Un investigador de seguridad cibernética de ESET publicó hoy un análisis de una nueva pieza de malware, una muestra que se detectó en el motor de escaneo de malware Virustotal y que se cree que el hacker detrás del malware esté probablemente interesado en algunas computadoras de alto valor protegidas detrás de redes con espacio de aire.

Apodado como *«Ramsay»,* el malware aún está en desarrollo con dos variantes más (v2.a y v2.b), detectadas en la naturaleza y todavía no parece ser un marco de ataque complejo basado en los detalles que el investigador compartió.

Sin embargo, se debe tener en cuenta que el malware en sí no aprovecha ninguna técnica extraordinaria o avanzada que pueda permitir a los atacantes saltar redes con espacio de aire para infiltrarse o exfiltrarse y obtener datos de las computadoras objetivo.

Según Ignacio Sanmillan, investigador de ESET, Ramsay se infiltra en las computadoras seleccionadas por medio de documentos maliciosos, potencialmente enviados a través de un correo electrónico de phishing o mediante una unidad USB, y luego explota una antigua vulnerabilidad de ejecución de código en Microsoft Office para apoderarse del sistema.

> *«Se encontraron varios casos de estos mismos documentos maliciosos cargados en motores de sandbox públicos, etiquetados como artefactos de prueba como access_test.docx o Test.docx que denotan un esfuerzo continuo para probar el vector de ataque específico»*, dijo el investigador.

El malware Ramsay se compone principalmente de dos funcionalidades principales:

- Recopilar todos los documentos de Word, archivos PDF y archivos ZIP existentes dentro del sistema de archivos del destino y almacenarlos en una ubicación predefinida en el mismo sistema directamente en una red o unidades extraíbles.
- Extendiéndose a otras computadoras que se utilizan dentro de la misma instalación aislada infectando todos los archivos ejecutables disponibles en una red compartida y unidades extraíbles.

Según el investigador, las muestras de Ramsay que encontraron no tienen un protocolo de comunicación C&C basado en la red, ni ningún intento de conectarse a un host remoto con fines de comunicación.

Aunque no se sabe cómo los atacantes deben filtrar datos de un sistema comprometido, el investigador especula que el malware podría haber sido *«adaptado para redes con espacio de aire»* con escenarios similares, considerando que la única opción que queda es el acceso físico a la máquina para robar los datos recopilados con un USB armado.

> *«Es importante notar que existe una correlación entre las unidades de destino que Ramsay escanea para la propagación y la recuperación de documentos de control»,* dijo el investigador de ESET.
>
> *«Esto evalúa la relación entre las capacidades de difusión y control de Ramsay que muestran cómo los operadores de Ramsay aprovechan el marco para el movimiento lateral, lo que denota la probabilidad de que este marco haya sido diseñado para operar dentro de redes con espacios de aire».*
>
> *«La visibilidad actual de los objetivos es baja, según la telemetría de ESET, se han descubierto pocas víctimas hasta la fecha. Creemos que esta escasez de víctimas refuerza la hipótesis de que este marco se encuentra en un proceso de desarrollo continuo, aunque la baja visibilidad de las víctimas también podría ser debido a la naturaleza de los sistemas específicos que se encuentran en redes con espacios de aire»*, agregó.

Aún así, debido a que el malware aún está en desarrollo, esta teoría sigue siendo una suposición general, también debido a la falta de evidencia técnica y estadística.

Sanmillan informó lo siguiente a The Hacker News:

> *«Solo tenemos una copia del agente Ramsay, que solo tiene código para agregar y comprimir los datos robados de una forma muy descentralizada y encubierta en el sistema de archivos local del host infectado. En base a esto, asumimos que otro componente es responsable de escanear el sistema de archivos, localizar los archivos comprimidos y realizar la exfiltración real».*

En cuanto al cuestionamiento acerca de que si el atacante debe confiar en el acceso físico para la filtración de datos, el investigador dijo:

> *«Existen distintas formas en que el atacante podría hacer esto. No hemos visto que se realice esta operación, sin embargo, tenemos algunas hipótesis sobre cómo el atacante podría hacer esto. Esas son solo nuestras suposiciones mejor educadas y la pura especulación en este momento, así que por favor trate esos dos escenarios hipotéticos como tales».*
>
> *«Escenario 1: Imagine el Sistema A, conectado a Internet y bajo el control total de los operadores de Ramsay, y el Sistema B, una computadora con espacio de aire infectado por el agente de Ramsay. Luego imagine a un usuario legítimo de esos sistemas ocasionalmente transfiriendo archivos entre ambos sistemas utilizando una unidad extraíble».*
>
> *«Cuando la unidad se inserta en el Sistema A, el atacante podría decidir colocar un archivo de control especial en la unidad extraíble que, cuando se conecta al Sistema B, haría que el agente Ramsey ejecute el exfiltrador Ramsay que se construiría para recuperar la puesta en escena, luego copiar los datos robados en la unidad extraíble para su posterior recuperación una vez que la unidad extraíble se*

> *conecte al Sistema A. Este escenario es una variación de cómo Sednit/APT28 operaba USBStealer».*
>
> *«USBStealer copió de forma sistemática los datos robados en la unidad extraíble utilizada entre el Sistema A y el Sistema B, mientras que Ramsay organiza los datos robados localmente para una futura exfiltración explícita».*
>
> *«Escenario 2: Imagine al agente de Ramsay ejecutándose por días o semanas en una red con espacio de aire, organizando en el sistema de archivos local todos los datos que se pueden encontrar en las unidades de red y todas las unidades extraíbles que se conectaron al sistema».*
>
> *«Entonces, en algún momento, el atacante decide que es tiempo de exfiltración. Tendría que obtener acceso físico al sistema infectado y obtener la ejecución del código para ejecutar el exfiltrador Ramsay, o en caso de que el sistema no tenga cifrado de disco completo, iniciar el sistema desde una unidad extraíble, montar el sistema de archivos, analizarlo y recuperar los datos robados organizados y salir».*
>
> *«Este escenario es más elaborado y requiere la presencia física de un operativo/cómplice, pero aún podría ser plausible ya que permitiría una operación muy rápida en el sitio».*

También se le preguntó al investigador si podría integrar el módulo de comunicación C&C remoto en futuras versiones, a lo que respondió que:

> *«Ramsay tiene una serie de funcionalidades comunes implementadas en sus versiones, que es el protocolo basado en el archivo de control y cómo se recuperan los artefactos involucrados en este protocolo de medios extraíbles y recursos*

> *compartidos de red».*
>
> *«Esto denota que la evaluación de estas técnicas se tuvo en cuenta al diseñar este malware, todo lo cual apunta a la implementación de capacidades para la operación sin la necesidad de ninguna conexión de red».*
>
> *«Parece que si los atacantes aprovecharan las técnicas que dependen de los artefactos de la red no se correlacionarían con la filosofía de este malware. De hecho, creemos que Ramsay puede estar en desarrollo, pero estamos muy inclinados a creer que no introducirán un componente de exfiltración en una red».*