Ensayo: Conflicto Rusia - Ucrania

Luis Felipe Flores Sánchez

Department: Computación
Course: TE3001B - Ciberseguridad II
Instructor: Gualberto Aguilar Torres, PhD.
Date: November 9, 2022

Abstract

Este ensayo tiene como propósito dar a conocer más detalles sobre el conflicto entre Rusia y Ucrania en temas de operaciones cibernéticas, jugando un papel importante sobre el tema de ciberseguridad en la política, ataques en infraestructura crítica, desconfiguración de sitios web y bancos, y redes militares ocasionando ciberataques entre estas dos naciones, así como también conocer algunos marcos de modelación como MITRE ATTCK, MITRE D3FEND, Cyber Kill Chain y Modelado de Diamante.

Hoy en día todas las organizaciones están en riesgo de sufrir ataques cibernéticos, gobiernos, campos empresariales, agencias de inteligencia de todo el mundo y en todos los campos donde se guarde información que pueda ser relevante para sacar un bien propio.Todos estos ataques a medida que avanza el tiempo se vuelven más sofisticados, donde ningún lugar es seguro, existiando la manera de adaptar y poder encontrar vulnerabilidades para posteriormente crear amenazas que atenten con una organización.Esto tomando de base de los marcos complementarios de MITRE ATTCK y MITRE D3FEND, describiendo las técnicas de los adversarios y las contramedidas de defensa respectivamente.

El concepto de ciberseguridad nace de la necesidad de organizaciones de proteger sistemas informáticos de ataques que pudieran comprometer el mal funcionamiento, un gran ejemplo es la guerra Cibernética entre Rusia y Ucrania, donde existe el conflicto entre estos dos países para comprometer datos que pueden ser sensibles de alguna organización. El objetivo principal de las operaciones de ciberataque es cesar la infraestructura crítica que consiste en la extracción o modificación de valiosa información empresarial, tecnológica, militar, o en un ataque de denegación de servicio que paralice las operaciones y dañe a la sociedad o a un grupo de personas.

1 Conflicto Rusia-Ucrania

A lo largo de la historia de ciberataques, Ucrania ha sido principalmente afectada por temas de ciberseguridad interrumpiendo sus sistemas digitales, donde mucha de su infraestructura no se encuentra disponible, diversos grupos asociados a Rusia tienen que ver en intrusiones en todas las acciones ocasionadas a Ucrania. Este conflicto nace de la negativa rusa a aceptar el acercamiento de la OTAN y de la Unión Europea a la antigua república soviética, a la que Moscú considera parte de su identidad y de su espacio de influencia, siendo parte fundamental para empezar ciberataques.(ELPAIS 2022)

Los grupos que se dedican a hacer este tipo de actividades son equipos altamente especializados con una alta preparación y sofisticación que utilizan técnicas complejas para realizar este tipo de acciones, considerados como APTs. A pesar de los avances de análisis de mitigación de vulnerabilidades con software especializado, los actores de APT han mostrado que son capaces de comprome-

ter sistemas mediante el uso de malware especializado, herramientas avanzadas, Exploit que muchos antivirus no pueden detectar donde cada día evoluciona la complejidad de las intrusiones y el conocimiento de amenazas. Y este es el caso para Rusia con todas las APTs asociados con todos estos ataques.

La mitigación viene desde el control de la infraestructura, la seguridad TI se componen de un conjunto de acciones de ciberseuridad que prohiben el acceso no autorizado a computadoras, redes y datos, manteniendo 4 pilares importantes como lo es disponibilidad, integridad, confidencialidad y no repudio sobre la información al bloquear el acceso de lo atacantes, prestando especial cuidado en todo punto, donde según Kevin Mitnick menciona que "Una compañía puede gastar cientos de miles de euros en firewalls, sistemas de cifrado y demás tecnologías de seguridad, pero si un atacante engaña a un empleado, todo ese dinero no habrá servido para nada"(Mitnick, 2020). Dando toda la razón para tener mejores prácticas de ciberseguridad.

No existe como tal un lugar seguro para proteger nuestros sistemas operativos digitales, siempre se tendrán en consideración riesgos, vulnerabilidades, amenazas, actores como APTs en busca de un beneficio propio, este conflicto de Ucrania-Rusia nos da un ejemplo de la búsqueda de poder, con temas de ciberseguridad para derribar un país entero y su infraestructura donde Gene Spafford quien es profesor estadounidense de informática en la Universidad de Purdue y experto en seguridad informática menciona "El único sistema completamente seguro es aquel que está apagado, encerrado en un bloque de cemento y sellado en una habitación rodeada de alambradas y guardias armados"(Spafford, G).

Claro que esto no es posible dado que Ucrania cuenta con mucha infraestructura conectada a Internet, donde ponemos algunos ejemplos como sistemas de banco, BlackEnergy donde la red eléctrica de Ucrania se vio interrumpida por un ataque cibernético llamado BlackEnergy, NotPetya que es un software destructivo que se ocultó en una actualización de un popular software de contabilidad utilizado en Ucrania encriptando grandes cantidades de datos donde estos son algunos ejemplos de como todo esta conectado y se deben de tomar medidas de ciberseguridad.

Se deben de considerar medidas de control que puedan ser de gran ayuda para defender y si es posible dar un contraataque empleando diversas herramientas

como metodológicas OSINT (Open Source Intelligence) y SOCMINT (Social Media Intelligence), fuentes abiertas con fines militares pero no queda solamente aprovechada para fines buenos, si no también para cibercriminales que aprovechan para obtener información relevante, entrando un tema importante como lo es la ingeniería social que es factor para engañar y atentar con una persona de una organización determinada. Es importante conocer el modelo de inteligencia de amenazas, para identificar y predecir intenciones de los ciberataques.

