Los hackers se han aprovechado de la propagación de SARS-COV-II (el virus), que causa COVID-19 (la enfermedad), como una oportunidad para propagar malware e iniciar ataques cibernéticos.

Reason Security lanzó un informe de análisis de amenazas que detalla un nuevo ataque que aprovecha el creciente deseo de los usuarios de Internet para obtener información sobre el nuevo coronavirus que está causando temor en todo el mundo.

El ataque de malware apunta de forma específica a quienes buscan presentaciones cartográficas de la propagación de COVID-19 en Internet, y los engaña para que descarguen y ejecuten una aplicación maliciosa que, en su interfaz, muestra un mapa cargado desde un archivo legítimo en línea, pero que finalmente compromete la computadora.

La última amenaza, diseñada para robar información de víctimas involuntarias, fue descubierta por primera vez por MalwareHunterTeam la semana pasada, y ahora fue analizada por Shai Alfasi, investigadora de seguridad cibernética en Reason Labs.

Se trata de un malware identificado como AZORult, un software malicioso que roba información y fue descubierto en 2016. El malware AZORult recopila información almacenada en navegadores web, particularmente cookies, historiales de navegación, ID de usuario, contraseñas e incluso claves de criptomonedas.

Con estos datos extraídos de los navegadores, los hackers pueden robar números de tarjetas de crédito, credenciales de inicio de sesión y otra información confidencial.

Según los informes, AZORult se discute en foros subterráneos rusos como una herramienta para recopilar datos confidenciales de las computadoras. Cuenta con una variante que es capaz de generar una cuenta de administrador oculta en las computadoras infectadas para permitir conexiones por medio del protocolo de escritorio remoto (RDP).

Análisis de muestra

Alfasi proporciona detalles técnicos sobre el estudio del malware, que está incrustado en el archivo, generalmente denominado *Corona-virus-Map.com.exe* y es un archivo Win 32 EXE con un tamaño de carga útil de solo 3.26 MB.

Al ejecutar el archivo, se abre una ventana que muestra información sobre la propagación de COVID-19. La pieza central es un *«mapa de infecciones»* similar al presentado por la Universidad Johns Hopkins, una fuente legítima en línea para visualizar y rastrear casos de coronavirus reportados en tiempo real.

El número de casos confirmados en diferentes países se presenta del lado izquierdo, mientras que las estadísticas sobre muertes y recuperaciones se encuentran a la derecha. La ventana parece ser interactiva, con pestañas para otra información relacionada y enlaces a fuentes.

Presenta una GUI convincente que no muchos creerían que es dañina. La información presentada no es un conjunto de datos aleatorios, sino información real de COVID-19 agrupada del sitio web de Johns Hopkins.

Cabe mencionar que el mapa original de coronavirus alojado en línea por la Universidad Johns Hopkins o ArcGIS, no está infectado ni ha retrocedido en ninguna forma, por lo que es seguro visitarlo.

El software malicioso utiliza algunas capas de empaque junto con una técnica de subproceso múltiple infundida para que sea difícil de detectar y analizar para los investigadores. Además, emplea un programador de tareas para que pueda seguir funcionando.

Signos de infección

La ejecución de *Corona-virus-Map.com.exe* tiene como resultado la creación de duplicados del archivo mencionado y múltiples Corona.exe, Bin.exe, Build.exe y

Windows.Globalization.FontGroups.module.exe, entre otros.

Además, el malware modifica un grupo de registros en ZoneMap y LanguageList, además de crear varios mutexes. La ejecución del malware activa los procesos antes mencionados, y luego intentan conectarse a distintas URL.

Estos procesos y URL son solo una muestra de lo que implica el ataque. Existen muchos otros archivos generados y procesos iniciados. Crean diversas actividades de comunicación de red a medida que el malware intenta recopilar diferentes tipos de información.

Alfasi presentó una cuenta detallada de cómo diseccionó el malware en una publicación de blog en Reason Security. Un detalle destacado es su análisis del proceso Bin.exe con Ollydbg. En consecuencia, el proceso describió algunas bibliotecas de enlaces dinámicos (DLL). El archivo DLL *«nss3.dll»* llamó su atención debido a que es algo que conocía de distintos actores.

Alfasi observó una carga estática de API asociadas con nss3.dll. Esas API parecen facilitar el descifrado de contraseñas almacenadas, así como la generación de datos de salida.

Este es un enfoque común utilizado por los ladrones de datos. Relativamente simple, solo captura los datos de inicio de sesión del navegador web infectado y los mueve a la carpeta C:\Windows\Temp.

Es uno de los sellos distintivos de un ataque AZORult, en el que el malware extrae datos, genera una identificación única de la computadora infectada, aplica el cifrado XOR y luego inicia la comunicación C2.

El malware realiza llamadas específicas en un intento de robar datos de inicio de sesión de cuentas en línea comunes como Telegram y Steam.

La ejecución del malware es el único paso necesario para que pueda seguir con sus procesos de robo de información. Las víctimas no necesitan interactuar con la ventana o ingresar información confidencial en ella.