Los hackers que se observaron anteriormente entregando BazaLoader e IceID como parte de sus campañas de malware han hecho la transición a un nuevo cargador llamado Bumblebee que está en desarrollo activo.

> *«Según el momento de su aparición en el panorama de amenazas y el uso por parte de múltiples grupos de ciberdelincuentes, es probable que Bumblebee sea, si no un reemplazo directo de BazaLoader, una nueva herramienta multifuncional utilizada por actores que históricamente favorecieron a otro malware»,* dijo la compañía de seguridad Proofpoint.

Las campañas que distribuyen el nuevo cargador altamente sofisticado comenzaron en marzo de 2022, mientras se superponen con actividades maliciosas que conducen al despliegue de ransomware Conti y Diavol, lo que aumenta la posibilidad de que el cargador actúe como precursor de ataques de ransomware.

> *«Los actores de amenazas que usan Bumblebee están asociados con cargas útiles de malware que se han vinculado a campañas de ransomware de seguimiento»,* dijeron los investigadores.

Además de presentar controles antivirtualización, Bumblebee está escrito en C++ y está diseñado para actuar como un descargador para recuperar y ejecutar cargas útiles de siguiente etapa, incluidos Cobalt Strike, Sliver, Meterpreter y Shellcode.

La mayor detección del cargador de malware en el panorama de amenazas corresponde a una caída en las implementaciones de BazaLoader desde febrero de 2022, otro cargador popular utilizado para entregar malware de cifrado de archivos y desarrollado por el grupo ahora desaparecido, TrickBot, que desde entonces ha sido absorbido por Conti.

Las cadenas de ataque que distribuyen Bumblebee tomaron la forma de señuelos de phishing

de correo electrónico con la marca DocuSign, que incorporan enlaces fraudulentos o archivos adjuntos HTML, lo que lleva a las víctimas potenciales a un archivo ISO comprimido alojado en Microsoft OneDrive.

Además, la URL incrustada en el archivo adjunto HTML utiliza un sistema de dirección de tráfico (TDS) denominado Prometheus, que está disponible para la venta en plataformas clandestinas por 250 dólares al mes, para redirigir las URL a los archivos de almacenamiento en función de la zona horaria y cookies de las víctimas.

Los archivos ZIP, a su vez, incluyen archivos .LNK y .DAT, y el archivo de acceso directo de Windows ejecuta este último que contiene el descargador de Bumblebee, antes de usarlo para entregar el malware BazaLoader e IceID.

Una segunda campaña en abril de 2022 involucró un esquema de secuestro de hilos en el que se tomaron correos electrónicos legítimos con temas de facturas para enviar archivos ISO comprimidos, que luego se utilizaron para ejecutar un archivo DLL para activar el cargador.

También se ha observado el abuso del formulario de contacto presente en el sitio web del objetivo para enviar un mensaje reclamando violaciones de derechos de autor de las imágenes, dirigiendo a la víctima a un enlace de Google Cloud Storage, que resulta en la descarga de un archivo ISO comprimido, siguiendo así la secuencia de infección antes mencionada.

La transición de BazaLoader a Bumblebee es una prueba más de que estos actores de amenazas, probablemente corredores de acceso inicial que se infiltran en los objetivos y luego venden ese acceso a otros, están recibiendo el malware de una fuente común, al tiempo que señalan una partida después de que el conjunto de herramientas de ataque del grupo Conti se convirtió en conocimiento público al mismo tiempo.

El desarrollo también coincide con el hecho de que Conti se hizo cargo de la red de bots de TrickBot y la cerró para centrarse en el desarrollo del malware BazaLoader y Anchor. No está claro aún si Bumblebee es obra de los actores de TrickBot y si las filtraciones llevaron al grupo a abandonar BazaLoader en favor de un malware completamente nuevo.

Pero el investigador de malware de Cybereason, Eli Salem, en un análisis independiente, identificó puntos de similitudes entre Bumblebee y TrickBot, incluido el uso del módulo de inyección web de este último y la misma técnica de evasión, dando crédito a la posibilidad de que los autores detrás de Bumblebee hayan tenido acceso al código fuente de TrickBot.

> *«La introducción del cargador Bumblebee en el panorama de amenazas de crimeware y su aparente reemplazo para BazaLoader demuestra la flexibilidad que tienen los actores de amenazas para cambiar rápidamente los TTP y adoptar nuevo malware»*, dijo Sherrod DeGrippo, vicepresidente de investigación y detección de amenazas en Proofpoint.

> *«Además, el malware es bastante sofisticado y demuestra estar en desarrollo activo y continuo, introduciendo nuevos métodos para evadir la detección»*, agregó DeGrippo.