Impacto De Grupos APT Sobre El Mundo Moderno

Giovanni Dueck

Octubre, 2023

Resumen

Abstract

1. Definiciones

1.1. APT

Una Amenaza Persistente Avanzada, o APT (Advanced Persistent Threat, por sus siglas 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.

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. No se limitan a grupos apoyados por estados.

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 son altamente selectivas en su objetivo.

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.

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.

1.4.1. Ransomware

Malware que bloquea el acceso a información o sistemas informáticos y amenaza con publicar o destruir dicha información a menos que se pague un rescate. Ransomware simple puede simplemente bloquear el acceso al sistema operativo sin dañar archivos, pero malware más avanzados usan técnicas de encripción, que efectivamente destruyen la información, y exigen un pago a cambio de la llave.

1.4.2. Rootkit

Una colección de software diseñado para dar acceso a una computadora de forma no permitida normalmente. Root se refiere al superusuario *root* en sistemas Unix-like, y *kit* al conjunto de herramientas.

Típicamente pueden ocultar su presencia sin dejar de permanecer activos, e incluso pueden proveer una forma de instalar otros tipos de malware sin ser detectados.

1.4.3. Spyware

Spyware es software de espionage (*spying software*, en inglés). Es todo software con comportamiento maligno que apunta a la recolección de información sobre una persona u organización y enviarla a otra entidad de una forma que hiere al usuario violando su privacidad, amenazando su seguridad, entre otras formas.

Frecuentemente está asociado a software publicitario, y su funcionalidad está incluida en muchas aplicaciones legítimas. Sin embargo, también se emplea en programas varios y malware empleado por gobiernos y APTs.

1.4.4. Troyano

Cualquier malware que engaña al usuario y oculta sus intenciones haciéndose pasar por software legítimo. Su nombre proviene del caballo de Troya.

1.4.5. Virus

Malware que, una vez ejecutado, se reproduce mediante inyección de código en otro programa. Si es exitoso, se dice que este programa está infectado. Típicamente requiere de un programa huésped y una acción por parte del usuario, el virus debe ser ejecutado.

1.4.6. Wiper

Todo malware diseñado para borrar (wipe, en inglés) un medio de almacenamiento de datos.

1.4.7. Worm

Malware independiente que se reproduce para alcanzar a otras computadoras. Típicamente lo hace a través de redes de computadoras, pero puede también hacer uso de medios físicos. A diferencia de un virus, es un programa independiente que no necesita de interacción con el usuario.

1.5. Ingeniería Social

Cualquier acto que intente o logre influenciar a una persona a actuar de una manera que pueda o no ser de beneficio es un acto de ingeniería social. La principal forma de ingeniería social en la ciberseguridad es el phishing, pero también existen técnicas que involucran hacerse pasar por otra persona, llamadas de voz o mensajes SMS.

1.6. Phishing

Phishing proviene de *fishing* en inglés, y consiste en una táctica de ingeniería social para "pescar"víctimas mediante un engaño. La forma más típica es mediante un correo electrónico, en el cual el atacante intenta parecer lo más

cercanamente posible a algún servicio legítimo o alguna persona de confianza, con el fin de vulnerar a la víctima de alguna forma.

Spear-phishing es una variante del phishing con un enfoque muy preciso en cuanto a su objetivo, mientras que campañas de phishing típicas suelen no ser muy selectivas.

1.7. Zero-day

Un Zero-day 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.

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.

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).

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.

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.

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.

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.

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.

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.

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. Su operación más conocida es la de Stuxnet, en la que colaboró con la NSA de los EE.UU.

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.

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.

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.

3. Eventos y operaciones

3.1. Moonlight Maze (1990)

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.

Un equipo de investigación fue formado en 1999, y la investigación recibió el nombre de "Moonlight Maze..[En] un principio, atribución era muy difícil, pero una investigación reciente por parte de un equipo en Kaspersky reveló 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.

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.

Ataques de esta magnitud muestran que los APTs bien financiados y capaces no son un fenómeno nuevo, existen desde los comienzos del internet moderno y no irán a desaparecer.

4. Conclusión