AMENAZAS PERSISTENTES AVANZADAS (APT): MODELO DE FUNCIONAMIENTO Y ANÁLISIS AL CASO DE ESTUDIO PROJECTSAURON

Cortés Novoa, Andrés Felipe.
Universidad Piloto de Colombia

***Resumen*— Los sistemas informáticos y de comunicación son considerados dos conceptos que tienen mayor impacto en la actualidad, ya que han permitido que desde las actividades diarias de los seres humanos hasta la dirección de las empresas y naciones enteras se apoyen y dependan cada vez más del procesamiento, transferencia y almacenamiento de información. Teniendo en cuenta lo anterior, dado el impacto que estos sistemas generan, las amenazas a la seguridad de la información han evolucionado exponencialmente y por ende las herramientas para explotación de vulnerabilidades son cada vez más estructuradas y generan mayor impacto. Algunas de ellas pueden basarse en pequeños scripts que van de la mano de algunas herramientas con desarrollos simples y otros pueden ser un conjunto orquestado de procesos complejos y continuos que pueden llegar poner en riesgo a toda una nación e incluso a la población mundial.**

***Palabras clave* — Amenazas, información, seguridad, comunicación, vulnerabilidades, riesgo.**

***Abstract*— Computer and communication systems are considered two concepts that have greater impact today as they have allowed from the daily activities of humans to the management of companies and entire nations support and rely increasingly processing, transfer and storage. Given the above, assumed the impact that these systems generate threats to information security have evolved exponentially and thus the tools to exploit vulnerabilities are becoming more structured time and generate greater impact. Some of them may be based on small scripts that go hand in hand with simple tools of some developments and others can be an orchestrated set of complex and continuous processes that can get endanger an entire nation and even the world's population.**

***Keywords* — Threats, information, security, communication, vulnerability, risk.**

I. INTRODUCCIÓN

En la actualidad los ataques cibernéticos han evolucionado progresivamente y se han vuelto cada vez más sofisticados, con mayor impacto, más efectivos y serios. Bajo esta perspectiva y teniendo en cuenta que recientemente se han presentado cambios en términos de infraestructura, desarrollo, redes y modelos de procesamiento de información incluyendo la movilidad, los servicios cloud, virtualización, entre otros, es posible observar el surgimiento de nuevos ambientes y objetivos para los atacantes.

Con base en lo descrito anteriormente, este documento se fundamenta en el análisis del modelo de funcionamiento de las amenazas persistentes avanzadas (APT) teniendo en cuenta su definición y características que lo diferencian de un proceso clásico de explotación de amenazas y que lo convierten en un concepto relevante dentro del ámbito de la seguridad de la información a escalas mundiales.

Finalmente, dado que cada año son descubiertos nuevos métodos de violación de la seguridad de personas, entidades y naciones, este documento presenta un análisis de uno de los casos de APT más importantes identificados hasta ahora y que actualmente es considerado como el top-level en ciber-espionaje que puede poner en riesgo la información de seguridad nacional de algunos países, dando beneficios estratégicos a actores específicos.

II. DEFINICIÓN DE APT

Teniendo en cuenta los recientes acontecimientos relacionados con la fuga de información en las grandes compañías y entidades del estado alrededor del mundo, es evidente que la brecha de seguridad es cada vez más amplia y deja en evidencia información valiosa que puede ser utilizada con diferentes finalidades, algunas de ellas incluso en apoyo a actividades terroristas que afectan la seguridad mundial.

De acuerdo con lo expuesto anteriormente, existe un tipo de ataques a la seguridad de la información que tienen una planificación dirigida y pueden combinar diferentes técnicas de explotación que concretadas pueden actuar de manera sincronizada para afectar la confidencialidad, integridad o disponibilidad de la información, este tipo de ataques se conocen como APT (Advanced Persistent Threats).

En este sentido, es conveniente entender al detalle el significado de cada elemento de los APT antes de abordar con a profundidad su modelo de funcionamiento, con el fin de comprender mejor sus motivaciones y comportamientos. A continuación presenta una breve explicación de cada concepto.

A. *Amenaza*

Es un hecho que puede causar un daño ya sea por causas naturales o humanas en ocasiones buscando un objetivo particular.

En términos de seguridad, este concepto es interpretado como la existencia de un hecho que tiene una intención o motivación en busca un objetivo de daño particular.

B. *Persistente*

De acuerdo con la real academia de la lengua española, el término hace referencia a "mantenerse firme o constante en algo o durar por largo tiempo".

Teniendo en cuenta lo anterior, en términos de seguridad, es posible realizar una interpretación al respecto como un acto que puede tener un alto nivel de planeación dada su durabilidad.

C. *Avanzada*

De acuerdo con el diccionario de la real academia de la lengua española, el término hace referencia a "aquello que se adelanta, anticipa o aparece en primer término"[1]. También puede explicarse como algo adelantado en ideas o doctrinas muy nuevas.

Al visualizar este término en el contexto de la seguridad se puede interpretar como algo innovador o con un alto nivel de complejidad en su diseño y ejecución.

