sedian

Seguridad Digital
de Andalucía

Gestión de amenazas avanzadas persistentes (APT-Advanced Persistent Threats)

Junta de Andalucía

Consejería de Economía, Conocimiento,
Empresas y Universidad

Índice

¿Qué es una APT?

Las APT (Advanced Persistent Threat o Amenazas Avanzadas Persistentes) son ciberataques muy complejos y avanzados que buscan mantenerse dentro de la organización víctima.

Se definen como el conjunto de ataques y técnicas llevadas a cabo por un mismo grupo financiado a través de un tercero.

¿Qué tipo de organizaciones crees que financian a estos grupos?

¿De qué país principalmente provienen este tipo de ataques?

Principales diferencias entre APT y malware

	APT	Malware
Ejecución	Es una combinación de varios ciberataques complejos que se componen de capacidad logística y operativa avanzada para campañas de intrusión a largo plazo.	La mayoría de los ataques de malware son ataques rápidos, con objetivos específicos, donde un atacante crea software malicioso que se instala en el sistema de la víctima.
Detección	Las APTs pueden ser indetectables por un largo período de tiempo.	Los malwares pueden ser detectados y erradicados por antivirus.
Protección	Se requiere un sistema de seguridad robusto para detectar, analizar y erradicar las APT	Es necesario protección del entorno llevando una serie de medidas sistemáticas.

¿Quién está detrás de estas amenazas?

- Grupos cibercriminales organizados
- Gobiernos
- Grandes corporaciones
- Hacktivistas

Objetivos de una APT

Las APTs tienen como objetivo principal aquellas infraestructuras que son críticas o que poseen información sensible (proyectos, código, armamentos, etc.).

A su vez, existen APTs cuyos objetivos son puramente políticos, dirigidos por activistas que realizan sus labores en contra de un gobierno. Por tanto, podemos establecer una similitud entre los objetivos y las **motivaciones**.

- **Económica:** Es la principal motivación
- **Políticas** (Patrocinado por estados o ataques entre estados)
- **Ideológico** (Hacktivismo)

Algunos grupos famosos:

- **APT37:** Corea del Norte
- **APT34, APT33:** Irán
- **APT32 (Ocean Lotus):** Vietnam
- **APT28 (Fancy Bear):** Rusia
- **FamousSparrow:** Desconocido
- ¿España?

Grupo Cibercriminal - APT28

- **Origen**: Rusia
- **Objetivo**: Políticos
- **Escenarios**: Aeroespacial, defensa, energía, administraciones públicas y medios de comunicación
- **Tipo**: Organización cibercriminal
- **Otros nombres**: Fancy Bear, Pawn Storm, Sofacy Group, Sednit, Strontium o Tsar Team
- **Status**: Activo desde 2007

Grupo Cibercriminal - APT33

- **Origen**: Irán
- **Objetivo**: Políticos
- **Escenarios**: dirigido a organizaciones de múltiples industrias en los Estados Unidos, Arabia Saudita y Corea del Sur, con un interés particular en los sectores de la aviación y la energía
- **Tipo**: Organización Cibercriminal
- **Status**: Activo desde 2013

Grupo Cibercriminal - APT34

- **Origen**: Iraní
- **Objetivo**: Gobiernos Extranjeros
- **Tipo**: Organización Cibercriminal
- **Año de identificación**: 2014.
- **Otros nombres**: OilRig, Helix Kitten, Crambus, ATK 40...
- **Status**: Activo

Grupo Cibercriminal - APT37

- **Origen**: Corea del Norte
- **Objetivo**: Países de Medio Oriente, Productos Químicos, Electrónica, ISP's, Sector Financiero…
- **Tipo**: Organización Cibercriminal.
- **Año de identificación**: 2012
- **Otros nombres**: Reaper, DOGCALL, POORAIM, MILKDROP…
- **Status**: Activo hasta 2020

Grupo Cibercriminal - FamousSparrow

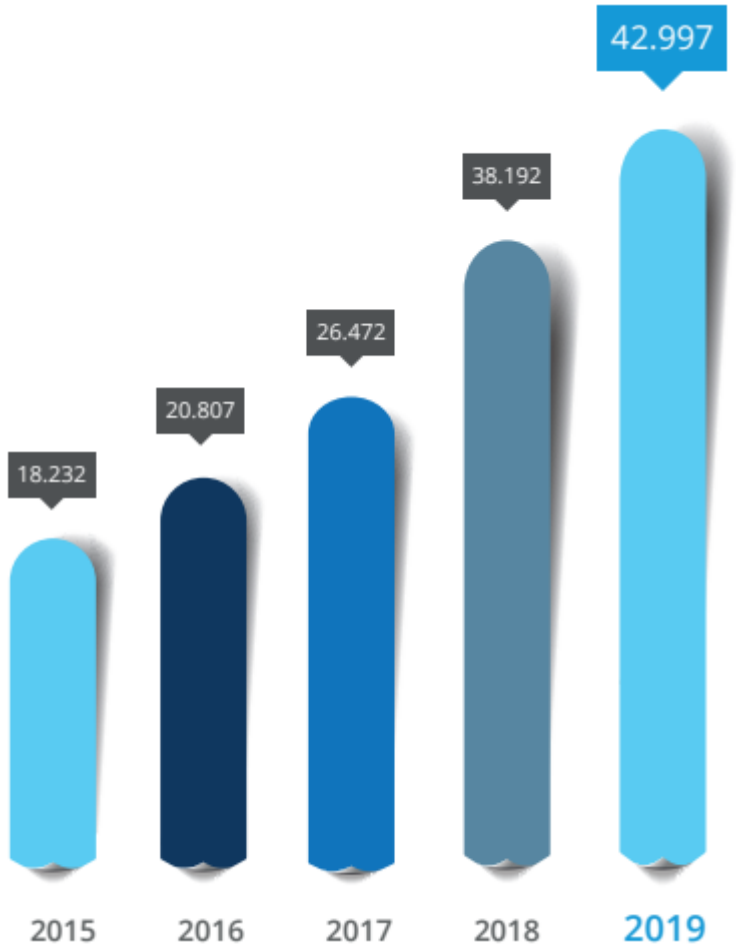
- **Origen**: Desconocido
- **Objetivo**: Países, Ciberespionaje o espionaje cibernético, Hoteles...
- **Tipo**: Organización Cibercriminal
- **Año de identificación**: 2019
- **Otros nombres**: N/A
- **Status**: Activo

¿En España…?

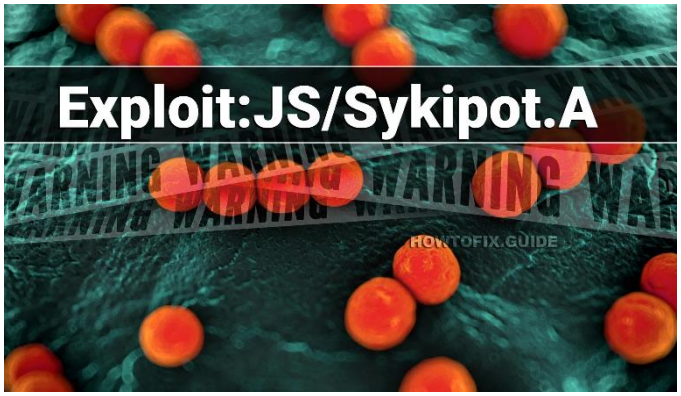
¿Crees que en España existen APTs?

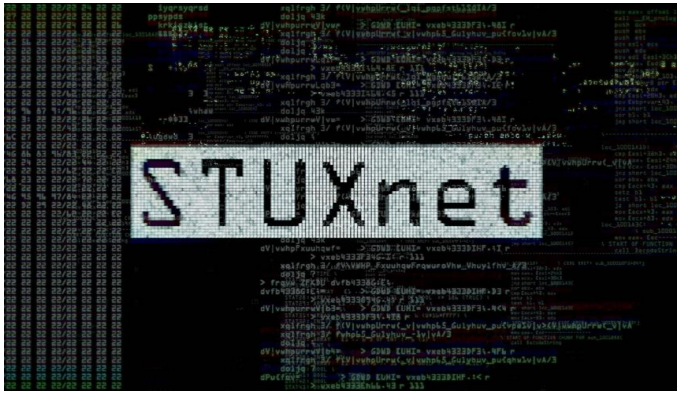
Panorama general

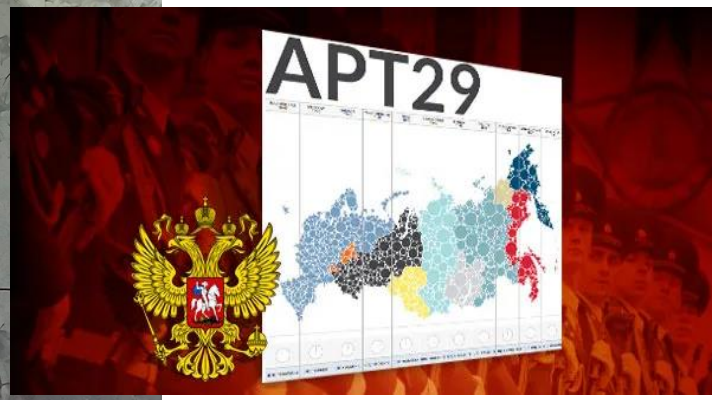
En 2019, el CCN-CERT gestionó 42.997 ciberincidentes (más de un 11 % con respecto al año 2018), de los cuales casi un 7,5 % fueron de **peligrosidad muy alta o crítica**.



