Los falsos instaladores de Adobe Acrobat Reader están siendo utilizados como vehículo para distribuir un nuevo malware multifuncional denominado Byakugan.

El punto de partida de este ataque es un archivo PDF en portugués que, una vez abierto, muestra una imagen borrosa y solicita a la víctima que haga clic en un enlace para descargar la aplicación Reader y ver el contenido.

De acuerdo con Fortinet FortiGuard Labs, al hacer clic en el enlace se descarga un instalador («Reader_Install_Setup.exe») que activa la secuencia de infección. Los detalles de esta campaña fueron revelados inicialmente por el Centro de Inteligencia de Seguridad AhnLab (ASEC) el mes pasado.

Este ataque hace uso de técnicas como el secuestro de DLL y el bypass del Control de Acceso de Usuario (UAC) de Windows para cargar un archivo de biblioteca de enlaces dinámicos (DLL) malicioso llamado «*BluetoothDiagnosticUtil.dll*«, el cual a su vez ejecuta el payload final. Además, despliega un instalador legítimo de un lector de PDF, como Wondershare PDFelement.

El archivo binario está programado para recopilar y enviar metadatos del sistema a un servidor de comando y control (C2) y luego descargar el módulo principal («chrome.exe») desde otro servidor que también sirve como C2, para recibir archivos y comandos.

> *«Byakugan es un malware basado en node.js que ha sido empaquetado en su ejecutable utilizando la herramienta pkg. Además del script principal, hay varias librerías que corresponden a diversas funcionalidades»,* comentó el investigador de seguridad Pei Han Liao.

Esto incluye la configuración de persistencia, el monitoreo del escritorio de la víctima mediante OBS Studio, la captura de pantallas, la descarga de mineros de criptomonedas, el registro de pulsaciones de teclas, la enumeración y carga de archivos, y la extracción de datos almacenados en navegadores web.

> *«Hay una tendencia creciente a utilizar tanto componentes limpios como maliciosos en el malware, y Byakugan no es una excepción. Este enfoque incrementa el ruido generado durante el análisis, lo que dificulta la detección precisa»,* advirtió Fortinet.

Esta revelación se produce después de que ASEC informara sobre una nueva campaña que propaga el robainformación Rhadamanthys, disfrazándolo de un instalador para software de colaboración en grupo.

> *«El actor de amenazas creó un sitio web falso para imitar al original y lo promocionó mediante anuncios en motores de búsqueda. El malware distribuido utiliza la técnica de syscall indirecto para evadir la detección de soluciones de seguridad»*, indicó la firma de ciberseguridad surcoreana.

Asimismo, este desarrollo se produce tras el descubrimiento de que una versión manipulada de Notepad++ está siendo utilizada por actores de amenazas no identificados para propagar el malware WikiLoader (también conocido como WailingCrab).