UNIVERSIDAD
CATÓLICA DE CÓRDOBA
Universidad Jesuita

Advanced Persistent Threats

Asignatura: Auditoria y Seguridad Informática

Alumnos: Emiliano Cussino, Ignacio Achaval Palacio

Carrera: Ingeniería en Sistemas

Advanced Persistent Threats

Introducción

Una amenaza persistente avanzada (Advanced Persistent Threat o APT) es un ataque cibernético prolongado y dirigido en el que un intruso obtiene acceso a una red y permanece sin ser detectado por un período de tiempo. La intención de un ataque APT generalmente es monitorear la actividad de la red y robar datos en lugar de causar daños a la red u organización.

Los ataques APT generalmente apuntan a organizaciones en sectores como la defensa nacional, la industria manufacturera y la industria financiera, ya que esas empresas manejan información de alto valor, incluida la propiedad intelectual, planes militares y otros datos de gobiernos y organizaciones empresariales.

El objetivo de la mayoría de los ataques APT es lograr y mantener el acceso continuo a la red objetivo en lugar de entrar y salir lo más rápido posible. Debido a que se requiere una gran cantidad de esfuerzo y recursos para llevar a cabo ataques APT, los piratas informáticos suelen apuntar a objetivos de alto valor, como los estados o naciones y las grandes corporaciones, con el objetivo final de robar información durante un largo período de tiempo.

Para obtener acceso, los grupos de APT a menudo usan métodos avanzados de ataque, que incluyen exploits avanzados de vulnerabilidades de día cero, así como el spear phishing y otras técnicas de ingeniería social. Para mantener el acceso a la red objetivo sin ser descubierto, los actores de amenazas utilizan métodos avanzados, incluida la reescritura continua de códigos maliciosos para evitar la detección y otras técnicas sofisticadas de evasión. Algunas APT son tan complejas que requieren administradores de tiempo completo para mantener los sistemas y el software comprometidos en la red objetivo.

Los motivos de los actores avanzados de amenazas persistentes son variados. Por ejemplo, los atacantes patrocinados por los estados nacionales pueden apuntar a la propiedad intelectual para obtener una ventaja competitiva en ciertas industrias. Otros objetivos pueden incluir servicios de distribución de energía y telecomunicaciones y otros sistemas de infraestructura, redes sociales, organizaciones de medios, así como objetivos electorales y otros objetivos políticos. Los grupos del crimen organizado pueden patrocinar amenazas persistentes avanzadas para obtener información que puedan usar para llevar a cabo actos criminales con fines de lucro.

Aunque los ataques APT pueden ser difíciles de identificar, el robo de datos nunca es completamente indetectable. Sin embargo, el acto de extraer datos de una organización puede ser la única pista que tienen los defensores de que sus redes están bajo ataque. Los profesionales de seguridad cibernética a menudo se centran en detectar anomalías en los datos salientes para ver si la red ha sido el objetivo de un ataque APT.

¿Cuáles son las características principales de una APT?

- Personal: el atacante selecciona objetivos con base en intereses políticos, comerciales o de seguridad y tiene una definición clara de la información que busca obtener de la víctima.

- Persistencia: si un objetivo se resiste a ser penetrado, el *hacker* no abandonará la misión, lo que hará es cambiar la estrategia y desarrollará un nuevo tipo de ataque. Incluso podría decidirse por pasar de un vector de ataque externo a uno
  interno.

- Control y enfoque: una APT está enfocada en tomar control de elementos cruciales de la infraestructura, como redes de
  distribución eléctrica o sistemas de comunicaciones; también busca comprometer la propiedad intelectual de otros o información de seguridad nacional, mientras que los datos personales no suelen ser de interés para un atacante de este
  estilo.

- Tiempo y dinero: los perpetradores de una APT no suelen preocuparse por el costo del ataque, incluso pueden no preocuparse de los ingresos a partir del mismo, ya que a menudo están financiados por estados nacionales o por el crimen organizado.

- Automatización: los *hackers* hacen uso de *software* y sistemas automatizados para aumentar el poder de penetración contra un solo objetivo, a diferencia de otros tipos de ataques que utilizan sistemas automatizados para atacar múltiples objetivos.

- Una sola capa: solo un grupo u organización posee y controla todos los roles y responsabilidades durante el ataque. Estos roles y responsabilidades no están distribuidos en grupos externos a la organización atacante.

¿Por qué es tan difícil detectar una APT?