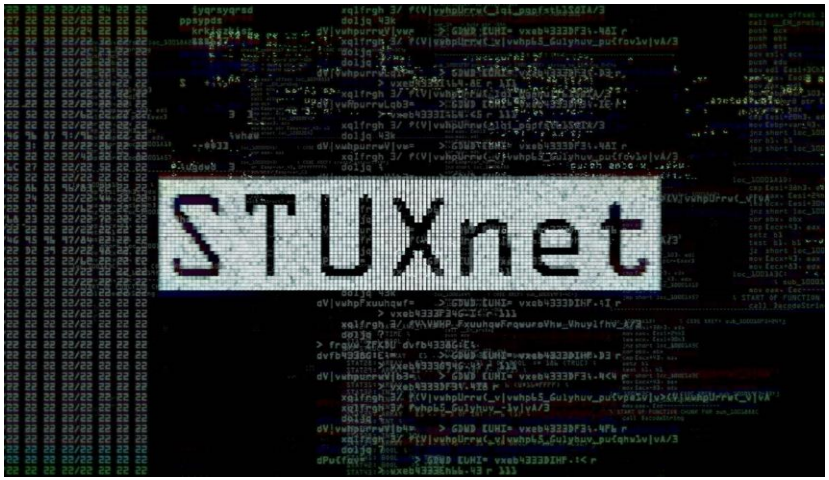
Algunos ejemplos de APT







Caso STUXnet



- **Origen**: Desconocido
- **Objetivo**: Infraestructuras críticas y Sistemas SCADA
- **Tipo Malware**: Gusano
- **Año de identificación**: 2010
- **Status**: Inactivo

Caso STUXnet

Tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse.

Fue la primera vez que un ataque cibernético logró dañar la infraestructura del "mundo real".

El código altamente avanzado de Stuxnet había sido diseñado con una mentalidad bélica.

Caso CARBANAK

- **Origen**: Desconocido
- **Objetivo**: Sistemas y Cajeros Bancarios
- **Tipo Malware**: Troyano
- **Año de identificación**: 2014
- **Consecuencias**: Robo de más de 1.000M de Dólares
- **Status**: Inactivo

Caso CARBANAK

Dirigida (pero no limitada) a las instituciones financieras. Los delincuentes pudieron manipular su acceso a las respectivas redes bancarias para robar el dinero de diversas maneras.

En algunos casos, se instruyó a los cajeros automáticos para que despacharan el dinero sin tener que interactuar localmente con la terminal.

Las mulas recogían el dinero y lo transferían a través de la red SWIFT a las cuentas de los criminales.

El grupo Carbanak llegó a alterar las bases de datos y aumentar los saldos de las cuentas existentes y se embolsó la diferencia sin que el usuario lo supiera, cuyo saldo original sigue intacto.

Caso SYKIPOT

- **Origen**: Desconocido
- **Objetivo**: Información confidencial, propiedad intelectual, patentes...
- Tipo malware: varios (Troyano, Exploit, Rootkit...)
- **Año de identificación**: 2007
- **Consecuencias**: Robo de información sensible de aerolíneas civiles de EEUU
- **Status**: Inactivo

Caso SYKIPOT

Sykipot es un malware que se ha utilizado en campañas de phishing desde aproximadamente 2007, principalmente contra víctimas de los EE. UU.

Una variante de Sykipot secuestra las tarjetas inteligentes de las víctimas.

Actores más activos

Según el informe de ciberamenazas y tendencias de CCN-CERT, en su edición del 2020, los actores más activos durante el año 2019 han sido los siguientes:

Grupo Snake: uno de los grupos más activos en los últimos años, centrado principalmente en el Sector Público y en empresas del sector defensa.

Grupo APT27/Emissary Panda: grupo muy activo contra empresas tecnológicas y del sector aeroespacial, su principal objetivo es el robo de propiedad intelectual.

Grupo APT28/Sofacy: grupo muy activo contra el Sector Público y sector defensa, con numerosos intentos de intrusión a través de campañas de spear-phishing.

¿Qué es MITRE ATT&CK?

MITRE ATT & CK es una base de conocimiento accesible a nivel mundial de tácticas y técnicas adversas, basadas en observaciones a las amenazas de la seguridad cibernética.

Se muestran en matrices organizadas por etapas de ataque, desde el acceso inicial al sistema hasta el robo de datos o el control de la máquina. Existen matrices para plataformas de escritorio comunes (Linux, macOS y Windows), así como para plataformas móviles.

