Los operadores vinculados al malware QakBot (también conocido como QBot) han puesto en marcha 15 nuevos servidores de comando y control (C2) a finales de junio de 2023.

Estos descubrimientos son una continuación del análisis de la infraestructura del malware realizado por el Equipo Cymru y llegan un poco más de dos meses después de que Lumen Black Lotus Labs revelara que el 25% de sus servidores C2 están activos solo durante un día.

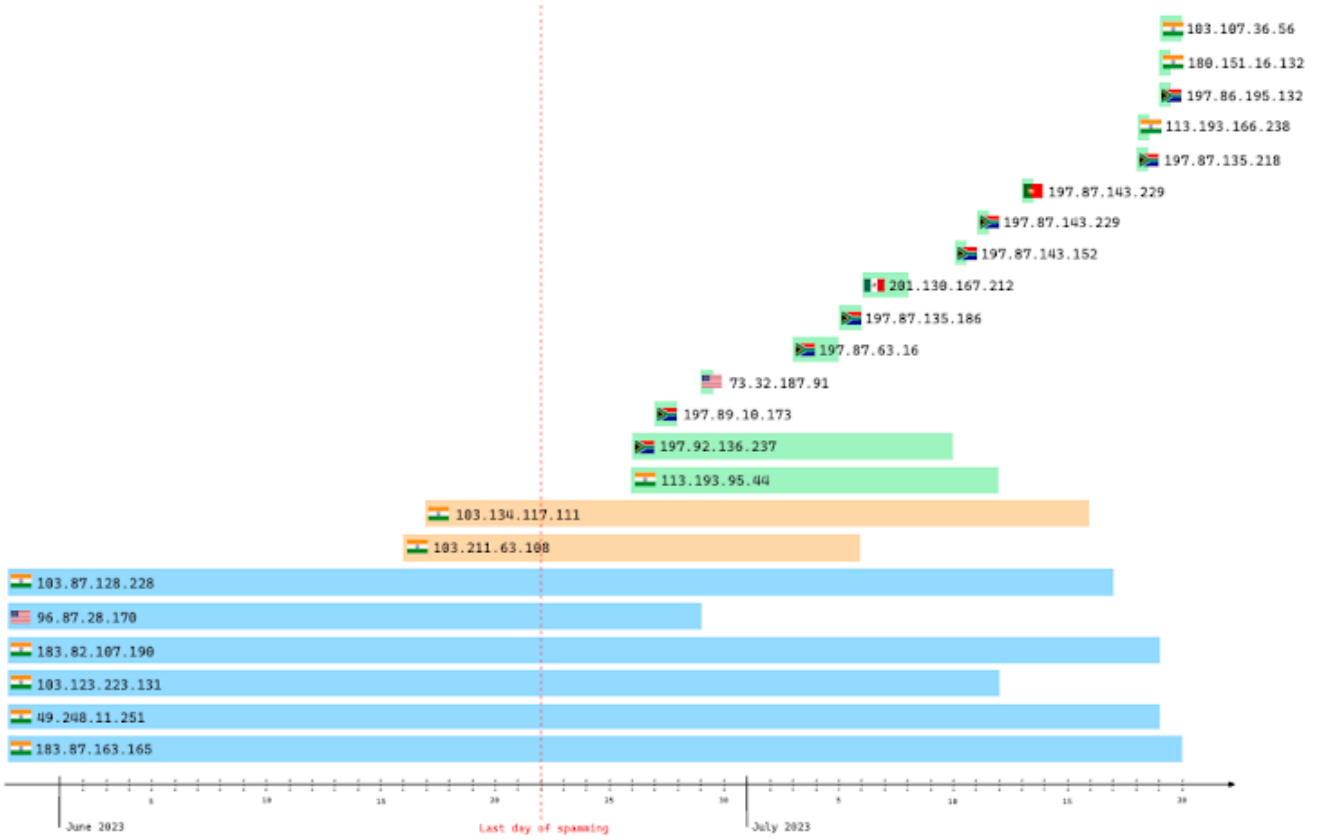
> *«QakBot tiene un historial de tomarse un descanso prolongado cada verano antes de regresar en algún momento de septiembre. Las actividades de envío de spam de este año se detuvieron alrededor del 22 de junio de 2023»,* indicó la empresa de ciberseguridad.

> *«Pero, ¿realmente están de vacaciones los operadores de QakBot cuando no están enviando spam, o es este 'descanso' un tiempo que utilizan para mejorar y actualizar su infraestructura y herramientas?»*

La red C2 de QakBot, similar a lo observado en los casos de Emotet e IcedID, se caracteriza por una arquitectura escalonada en la que los nodos C2 se comunican con nodos de nivel 2 (T2) ubicados aguas arriba, alojados en proveedores de servicios virtuales (VPS) con geolocalización en Rusia.

La mayoría de los servidores C2 de bots, que mantienen comunicación con las máquinas víctimas, se encuentran en India y Estados Unidos. Las direcciones IP de destino identificadas en las conexiones T2 salientes se localizan principalmente en Estados Unidos, India, México y Venezuela.

También presente junto a los C2 y los T2 C2 se encuentra un servidor BackConnect (BC) que convierte a los bots infectados en un proxy para otros fines maliciosos.



La más reciente investigación del Equipo Cymru revela que la cantidad de C2 existentes que están comunicándose con la capa T2 ha experimentado una disminución considerable, quedando únicamente ocho en funcionamiento. Este declive se debe en parte a la acción de Black Lotus Labs de anular la ruta hacia la infraestructura de nivel superior en mayo de 2023.

«Observamos que para el 2 de junio, los C2 en Estados Unidos prácticamente habían desaparecido, y el tráfico proveniente de los C2 en India había disminuido de manera significativa», indicó la compañía, atribuyendo la falta de actividad en Estados Unidos a la anulación de la ruta hacia la capa T2.

Aparte de los 15 servidores C2, seis servidores C2 que ya estaban activos antes de junio y dos servidores C2 que comenzaron a operar en junio, han continuado mostrando actividad

durante julio después de finalizar el envío de correos no deseados (spam).

Un análisis más detallado de los datos de flujo de red revela un patrón en el que *«los momentos de incremento en las conexiones T2 salientes a menudo coinciden con aumentos en la actividad de las conexiones entrantes de los C2 de los bots», y «los picos de conexiones T2 salientes frecuentemente concuerdan con una disminución en la actividad de los C2 de los bots».*

> *«Al transformar a las víctimas en infraestructura C2 con comunicación T2, QakBot efectivamente castiga a los usuarios en dos ocasiones: primero, en la comprometida inicial, y segundo, en el riesgo potencial para la reputación de un host que pueda ser identificado públicamente como malicioso»,* señaló el Equipo Cymru.

Al bloquear las comunicaciones hacia los servidores aguas arriba, la compañía resaltó que se evita que las víctimas reciban instrucciones de los C2, protegiendo de manera efectiva a los usuarios actuales y futuros contra posibles compromisos.