- Más que tomar control de las aplicaciones y de la infraestructura de la red, buscan aprovecharse de los recursos y privilegios de las personas que forman parte de la organización.

- Usan firmas de ataque únicas y de gran creatividad.

- Más que tomar control de los componentes y de las aplicaciones de la red, una ATP se basa en los recursos de los usuarios y sus privilegios.

- El comportamiento y las “firmas” de un ataque de este tipo son difíciles de correlacionar con los de ataques conocidos, incluso si la empresa utiliza un correlacionador o un SIEM (*Security Incident and Event Management*).

- Normalmente una APT es distribuida a lo largo de periodos de tiempo prolongados, haciéndola difícil de correlacionar con base en los datos de fecha y hora.

- Los ataques parecieran venir de una gran variedad de fuentes. Las *botnets* distribuidas son usadas con frecuencia para generar los ataques, haciendo muy difícil la identificación de la red hostil.

- El tráfico de datos del ataque por lo general se encubre a través de cifrado, compresión o enmascarando las transmisiones dentro del comportamiento "normal" de programas comprometidos.

- Muchas APT son diseñadas de manera específica para operaciones encubiertas y se mueven de un sistema comprometido a otro sin generar el tráfico predecible que se ve en otra clase de *malware*. Los ataques APT suelen diseñarse para evadir las soluciones *antimalware* y los *IPS*, además de que pueden ser compilados para una industria u organización específica.

¿Cuáles son las cualidades de una APT?

Aunque los métodos y tecnologías usadas pueden variar mucho, casi siempre exhiben estas cualidades:

- **Ataques personalizados basados en la organización objetivo:** Los *hackers* seleccionan sus objetivos y diseñan sus métodos de ataque e infiltración para tener el mayor efecto posible en los sistemas, defensas y personal de las organizaciones objetivo. Atacan a los empleados y a los usuarios válidos de alto nivel que tienen privilegios en los sistemas y procesos que necesitan atacar. Emplean técnicas de reconocimiento e inteligencia para entender los sistemas, aplicaciones y redes de la víctima, de tal manera que puedan ser más eficientes, atacando sistemas con vulnerabilidades no corregidas o desconocidas (*zero-day*).

- **Bajo y lento:** Para evadir la detección, los *hackers* mantienen un perfil bajo dentro del ambiente de TI de las organizaciones que infiltran, incluso pueden llegar a esperar meses enteros para que se den las condiciones óptimas para un ataque. El monitoreo sistemático y la interacción con los sistemas comprometidos durante períodos largos de tiempo son la marca típica de una ATP.

- **Organizado y bien financiado:** Los grupos y organizaciones detrás de una APT suelen poseer suficientes recursos financieros para mantener ataques durante largos periodos de tiempo. La sofisticación de las APT sugiere que estos grupos incluyen equipos multidisciplinarios de *hackers* con amplias habilidades y experiencia para lograr el acceso a infraestructuras complejas de TI, evolucionando con ello las cadenas de suministro criminal y sus capacidades de investigación y desarrollo. Además, estos grupos tienen la habilidad de comprar recursos de cómputo en la nube, utilizar *exploits* para vulnerabilidades no descubiertas y usar *botnets* completas para sus propósitos.

- **Métodos de ataque simultáneos y diversos:** Una APT muchas veces utiliza múltiples vectores de ataque simultáneos, tanto automatizados como

humanos. Usan una gran cantidad de métodos y tecnologías para infiltrarse e infectar nodos en los ambientes de TI de sus víctimas y, con frecuencia utilizan ataques de bajo riesgo para distraer a los administradores y a los analistas de seguridad, evitando que se percaten del ataque verdadero.

- **Redes sociales:** Es muy común el uso de herramientas de redes sociales, como invitaciones falsas de Linkedln®, para ganar la confianza de las víctimas y comprometer así los sistemas y las credenciales de acceso a los mismos. Es importante entender el elemento humano de una APT pues es uno de los elementos que hacen tan efectivos este tipo de ataques, ya que utilizan la tendencia de la gente a confiar en otros para así manipular a los empleados y terminar instalando *malware* en los sistemas.

¿Por qué una APT suele ser más exitosa que otro tipo de ataques?

- Los entornos de TI son cada vez más complejos: la mayoría de las grandes organizaciones tienen ambientes muy complejos que incluyen servidores legados, *mainframes*, centros de datos virtualizados, servicios en la nube, etcétera. Estos sistemas
  tan diversos crean muchos desafíos para los equipos de seguridad de TI, que deben cubrir infraestructuras cada vez más grandes cuyo monitoreo y correlación es cada vez más complejo.

