AWERTY

Con el ánimo de ayudar a las organizaciones en todo lo que concierne al teletrabajo, hemos identificado y agrupado aspectos que nuestros clientes principales tienen en consideración en materia de seguridad contra malware.

**ÁREA DE INFRAESTRUCTURA CLOUD**
Abril 2020

Gold
Microsoft Partner

Microsoft

Índice

# MALWARE, CONCEPTO

***"Se llama malware, del inglés malicious software, programa malicioso, programa maligno, badware, código maligno, software maligno, software dañino o software malintencionado a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada (al contrario que el «software defectuoso») y sin el conocimiento del usuario".***

es.wikipedia.org

El Ransomware es el malware de mayor propagación a nivel mundial en los sistemas informáticos.

## ¿Qué es el Ransomware?

El Ransomware es un tipo de malware que secuestra los datos de un equipo por medio de la encriptación y que exige una compensación económica a cambio de desencriptarlos.
En la mayoría de los casos, este tipo de ciber ataque reclama el pago por medio de criptomoneda para desencriptar los archivos. Aunque se acceda al chantaje y se pague la cantidad exigida, no existe ninguna garantía de que se desencripten los archivos. Por tanto, la recomendación a seguir es no pagar nunca.
Este tipo de ataques evolucionan y mejoran año tras año, de tal manera que no es raro que cada vez haya más personas afectadas. El aumento del uso de criptomonedas a nivel general permite que los pagos sean fáciles y prácticamente imposibles de rastrear. Debido a esto, el precio exigido por los rescates también crece constantemente.

## ¿A qué dispositivos afecta?

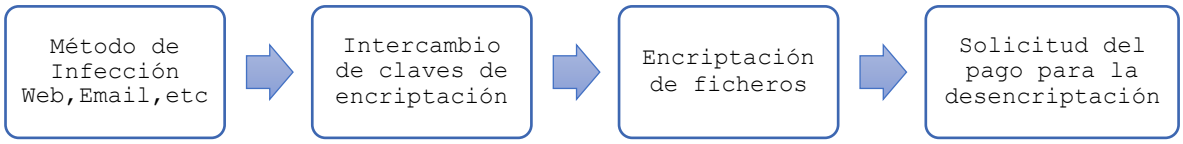
Puede afectar a todo tipo de equipos: ordenadores de los usuarios, servidores, tabletas y dispositivos móviles. Tras afectar a los dispositivos primariamente infectados, tiene también la intención de propagarse al resto de dispositivos con los que estén conectados.

## ¿Cómo accede a nuestro entorno?

Los principales métodos de infección son:

- A través de archivos o enlaces maliciosos enviados por correo electrónico.
- A través de suplantación de identidad dónde, por ejemplo, la víctima está accediendo, sin saberlo, a una web maliciosa navegando por Internet.
- Infección a través de la red local, con origen en otro equipo de la organización.
- También hay otros casos menos habituales, aunque recientes, que se aprovechan de protocolos vulnerables, como, por ejemplo, la conexión remota de Windows (RDP) utilizando el puerto 3389 para ejecutar este código malicioso si el Sistema Operativo no está actualizado.

### Patrón de ataque que usa



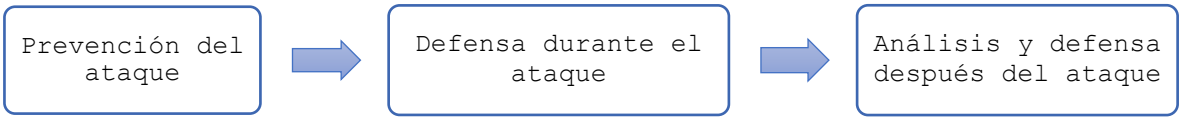

En primer lugar, el malware tiene que acceder al entorno informático para poder ejecutarse y posteriormente propagarse lo máximo posible. Cuando se ejecuta, identifica los archivos, normalmente por el tipo de extensión, y cifra todos los archivos menos los esenciales, para que el sistema operativo siga funcionando. De esta manera la víctima, puede utilizar el sistema operativo como mínimo para ver la petición de recompensa y realizar el pago.