ATT & CK significa tácticas, técnicas y conocimiento común contradictorios.

https://attack.mitre.org/groups/

GRUPOS

Grupos

Los grupos son conjuntos de actividad de intrusión relacionada que se rastrean con un nombre común en la comunidad de seguridad. Los analistas rastrean grupos de actividades utilizando diversas metodologías analíticas y términos como grupos de amenazas, grupos de actividades, actores de amenazas, conjuntos de intrusiones y campañas. Algunos grupos tienen varios nombres asociados con actividades similares debido a que varias organizaciones realizan un seguimiento de actividades similares con nombres diferentes. Las definiciones de grupo de las organizaciones pueden superponerse parcialmente con los grupos designados por otras organizaciones y pueden estar en desacuerdo sobre una actividad específica.

Para los propósitos de las páginas del Grupo, el equipo de MITRE ATT & CK usa el término Grupo para referirse a cualquiera de las designaciones anteriores para un grupo de actividad del adversario. El equipo hace un mayor esfuerzo para rastrear las superposiciones entre los nombres según las asociaciones informadas públicamente, que se designan como "Grupos asociados" en cada página (anteriormente denominados "Alias"), porque creemos que estas superposiciones son útiles para la conciencia de los analistas. No representamos estos nombres como superposiciones exactas y alentamos a los analistas a realizar investigaciones adicionales.

Los grupos se asignan al uso de la técnica informado públicamente y se incluyen referencias originales. La información proporcionada no representa todo el posible uso de técnicas por los Grupos, sino más bien un subconjunto que está disponible únicamente a través de informes de código abierto. Los grupos también se asignan al Software informado utilizado, y el uso de la técnica para ese Software se rastrea por separado en cada página de Software.

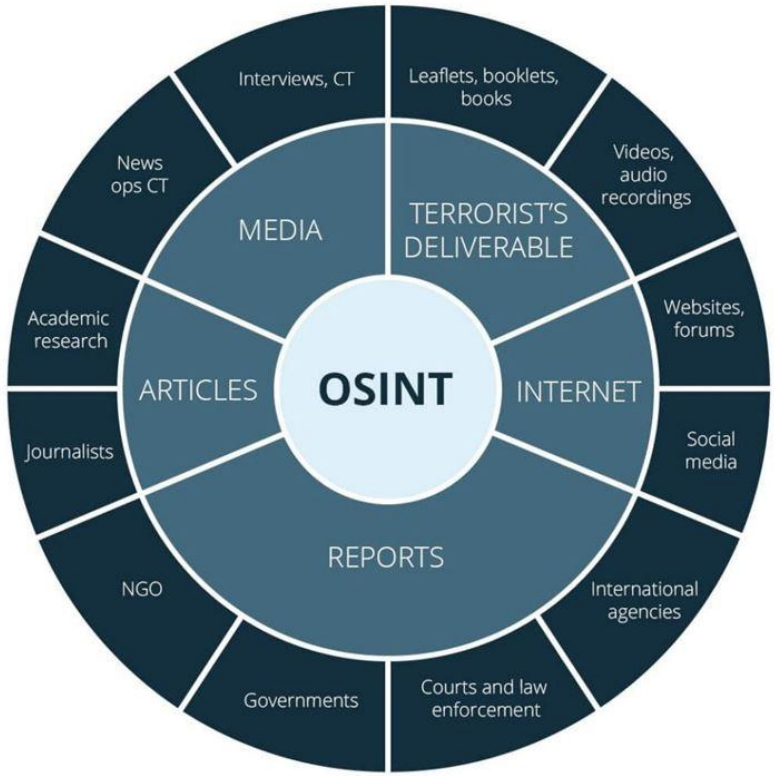
Grupos: 129

IDENTIFICACIÓN	Nombre	Grupos asociados	Descripción
G0018	admin @ 338		admin @ 338 es un grupo de amenazas cibernéticas con sede en China. Anteriormente, ha utilizado eventos de interés periodístico como señuelos para distribuir malware y se ha dirigido principalmente a organizaciones involucradas en políticas financieras, económicas y comerciales, generalmente utilizando RAT disponibles públicamente como PoisonIvy , así como algunas puertas traseras no públicas.
G0130	Equipo de seguridad de Ajax	Operación Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operación Saffron Rose	Ajax Security Team es un grupo que ha estado activo desde al menos 2010 y se cree que opera desde Irán. En 2014 , el equipo de seguridad de Ajax pasó de las operaciones de desfiguración de sitios web a campañas de ciberespionaje basadas en malware dirigidas a la base industrial de defensa de EE. UU. Y a los usuarios iraníes de tecnologías anti-censura.
G0138	Andariel	Chollima silencioso	Andariel es un grupo de amenazas patrocinado por el estado de Corea del Norte que ha estado activo desde al menos 2009. Andariel se ha centrado principalmente en sus operaciones, que han incluido ataques

