. Un diagrama delinieando este proceso se muestra en la figura 1.

Stuxnet era capaz de alterar las frecuencias a las que operaban las centrífugas; al mismo tiempo reportaba frecuencias normales al sistema de monitoreo. De esta forma, las centrífugas se desgastan y hasta autodestruyen mucho más rápidamente. Se estiman que alrededor de 1.000 centrífugas fueron dañadas durante la operación, y el gas de uranio que contenían, desperdiciado. [56] [29]

El virus finalmente fue descubierto por analistas de VirusBlokAda, un proveedor de antivirus, al escapar de la planta por medio de una computadora transportada fuera del predio. Un reporte por Symantec luego afirmó que computadoras alrededor del mundo habian sido infectadas, con la gran mayoría de ellas en Irán. Se reportaron también que varios de los exploits utilizados ya se habían encontrado anteriormente por otras operaciones del APT Equation Group, por lo cual el ataque les fue atribuído. [25]

Stuxnet inició debates sobre la guerra en el plano de la información. Fue la primera vez que un virus mostró la capacidad de subvertir sistemas de control

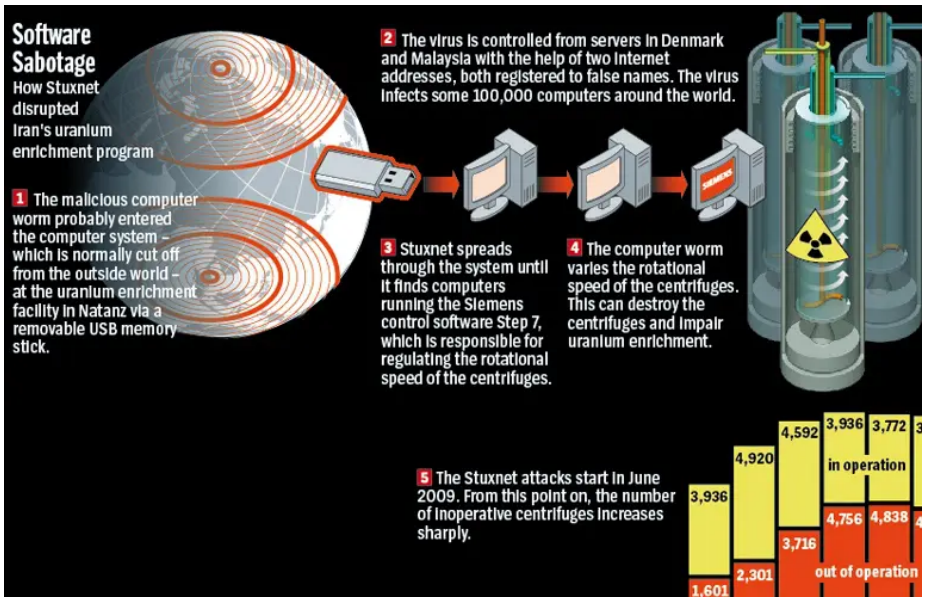

Figura 1: funcionamiento de Stuxnet [20]

industrial de manera tan sofisticada. Hasta este punto, la guerra cibernética no se había definido. El hecho de ser un ataque cibernético otorga cierta negación plausible (que no es posible con un ataque con misiles o bombas), y tampoco es claro si un ataque cibernético constituye un acto de guerra. [41] [36]

3.5. Sony (2014)

En respuesta a la producción de la película satírica *The Interview*, Sony Pictures fue hackeada en 2014 por operativos de Corea del Norte. El ataque consistió en el robo de información, entre otros sobre obras en producción y datos de empleados, y la implantación de un virus *wiper* [2].

Mientras que este ataque fue el que puso a Corea del Norte en el mapa, el grupo autodenominado *Guardians of Peace* (Guardianes de la Paz) mostró signos de actividad desde al menos 2009 y parece ser responsable de más de 45 familias de malware. El ataque a Sony demostró una capacidad que no pudo haber aparecido en solo un año.

Hoy en día el grupo es mejor conocido como Lazarus Group. Hasta este momento no parecía ser un grupo muy sofisticado, con métodos crudos y operaciones de magnitud limitada, pero no lo necesitaba ser. Con las herramientas que poseían, ya demostraban ser un grupo peligroso y capaz de alcanzar sus objetivos. [58]

[2]Del inglés. *Wipers* son una clase de malware cuyo objetivo es la destrucción de datos y/o sistemas informáticos

El mismo grupo continuó su trayectoria de ciberespionaje y extorsióna a través de las numerosas campañas que le siguen a esta primera.

