MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

COLCERT

Identificador
[COLCERT- AD-1213- 0011]

13/12/2022

Advertencia de Seguridad Digital

TLP:CLEAR

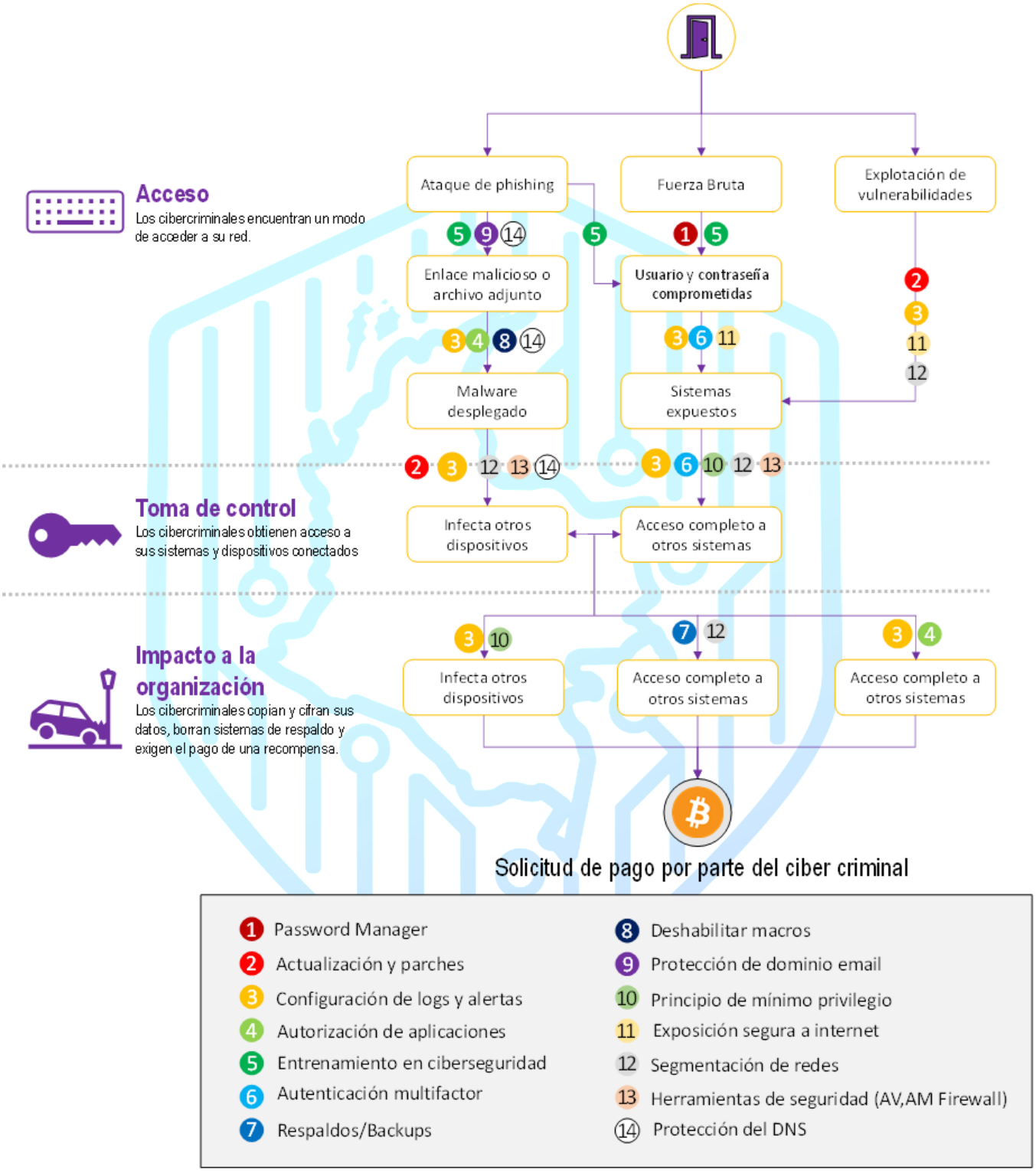
¿Qué es el Ransomware?

