Investigadores de Cisco Talos descubrieron una campaña nueva que distribuye el troyano malicioso de acceso remoto (RAT) ObliqueRAT.

Anteriormente, Talos informó que ObliqueRAT y otra campaña de diciembre de 2019 estaban distribuyendo CrimsonRAT. Estas dos familias de malware comparte macros y maldocs similares, sin embargo, esta nueva campaña utiliza un código de macro completamente diferente para descargar e implementar la carga útil de ObliqueRAT.

Además, los atacantes actualizaron la cadena de infección para entregar ObliqueRAT por medio de sitios web controlados por el adversario.

Este RAT se coloca en el punto final de la víctima mediante documentos maliciosos de Microsoft Office (maldocs). Sin embargo, estos maldocs no contienen la carga útil de ObliqueRAT directamente incrustada, como en las campañas anteriores. En cambio, los atacantes utilizan una técnica novedosa en su cadena de infección para infectar los puntos finales específicos al señalar a los usuarios a URL maliciosas.

Las nuevas capacidades técnicas centrales de ObliqueRAT incluyen:

- Cadena de infección basada en maldocs
- Cambios/actualizaciones a su carga útil
- Enlaces adicionales a ataques de malware previamente observados en la naturaleza.

Las modificaciones en las cargas útiles de ObliqueRAT también destacan el uso de técnicas de ofuscación que se pueden utilizar para evadir los mecanismos de detección tradicionales basados en firmas. Aunque la detección basada en la red y la firma de archivos es importante, se puede complementar con análisis de comportamiento del sistema y protecciones de terminales para obtener capas adicionales de seguridad.

Los maldocs analizados en ataques anteriores de ObliqueRAT utilizaron mecanismos idénticos a los maldocs de entrega CrimsonRAT. La última campaña que distribuye

ObliqueRAT ahora utiliza un código macro completamente diferente en sus maldocs.

El ataque ha sido actualizado para incluye nuevas funcionalidades como las siguientes:

- Las cargas útiles se alojan en sitios web comprometidos
- Las cargas útiles alojadas en los sitios web consisten en archivos de imagen BMP aparentemente benignos
- Las macros maliciosas descargan las imágenes y la carga útil de ObliqueRAT se extrae al disco
- La carga útil de ObliqueRAT se renombra con la extensión de archivo .pif.

Otra instancia de un maldoc utiliza una técnica similar con la diferencia de que la carga útil alojada en el sitio web comprometido es una imagen BMP que contiene un archivo ZIP con la carga útil de ObliqueRAT. Las macros maliciosas son responsables de extraer el ZIP y, posteriormente, la carga útil de ObliqueRAT en el punto final.

Las macros también son responsables de lograr la persistencia de reinicio para las cargas útiles de ObliqueRAT. Esto se hace al crear un acceso directo (extensión de archivo .url) en el directorio de inicio del usuario infectado.

Los archivos de imagen utilizados son archivos BMP alojados en sitios web controlados por atacantes. Los archivos de imagen contienen datos legítimos y bytes ejecutables maliciosos ocultos en los datos de imagen.

Carga útil de ObliqueRAT

Talos descubrió tres versiones nuevas de ObliqueRAT en su investigación. Luego del descubrimiento de la carga útil de ObliqueRAT anterior (versión 5.2), los investigadores observaron cuatro versiones nuevas:

- 6.1, desarrollada en abril de 2020
- 6.2.3, desarrollada en septiembre de 2020

- 6.3.4, desarrollada en octubre de 2020
- 6.3.5, desarrollada en noviembre de 2020

Según los investigadores, esta campaña muestra a un actor de amenazas evolucionando sus técnicas de infección para que ya no se parezcan a las que se utilizaban antes. Es probable que estos cambios sean una respuesta a divulgaciones anteriores para lograr la evasión de las nuevas campañas.

El uso de sitios web comprometidos es otro intento de evasión de detección. Por otro lado, los adversarios también introdujeron la esteganografía como una forma de ocultar las cargas útiles de ObliqueRAT en archivos de imagen.

La técnica de esteganografía es nueva para la cadena de distribución de ObliqueRAT. Esta nueva campaña de distribución comenzó en abril de 2020 y sigue en curso.