Aunque Rusia aún mantiene una reputación de economía estancada y sin diversificar, fue uno de los primeros países del mundo en darse cuenta del valor de las intrusiones cibernéticas realizadas remotamente.

En los últimos años, muchos grupos de hackers de Rusia se han convertido en los actores más sofisticados de los Estados-nación en el ciberespacio, produciendo técnicas de piratería y kits de herramientas altamente especializados para el espionaje cibernético.

En los últimos 30 años, muchos incidentes de piratería de alto perfil, como infiltrarse en las elecciones presidenciales de Estados Unidos, dirigirse a un país con el ransomware NotPetya, causar un apagón en la capital ucraniana Kiev, y la violación del Pentágono, se han atribuido a grupos de hackers rusos, incluyendo Fancy Bear (Sofacy), Turla, Cozy Bear, Sandworm Team y Berserk Bear.

Además de expandir de forma continua sus capacidades de guerra cibernética, el ecosistema de los grupos APT rusos también se ha convertido en una estructura muy compleja, lo que hace que sea más difícil entender quienes son los actores en el espionaje cibernético ruso.

Mientras tanto, los investigadores de Intezer y Check Point Research, unieron sus esfuerzos para lanzar un mapa interactivo basado en la web que ofrece una visión general completa sobre este ecosistema.

Denominado como «Mapa APT ruso», cualquiera puede hacer uso de él para obtener información sobre las conexiones entre diferentes muestras del malware APT ruso, familias de malware y actores de amenazas, todo simplemente haciendo clic en los nodos en el mapa.

> *«El mapa es básicamente una ventanilla única para cualquier persona interesada en aprender y comprender las conexiones y atribuciones de las muestras, módulos, familias y actores que juntos componen este ecosistema. Al hacer clic en los nodos en el gráfico, se mostrará un panel lateral que contiene información sobre la familia*

> *de malware a la que pertenece el nodo, así como enlaces a informes de análisis en la plataforma de Intezer y enlaces externos a artículos y publicaciones relacionados»*, dijeron los investigadores a THN.

Este mapa es el resultado de una investigación exhaustiva en la que los investigadores reunieron, clasificaron y analizaron más de 2000 muestras de malware atribuidas a grupos de piratería rusos, y mapearon cerca de 22 mil conexiones entre ellos a 3.85 millones de piezas de código que compartieron.

> *«Cada actor u organización bajo el paraguas Russian APT tiene sus propios equipos dedicados de desarrollo de malware, trabajando durante años en paralelo en kits de herramientas y marcos de malware similares. Sabiendo que muchos de estos kits de herramientas tienen el mismo propósito, es posible detectar redundancia en esta actividad paralela».*

El mapa ruso APT también revela que, aunque la mayoría de los grupos de hackers estaban reutilizando su propio código en sus propias herramientas y marcos, no se encontraron grupos diferentes utilizando el código.

> *«Al evitar que diferentes organizaciones reutilicen las mismas herramientas en una amplia gama de objetivos, superan el riesgo de que una operación comprometida exponga otras operaciones activas, evitando el colapso de un castillo de naipes sensible»,* agregaron los investigadores.

Otra hipótesis es que las diferentes organizaciones no comparten código debido a la *«política interna»*.

Para hacerlo más eficiente y actualizado en el futuro, los investigadores abrieron el mapa y

los datos detrás de él.

Además, los investigadores también lanzaron una herramienta de escaneo basada en reglas de Yara, denominada «Detector APT ruso», que cualquier usuario puede utilizar para escanear un archivo específico, una carpeta o un sistema de archivos completo y buscar infecciones por piratas informáticos rusos.