Teniendo en cuenta los tres conceptos anteriores, el significado de APT puede ser definido como:

"Un conjunto orquestado de actividades y procesos informáticos de alta complejidad basado en la identificación de amenazas y bajo un contexto sigiloso y continuo de planeación, con una motivación particular para quebrantar la seguridad de la información en un entorno específico atacando sistemas informáticos y de comunicaciones bajo métodos no convencionales."

III. Características de las APT

La definición anterior permite realizar un análisis de la distinción entre las amenazas tradicionales y los APT teniendo en cuenta propiedades específicas. Dentro de las características principales que distinguen un APT se encuentran:

A. *Tiene objetivos claros y específicos*

Los objetivos son generalmente gobiernos u organizaciones que contienen un alto valor en términos de propiedad intelectual. A diferencia de las amenazas tradicionales que se ocupan de propagarse lo más pronto posible con el fin de incrementar las posibilidades de recolectar información, el APT ataca solo puntos focales de sus objetivos predefinidos, limitando el rango de ataque.

Otro factor diferenciador considerado relevante de un APT en comparación con un ataque tradicional es la búsqueda de activos digitales que puedan dar un beneficio estratégico o ventaja competitiva como información de seguridad nacional, propiedad intelectual, secretos de estado, entre otros. En contraste, una amenaza tradicional busca información personal como números de seguridad social, tarjetas de crédito o cualquier otra información que permita ganancias monetarias.

B. *Tiene un alto nivel de planeación y los atacantes cuentan con los recursos necesarios*

Los actores detrás de un APT son a menudo un grupo de especialistas en hacking trabajando bajo una misma línea, algunos de ellos trabajan para gobiernos o en unidades cibernéticas de organizaciones militares e incluso son contratados por compañías privadas, teniendo así los recursos técnicos y financieros disponibles para trabajar por largos periodos de tiempo y tener acceso a herramientas de ataque sofisticadas.

C. *Tiene una larga duración e intentos repetitivos*

Comúnmente es una actividad de larga durabilidad que puede permanecer en el anonimato para la red objetivo por varios meses o años. Esto se produce como consecuencia de la persistencia que tiene el atacante especialista para ejecutar intentos e ir modificando sus modalidades de ataque de acuerdo a los intentos que resulten fallidos.

D. *Está basado en técnicas sigilosas y evasivas*

Estos ataques tienen la habilidad de permanecer indetectables, ocultándose dentro de los parámetros normales de tráfico de red de la entidad objetivo e interactuando sólo lo suficiente con el fin de alcanzar los objetivos definidos.

Comúnmente son usadas herramientas de red que permitan administrar el tráfico entrante o saliente con el fin de prevenir detecciones de grandes volúmenes de tráfico que alerten a los administradores de los sistemas.

Teniendo en cuenta las características anteriormente mencionadas, así como también las definiciones iniciales y el concepto general, la siguiente tabla muestra la comparación entre un tipo de ataque común y un APT teniendo en cuenta algunas de sus propiedades mas importantes (Tabla. 1).

TABLA I
COMPARACIÓN DE ATAQUES TRADICIONALES Y DE APT[2]

Propiedad	**Ataques tradicionales**	**Ataques APT**
Atacante	Comúnmente es un solo individuo	Un grupo organizado con alta disponibilidad de recursos y patrocinio.

[1] Tomado de: http://dle.rae.es/?id=4WjlsYm

[2] Fuente: El autor

Objetivo	Múltiples objetivos que incluyen personas o entidades.	Organizaciones específicas con información relevante de propiedad intelectual, gubernamental y de seguridad nacional.
Propósito	Beneficios financieros o reconocimientos	Avances competitivos, espionaje o beneficios estratégicos.
Ejecución	Comúnmente en un solo intento por un corto periodo de tiempo	Múltiples intentos dentro de un largo periodo de tiempo.

IV. Modelo de ataques en APT

Como se mencionó anteriormente, los APT son ataques planeados a un alto nivel de detalle, que incluso puede dejar al descubierto vulnerabilidades que se convierten en el argumento de futuras investigaciones y un problema más por resolver para los profesionales en seguridad.

En este contexto, es indispensable realizar un análisis de los pasos y técnicas utilizadas por este tipo de amenazas para materializarse en ataques de gran impacto para entidades, naciones y sociedades enteras.

Dicho lo anterior, es posible realizar un análisis del funcionamiento del APT basado en fases.

A. Reconocimiento

Recolección de información del objetivo, mediante la observación de áreas especificas en las que se puede enfocar al atacante para lograr un compromiso del sistema de larga duración con el mínimo esfuerzo posible.

En este paso es necesario que los atacantes cuenten con la habilidad para identificar y realizar una evaluación profunda del objetivo, recolectando la mayor cantidad de información relevante posible con respecto al ambiente técnico y a los empleados clave dentro de la organización. Esta información es a menudo obtenida mediante las siguientes técnicas:

1) Ingeniería Social: Es un tipo de manipulación psicológica de las personas con el fin de lograr cierto objetivo. En términos de ataques cibernéticos, es a menudo utilizado para obtener información sensitiva o hacer que la víctima realice una acción determinada (Ejemplo: abrir un archivo que almacena una supuesta información pero que puede contener malware).

