Impacto De APTs Sobre El Mundo Moderno

Giovanni Dueck

Octubre, 2023

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 estado, 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. [17]

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. [11]

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. [26]

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. [4]

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. [28]

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. [27]

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. [16]

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). [21]

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. [3]

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. [14]

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. [25]

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. [9]

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. [18]

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. [20]

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. [18]

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. [30] [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. [19]

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. [12] [13]

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. [22]

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. [10]

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. [9]

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. [8]

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.[29] [2]

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. [31]

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. [5]

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. [32]

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, más tarde se encontrarían versiones en uso desde 2007. Sin embargo, la versión descubierta en 2010 hacía uso de varios *exploits* (FOOTNOTE del inglés, fragmento de software utilizado en la explotación de una vulnerabilidad de software) críticos de Microsoft Windows y poseía capacidades impensables para la época. Con un total de cuatro zero-days, Stuxnet tiene una 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. [6] [7]

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.

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.

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. [33] [18]

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. [15]

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 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. [24] [23]

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] 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.

[3] 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/.

[4] Michael Aaron Dennis. *cybercrime*. Disponible en https://www.britannica.com/topic/cybercrime (2023-09-20).

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

[6] 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.

[7] 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.

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

[9] 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/.

[10] 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/.

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

[12] 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/.

[13] 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/.

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

[15] 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.

[16] 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.

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

[18] 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.

[19] 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/.

[20] 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 (2017-09-20).

[21] «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.

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

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

[24] 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.

[25] 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.

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

[27] Symantec. *What is a Zero-Day Vulnerability?* Archivado en https://web.archive.org/web/20170704035927/http://www.pctools.com/security-news/zero-day-vulnerability/ (2017-07-04).

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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/.

[33] 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.