- Robo de credenciales de acceso empresarial: investigaciones de la empresa RSA encontraron que 88% de las compañías en la lista Fortune 500 tienen empleados infectados con Zeus, además, reportes de la misma empresa han informado que es común el empleo de credenciales de acceso empresarial por parte de los atacantes en los puntos de recolección de información por parte de los criminales. Lo anterior demuestra que los *hackers* ya tienen las herramientas de *malware* y los puntos de acceso para comprometer ambientes empresariales de TI.

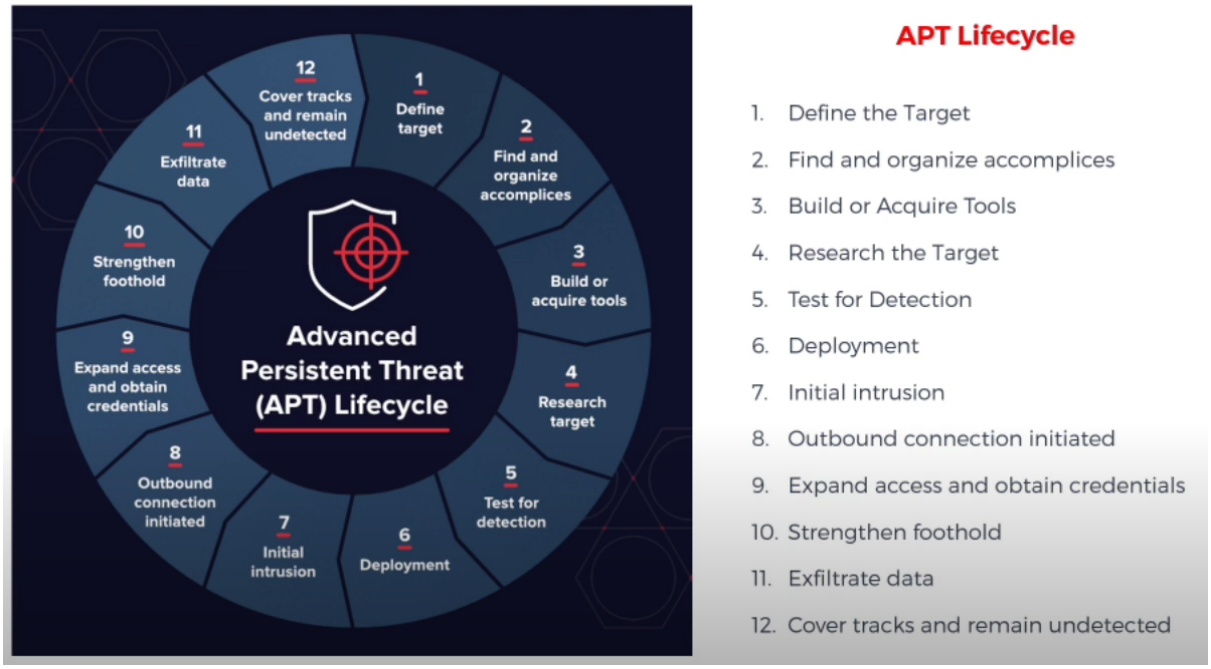
- Costo decreciente: los ataques de APT se han vuelto menos caros de manufacturar e implantar, por lo que muchos grupos criminales han tomado ventaja de los costos, desempeño y escalabilidad del cómputo en la nube.

- Este menor costo incrementa el ROI (retorno de inversión) potencial de un ataque.

Otro punto importante de recordar es que los grupos detrás de este tipo de ataques están motivados por la ganancia que pueden obtener al extraer información de sus víctimas, por lo que se estructuran de manera similar a cualquier otro modelo de negocio que analiza el valor de la información a obtener contra el costo de la obtención.

Ciclo de vida de APT

El ciclo de vida de una APT es mucho más largo y complejo que otros tipos de ataques.