Es un tipo de software malicioso que impide el acceso a archivos o sistemas cifrando o eliminando los datos hasta que se pague una suma de dinero. Se podría decir coloquialmente que es un secuestro de información.

Dinero Representado en Bitcoins, para prevenir el rastreo de los ciberdelincuentes

Las últimas variantes de ransomware, indican que se sustrae la información hacia los servidores del atacante, luego se cifra y termina con el chantaje a los clientes; con este mecanismo se extorsiona de tres formas si no se cancela el monto estipulado: exposición de la información, no se proporciona la llave de descifrado para liberar los datos cifrados y se presiona para actuar en beneficio de los atacantes.

¿Cómo ocurre un incidente de ransomware y cómo prevenirlos?



Mecanismo de operación de un Ransomware. Fuente: Adaptado de Canadian Centre for Cyber Security

¿Cómo puede preparar su organización?

Hay varias maneras de minimizar el riesgo y preparar su organización si se produce un ataque de ransomware.

1. **Planee con antelación.**
   Desarrolle un plan de respuesta a incidentes para definir como su organización identificará, protegerá, detectará, responderá y se recuperará a un incidente de seguridad digital, como un ataque de ransomware, así mismo se deben designar roles a los equipos técnicos y concientizar a los colaboradores con instrucciones detalladas en caso de presentarse un incidente.

2. **Educación y concientización en seguridad digital a sus colaboradores.**
   Realice capacitación a los usuarios en seguridad digital, explicando los riesgos a los que se encuentran expuestos diariamente cuanto interactúan en el ciberespacio.

3. **Copias de seguridad y respaldo de datos.**
   Establezca procedimientos para la realización de copias de seguridad y respaldo de recuperación y continuidad de la operación y configure segmentos de red aislados para la plataforma de copias de seguridad; de manera periódica pruebe los planes de continuidad de la operación mediante la restauración de datos, para evitar la pérdida de éstos y poder recuperarlos en caso de daño o mal funcionamiento de la infraestructura de copias de seguridad; las copias de seguridad funcionales, permitirán a la organización ser más resilientes en caso de un incidente de ransomware.

4. **Actualizaciones y parches de seguridad**
   Compruebe si hay publicaciones de actualizaciones y parches de seguridad a sus equipos de seguridad, servidores y computadores de manera permanente para reparar fallos de seguridad y reducir las vulnerabilidades que puedan ser explotadas por los ciberdelincuentes, en su software, firmware y sistemas operativos.

5. **Planes de recuperación ante desastres**
   Desarrolle un plan de recuperación que contenga instrucciones detalladas sobre cómo responder a incidentes no planificados como desastres naturales, cortes de energía, ciberataques y cualquier otro suceso que afecte la continuidad de la operación de la organización y permita restablecer rápidamente los procesos más importantes de la organización, definiendo roles y responsables en este plan.

¿Cómo puede proteger su información?

1. **Políticas de Seguridad de la Información**
   Defina sus políticas de gestión de la seguridad de la información, procurando responder al contexto de su organización, objetivos de negocio, misión y enfoque de su análisis de riesgos de seguridad de la información.

2. **Plan de Continuidad del Negocio.**
   Desarrolle y busque la aprobación del plan de continuidad del negocio, para definir las aplicaciones de misión crítica que deben ser respaldadas en sitio alterno para la recuperación y restablecimiento de las operaciones según el tiempo tolerable necesario para que los sistemas críticos vuelvan a estar operativos (RTO) y la cantidad máxima aceptable de pérdida de datos entre la última copia de seguridad y la fecha en que ocurre del incidente (RPO).

3. **Copia de seguridad de los datos de aplicaciones y servicios críticos.**
   Implemente y operacionalice procedimientos de respaldos o copias de seguridad/backups. Tenga en cuenta que estas copias de seguridad deben ser generadas y almacenadas en segmentos aislados para evitar ser alcanzado por el ransomware.

4. **Principio del mínimo privilegio- Zero Trust**
   Administre y supervise las cuentas de usuario y el acceso aplicando el principio de mínimos privilegios.

5. **Deshabilitar macros**
   Asegúrese de deshabilitar las macros como predeterminadas, para reducir el riesgo que el ransomware se propague a través de los archivos adjuntos de Microsoft Office.

6. **Configuración de herramientas de seguridad**
   Procure instalar firewall de red y de aplicaciones -WAF, sistema Endpoint Detection Response EDR, para obtener visibilidad en la red.

¿Cómo detectar el ransomware?

- **Alertas de seguridad de plataformas antivirus y soluciones EDR**
- **Cambios en las extensiones de los archivos.**
- **Cambios en los nombres de los archivos.**
- **Tráfico de red anormal.**
- **Archivos cifrados e inaccesibles.**
- **Aparición de algún tipo de nota de rescate.**

¿Cómo me recupero de un Ransomware?

- ✓ **Ponga el equipo en cuarentena aísle el dispositivo inmediatamente:** Desconecte los dispositivos afectados de todas las interfaces de red (ethernet, wifi, bluetooth, etc.).

- ✓ **Dejar la computadora y servidores encendidos:** Mantenga los dispositivos prendidos para aumentar la probabilidad de recuperación, no apagar los dispositivos para evitar la pérdida de memoria volátil y realizar la investigación forense.

- ✓ **Identifique el tipo de ransomware:** Utilice la información en la nota de rescate (por ejemplo, las URL listadas) y las extensiones de archivo que tienen los archivos cifrados, para identificar la cepa del ransomware e investigar ataques recurrentes.

- ✓ **Realice una investigación:** Para identificar vector de ataque, indicadores de compromiso – IoC y posibles mecanismos de propagación con el propósito de realizar seguimiento al comportamiento del ransomware a las técnicas y tácticas empleadas por los ciberdelincuentes.

- ✓ **Restablezca el dispositivo y borre todos los datos:** Si no hay ninguna herramienta de descifrado disponible en línea para su cepa de ransomware, limpie de forma segura su dispositivo y vuelva a instalar el sistema operativo, instale nuevamente la solución de antivirus y de ser posible realice una imagen forense a equipos afectados como evidencia digital.

- ✓ **Restaure desde su copia de seguridad:** Analice sus archivos de copia de seguridad y asegúrese de que estén libres del ransomware o cualquier otro malware

Recomendaciones Generales de Seguridad

- ➢ Haga copias de seguridad de sus datos e información crítica de manera regular.

- ➢ Asegúrese de que las copias de seguridad están en la nube, en un disco duro o en dispositivos de almacenamiento externo.

- ➢ Realice pruebas de restauración de las copias de seguridad y, analice con su solución de antivirus sus copias antes de ponerlas en ejecución.

- ➢ Utilice contraseñas robustas, largas y complejas, al igual que cámbielas periódicamente, establezca políticas de acceso y uso de contraseñas.

- ➢ Supervise los informes sobre amenazas cibernéticas en relación con la publicación de credenciales de inicio de sesión de VPN comprometidas y cambie las contraseñas/configuraciones si corresponde.

- ➢ Restrinja las comunicaciones de uso compartido de archivos como SMB y RDP.

- ➢ Supervise procesos que puedan abusar del Shell de comandos de Windows y restrinja los permisos elevados solo a personal con rol de administración.

- ➢ Mantenga siempre su sistema operativo y software de seguridad actualizado. Las actualizaciones a menudo incluyen parches de seguridad que pueden ayudar a prevenir que su dispositivo sea vulnerable a ataques de ransomware.

- Instale y actualice regularmente el software antivirus o antimalware en todos los dispositivos (servidores, computadores, celulares).

- Identifique archivos anómalos y apúntelos para tenerlos como referencias en la revisión de otros paths y directorios, observe las marcas de fecha y hora de esos archivos ya que puede encontrar otras copias de la infección en el sistema al identificar archivos o carpetas con una marca de tiempo similar. Abra Regedit como administrador y busque los nombres de archivos y paths identificados. Es posible que se encuentre con una entrada Default = [filename].dll dentro de una clave de registro con un GUID. Copie el GUID y luego haga una búsqueda con este identificador.

Canales de Atención

Si tiene alguna consulta técnica, puede comunicarse con CSIRT Gobierno de tratarse de una entidad del Estado, o con COLCERT si pertenece a cualquier otro sector de la economía, a través de los siguientes canales:

Bogotá: +57 601 344 22 22
Línea Gratuita Nacional: 018000952525 Opción 2

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT