Un investigador de seguridad cibernética que buscaba recompensas de errores, descubrió el mes pasado que una red de bots de minería de criptomonedas estaba dentro de un servidor web operado por el Departamento de Defensa de Estados Unidos (DOD).

El problema fue descubierto e informado por medio del programa oficial de recompensas de errores del DOD, por el investigador indio Nitesh Surana.

En un principio, el informe de error se archivó en relación con un servidor de automatización Jenkins mal configurado, que se ejecuta en un servidor de Amazon Web Services (AWS) asociado con un dominio DOD.

Surana descubrió que cualquiera podía acceder al servidor Jenkins sin credenciales de inicio de sesión. Aparentemente, el acceso completo era posible, aún al sistema de archivos. El investigador asegura que la carpeta /script, parte de la instalación de Jenkins, también estaba abierta para cualquiera.

Esta carpeta es donde los usuarios cargan archivos que el servidor Jenkins lee y ejecuta de forma automática a intervalos regulares.

Surana informó al Departamento de Defensa que un hacker podría cargar archivos maliciosos dentro de esa carpeta e instalar una puerta trasera permanente o hacerse cargo de todo el servidor.

El DOD aseguró el servidor vulnerable, pero al revisar sus hallazgos, Suranta también se percató de que el servidor Jenkins ya había sido comprometido antes de eso.

El investigador mencionó que rastreó las pistas que encontró sobre una operación de malware especializada en hackear servidores en la nube e instalar malware para minar Monero.

ZDNet informa que la dirección de billetera de Monero asociada a la botnet, muestra decenas de menciones en los motores de búsqueda desde agosto de 2018.

La mayoría de las menciones son de usuarios chinos, que informaron haber encontrado un minero de Monero en sus servidores en la nube.

Con el servicio XMRHunter, se descubrió que la dirección de Monero actualmente tiene 35.4 monedas de XMR, con un valor de poco más de 2700 dólares. Sin embargo, los fondos anteriores podrían haberse retirado a otras cuentas a intervalos regulares, por lo que no se puede estimar con precisión la operación de la botnet solo en esa dirección.

Surana informó sus hallazgos mediante el Programa Oficial de Recompensas de Errores del DOD, alojado en la plataforma HackerOne.

La unidad más reciente de búsqueda de errores del DOD finalizó el mes pasado, en la que el departamento pagó 275 mil dólares a los investigadores de seguridad cibernética por su trabajo en la búsqueda de errores en los servidores web relacionados con el Ejército de Estados Unidos.

Debido a la naturaleza sensible de la infraestructura DOD, el informe de Surana fue redactado para eliminar el nombre y la URL del servidor DOD que se vio comprometido por la botnet de extracción de monedas.