1. **Defina el objetivo:** determine a quién se dirige, qué espera lograr y por qué.
2. **Encuentre y organice cómplices:** seleccione miembros del equipo, identifique las habilidades necesarias y busque acceso interno.
3. **Cree o adquiera herramientas:** busque las herramientas disponibles actualmente o cree nuevas aplicaciones para obtener las herramientas adecuadas para el trabajo.
4. **Objetivo de investigación:** descubra quién tiene el acceso que necesita, qué hardware y software utiliza el objetivo y cómo diseñar mejor el ataque.
5. **Prueba de detección:** implemente una pequeña versión de reconocimiento de su software, pruebe las comunicaciones y alarmas, identifique los puntos débiles.
6. **Despliegue:** comienza el baile. Implemente la suite completa y comience la infiltración.
7. **Intrusión inicial: una** vez que esté dentro de la red, averigüe a dónde ir y encuentre su objetivo.
8. **Conexión saliente iniciada:** objetivo adquirido, solicitando evacuación. Cree un túnel para comenzar a enviar datos desde el objetivo.

9. **Amplíe el acceso y obtenga credenciales:** cree una "red fantasma" bajo su control dentro de la red de destino, aprovechando su acceso para ganar más movimiento.
10. **Fortalezca su posición:** aproveche otras vulnerabilidades para establecer más zombis o extender su acceso a otras ubicaciones valiosas.
11. **Extraer datos: una** vez que encuentre lo que estaba buscando, devuélvalo a la base.
12. **Cubra pistas y no lo detecten:** toda la operación depende de su capacidad para permanecer oculto en la red. Permanecer indetectable en sus controles de sigilo y asegúrese de limpiar todo rastro de intrusion.

Detección

Características de un ataque APT

Se pueden definir algunas características de los ataques apt:

- Actividad inusual en las cuentas de usuario, como un aumento en los inicios de sesión de alto nivel o grandes transferencias de datos fuera del horario normal de oficina o en ubicaciones inusuales
- Incrementos repentinos en el tráfico de red,sobre todo en las transferencias salientes.
- Presencia generalizada de troyanos de puerta trasera
- Paquetes de datos inesperados o inusuales, que pueden indicar que los datos se han acumulado en preparación para la exfiltración
- anomalías en los datos salientes o un aumento repentino e inusual en las operaciones de la base de datos que involucran cantidades masivas de datos
- Consultas repetidas a nombres DNS dinámicos
- Búsquedas inusuales de directorios y archivos de interés para un atacante, por ejemplo, búsquedas en repositorios de código fuente
- Archivos de salida grandes no reconocidos que se han comprimido, cifrados y protegidos con contraseña
- Detección de comunicaciones hacia / desde direcciones IP falsas
- Cambios inexplicables en las configuraciones de plataformas, enrutadores o firewalls
- Mayor volumen de eventos/alertas de IDS (sistema de detección de intrusiones)

Defensa y protección de APT

APT es un ataque multifacético y las defensas deben incluir múltiples herramientas y técnicas de seguridad. Éstas incluyen:

- **Filtrado de correo electrónico** : la mayoría de los ataques APT aprovechan el phishing para obtener acceso inicial. Filtrar correos electrónicos y bloquear enlaces o archivos adjuntos maliciosos dentro de los correos electrónicos puede detener estos intentos de penetración.
- **Protección de endpoints** : todos los ataques APT implican la toma de control de dispositivos endpoints. La protección antimalware avanzada y la detección y respuesta de endpoints pueden ayudar a identificar y reaccionar ante el un endpoint comprometido por parte de los actores de APT.
- **Control de acceso :** las medidas de autenticación sólidas y la administración cercana de las cuentas de usuario, con un enfoque especial en las cuentas privilegiadas, pueden reducir los riesgos de APT.
- **Monitoreo del tráfico, comportamiento de usuarios y entidades :** puede ayudar a identificar penetraciones, movimientos laterales y exfiltración en diferentes etapas de un ataque APT. Monitoreo del tráfico entrante y saliente de nuestra red, sobre todo el saliente.
- **Adquirir o incorporar a la infraestructura de seguridad:** existente alguna solución Anti-APTs
  de las existentes en el mercado (FireEye, Trend Micro, McAfee, Palo Alto, Kaspersky Labs,).
- **Promover la importancia de la seguridad dentro de nuestra organización:** mediante formación interna, cursos online, capacitación constante.

Mitigaciones

La **Dirección de Seguridad de la Información de los EE.UU.** (IAD) redactó una publicación con sus **Estrategias de Mitigación para la Seguridad Informática** con alguna referencia a las APTs.

Se destacan cuatro áreas clave:

- Integridad del dispositivo
- Contención de daños
- Protección de cuentas
- Transporte seguro y disponible.

Otra de las guías disponibles para mitigar intrusiones cibernéticas selectivas, proviene de la Dirección Australiana de Señales (ASD).

