La Agencia de Seguridad Nacional de Estados Unidos (NSA), publicó este martes una alerta de seguridad sobre una nueva ola de ataques cibernéticos contra servidores de correo electrónico, realizados por una de las unidades de espionaje cibernético más avanzadas de Rusia.

La NSA afirma que los miembros de la Unidad 74455 del Centro Principal de Tecnologías Especiales GRU (GTsST), una división del servicio de inteligencia militar ruso, han estado llevando a cabo ataques a servidores de correo electrónico que ejecutan el agente de transferencia de correo Exim (MTA).

También conocido como *«Sandworm»*, este grupo ha estado pirateando servidores Exim desde agosto de 2019, al explotar una vulnerabilidad identificada como CVE-2019-10149, dijo la NSA en una alerta de seguridad.

> *«Cuando Sandworm explotó CVE-2019-10149, la máquina víctima posteriormente descargaría y ejecutaría un script de shell desde un dominio controlado por Sandworm»,* dijo la NSA.

El script de shell puede ejecutar acciones como:

- Agregar usuarios privilegiados
- Deshabilitar la configuración de seguridad de red
- Actualizar las configuraciones de SSH para permitir el acceso remoto adicional
- Ejecutar un script adicional para permitir la explotación de seguimiento

La NSA advierte a las organizaciones privadas y gubernamentales que actualicen sus servidores Exim a la versión 4.93 y busquen signos de compromiso. Los indicadores de compromiso están disponibles en el documento de la NSA.

El grupo Sandworm ha estado activo desde 2005 aproximadamente, y se cree que es el grupo de hackers responsable del desarrollo del malware BlackEnergy, que causó un apagón

en Ucrania en diciembre de 2015 y diciembre de 2016, y también, serían los desarrolladores del ransomware NotPetya que causó daños por miles de millones de dólares a empresas de todo el mundo.

Actualmente se considera como uno de los grupos de hackers más avanzados patrocinados por el estado ruso, junto con Turla.

La vulnerabilidad CVE-2010-10149 se reveló en junio de 2019 y recibió el nombre en código *«Return of the WIZard».* Una semana después de revelarse, los grupos de piratas informáticos comenzaron a explotarla.

Luego de dos semanas, Microsoft también emitió una alerta, advirtiendo a los clientes de Azure que un actor de amenazas había desarrollado un gusano autoexpandible en Exim, que explotaba la vulnerabilidad para hacerse cargo de los servidores que se ejecutan en la infraestructura de Azure.

Casi la mitad de los servidores de correo electrónico de Internet funcionan con Exim. Según las estadísticas del 1 de mayo de 2020, solo la mitad de todos los servidores Exim se han actualizado a la versión 4.93 o posterior, dejando muchas instancias de Exim expuestas a ataques.

> *«Muchas organizaciones se fijan en lo nuevo y brillante, como la nube y los dispositivos móviles. Sin embargo, olvidan que los servicios realmente antiguos como SMTP tienen una gran parte de su vida personal y comercial, y por definición esos servicios están expuestos a Internet»*, dijo Richard Bejtlich, estratega de seguridad principal de la compañía Corelight.
>
> *«Se convierten en objetivos perfectos para los adversarios cuando se enfrentan a Internet, manejan los datos más confidenciales y las personas los tratan como dispositivos, lo que significa que a menudo se olvidan siempre que siguen trabajando y no son monitoreados»*, agregó.

Este aviso de la NSA llama mucho la atención sobre las operaciones de ciberespionaje de Rusia. Muchas de las operaciones rusas por lo general cruzan una línea de lo que es aceptable en la reunión de ciberinteligencia moderna al causar problemas en el mundo real (como es el caso de NotPetya, BadRabbit, BlackEnergy, etc.).