3.6. Banco de Bangladesh (2016)

En 2016, Lazarus Group se infiltró en el Banco de Bangladesh y realizó transferencias SWIFT de casi US$ 1.000 millones a varias cuentas bancarias pertenecientes al grupo en diversos bancos, algunos de ellos en las Filipinas. Sin embargo, un error de tipografía en las intrucciones de transferencia detectado por un empleado bancario realzó sospechas, por lo que la mayoría de las transferencias fueron bloqueadas. El monto robado terminó siendo de alrededor de US$ 81 millones.

El 4 de febrero, los hackers lograron enviar más de tres docenas de transferencias fraudulentas usando credenciales del sistema SWIFT del Banco de Bangladesh. US$ 81 millones fueron enviados exitosamente a varias cuentas bancarias en las Filipinas, mientras que la mayor parte, unos US$ 850 millones, fue bloqueada al encontrar un error en la instrucción de transferencia.

El Banco de Bangladesh pudo descubrir el robo gracias a un error de una impresora, la cual estaba configurada para imprimir un registro constante de cada transferencia SWIFT realizada pero había fallado durante el ataque. Al finalmente reiniciar la impresora, se dieron cuenta de las transferencias realizadas. El Banco de la Reserva Federal de Nueva York había intentado contactar con el Banco de Bangladesh, pero nadie respondió gracias al fin de semana en el país. Cuando intentan contactar a SWIFT y a Nueva York para responder a los mensajes, nadie respondió gracias al fin de semana en los EE.UU. Cuando al fin logran establecer las comunicaciones el lunes siguiente, descubren que varias de las transferencias han sido aprobadas: un total de US$ 101 millones. Intentos de contactar con el banco RCBC de las Filipinas también se atrasaron por un día feriado, el año nuevo chino. [57] [44]

US$ 20 millones fueron recuperados más tarde, pero Lazarus continuó sus planes con los demás US$ 81 millones. Por medio de unos apostadores chinos, el dinero se lava y desaparece. [24]

Lazarus Group ahora ya no es solo un grupo de espionaje, sabotaje y extorsión, sino también un grupo criminal. Con la cantidad limitada de comercio exterior del país marginado, y con la serie de otros ataques similares menores, el dinero robado por parte del programa de hackers norcoreano debe componer una buena parte del producto interno bruto anual. Esto hace a Corea del Norte el único APT que realiza operaciones netamente cibercriminales y el único estado con el robo como significante contribuyente a la economía.

3.7. The Shadow Brokers (2016)

En agosto de 2016, un grupo nuevo anunció que había hackeado a la NSA. Específicamente, afirmaban haber hackeado a Equation Group y robado nume-

rosas ciberarmas. Este grupo se llamaba *The Shadow Brokers* [3].

Shadow Brokers realizaron muchas afirmaciones exageradas, incluso que las herramientas robadas eran mejores que Stuxnet, pero resultó ser cierto que estas herramientas debían proveer de Equation Group, específicamente la unidad entonces llamada TAO. [4] [3]

Inicialmente solo disponibilizaron unas pocas muestras, con la intención de subastar el resto al mejor postor, o al público general si el total de las ofertas llegase a BTC 1.000.000 (alrededor de US$ 600 millones en ese tiempo). Pero como no lograron recaudar un monto significante, el grupo decidió publicar las herramientas descubiertas al público general.

Hacer de acceso público armas cibernéticas sofisticadas, algunas incluso datando a los años 90 y las más recientes a 2013, significó un riesgo importante al mundo entero. Ahora no solo APTs podían acceder a armas cibernéticas sofisticadas, sino grupos de criminales comunes.

Además, Shadow Brokers demostraron también que posían información operacional. Jake Williams, fundador de Rendition Security, publicó bastante sobre el grupo. En respuesta, un mensaje dirigido a Williams lo expuso como ex miembro de Equation Group, lo cual era información clasificada, y este lo confirma. [45] [37]

La NSA tiene una mala racha de ser expuesta por sus operaciones. Primero, Stuxnet escapa de su objetivo para luego infectar al mundo y exponer las capacidades de creación de ciberarmas de Equation Group. Luego, en 2013 Edward Snowden, ex contratista de la NSA, filtra miles de documentos revelando las capacidades de ciberespionaje y programas vigilancia masiva de la agencia. Ahora, hackers logran acceder a y distribuir herramientas altamente peligrosas, las cuales la NSA ha estado acumulando desde los años 90 sin contactar a los proveedores de los productos afectados.

