Reporte Incidente: USB Estacionamiento 2024-09-30 #1  
Hospital Samic

Escenario

Como contratado de ciberseguridad del Hospital Samic se me informa que uno de los empleados de seguridad encontró en el suelo del estacionamiento, una memoria USB con el logotipo del hospital impreso en ella. No hay nadie cerca que haya identificado como para haberlo tirado, así que decide recogerlo y lo reporta en la guardia.

Se lleva la memoria USB a la oficina de sistemas, donde el equipo tiene instalado un software de virtualización en una estación de trabajo. El software de virtualización se puede utilizar para este mismo propósito porque es una de las únicas formas de investigar con seguridad una memoria USB desconocida.

El software funciona ejecutando una instancia simulada del ordenador en la misma estación de trabajo.

Esta simulación no está conectada a otros archivos o redes, por lo que la unidad USB no puede afectar a otros sistemas si resulta estar infectada con software malicioso.

Inspección del contenido de la memoria USB

Se crea un entorno virtual y conecta la unidad USB a la estación de trabajo. El contenido del dispositivo parece pertenecer a Jorge Horrisberger, director de recursos humanos del Hospital Samic.

La unidad de Jorge contiene una mezcla de archivos personales y relacionados con el trabajo. Por ejemplo, contiene carpetas que parecen almacenar fotos familiares y de mascotas. También hay una carta de nueva contratación y un horario de turnos de los empleados.

Revisé los tipos de información que Jorge tiene almacenados en este dispositivo. A continuación, en la fila contenido de la tabla, se describe sobre el tipo de información que hay almacenada en la unidad USB.

Nota: Las unidades USB suelen contener una gran variedad de información de identificación personal (IIP). Los atacantes pueden utilizar fácilmente esta información sensible para atacar al propietario de los datos o a otras personas de su entorno.

Aplicando la mentalidad de ataque al contenido de la unidad USB

La unidad flash parece contener una mezcla de archivos personales y relacionados con el trabajo.

Se consideró cómo podría utilizar esta información un atacante si la obtuviera. Además, se consideró si todo este suceso fue una puesta en escena.

Por ejemplo, un atacante podría haber colocado estos archivos en la unidad USB como distracción.

Podrían haber apuntado a Jorge o a alguien que él conoce, esperando que encontraran el dispositivo y lo conectaran a su estación de trabajo.

Al hacerlo, el atacante podría establecer una puerta trasera en los sistemas de la empresa mientras el objetivo desprevenido hojeaba los archivos.

En la fila "Mentalidad del atacante " de la tabla se describe sobre cómo podría utilizarse esta información contra Jorge o el hospital.

*Consejo profesional:* La *Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) ofrece algunos* [*consejos de seguridad sobre cómo actuar con precaución con las unidades USB*](https://www.cisa.gov/news-events/news/using-caution-usb-drives)*, como mantener separadas las unidades personales de las de la empresa.*

Análisis de los riesgos de encontrar un USB

Los atacantes a veces realizan ataques de cebo USB para entregar código malicioso que han elaborado.

Sin embargo, esta unidad USB seguía siendo un riesgo para la seguridad aunque no contuviera código malicioso. Podría haber sido encontrada fácilmente por un atacante que podría haber utilizado su contenido para planear diversos ataques.

Se consideró algunos de los riesgos asociados a los ataques de cebo USB:

¿Qué tipos de software malicioso podrían esconderse en estos dispositivos? ¿Qué podría haber ocurrido si el dispositivo estuviera infectado y fuera descubierto por otro empleado?

¿Qué información sensible podría encontrar un actor de amenazas en un dispositivo de este tipo?

¿Cómo podría utilizarse esa información contra un individuo o una organización?

En la fila Análisis de riesgos de la tabla se describen los controles técnicos, operativos o de gestión que podrían mitigar los ataques de cebo USB.

Análisis Incidente USB

| **Análisis de Incidente del USB** | |
| --- | --- |
| **Contenido** | ¿Hay archivos que puedan contener información personal identificable?¿Hay archivos laborales confidenciales? ¿Es seguro almacenar archivos personales junto con archivos laborales?  El contenido de la unidad USB contiene archivos que parecen pertenecer a una persona concreta.  Contiene una mezcla de información personal y relacionada con el hospital.  Los archivos personales y archivos laborales no deberían almacenarse en el mismo lugar.  Algunos documentos parecen contener información personal que Jorge no querría que se hiciera pública.  Los archivos de trabajo incluyen información de identificación personal de otras personas.  Además, los archivos de trabajo contienen información sobre las operaciones del hospital. |
| **Mentalidad**  **del atacante** | ¿Podría usarse la información en contra de otros empleados? ¿Podría usarse la información en contra de familiares? ¿Podría la información brindar acceso a la empresa?  Cualquier Información que obtenga un atacante puede ser utilizada contra alguien.  Si hay información que ayude al atacante es posible.  Las planillas de horas pueden brindarle a un atacante información sobre otras personas con las que trabaja Jorge.  Tanto la información personal como la laboral podrían utilizarse para engañar a Jorge.  Por ejemplo, un correo electrónico malicioso puede estar diseñado para que parezca que proviene de un compañero de trabajo o un familiar. |
| **Análisis de riesgo** | ¿Qué tipos de software malicioso podrían estar ocultos en estos dispositivos? ¿Qué podría haber sucedido si el dispositivo se hubiera infectado y lo hubiera descubierto otro empleado? ¿Qué información confidencial podría encontrar un agente de amenazas en un dispositivo como este?¿Cómo podría usarse esa información contra una persona o una organización?  Promover la concienciación de los empleados sobre este tipo de ataques y qué hacer cuando una unidad USB sospechosa es un control gerencial que puede reducir el riesgo de un incidente negativo.  Establecer exploraciones antivirus rutinarias es un control operativo que se puede implementar.  Otra línea de defensa podría ser un control técnico, como deshabilitar la reproducción automática en las PC de la empresa que evitará que una computadora ejecute automáticamente código malicioso cuando se conecte una unidad USB. |