2) OSINT: Este es un tipo de información de inteligencia recolectada por la publicidad disponible. Esta fuente de información es libre, gratuita y desclasificada. También puede ser utilizada en la toma de decisiones.

Además de utilizar este tipo de técnicas, los atacantes pueden hacer uso de minería de datos o big data para procesar automáticamente grandes volúmenes de datos. Basados en estos análisis, los actores involucrados pueden construir un plan de ataque y preparar las herramientas necesarias de acuerdo a sus necesidades. A menudo estos planes contienen diversos vectores de ataque previamente evaluados para que sean adaptados de acuerdo a los cambios que se presenten en el ambiente del objetivo.

B. Intrusión Inicial

En esta etapa, los atacantes realizan el envío de las herramientas (exploits) que requieren para infiltrarse en la red del objetivo. Existen dos mecanismos que pueden ser utilizados para este tipo de intrusión.

1) Intrusión inicial directa: En este tipo de mecanismo, los atacantes pueden realizar el envió de los exploits a los objetivos haciendo uso de técnicas de ingeniería social como el phishing.

2) Intrusión inicial indirecta: Este es un mecanismo sigiloso que puede hacer uso de terceros que tengan relación con el objetivo como por ejemplo un proveedor y para el envío de los exploits a través del mismo. También puede ser comprometido un sitio web usado por los usuarios de la entidad objetivo, ya que existe una relación de confianza entre las dos entidades que puede ser usado como arma para la intrusión requerida.

Como complemento de esta etapa, la intrusión inicial se completa cuando el atacante logra el primer acceso no autorizado a la red del objetivo. Este acceso puede presentarse en un modo "legítimo" después de realizar un ataque de ingeniería social y obtener las credenciales o ejecutando código malicioso que permita explotar alguna vulnerabilidad de un dispositivo de propiedad del objetivo.

En el caso de que la intrusión inicial se realice por medio de un acceso "no legítimo" es necesario que el atacante realice actividades de footprinting y de escaneo de los activos críticos del objetivo para poder conocer los posibles vectores de ataque que puede aprovechar.

En los APT, los actores del proceso basan sus vectores de ataque en aplicaciones como Adobe PDF reader, Adobe flash, documentos de office y navegadores web. En algunas ocasiones basta con un simple correo que contenga un link con una supuesta información de interés para poder lograr la intrusión inicial deseada.

C. Inicio del comando y control

El objetivo de este paso es establecer una puerta trasera que permita al atacante obtener el control del sistema comprometido.

Es importante tener en cuenta que para los atacantes es necesario mantener el anonimato y ser sigilosos al momento de controlar los activos comprometidos del objetivo, para esto

hace uso de varios servicios legítimos y de herramientas de publicidad válidas que son explicadas a continuación.

1) Redes sociales: Los atacantes pueden hacer uso de las redes sociales creando varias cuentas y blogs para publicar la información obtenida del sistema comprometido.

2) Redes privadas: La red TOR es actualmente usada por muchos atacantes para poder utilizar servicios ocultos para obtención, publicación o transferencia de información y es altamente efectivo para evadir cualquier intento de rastreo del ataque.

3) *Herramientas de acceso remoto (RAT – Remote access tool por sus siglas en inglés):* Aunque estas herramientas a menudo son utilizadas para acceso remoto legítimo de administradores de sistemas, las RAT son comúnmente utilizadas en los ciber ataques debido a su estructura basada en un cliente-servidor, en donde el cliente se ejecuta en la máquina del atacante y el servidor es el dispositivo de la víctima. Para activar este tipo de herramienta, es necesario que del lado del servidor sea activada la conexión, esto a menudo puede ser posible con el envío de un mail con información interesante para la víctima con algún tipo de archivo o enlace que lleve consigo código de conexión hacia el cliente.

D. Obtención de credenciales

Una vez la comunicación de los sistemas comprometidos y los sistemas del atacante es establecida bajo un entorno de red anónimo como el caso de TOR, los autores del APT pueden moverse el entorno para expandir el control de los sistemas de la víctima. Para lograr esto, los atacantes deben asegurarse de obtener las credenciales de accesos privilegiados (como el caso de los administradores de sistemas) mediante el uso de métodos como:

1) *Ataques de diccionario:* En caso de que el atacante haya podido realizar un estudio del objetivo e incluso se haya infiltrado haciendo ataques de ingeniería social a los recursos claves de la víctima, es posible ejecutar ataques de diccionario con posibles password teniendo en cuenta el tipo de víctima y su comportamiento.

2) *Fuerza bruta:* Teniendo en cuenta la naturaleza persistente de este tipo de amenazas, la fuerza bruta también es una opción que puede ser utilizada por los atacantes para poder obtener credenciales restándole importancia al tiempo que se pueda demorar la ejecución de esta modalidad de ataque.

3) *Secuestro de cuentas de usuario:* En estos casos es probable que el atacante tenga acceso a directorios con archivos que contengan passwords cifrados como el caso del directorio etc/passwd en sistemas Linux. En algunos casos esta modalidad aplica para entornos no virtuales en donde incluso algunos administradores de sistemas pueden dejar en evidencia un password en un documento físico.

4) Keylogger: Este tipo de ataques es muy utilizado por los actores de las amenazas una vez logran su primer acceso, con lo cual pueden además de obtener password, monitorear la información que manejan los recursos humanos claves del objetivo.