Esta última tendencia, la de acumular exploits para su uso en ciberarmas, se vio especialmente criticada en los años posteriores a este incidente por autores y periodistas. [43]. El exploit más significante del conjunto, nombrado EternalBlue, causó graves daños al ser usado por Lazarus Group de Corea del Norte y Sandworm de Rusia en ataques masivos que lograron llevar a algunas de las empresas y agencias de gobierno más grandes del mundo a la era del lapiz y papel. Curiosamente, un parche para la vulnerabilidad fue lanzada poco tiempo antes de que el exploit sea revelado al público, llevando a especular que la NSA advirtió a Microsoft una vez que se enteraron de la brecha.

3.8. WannaCry (2017)

En mayo de 2017, el ciberataque más devastador hasta entonces empezó. Un ransomware llamado WannaCry, usando el exploit EternalBlue, se estaba

[3] en inglés, *shadow* significa sombra, y *broker* significa corredor o agente de bolsa y se refiere a un negociante.

[4] en inglés, *Tailored Access Operations*, operaciones de acceso a medida, es una unidad especializada en el desarrollo de tanto hardware como software de espionaje e infiltración cibernética. El nombre actual de la unidad es *Computer Network Operations*.

Figura 2: pantalla de una computadora infectada con el ransomware WannaCry

propagando por las computadoras de organizaciones e individuos, encriptando archivos, y demandando un pago por la recuperación de la información.

EternalBlue, una de las ciberarmas de la NSA robadas por los Shadow Brokers, se aprovecha de una vulnerabilidad de ejecución remota de código en el protocolo de transferencia de archivos SMB en Windows. MS17-010, como la llamó Microsoft, es una vulnerabilidad tan severa que hasta productos viejos sin garantía de soporte recibieron un parche para mitigarla, y WannaCry demostró por primera vez esta severidad a gran escala. [2]

Dentro de pocos minutos, el virus es capaz de infectar una organización entera. Entre las afectadas está la NHS, el servicio nacional de la salud del Reino Unido. Este se vió obligado a desconectar a varios hospitales del internet, varios otros tuvieron que suspender sus actividades o continuarlas en papel y pizarras.

El virus consiste de dos módulos: un gusano, que mediante EternalBlue se propaga a nuevas máquinas, descarga y ejecuta las herramientas para ejecutar el ataque sobre los archivos, y las herramientas de encripción, que causan un daño crítico a los archivos de una computadora. Finalmente, una pantalla de ransomware informa a la víctima de su destino y propone las instrucciones para la decodificación de sus archivos: un pago de US$ 300 a US$ 600 en Bitcoin.

Sin embargo, el virus posee un punto débil. Un *killswitch*, un interruptor de apagado, que consiste en una prueba de conexión a una URL de nombre aparentemente aleatorio. Cuando un analista independiente registra el nombre de dominio unas horas luego del inicio del ataque, encuentra que al lograr conectarse, el virus desactiva la herramienta de encripción y detiene el ataque. Múltiples

