JhoneRAT Descripción

El JhoneRAT es un impresionante RAT (troyano de acceso remoto) cuya actividad se ha disparado recientemente. Después de estudiar esta amenaza, los analistas de malware concluyeron que probablemente se haya construido desde cero. Esto no es inusual, pero muchos autores de RAT prefieren tomar prestado el código de las amenazas existentes en lugar de crear una herramienta desde cero. Según los expertos, el JhoneRAT está escrito en el lenguaje de programación Python.

Método de propagación

El JhoneRAT se distribuye con la ayuda de campañas de correo electrónico no deseado. Este es un método de propagación muy popular cuando se trata de propagar malware. Por lo general, los correos electrónicos no deseados contendrían un archivo adjunto dañado. Este es el caso también con el JhoneRAT. Los archivos adjuntos utilizados en la propagación de JhoneRAT tienen dos tipos: uno dice ser un documento importante que debe abrirse con urgencia, mientras que el otro afirma que es un archivo que contiene las credenciales de inicio de sesión de Facebook que se han filtrado. Si los usuarios caen en este truco y abren el archivo adjunto, activarán la ejecución del siguiente paso del ataque de JhoneRAT.

Evita la detección mediante herramientas antimalware

Los autores de JhoneRAT usan un truco muy inteligente para enmascarar la actividad insegura de esta amenaza. Al comprometer el sistema objetivo, el JhoneRAT también descargaría otro documento de Microsoft Office alojado en Google Drive. Una vez descargado, el documento se iniciará en el sistema. Los atacantes se han asegurado de que se priorice el uso de aplicaciones de terceros (como Google Drive). Esto ayuda a los autores de este RAT a disfrazar la actividad de la amenaza y engañar a las herramientas de seguridad para que lo enumeren como legítimo.

Técnicas de autoconservación

El documento adicional que el JhoneRAT obtiene de Google Drive lleva un módulo que es capaz de escanear el sistema infiltrado en busca de un número de serie del disco duro, ya que las computadoras que se utilizan para la depuración de malware a menudo carecen de tal. Esto significa que JhoneRAT puede detectar si se está ejecutando en un entorno de espacio aislado o en una computadora normal. Si el análisis determina que el sistema no se usa para la depuración de malware, el JhoneRAT procederá con el ataque y buscará una imagen de Google Drive.

Se dirige a usuarios de Medio Oriente y África del Norte

La imagen que descargaría JhoneRAT contiene una cadena enmascarada que está codificada con base64. A continuación, JhoneRAT decodificaría la cadena en cuestión y la extraería como un script de AutoIT. Este script sirve como un descargador cuyo objetivo es obtener la última carga alojada en Google Drive. Luego, el JhoneRAT procedería con el ataque comprobando el teclado que la víctima está usando. El JhoneRAT solo continuará la campaña si detecta que la víctima está usando un teclado

típico de Irak, Arabia Saudita, Libia, Kuwait, Líbano, Emiratos Árabes Unidos, Marruecos, Túnez, Omán, Egipto, Bahrein, Yemen o Argelia.

Curiosamente, el JhoneRAT recibe comandos a través de un perfil de Twitter. Esta amenaza se conectaría a la cuenta de Twitter en cuestión y correría a través de todos sus tweets más recientes. Según los investigadores de ciberseguridad, los creadores de JhoneRAT tuitean comandos que son interceptados por RAT y ejecutados en consecuencia. Desde entonces, Twitter agitó la cuenta en cuestión. Desafortunadamente, los autores de JhoneRAT pueden crear una nueva cuenta de Twitter y continuar su campaña fácilmente.

Capacidades

JhoneRAT se basa en aplicaciones de terceros para ejecutar sus comandos. Esta amenaza puede tomar capturas de pantalla del escritorio de la víctima y las ventanas activas. Los datos se transfieren a un servicio de alojamiento de imágenes llamado ImgBB. Los atacantes también pueden ordenar al JhoneRAT que descargue y ejecute cargas útiles adicionales desde Google Drive. Los autores de JhoneRAT también pueden usarlo para ejecutar un comando del sistema. El resultado registrado como respuesta se coloca en un documento de Google Forms que es privado y, por lo tanto, accesible solo para los atacantes.

A pesar de la lista relativamente corta de capacidades que posee el JhoneRAT, el hecho de que esta amenaza pueda enmascarar su tráfico inventado utilizando servicios legítimos lo hace bastante amenazante porque las herramientas antivirus pueden no ser capaces de detectarlo. Es probable que los autores de JhoneRAT tengan mucha experiencia y mucha habilidad.

Fuente: https://www.enigmasoftware.es/jhonerat-eliminar/