Investigadores de seguridad cibernética descubrieron un nuevo troyano de acceso remoto (RAT) para Linux, que emplea una técnica de sigilo nunca antes vista que implica enmascarar sus acciones maliciosas programándolas para su ejecución el 31 de febrero, un día calendario que no existe.

Apodado como CronRAT, el malware furtivo *«permite el robo de datos Magecart del lado del servidor, que pasa por alto las soluciones de seguridad basadas en navegador»*, dijo Sansec Threat Research. La compañía de seguridad cibernética holandesa dijo que encontró muestras del RAT en varias tiendas online.

La característica más destacada de CronRAT es su capacidad para aprovechar la utilidad de programación de trabajos con para Unix, para ocultar cargas útiles maliciosas utilizando nombres de tareas programadas para ejecutarse el 31 de febrero.

Esto no solo permite que el malware eluda la detección de software de seguridad, sino que también le permite lanzar una serie de comandos de ataque que podrían poner en riesgo los servidores de comercio electrónico de Linux.

> *«CronRAT agrega una serie de tareas a crontab con una curiosa especificación de fecha: 52 23 31 23. Estas líneas son sintácticamente válidas, pero generarían un error de tiempo de ejecución cuando se ejecutan. Sin embargo, esto nunca sucederá ya que están programadas para ejecutarse el 31 de febrero»,* dijeron los investigadores.

El RAT, un *«programa Bash sofisticado»,* también utiliza muchos niveles de ofuscación para dificultar el análisis, como colocar código detrás de las barreras de codificación y compresión, e implementar un protocolo binario personalizado con sumas de verificación aleatorias para pasar los firewalls y los inspectores de paquetes, antes de establecer comunicaciones con un servidor de control remoto para esperar instrucciones adicionales.

Armados con este acceso de puerta trasera, los atacantes asociados con CronRAT pueden

ejecutar cualquier código en el sistema comprometido, agregaron los investigadores.

> *«El skimming digital se está moviendo del navegador al servidor y este es otro ejemplo. La mayoría de las tiendas en línea solo han implementado defensas basadas en navegador, y los delincuentes aprovechan el back-end desprotegido. Los profesionales de seguridad realmente deberían considerar la superficie de ataque completa»,* dijo el Director de Investigación de Amenazas de Sansec, Willem de Groot.