Un grupo que se dedica al spam ha aprendido un truco muy inteligente que le ha permitido pasar por alto los filtros de correo electrónico y los sistemas de seguridad, para llegar a más bandejas de entrada de lo normal.

El truco se basa en una peculiaridad de RFC791, un estándar que describe el Protocolo de Internet (IP).

Entre los diversos detalles técnicos, RFC791 es también el estándar que describe cómo se ven las direcciones IP. En su mayoría, se conocen en su forma más común de dirección decimal con puntos.

Sin embargo, las direcciones IP también se pueden escribir en otros tres formatos:

- Octal: 0300.0250.0000.0001, convirtiendo cada número decimal a base octal, para el ejemplo 192.168.0.1.
- Hexadecimal: 0xc0a80001, convirtiendo cada número decimal a hexadecimal.
- Integer/DWORD: 3232235521, convirtiendo la IP hexadecimal en un entero.

Según un informe publicado ayer por Trustwave, un grupo spammer adoptó direcciones IP hexadecimales para sus campañas desde inicios de este año hasta julio.

El grupo ha estado enviando correos electrónicos que contienen enlaces a sus sitios de spam, pero en lugar de nombres de dominio como *«spam-website.com»*, los correos electrónicos contienen URL de aspecto extraño como *http:// 0xD83AC75R*.

Se trata de direcciones IP hexadecimales donde los spammers alojan la infraestructura de su sitio web de spam.

Aunque los navegadores web son capaces de interpretar direcciones IP hexadecimales y cargar el sitio web que se encuentra en el servidor, parece que el truco fue suficiente para ayudar a los grupos de spam a evadir la detección mientras arrojan grandes volúmenes de correos spam farmacéuticos.

Trustwave asegura que las operaciones del grupo aumentaron de forma significativa desde que adoptaron este truco, ya que pudieron enviar más mensajes a las bandejas de entrada de los usuarios.

Esta campaña también marca la segunda vez que se detecta el uso de direcciones IP hexadecimales en una campaña de malware en los últimos años.

En el verano de 2019, los operadores del troyano PsiXbot también utilizaron direcciones IP hexadecimales para ocultar la ubicación de sus servidores de comando y control.

Sin embargo, además de la versión hexadecimal, los autores de malware también abusaron de otros esquemas de direccionamiento IP. En 2011, Zscaler encontró documentos de Word maliciosos que utilizaban direcciones IP Integer/DWORD para ocultar la ubicación de recursos maliciosos almacenados de forma remota que descargarían en hosts infectados.

Al igual que en el informe de Trustwave, las operaciones anteriores utilizaron estos extraños esquemas de direccionamiento IP como una forma de evitar la detección, ya que no todo el software de seguridad es totalmente compatible con RFC791.