1.1 Modelo de inteligencia de amenazas y modelado de intrusiones

La inteligencia de ciberamenazas es un proceso de recopilación y análisis de datos en relación de ciberataques para analizar, rastrear, localizar, predecir futuras intenciones de adversarios, donde se tienen en consideración diversos marcos que pueden ser de gran ayuda para conocer más sobre la ciberseguridad ofensiva y defensiva, siendo matrices de procedimientos y recomendaciones para generar táticas y técnicas que puedan ser usados para mitigar riesgos y vulnerabilidades que en consecuencia se vuelven amenazas.

Stephane Nappo quién es Director Global de Seguridad de la Información (CISO) menciona "La prevención exhaustiva es una ilusión. No podemos asegurar la mala configuración, la sombra de TI, terceras artes, error humano, exempleados. Enfóquese en lo que importa más y esté listo para reaccionar"(Napp, S). En todo momento una organización debe de ser capaz de responder modelando con antecendetes las situaciones que pueden surgir y conociendo el modelo de amenazas para estar informados sobre donde podría entrar el adversario a interrumpir nuestros sistemas informáticos.

Los marcos que son considerados son MITRE ATTCK y MITRE D3FEND, claro que cada uno con sus funciones que desempeñan.

- MITRE ATTCK: Puede ser útil para la inteligencia contra amenazas informáticas, ya que permite describir comportamientos adversarios de manera estándar.(MITREATTCK 2022)
- MITRE D3FEND: Ayudar a estandarizar el vocabulario utilizado para de-

scribir la funcionalidad de la tecnología de ciberseguridad en el área defensiva.(CRONUP 2021)

Se tiene en cuenta los modelos de intrusiones de ciberataque como (OscarSandovalCarlos 2022):

- Cyber Kill Chain: Donde un agresor debe desarrollar un método para entrar en un entorno de confianza con el fin de establecer una presencia y tomar acciones hacia algún objetivo que le gustaría lograr en la red.
  - Reconocimiento
  - Armamento
  - Entrega
  - Explotación
  - Instalación
  - Mando y control
  - Acción sobre objetivos
- Modelo diamante: El Modelo Diamante de Análisis de Intrusiones, describe cómo un adversario utiliza la capacidad de una infraestructura contra una víctima. Este modelo consta de cuatro elementos básicos: adversario, infraestructura, capacidad y víctima que proporcionan cuatro cuadrantes como un diamante.

En estos marcos se tienen en consideración APTs de tal forma ver el informa y visualizar como estos pueden atacar desde diferentes puntos, donde se tiene en presencia las siguientes organizaciones (OscarSandovalCarlos 2022):

- APT28 es un grupo de amenazas que se ha atribuido al Centro Principal de Servicios Especiales de la Dirección Principal de Inteligencia del Estado Mayor de Rusia (GRU)
- APT29 es un grupo de amenazas que se ha atribuido al Servicio de Inteligencia Exterior (SVR) de Rusia. Han operado desde al menos 2008.
- Turla es un grupo de amenazas con sede en Rusia que ha infectado a víctimas en más de 45 países, abarcando una amplia gama de industrias.

MITRE ofrece un gran desglose como táticas, técnicas, fuentes de datos, mitigaciones, grupos, software, recursos que pueden ser de gran utilidad para mejorar la infraestructura de una organización, en el caso de la guerra entre Rusia y Ucrania estos informes pueden ser de gran utilidad para prevenir que estas APTs que se mencionaron anteriormente puedan penetrar otras organizaciones. Además ofrece un gran visualización de que hace cada APT y las herramientas que utiliza, esto puede ser un gran ventaja concocer estas herramientas y tomar las medidas adecuadas.

2 Conclusión

En conclusión profundizar y explorar estos conceptos nos pueden ayudar a tener una mejor visualización de un panorama en general sobre el tema de ciberseguridad, nosotros como personas de esta área debemos de tener en cuenta mejores prácticas, así como también entender como nosotros podemos contrarrestar y hacer el mínimo error posibles en contra de amenazas que potencialmente pueden tirar una organización. El caso de Rusia-Ucrania nos da un ejemplo de un cambio de paradigma que ahora las guerras entre naciones se trata en temas de ataques cibernéticos, donde Rusia por temas de política ataca a Ucrania, atentando contra la OTAN y los aliados de Ucrania, haciendo más visible el temor de la ciberseguridad que pueden lograr acciones que comprometan el robo de información y propagación de malware.

Estar informado y conocer los macros de modelación puede ser una gran ventaja, claro que para hacer todo esto se necesitó aprender de antecedentes de ataques, donde hoy en día se va evolucionando con nuevo software y poder computacional y debemos de estar en constante cambio para prevenir que estos ataques se vuelvan potencialmente altos, recopilando todo tipo de incidentes, aprendiendo de los errores porque no somos perfectos y tener mejores prácticas de ciberseguridad.

References

[1] CRONUP. *D3FEND by MITRE ATTCK*. 2021. URL: https://acortar.link/64Vmrb.

[2] ELPAIS. *¿Cuál es el origen del conflicto entre Rusia y Ucrania? Fechas clave de la guerra*. 2022. URL: https://acortar.link/b0WIwq.

[3] MITREATTCK. *MITRE ATTCK*. 2022. URL: https://attack.mitre.org/.

[4] OscarSandovalCarlos. "Uso de la inteligencia de ciberamenazas como apoyo a la comprensión del adversario aplicada al conflicto Rusia - Ucrania". In: *None* 1.1 (2022), pp. 1–27. DOI: https://arxiv.org/ftp/arxiv/papers/2205/2205.03469.pdf.