Un grupo de hackers probablemente con sede en Rumania y activo desde al menos 2020, ha estado detrás de una campaña de criptojacking activa dirigida a máquinas basadas en Linux con fuerza bruta SSH previamente indocumentada escrita en Golang.

Nombrada como Diicot Brute, la herramienta de descifrado de contraseñas se distribuye a través de un modelo de software como servicio, y cada actor de amenazas proporciona sus propias claves API únicas para facilitar las intrusiones, según informaron los investigadores de Bitdefender en un informe publicado la semana pasada.

Aunque el objetivo de la campaña es implementar el malware de minería Monero comprometiendo de forma remota los dispositivos por medio de ataques de fuerza bruta, los investigadores conectaron a la pandilla a al menos dos redes de bots DDoS, incluida una variante de Demonbot llamada chernobyl y un bot de IRC de Perl, con XMRig, una carga útil de minería alojada en un dominio llamado mexalz[.]us desde febrero de 2021.

La compañía rumana de tecnología de seguridad cibernética dijo que comenzó su investigación sobre las actividades cibernéticas del grupo en mayo de 2021, lo que llevó al posterior descubrimiento de la infraestructura del ataque y el kit de herramientas del adversario.

El grupo también es conocido por confiar en una variedad de trucos de ofuscación que les permiten pasar desapercibidos. Con este fin, los scripts de Bash se compilan con un compilador de scripts de shell (shc), y se descubrió que la cadena de ataque aprovecha Discord para informar a un canal bajo su control, siendo esta una técnica que se ha vuelto cada vez más común entre los actores maliciosos para comunicaciones de mando y control y evadir la seguridad.

El uso de Discord como plataforma de exfiltración de datos también elimina la necesidad de que los actores de amenazas alojen su propio servidor de comando y control, sin mencionar la habilitación del soporte para crear comunidades centradas en la compra y venta de código fuente y de servicios de malware.

> *«Los hackers que buscan credenciales SSH débiles no son infrecuentes. Entre los mayores problemas de seguridad se encuentran los nombres de usuario y contraseñas predeterminados, o las credenciales débiles que los piratas informáticos pueden superar fácilmente con la fuerza bruta. La parte complicada no es necesariamente forzar esas credenciales, sino hacerlo de una forma que permite que los atacantes pasen desapercibidos»,* dijeron los investigadores.