Un actor de amenazas no identificado fue vinculado a un conjunto de herramientas de malware en desarrollo activo llamado *«Eternity Project»*, que permite a los hackers la compra de ladrones, cortadores, gusanos, mineros, ransomware y un bot de denegación de servicio distribuido (DDoS).

Lo que hace que este malware como servicio (MaaS) se destaque es que además de utilizar un canal de Telegram para comunicar actualizaciones sobre las funciones más recientes, también emplea un Bot de Telegram que permite a los controladores construir el binario.

> *«Los atacantes brindan una opción en el canal de Telegram para personalizar las funciones binarias, lo que proporciona una forma efectiva de crear binario sin dependencias»,* dijeron los investigadores de Cyble.

Cada uno de los módulos se puede arrendar de forma separada y brinda acceso pago a una amplia variedad de funciones:

- Eternity Stealer ($260 por suscripción anual): Extrae contraseñas, cookies, tarjetas de crédito, extensiones de criptomonedas del navegador, billeteras criptográficas, clientes VPN y aplicaciones de correo electrónico de la máquina de la víctima y las envía al Bot de Telegram.
- Eternity Miner ($90 por suscripción anual): Abusa de los recursos informáticos de una máquina comprometida para extraer criptomonedas.
- Eternity Clipper ($110): Un programa de criptografía que roba criptomonedas durante una transacción al sustituir la dirección de la billetera original guardada en el portapapeles con la dirección de la billetera del atacante.
- Eternity Ransomware ($490): Un ejecutable de ransomware de 130 kb para cifrar todos los archivos de los usuarios hasta que se pague un rescate.
- Eternity Worm ($390): Un malware que se propaga a través de unidades USB, redes locales compartidas, archivos locales y mensajes de spam transmitidos en Discord y Telegram.
- Eternity DDoS Bot (N/A): Se dice que la característica está actualmente en desarrollo.

Cyble también dijo que hay indicios de que los autores de malware pueden estar reutilizando el código existente relacionado con DynamicStealer, que está disponible en GitHub, y comerciándolo con un nuevo nombre para obtener ganancias.

Cabe mencionar que Jester Stealer, otro malware que salió a la luz en febrero de 2022 y desde entonces se ha utilizado en ataques de phishing contra Ucrania, también usa el mismo repositorio de GitHub para descargar proxies TOR, lo que indica posibles vínculos entre los dos actores de amenazas.

La compañía de ciberseguridad también mencionó que *«ha observado un aumento significativo en los delitos cibernéticos a través de los canales de Telegram y los foros de delitos cibernéticos donde [los actores de amenazas] venden sus productos sin ninguna regulación».*

La semana pasada, BlackBerry expuso el funcionamiento interno de un troyano de acceso remoto llamado DCRat (también conocido como DarkCrystal RAT) que está disponible para la venta a precios económicos en foros rusos de piratería y utiliza un canal de Telegram para compartir detalles sobre actualizaciones de software y complementos.