Una técnica innovadora utiliza el marco de accesibilidad de Windows conocido como UI Automation (UIA) para realizar diversas actividades maliciosas sin ser detectada por las soluciones de detección y respuesta de endpoints (EDR).

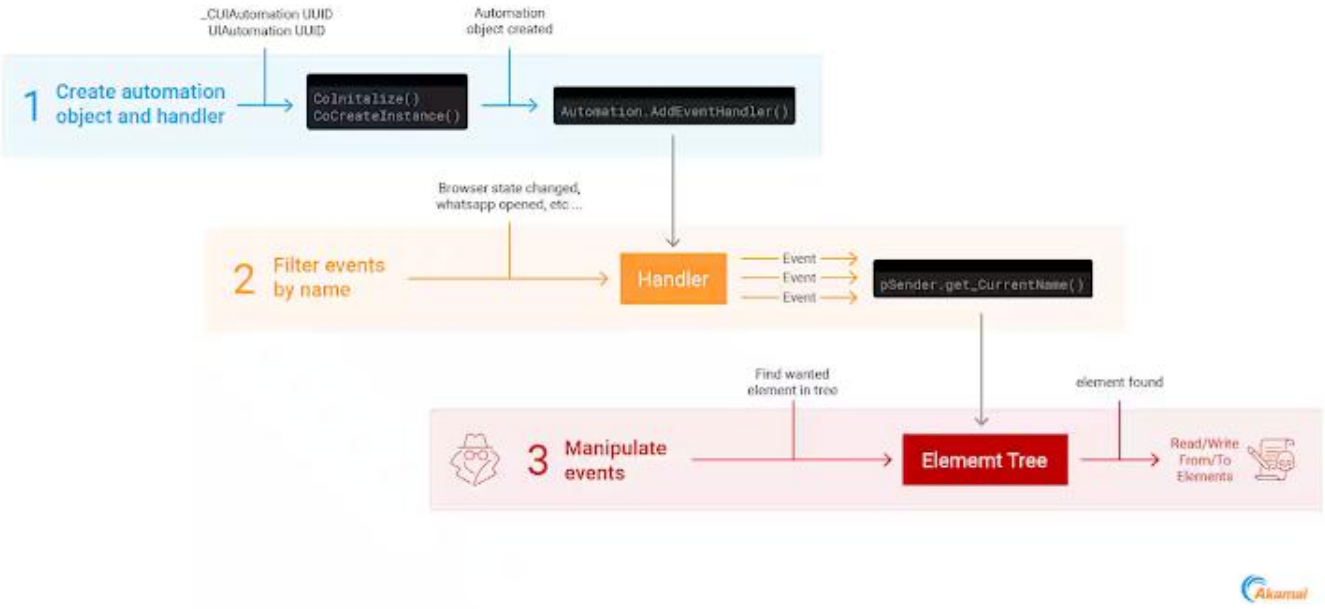
> *«Para aprovechar esta técnica, es necesario convencer a un usuario de que ejecute un programa que emplee UI Automation. Esto permite ejecutar comandos de manera discreta, recolectar datos confidenciales, redirigir navegadores a sitios de phishing y mucho más»*, explicó Tomer Peled, investigador de seguridad de Akamai, en un informe.

Lo que resulta aún más preocupante es que atacantes locales podrían explotar esta vulnerabilidad para ejecutar comandos o leer y escribir mensajes en aplicaciones de mensajería como Slack y WhatsApp. Además, existe el potencial de usar esta técnica para manipular elementos de la interfaz de usuario de forma remota a través de una red.

UI Automation, introducido originalmente en Windows XP como parte de Microsoft .NET Framework, está diseñado para proporcionar acceso programado a elementos de la interfaz de usuario (UI) y facilitar su manipulación mediante productos de tecnología asistiva, como lectores de pantalla. También tiene aplicaciones en pruebas automatizadas.

> *«Las aplicaciones de tecnología asistiva necesitan acceder a elementos protegidos de la interfaz del sistema o a procesos que operan con privilegios más altos. Por esta razón, estas aplicaciones deben ser de confianza para el sistema y ejecutarse con privilegios especiales»,* señala Microsoft en un documento técnico.
>
> *«Para acceder a procesos con un nivel de integridad (IL) más alto, las aplicaciones de tecnología asistiva deben activar la bandera UIAccess en su manifiesto y ser ejecutadas por un usuario con privilegios administrativos».*

La interacción con elementos de la UI de otras aplicaciones se realiza a través del Modelo de Objetos Componentes (COM), que actúa como un mecanismo de comunicación entre procesos (IPC). Esto permite crear objetos UIA que interactúan con aplicaciones activas, configurando controladores de eventos que responden a cambios específicos en la interfaz.



