Los investigadores en ciberseguridad han proporcionado más detalles sobre un actor chino denominado SecShow, que ha sido observado llevando a cabo actividades relacionadas con el Sistema de Nombres de Dominio (DNS) a nivel global desde al menos junio de 2023.

El adversario, según los investigadores de seguridad de Infoblox, la Dra. Renée Burton y Dave Mitchell, opera desde la Red China de Educación e Investigación (CERNET), un proyecto financiado por el gobierno chino.

> *«Estas sondas buscan encontrar y medir las respuestas DNS en resolutores abiertos. El objetivo final de las operaciones de SecShow es desconocido, pero la información recopilada puede ser utilizada para actividades maliciosas y solo beneficia al actor»*, afirmaron en un informe publicado la semana pasada.

Dicho esto, hay alguna evidencia que sugiere que podría estar vinculado a algún tipo de investigación académica relacionada con *«realizar mediciones utilizando técnicas de suplantación de direcciones IP en dominios dentro de secshow.net»*, empleando la misma técnica que el Closed Resolver Project.

Sin embargo, esto plantea más preguntas de las que responde, incluyendo el alcance total del proyecto, el propósito detrás de la recopilación de datos, la elección de una dirección de Gmail genérica para recibir comentarios y la falta general de transparencia.

Los resolutores abiertos son servidores DNS capaces de aceptar y resolver nombres de dominio de manera recursiva para cualquier usuario en internet, lo que los hace vulnerables a ser explotados por actores malintencionados para iniciar ataques distribuidos de denegación de servicio (DDoS), como un ataque de amplificación DNS.

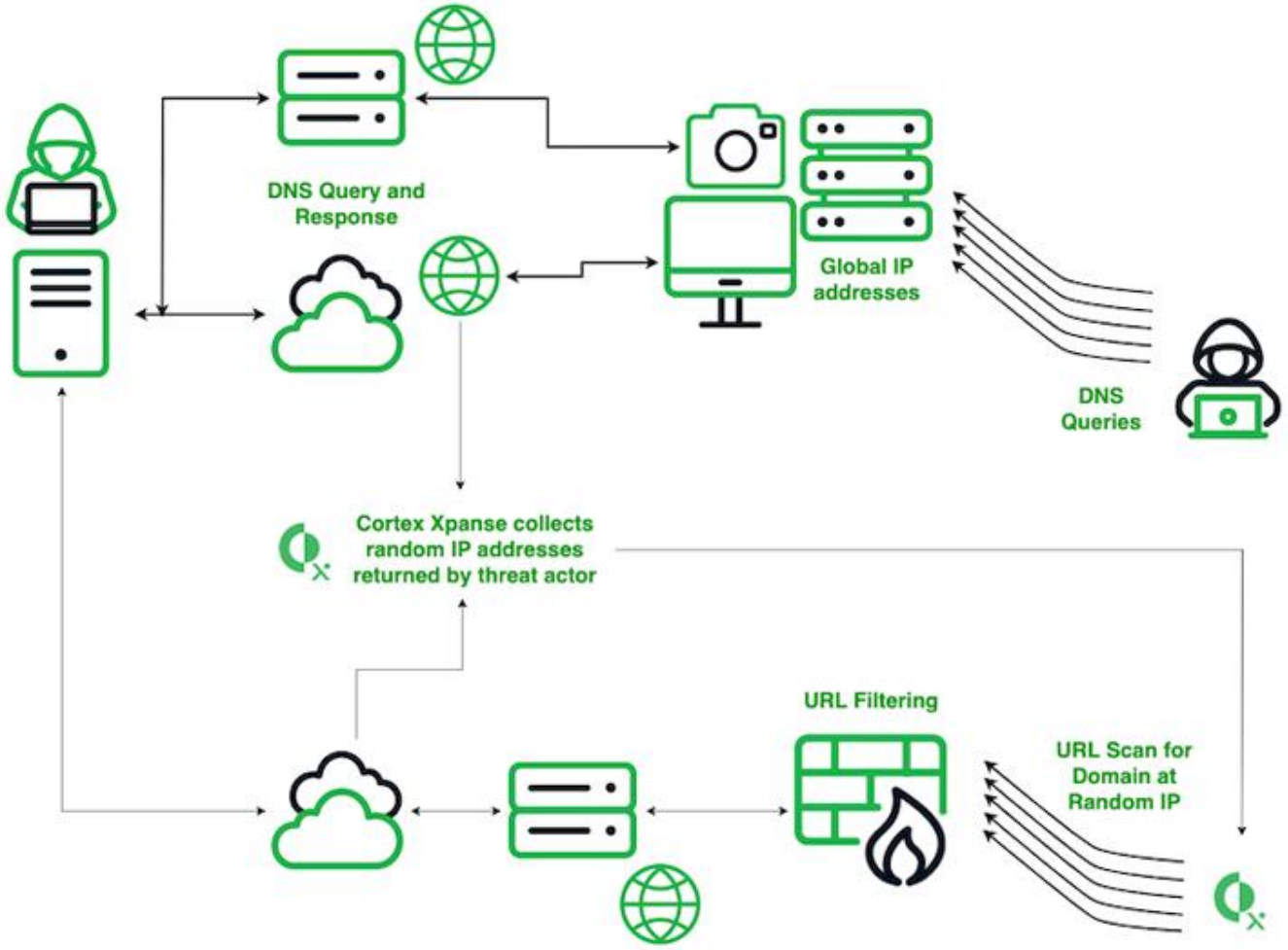
En el centro de las sondas está el uso de los servidores de nombres de CERNET para identificar resolutores DNS abiertos y calcular respuestas DNS. Esto implica enviar una consulta DNS desde un origen aún no determinado a un resolutor abierto, haciendo que el servidor de nombres controlado por SecShow devuelva una dirección IP aleatoria.

