Trabajo Final de Ciberseguridad

Alumno : Diaz Ricardo Exequiel.

**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

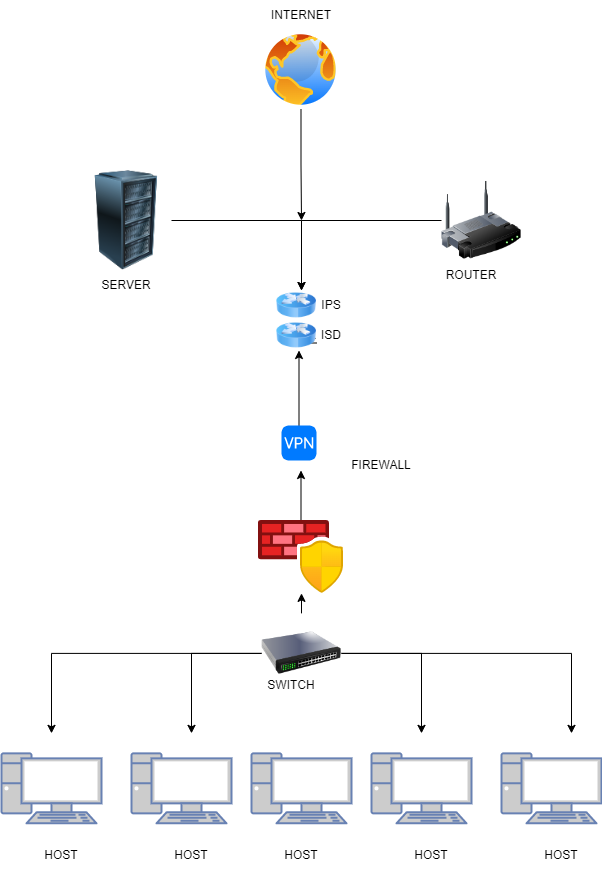
|  |  |
| --- | --- |
| **NOMBRE DE LA MUESTRA** | Setup.exe |
| **FECHA DEL ANALISIS** | 28 de Septiembre 2022 22:04:49 |
| **OS UTILIZADO PARA ANALISIS** | Win 7 Professional Service Pack 1(build 7601, 32 bit) |
| **MD5** | E760739CCE7B7076793906A90F0EC9FF |
| **NOMBRE DEL RAMSONWARE** | ShinoLocker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

**Muestra analizada.**

El Ransomware ShinoLocker tiene como objetivo la encriptación de información debido a esto es que se hace casi imposible recuperar esa información encriptada sin tener que abonar una suma de dinero o algún otro bien. Realizar el pago no siempre es un indicativo de que la persona que realizo la acción de la encriptación de la información nos vaya a dar la clave de desbloqueo. A raíz de este ataque sufrió al empresa Luxor en día 28 de Septiembre del 2022 es que se recomienda llevar a cabo las siguientes acciones.

* Fortalecer las medidas de seguridad de la red teniendo siempre actualizados los sistemas con los últimos parches de seguridad.
* implementar sistemas de detección de intrusos (IDS) con el fin de monitorear el trafico de datos que se transfieren entre redes publicas y privadas.
* Introducir también sistemas de prevención de intrusiones (IPS)con el fin de filtrar los paquetes de datos que se van a recibir o no.
* Colocar FIREWALL que sean capas de filtrar la información a las que los empleados de la empresa puedan acceder. Dar un manejo libre de internet a los empleados es un error siempre y cuando estas personas no estén capacitadas y sean capaces de diferenciar y concientizar de los problemas que pueden acarrear una manipulación errónea de la red.
* Realizar fuertes campañas de concientización con respecto a la ciberseguridad y la seguridad de la información. Instruir de forma periodica al personal con respecto a la importancia de una buena seguridad. Realizar ataque controlados durante el mes para ver si la capacitación brindada esta dando futos. Para obtener un resultado real es indispensable que nadie sepa del día ni la hora de ataque, ya que esto nos daría resultados negativos y el fin del ejercicio no serviría.
* Realizar un bloqueo mediante software de los puertos USB y que solo sean capas de leer información con la autorización de algún supervisor o del equipo técnico.
* Realizar una buena distribución de permisos de accesos y que una vez que ese personal quede desafectado de la empresa , esos permisos inmediatamente sean revocados.
* Algo muy importante es la entrega de equipos para el trabajo remoto. Realizar una formateo bit a bit para que el nuevo empleado no sea capas de levantar información sensible de la empresa. Por que hay que tener en cuenta quien fue el personal que utilizo ese ordenador antes y que puesto ocupaba dentro de la misma.
* Realizar backup de la información sensible de la empresa y mantenerla fuera del sistema ya que si en algún momento los activos se ven comprometidos por algún tipo de malware, este mismo sea incapaz de afectar a la copia de respaldo, esto permitirá aislar a el o los host infectados y luego de realizar una búsqueda de replicación del malware en el sistema , si todo es positivo poder levantar nuevamente y dejar todo funcionando.

**Conclusión.**

El mantenimiento de los sistemas como así también la capacitación del personal es optima para que un ecosistema funciones al cien por ciento. Estar siempre innovando con el hardware utilizado para tal fin es muy importante y entender que si la parte informática no va de la mano con el sector humano, es difícil que se pueda llegar a la excelencia en el trabajo.

‘QUIEN CONTROLA LOS DATOS, CONTROLA AL MUNDO’ Yuval Noah Harari.