El cargador de malware conocido como Bumblebee está siendo cooptado cada vez más por hackers asociados con BazarLoader, TrickBot e IceID en sus campañas para violar redes objetivo para actividades posteriores a la explotación.

> *«Los operadores de Bumblebee realizan actividades de reconocimiento intensivo y redirigen la salida de los comandos ejecutados a archivos para su exfiltración»*, dijeron los investigadores de Cybereason, Mereoujan Antonyan y Alon Laufer.

Bumblebee salió a la luz por primera vez en marzo de 2022 cuando el Grupo de Análisis de Amenazas (TAG) de Google desenmascaró las actividades de un corredor de acceso inicial denominado Exotic Lily, con vínculos con TrickBot y los colectivos más grandes de Conti.

Generalmente entregado por medio del acceso inicial adquirido por medio de campañas de spear-phishing, el modus operandi se modificó desde entonces al evitar documentos con macros en favor de archivos ISO y LNK, principalmente en respuesta a la decisión de Microsoft de bloquear las macros de forma predeterminada.

> *«La distribución del malware se realiza mediante correos electrónicos de phishing con un archivo adjunto o un enlace a un archivo malicioso que contiene Bumblebee. La ejecución inicial se basa en la ejecución del usuario final que tiene que extraer el archivo, montar un archivo de imagen ISO y hacer clic en un archivo de acceso directo de Windows (LNK)»*, dijeron los investigadores.

El archivo LNK, por su parte, contiene el comando para iniciar el cargador Bumblebee, que después se utiliza como conducto para las acciones de la siguiente etapa, como la persistencia, la escalada de privilegios, el reconocimiento y el robo de credenciales.

Durante el ataque cibernético también se empleó el marco de simulación de adversarios Cobalt Strike al obtener privilegios elevados en los puntos finales infectados, lo que permite

que el atacante se mueva lateralmente por medio de la red. La persistencia se logra implementando el software de escritorio remoto AnyDesk.

En el incidente analizado por Cybereason, las credenciales robadas de un usuario con muchos privilegios se usaron posteriormente para tomar el control de Active Directory, sin mencionar la creación de una cuenta de usuario local para la exfiltración de datos.

> *«El tiempo que pasó entre el acceso inicial y el compromiso de Active Directory fue menos de dos días. Los ataques que involucran a Bumblebee deben tratarse como críticos y este cargador es conocido por la entrega de ransomware»,* dijo la compañía de ciberseguridad.