Fases de una APT

1. Selección e investigación del objetivo
2. Penetración en la organización
3. Generar persistencia
4. Ejecución de acciones
5. Eliminación de rastro y ataque continuo

1. Selección e investigación del objetivo



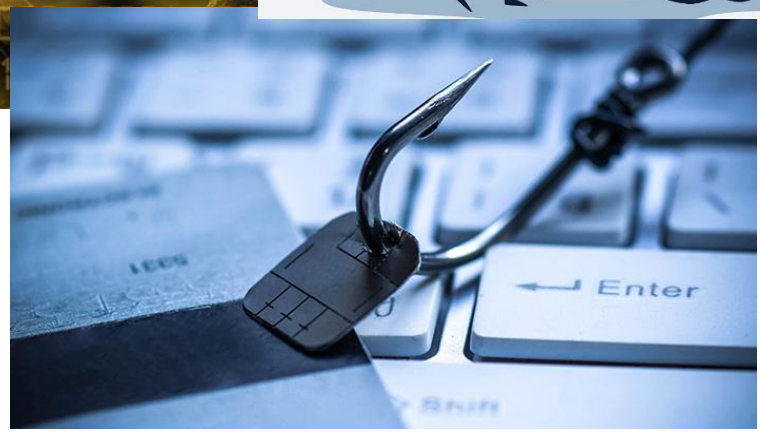
1. Selección e investigación del objetivo

1. Identificar los principales responsables de la organización, en el ámbito de TI.

2. Investigar profesional y personalmente a cada uno de los miembros.

3. Localizar información relevante (nombres de usuario, contraseñas, sitios habituales, hijos, mujer...)

2. Penetración en la organización



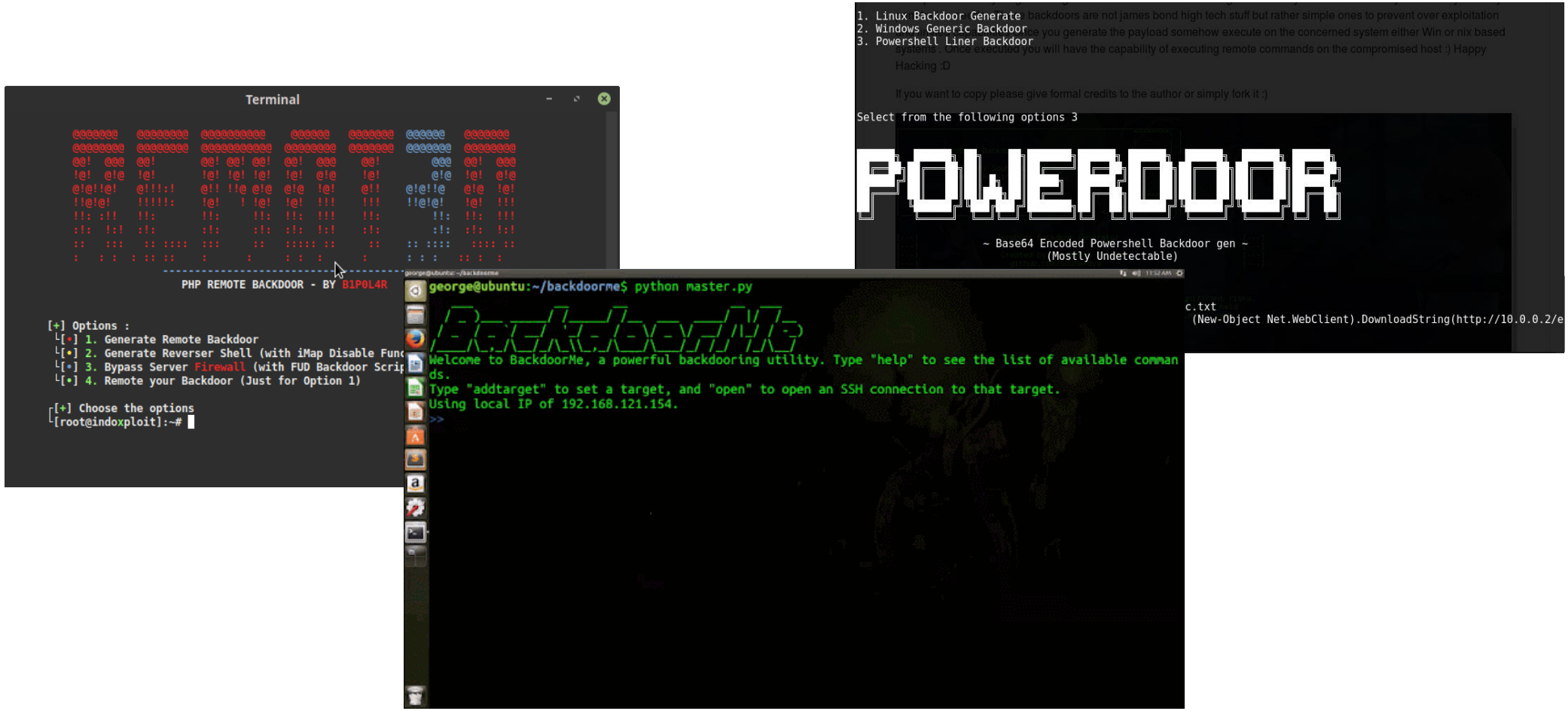
2. Penetración en la organización

1. Intrusión bajo cualquier concepto.

2. Infección por malware, campañas de phishing dirigidas y explotación de vulnerabilidades.

3. Incluso en ocasiones se llega a **extorsionar** al personal de la organización víctima.

3. Generar persistencia



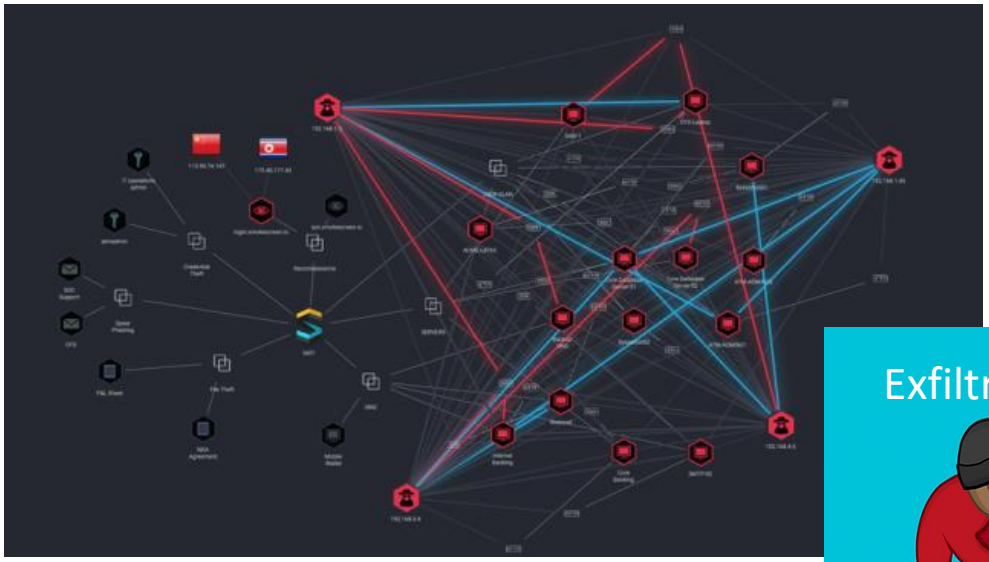
3. Generar persistencia

1. Generar métodos para continuar la intrusión.
2. Obtención de nuevas credenciales, mediante métodos tipo mimikatz.
3. Creación de Backdoors.
4. Conexión con el C&C.

4. Ejecución de Acciones

Selección de Información

Movimiento Lateral

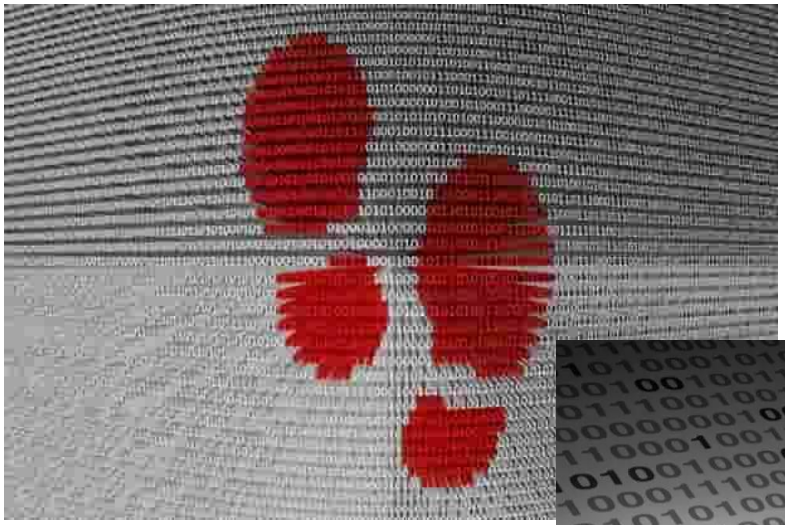


Exfiltración de datos

4. Ejecución de Acciones

1. Movimientos laterales.
2. Acceso a nuevas credenciales y ataques al directorio activo.
3. Escaladas de privilegios en otras partes de la red.
4. Selección y exfiltración de información.
5. Despliegue de Ransomwares.