En un giro interesante, estos servidores de nombres están configurados para devolver una nueva dirección IP aleatoria cada vez que la consulta se realiza desde un resolutor abierto diferente, un comportamiento que desencadena una amplificación de consultas por el producto Cortex Xpanse de Palo Alto.

> *«Cortex Xpanse trata el nombre de dominio en la consulta DNS como una URL e intenta recuperar contenido desde la dirección IP aleatoria para ese nombre de dominio. Los firewalls, incluyendo Palo Alto y Check Point, así como otros dispositivos de seguridad, realizan filtrado de URL cuando reciben la solicitud de Cortex Xpanse»,* explicaron los investigadores.

Este paso de filtrado inicia una nueva consulta DNS para el dominio, lo que hace que el servidor de nombres devuelva una dirección IP aleatoria diferente.

Es importante destacar que algunos aspectos de estas actividades de escaneo fueron revelados previamente por Dataplane.org y los investigadores de Unit 42 en los últimos dos meses. Los servidores de nombres de SecShow dejaron de responder desde mediados de mayo de 2024.



SecShow es el segundo actor de amenazas vinculado a China, después de Muddling Meerkat, en llevar a cabo actividades de sondeo DNS a gran escala en internet.

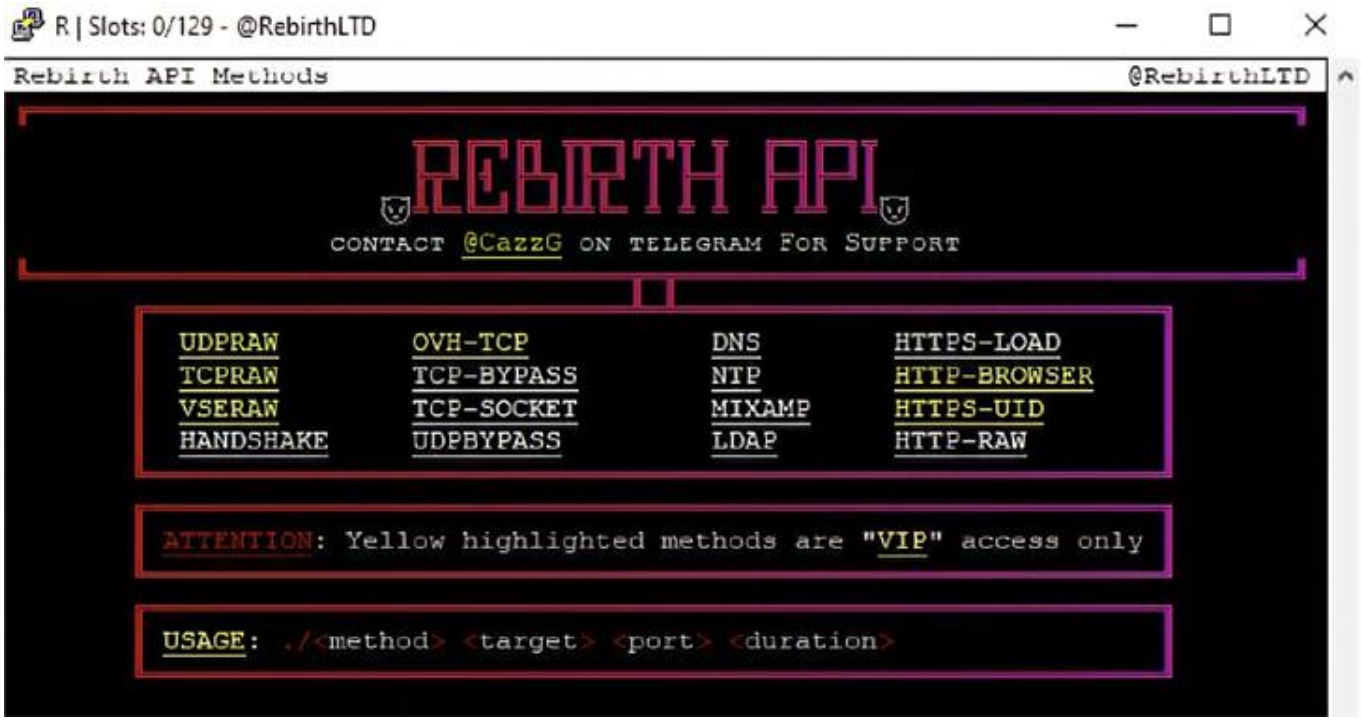
> *«Las consultas de Muddling Meerkat están diseñadas para mezclarse con el tráfico DNS global y han pasado desapercibidas durante más de cuatro años, mientras que las consultas de SecShow son codificaciones transparentes de direcciones IP y datos de medición»,* explicaron los investigadores.