La lista completa de estrategias de mitigación de la ASD comprende un total de 35 puntos.

A través de un análisis exhaustivo y completo de los ataques y amenazas locales, la ASD ha encontrado que al menos el 85 por ciento de las intrusiones cibernéticas dirigidas a las que responde podría mitigarse con cuatro estrategias básicas:

- El uso de listas blancas de aplicaciones ayuda a prevenir la ejecución de software malicioso y programas no autorizados.
- Parchar aplicaciones, por ejemplo, Java, visualizadores PDF, Flash, navegadores web y Microsoft Office.
- Parchear vulnerabilidades del sistema operativo.
- Restringir los privilegios administrativos a los sistemas operativos y aplicaciones, en base a los derechos de los usuarios

Estas medidas se consideran tan eficaces que han sido recomendadas para todas las agencias del gobierno australiano.

Cabe destacar que ninguna organización está fuera de riesgo de ser víctima de estos ataques, ya que los atacantes no solo buscan información crítica. Los datos corporativos confidenciales, propiedad intelectual, datos científicos o de acuerdos gubernamentales están todos en la mira. E incluso, en el caso de que la organización no sea un blanco crítico, puede ser utilizada como carnada para desplegar un ataque más ambicioso.

Estrategias de mitigación de la ASD

Si bien la lista cuenta de 35 puntos, estos se podrían agrupar en cuatro tipos lógicos según el enfoque de implementación:

Medidas	**Breve descripción**
Administrativas	Capacitación, seguridad física
Redes	Estas medidas son más fáciles de implementar a nivel de hardware de red
Administración del sistema	El sistema operativo contiene todo lo necesario para su implementación
Soluciones especializadas de seguridad	Se puede utilizar software de seguridad especializado

Administrativas: capacitación de los empleados, mejoramiento de la seguridad física de la oficina, etc. Casi ni se menciona el hardware ni el software salvo las medidas para implementar sistemas de control de acceso físico o la capacitación virtual.

Redes: a nivel de redes se pueden tomar muchas medidas de mitigación como por ejemplo, en el décimo lugar de la lista, la "segmentación y segregación de la red" se clasifica como "excelente" para la eficacia de la seguridad en general. En el 23° lugar, "Denegar el acceso directo a Internet desde estaciones de trabajo" está calificado como "bueno" (tercer grado después de "esencial" y "excelente") en términos de importancia para la seguridad.

Administración del sistema: El fortalecimiento de los sistemas contra los ataques selectivos puede generar bastante trabajo para los administradores de sistemas. La parte esencial de las cuatro medidas es la **restricción de privilegios administrativos**.

Soluciones especializadas de seguridad: Como por ejemplo, Kaspersky Lab.

Lista ASD con 30 puntos importantes:

Clasificación de la ASD	Estrategia de mitigación, nombre corto	Tecnologías de Kaspersky Lab
1	Listas blancas de aplicaciones	Listas blancas dinámicas
2	Parchar vulnerabilidades en las aplicaciones	Evaluación de la vulnerabilidad y gestión de parches
3	Parchar vulnerabilidades en el sistema operativo	
5	Endurecimiento de la configuración de las aplicaciones del usuario	Web Control (bloqueo de scripts en navegadores web), Web Anti-Virus
6	Análisis dinámico automatizado de correo electrónico y contenidos web	Mail Anti-Virus y Web Anti-Virus, Security for Mail Server, Security for Internet Gateway, DLP for Mail y Collaboration add-ons
7	Mitigación de vulneraciones genéricas del sistema operativo	Prevención automática de exploits

8	HIDS / HIPS	System Watcher y Application Privilege Control
12	Cortafuegos de aplicaciones basadas en software para el tráfico de entrada	Advanced Firewall
13	Cortafuegos de aplicaciones basadas en software para el tráfico de salida	Advanced Firewall
15	Registro de sucesos del ordenador	Kaspersky Security Center
16	Registro de actividad de la red	Kaspersky Security Center
17	Filtrado de contenidos de correo	Kaspersky Security for Mail Sever
18	Filtrado de contenidos de Internet	Web Control
19	Listas blancas de dominios web	Web Control
20	Bloqueo de mensajes de correo fraudulentos	Anti-Spam
22	Solución antivirus en base al método heurístico y clasificaciones automáticas de reputación en Internet	Anti-Malware
26	Control de medios removibles y portátiles	Device Control
29	Inspección de archivos de Microsoft Office en estaciones de trabajo	Anti-Malware
30	Solución antivirus en base a firmas	Anti-Malware

