Guia Sobre Ransomware

PRESIDENCIA DE LA REPÚBLICA DOMINICANA

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

RANSOMWARE:
GUÍA PARA EL EMPRESARIO

El desarrollo de las tecnologías de la información y comunicación facilita a los usuarios la realización de las actividades cotidianas, tanto personales como laborales, lo cual está provocando una verdadera invasión de dispositivos, redes y aplicaciones más conectadas, a la vez que hace a los usuarios más dependientes de las mismas.

Como es de esperarse, estos beneficios de conexión en cualquier lugar y cualquier momento traen consigo riesgos, ya que las mismas ventajas de inmediatez, movilidad y comunicación de las que nos beneficiamos son también aprovechadas por los que se dedican a realizar actividades ilícitas. En este sentido, se han desarrollado diferentes actividades ilícitas para lograr comprometer la información que utiliza el usuario. Pero hay una en particular, que data de los años 80, pero que se ha estado desarrollando desde el 2017 con una gran rapidez, causando gran impacto tanto en empresas como en los ciudadanos.

Ransomware es el software malicioso que trata de infectar computadoras y dispositivos móviles con el objetivo de bloquear el uso del dispositivo, o parte de la información que contiene, para luego pedir un rescate. Afecta a cualquier usuario, negocio o actividad que pueda pagar a cambio de la devolución de su información y causa pérdidas temporales o permanentes de información interrumpiendo la actividad normal y en algunos casos causando danos de reputación.

¿Qué es?

Es un tipo de malware o software malicioso, que actualmente se está propagando de forma muy activa por internet, que impide el acceso y amenaza con destruir los documentos y otros activos de las víctimas si estas no acceden a pagar un rescate.

Este software, al llegar a los ordenadores víctimas, los infecta manipulando el sistema y provocando mal funcionamiento o la realización de acciones maliciosas; cifra ciertos archivos o bien todo el disco duro de la víctima, impidiendo el acceso del usuario y solicitando un rescate para recuperar el acceso.

El método más común de propagación es mediante el envío de correos electrónicos maliciosos a las víctimas quienes serán infectadas una vez abran o hagan clic en un vínculo o archivo.

¿Como me infecto?

Para el proceso de infección los ciberatacantes utilizan varias vías:

- agujeros de seguridad de los softwares y sistemas operativos instalados en los equipos;
- servidores web desactualizados;
- sistemas SCADA conectados a internet sin las medidas de seguridad correctas;
- cuentas con privilegios de administrador obtenidas mediante engaños o vulnerabilidades de software;
- mediante el engaño a los usuarios utilizando técnicas de ingeniería social para que instalen el malware, o
- mediante spam con enlaces web maliciosos o archivos adjuntos que contienen falsos macros que descargan el malware.

El ransomware es una actividad ilícita que tiene muchas formas y cada vez se hace más sofisticado y destructivo.

Medidas de seguridad

Para protegerse ante una infección de este malware es necesario implementar una serie de buenas prácticas con dos propósitos:

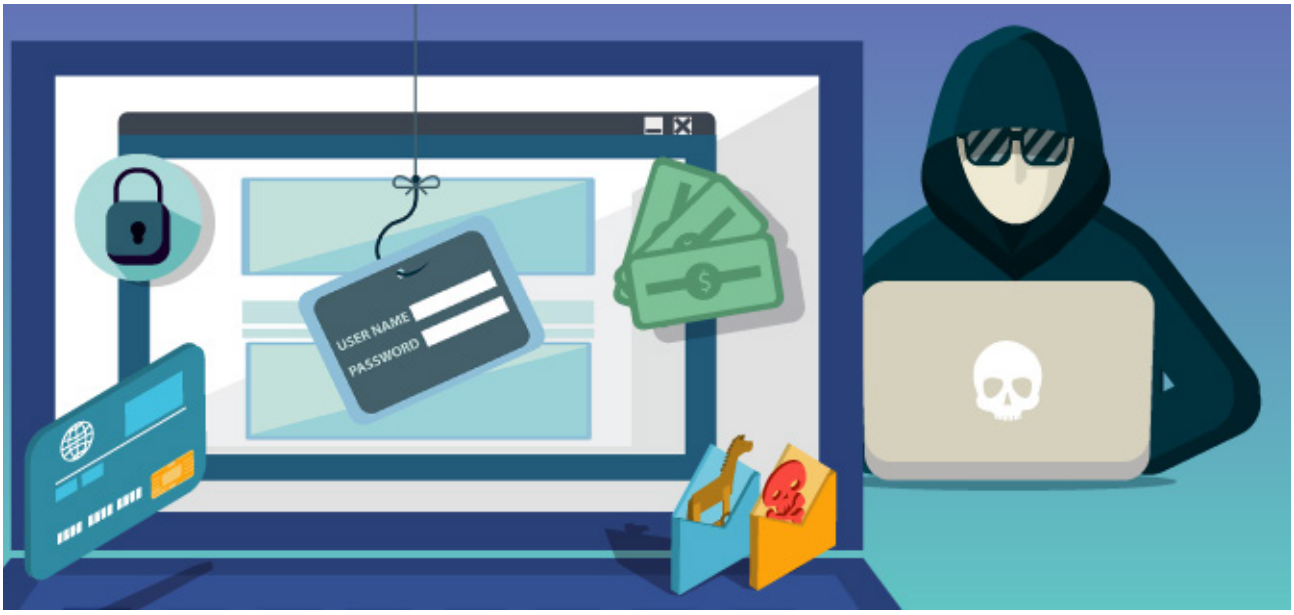
- Concientización, para evitar caer en los engaños y las técnicas de ingeniería social y
- configuración robusta de seguridad, para mantener los sistemas, aplicaciones y servicios actualizados y monitoreados y así reducir las vulnerabilidades.

La mayoría de las infecciones con ransomware tienen lugar por medio de ataques de ingeniería social. Se engaña al usuario a fin de que de acceso ya sea para instalar el malware o para conseguir las contraseñas con las que podrán ingresar para instalarlo. Es por esto que es esencial que fomentemos y concienticemos a nuestros usurarios ensenándoles a reconocer estas situaciones y cómo actuar.

Ingeniería social

El primer paso de este ataque es reunir toda la información posible sobre la empresa o el usuario que puede ser útil, luego contactar a la víctima y buscar establecer una relación que le permita ganarse su confianza utilizando la información obtenida.

Una vez obtenida la confianza de la víctima, se le manipula para obtener información necesaria, como credenciales, información confidencial o se le incita a realizar acciones como instalar programas, enviar correos o brindar acceso a las instalaciones.



¿Cómo reconocer un ataque de ingeniería social?

- Desconfíe de cualquier mensaje recibido por correo electrónico, SMS, WhatsApp o redes sociales en el que se le coaccione o apremie a hacer una acción ante una posible sanción.
- No abra ni conteste correos de usuarios desconocidos o de procedencia sospechosa.
- Revise los enlaces antes de darles clic, aunque sean de contactos conocidos.
- Utilice el antivirus para los archivos adjuntos antes de abrirlos.
- Tenga siempre actualizado su sistema operativo y antimalware.
- Asegúrese de que las cuentas de usuarios cuentan con contraseñas robustas y solo con los privilegios necesarios para sus tareas.

Además de la concientización y de saber identificar un ataque de ingeniería social, es importante implementar medidas técnicas y procedimientos. Esto va a permitir que nuestros sistemas no tengan agujeros de seguridad, manteniéndolos actualizados y bien configurados.

Ingeniería social

Debemos establecer un buen diseño de red para reducir la exposición de servicios internos al exterior y, por otra parte, instituir procedimientos que indiquen las acciones a tomar para: tener actualizados todos los softwares, hacer copiar de seguridad, controlar el acceso, restringir el uso de aplicaciones y cómo actuar en caso de un incidente, entre otros.
A continuación, algunas medidas a tomar para evadir una infección por ransomware.

Copias de seguridad

- Realizar y conservar como mínimo dos copias de seguridad actualizada;
- identificar lugares diferentes al del servidor de archivo para conservar los respaldos ;
- tener en cuenta que, si el respaldo es por la nube, existen ransomwares que cifran y bloquean este tipo de respaldos, y
- comprobar que las copias de seguridad realizadas funcionan correctamente y se conoce el procedimiento de restauración.

Actualización

- Establecer un procedimiento de actualización tomando en cuenta las publicaciones realizadas por los proveedores directos y realizar el proceso de una forma automática y centralizada.

Privilegios mínimos

- Establecer privilegios limitados, según sus actividades, para las cuentas de usuario;
- hacer obligatorio el uso de contraseñas robustas y el bloqueo de cuentas ante un número determinado de intentos;
- no utilizar cuentas de administrador para tareas cotidianas, y
- deshabilitar y documentar las cuentas que no sean necesarias.

Mínima exposición

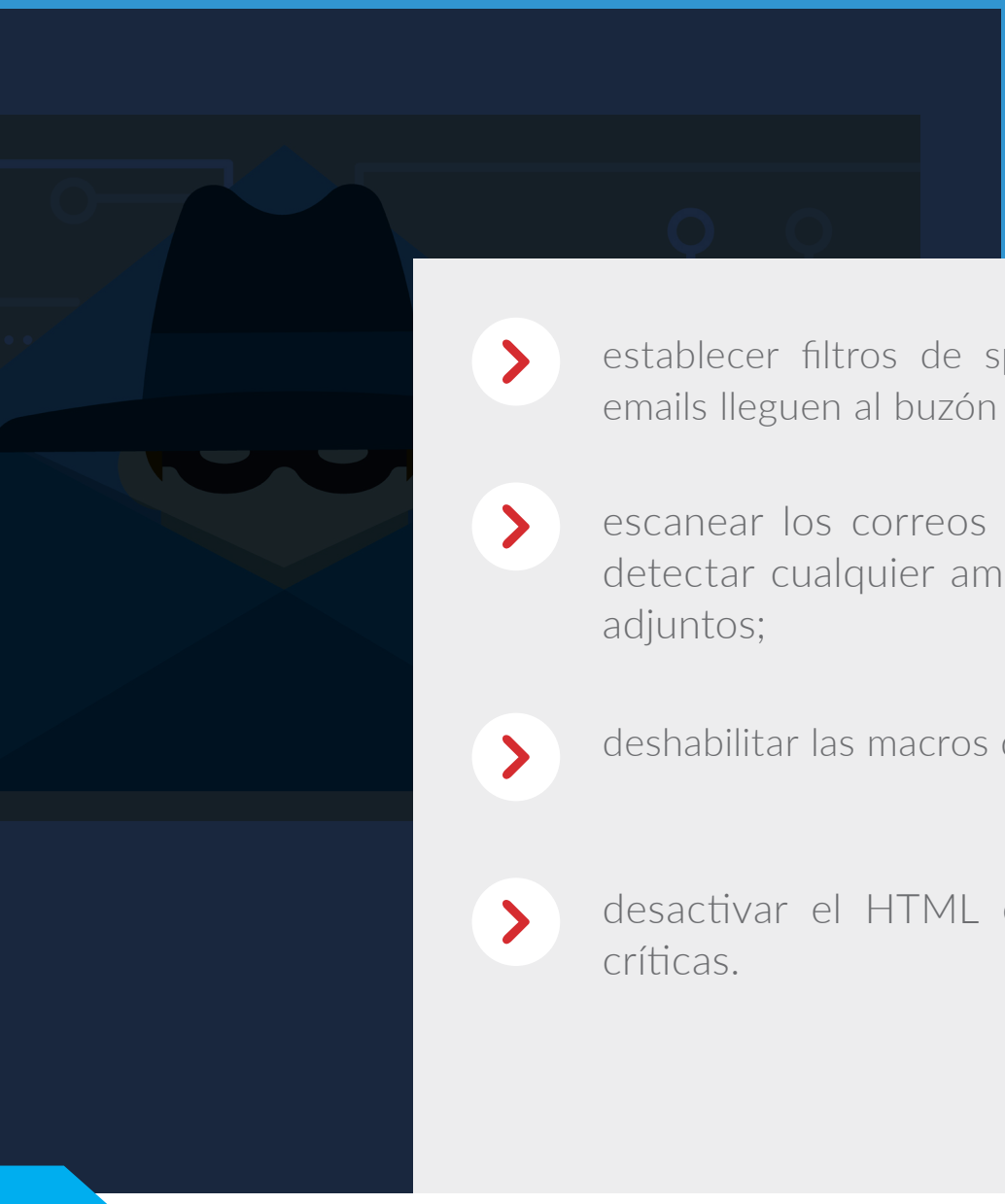
Evitar la exposición al exterior de la información interna de la empresa o de aquella información o servicio que no necesita ser accesible desde el exterior es otro principio básico de seguridad.

Si es necesario acceder a herramientas desde fuera de la empresa para la ejecución de actividades relacionadas con sus funciones, es importante tomar las siguientes medidas:

- separar los servidores accesibles desde el exterior de los servidores privados;
- implementar un sistema de seguridad capaz de establecer reglas para bloquear o permitir conexiones de entrada o salida de nuestra red;
- establecer una zona o red desmilitarizada, o sea, una red aislada del resto de la red interna, donde se ubiquen únicamente los servidores que deben ser accesibles desde internet, y
- establecer escaneos con un antimalware para el monitoreo de los equipos.

Es importante realizar periódicamente una auditoria a los sistemas de información tanto para poner a prueba los mecanismos de seguridad y procedimiento de respuesta ante un incidente.

Correo electrónico

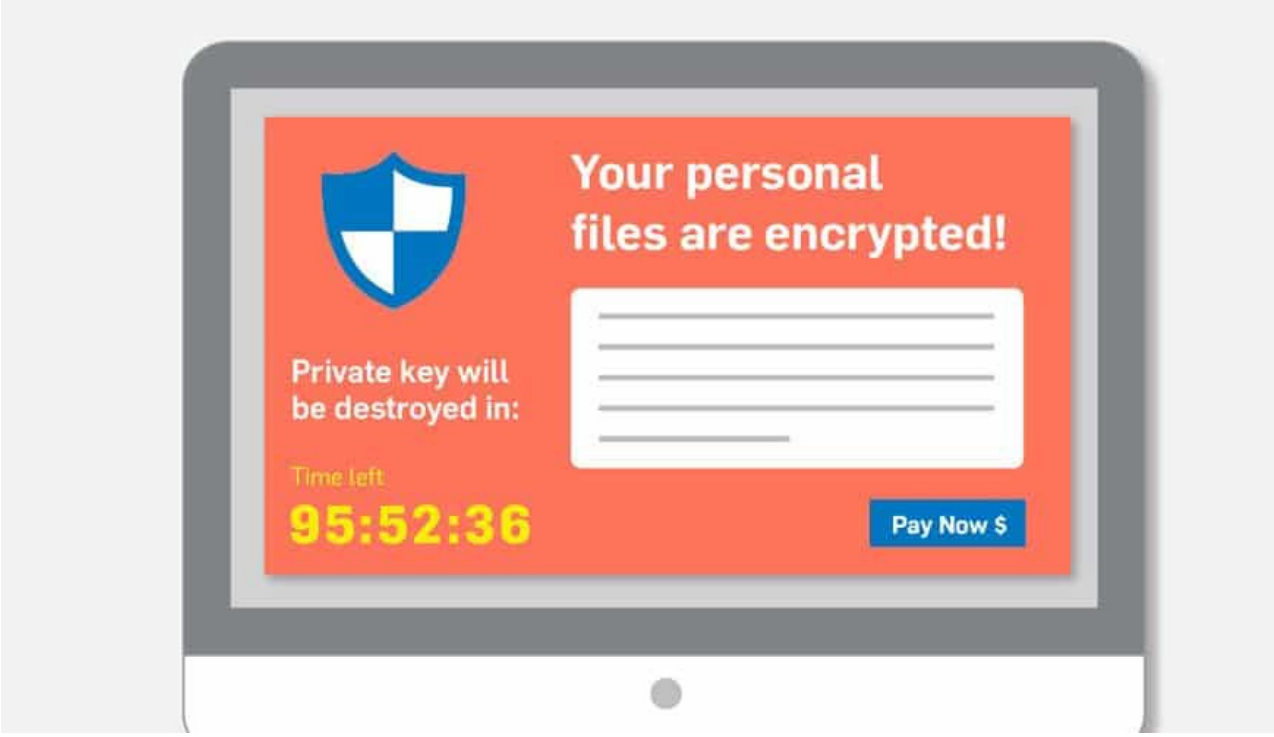


- establecer filtros de spam para evitar que estos emails lleguen al buzón de correo;
- escanear los correos entrantes y salientes para detectar cualquier amenaza y filtrar los archivos adjuntos;
- deshabilitar las macros de los archivos de office, y
- desactivar el HTML en las cuentas de correo críticas.

En caso de infección

Si estás comprometido por algún ransomware y te están extorsionando para pagar un rescate, debes seguir estas recomendaciones:

- **NO PAGAR** nunca el soborno.
- Activar el un plan de respuesta a incidentes, si se cuenta con uno, para poder minimizar los daños que podría causar recuperar la actividad lo más antes posible.
- en caso no tener un plan de respuesta, utiliza el último respaldo realizado para recuperar la información perdida.



Otras medidas a tomar:

- Contactar con el Centro Nacional de Respuesta a Incidentes CSIRT-RD: te ayudarán a resolver el incidente, te indicarán cómo actuar y, en caso de que exista algún mecanismo probado para recuperar los archivos, te lo indicarán.

- Aísla los equipos infectados inmediatamente, desconectándolos de la red para evitar expansión.
- Clona los discos duros de los equipos infectados, pueden servir de evidencia si se procederá con una denuncia. Este procedimiento lo debe realizar un técnico especializado.
- Si es posible, debes recoger y aislar muestras de archivos cifrados o del propio malware para fines de análisis.
- Si es posible, realizar el cambio de contraseña para todos los dispositivos de red y cuentas online, y después de eliminado el Ransomware volver a realizar el cambio.
- Desinfectar los equipos y recuperar los archivos cifrados en caso de ser posible.

- Restaurar los equipos para continuar la actividad y, en caso de ser posible, reinstalar el equipo con el software original o arrancar en modo seguridad para recuperar el respaldo previo en caso de poseerlo
- Denuncia el caso a las autoridades correspondientes:
  o Policía Nacional – Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT).