Durante la última semana, muchas supercomputadoras en Europa se infectaron con malware de minería de criptomonedas y tuvieron que ser cerradas para investigar las intrusiones.

Se informaron incidentes de seguridad en el Reino Unido, Alemania y Suiza, mientras que también existen rumores de intrusión similar en un centro de cómputo de alto rendimiento en España.

El primer informe de un ataque se dio a conocer el lunes, por parte de la Universidad de Edimburgo, que dirige la supercomputadora ARCHER. La organización mencionó que se registró una *«explotación de seguridad en los nodos de inicio de sesión de ARCHER»,* por lo que apagaron el sistema ARCHER para investigar y restablecer las contraseñas SSH para evitar más intrusiones.

El bwHPC, la organización responsable de la coordinación de proyectos de investigación en supercomputadoras en el estado de Baden-Württemberg, Alemania, también anunció el lunes que cinco de sus clústeres informáticos de alto rendimiento tuvieron que cerrarse debido a *«incidentes de seguridad»* similares, incluyendo:

- La supercomputadora Hawk en el Centro de Computación de Alto Rendimiento de Stuttgart (HLRS) en la Universidad de Stuttgart
- Los grupos bwUniCluster 2.0 y ForHLR II en el Instituto de Tecnología de Karlsruhe (KIT)
- La supercomputadora bwForcluster JUSTUS de química y ciencia cuántica en la Universidad de Ulm
- La supercomputadora de bioinformática bwForCluster BinAC en la Universidad de Tübingen

Los informes siguieron el miércoles cuando el investigador de seguridad Felix Von Leither afirmó en una publicación que una supercomputadora alojada en Barcelona, España, también se vio afectada por un problema de seguridad, y como resultado, se cerró.

Otros incidentes se dieron a conocer al día siguiente. El primero provino del Leibniz

Computing Center (LRZ), un instituto de la Academia de Ciencias de Baviera, que dijo que se desconectó un clúster informático de Internet luego de una violación de seguridad.

Después de ese anuncio, otro informe del Centro de Investigación Julich en Alemania, declaró por parte de las autoridades que se tuvieron que cerrar las supercomputadoras JURECA, JUDAC y JUWELS después de un *«incidente de seguridad de TI».*

Finalmente, este sábado se dieron a conocer nuevas violaciones de seguridad. El científico alemán Robert Helling publicó un análisis acerca del malware que infectó el clúster informático de alto rendimiento en la Facultad de Física de la Universidad Ludwig-Maximilians en Munich, Alemania.

El Centro Suizo de Computación Científica (CSCS) en Zurich, Suiza, también cerró el acceso externo a su infraestructura de supercomputadora después de un *«incidente cibernético hasta que se haya restaurado un entorno seguro».*

Los hackers obtuvieron acceso a través de inicios de sesión SSH

Ninguna de las organizaciones anteriores publicó ningún detalle sobre las intrusiones. Sin embargo, este sábado, el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) para la Infraestructura de Red Europea (EGI), una organización paneruopea que coordina la investigación sobre supercomputadoras en Europa, publicó muestras de malware e incidentes de compromiso de red de algunos de estos incidentes.

Las muestras de malware fueron revisadas hoy por Cado Security, una compañía de seguridad cibernética con sede en Estados Unidos. La compañía dijo que los atacantes parecen haber obtenido acceso a los grupos de supercomputadoras por medio de credenciales SSH comprometidas.

Las credenciales parecen haber sido robadas de los mienbros de la universidad a quienes se

les brindó acceso a las supercomputadoras para ejecutar trabajos informáticos. Los inicios de sesión secuestrados de SSH pertenecían a universidades de Canadá, China y Polonia.

Chris Doman, cofundador de Cado Security, dijo a ZDNet que aunque no existe evidencia oficial para confirmar que todas las intrusiones fueron realizadas por el mismo grupo, la evidencia como nombres de archivos de malware similares e indicadores de red sugieren que podría ser el mismo actor de la amenaza.

Según el análisis de Doman, una vez que los atacantes obtuvieron acceso a un nodo de supercomputación, utilizaron un exploit para la vulnerabilidad CVE-2019-15666, para obtener acceso a la raíz y luego implementar una aplicación que extraía la criptomoneda Monero (XMR).

Algo que empeora todo, es que muchas de las organizaciones que tenían supercomputadoras activas, anunciaron esta semana que estaba priorizando la investigación sobre el brote de COVID-19, que ahora probablemente ha sido obstaculizado como resultado de la intrusión y el tiempo de inactividad posterior.