Investigadores de seguridad informática informaron que encontraron un nuevo tipo de malware que toma instrucciones en un código oculto en los memes publicados en Twitter.

El malware no es tan eficiente, pues como la mayoría de los troyanos de acceso remoto primitivos (RAT), el malware infecta silenciosamente una computadora vulnerable, luego toma capturas de pantalla y extrae datos del sistema afectado para enviarlos al servidor de comando y control del malware.

Lo que resultó interesante para los especialistas, es cómo el malware utiliza Twitter como un conducto no dispuesto para comunicarse con su servidor malicioso.

Trend Micro afirmó en una publicación en su blog, que el malware toma los comandos de una cuenta de Twitter ejecutada por el operador del malware. Los investigadores encontraron dos tweets que utilizaron la estenografía para ocultar los comandos «/ print» en las imágenes de los memes, lo que hizo que el malware tomara una captura de pantalla de una computadora infectada.

Después, el malware obtiene por separado la dirección donde se encuentra su servidor de comando y control de una publicación de Pastebin, que dirige al troyano a dónde enviar las capturas de pantalla.

Los investigadores aseguraron que los memes subidos a Twitter podrían haber incluido otros comandos, como «/ processos», para recuperar una lista de aplicaciones y procesos en ejecución, «/ clip», para robar el contenido del portapapeles de un usuario, y «/ docs» para recuperar nombres de archivos de carpetas específicas.

Al parecer, el malware apareció por primera vez a mediados de octubre, según un análisis de hash realizado por VirusTotal, aproximadamente cuando se creó la publicación de Pastebin.

Sin embargo, los especialistas aseguran que no tienen todas las respuestas a los cuestionamientos de seguridad, ya que necesitan realizar más trabajo para comprender completamente el funcionamiento del malware.

No se sabe a ciencia cierta de dónde vino el malware, cómo infecta a las víctimas o quién es el desarrollador. Tampoco se sabe para qué fue desarrollado exactamente.

Twitter no albergó contenido malicioso, ni los tweets provocaron infección de malware, pero es una forma interesante de utilizar las redes sociales como una forma inteligente de comunicarse con el troyano.

Lo que sería lógico, es que al utilizar Twitter, el malware se conecte con twitter.com, que es mucho menos probable que esté marcado o bloqueado por un software antimalware que un servidor con aspecto poco confiable.

Después de que Trend Micro informara lo sucedido a Twitter, la plataforma desconectó y suspendió la cuenta que publicó los memes de forma permanente.

No es la primera vez que operadores de malware o botnets utilizan Twitter como plataforma para comunicarse con sus redes. Desde 2009, Twitter se usó como una fuente para envío de comandos a una botnet, y en 2016, un malware para Android se comunicaba con una cuenta de Twitter predefinida para recibir comandos.