El Laboratorio de Inteligencia de Amenazas Cibernéticas de Bitdefender, descubrió un caso más de ataque de espionaje dirigido a una empresa de producción de video y arquitectura internacional no identificada, que tenía todas las características de una campaña cuidadosamente orquestada.

> *«El grupo de ciberdelincuentes se infiltró en la empresa utilizando un complemento contaminado y especialmente diseñado para Autodesk 3ds Max»,* dijeron los investigadores de Bitdefender.
>
> *«La investigación también encontró que la infraestructura de comando y control utilizada por el grupo de piratas informáticos para probar su carga útil maliciosa contra la solución de seguridad de la organización, se encuentra en Corea del Sur».*

Aunque antes existieron ataques de grupos APT como Dark Basin y Deceptikons o DeathStalker, dirigidos al sector financiero y legal, esta es la primera vez que un actor de amenazas ha empleado el mismo modus operandi en la industria inmobiliaria.

El mes pasado se descubrió una campaña parecida, llamada StrongPity, que utilizaba instaladores de software contaminados como cuentagotas para ingresar una puerta trasera para la exfiltración de documentos.

> *«Es probable que esto se convierta en la nueva normalidad en términos de la mercantilización de los grupos de APT, no solo los actores patrocinados por el estado, sino cualquiera que busque sus servicios para beneficio personal, en todas las industrias»,* dijo la compañía de seguridad.

Complemento de Autodesk 3ds Max infectado

En un aviso publicado a inicios del mes, Autodesk advirtió a los usuarios sobre una variante del exploit MAXScript *«PhysXPluginMfx»*, que puede dañar la configuración de 3ds Max, ejecutar código malicioso y propagarse a otros archivos MAX en un sistema Windows al cargar los archivos infectados en el software.

Pero según el análisis forense de BitDefender, esta muestra incompleta de MAXScript Encrypted («PhysXPluginStl.mse»), contenía un archivo DLL incrustado, que posteriormente descargó binarios .NET adicionales dede el servidor C&C con el objetivo final de robar documentos importantes.

Los binarios, a su vez, son responsables de descargar otros MAXScripts maliciosos, capaces de recopilar información sobre la máquina comprometida y exfiltrar los detalles al servidor remoto, que transmite una carga útil final que puede hacer capturas de pantalla y recopilar contraseñas de navegadores web como Firefox, Google Chrome e Internet Explorer.

Además del mecanismo de suspensión para pasar desapercibido y evadir la detección, los investigadores de Bitdefender también descubrieron que los autores del malware tenían un conjunto completo de herramientas para espiar a sus víctimas, incluido un binario *«HdCrawler»*, cuyo trabajo es enumerar y cargar archivos con extensiones (.webp, .jpg, .png, .zip, .obb, .uasset, etc.) al servidor y un ladrón de información con amplias funciones.

La información reunida por el malware incluyen el nombre de usuario, nombre del equipo, las direcciones IP de los adaptadores de red, Windows ProductName, la versión de .NET Framework, procesadores, la memoria RAM total y libre disponibles, detalles de almacenamiento para los nombres de los procesos que se ejecutan en el sistema, los archivos configurados para iniciarse automáticamente después de un arranque y la lista de archivos recientes a los que se accedió.

Los datos de telemetría de Bitdefender también encontraron otras muestras de malware similares que se comunican con el mismo servidor C&C, que datan de hace poco menos de un mes, lo que significa que el grupo apunta a otras víctimas.

Los usuarios de 3ds Max deben descargar la última versión de Security Tools para Autodesk 3ds Max 2021-2015SP1, para identificar y eliminar el malware PhysXPluginMfx MAXScript.

> *«La sofisticación del ataque revela un grupo de estilo APT que tenía conocimiento previo de los sistemas de seguridad de la empresa y utilizaba aplicaciones de software, planificando cuidadosamente su ataque para infiltrarse en la empresa y extraer datos sin ser detectados»,* dijeron los investigadores.
>
> *«El espionaje industrial no es nuevo, y debido a que la industria inmobiliaria es altamente competitiva, con contratos valorados en miles de millones de dólares, hay mucho en juego para ganar contratos para proyectos de lujo y podría justificar recurrir a grupos APT mercenarios para obtener una ventaja de negociación».*