Los usuarios de habla hispana en América Latina se han encontrado en el extremo receptor de un nuevo malware de botnet denominado Horabot, desde al menos noviembre de 2020.

> *«Horabot permite que el hacker controle el buzón de Outlook de la víctima, extraiga las direcciones de correo electrónico de los contactos y envíe correos electrónicos de phishing con archivos adjuntos HTML maliciosos a todas las direcciones en el buzón de la víctima»,* dijo el investigador de Cisco Talos, Chetan Raghuprasad.

El programa botnet también ofrece un troyano financiero basado en Windows y una herramienta de correo no deseado para recopilar credenciales bancarias en línea, así como para comprometer Gmail, Outlook y Yahoo! para eliminar los correos electrónicos no deseados.

La compañía de seguridad cibernética dijo que la mayoría de las infecciones están ubicadas en México, con víctimas limitadas identificadas en Uruguay, Brasil, Venezuela, Argentina, Guatemala y Panamá. Se cree que el atacante detrás de la campaña se encuentra en Brasil.

Los usuarios objetivo de la campaña en curso abarcan principalmente las verticales de contabilidad, construcción e ingeniería, distribución mayorista e inversión, aunque se sospecha que otros sectores de la región también pueden verse afectados.

Los ataques comienzan con correos electrónicos de phishing con señuelos relacionados con los impuestos que atraen a los destinatarios a abrir un archivo adjunto HTML, que a su vez, incrusta un enlace que contiene un archivo RAR.

Abrir el contenido del archivo da como resultado la ejecución de un script de descarga de PowerShell que es responsable de recuperar un archivo ZIP que contiene las cargas útiles principales de un servidor remoto y reiniciar la máquina.

El reinicio del sistema también sirve como plataforma de lanzamiento para el troyano bancario y la herramienta de correo no deseado, lo que permite al atacante robar datos,

registrar pulsaciones de teclas, realizar capturas de pantalla y difundir correos electrónicos de phishing adicionales a los contactos de la víctima.

> *«Esta campaña implica una cadena de ataque de varias etapas que comienza con un correo electrónico de phishing y conduce a la entrega de carga útil por medio de la ejecución de un script de descarga de PowerShell y la descarga a ejecutables legítimos»,* dijo Raghuprasad.

El troyano bancario es una DLL de Windows de 32 bits escrita en el lenguaje de programación Delphi y comparte superposiciones con otras familiar de malware brasileñas como Mekotio y Casbaneiro.

Horabot, por su parte, es un programa de botnet de phishing de Outlook escrito en PowerShell que es capaz de enviar correos electrónicos de phishing a todas las direcciones de correo electrónico en el buzón de la víctima para propagar la infección. También es un intento deliberado de minimizar la exposición de la infraestructura de phishing del atacante.

La divulgación llega una semana después de que SentinelOne atribuyó a un hacker brasileño desconocido a una campaña de larga duración dirigida a más de 30 instituciones financieras portuguesas con malware de robo de información desde 2021.

También sigue al descubrimiento de un nuevo troyano bancario para Android denominado PixBankBot, que abusa de los servicios de accesibilidad del sistema operativo para realizar transferencias de dinero fraudulentas por medio de la plataforma de pagos PIX de Brasil.

PixBankBot es también el ejemplo más reciente de malware que se centra específicamente en los bancos brasileños y presenta capacidades similares a BrasDex, PixPirate y GoatRAT, que se han detectado en los últimos meses.

En todo caso, los desarrollos representan otra interacción de un grupo más amplio de esfuerzos de hacking motivados financieramente que emanan de Brasil, por lo que es crucial que los usuarios permanezcan atentos para evitar ser víctimas de dichas amenazas.