Se ha observado que al menos la mitad de una docena de cuentas de GitHub de investigadores falsos asociados con una empresa de seguridad cibernética fraudulenta introducen repositorios maliciosos en el servicio de alojamiento de código.

Los siete repositorios, que aún están disponibles hasta ahora, afirman ser un exploit de prueba de concepto (PoC) para supuestas vulnerabilidades de día cero en Discord, Google Chrome y Microsoft Exchange Server.

VulnCheck, que descubrió la actividad, dijo: *«Las personas que crean estos repositorios han hecho un gran esfuerzo para que parezcan legítimos mediante la creación de una red de cuentas y perfiles de Twitter, fingiendo ser parte de una empresa inexistente llamada High Sierra Cyber Security».*

La compañía de seguridad cibernética dijo que se encontró por primera vez con los repositorios deshonestos a principios de mayo cuando se observó que lanzaban exploits PoC similares para errores de día cero en Signal y WhatsApp. Desde entonces, los dos repositorios fueron eliminados.

Además de compartir algunos de los supuestos hallazgos en Twitter en un intento de generar legitimidad, se descubrió que el conjunto de cuentas usa fotografías de investigadores de seguridad reales de compañías como Rapid7, lo que sugiere que los hackers han hecho todo lo posible para ejecutar la campaña.

El PoC es un script de Python que está diseñado para descargar un binario malicioso y ejecutarlo en el sistema operativo de la víctima, ya sea Windows o Linux.

La lista de repositorios de GitHub y cuentas de Twitter falsas es la siguiente:

- github.com/AKuzmanHSCS/Microsoft-Exchange-RCE
- github.com/BAdithyaHSCS/Exchange-0-Day
- github.com/DLandonHSCS/Discord-RCE
- github.com/GSandersonHSCS/discord-0-day-fix

- github.com/MHadzicHSCS/Chrome-0-day
- github.com/RShahHSCS/Discord-0-Day-Exploit
- github.com/SsankkarHSCS/Chromium-0-Day
- twitter.com/AKuzmanHSCS
- twitter.com/DLandonHSCS
- twitter.com/GSandersonHSCS
- twitter.com/MHadzicHSCS

> *«El atacante ha hecho un gran esfuerzo para crear todas estas personas falsas, solo para entregar un malware muy obvio. No está claro si han tenido éxito, pero dado que han seguido con esta vía de ataques, parece que creen que tendrán éxito»,* dijo el investigador de VulnCheck, Jacob Baines.

Actualmente no se sabe si se trata del trabajo de un actor aficionado o de una amenaza persistente avanzada (APT). Pero los investigadores de seguridad han pasado previamente bajo el radar de los grupos de estados-nación de Corea del Norte, como lo reveló Google en enero de 2021.

En todo caso, los hallazgos muestran la necesidad de tener precaución cuando se trata de descargar código de repositorios de código abierto. También es esencial que los usuarios analicen el código antes de ejecutarlo para asegurarse de que no represente ningún riesgo de seguridad.