El malware Emotet piratea redes WiFi para infectar a sus víctimas

Autor: I. Stepanenko

Fecha: Friday 23rd of October 2020 11:03:03 AM

Emotet, el troyano detrás de una serie de campañas se spam impulsadas por botnets y ataques de ransomware, encontró un nuevo vector de ataque: el uso de dispositivos ya infectados para identificar nuevas víctimas que están conectadas a redes Wi-Fi cercanas.

Según los investigadores de Binary Defense, la muestra recientemente descubierta de Emotet aprovecha un módulo *«esparcidor de WiFi»* para escanear redes de WiFi, y luego intenta infectar los dispositivos que están conectados a ellas.

La compañía de seguridad cibernética dijo que el difusor de WiFi tiene una marca de tiempo del 16 de abril de 2018, lo que indica que el comportamiento de propagación ha estado funcionando *«inadvertido»* durante casi dos años hasta que se detectó por primera vez el mes pasado.

El desarrollo marca una escalera de las capacidades de Emotet, ya que las redes cercanas a la víctima original ahora son susceptibles a la infección.

La versión actualizada del malware funciona al aprovechar un host ya comprometido para enumerar todas las redes WiFi cercanas. Para esto, utiliza la interfaz wlanAPI para extraer el SSID, la intensidad de la señal, el método de autenticación (WPA, WPA2 o WEP) y el modo de cifrado utilizado para proteger las contraseñas.

Al obtener la información para cada red de esta forma, el gusano intenta conectarse a las redes mediante un ataque de fuerza bruta utilizando las contraseñas obtenidas de una de las dos listas de contraseñas internas. Siempre que la conexión falle, pasa a la siguiente contraseña de la lista. No está claro cómo se creó la lista de las contraseñas.

Si la operación tiene éxito, el malware conecta el sistema comprometido en la red de acceso reciente y comienza a enumerar todos los recursos compartidos no ocultos. Después, lleva a cabo una segunda ronda de ataque de fuerza bruta para adivinar los nombres de usuario y las contraseñas de todos los usuarios conectados al recurso de red.

Después de tener usuarios forzados con fuerza bruta y sus contraseñas, el gusano pasa a la siguiente fase instalando cargas maliciosas, llamadas *«service.exe»*, en los sistemas remotos recién infectados. Para ocultar su comportamiento, la carga útil se instala como un servicio del sistema de Windows Defender (WinDefService).

Además de comunicarse con un servidor de comando y control (C2), el servicio actúa como un cuentagotas y ejecuta el binario Emotet en el host infectado.

El hecho de que Emotet pueda saltar de una red WiFi a otra pone a las empresas a su disposición para proteger sus redes con contraseñas seguras para evitar el acceso no autorizado. El malware también se puede detectar monitoreando activamente los procesos que se ejecutan desde carpetas temporales y carpetas de datos de aplicaciones de perfil de usuario.

Emotet se identificó por primera vez en 2014, y se ha transformado de un troyano bancario a *«una navaja suiza»* que puede servir como descargador, ladrón de información y spambot dependiendo de cómo se implemente.

Con los años, también ha sido un mecanismo de entrega eficaz para ransomware. La red de TI de Lake City quedó paralizada en junio pasado luego de que un empleado abriera por accidente un correo electrónico sospechoso que descargó el troyano Emotet, que a su vez descargó el troyano TrickBot y el ransomware Ryuk.

Aunque las campañas impulsadas por Emotet desaparecieron en gran medida durante el verano de 2019, regresaron en septiembre por medio de *«correos electrónicos orientados geográficamente con señuelos y marcas en el idioma local, a menudo de temas financieros, y utilizando archivos adjuntos de documentos maliciosos o enlaces a documentos similares, que cuando los usuarios habilitaron macros, instalaron Emotet».*

> «Con este tipo de cargador recientemente descubierto utilizado por Emotet, se introduce un nuevo vector de amenaza a las capacidades de Emotet. Emotet puede usar este tipo de cargador para propagarse a través de redes inalámbricas cercanas si las redes usan contraseñas inseguras», dijeron los investigadores de Defensa Binaria.