5. Eliminación de rastro y ataque continuo

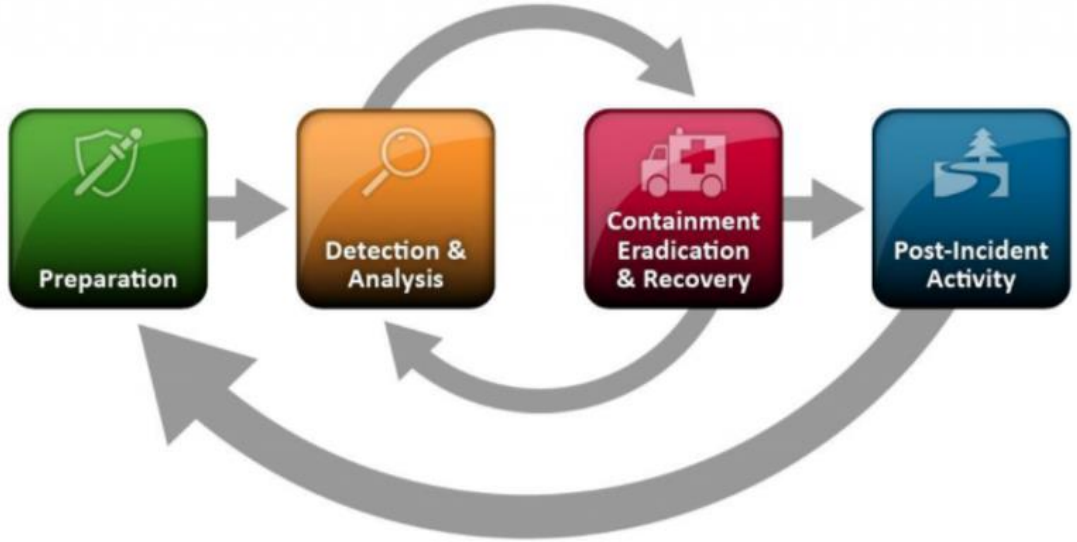


5. Eliminación de rastro y ataque continuo

1. Eliminar Logs.
2. Desviar la atención con otros malwares.
3. Borrar servidores.
4. Causar fallos en servicios críticos.
5. Desinstalar el Malware original.

¿Cómo detectar una APT?

Monitorización Activa



Threat Hunting

¿Qué tipo de acciones se deben hacer de forma preventiva?

¿Cómo controlarían las conexiones para saber si hay backdoors instaladas en la red?

¿Cómo prevenir una APT?

COPIAS DE SEGURIDAD

Realiza copias de seguridad periódicas

BORRADO

Haz un borrado seguro de la información una vez que está ya no sea necesaria.

ENLACES Y DESCARGAS

No abras ningún enlace ni fichero adjunto procedente de un coreo electrónico que presente cualquier indicio o patrón fuera de lo habitual.

ACTUALIZACIONES

Mantén actualizadas las aplicaciones y el sistema operativo.

CIBERSEGURIDAD

La cultura de la ciberseguridad y la concicenciación del empleado deber ser objetivos prioritarios para las organizaciones.

CIFRADO

Cifra la información sensible, no hay otra alternativa.

CONTRASEÑAS

Utiliza contraseñas adaptadas a la funcionalidad y utiliza la doble autenticación.

PRECAUCIÓN

Limita la superficie de exposición a las amenazas.

SOFTWARE DE SEGURIDAD

Utiliza software de seguridad, herramientas antivirus y antimalware, cortafuegos personales, herramientas de borrado seguro, etc.

sedian Seguridad Digital de Andalucía

¿Cómo prevenir una APT?

- Identificación de activos críticos
- **Implementar soluciones como CARMEN del CCN-CERT(*)**
- Filtrar emails, monitorización del tráfico y control de acceso
- Segmentar la red
- Implementar modelo de seguridad de red basado en un proceso estricto de verificación de identidad, *Zero Trust*
- Formar y concienciar a los empleados
- Realizar tests de intrusión (*Pentest*) recurrentes
- Regla 1-10-60: una intrusión debería detectarse en 1 minuto, investigarse en 10 minutos, contenerla y solucionarla en 60 minutos

¿Cómo prevenir una APT?

(*) Carmen es una solución desarrollada con el objetivo de identificar el compromiso de la red de una organización por parte de amenazas persistentes avanzadas (APT).

En este sentido, constituye la primera capacidad española, basada en conocimiento y tecnología nacionales.