Adicionalmente, tras obtener el acceso al entorno, los atacantes aprovechan una de estas técnicas para explotar el malware en otros equipos. Es lo que se llama propagación horizontal.

- Ingeniería social/phishing que, con la ayuda involuntaria de un usuario, permite exponer las credenciales o instalar software malicioso.
- Uso de credenciales robadas o vendidas, normalmente por una brecha de seguridad.
- Explotación de una vulnerabilidad de una aplicación o servicio.

## TIPOS DE RESPUESTA ANTE EL MALWARE

Una correcta política anti-malware exige trabajar en tres escenarios, todos ellos importantes.




### 10 prácticas para prevenir los ataques

Todas y cada una de estas acciones que vamos a describir requieren un servicio permanente de monitoreo y resolución de incidencias. La experiencia nos indica que el principal causante de una entrada de malware radica en la falta de mantenimiento de medidas de prevención.

- Concienciación y formación periódica sobre seguridad a los usuarios.
- Realizar evaluaciones de riesgo periódicas para identificar vulnerabilidades de seguridad en la organización.
- Software y Sistemas Operativos al día con actualizaciones y parches de seguridad.
- Protección y filtro de contenidos ante las llamadas DNS.
- Firewall perimetral en las sedes e individual en los equipos de teletrabajo.
- Software anti-malware en cada equipo.
- Factor de doble autenticación en los servicios de correo, ficheros y Cloud en general.
- Disponer de historial de versionado de documentos.
- Política de seguridad anti-malware en el correo electrónico.
- Privilegios de usuario restrictivos, nunca derechos de administrador local.

## Prácticas para defenderse durante el ataque

En ocasiones nos podemos encontrar que ya hemos sido atacados por algún tipo de malware, siendo así demasiado tarde para tratar de detener su propagación. Pero, si lo detectamos a tiempo, podemos poner en marcha una serie de prácticas para minimizar su impacto a través de la organización.

- Disponer de tecnologías que detecten y nos notifiquen el momento en que se está generando el ataque. Normalmente, podemos obtener esta información gracias a servicios de monitorización de red que nos alertan de consumos anómalos, o también mediante servicios de análisis de Logs centralizados (SIEM) que nos alertan de eventos sospechosos.
- En el ámbito del networking, disponer de tecnología que permita una segmentación de red adecuada para aplicar aislamientos de forma rápida, tanto dentro de la red local como de Internet.
- Disponer de un equipo humano de respuesta rápida en la organización. No tienen que ser personas de IT. Lo componen el suficiente número de personas para revisar cada una de ellas una serie de equipos informáticos.
- Disponer de un protocolo previo de actuación con las pautas a seguir para iniciar procesos de detección y eliminación del problema cuanto antes, así como registrar y notificar cada una de las acciones.
- Formación al equipo de dicho protocolo.
- Entre algunos puntos de control, el más común es el de aislar el equipo de la red de trabajo para evitar que se propague hacia los demás. Desconectar el cable ethernet o desactivar el Wifi puede ser suficiente.

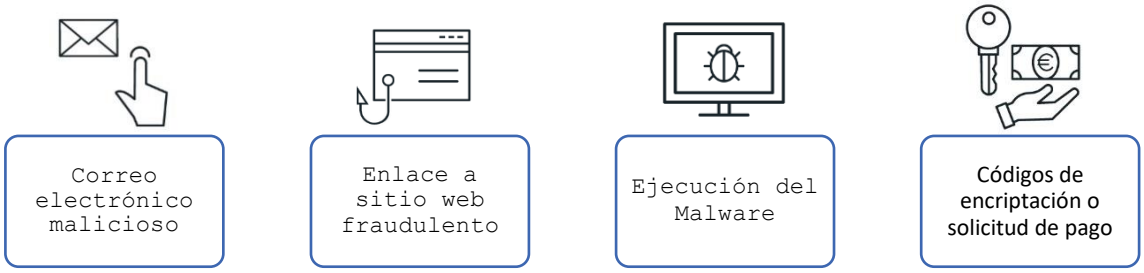
## Prácticas para defenderse después del ataque

Una vez el malware ha hecho todo el daño que podía hacer, solo nos queda restablecer el entorno a un estado anterior, analizar el origen del problema y tomar las medidas necesarias para que no vuelva a producirse un ataque.

- Cuando superamos un ataque, lo primero de todo es tratar de reanudar las operaciones comerciales.
- Puede entrar en juego la restauración de los datos y equipos mediante las copias de seguridad disponibles.
- Recolectar y preservar evidencias para la aplicación de la ley y para propósitos de auditoría.
- Analizar los datos forenses que ofrecen las aplicaciones anti-malware para predecir y prevenir futuros ataques.
- Realizar análisis de causa, identificar lecciones aprendidas y aumentar la seguridad con los niveles de protección necesarios. Entre ellos, los protocolos de seguridad de prevención y actuación frente a malware.

# TECNOLOGÍAS ANTI-MALWARE

Desde AWERTY recomendamos varias herramientas que se encargan de proteger cualquier fase de vulnerabilidad en las que se basan los ataques más comunes y críticos.




## Correo electrónico malicioso

Contamos con herramientas que nos protegen antes de que el malware pueda acceder al entorno. Por ejemplo, antes de que un usuario reciba un email con contenido malicioso.

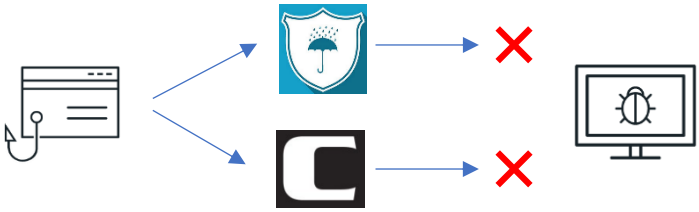
- Office 365 Advanced Threat Protection: filtra el contenido de los correos electrónicos (enlaces y archivos adjuntos) en el datacenter de Microsoft antes de que el correo sea remitido al usuario.


## Enlace a sitio web fraudulento

El usuario puede ser víctima de phishing por culpa del acceso a páginas web maliciosas o que provengan del correo electrónico no filtrado. Contamos con varias tecnologías de protección

- Cisco Umbrella: a nivel de dispositivo de usuario y a través del datacenter de Cisco, se aplican filtros para evitar el acceso a páginas web potencialmente maliciosas. Resulta especialmente útil para dispositivos con movilidad, pero también es aplicable dentro de la red local.

- Firewall Clavister: con estos dispositivos físicos ubicados en la red local podemos aplicar filtros de contenido web en función de categorías, según perfiles de usuario o por franjas horarias, entre muchas otras configuraciones.



## Ejecución del malware

El archivo malicioso ya se encuentra en el dispositivo dispuesto a ejecutarse y propagarse para realizar la infección. En este punto disponemos de herramientas para detectar, evitar y aislar la ejecución del malware.

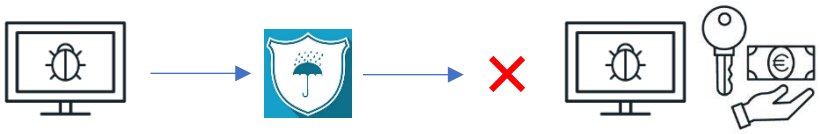
- Microsoft Defender Advanced Threat Protection: se trata de un software de protección en tiempo real que se encuentra en los dispositivos de usuario. Si detecta una amenaza, la bloquea poniéndola en cuarentena y lo notifica para que pueda ser gestionada con detalle.

- Microsoft Intune: se encarga de administrar los dispositivos, incluyendo actualizaciones de software y Sistema Operativo con políticas para limitar el uso del dispositivo por parte del usuario.


## Códigos de encriptación o solicitud de pagos

En ocasiones el malware puede requerir de una petición externa para completar la infección, por ejemplo, en el caso de un Ransomware, el encriptado del dato.

- Cisco Umbrella: cuando el ransomware trata de acceder a internet para descargar las claves de encriptación, Umbrella lo bloquea e impide que el Ransomware pueda encriptar los datos.



Para completar el esquema de seguridad, es necesario disponer de backups de los equipos y de los datos de la empresa. El servidor de backup debería estar ubicado, si es posible, fuera de la red y del dominio principal. De esta manera, en caso de ser infectados, no sería posible corromper el servidor de backup y podríamos restaurar los equipos y sus datos.

- Arcserve: se trata de un software de backup con una consola centralizada que permite gestionar todo lo relativo a las copias de seguridad. En este caso, tanto de los equipos de usuario y de los servidores como de los datos de Office 365. Existe una versión 100% Cloud en los datacenters de Arcserve.

# LAS SOLUCIONES, AL DETALLE

## Cisco Umbrella

Capa de protección frente a infecciones vía DNS para una red empresarial o por dispositivo de usuario (portátiles, teléfonos móviles, tablets, etc.)

Este software como servicio se encarga de filtrar las peticiones DNS de una forma centralizada en el Cloud de Cisco.

La protección se puede aplicar cambiando manualmente los registros DNS del router o firewall de una red local o instalando un agente liviano en los dispositivos con movilidad.

La gestión de este servicio nos permite configurar diferentes políticas para, por ejemplo, evitar que los usuarios entren en determinadas páginas web o detectar si su contenido es malicioso y bloquear su acceso.

Para más información:
https://www.awerty.net/infraestructura-cloud/awerty-cisco-umbrella/

## Dispositivos firewall de Clavister

Toda empresa necesita un firewall físico para tener una garantía de seguridad en sus datos, tanto entrantes como salientes. Con el paso de los años, estos dispositivos han evolucionado para ofrecer más técnicas de protección en un único dispositivo.

Con un firewall de Clavister tenemos la garantía de seguridad en nuestra red, bloqueando el acceso a todos los puertos que no sean necesarios, sumándole un filtro web para evitar accesos de los usuarios a webs maliciosas y con una capa adicional de servicios de protección de ataques como Botnets o DDoS.

Para más información:
https://www.awerty.net/infraestructura-cloud/awerty-clavister/

## Office 365 Advanced Threat Protection

Protege a la organización contra potenciales amenazas incluidas en mensajes de correo electrónico, como podrían ser los vínculos y archivos adjuntos. Utiliza directivas de protección, informes en tiempo real y el uso de herramientas para investigar y responder ante una amenaza de manera automática.

Para más información:
https://www.microsoft.com/es-es/microsoft-365/exchange/advance-threat-protection#office-ProductsCompare-785zwzq
https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

## Microsoft Defender Advanced Threat Protection

Es una plataforma diseñada para ayudar a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas siempre que dispongamos del Sistema Operativo Windows 10.

- Sensores de comportamiento. Recopilan y procesan señales del Sistema Operativo y las envían a la nube de Microsoft Defender ATP.
- Análisis de seguridad en la nube. Perspectivas, detecciones y respuestas recomendadas ante amenazas avanzadas.
- Inteligencia de amenazas. Gracias a la inteligencia proporcionada, permite a Microsoft Defender ATP identificar a los atacantes (herramientas, técnicas, procedimientos) y generar alertas cuando se cumplan los datos de los sensores.

Para más información:
https://docs.microsoft.com/es-es/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection

## Arcserve

Software de copias de seguridad que permite realizar backups de equipos locales y virtuales. También, a su vez, permite realizar réplicas a servidores que se encuentran en otra ubicación para tener disponibilidad del backup incluso si el servidor principal ha sufrido un ataque.

Es compatible con plataformas Cloud como Microsoft Azure.

Para más información:
https://www.awerty.net/infraestructura-cloud/awerty-cloud-backup/