La botnet Emotet, que regresó en noviembre de 2021 luego de una pausa de 10 meses, muestra una vez más signos de crecimiento constante, acumulando un enjambre de más de 100 mil hosts infectados por perpetrar sus actividades maliciosas.

> *«Aunque Emotet aún no ha alcanzado la misma escala que alguna vez tuvo, la botnet está mostrando un fuerte resurgimiento con un total de aproximadamente 130 mil bots únicos repartidos en 179 países desde noviembre de 2021»,* dijeron investigadores de Black Lotus Labs de Lumen.

Emotet, antes de su desmantelamiento a fines de enero de 2021 como parte de una operación policial coordinada denominada «Ladybird», había infectado no menos de 1.6 millones de dispositivos en todo el mundo, actuando como conducto para que los atacantes instalaran otros tipos de malware, como troyanos bancarios o ransomware en los sistemas comprometidos.

El malware resurgió oficialmente en noviembre de 2021 utilizando TrickBot como vehículo de entrega, y este último cerró su infraestructura de ataque a fines del mes pasado después de que varios miembros clave del grupo fueran absorbidos por el cartel del ransomware Conti.

Al parecer, la resurrección de Emotet fue orquestada por la propia pandilla Conti en un intento de cambiar la táctica en respuesta al mayor escrutinio policial sobre las actividades de distribución de malware de TrickBot.

Black Lotus Labs dijo que la *«agregación de bots realmente no comenzó en serio hasta enero»*, y dijo que las nuevas variantes de Emotet cambiaron el esquema de cifrado RSA a favor de la criptografía de curva elíptica (ECC) para cifrar el tráfico de red.

Otra nueva incorporación a sus capacidades es su capacidad para recopilar información adicional del sistema más allá de una lista de procesos en ejecución de las máquinas comprometidas.

Además, la infraestructura de botnet de Emotet abarca casi 200 servidores de comando y control (C2), con la mayoría de los dominios ubicados en Estados Unidos, Alemania, Francia, Brasil, Tailandia, Singapur, Indonesia, Canadá, Reino Unido e India.

Los bots infectados, por otro lado, se concentran en gran medida en Asia, principalmente en Japón, India, Indonesia y Tailandia, seguidos de Sudáfrica, México, Estados Unidos, China, Brasil e Italia. *«Esto no es sorprendente dada la preponderancia de hosts de Windows vulnerables u obsoletos en la región»,* dijeron los investigadores.

> *«El crecimiento y la distribución de bots es un indicador importante del progreso de Emotet en la restauración de su infraestructura que alguna vez fue en expansión. Cada bot es un punto de apoyo potencial para una red codiciada y presenta una oportunidad para implementar Cobalt Strike o eventualmente ser promovido a un Bot C2»,* dijo Black Lotus Labs.