En la más reciente evolución de cómo los actores de amenazas han empezado a utilizar infraestructura legítima con fines maliciosos, nuevos hallazgos revelan que grupos de piratería respaldados por estados nacionales han incursionado en el aprovechamiento de la plataforma social para atacar infraestructuras críticas.

En los últimos años, Discord se ha convertido en un objetivo atractivo, al servir como un lugar fértil para alojar malware utilizando su red de entrega de contenido (CDN) y permitiendo a los ladrones de información extraer datos sensibles de la aplicación, además de facilitar la extracción de datos mediante webhooks.

> *«El uso de Discord generalmente se limita a aquellos que buscan robar información y a quienes recopilan datos, y estas herramientas están disponibles para cualquiera en Internet»,* informaron los investigadores de Trellix, Ernesto Fernández Provecho y David Pastor Sanz, en un informe publicado el lunes.

Sin embargo, esto podría estar cambiando, ya que la empresa de ciberseguridad ha encontrado pruebas de un artefacto dirigido a infraestructuras críticas en Ucrania. Hasta el momento, no se ha encontrado evidencia que lo vincule con algún grupo de amenazas conocido.

> *«La potencial aparición de campañas de malware de APT que explotan las funcionalidades de Discord agrega un nuevo nivel de complejidad al panorama de amenazas»,* destacaron los investigadores.

La muestra es un archivo de Microsoft OneNote que se distribuye a través de un mensaje de correo electrónico que se hace pasar por la organización sin fines de lucro dobro.ua.

Una vez que se abre el archivo, contiene referencias a soldados ucranianos con el fin de engañar a los destinatarios y lograr que realicen donaciones al hacer clic en un botón

trampa, lo que resulta en la ejecución de un script de Visual Basic (VBS) diseñado para extraer y ejecutar un script de PowerShell que descarga otro script de PowerShell desde un repositorio en GitHub.

En la etapa final, PowerShell aprovecha un webhook de Discord para extraer metadatos del sistema.

> *«El hecho de que el único objetivo de la carga final sea obtener información sobre el sistema indica que la campaña todavía se encuentra en una etapa temprana, lo que también concuerda con el uso de Discord como [centro de control y comando]»*, señalaron los investigadores.

> *«Sin embargo, es importante destacar que el atacante podría entregar un malware más sofisticado a los sistemas comprometidos en el futuro mediante la modificación del archivo almacenado en el repositorio de GitHub».*

El análisis de Trellix también reveló que cargadores como SmokeLoader, PrivateLoader y GuLoader se encuentran entre las familias de malware más comunes que utilizan la CDN de Discord para descargar una carga de siguiente etapa, que incluye ladrones de información como RedLine, Vidar, Agent Tesla y Umbral.

Además, se han observado algunas de las familias de malware más frecuentes que utilizan webhooks de Discord, como Mercurial Grabber, Stealerium, Typhon Stealer y Venom RAT.

> *«El abuso de la CDN de Discord como mecanismo de distribución para cargas de malware adicionales muestra la capacidad de los ciberdelincuentes para adaptarse y aprovechar aplicaciones colaborativas en su beneficio»,* afirmaron los investigadores.

> *«Las APT son conocidas por sus ataques sofisticados y dirigidos, y al infiltrarse en plataformas de comunicación ampliamente utilizadas como Discord, pueden establecer eficazmente posiciones sólidas a largo plazo dentro de las redes, poniendo en riesgo infraestructuras críticas y datos sensibles».*