Se detectó a un grupo de amenazas no identificado hasta ahora, que emplea un cargador de malware *«complejo y poderoso»* con el objetivo final de implementar mineros de criptomonedas en sistemas comprometidos y facilitar potencialmente el robo de tokens de Discord.

> *«La evidencia encontrada en las redes de las víctimas parece indicar que el objetivo del atacante era instalar software de minería de criptomonedas en las máquinas de las víctimas»,* dijeron los investigadores del Symantec Threat Hunter Team, parte de Broadcom Software.

> *«Esto parecería ser un objetivo de recompensa relativamente baja para el atacante dado el nivel de esfuerzo que se habría requerido para desarrollar este sofisticado malware»,* agregaron.

Se cree que esta pieza avanzada de malware, denominada Verblecon, se detectó por primera vez hace dos meses, en enero de 2022, y la carga útil incorporó cualidades polimórficas para evadir las detecciones basadas en firmas por parte del software de seguridad.

Además, el cargador realiza más comprobaciones anti análisis para determinar si actualmente se está depurando o abriendo en un entorno virtual o de espacio aislado, antes de proceder a copiarse en la máquina y conectarse a un servidor remoto para recuperar un blob cifrado que contiene un URL, que luego se utiliza para obtener las cargas útiles del minero.

> *«La actividad que hemos visto llevar a cabo usando este cargador sofisticado indica que está siendo manejado por un individuo que puede no darse cuenta de las capacidades del malware que está usando»*, dijeron los investigadores.

> *«Sin embargo, si cae en manos de un actor más sofisticado, existe la posibilidad de que este cargador se utilice para ataques más graves, incluidas campañas de espionaje y ransomware»,* agregaron.