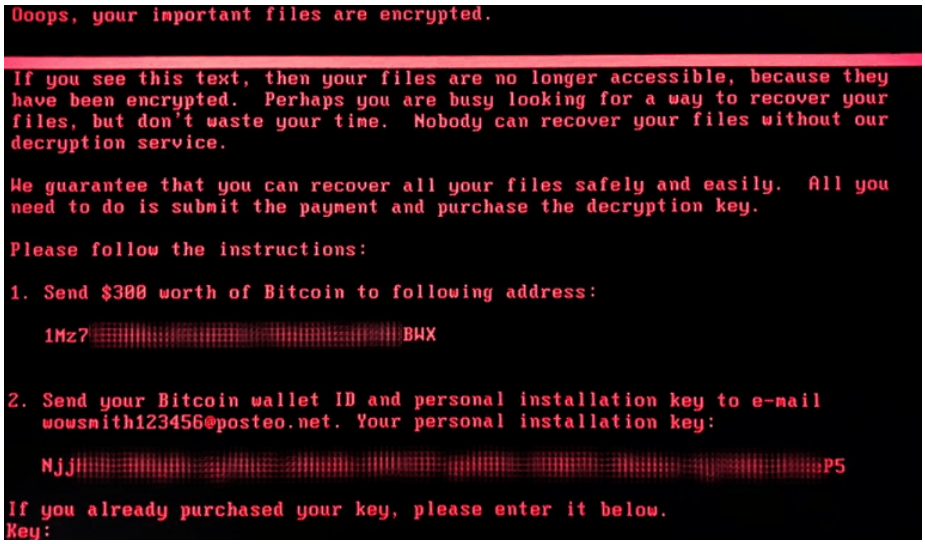

Figura 3: pantalla de una computadora infectada con el wiper NotPetya

versiones aparecieron luego de activarse el killswitch, tanto con un URL diferente como sin killswitch, pero ya no llegaron a causar el mismo impacto que la primera oleada. [39]

El Departamento de Justicia de los Estados Unidos comunicó a la prensa en 2018 una acusación a un programador de Corea del Norte por su participación en Lazarus Group y los ataques a Sony, robo al Banco de Bangladesh y ataque WannaCry. [22]

3.9. NotPetya (2017)

Antes de la invasión a gran escala, Rusia invadió a Ucrania en 2014 y anexó al territorio de Crimea. Desde entonces, ha ocupado el territorio de Donbas y está causando sufrimiento para el país ex soviético, que en el pasado se había llamado el granero de la Unión Soviética.

Entre 2014 y 2022 ha regido un caos en el plano cibernético, el cual expertos clasifican como la primera guerra cibernética real. El grupo Sandworm, un APT operado por la unidad militar 74455 de la GRU, el servicio de inteligencia militar de Rusia, llevó a cabo varios ataques cibernéticos sobre la infraestructura militar y civil de Ucrania. Entre los primeros, están varios ataques destructivos a la red eléctrica del país en 2015 y 2016. [23]

En 2017, Sandworm lanza el virus más tarde denominado "NotPetya"[5] por medio de una actualización maliciosa al programa M.E.Doc, un servicio al cual

[5] un ransomware llamado Petya fue usado como la base de este ataque, pero las modificaciones eran sustanciales tanto en su rutina de encripción como en su forma de propagación. Por esta razón, Kaspersky lo llamó ExPetr, o NotPetya. [40]

se habían infiltrado unos meses antes. M.E.Doc es un software para el manejo de impuestos en Ucrania, por lo que una infección a este programa resultaría en una infección a la nación entera. Para infectar a las demás computadoras, se empleó una versión modificada de EternalBlue, el mismo exploit usado en WannaCry, y el exploit EternalRomance, también del paquete filtrado por Shadow Brokers.

En realidad, NotPetya no era realmente un ransomware, ya que los autores no proveían los datos necesarios para generar una clave de decodificación. Esto significa que en realidad era un *wiper*, con el objetivo de destruir datos y sistemas informáticos a escala masiva, tanto en empresas como instituciones públicas.

Residentes de Ucrania perdieron acceso al pago electrónico del transporte público y la mayoría de los ATMs, supermercados perdieron la habilidad de vender sus productos ya que las cajas se encontraban mostrando una pantalla como en la figura 3. Todo servicio ucraniano conectado directa o indirectamente a internet se vió afectado.

Pero un worm no conoce límites geográficos. Aunque la mayor parte de las infecciones se dieron en Ucrania, Rusia también se vió muy afectada ya que tenía muchas conexiones con Ucrania. Empresas multinacionales con sedes en Ucrania también fueron atacadas. [14]

Uno de los casos más destructivos es el de Maersk, la empresa de transporte marítimo. Esta perdió la gran mayoría de sus sistemas informáticos, lo que causó filas de decenas de miles de camiones con pedidos que no podían completar, en algunos casos de productos perecederos. Barcos llenos de contenedores llegaban a puertos, pero nadie sabía qué carga tenían los contenedores. El incidente casi destruyó a la empresa, y causó la reconstrucción total de su infraestructura de TIC. [38]

Andy Greenberg, un experto en el grupo Sandworm, llamó al ataque de NotPetya el más destructivo de la historia. Ataques de esta escala brindan un ejemplo de lo que es la guerra cibernética, y de lo que son capaces los grupos APT cuando tienen acceso a armas cibernéticas de grado militar como lo fue EternalBlue. [18] [17]

