Analizaremos parte de las IPs conseguidas mediante consultas y las geolocalizaciones mostradas en el Dataset objeto de estudio

A - IPs origen ciberataques: focos o lugares importantes en el análisis de estas IPs:

1.- Numerosas IPs han salido en el mar y en la zona de la Antártida, pudiendo tratarse de un error o el uso de VPN, proxys o la red Tor, para ocultar la ubicación real los delincuentes.

2.- En África, se observa un fuerte lugar de concentración, siendo Somalia e Etiopía. Aquí aparecen frente a las costas de Somalia existe un fuerte problema con la Piratería, por lo que podrían tratarse de barcos con sistemas parala conexión a internet(vía satélite u otras).

3.- La zona del Golfo de Adén, Yemen, Omán, Emiratos Árabes (EAU)[mucha concentración] Irán, Pakistán, Arabia Saudita(zona cerca de Jordania),Irak, Irán, Siria, Chipre, Turquía, gran concentración en la zona sur de Ucrania( Sebastopol y en la Bahía de Arabat) u en la zona Norte( Rivne y alrededores), Bielorrusia( gran concentración), Lituania. y algún otro país del este, Rusia y una gran acumulación alrededor de las Islas Georgias del Sur y Sandwich del Sur, situadas en el atlántico Sur(GSGSSI), pertenecientes a Reino Unido.

EXPLICACIONES:

1.- Zona Antártida y alrededores marítimos.- La ubicación remota, poco poblada, condiciones climáticas adversas, déficit de infraestructura de telecomunicaciones, lo cual dificulta la identificación de la ubicación real de los ciberatacantes y su investigación, asi como la vigilancia de las comunicaciones electrónicas.

2.- En Somalia, su zona costera, el golfo de Edén hasta Yemen, existe alta concentración de orígenes de ciberataques. Estos países del "Cuerno de África" destacan por inestabilidad política, pobreza, desigualdad y violencia, un caldo de cultivo propio para la actividad cibercriminal, formada por grupos motivado por fines de lucro, políticos o religiosos, destacando en ataques DDoS y Malware.

3.- Emiratos Árabes( EAU).- Las causas del origen de los ataques se basan en que poseen una infraestructura de telecomunicaciones avanzada, alta alfabetización en tecnologías, y un régimen político autoritario, que dificulta su investigación, facilitando la contratación de cibercriminales y el lanzamiento de ataques cibernéticos desde su territorio, destacando en ataques DDoS y Malware.

4.- Pakistán, Irán y la India. - Pakistán e Irán han sido acusados de efectuar numerosos ataques contra otras organizaciones gubernamentales de EEUU e Israel, con apoyo de sus gobiernos a los cibercriminales. Por otra parte, la India, también ha sido acusada de realizar ataques contra Pakistán, China y otros países, destacando en ataques DDoS, Malware, Intrusión.

Hay que tener en cuenta que existe una columna dentro del Dataset, con geolocalizaciones en ciudades de los 28 estados de la India, apareciendo, entre ostras muchas, las ciudades más importantes de la India como Delhi, Mumbai,Kolkata , Chennai , Bengaluru , Hyderabad , Ahmedabad , Pune y Surat , apareciendo un número muy elevado de veces.

5.- Arabia Saudita (Zona cercana a Jordania). - Es un fuerte aliado de EEUU y con un gran poder militar, habiendo sido acusados de usar ciberataques por intrusión para espiar a sus opositores, apoyando económica y logísticamente desde el gobierno a estos cibercriminales. Además, se encentra en una región estratégica, lo que le da un acceso fácil a redes globales.

6.- Irak y Siria. - El conflicto bélico en Irak y Siria favorece los ciberataques, que han tenido un impacto organizaciones de todo el mundo, provocando inestabilidad política y económica en la región, lo que ha debilitado sus capacidades de ciberseguridad, creando un entorno de confusión y caos, lo que facilita a los ciberatacantes operar sin ser detectados, destacando en ataques DDoS y Malware.

-Ucrania. - Los ataques cibernéticos de Ucrania se han vuelto más sofisticados a medida que la guerra contra Rusia, dirigiendo los mismos a una amplia gama de objetivos, incluyendo infraestructuras críticas, empresas privadas y organizaciones gubernamentales, los cuales han tenido un impacto significativo en la capacidad de Rusia para llevar a cabo su invasión de Ucrania.

En este punto hay que destacar que, los ataques cibernéticos de Ucrania son un ejemplo de cómo la ciberguerra está jugando un papel cada vez más importante en los conflictos modernos, pudiendo ser utilizados para debilitar a un adversario, interrumpir sus operaciones y difundir desinformación.

