DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°190**	**Fecha: 14-08-2023** **Página: 6 de 13**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nuevo troyano de acceso remoto "QwixxRAT" en venta a través de Telegram y Discord		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código malicioso		

Descripción

1. **ANTECEDENTES:**

El equipo de Investigación de Amenazas de Uptycs, han descubierto un nuevo troyano de acceso remoto (RAT) llamado "QwixxRAT" (también conocido como "TelegramRAT"), que está siendo distribuido para su venta por su operador a través de las plataformas de Telegram y Discord a nivel global. Un ataque exitoso podría permitir a un actor de amenazas recopilar datos confidenciales, así como obtener acceso no autorizado a la información confidencial de la víctima.

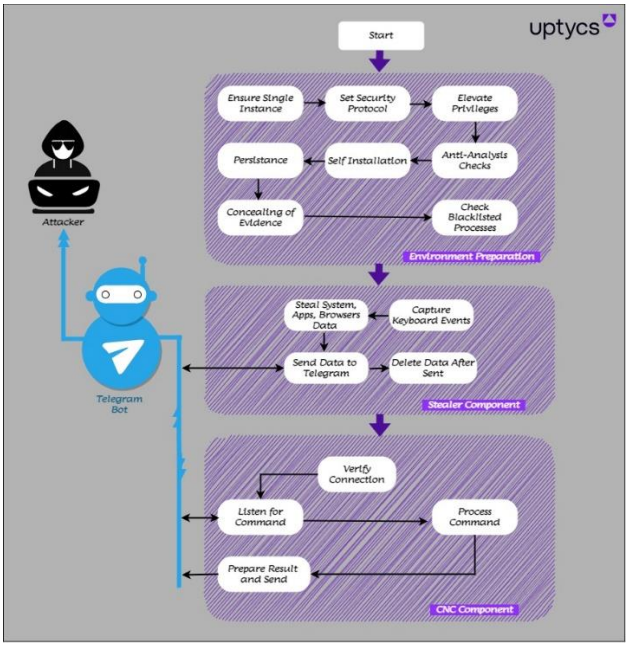
2. **DETALLES:**

Los investigadores de Uptycs, indicaron que una vez instalada el RAT en las máquinas de la plataforma Windows de la víctima, el troyano comienza a recopilar sigilosamente datos confidenciales de su potencial víctima, para luego enviarlo al bot de Telegram del atacante, brindándole acceso no autorizado a la información confidencial de la víctima.

El malware "QwixxRAT" está especialmente diseñado para recolectar una amplia gama de información, desde el historial de los navegadores web, marcadores, cookies, información de tarjetas de crédito, pulsaciones de teclas, capturas de pantalla, archivos que coinciden con ciertas extensiones y datos de aplicaciones como Steam y Telegram. Igualmente, el malware utiliza herramientas administrativas remotas formidables que permite a los atacantes controlar dispositivos de las víctimas, ejecutar comandos e incluso desestabilizar sistemas.

Por otro lado, para evitar la detección por software antivirus, la RAT emplea la funcionalidad de comando y control (C2) a través de un bot de Telegram. Esto permite al atacante controlar de forma remota el RAT y administrar sus operaciones.

El actor de amenazas utiliza las plataformas de Telegram y Discord para distribuir y vender la herramienta RAT en rublos (moneda rusa), 150 rublos por el acceso semanal y 500 rublos por una licencia perpetua. Luego de la compra, el equipo establece un canal separado dedicado a acceder a los datos adquiridos.



Flujo de trabajo de QwixxRAT

El archivo RAT es un binario compilado C #, que funciona como un archivo ejecutable de 32 bits diseñado para operaciones de CPU. La función principal del malware consta de 19 funciones individuales, cada una con un objetivo único.

El RAT viene con varias características anti-análisis para permanecer encubierto y evadir la detección. Esto incluye una función de suspensión para introducir un retraso en el proceso de ejecución, así como ejecutar comprobaciones para determinar si está operando dentro de un entorno de pruebas o virtual. Otras funciones le permiten monitorear una lista específica de procesos (taskmgr, processhacker, netstat, netmon, tcpview y wireshark) y, si se detecta, detiene su propia actividad hasta que se da por terminado el proceso.

"QwixxRAT" también incorpora un clipper que accede sigilosamente a información confidencial copiada en el portapapeles del dispositivo con el objetivo de realizar transferencias ilícitas de fondos desde billeteras de criptomonedas.

El C2 del RAT se facilita por medio de un bot de Telegram, a través del cual se envían comandos para llevar a cabo una recopilación de datos adicionales, como grabaciones de audio y cámara web, e incluso apagar o reiniciar de forma remota el host infectado.

El RAT está equipado con una función de configuración que determina su comportamiento en la máquina de destino. Esta función de configuración contiene varios valores, que pueden ser en forma de booleanos, extensiones de archivo u otros tipos de datos. Sobre la base de estos valores, la RAT adapta sus acciones en consecuencia.

A. Indicadores de Compromiso (IoC):

MD5:

- 46d6f885d323df5f00218da715239a7b / QwixxRAT.exe.

URL:

- hxxps [:] //raw.githubusercontent [.] com / tedburke [.] commandCam / master [.] commandCam [.] exe;
- hxxps [:] //raw.githubusercontent [.] com / LimerBoy / hackpy / master / modules / audio [.] zip;
- hxxps [:] //api.telegram.org/;
- hxxps [:] //raw.githubusercontent [.] com / LimerBoy / ToxicEye / master / TelegramRAT / TelegramRAT / core / libs / AudioSwitcher.AudioApi [.] dll;
- hxxps [:] //raw.githubusercontent [.] com / LimerBoy / ToxicEye / master / TelegramRAT / TelegramRAT / core / libs / AudioSwitcher.AudioApi.CoreAudio];
- hxxps [:] // api [.] mylnikov [.] org / geolocalización / wifi?bssid =
- google [.] com.

3. RECOMENDACIONES:

- Informar inmediatamente sobre cualquier robo e incidente de seguridad a las autoridades correspondientes, como la policía, los bancos o las compañías de tarjetas de crédito, para contrarrestar el robo de identidad y el fraude monetario de inmediato.
- Examinar regularmente los extractos de su banco y tarjeta de crédito en busca de anomalías. Alertar a las autoridades sobre cualquier actividad no reconocida.
- Renovar periódicamente sus contraseñas utilizando combinaciones sólidas y únicas para reducir el riesgo de mal uso de datos o intentos de phishing.
- Introducir una capa de seguridad adicional contra infracciones no autorizadas mediante el empleo de autenticación de dos factores (2FA) en cuentas vitales, incluidas las billeteras de criptomonedas.
- Asegurar la seguridad de la cámara web cubriéndola o desconectándola cuando esté inactivo.
- Tener cuidado con los correos electrónicos dudosos, enlaces o archivos adjuntos. Evitar revelar detalles personales o comprometerse con enlaces desconocidos.
- Mantener informado al personal sobre las normas de ciberseguridad y sobre las posibles amenazas y prácticas de seguridad.

Fuente de Información:	• hxxps://www.uptycs.com/blog/remote-access-trojan-qwixx-telegram