El actor de amenazas con vínculos en Pakistán, conocido como SideCopy, ha sido detectado utilizando la reciente vulnerabilidad de seguridad en WinRAR en sus ataques dirigidos a organismos gubernamentales en la India, con el fin de distribuir diversos troyanos de acceso remoto, tales como AllaKore RAT, Ares RAT y DRat.

La firma de seguridad empresarial SEQRITE ha descrito esta campaña como una operación de múltiples plataformas, ya que los ataques también han sido diseñados para infiltrar sistemas Linux que sean compatibles con una versión de Ares RAT.

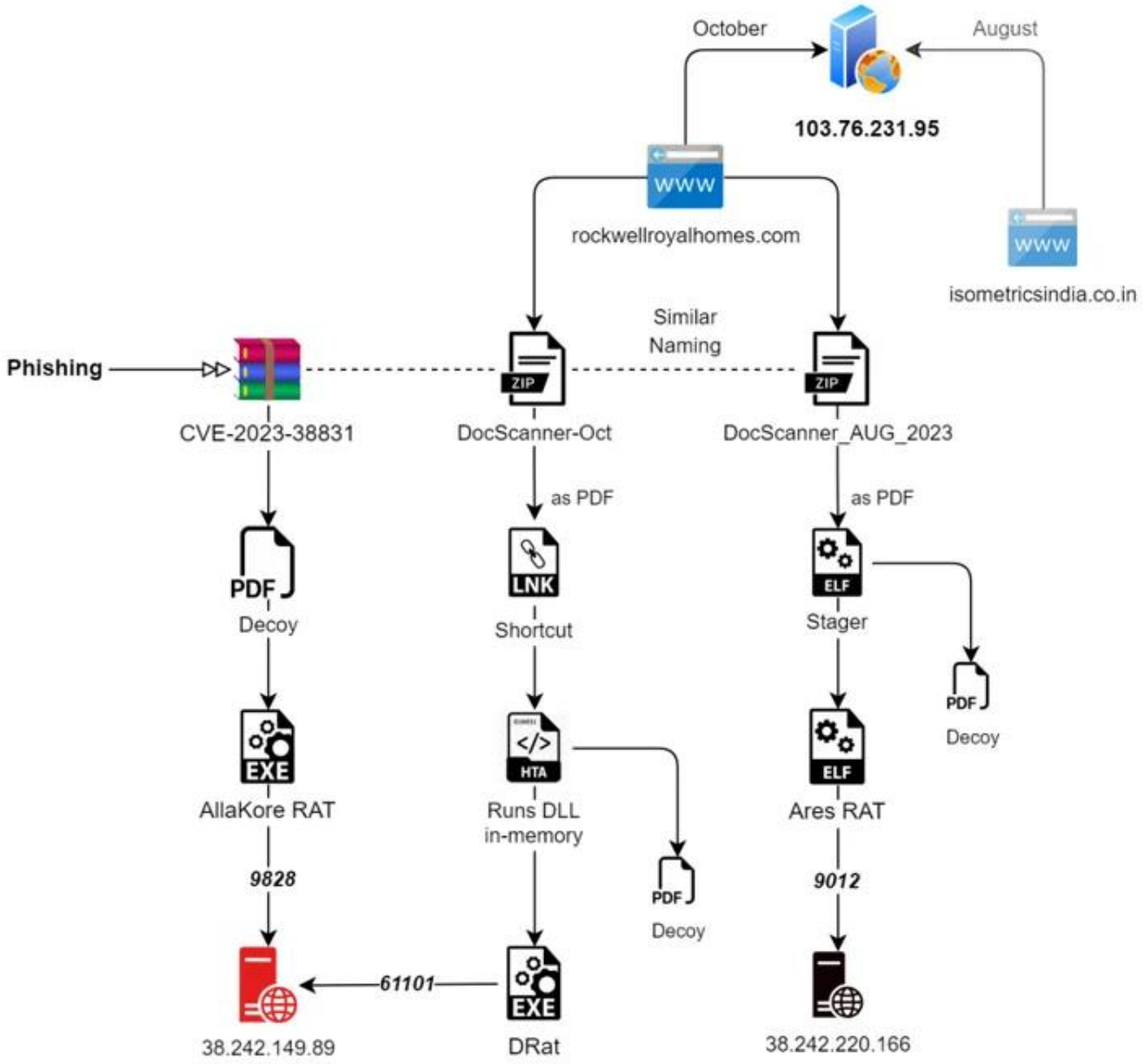
SideCopy ha estado activo desde al menos 2019 y es conocido por sus ataques dirigidos a entidades en la India y Afganistán. Se sospecha que podría ser un subgrupo del actor conocido como Transparent Tribe (también identificado como APT36).

> *«SideCopy y APT36 comparten tanto infraestructura como código para llevar a cabo agresivos ataques contra la India»*, señaló el investigador de SEQRITE, Sathwik Ram Prakki, en un informe publicado el lunes.

En mayo anterior, este grupo fue vinculado a una campaña de phishing que se valía de señuelos relacionados con la Organización de Investigación y Desarrollo de Defensa de la India (DRDO) para distribuir malware destinado al robo de información.

Desde entonces, SideCopy también ha sido vinculado a una serie de ataques de phishing que tenían como objetivo el sector de defensa de la India, y que utilizaban archivos adjuntos en formato ZIP para propagar el troyano Action RAT, así como un nuevo troyano basado en .NET que tiene la capacidad de ejecutar 18 comandos diferentes.

Las nuevas campañas de phishing que han sido detectadas por SEQRITE implican dos cadenas de ataque diferentes, cada una de ellas dirigida a sistemas operativos Linux y Windows.



La primera se centra en un binario ELF basado en Golang, que allana el camino para una versión de Ares RAT compatible con Linux, capaz de enumerar archivos, tomar capturas de pantalla y realizar descargas y cargas de archivos, entre otras funciones.

Por otro lado, la segunda campaña involucra la explotación de CVE-2023-38831, una vulnerabilidad de seguridad en la herramienta de archivado WinRAR, con el fin de desencadenar la ejecución de código malicioso que da lugar a la implantación de AllaKore RAT, Ares RAT y dos nuevos troyanos conocidos como DRat y Key RAT.

> *«[AllaKore RAT] posee funcionalidades para robar información del sistema, registrar pulsaciones de teclado, tomar capturas de pantalla, cargar y descargar archivos, además de tomar el control remoto de la máquina de la víctima para recibir comandos y cargar datos robados en el C2»,* mencionó Ram Prakki.

DRat tiene la capacidad de interpretar hasta 13 comandos provenientes del servidor C2 para recopilar información del sistema, descargar y ejecutar cargas útiles adicionales y llevar a cabo otras operaciones relacionadas con archivos.

La orientación hacia Linux no es fortuita y probablemente esté motivada por la decisión de la India de reemplazar Microsoft Windows por una variante de Linux conocida como Maya OS en los sectores gubernamentales y de defensa.

> *«Mediante la expansión de su arsenal con vulnerabilidades de día cero, SideCopy se enfoca de manera constante en atacar a organizaciones de defensa en la India utilizando diversos troyanos de acceso remoto»*, afirmó Ram Prakki.

> *«APT36 continúa ampliando su conjunto de herramientas en el ámbito de Linux de forma constante, y se ha observado que comparte implementaciones de Linux con SideCopy para llevar a cabo la distribución de un troyano de acceso remoto de código abierto basado en Python conocido como Ares».*