3.10. SolarWinds (2020)

En diciembre de 2020, Fireeye descubrió una intrusión en sus sistemas que compartió con el mundo. El ministerio de defensa estadounidense inició una investigación relacionada a una brecha similar en sus sistemas, asi también empresas como Microsoft y Mandiant. [59] [50]

La investigación rápidamente concluyó que el actor mostraba señales de ser un grupo ruso, cuyo objetivo era principalmente el ciberespionaje antes que la destrucción. En 2022, Mandiant reveló al actor, llamado *Dark Halo* y *UNC2452*, como APT29, también conocido como Cozy Bear.

Entre marzo y mayo, los atacantes logran infiltrarse en los sistemas de la empresa SolarWinds, la cual provee Orion, un producto de monitoreo de redes. Este producto es usado en muchas empresas importantes de diversos sectores, como Fireeye y Microsoft, y en muchas organizaciones gubernamentales.

El ataque consiste de un troyano de acceso remoto, o RAT. Una actualización se publica con código malicioso, llamado SUNBURST, que permite a los atacantes acceder a cualquier sistema de forma sigilosa. Para evitar que se descubra la manipulación del código, los atacantes incluyeron fragmentos de software en el proceso de construcción de Orion. Esto permitió inyectar el código malicioso sin modificar el código legible por humanos, antes de generar la firma digital que previene la modificación posterior de la herramienta y que asegura que el producto no fue manipulado.

Un ataque de este tipo se denomina un ataque de cadena de suministro, y con los miles de clientes se lograría atacar a muchos objetivos de forma sencilla. Protegerse de este tipo de actores implica, por lo tanto, no solo verificar los sistemas y productos propios de una organización, sino también la verificación de toda herramienta proveída por terceros. Se estima que unos 18.000 clientes fueron infectados, de los cuales alrededor de mil fueron atacados.

Entre las víctimas más importantes se encuentra Fireeye, una empresa de ciberseguridad, que estimó que muchas herramientas de testeo de penetración, es decir herramientas de hackeo, fueron robadas.

Con ocho meses entre la infección inicial y la detección, el ataque reveló el aumento drástico en las capacidades de APT29. Revela también un nuevo nivel de sofisticación en la seguridad operacional (OPSEC) de grupos adversarios, un alto grado de persistencia y un abordaje cada vez más agresivo a la recolección de información. El presidente de Fireeye afirmó que el ataque a SolarWinds fue uno de los más sofisticados visto en la historia de la empresa. [28] [11]

El presidente de los EE.UU. Joe Biden respondió con medidas y sanciones agresivas de una manera no vista frecuentemente. El ataque fue comparado con Moonlight Maze por varios analistas de seguridad y como una declaración implícita de guerra por otros, reforzando la retórica de disuación por medio de medidas contra actores cibernéticos hostiles. Este tipo de ataques surgen como la mejor, y tal vez la única, alternativa a un ataque convencional, ya que los EE.UU. poseen las fuerzas militares más poderosas del mundo. [6]

3.11. Axie Infinity (2022)

En marzo del 2022, el creador del juego basado en criptomonedas y NFT *Axie Infinity* anunció que había descubierto una brecha. Esta resultó en el robo de unos US$ 620 millones, el robo de criptomonedas más grande de la historia. En abril, autoridades estadounidenses anunciaron que vincularon una de las direcciones de billetera a Lazarus Group. [42]

La fundación del juego es la blockchain llamada Ronin Network, creada con juegos en mente. A diferencia de una cadena como la de Bitcoin, Ronin se diseñó con la intención de soportar una gran cantidad de transacciones por segundo. Para alcanzar este objetivo, un método de validación de bloques de prueba de trabajo (comúnmente llamada minería) sería poco ideal por la gran cantidad de trabajo desperdiciado para las frecuentes transacciones que implica el diseño de un videojuego. En su lugar, Ronin utilizaba un sistema llamado Prueba de

Autoridad, en donde nodos llamados *validadores* votan para aprobar bloques nuevos de transacciones. [31]

Los hackers que penetraron a Sky Mavis, la empresa desarrolladora del juego, notaron que cuatro del total de nueve claves validadoras se encontraban en manos de la empresa. Como cuatro de nueve no superan la mitad de los validadores, era necesaria una clave más para forjar transacciones ilícitas; es para estos casos que existen multiples nodos validadores.