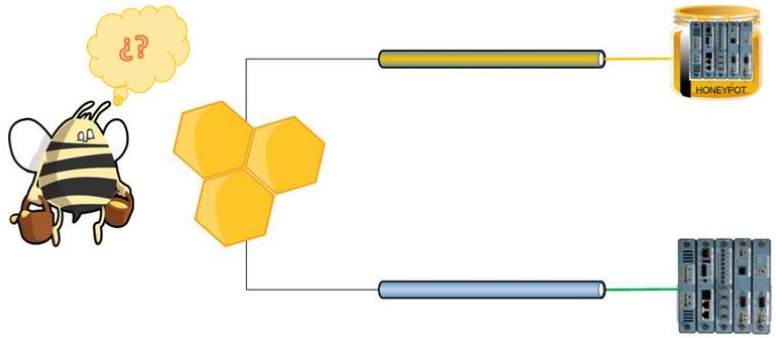
Aporta capacidades para la detección de la amenaza en la etapa de persistencia, por lo que uno de sus objetivos fundamentales es la identificación de movimientos externos, como exfiltraciones o comunicaciones con servidores de mando y control, así como el reconocimiento de movimientos laterales de mantenimiento de persistencia o de robo de información en la red corporativa.

¿Cómo protegerse de una APT?

Firewalls

IDS/IPS

Antimalwares



HoneyNet

¿Cómo protegerse de una APT?

Herramientas de detección

1. **Snort**: Un sistema de prevención y detección de intrusiones basado en red de fuente abierta (IDS / IPS) que emplea firmas y protocolos, así como inspección basada en anomalías.

2. **OSSEC**: Un IDS de código abierto basado en el host, a diferencia de Snort. Su motor de correlación y análisis proporciona análisis de registro, comprobación de integridad de archivos, supervisión de registro de Windows, detección de rootkits, alertas basadas en tiempo, así como respuesta activa, además puede admitir la mayoría de los sistemas operativos.

¿Cómo protegerse de una APT?

Herramientas de detección

1. **Splunk**: Una herramienta de búsqueda, monitorización e informes que integra registros y otros datos de aplicaciones, servidores y dispositivos de red. El repositorio de datos está indexado y puede consultarse para crear gráficos, informes y alertas.

2. **Sguil**: Incluye una GUI intuitiva que proporciona acceso a eventos en tiempo real, datos de sesión y capturas de paquetes sin formato. Sguil facilita la práctica de la supervisión de la seguridad de la red y el análisis impulsado por eventos.

3. **Squert**: Una aplicación web utilizada para consultar y visualizar datos de eventos almacenados en una base de datos Sguil. Mediante el uso de metadatos, representaciones de series temporales, conjuntos de resultados ponderados y agrupados lógicamente, proporciona un contexto adicional a los eventos.

¿Cómo protegerse de una APT?

Indicadores de compromiso (IOC)

1. Tráfico de red saliente inusual.
2. Acceso a IPs/Dominios en blacklist.
3. Conexiones inusuales en equipos internos.
4. Actividad geográfica en inicios de sesión inusuales o patrones de acceso.
5. Señales de envenenamiento de caché ARP, suplantación de ARP y otros ataques de MITM.
6. Anomalías en la actividad de la cuenta de usuario privilegiado o cambios de permisos.
7. Cambios en las configuraciones de Firewall y cuentas de usuario locales.
8. Cambios en los servidores DNS.

¿Cómo actuar ante una APT?

Identificar y Erradicar el origen de la amenaza

Acciones Post-Incidente – Análisis forense

¿Cómo actuar ante una APT?

Identificar y Erradicar el origen de la amenaza:

- Vigilancia constante mediante herramientas automatizadas de monitorización en tiempo real
- Buscar comportamientos anómalos en la infraestructura TIC

Acciones Post-Incidente. Análisis forense:

- Borrado de huellas e historial
- Reparación de sistemas y equipos
- Recuperación de datos

Referencias

1. https://www.ccn-cert.cni.es/soluciones-seguridad/carmen.html

2. https://attack.mitre.org/

3. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html
4. https://www.andaluciaesdigital.es/documents/410971/1437699/Amenazas+avanzadas+persistentes/a314ff20-2c70-40f7-b1f1-36871373112e

Referencias imágenes

1. https://howtofix.guide/exploit-js-sykipot-a/
2. https://www.kaspersky.es/blog/carbanak-source-code-leaked/18334/
3. https://www.ciberseguridadlatam.com/2021/01/08/ciberdelincuentes-norcoreanos-lanzan-el-troyano-rokrat-en-campanas-contra-corea-del-sur/
4. https://www.a2secure.com/blog/descubriendo-las-amenazas-persistentes-avanzadas-apt/
5. https://pixabay.com/es/

sedian Seguridad Digital de Andalucía