Se descubrió una nueva campaña de malware dirigida a los usuarios de criptomonedas, tokens no fungibles (NFT) y DeFi, por medio de los canales de Discord para implementar un criptográfico llamado Babadeda, que es capaz de eludir las soluciones antivirus y realizar varios ataques.

*«El instalador de malware se ha utilizado en una variedad de campañas recientes para ofrecer ladrones de información, RAT e incluso el ransomware LockBit»,* dijeron los investigadores de Morphisec. Se cree que los ataques de distribución de malware comenzaron en mayo de 2021.

Los cifradores son un tipo de software utilizado por los hackers que pueden cifrar, ofuscar y manipular códigos maliciosos para que parezcan inocuos y dificulten su detección por parte de los programas de seguridad.

Las infiltraciones observadas por Morphisec involucraron al atacante enviando mensajes señuelo a posibles usuarios en los canales de Discord relacionados con juegos basados en blockchain como Mines of Dalarnia, instándolos a descargar una aplicación.

Si una víctima hace clic en una URL incrustada en el mensaje, se dirige a la persona a un dominio de phishing diseñado para parecerse al sitio web legítimo del juego e incluye un enlace a un instalador malicioso que contiene el criptográfico Babadeda.

Luego de la ejecución, el instalador desencadena una secuencia de infección que decodifica y ejecuta la carga útil cifrada, en este caso BitRAT y Remcos, para recopilar información valiosa.

Morphisec atribuyó los ataques a un actor de amenazas de un país de habla rusa, debido al texto en ruso que se observa en uno de los sitios de señuelo. Hasta ahora se han identificado hasta 84 dominios maliciosos, creados entre el 24 de julio de 2021 y el 17 de noviembre de

2021.

> *«Dirigirse a los usuarios de criptomonedas por medio de vectores de ataque confiables les da a sus distribuidores una selección de víctimas potenciales de rápido crecimiento. Una vez en la máquina de la víctima, hacerse pasar por una aplicación conocida con una ofuscación compleja también significa que en cualquiera que confíe en el malware basado en firmas no tiene forma de saber que Babadeda está en su máquina, o de detener su ejecución»,* dijeron los investigadores.