Microsoft informó este lunes que hackers patrocinados por el estado iraní han estado explotando la vulnerabilidad de Zerologon en campañas de piratería informática en la naturaleza.

Los ataques exitosos permitirían a los hackers hacerse cargo de los servidores conocidos como controladores de dominio (DC), que son pieza fundamental de la mayoría de redes empresariales y permitirían a los intrusos obtener control total sobre sus objetivos.

Los ataques iraníes fueron detectados por el Centro de Inteligencia de Amenazas de Microsoft (MSTIC), y han estado ocurriendo por al menos dos semanas, según informó la compañía.

MSTIC vinculó los ataques a un grupo de piratas informáticos iraníes que la compañías rastrea como MERCURY, pero que también son conocidos como MuddyWatter.

Parece ser que el grupo es contratista del gobierno iraní, que trabaja bajo órdenes del Cuerpo de la Guardia Revolucionaria Islámica, el servicio militar y de inteligencia principal de Irán.

Según el informe de Defensa Digital de Microsoft, este grupo históricamente se ha dirigido a ONG, organizaciones intergubernamentales, ayuda humanitaria del gobierno y organizaciones de derechos humanos.

No obstante, Microsoft afirma que los objetivos más recientes de Mercury incluyen *«un gran número de objetivos involucrados en el trabajo con refugiados y proveedores de tecnología de red en el Medio Oriente».*

Zerologon se ha descrito como el error más peligroso revelado este año. La vulnerabilidad reside en Netlogon, el protocolo utilizado por los sistemas Windows para autenticarse en un servidor Windows que se ejecuta como controlador de dominio.

La explotación de Zerologon puede permitir a los hackers hacerse cargo de un controlador de dominio sin parches, y de forma inherente, la red interna de una empresa.

Los ataques por lo general, se llevan a cabo en redes internas, pero si el controlador de dominio está expuesto en línea, también se pueden realizar de forma remota por Internet.

Microsoft emitió parches para Zerologon (CVE-2020-1472) en agosto, pero el primer artículo detallado sobre el error fue publicado en septiembre, retrasando la mayoría de los ataques.

Mientras los investigadores de seguridad cibernética retrasaron la publicación de los detalles para dar a los administradores de sistemas más tiempo para instalar los parches, el código de prueba de concepto creado para Zerologon se publicó casi el mismo día que el informe detallado, lo que provocó una ola de ataque en pocos días.

Luego de la divulgación del error, el DHS dio a las agencias federales tres días para parchear los controladores de dominio o desconectarlos de las redes federales, con el fin de evitar ataques, que la agencia esperaba que ocurrieran, y así fue unos días después.

Los ataques de Mercury parecen haber comenzado alrededor de una semana después de la publicación del código de prueba de concepto, y aproximadamente al mismo tiempo, Microsoft comenzó a detectar los primeros intentos de explotación de Zerologon.