Casos resonantes:

Stuxnet:

Esta ha sido una de las APT más mencionada en los últimos años, debido a la sofisticación e impacto de haberse materializado, considerada una de las primeras armas de la ciberguerra , Stuxnet es un gusano informático que aprovechando una vulnerabilidad de los sistemas operativos Windows, lograba llegar a explotar otras cuatro vulnerabilidades de día cero que emplean los programas de monitorización y control industrial (SCADA), se cree que este gusano se creó para sabotear el programa nuclear iraní por los gobiernos de Estados Unidos e Israel, con el fin de generar un daño en la planta nuclear cambiando la velocidad de las centrifugadoras que enrriquecian el uranio, acelerándolas y realentizándolas de manera paulatina hasta que esta colapsaron.

- Stuxnet penetró en la red

Según la firma de seguridad cibernética Symantec, Stuxnet probablemente llegó al programa nuclear de Natanz de Irán en una memoria USB infectada.

Alguien habría tenido que insertar físicamente el USB a una computadora conectada a la red. El gusano penetró así en el sistema informático de la planta.

- El gusano se propagó a través de las computadoras

Una vez dentro del sistema informático, Stuxnet buscó el software que controla las máquinas llamadas centrifugadoras.

Las centrífugas giran a altas velocidades para separar componentes. En la planta de Natanz, las centrifugadoras estaban separando los diferentes tipos de uranio, para aislar el uranio enriquecido que es fundamental tanto para la energía como para las armas nucleares.

- Stuxnet reprogramó las centrifugadoras

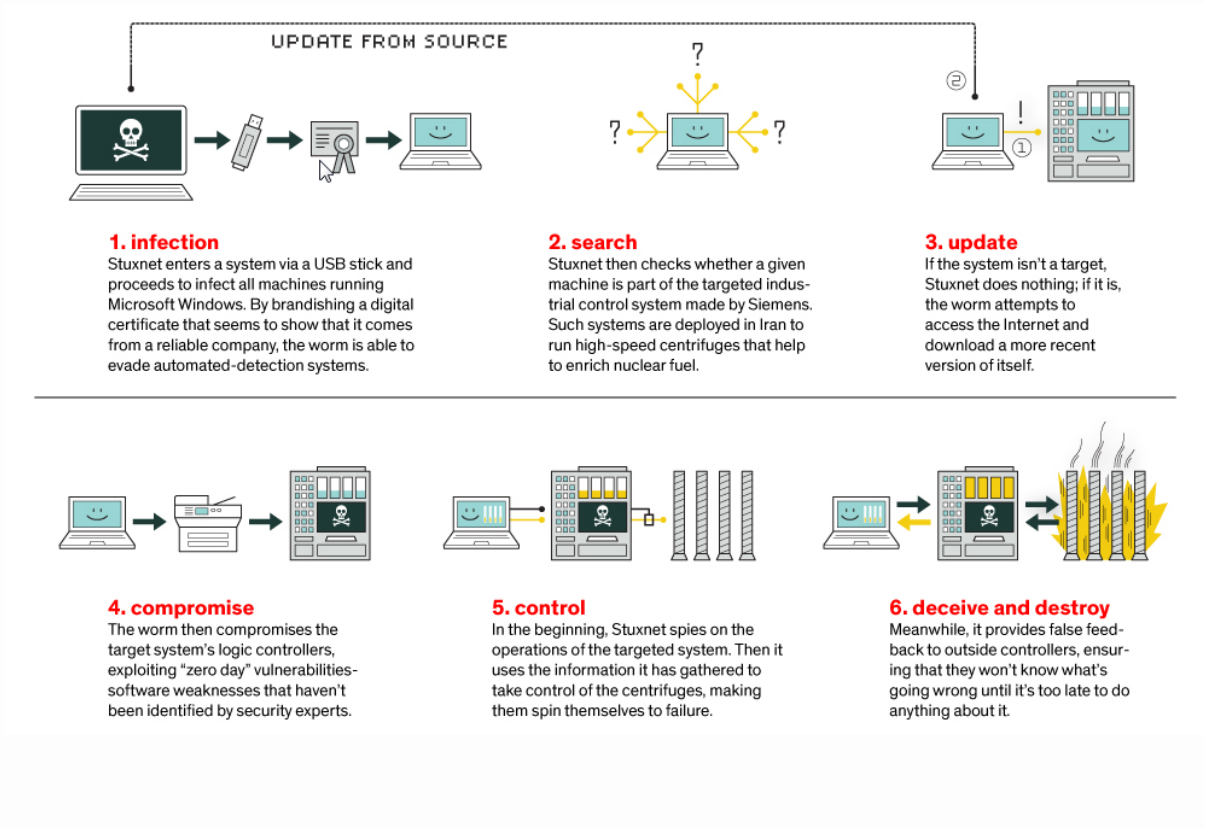
El gusano encontró el software que controla las centrifugadoras y se insertó en él, tomando el control de las máquinas.