Las técnicas anteriores pueden ser usadas para poder obtener credenciales y así realizar un escalamiento de privilegios efectivo.

E. Instalación de herramientas

Basado en los puntos descritos anteriormente, en esta etapa el atacante se puede enfocar ahora en realizar todas las actividades necesarias para asegurar la persistencia y total control de los sistemas del objetivo. Esto requiere una incursión a profundidad en la red con el fin de realizar actividades de recolección de toda la información posible de los activos que almacenan la información que es de especial interés para los involucrados.

Para poder ejecutar este proceso, el atacante hace uso de herramientas que pueden ser legítimamente usadas por el sistema operativo y que son comúnmente usadas por los administradores de TI, con el fin de que sus actividades sean indetectables.

Este paso involucra un largo periodo de tiempo, ya que es de vital importancia no afectar los niveles normales de tráfico de red y de uso de recursos de los activos de la víctima. En algunas ocasiones se puede hacer uso de herramientas especializadas en filtro de información con algoritmos diseñados para uso de recursos mínimos e incluso de actividad en segundo plano cuando el dispositivo este siendo utilizado sin afectar su funcionamiento aparentemente normal.

F. Extracción de datos

Teniendo en cuenta que el objetivo primario de un APT es el robo o filtración de información sensitiva para la obtención de beneficios estratégicos, la extracción de datos es un paso crítico para los atacantes. Esta etapa es usualmente ejecutada mediante canales seguros y ocultos como la red TOR y con herramientas de cifrado que pueden hacer parecer que la información transferida por la red sea de tráfico normal.

Es preciso considerar que cualquier intento de extracción de datos que no sea planificado de manera correcta por el atacante, puede permitir que se rastree el tráfico generado y que sea posible detectar la dirección a la cual se están transfiriendo los datos. Es por este motivo que en ocasiones también se hace uso de botnets que permiten al atacante llevar los datos a varios puntos en varios saltos y sobre varios dispositivos de datos de la red para ocultar su verdadero destino.

Finalmente, después de seguir estos pasos es posible materializar un APT, cabe resaltar que cada ataque puede variar en lo correspondiente a su técnica, su modelo de recolección de información e incluso las herramientas que puede utilizar para vulnerar los activos del objetivo de acuerdo con los vectores de ataque establecidos, siendo estas últimas de alto nivel de sofisticación (en términos de uso por parte de los atacantes y de desarrollo por parte de los creadores), sin embargo estos son los pasos generales que son

a menudo usados dentro del modelo de ataque (Fig. 1).

Fig. 1 Pasos generales en la ejecución de ataques basados en APT[3]

V. Caso de estudio ProjectSauron

En Septiembre de 2015 fue descubierto un tráfico anómalo en la red de una organización de gobierno. Al realizar un análisis del incidente por parte de los laboratorios de la empresa de seguridad Kaspersky, se encuentra una extraña librería ejecutable cargada en la memoria del servidor que contiene el controlador de dominio de la organización.

Esta librería fue registrada como un filtro de manejo de password de Windows que podía tener acceso a información sensitiva como la contraseña de administrador en texto claro.

Dentro de las investigaciones reveladas por el equipo de Karspersky Labs se reveló que la amenaza detrás de los comandos ejecutados en el ProjectSauron representa un cambio substancial para el ciber-espionaje, ya que fue diseñado como una plataforma completa y sofisticada para ejecutar largas campañas a través de mecanismos sigilosos de supervivencia con múltiples métodos de extracción de datos.

La plataforma de ProjectSauron fue bautizada con este nombre debido a que en una porción del código se hace alusión a la palabra “Sauron” en los archivos de configuración de una de las bibliotecas de ejecución que se presentan como un archivo de configuración del sistema que contiene una llave de cifrado como se muestra en la siguiente imagen (Fig. 2).

```
KBLOG_ROTATE_SECS = 10800
tmp_dir = os.getenv("WINDIR") .. "\\temp\\"
drive = "C:\\"
SAURON_KBLOG_KEY = "mISfx1q2Ef/QJPO4gi6DMKD5lxeQ380knDrULcZyTF5vFNWb
create_log = function(l_1_0, l_1_1, l_1_2, l_1_3)
  local f = ""
  repeat
    w.sleep(1000)
    t1 = "b"
    t2 = "k"
    t3 = "a"
```

Fig. 2 Llave utilizada en librerías del ProjectSauron[4]

Después de realizar unos análisis de telemetría, se descubrió que este es un tipo de plataforma modular diseñada para ejecutar campañas de ciber espionaje a largo plazo.

Este tipo de plataformas también son consideradas dinámicas ya que pueden aprovecharse de una variedad de herramientas y vulnerabilidades disponibles en los sistemas operativos del hardware del objetivo, haciendo que las operaciones que se ejecuten dentro del activo sean transparentes ante un log de cambios y que parezcan totalmente legítimas para los administradores de estos sistemas.

Al ser considerada una plataforma modular, se encuentran características relevantes que hacen de esta amenaza un claro ejemplo de la sofisticación de los nuevos ataques y de la manera en que han ido aprendiendo los actores de este proyecto a no cometer los mismos errores de pasados intentos de otros actores que han sido rastreados en sus pruebas de penetración.

