Un reciente troyano de acceso remoto (Remote Access Trojan, RAT) conocido como QwixxRAT está siendo promocionado para su venta por parte de su actor de amenazas a través de las plataformas de Telegram y Discord.

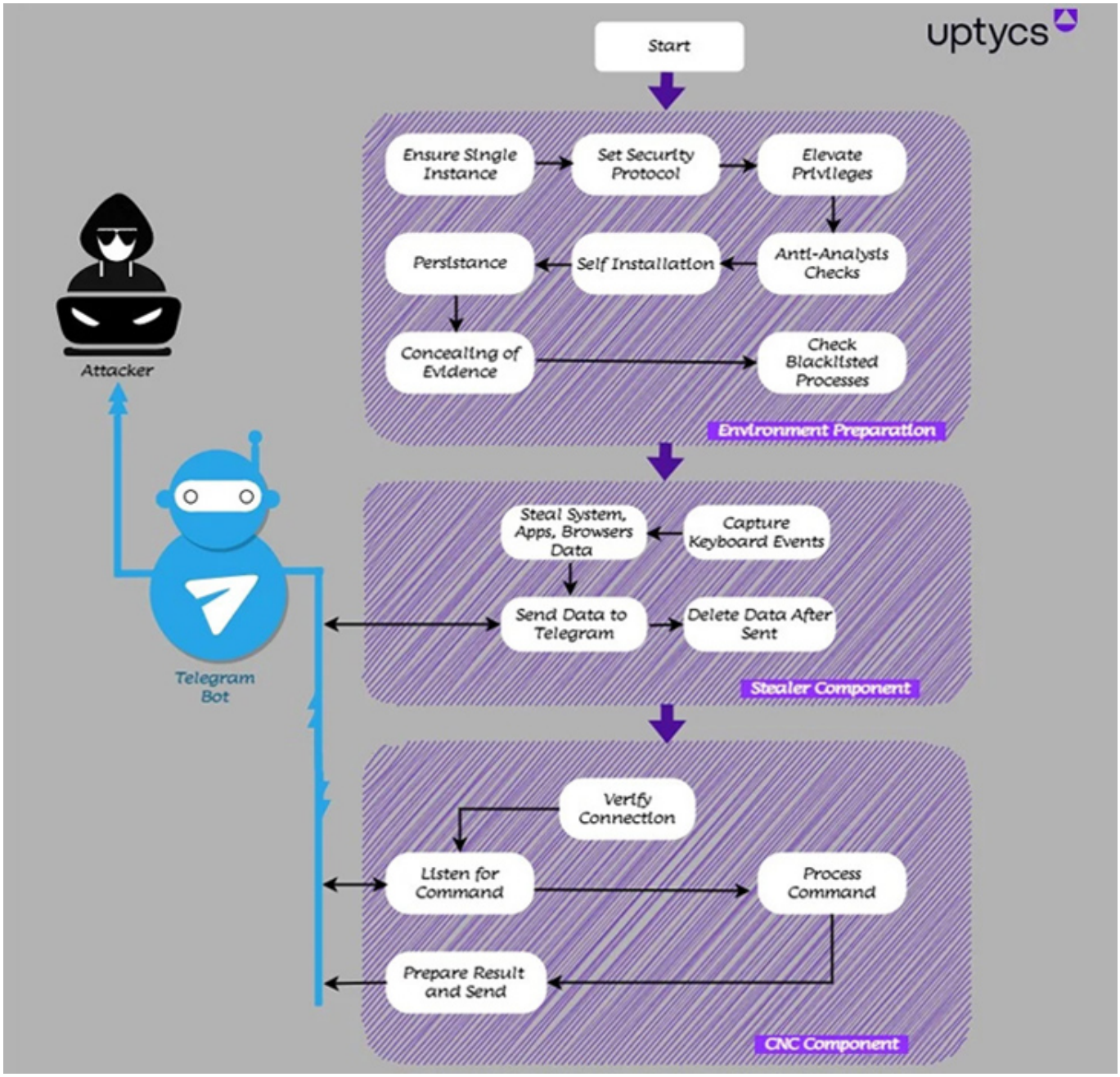
> *«Una vez que se instala en las computadoras con sistema operativo Windows de las víctimas, el RAT recopila de manera sigilosa datos sensibles, los cuales son posteriormente enviados al bot de Telegram del atacante, otorgándoles acceso no autorizado a la información confidencial de la víctima»,* reportó Uptycs en un nuevo informe publicado hoy.

La compañía de ciberseguridad, la cual descubrió el malware a principios de este mes, señala que ha sido *«cuidadosamente diseñado»* para recolectar historiales de navegación web, marcadores, cookies, información de tarjetas de crédito, pulsaciones de teclas, capturas de pantalla, archivos que tengan ciertas extensiones y datos de aplicaciones como Steam y Telegram.

Esta herramienta se ofrece por 150 rublos para acceder durante una semana y por 500 rublos para una licencia de por vida. También existe una versión gratuita y limitada disponible.

Desarrollado en C#, QwixxRAT cuenta con diversas características anti-análisis para mantenerse oculto y evadir la detección. Esto incluye una función de pausa para introducir un retraso en el proceso de ejecución, así como verificaciones para determinar si está funcionando dentro de un entorno de pruebas o virtual.

Otras funciones le permiten monitorear una lista específica de procesos (como «taskmgr», «processhacker», «netstat», «netmon», «tcpview» y «wireshark»), y si alguno de estos es detectado, detiene su propia actividad hasta que el proceso sea terminado.



También incluido en QwixxRAT se encuentra un clipper que de manera furtiva accede a información delicada que ha sido copiada al portapapeles del dispositivo, con el propósito de llevar a cabo transferencias de fondos ilícitas desde billeteras de criptomonedas.

La comunicación y el control (C2) se realizan a través de un bot en Telegram, mediante el cual se envían órdenes para llevar a cabo recopilación adicional de datos, como grabaciones de audio y video desde la cámara web, e incluso para apagar o reiniciar de forma remota el dispositivo infectado.

Esta revelación se produce semanas después de que Cyberint diera a conocer detalles de otras dos variantes de RAT llamadas RevolutionRAT y Venom Control RAT, las cuales también son anunciadas en varios canales de Telegram con características de extracción de datos y conectividad C2.