En 2021, Sky Mavis fue otorgada acceso al validador de la organización descentralizada autónoma (DAO por sus siglas en inglés, *Decentralized Autonomous Organization*) de Axie Infinity para ayudar al DAO a distribuir transacciones libres de tarifas por una inmensa carga de usuarios. Como el permiso de operar esta clave no fue denegado al volver a la normalidad, los hackers lograron acceder a la clave, en efecto otorgándose la autoridad de votar por transacciones ilegales de retiros de fondos. [30]

Una diferencia clave entre las finanzas tradicionales y las descentralizadas es que las transacciones en blockchain son irreversibles. En el robo al Banco de Bangladesh, la gran mayoría de las transacciones ilegales del sistema SWIFT fueron bloqueadas. Esto es imposible con blockchain por diseño; la cadena no puede ser modificada y no miente. Transacciones aprobadas en cryptomonedas no son reversibles, lo que hace a este mundo un objetivo interesante tanto para estafas como robos. [51]

Investigadores notaron que Lazarus robó alrededor de US$ 400 millones en 2021, haciendo a este incidente particularmente lucrativo para el gobierno de Corea del Norte. El grupo ha mostrado la capacidad de penetrar cualquier industria, ya sea de entretenimiento en el caso de Sony, bancos centrales como el de Bangladesh, o monedas descentralizadas como en el caso de Ronin Network. El ataque evidenció que ninguna empresa y ningún sistema es inmune a las amenazas cibernéticas. [42]

4. Conclusión

This is what cyberwar looks like: an invisible force capable of striking out from an unknown origin to sabotage, on a massive scale, the technologies that underpin civilization. - Andy Greenberg

Referencias

[1] Richard Behar. «Inside Israel's Secret Startup Machine». En: *Forbes* (11 de mayo de 2016). URL: https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine.

[2] Alex Berry, Josh Homan y Randi Eitzman. *WannaCry Malware Profile*. Inf. téc. 23 de mayo de 2017. URL: https://www.mandiant.com/resources/blog/wannacry-malware-profile.

[3] Bill Brenner. «Shadow Brokers return with a password and message for Trump». En: *Sophos News* (10 de abr. de 2017). URL: https://news.sophos.com/en-us/2017/04/10/shadow-brokers-return-with-a-password-and-message-for-trump/.

[4] Bill Brenner. «The lesson of Titan Rain: Articulate the dangers of cyber attack to upper management». En: *Homeland Security News Wire* (14 de dic. de 2005). URL: https://www.homelandsecuritynewswire.com/lesson-titan-rain-articulate-dangers-cyber-attack-upper-management.

[5] Catalin Cimpanu. «US charges five hackers from Chinese state-sponsored group APT41». En: *ZDNET* (16 de sep. de 2020). URL: https://www.zdnet.com/article/us-charges-five-hackers-part-of-chinese-state-sponsored-group-apt41/.

[6] CNBC. *The SolarWinds Hack And The Future Of Cyber Espionage*. Youtube. 22 de ene. de 2021. URL: https://www.youtube.com/watch?v=jxTxGlE9X5s.

[7] Michael Aaron Dennis. *cybercrime*. Disponible en https://www.britannica.com/topic/cybercrime. 20 de sep. de 2023.

[8] David Drummond. *A new approach to China*. Disponible en https://googleblog.blogspot.com/2010/01/new-approach-to-china.html. 12 de ene. de 2010.

[9] Nicolas Falliere, Liam O Murchu y Eric Chien. *W32.Stuxnet Dossier*. Inf. téc. Cupertino CA, Estados Unidos, feb. de 2011. URL: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[10] Jim Finkle. «Researchers say Stuxnet was deployed against Iran in 2007». En: *Reuters* (26 de feb. de 2013). URL: https://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226.

[11] FireEye. «Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor». En: *Mandiant* (13 de dic. de 2020). URL: https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.

[12] Council on Foreign Relations. *Titan Rain*. Disponible en https://www.cfr.org/cyber-operations/titan-rain.

[13] Kaspersky Lab Global Research & Analysis Team. «Equation: The Death Star of Malware Galaxy». En: *SECURE LIST* (16 de feb. de 2015). URL: https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/.

