

Busca una noticia o artículo real sobre cada uno de los siguientes tipos de malware:virus, gusano, troyano, ransomware, spyware o adware.

Malware

Actividad 2

Cristóbal Suárez Abad
Seguridad y Alta disponibilidad – 2º ASIR

Actividad 2 - Malware

Requisitos de finalización

Busca una noticia o artículo real sobre cada uno de los siguientes tipos de malware:
virus, gusano, troyano, ransomware, spyware o adware.

En un breve texto indica:

1. **Tipo de malware y fuente** (título, medio y enlace).
2. **Qué ocurrió** (resumen de la noticia).
3. **Modo de infección** (cómo se propagó).
4. **Síntomas o consecuencias** (qué efectos tuvo).
5. **Medidas tomadas o recomendadas.**

Virus:

1. Tipo de malware y fuente (título, medio y enlace).

Virus “I love you”.

Medio: Cadena SER.

Enlace: <https://cadenaser.com/nacional/2025/05/03/se-cumplen-25-anos-del-virus-informatico-i-love-you-que-infecto-a-45-millones-de-ordenadores-en-el-2000-cadena-ser/>

2. Qué ocurrió (resumen de la noticia).

Se infectaron 45 millones de ordenadores, el 10% de los equipos que en aquellos momentos estaban conectados a la red. Provocando unos 5.000 millones de dólares de pérdida en todo el mundo (unos 9.500 millones de dólares actuales).

3. Modo de infección (cómo se propagó).

Usando la agenda de Outlook de la víctima se propagaba a sus contactos haciéndose pasar por esta. En el email adjuntaba un documento llamado “I love you” en el cual estaba el virus.

4. Síntomas o consecuencias (qué efectos tuvo).

Los síntomas son que destruía los archivos que hubiese en el ordenador, dejándolo inservible.

5. Medidas tomadas o recomendadas.

Se recomendó a los usuarios no abrir y borrar inmediatamente cualquier correo que tuviese el asunto “I love you” o un archivo adjunto del mismo nombre, incluso si venia por parte de un conocido.

Gusano:

1. Tipo de malware y fuente (título, medio y enlace).

Tipo: Gusano “Shai-Hulud”.

Medio: Unaaldia y Unit42

Enlace: <https://unaaldia.hispasec.com/2025/09/gusano-shai-hulud-compromete-cientos-de-paquetes-npm-y-roba-credenciales.html>

<https://unit42.paloaltonetworks.com/npm-supply-chain-attack/>

2. Qué ocurrió (resumen de la noticia).

El 15 de septiembre algunos analistas descubrieron versiones comprometidas de un NPM muy popular (“@ctrl/tinycolor”) y en horas posteriores se comprobó que otros paquetes de diferentes mantenedores también habían sido infectados, incrementando el número en cientos de paquetes.

3. Modo de infección (cómo se propagó).

Cuando infecta el entorno de un mantenedor de NPM, el malware obtiene un token válido de NPM y comienza un proceso de automatización con el que crea nuevas versiones de todos los paquetes que el mantenedor controla.

4. Síntomas o consecuencias (qué efectos tuvo).

Robo de credenciales de los desarrolladores. Se les pregunta a los desarrolladores que actualicen su sistema de autenticación multifactorial (MFA) y es entonces cuando se consigue acceso a las credenciales.

El gusano crea un repositorio público en la cuenta GitHub de la víctima donde expone las credenciales. Después identifica otros paquetes que mantiene el desarrollador e inyecta código malicioso en ellos de manera automática.

5. Medidas tomadas o recomendadas.

<https://unit42.paloaltonetworks.com/npm-supply-chain-attack/>

- Renovación inmediata de todas las credenciales de desarrollador (tokens, claves SSH, etc). Se debe asumir que todas las claves que haya en la máquina del desarrollador están comprometidas.
- Se debe llevar a cabo la auditoría de todas las dependencias: usa herramientas como “npm audit”. Se deben eliminar o actualizar cualquier paquete comprometido.

- Revisar la cuenta de GitHub: repositorios extraños, commits o modificaciones sospechosas.
- Imponer (si no había) la MFA en todas las herramientas y cuentas del desarrollador.

Troyano.

1. Tipo de malware y fuente (título, medio y enlace).

Tipo: Troyano “Astaroth”.

Medio: Cybereason.

Enlace: <https://www.cybereason.com/blog/research/information-stealing-malware-targeting-brazil-full-research>

2. Qué ocurrió (resumen de la noticia).

En una campaña masiva de spam dirigida a Brasil y parte de Europa se encontró una nueva versión del Troyano Astaroth. Este hace uso de herramientas ya presentes en el equipo (“Living of the land”: LOLbins) para explotar procesos de seguridad y propagarse, haciendo más difícil su detección y aprovecha para robar credenciales y otros datos personales de sus víctimas.

3. Modo de infección (cómo se propagó).

La infección se inicia a través de un archivo comprimido que le llega a la víctima por correo o tras pinchar en un enlace. Este archivo contiene un archivo de acceso directo el cual inicia el malware una vez se ejecuta. Este inicia un comando ofuscado que usa una herramienta legítima de Windows, “wmic.exe” para lanzar un script el cual conectará el equipo con un dominio remoto desde donde conseguirá el script malicioso. Este software después se inyectará en otras herramientas legítimas de Windows para evitar su detección.