7.- Bielorrusia. - Es un país atractivo para los cibercriminales, debido a que tiene un gobierno autoritario que es tolerante con la actividad cibercriminal, además de ser una población altamente alfabetizada y con acceso a Internet, lo que la convierte en un buen caldo de cultivo para llevar a cabo ciberataques.

- GSGSSI. - Las Islas Georgias del Sur y Sandwich del Sur pertenecientes a Reino Unido, están deshabitadas, existiendo únicamente un centro de investigación científica, el cual sufrió un gran ataque en 2023(Infraestructura Crítica Europeas). Además, al estar en una ubicación remota y con pocas medidas de vigilancia, los ciberdelincuentes han usado las IPs de estas islas, para lanzar ataques contra organizaciones gubernamentales y privadas de todo el mundo, ocultando de esta forma su ubicación real.

B - IPs destino ciberataques: focos o lugares importantes en el análisis de estas IPs:

1.- Zona Antártida y alrededores marítimos. - Como ya dijimos, zona poco poblada con una infraestructura tecnológica limitada y vulnerable, dependiendo en gran medida de satélites para su funcionamiento, donde se llevan a cabo investigaciones científicas, comerciales y militares. Además, es un territorio de interés geopolítico para muchos países que quieren establecer bases en esa zona, generando conflictos y tensiones diplomáticas. Por todo ello, existe una gran concentración de ataques en esta zona, aunque también pueden usar ésta, para camuflar su ubicación real los ciberdelincuentes

2.- En Somalia, su zona costera, el golfo de Edén hasta Yemen: Alta concentración de ataques, que por la inestabilidad política y de seguridad en estas regiones, pueden fomentar el uso de estos países por los cibercriminales para ocultar su ubicación. EL golfo de Edén es una importante vía de comunicación y navegación para el comercio, existiendo intereses geopolíticos sobre su control. Además. Como ya se comentó, Somalia es un país donde la piratería marítima es medio de vida, por lo al igual que realizan ataques como ya vimos en el apartado anterior, puede ser objetivo de los mismos.

3.- Emiratos Árabes(EAU).- País con gran importancia política y económica en Oriente Medio, teniendo a Dubái con centro financiero y de negocios a nivel mundial, unido a la presencia de infraestructuras tecnológicas avanzadas, el amplio uso de ellas por la población, hacen que los cibercriminales busquen lucrarse explotando vulnerabilidades de los sistemas, siendo los principales ataques recibidos intrusión(espionaje) y activismo cibernético para mostrar discrepancias políticas o empresariales.

4.- Arabia Saudita. - Este País ha sufrido ataques interno y externamente por grupos de cibercriminales, motivados por ánimo de lucro, debido a sus grandes reservas de petróleo y de gas, que buscan información confidencial o causar daños a sus instalaciones. Además, es un país con gran influencia política y religiosa en la zona de Oriente Medio, por lo que está en el objetivo de grupos radicales o terroristas con la intención de desestabilizarlo.

5. Irak y Siria. - Irak es un país que ha sido escenario de conflictos geopolíticos, económicos y sociales que pueden motivar a los ciberdelincuentes a atacarlo, unido a sus bajos niveles de seguridad, pudiendo ser usado también, para ocultar la verdadera ubicación de los atacantes. El Centro de Seguridad Cibernética de la Unión Europea (ENISA) incluyó a Irak en su lista de países de alto riesgo porque era un objetivo atractivo para los ciberatacantes, debido a su infraestructura crítica insegura y su falta de recursos para la ciberseguridad. En Siria, se vive una guerra civil desde 2011 entre el gobierno reconocido internacionalmente y los rebeldes apoyados por Rusia e Irán, provocando una grave crisis humanitaria, por lo que es un país en guerra y la ciberguerra forma parte de ella.

6.- Las Islas Georgias del Sur y Sandwich del Sur, han sufrido muchos ciberataques de DDoS y Ataques Malware, debido a sus escasas medidas de seguridad, ya que esta deshabitado y sólo alberga un gran centro de investigación científica de Reino Unido (Infraestructura crítica), el cual sufrió un gran ataque en 2023, habiendo sido usadas sus IPs para ocultar la verdadera ubicación de los cibercriminales en ciberataques.

7.- En la Zona Norte de Italia, aparece en el Dataset una gran concentración en un punto situado cerca Tasullo(zona norte de Italia), donde se concentran una gran cantidad de empresas de infraestructura crítica, como el sector automotriz, el químico y el farmacéutico, por lo que puede ser un objetivo atractivo para los ciberatacantes.