[14] Kaspersky Lab Global Research & Analysis Team. «Schroedinger's Pet(ya)». En: *SECURE LIST* (27 de jun. de 2017). URL: https://securelist.com/schroedingers-petya/78870/.

[15] Kaspersky Lab Global Research & Analysis Team. «The Epic Turla Operation». En: *SECURE LIST* (7 de ago. de 2014). URL: https://securelist.com/the-epic-turla-operation/65545/.

[16] IT Governance. *Advanced Persistent Threats (APTs)*. Disponible en https://www.itgovernance.co.uk/advanced-persistent-threats-apt.

[17] Andy Greenberg. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. 1.ª ed. New York City NY, Estados Unidos: Doubleday, 2019.

[18] Andy Greenberg. «The Untold Story of NotPetya, the Most Devastating Cyberattack in History». En: *WIRED* (22 de ago. de 2018). URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[19] Andy Greenberg. «The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History». En: *WIRED* (17 de oct. de 2019). URL: https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

[20] Joel Hruska. «Windows PCs vulnerable to Stuxnet attack – five years after patch». En: *ExtremeTech* (11 de mar. de 2015). URL: https://www.extremetech.com/defense/200898-windows-pcs-vulnerable-to-stuxnet-attack-five-years-after-patches.

[21] Kyaw Pyiyt Htet. *Lazarus Group*. Disponible en https://attack.mitre.org/groups/G0032/.

[22] Departamento de Justicia. *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. Comunicado de Prensa N° 18-1452. Disponible en https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and. Estados Unidos, 6 de sep. de 2018.

[23] Departamento de Justicia. *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*. Comunicado de Prensa N° 20-1,117. Disponible en https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and. Estados Unidos, 19 de oct. de 2020.

[24] Alan Katz y Wenxin Fan. «A Baccarat Binge Helped Launder the World's Biggest Cyberheist». En: *Bloomberg* (3 de ago. de 2017). URL: https://www.bloomberg.com/news/features/2017-08-03/a-baccarat-binge-helped-launder-the-world-s-biggest-cyberheist.

[25] Gregg Keizer. «Is Stuxnet the 'best' malware ever?» En: *InfoWorld* (16 de sep. de 2010). URL: https://www.infoworld.com/article/2626009/is-stuxnet-the--best--malware-ever-.html.

[26] Dave Lee. «The Comment Group: The hackers hunting for clues about you». En: *BBC News* (12 de feb. de 2013). URL: https://www.bbc.com/news/business-21371608.

[27] Sarah Maloney. *What is an Advanced Persistent Threat (APT)?* Disponible en https://www.cybereason.com/blog/advanced-persistent-threat-apt.

[28] Kevin Mandia. «Global Intrusion Campaign Leverages Software Supply Chain Compromise». En: *FireEye Stories* (13 de dic. de 2020). URL: https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html.

[29] Ellen Nakashima y Joby Warrick. «Stuxnet was work of U.S. and Israeli experts, officials say». En: *The Washington Post* (2 de jun. de 2012). URL: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[30] Ronin Network. «Back to Building: Ronin Security Breach Postmortem». En: *Ronin's Newsletter* (27 de abr. de 2022). URL: https://blog.roninchain.com/p/back-to-building-ronin-security-breach.

[31] Ronin Network. *Introduction to Ronin*. Disponible en https://docs.roninchain.com/docs/basics/introduction. 26 de jul. de 2023.

[32] Patrick Nohe. «Fancy Bear and Cozy Bear, APT28 & APT29, Already Targeting 2018 US Election». En: *hashed out* (21 de sep. de 2018). URL: https://www.thesslstore.com/blog/apt28-apt29/.

[33] Jacqueline O'Leary et al. *Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware*. Disponible en https://www.mandiant.com/resources/blog/apt33-insights-into-iranian-cyber-espionage. 20 de sep. de 2017.

[34] «Operation Cloud Hopper: What You Need to Know». En: *Trend Micro* (10 de abr. de 2017). URL: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know.

[35] Costin Raiu et al. «Penquin's Moonlit Maze». En: *SECURE LIST* (3 de abr. de 2017). URL: https://securelist.com/penquins-moonlit-maze/77883/.

[36] Jack Rhysider. *EP 29: Stuxnet*. Darknet Diaries, 2 de ene. de 2019. URL: https://darknetdiaries.com/transcript/29/.