Stuxnet llevó a cabo dos ataques diferentes. En primer lugar, hizo que las centrifugadoras giraran peligrosamente rápido, durante unos 15 minutos, antes de volver a la velocidad normal. Luego, aproximadamente un mes después, desaceleró las centrifugadoras durante unos 50 minutos. Esto se repitió en distintas ocasiones durante varios meses.

- Destrucción de las máquinas

Con el tiempo, la tensión provocada por las velocidades excesivas causó que las máquinas infectadas, unas 1000, se desintegraran.

Durante el ataque cibernético, alrededor del 20 por ciento de las centrifugadoras en la planta de Natanz quedaron fuera de servicio



Operación Aurora:

APT descubierta a finales de 2009 pero se cree que esta se ha estado desarrollando y evolucionando desde el año 2006, afectó empresas como Google, Adobe, Yahoo, Symantec, Juniper Systems, Rackspace, entre otros, todas referencias de investigación coinciden con que su origen es chino. Con respecto a sus objetivos existen varias hipótesis. Sin embargo, hay dos de ellas que coinciden en las referencias consultadas, por un lado, que el ataque fue motivado con el ánimo de robar propiedad intelectual a grandes compañías; y por el otro, que su objetivo principal fue la intención de robar cuentas de Gmail de activistas de derechos humanos en China. Para este ataque se utilizó principalmente un ataque de día cero para Internet Explorer en su versión 6.0 mediante Java Scripts que redirigían a un sitio web con software malicioso que se descargaba automáticamente, y una vez puesto en memoria extraía información sensible de las máquinas infectadas. Las contramedidas tomadas para esta APT fue instalar los parches lanzados pocos días después de la detección, además de implementar controles como agentes de antivirus basados en firmas, filtros de correos y IDS/IPS, no obstante, esta APT logró generar gran controversia en muchas de las empresas involucradas, así como impactos en su imagen, dentro de las empresas afectadas por esta APT se encontraban Google, Symantec, Yahoo, Adobe, Juniper y RackSpace .

GhostNet:

Esta es una APT que tuvo como objetivo espiar los colaboradores de Dalai Lama en medio del conflicto entre China y el Tibet, específicamente un ataque generado desde la República Popular de China hacia los sistemas informáticos pertenecientes a embajadas, ministerios de asuntos exteriores y otras oficinas gubernamentales, y los centros de exiliados tibetanos del Dalai Lama en India, Londres y la ciudad de Nueva York se vieron comprometidos esto asociado al conflicto entre China y el Tibet .Esta APT se logró mediante técnicas de phishing dirigido conocido como spear phishing y muy usada en la actualidad, los correos electrónicos se envían a organizaciones específicas que contienen información relevante al contexto que manejaban estas organizaciones. Estos correos electrónicos contenían archivos adjuntos maliciosos, que cuando se abrían, insertan un troyano en el sistema. Este troyano se conectaba de nuevo a un servidor de comando y control, generalmente ubicado en China, para recibir comandos. El computador infectado ejecutaba comandos especificados por el servidor de comando y control. En ocasiones, el comando especificado por el servidor de control hacia que el computador infectado descarga e instala un troyano conocido como Gh0st Rat que permitia a los atacantes obtener un control completo y en tiempo real de los computadores con Microsoft Windows . Los investigadores declararon que no podían concluir que el gobierno chino era responsable de la red de espionaje. Sin embargo, un informe de investigadores de la Universidad de Cambridge menciona que el gobierno chino puede estar detrás de las intrusiones que analizaron en la Oficina del Dalai Lama.