El análisis de Akamai reveló que este método también puede ser utilizado de forma malintencionada, permitiendo que actores maliciosos lean o escriban mensajes, roben información introducida en sitios web (como datos de pago) y ejecuten comandos que redirijan a las víctimas a sitios peligrosos cuando una página web en un navegador se actualiza o cambia.

> *«Además de los elementos visibles en pantalla con los que podemos interactuar, existen otros elementos precargados en una memoria caché. También podemos interactuar con estos elementos, como leer mensajes que no se muestran en pantalla o incluso establecer texto en un cuadro de diálogo y enviarlo sin que esto*

> *se refleje visualmente»,* explicó Peled.

Es importante mencionar que estas capacidades maliciosas son, en realidad, funciones legítimas de UI Automation, similar a cómo las API de accesibilidad de Android han sido utilizadas por software malicioso para extraer información de dispositivos comprometidos.

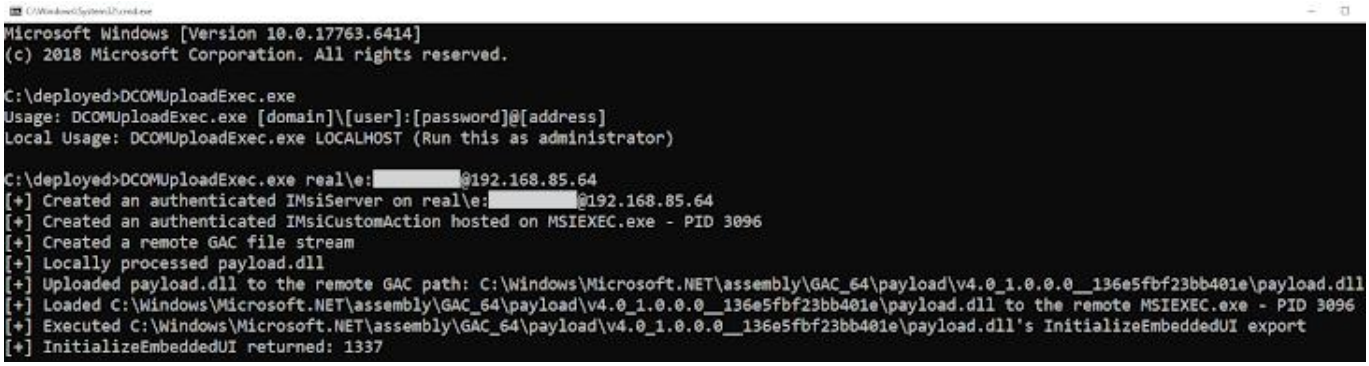
> *«Esto está relacionado con el propósito original de la herramienta: estos niveles de permiso son necesarios para su funcionamiento. Por eso UIA puede pasar desapercibido para Defender: el sistema no detecta nada anómalo. Si algo es considerado una característica y no un fallo, la lógica del sistema tratará esa función como legítima»*, añadió Peled.

De COM a DCOM: un nuevo vector para movimientos laterales

Este descubrimiento coincide con un informe de Deep Instinct que detalla cómo el Protocolo Remoto COM Distribuido (DCOM), que permite la comunicación entre componentes de software a través de una red, podría ser manipulado para insertar cargas personalizadas y establecer una puerta trasera persistente.

> *El ataque permite que se escriban DLLs personalizadas en una máquina objetivo, se carguen en un servicio y se ejecuten con parámetros definidos de forma arbitraria. Este ataque, con características similares a un backdoor, explota la interfaz COM de IMsiServer»*, señaló Eliran Nissan investigador en seguridad.

Sin embargo, la compañía de ciberseguridad israelí destacó que este tipo de ataque genera indicadores de compromiso (IoCs) claros, los cuales pueden ser identificados y neutralizados. Además, requiere que tanto el equipo del atacante como el de la víctima pertenezcan al mismo dominio.



> *«Hasta el momento, los ataques de movimiento lateral utilizando DCOM se han investigado únicamente en objetos COM basados en IDispatch debido a su capacidad para ser manipulados mediante scripts. El método 'DCOM Upload & Execute' «escribe cargas útiles personalizadas de forma remota en la [Caché Global de Ensamblados] del equipo objetivo, las ejecuta desde el contexto de un servicio y se comunica con ellas, actuando como un backdoor integrado»,* explicó Nissan.
>
> *«Esta investigación demuestra que una gran cantidad de objetos DCOM, previamente no considerados, podrían ser explotados para movimientos laterales, lo que subraya la necesidad de fortalecer las defensas adecuadas».*