[37] Jack Rhysider. *EP 53: Shadow Brokers*. Darknet Diaries, 10 de dic. de 2019. URL: https://darknetdiaries.com/transcript/53/.

[38] Jack Rhysider. *EP 54: NotPetya*. Darknet Diaries, 24 de dic. de 2019. URL: https://darknetdiaries.com/transcript/54/.

[39] Jack Rhysider. *EP 73: WannaCry*. Darknet Diaries, 1 de sep. de 2020. URL: https://darknetdiaries.com/transcript/73/.

[40] Marvin the Robot. «New Petya / NotPetya / ExPetr ransomware outbreak». En: *Kaspersky Daily* (27 de jun. de 2017). URL: https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/.

[41] David Sanger. «Obama Order Sped Up Wave of Cyberattacks Against Iran». En: *The Washington Post* (1 de jun. de 2012). URL: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[42] Aaron Schaffer. «North Korean hackers linked to $620 million Axie Infinity crypto heist». En: *The Washington Post* (14 de abr. de 2022). URL: https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea/.

[43] Bruce Schneier. «The NSA Is Hoarding Vulnerabilities». En: *Schneier on Security* (26 de ago. de 2016). URL: https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html.

[44] Jamie Schram. «Congresswoman wants probe of 'brazen' $81M theft from New York Fed». En: *New York Post* (22 de mar. de 2016). URL: https://nypost.com/2016/03/22/congresswoman-wants-probe-of-brazen-81m-theft-from-new-york-fed/.

[45] Scott Shane, Nicole Perlroth y David E. Sanger. «Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core». En: *The New York Times* (12 de nov. de 2017). URL: https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

[46] Olivia Solon. «WannaCry ransomware has links to North Korea, cybersecurity experts say». En: *The Guardian* (15 de mayo de 2017). URL: https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group.

[47] Tim Stevens. «Cyberweapons: an emerging global governance architecture». En: *Palgrave Commun* 3.16102 (2017). URL: https://www.nature.com/articles/palcomms2016102.

[48] Symantec. *What is a Zero-Day Vulnerability?* Archivado en https://web.archive.org/web/20170704035927/http://www.pctools.com/security-news/zero-day-vulnerability/. 4 de jul. de 2017.

[49] Rabia Tahir. «A Study on Malware and Malware Detection Techniques». En: *I.J. Education and Management Engineering* 8.2 (2018), págs. 20-30. URL: https://web.archive.org/web/20230110063748/https://www.mecs-press.net/ijeme/ijeme-v8-n2/IJEME-V8-N2-3.pdf.

[50] Dina Temple-Raston. «A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack». En: *NPR* (16 de abr. de 2021). URL: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

[51] James Tetazoo. *Documented Timeline of DeFi Exploits*. Disponible en https://chainsec.io/defi-hacks/. 2005.

[52] Nathan Thornburgh. «The Invasion of the Chinese Cyberspies». En: *TIME* (29 de ago. de 2005). URL: https://content.time.com/time/subscriber/article/0,33009,1098961,00.html.

[53] Tali Tsipori. «8200 graduates aren't like 23 year-olds in Texas or Norway». En: *Globes* (5 de jun. de 2017). URL: https://en.globes.co.il/en/article-8200-graduates-are-not-like-23-year-olds-in-texas-or-norway-1001191294.

[54] Jaikumar Vijayan. «Reverse hacker wins $4.3M in suit against Sandia Labs». En: *COMPUTERWORLD* (14 de feb. de 2007). URL: https://www.computerworld.com/article/2543470/reverse-hacker-wins--4-3m-in-suit-against-sandia-labs.html.

[55] Kim Zetter. «'Google' Hackers Had Ability to Alter Source Code». En: *WIRED* (3 de mar. de 2010). URL: https://www.wired.com/2010/03/source-code-hacks/.

[56] Kim Zetter. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. 1.ª ed. New York City NY, Estados Unidos: Crown, 2014.

[57] Kim Zetter. «That Insane, $81M Bangladesh Bank Heist? Here's What We Know». En: *WIRED* (17 de mayo de 2016). URL: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.

[58] Kim Zetter. «The Sony Hackers Were Causing Mayhem Years Before They Hit the Company». En: *WIRED* (24 de feb. de 2016). URL: https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/.

[59] Kim Zetter. «The Untold Story of the Boldest Supply-Chain Hack Ever». En: *WIRED* (2 de mayo de 2023). URL: https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/.