MACHETE:

Dentro de los eventos de APT más recientes en Latinoamérica se encuentra la APT Machete y la APT38, bautizada con este identificador por una de las empresas más

importantes de investigación en el mundo, FireEye. Machete fue una APT que dejó más 778 víctimas en Latinoamérica. Su objetivo principal era el ciberespionaje y sus primeras apariciones fueron en 2010 con mejoras en 2012, la empresa Kaspersky Labs asegura que los creadores de Machete son de América Latina, pero no es posible determinar exactamente el país de procedencia. Su interés en los documentos diplomáticos generó que hasta una embajada en Rusia sea destino de la maliciosa operación. Los países mas afectados por esta APT fueron Venezuela con un 42%, Ecuador con un 36% y Colombia con un 11% .Machete fue distribuida a través de phishing que contenían malware capaz de realizar diversas funciones:

- Registro de pulsaciones de teclas
- Captura de audio desde el micrófono de la computadora
- Captura de capturas de pantalla
- Captura de datos de geolocalización
- Tomar fotografías desde la cámara web de la computadora
- Copiar archivos a un servidor remoto
- Copiar archivos a un dispositivo USB especial si está insertado

APT38:

A finales de 2018 se presentó un conocido incidente perpetrado a la banca chilena, este incidente fue bautizado por FireEye Inc. como APT38, el cual intentó robar al menos USD $1.100 millones en todo el mundo, esta conocida APT a logrado robar un estimado de USD $100 millones, con un estimado del 10% únicamente en en el Banco de Chile , a este país se suman países en Latinoamérica como el Banco del Austro en Ecuador y otros bancos en Brazil, Paraguay y México. Esta APT presuntamente se orquestó desde Korea del Norte y aún se desconoce si este grupo forma parte del conocido grupo Lazarus a quien presuntamente se le atribuyeron los ataques a la empresa Sony en 2014.De lo que se tiene certeza es que este grupo es uno de los mejores ejemplos de la ejecución del ataque en el momento adecuado mediante herramientas de evasión, escalamiento de privilegios, fuerza bruta y herramientas de password cracking, esperando en algunos casos meses y hasta años de reconocimiento y vigilancia antes de dar el golpe final.

Sectores objetivo: instituciones financieras en todo el mundo

Malware asociado: este grupo grande y prolífico utiliza una variedad de familias de malware personalizadas:

- un back doors llamado QUICKRIDE, para comunicarse con el servidor C2 a través de HTTP y HTTPS
- utilizó un troyano llamado KEYLIME para recopilar datos del portapapeles,
- Tunelizadores de línea de comandos, NACHOCHEESE, para darles acceso al shell a la máquina de la víctima.
- Implementation una función para la eliminación segura y personalizada para hacer que los archivos eliminados sean irrecuperables
- Se utilizó el ransomware Hermes para cifrar archivos con AES256.
- Para la manipulación de datos en tiempo de ejecución utilizaron DYEPACK.FOX para manipular datos PDF a medida que se accede a ellos para eliminar rastros de transacciones SWIFT fraudulentas de los datos que se muestran al usuario final.
- Para la manipulación de datos transmitidos utilizado DYEPACK para manipular mensajes SWIFT en ruta a una impresora.
- Para la manipulación de datos almacenados ha utilizado DYEPACK para crear, eliminar y modificar registros en bases de datos utilizadas para transacciones SWIFT
- Limpiaron el disco con BOOTWRECK,
- También se uso un backdoor llamado NESTEGG, que tiene la capacidad de descargar y cargar archivos desde y hacia la máquina de la víctima.
- Modificaron registros usando una herramienta llamada CLEANTOAD que tiene la capacidad de modificar las claves del Registro.
- Para descubrir las conexiones de red del sistema se instaló una herramienta de monitoreo de puertos, MAPMAKER, para imprimir las conexiones TCP activas en el sistema local.

Bibliografia:

- https://www.cynet.com/network-attacks/advanced-persistent-threat-apt-attacks/
- https://www.paubox.com/blog/advanced-persistent-threat-apt/
- https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/
- Algunos casos mas : https://www.fireeye.com/current-threats/apt-groups.html
- https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/
- https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/advanced_persistent_threat_incident_handling_handbook
- https://www.swisscyberforum.com/blog/guide-of-advanced-persistent-threat-apt/
- https://searchdatacenter.techtarget.com/es/definicion/Amenaza-persistente-avanzada-o-APT
- https://www.magazcitum.com.mx/?p=1547
- https://www.muyseguridad.net/2014/08/23/apt-machete-latinoamerica/
- https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2010/Aurora_HBGARY_DRAFT.pdf
- https://www.welivesecurity.com/la-es/2010/01/21/que-es-operacion-aurora/
- https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf