PRIMERA ENTREGA

Dato fuente de la información

Para la elaboración del presente informe, han sido analizadas las siguientes fuentes de información:

* Informe de estatus de situación actual.
* Muestra de malware entregado por el equipo de soporte técnico de CoderHouse

Análisis del Malware

El presente informe responde a la necesidad de conocer el alcance del incidente de seguridad provocado por el cifrado masivo de archivos (ransonware) en la infraestructura de Corporación Luxor , identificado el día 28 de Septiembre del 2022 a las 22:04 hs. Con base en las actuaciones de respuesta , los técnicos de Corporación Luxor tomaron las medidas de contención que consideraron necesarias para impedir su propagación en el sistema y llevaron a cabo la restauración de los sistemas infectados por el ataque . Como resultado del análisis de malware, se ha identificado lo siguiente:

Adicionales:

* No se ha podido determinar inequívocamente la via de entrada del ataque debido a la ausencia de fuentes de datos clave que permita conocer el alcance completo del incidente.
* No obstante, planteo la siguiente hipótesis en base a las fuentes de información analizada.
  + Un usuario de la empresa quiso realizar la descarga de una aplicación , y en vez de descargar el ejecutable de esa App, descargo un ejecutable con un contenido malicioso.
  + Una vez realizada la descarga, este mismo se ejecuto trayendo aparejada la propagación del malware por el sistema. En este caso el malware es un ransonware , lo que produjo una inhabilitación total y la encriptación de la información.
  + Una vez ejecutado el ransonware se procedió a acceder a la utilidad VSSADMIN.exe para eliminar todas las copia de volúmenes presente en las computadoras. Esta utilidad requiere de privilegios administrativos para ejecutarse por lo cual seguramente al ejecutar el instalador se deben haber otorgado tales permiso.
  + A posterior se comenzó la ejecución de un archivo llamado HDa0Q8XU.exe con un total de 13 veces el cual fue descargado de forma automática. Se descargaron 2 archivos:
    - C:\Users\admin\AppData\Local\Temp\HDa0Q8XU.exe
    - C:\Users\admin\AppData\Local\Temp\lGwUImoN.exe

**Muestra analizada con Any.run**

|  |  |
| --- | --- |
| **NOMBRE DE LA MUESTRA** | Setup.exe |
| **FECHA DEL ANALISIS** | 28 de Septiembre 2022 22:04:49 |
| **OS UTILIZADO PARA ANALISIS** | Win 7 Professional Service Pack 1(build 7601, 32 bit) |
| **MD5** | E760739CCE7B7076793906A90F0EC9FF |

**Comportamiento**

**Texto, Tabla

Descripción generada automáticamente**

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**

**Informacion Estatica Encontrada**

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**

**Tabla

Descripción generada automáticamente con confianza media**

Tabla

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Captura de Pantalla de la Simulación**

**Interfaz de usuario gráfica

Descripción generada automáticamente**

Interfaz de usuario gráfica, Texto

Descripción generada automáticamenteInterfaz de usuario gráfica

Descripción generada automáticamente

**Diagrama de procesos de comportamiento**