Para este caso en cuestión el ProjectSauron toma grandes ventajas de herramientas sofisticadas creadas en el pasado para realizar ciber-espionage como el caso de Duqu que es un malware el cual está relacionado con ataques de tipo Stuxnet (ataques que afectan la seguridad de los controladores lógicos programables) y que hace uso de vulnerabilidades de zero-day las cuales se han convertido en uno de los principales problemas para entidades y fabricantes de tecnología generando eternos bugs y fixes para poder minimizar o tratar estos riesgos, esto sin mencionar el gasto económico y de recurso humano que se debe invertir para la corrección de este tipo de vulnerabilidades y tampoco sin restarle importancia al recurso tecnológico que en ocasiones debe ampliarse para poder gestionar este tipo de amenazas.

El siguiente gráfico (Fig. 3) presenta en su generalidad las herramientas interrelacionadas y sus características que fueron la base de la creación de la plataforma de ProjectSauron y que

[3] Fuente: El autor.

[4] Fuente: https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf

son parte del éxito que tiene esta herramienta para ejecutar las actividades de ciber-espionaje.

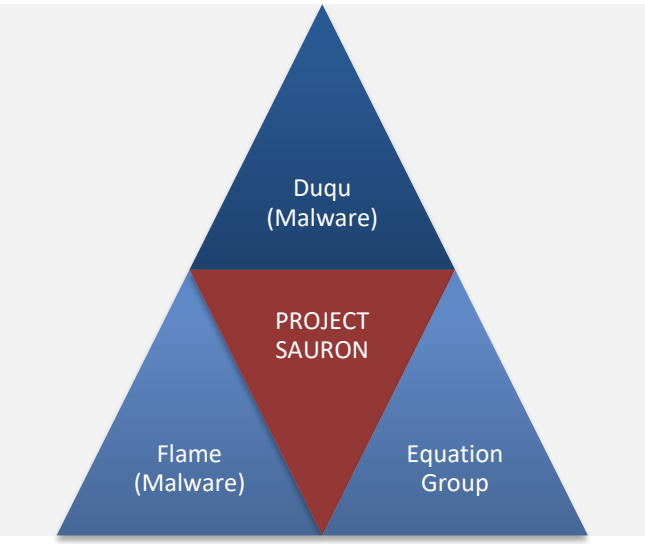

Fig. 3 Bases de creación de ProjectSauron[5]

Teniendo en cuenta la figura anterior, la modularidad que involucra la plataforma de Project Sauron esta basada en dos herramientas sofisticadas y la existencia Equation como un grupo de autores de amenazas reconocidos a nivel mundial por sus técnicas de ofuscación de algoritmos de cifrado.

Desde la perspectiva del APT, es posible realizar un análisis general de esta plataforma modular mediante el desglose de sus principales componentes (Fig. 4).

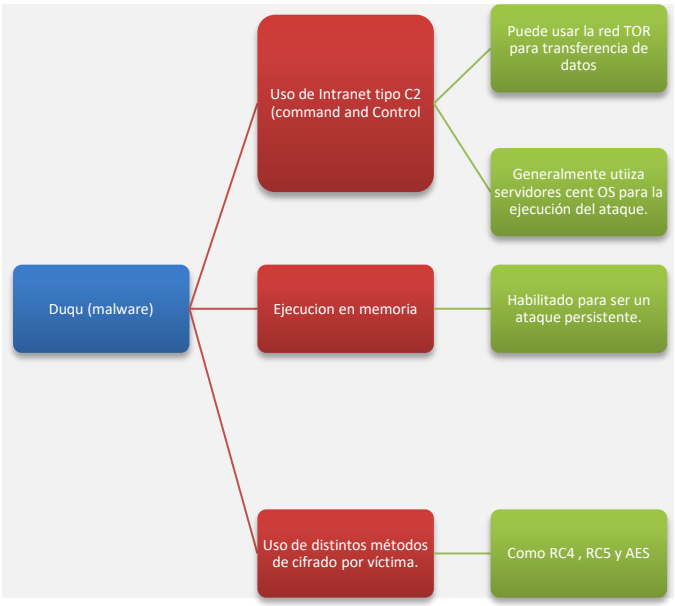

Fig. 4 Características del malware Duqu.[6]

El siguiente gráfico corresponde a las características del Malware conocido como Flame (F

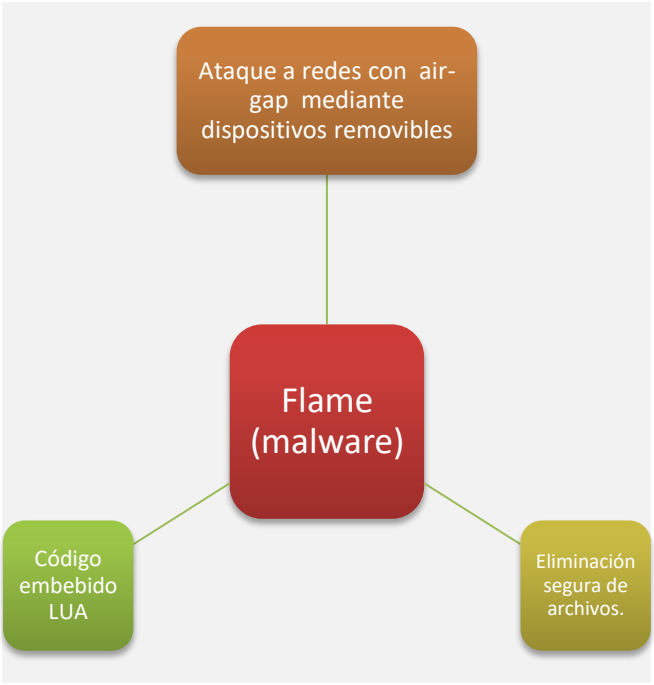

Fig. 5 Características de funcionamiento del malware tipo Flame[7]

Por último, con respecto al grupo Equation (Actores de las principales amenazas de seguridad a nivel mundial) se destacan distintas particularidades (Fig. 6).

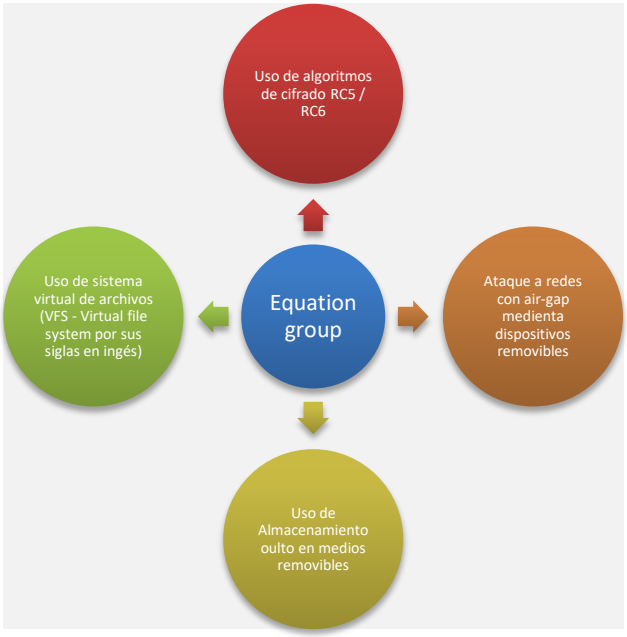

Fig. 6 Características principales del grupo Equation.[8]

[5] Fuente: El autor
[6] Fuente: El autor
[7] Fuente: El autor
[8] Fuente: El autor

Teniendo en cuenta las características y técnicas de cada herramienta presentada en los diagramas anteriores, es posible obtener una perspectiva del funcionamiento de la plataforma de ProjectSauron y sus tipologías, las cuales hacen de esta herramienta una utilidad completa al momento de ejecutar campañas de ciber-espionaje.

De acuerdo con la empresa Kaspersky labs, fueron encontradas más de 30 organizaciones en Rusia, Irán y Ruanda que resultaron infectadas por esta plataforma modular. Estas organizaciones pertenecen a diferentes actividades.

- Organizaciones de Gobierno
- Centros de investigación científica
- Militar
- Proveedores de telecomunicaciones
- Entidades Financieras

En términos técnicos, esta sofisticada plataforma utiliza un módulo persistente sobre los controladores de dominio como los filtros de contraseñas en el local system authority de Windows, la cual es usada por los administradores para poder gestionar las políticas de password y validación de nuevas contraseñas con el fin de que cumplan con los requerimientos específicos en términos de longitud y complejidad. Bajo esta premisa, el ProjectSauron incluye un módulo con una puerta trasera pasiva que permanece activa en todo momento, en todo el dominio y para todos los usuarios pertenecientes a ese dominio, e identifica en los logs de administrador los cambios de password y los recolecta en un texto plano.

Para los casos en donde el controlador de dominio carece de acceso a internet, los atacantes realizan la instalación de componentes adicionales en otros servidores de la intranet con salida a internet que les permiten utilizarlos como proxy con el fin de poder realizar la respectiva extracción de datos.

Una vez instalados estos componentes, se inician otros módulos de la plataforma que actúan clandestinamente con el fin de no mostrar actividad alguna en el tráfico de red y que se puedan ejecutar sólo al momento de que reciban una instrucción de tipo wake-up desde el tráfico de red entrante. Basado en este método, la plataforma de ProjectSauron asegura una persistencia extendida en los servidores de las organizaciones objetivo.

Dicho lo anterior, la mayoría de los procesos de ejecución de ProjectSauron trabajan como puertas traseras las cuales también pueden descargar nuevos módulos o ejecutar comandos desde el atacante únicamente en memoria, por lo que el único método posible para poder detectar estos módulos es realizando una copia del volcado de memoria y analizando sus registros en los sistemas infectados, lo cual es una actividad que tiene un alto nivel de complejidad para los administradores de TI.

Algunos módulos secundarios de la plataforma están diseñados para ejecutar funciones especificas como el robo de documentos, keylogger y secuestro de llaves de cifrado desde las máquinas infectadas.

Estos módulos tienen la característica particular de contener diferentes nombres de archivos y tamaños en cada una de las máquinas infectadas, por lo que el hecho de descubrir la vulnerabilidad en una máquina no significa que se pueda identificar en las demás por los nombres de archivo o el tamaño que contienen. En algunos casos estos archivos también contienen diferentes encabezados, por lo que puede convertirse en un gran problema para la identificación por parte de los software antivirus.

Dada la arquitectura modular que maneja esta plataforma, también implementa un sistema de archivos virtuales para poder almacenar plugins adicionales. De acuerdo con la investigación realizada por Kaspersky Labs existen más de 50 tipos de plugins en el ProjectSauron.

En lo que respecta a la ejecución en sistemas operativos, los módulos de esta plataforma pueden trabajar en sistemas Windows en versiones de 64 bits y de 32 bits y en las últimas versiones de Windows server. Por su parte, en términos de red usa protocolos comunes como ICMP, UDP, TCP, DNS, SMTP y HTTP.

Para le extracción de datos el ProjectSauron usa varios caminos para ocultarse con el fin de tener planes de contingencia en casos donde no sea posible filtrar la información por alguno de los métodos. Dentro de los caminos que utilizaba esta plataforma para el envío de los datos se encuentra la implementación de comunicación con comando y control en los proxy intermedios usando protocolos estándar y mediante redes seguras como la de TOR para que una vez la información saliera de la organización objetivo, no fuera posible rastrear su movimiento dentro de la red.

Una de las técnicas poco usuales que utiliza esta plataforma se basa en el tunneling de DNS usando el modo de bajo consumo de ancho de banda mediante instrucciones complejas (Fig. 7).

```
    domain = "bikessport[.]com"
execStr = string.format("sinfo | basex -b 32url | dext -l 30 a." ..
domain .. " | nslu -") res = w.exec2str(execStr)
```

Fig. 7. Ejemplo tunneling en DNS con bajo uso de ancho de banda.[9]

En esta simple instrucción escrita en lenguaje LUA se puede visualizar una llamada a una herramienta denominada “sinfo” para la recolección de información que es codificada en formato base-64 y que es enviada hacia el dominio a.bikessport[.]com con una longitud de 30 bytes por paquete enviado con el fin de no generar un tráfico inusual en los IDS de la organización objetivo. Por ultimo, la herramienta utilizada para el envío de los paquetes DNS uno a uno es NSLU.

[9] Fuente: https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf

De manera análoga, ProjectSauron utiliza e-mails como método alternativo para la extracción de la información, los cuales contienen encabezados similares a los que usa un servicio de correo electrónico como Gmail o Hotmail y contiene un archivo que a simple vista parece benigno porque proviene de un proveedor, pero que al ser ejecutado puede abrir una puerta trasera que utilice protocolos de red comunes que permitan enviar la información a la red TOR.

De acuerdo con el análisis anterior, se puede observar que las actividades de ciber-espionaje han sido desarrolladas a tal punto que combinan otros métodos de ataque que fueron efectivos en el pasado pero que actualmente funcionan como base de los nuevos desarrollos que los grupos como Equiation que tiene un alto nivel de experiencia en el ámbito de seguridad y que pueden poner en riesgo a cualquier organización.

Es oportuno ahora entender que el mundo actual está alojando día a día más amenazas en torno a la seguridad de la información, así como también los actores de estas amenazas surgen de manera exponencial y desarrollan cada vez mejor sus métodos de recolección de información, análisis de los objetivos, identificación de vectores de ataque, herramientas de explotación y técnicas de extracción de información.

Actualmente el software malicioso está siendo constantemente mejorado, al punto en que ya se adaptan al entorno que están vulnerando y tienen la capacidad de aprender en cada intento de ataque bajo métodos heurísticos. Por el contrario desde el contexto de las herramientas de prevención y control, es poco el desarrollo que existe para contraatacar un malware que presenta una casuística basada en APT.

Desde esta perspectiva, las naciones deben hacerse responsables por el cuidado de la información que puede representar un riesgo para la población basados en leyes y regulaciones en primera instancia.

Como segunda medida, los expertos en seguridad de la información independientemente de su rol deben asegurar que tanto en términos de gestión documental como en el ámbito técnico, se desarrollen las habilidades suficientes para poder garantizar mejores entornos defensivos en contra de agentes maliciosos que busquen obtener beneficios estratégicos que pueden generar impactos a gran escala.

Dicho lo anterior, el rol actual del profesional de seguridad es generalmente enmarcado dentro de un entorno exclusivamente corporativo que le brinda beneficios a una compañía con una lógica de negocio particular. Sin embargo, es válido considerar que la seguridad en la era actual no solo esta relacionada con el objetivo o políticas de una organización, sino que puede ser vista desde un ámbito social y como una necesidad que el mundo actual ha adquirido como consecuencia del desarrollo de nuevas amenazas a los sistemas de datos y telecomunicaciones.

Finalmente es posible considerar las APT como un concepto que no solo incluye dentro de sus objetivos a entidades públicas o privadas, sino que puede también tener un campo de acción que supere los límites organizacionales y se traslade a la sociedad, a tal punto que pueda llegar a afectar individualmente la información de las personas causando impactos de mayor magnitud que pueden dejar como consecuencia daños irreparables para un país, un continente o en el mundo entero.

Lo expuesto anteriormente hace parte de la responsabilidad que debería ser asumida también por los actuales expertos en seguridad, sin embargo, la gran mayoría basan sus actividades diarias únicamente en el objetivo de negocio de una compañía en particular, sin considerar que el ámbito social carece de propuestas y acciones de estos profesionales, lo cual puede abrir paso a un campo de investigación que no hace parte del alcance del presente articulo, pero si involucra a los APT como concepto relevante.

VI. Conclusiones

- La situación actual de los ataques cibernéticos es un asunto preocupante por el constante desarrollo que han tenido a través de la historia no solo para las organizaciones privadas, sino que en algunos casos se convierten en asuntos sociales y de seguridad nacional.
- Las amenazas persistentes avanzadas son un factor importante que requiere una profunda atención por parte de los profesionales involucrados en seguridad de TI, ya que día a día se vienen desarrollando nuevas técnicas y herramientas que ponen en riesgo la seguridad de la información.
- Los casos más reconocidos de ciber-espionaje están relacionados con APT bajo el uso de herramientas sofisticadas que no son detectables fácilmente.
- La seguridad de naciones enteras y de las sociedades puede llegar a depender del tipo de defensa implementado para contrarrestar ataques que permitan extraer información privilegiada y sensitiva para un beneficio estratégico de los actores.
- El funcionamiento de plataformas como las del ProjectSauron son una clara demostración de que las técnicas de ataque basadas en APT han evolucionado haciendo uso del aprendizaje de los errores en antiguas ejecuciones de ataques.
- Grupos como Equation, LulzSec, Anonymus y algunos cibercriminales individuales constituyen una amenaza en la red que puede llegar a jugar un papel importante en la economía y en el sustento de las naciones.
- El uso de redes privadas como TOR permite que los ataques se puedan propagar de manera anónima sin dejar rastro alguno lo cual representa una gran amenaza para los gobiernos del mundo que no tiene control a la fecha.
- Los nuevos profesionales de seguridad y los que se encuentran activos deben considerar su rol en ámbitos sociales que permitan asegurar a una población contra las APT.

VII. REFERENCIAS

[1] C. Eric. Advanced Persistent Threat: Understanding the danger and how to protect your Organization. Ed. Syngress. Año 2013. ISBN: 978-1-59749-949-1. Massachsetts. EE.UU.

[2] Global Research and Analysis Team – Kaspersky Labs. The ProjectSauron APT. Version 1.02. 2016. [Online] Disponible en: https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf

[3] A. Rui , B. Dannya, E. Hoda, F. Alexander, H. John, H. Tomonori, D. Johan and P.Alexander. Diagnosing Advanced Persistent Threats: A Position Paper. Palo Alto, CA 94304, USA. [Online] Disponible en: http://ceur-ws.org/Vol-1507/dx15paper25.pdf

[4] Fire Eye Labs. Madiant consulting M-Tends Labs 2016. California. 2016. [Online] Disponible en: https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

[5] C. Ping, D. Lieven and H. Christophe. A study on Advanced Persistent Threats. [Online] Disponible en: https://lirias.kuleuven.be/bitstream/123456789/461050/1/2014-apt-study.pdf

[6] Global Research and Analysis Team – Kaspersky Labs. Equiation Group: Questions and Answers. Version 1.5. Febrero 2015. [Online] Disponible en: https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

[7] H. Pengfei, L. Hongxing, F. Hao, C. Canserver and M. Prasant. Dynamic Defense Strategy against Advanced persisten threat with insiders. [Online] Disponible en: http://spirit.cs.ucdavis.edu/pubs/conf/infocom15-pengfei.pdf

[8] M. B. Salem, S. Hershkop, and S. J. Stolfo, “A survey of insider attack

[9] detection research,” in Insider Attack and Cyber Security. Springer,2008, pp. 69–90.

[10] Symantec Corporation. Advanced Persistent Threats: A Symantec Perspective. Año 2011. [Online] Disponible en: http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

[11] R. Ierusalimschy, L. H. de Figueiredo, W. Celes. Lua 5.1 Reference Manual. Año 2006. ISBN 85-903798-3-3

[12] M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest, “Flipit: The game of stealthy takeover,” Journal of Cryptology, vol. 26, no. 4, pp. 655–713, 2013.

[13] ISACA. Advanced persistent threat Awarness. 2015.

[14] Fire Eye. Prevención y defensa avanzada contra malware moderno y APT. Junio 2013. [Online] Disponible en: http://www.xnetworks.es/contents/FireEye/FireEye_SIC.pdf

[15] S. Backhaus, R. Bent, J. Bono, R. Lee, B. Tracey, D. Wolpert, D. Xie, and Y. Yildiz, “Cyber-physical security: A game theory model of humans interacting over control systems,” Smart Grid, IEEE Transactions on, vol. 4, no. 4, pp. 2320–2327, 2013.

[16] IEEE. Preparation of papers for IEEE Transactions And Journals. December 2013. [Online] Disponible en: https://www.ieee.org/documents/trans_jour.docx

[17] Real Academia de la Lengua Española. Diccionario. Disponible en: http://dle.rae.es/?w=diccionario