Encontrada Nueva Variante De Emotet

Una nueva campaña de **spam por correo electrónico**, circula en Alemania y está infectando con una nueva variante de un potente software malicioso bancario, una amenaza financiera diseñada para **robar credenciales de usuarios de bancos en línea**, de acuerdo con los investigadores de seguridad de Microsoft.

El malware, identificado como **Emotet**, fue visto por primera vez en junio pasado por los proveedores de **seguridad de Trend Micro**. Las características más sobresalientes de Emotet es su capacidad de rastrear o sniffear en la red, lo que le permite capturar los datos enviados a través de conexiones HTTPS seguras, de acuerdo con Trend Micro.

Microsoft ha estado monitoreando una **nueva variante de Emotet**, identificado como Trojan: Win32 / Emotet.C, desde noviembre del año pasado. Esta nueva variante se envió como parte de una campaña de correo electrónico spam que alcanzó su punto máximo en noviembre.

Los **mensajes de spam** se escriben de una manera tal que ganan fácilmente la atención de las posibles víctimas. Podría pasar por algún tipo de reclamación fraudulenta, como una factura de teléfono, una factura de un banco o un mensaje de PayPal.

Una vez que infecta un sistema, Emotet descarga un archivo de configuración que contiene una lista de bancos y servicios que está diseñado para robar credenciales, y también descarga un archivo que intercepta y registra el tráfico de la red.

El rastreo de la Red es especialmente una parte inquietante de este malware, ya que un atacante puede conocer toda la información que se intercambia en la red. En resumen, los usuarios pueden andar con sus operaciones bancarias en línea sin siquiera darse cuenta de que sus datos están siendo robados.

Emotet podría brindar credenciales de una variedad de programas de correo electrónico, incluidas las versiones de de Microsoft Outlook, Thunderbird de Mozilla y programas de mensajería instantánea como Yahoo Messenger y Windows Live Messenger.

> *Toda la información robada es enviada de nuevo a Emotet «comando y control de servidor donde se utiliza por otros componentes para enviar mensajes de spam y asi propagar la amenaza (C & C),» escribió Kang. «Detectamos el componente de Spam Emotet como Spammer: Win32 / Cetsiol.A.»*

Los mensajes de spam de Emotet que contienen el malware, son difíciles de filtrar para los servidores de correo

electrónico, porque en realidad se originan a partir de las cuentas de correo electrónico legítimo. Por lo tanto, las técnicas anti-spam típicas, como la verificación de devolución de llamada, no serán aplicables en él.