Rebirth Botnet Ofrece Servicios DDoS

Este desarrollo ocurre cuando un actor de amenazas con motivaciones financieras ha sido identificado promocionando un nuevo servicio de botnet llamado Rebirth para facilitar ataques DDoS.

El botnet DDoS como Servicio (DaaS) está *«basado en la familia de malware Mirai, y los operadores anuncian sus servicios a través de Telegram y una tienda en línea (rebirthltd.mysellix[.]io)»*, dijo el Equipo de Investigación de Amenazas de Sysdig en un análisis reciente.

La empresa de ciberseguridad señaló que Rebirth (también conocido como Vulcan) se enfoca principalmente en la comunidad de videojuegos, alquilando el botnet a otros actores a varios precios para atacar servidores de juegos con fines de lucro. La evidencia más temprana del uso del botnet en el campo data de 2019.



El plan más económico, llamado Rebirth Basic, cuesta $15, mientras que los niveles Premium, Advanced y Diamond tienen precios de $47, $55 y $73 respectivamente. También hay un plan de ACCESO API de Rebirth que se vende por $53.

El malware Rebirth permite lanzar ataques DDoS utilizando los protocolos TCP y UDP, como TCP ACK flood, TCP SYN flood y UDP flood.

Esta no es la primera vez que los servidores de juegos han sido atacados por botnets DDoS. En diciembre de 2022, Microsoft reveló detalles de otro botnet llamado MCCrash diseñado para atacar servidores privados de Minecraft.

Luego, en mayo de 2023, Akamai describió un botnet de DDoS por encargo conocido como Dark Frost, que ha sido observado lanzando ataques DDoS a empresas de videojuegos, proveedores de alojamiento de servidores de juegos, streamers en línea e incluso otros miembros de la comunidad de juegos.

> *«Con un botnet como Rebirth, una persona puede realizar un ataque DDoS al servidor del juego o a otros jugadores en un juego en vivo, haciendo que los juegos se ralenticen o se cuelguen o que las conexiones de otros jugadores se retrasen o se caigan»,* explicó Sysdig.
>
> *«Esto puede estar motivado financieramente para los usuarios de servicios de streaming como Twitch, cuyo modelo de negocio depende de que un jugador en streaming gane seguidores; esto esencialmente proporciona una forma de ingreso a través de la monetización de un juego defectuoso».*

La empresa con sede en California sugirió que los clientes potenciales de Rebirth también podrían usarlo para realizar trolling DDoS (también conocido como stresser trolling), donde se lanzan ataques contra servidores de juegos para interrumpir la experiencia de los jugadores legítimos.

Las cadenas de ataque que distribuyen el malware implican la explotación de vulnerabilidades de seguridad conocidas (por ejemplo, CVE-2023-25717) para desplegar un script bash que se encarga de descargar y ejecutar el malware del botnet DDoS según la arquitectura del procesador.

El canal de Telegram asociado con Rebirth ha sido eliminado para borrar todas las publicaciones antiguas, con un mensaje publicado el 30 de mayo de 2024, diciendo *«Pronto regresamos».* Casi tres horas después, anunciaron un servicio de alojamiento a prueba de balas llamado *«bulletproof-hosting[.]xyz».*