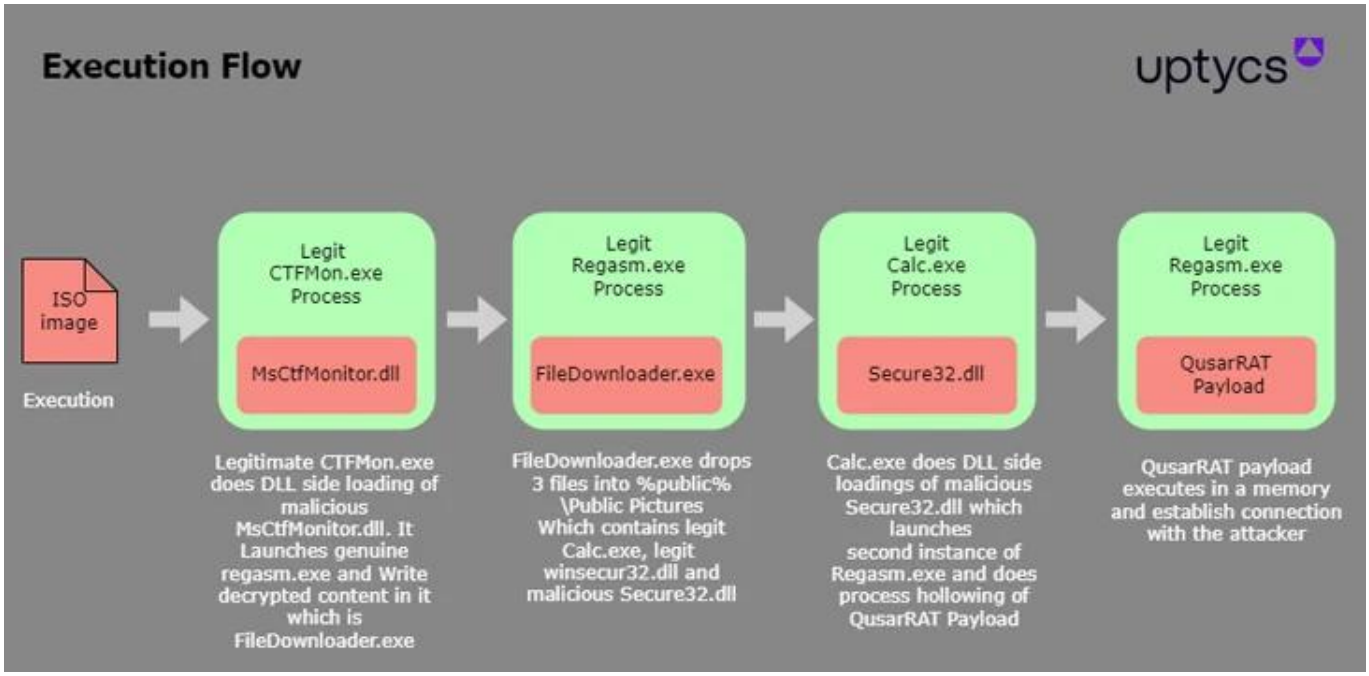
El troyano de acceso remoto de código abierto conocido como Quasar RAT ha sido visto empleando la técnica de *«carga lateral»* de DLL para pasar inadvertido y de manera sigilosa extraer datos de sistemas Windows comprometidos.

«Esta táctica se aprovecha de la confianza inherente que estos archivos generan dentro del entorno de Windows», expresaron los investigadores de Uptycs Tejaswini Sandapolla y Karthickkumar Kathiresan en un informe publicado la semana pasada. Detallaron la dependencia del malware en ctfmon.exe y calc.exe como parte de la secuencia de ataque.

Quasar RAT, también conocido bajo los nombres CinaRAT o Yggdrasil, es una herramienta de administración remota basada en C# que puede recopilar información del sistema, una lista de aplicaciones en ejecución, archivos, pulsaciones de teclas, capturas de pantalla y ejecutar comandos de consola arbitrarios.

La «carga lateral» de DLL es una técnica comúnmente utilizada por muchos actores de amenazas para ejecutar sus propias cargas útiles al introducir un archivo DLL falsificado con un nombre que se sabe que un programa legítimo está buscando.

> *«Los adversarios probablemente emplean la carga lateral como un método para encubrir las acciones que realizan bajo un proceso o software legítimo, confiable y posiblemente con permisos elevados»,* menciona MITRE en su explicación de este método de ataque.



El punto de inicio del ataque documentado por Uptycs es un archivo de imagen ISO que contiene tres archivos: un ejecutable legítimo llamado ctfmon.exe, renombrado como eBill-997358806.exe; un archivo MsCtfMonitor.dll, renombrado como monitor.ini; y un archivo MsCtfMonitor.dll malicioso.

> *«Cuando se ejecuta el archivo binario 'eBill-997358806.exe', inicia la carga de un archivo llamado 'MsCtfMonitor.dll' (con nombre encubierto) mediante la técnica de carga lateral de DLL, dentro de la cual se esconde código malicioso»*, informaron los investigadores.

El código oculto es otro programa ejecutable llamado «*FileDownloader*.exe», que se introduce en Regasm.exe, la Herramienta de Registro de Ensamblados de Windows, para lanzar la siguiente fase: un archivo calc.exe legítimo que, nuevamente, carga el falso archivo Secure32.dll mediante la carga lateral de DLL y ejecuta la carga útil final del troyano Quasar RAT.

El troyano, por su parte, establece conexiones con un servidor remoto para enviar información del sistema e incluso configura un proxy inverso para acceder de forma remota al sistema.

La identidad del actor de amenazas y el vector de acceso inicial exacto utilizado para llevar a cabo el ataque no están claros, pero es probable que se haya distribuido a través de correos electrónicos de phishing, por lo que es crucial que los usuarios se mantengan alerta frente a correos electrónicos, enlaces o adjuntos sospechosos.