4. Síntomas o consecuencias (qué efectos tuvo).

Fueron robadas de manera masiva contraseñas y otros datos personales (Gmail, Outlook, etc) y financieros.

5. Medidas tomadas o recomendadas.

En algunos casos el cliente puro parar el ataque deshabilitando la herramienta WMIC, impidiendo la extracción de datos. Pero en general se recomienda evitar ejecutar software dudoso.

Ransomware.

1. Tipo de malware y fuente (título, medio y enlace).

Tipo: Ransomware “Akira”.

Medio: Itdigalsecurity.

Enlace: <https://www.itdigalsecurity.es/endpoint/2025/11/el-ransomware-akira-y-los-ataques-a-microsoft-365-se-consolidan-como-principales-amenazas>

2. Qué ocurrió (resumen de la noticia).

La empresa de ciberseguridad Barracuda alertó sobre algunas de las amenazas más importantes, entre ellas el ransomware Akira. Este ransomware aprovecha una vulnerabilidad que en teoría ya está parcheada, pero algunos usuarios pueden haber descuidado y no llevar a cabo la actualización.

3. Modo de infección (cómo se propagó).

Akira se aprovecha de la vulnerabilidad “CVE-2024-40766” del firewall de SonicWall. Esto permite a los atacantes explotar credenciales robadas para interceptar contraseña de un solo uso y generar tokens válidos de inicio de sesión. Esto les permite evitar la MFA.

4. Síntomas o consecuencias (qué efectos tuvo).

Una vez que se consigue acceso a los equipos se lleva a cabo un cifrado de los archivos. Se usan herramientas legítimas del sistema para evitar la detección y además se desactivan otras medidas de seguridad y copia de seguridad de datos, para evitar cualquier intento de recuperación.

5. Medidas tomadas o recomendadas.

Aplicar el parche de seguridad para la vulnerabilidad “CVE-2024-40766” y otras actualizaciones necesarias.

Spyware.

1. Tipo de malware y fuente (título, medio y enlace).

Tipo: Spyware “Dante” y “LeetAgent”.

Medio: Escudo Digital.

Enlace: <https://www.escudodigital.com/ciberseguridad/memento-labs-pone-en-circulacion-dante-un-nuevo-spyware.html>

2. Qué ocurrió (resumen de la noticia).

El equipo GReAT de Kaspersky descubrió la “Operación ForumTroll”, una APT (Amenaza Persistente Avanzada), la cuál explotaba la vulnerabilidad CVE-2025-2783 de Google Chrome. Para ello usaban los spyware LeetAgen y Dante.

3. Modo de infección (cómo se propagó).

Se enviaban correos electrónicos de phishing personalizados, como si fuesen invitaciones al foro Primakov Readings¹. El objetivo era infectar a medios de comunicación, organismos gubernamentales, entidades financieras, etc. Sobre todo, de Rusia y Bielorrusia.

4. Síntomas o consecuencias (qué efectos tuvo).

No se menciona mucho de los síntomas, entendiéndose que al ser un spyware se dedica a extraer información de la víctima.

5. Medidas tomadas o recomendadas.

No se detallan medidas específicas tomadas por las víctimas o recomendaciones de seguridad en el texto proporcionado. Se asume la recomendación estándar de aplicar los parches de seguridad para la vulnerabilidad Chrome (y cualquier otro software) y también mantenerse alerta contra el phishing.

¹ https://en.wikipedia.org/wiki/Primakov_Readings

Adware.

1. Tipo de malware y fuente (título, medio y enlace).

Tipo: Adware “Superfish”.

Fuente: Kaspersky.

Enlace: <https://www.kaspersky.es/blog/superfish-adware-preinstalado-en-los-portatiles-de-lenovo/5437/>

2. Qué ocurrió (resumen de la noticia).

Se descubrió que Lenovo (fabricante de hardware) había estado sacando al mercado portátiles con el adware Superfish preinstalado durante varios meses (septiembre 2014 – febrero 2015). Este adware comprometía la seguridad de las conexiones cifradas (SSL/TLS).

3. Modo de infección (cómo se propagó).

El adware venía instalado de fábrica.

4. Síntomas o consecuencias (qué efectos tuvo).

Superfish instalaba su propia “Autoridad de Certificación” (CA) y generaba certificados autofirmados. Esto le permitía interceptar las sesiones de web de los usuarios con la intención de introducir anuncios. Este software tenía una clave privada que se hizo pública en internet y permitía generar certificados. Al saber la clave, un atacante podía usarla para espiar la información de las conexiones cifradas de la víctima e injectar código malicioso. Como síntoma, se menciona que al revisar el certificado SSL de un sitio web aparecía firmado por Superfish en vez de la CA legítima.

5. Medidas tomadas o recomendadas.

Se recomendó a los usuarios eliminar el software desde el Panel de Control de Windows y eliminar su certificado. Lenovo incluso creó una herramienta para llevar a cabo esta acción².

² https://support.lenovo.com/us/en/product_security/ps500066-superfish-uninstall-instructions