El grupo de piratas informáticos detrás de la campaña de malware DNSpionage está llevando a cabo una nueva operación sofisticada que infecta a las víctimas seleccionadas con una nueva variante del malware DNSpionage.

Descubiertos por primera vez en noviembre del año pasado, los ataques de DNSpionage utilizaron sitios comprometidos y documentos maliciosos diseñados para infectar las computadoras de las víctimas con el malware, una herramientas administrativa remota personalizada que utiliza comunicación HTTP y DNS para comunicarse con el servidor de control y comando controlado por el atacante.

Según un nuevo informe publicado por el equipo de investigación de amenazas Talos de Cisco, el grupo adoptó algunas nuevas tácticas, técnicas y procedimientos para mejorar la eficacia de sus operaciones, haciendo que sus ataques cibernéticos sean más específicos, organizados y sofisticados.

A diferencia de las campañas anteriores, los atacantes ahora comenzaron a realizar reconocimientos en sus víctimas antes de infectarlos con una nueva pieza de malware, llamada Karkoff, lo que les permite elegir de forma selectiva qué objetivos infectar para permanecer sin detectar.

> *«Identificamos las superposiciones de infraestructura en los casos DNSpionage y Karkoff»,* dijeron los investigadores.

Durante la fase de reconocimiento, los atacantes recopilan información del sistema relacionada con el entorno de la estación de trabajo, el sistema operativo, el dominio y la lista de procesos en ejecución en la máquina de las víctimas.

> *«El malware busca dos plataformas antivirus específicas: Avira y Avast. Si uno de estos productos de seguridad está instalado en el sistema e identificado durante la fase de reconocimiento, se establecerá una marca específica, y algunas opciones*

> *del archivo de configuración serán ignoradas»,* agregaron.

Desarrollado en .NET, Karkoff permite a los atacantes ejecutar código arbitrario en hosts comprometidos de forma remota desde su servidor de C&C. Cisco Talos identificó a Karkoff como malware indocumentado a principios de este mes.

Algo interesante es que el malware Karkoff genera un archivo de registro en los sistemas de las víctimas que contiene una lista de todos los comandos que ha ejecutado con una marca de tiempo.

> *«Este archivo de registro se puede usar fácilmente para crear una línea de tiempo de la ejecución del comando que puede ser extremadamente útil cuando se responde a este tipo de amenaza. Con esto en mente, una organización comprometida con este malware tendría la oportunidad de revisar el archivo de registro e identificar los comandos ejecutados en su contra»,* dicen los expertos.

Al igual que la última campaña de DNSpionage, los ataques recientemente descubiertos también apuntan a la región del Medio Oriente, incluido el Líbano y los Emiratos Árabes Unidos.

Además de deshabilitar macros y usar software antivirus confiable, lo más importante es mantenerse alerta y mantenerse informado sobre las técnicas de ingeniería social para reducir el riesgo de ser víctima de tales ataques.

Debido a varios informes públicos de ataques de secuestro de DNS, el Departamento de Seguridad Nacional (DHS) de Estados Unidos, emitió a inicios de este año una *«directiva de emergencia»* a todas las agencias federales que ordenan al personal de TI que audite los registros de DNS para sus respectivos dominios de sitios web y otros administrados por agencias.