South American Publishing

SAP Netnography. 2023; 1:22
doi: 10.62486/net202322

ORIGINAL

Cybercrime: Ransomware, and government actions for analyzing criminal behavior in the province of Córdoba

Cibercrimen: Ransomware, y las acciones gubernamentales para su análisis de la conducta criminal en la provincia de Córdoba

Agustín Ramiro Manrique Aguad[1], María Belén Gauna[1]

[1]Universidad Siglo 21, Licenciatura en Criminología y Seguridad. Argentina.

Cite as
Manrique Aguad AR, Gauna MB. Cybercrime: Ransomware, and government actions for analyzing criminal behavior in the province of Córdoba. SAP Netnography. 2023; 1:16. https://doi.org/10.62486/net202322

Publication History
Submitted: 14-03-2023
Revised: 03-07-2023
Accepted: 26-10-2023
Published: 27-10-2023

ABSTRACT

In this paper, government actions aimed at addressing the analysis of criminal behavior by cybercriminals in ransomware attacks through the use of ICT (information and communication technology) in private and public organizations in the province of Córdoba were described. The method used had a qualitative approach of a non- experimental type, with a descriptive and explanatory scope. In addition, as instruments, documents and a semi-structured interview were used. For its part, it was inquired about the application of the operational analysis of cases to this criminal typology by the Judiciary of Córdoba. In addition, the most resonant cases that occurred in Córdoba in the last ten years were established, and the difference between cybercrime and cybercrime of ransomware behavior was delimited. Among the results, there is a coincidence of factors and behaviors between cases and a great contextual influence of the situation in terms of computer security in organizations, in their ability to react. In turn, no information was found that shows that the operational analysis of cases has been used for these crimes in the province of Córdoba. Therefore, doors were opened to new lines of investigation and the creation of new methodologies of governmental approach. Emerging as the main recommendation, the creation of a specific case analysis method for the study of the behavior of cybercriminals and their victims, in order to identify the causal roots of the phenomenon and thus develop more effective government policies for its prevention and control.

Keywords: Cybercrime; Ransomware; Encryption; Cyberattack; Hacker; Malware; Software; ICT; Cyberspace; Cybercriminal.

RESUMEN

En este trabajo, se describieron las acciones gubernamentales tendientes a abordar el análisis de la conducta criminal por parte los ciberdelincuentes en los ataques ransomware mediante el uso de TIC (tecnología de información y comunicación) en organizaciones privadas y públicas, en la provincia de Córdoba. El método utilizado tuvo un enfoque cualitativo de tipo no experimental, con un alcance descriptivo y explicativo. Además, como instrumentos, se utilizaron documentos y una entrevista semiestructurada. Por su parte, se indagó sobre la aplicación del análisis operativo de casos a esta tipología delictual por parte del Poder Judicial de Córdoba. Además, se establecieron los casos más resonantes ocurridos en Córdoba en los últimos diez años, y se delimitó la diferencia entre ciberdelito y cibercrimen de la conducta ransomware. Entre los resultados, se halla una coincidencia de factores y conductas entre casos y una gran influencia contextual de la situación en cuanto a seguridad informática en los organismos, en la capacidad de reacción de estos. A su vez, no se encontró información que evidencie que el análisis operativo de casos se haya usado para estos delitos en la provincia de Córdoba. Por lo que se abrieron puertas a nuevas líneas de investigación y la creación de nuevas metodologías de abordaje gubernamental. Surgiendo como principal recomendación, la creación de un método de análisis de casos específico para el estudio de la conducta de cibercriminales y sus víctimas, con el fin de identificar las raíces causales del fenómeno y desarrollar así, políticas gubernamentales más eficaces para su prevención y control.

Palabras clave: Cibercrimen; Ransomware; Cifrado; Ciberataque; Hacker; Malware; Software; TIC; Ciberespacio; Cibercriminal.

© 2023; The Authors. This Open access article is distributed under the Creative Commons Attribution 4.0 license (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

INTRODUCCIÓN

El análisis del comportamiento criminal se construyó con base en distintos aportes realizados por la criminología y las ciencias de la conducta aplicados al campo de la práctica criminalística.

El uso de la psicología para comprender y prevenir la criminalidad debe considerarse desde los orígenes de la ciencia psicológica. Sin embargo, el empleo y la construcción de metodologías con fundamento empírico son relativamente recientes.

La construcción de perfiles psicológicos se basó principalmente en la consideración, empleo y desarrollo de clasificaciones propias de la psiquiatría, lo que terminó encasillando a delincuentes en posibles diagnósticos de enfermedades mentales. Con el paso del tiempo, se desarrollaron distintas teorías que comenzaron a considerar otro tipo de factores más allá de los psicológicos y que son fundamentales para una aproximación más precisa y certera del perfil de un criminal.

Según expone Chilo, los cimientos de esta disciplina se corresponden con prácticas realizadas en los Estados Unidos, en las que se invierte el proceso psicodiagnóstico y se estudia el resultado de los comportamientos y acciones de una persona desconocida para deducir el tipo de sujeto que podría haber llevado a cabo el hecho delictivo objeto de la investigación. De esta forma, se recopilan y se evalúan datos; se reconstruye la situación; se formulan hipótesis; se desarrolla y pone a prueba el perfil; y, finalmente, se informan los resultados.

Como antecedentes se pueden citar:

- En 1943, el Servicio Secreto de Estados Unidos le pide al psiquiatra Walter Langer la construcción de un perfil psicológico de Adolf Hitler. Langer debe pronosticar las posibles decisiones que tomaría Hitler en caso de ser derrotado. De ocho alternativas planteadas, Langer concluyo que Hitler optaría por el suicidio.
- En 1957, Jambes Brussel construye el primer perfil psicológico criminal considerado como tal de manera estricta. Por medio de la comparación de conductas delictivas con enfermedades mentales y teniendo en cuenta escenas de los crímenes, logra, a través de un método deductivo, delimitar un perfil cuyas afirmaciones correspondían con las del Mad Bomber, sujeto que plantó numerosas bombas en Nueva York en los años 50.
- Desde 1970, los aportes del FBI al desarrollo de esta técnica fueron numerosos. Crean la Unidad de Ciencias del Comportamiento. Robert Ressler, agente del FBI, crea el Proyecto de Investigación de la Personalidad Criminal, a partir del cual se comienzan a documentar los patrones de conducta y comportamiento de asesinos. Uno de sus aportes más importantes es el de la consideración de la serialidad criminal.

A medida que esta disciplina comienza a expandirse, son múltiples las metodologías, desarrollos y definiciones conceptuales que comienzan a surgir. Ressler considera los aportes realizados desde los Estados Unidos y señala que el perfil criminal ha sido descripto como una suma de pistas, como un intento de recopilar información específica y como un esbozo biográfico de patrones de conducta.

Holmes y Holmes consideran tres objetivos principales que se desprenden del análisis y estudio psicológico del delincuente:

1. Aproximación a una valoración desde la criminología social y psicológica de la personalidad del delincuente.
2. Consideración de las inferencias posibles en relación a las pertenencias del delincuente halladas en las distintas escenas del crimen.
3. Sentar las bases de posibles focos de indagación e hipótesis claves en la investigación penal.

En este contexto, entonces, la perfilación criminal busca generar una aproximación a las características del presunto agresor, lo que permite disminuir el espectro de la investigación y centrarse en aspectos más certeros y definidos. Esto resulta de gran importancia, considerando que al tratarse de delitos violentos y, sobre todo, de asesinatos seriales la movilización social es elevada, ya que se debe tener en cuenta, a su vez, que las probabilidades de que se cometa un nuevo crimen exigen que las intervenciones sean rápidas.

Esta técnica es factible de ser aplicada sobre todo en casos en los que existe serialidad, ya que la repetición posibilita determinar la presencia o no de una pauta o patrón de conducta, especialmente en los delitos de violación, homicidio, asesinato y piromanía.

En Europa, la escuela alemana fue la que mayor influencia tuvo en la determinación del análisis operativo de casos. Este fue usado como método inductivo en el estudio de la información proporcionada por las distintas ramas de ciencias físicas y naturales acerca de la criminalística y a través de la objetividad de las pruebas obtenidas mediante el análisis del comportamiento de un delincuente a lo largo de todo el hecho delictivo, considerando sus distintas fases, y mediante la comparación con otros hechos criminales.

Según Fortete, el análisis criminal implica analizar metódicamente la información criminal que llega a las diferentes áreas operativas y, gracias a la denuncia ciudadana, es posible determinar las condiciones sociopolíticas, demográficas y delictivas que caracterizan una región o utilizarlas para la resolución de casos particulares.

Por otra parte, es fundamental recalcar que la construcción de un perfil no debe limitarse solo a consideraciones psicológicas. Tampoco debe tomarse la construcción de ese perfil como algo rígido e inmodificable, dado que los distintos análisis han demostrado que de una situación pueden surgir distintos perfiles o que un mismo perfil puede modificarse debido al perfeccionamiento del autor en su carrera delictiva.

La metodología para la construcción de un perfil criminal consiste en analizar y evaluar distintos aspectos:

- La escena del crimen es el lugar y espacio que el delincuente ha escogido para cometer un crimen. Las escenas pueden ser distintas si el delincuente emplea y se desenvuelve en varios lugares, es decir, desde que captura a su víctima hasta que la abandona. En cualquier caso, la escena principal es donde tiene lugar la muerte o la agresión de mayor importancia. En este

sentido, es de fundamental importancia el cuidado y la preservación de dicha escena, ya que cada indicio y pista puede ser clave en la determinación de un tipo de personalidad, considerando a su vez la existencia o no de posibles manipulaciones de dicha escena.

- El modus operandi hace referencia al método o forma de operar.

Considera, principalmente, la manera o método que el agresor ha empleado para cometer el delito. De su análisis, se recoge información acerca de cómo actúa ese criminal, lo que hace posible delimitar y aproximarse a las características psicológicas deducibles de su forma de actuar.

- El estudio detallado de la información que brinda el modo de operar de los delincuentes permite definir indicios, tales como el momento del día elegido; la presencia o ausencia de perfeccionismo; manera de aproximarse a la víctima; si hay planificación y organización o no; el tiempo empleado; el nivel intelectual; las armas; entre otros.
- La firma, para Robert Keppel, constituye una parte de la escena del crimen que involucra distintas expresiones de las fantasías del criminal, es decir, es el conjunto de acciones que no son necesarias para cometer el delito. La firma tiende a ser uno de los patrones principales que posibilitan el establecimiento de la serialidad en distintos hechos, siendo posible la adjudicación de estos a un único autor.
- El análisis de delitos seriales se complementa con el análisis geográfico. Existen diversas teorías que explican el comportamiento espacial del autor de un hecho con finalidad de establecer la existencia o no de una relación entre estos lugares y las rutinas del victimario. Este perfil describe la conducta espacial y los terrenos donde se desplaza el delincuente, las escenas del crimen, los puntos de anclaje de los hechos, zonas de riesgo, base de operaciones, etc.

Se está viviendo en una época donde las TIC(tecnologías de la información y la comunicación), dispositivos electrónicos, redes sociales, medios de comunicación y otros servicios y productos los cuales son usados para satisfacer lo que llamamos “necesidades del siglo 21”, encontramos que además de ser utilizadas por el civil promedio y empresas, también lo son por Estados, gobiernos, municipios y organismos gubernamentales para distintos fines que pueden ser desde la seguridad, manejo de bancos centrales (capital económico), proveer de servicios básicos para la ciudadanía (energía, agua, gas, entre otros) sistemas educacionales, sistemas penitenciarios y demás donde estas tecnologías están presente día a día para facilitar procesos o actividades.

Nadie escapa a la realidad de que las TIC engloba a aquellos elementos y sistemas usados globalmente en la actualidad para el tratamiento, intercambio y comunicación de la información en la sociedad actual y muchos desconocen el alcance que estas actividades ilegales que se conocen como ciberdelito impactan en nuestra sociedad.

Toda tecnología que fue desarrollada a partir de los sesenta y setenta, con la llegada del internet sufrió un expansionismo y universalización de redes en donde todas las personas con acceso a un dispositivo electrónico e internet son parte directa e indirectamente de LA red de comunicación más grande y extendida por todo el mundo, también llamada como “la red de redes “Internet. Todo aquel que hoy en día cuente con un dispositivo inteligente como por ejemplo computadoras, celulares, televisores, y una gran variedad de electrodomésticos como las impresoras en oficinas está conectado a internet.

Como consecuencia de tal hito no solo mejoro la calidad de vida de las personas desde el entretenimiento hasta el trabajo y pasando por la medicina, sino que también dotó a aquellas personas con “conductas desviadas” de herramientas y abrió un abanico de posibilidades a quienes, con conocimiento y experticia en el uso de la informática, tecnología e ingeniería social supieron usarlo para fines personales y conseguir aquellos bienes u objetivos de valor bajo una nueva modalidad del delito, modalidad que se extendió vulnerando varios derechos como la integridad sexual, la propiedad y la libertad, delitos como la extorsión, fraude, engaños y ataques a bancos multinacionales u organizaciones de los gobiernos.

En muchos casos estas tecnologías son indispensables para la realización del trabajo, facilitándolo, siendo parte fundamental o critica para el mismo donde se usan computadoras, celulares, archivos que se guardan en la nube, programas/software, cuentas bancarias, inteligencia artificial entre otros. Cualquier fallo o intervención de cualquier identidad podría paralizar las actividades de los organismos que los utilizan produciendo problemas en función del tiempo en el que los servicios se ven paralizados, información es robada o expuesta o dañada, el pedido de rescate por dicha información página o cuenta es una práctica frecuente que llevan a cabo los criminales. Los efectos de estos fallos o intervenciones, producidos en el ámbito de las TIC y prioritariamente haciendo uso de estas para su comisión, se ven reflejados en la ciudadanía y en la calidad de vida de esta dependiendo el sector y grupo afectado.

El ciberdelito o delito informático como se lo conoce es el nombre que se le dio a esta “ya no tan nueva” modalidad de crimen, conforme pasaron las generaciones y así como con la tecnología fue evolucionando en cuanto a su concepción y significado siendo según Gustavo Sain[1] en que se considera ciberdelitos o delitos informáticos a toda conducta ilegal en donde un dispositivo informático interviene ya sea como medio para cometer el delito como fin del mismo, el primer caso contemplando los casos de extorción o chantaje o intimidación vía correo electrónico siendo el dispositivo informático el objeto o blanco y en el segundo caso es el dispositivo informático el blanco del crimen donde la persona envía un virus al dispositivo de otra persona dañándola o alternando su funcionamiento.

Lo mismo hicieron también las técnicas para su comisión o modus operandi (cibercriminalidad) y su diversificación en materia de delitos encontrando algunos ejemplos como los delitos de cuello blanco, phishing, malware, child grooming, difusión de pornografía infantil, fraude, robos de identidad, entre otros.

Si bien la variedad de delitos que se pueden cometer con el uso de las TIC es extensa, en este documento se hará foco en la comisión de ataques a organizaciones estatales y privadas con el uso de Ransomware o softwares maliciosos.

El ransomware se forma a partir de la unión de palabras en inglés de ransom (de rescate) y ware (de software), el ataque

ransomware puede tener muchas formas incluyendo a cualquier tipo de código malicioso o malware (en inglés) ya sean virus, los troyanos y gusanos informáticos. El método de propagación que se utiliza son el spam, vulnerabilidades o malas configuraciones de software, actualizaciones de software falsas, canales de descarga de software no confiables y herramientas de activación de programas no oficiales.[2,3,4] ¿El objetivo?

Se lleva a cabo mediante la infección de virus destructivos que se debe considerar, a su vez, como una tipología del más general comportamiento de distribución de malware o software malicioso destinado a dañar, controlar o modificar un sistema informático.

En los casos en el que se logra encriptar, controlar y negar el acceso de la información a la víctima el victimario solicitara un rescate por dicha información teniendo en algunos casos especificaciones sobre el cómo y con qué moneda hacer el pago por ejemplo el rescate en bitcoins, o cualquier otra moneda con tecnología blockchain, ya que esta moneda permite el anonimato y es el activo que muchos empresarios suelen tener.

El ransomware es probablemente una de las amenazas cibernéticas más graves con la que organización privadas y gubernamentales se pueden encontrar no solo por el daño que estas provocan sino porque los ciberdelincuentes constantemente perfeccionan el código malicioso haciéndolo más difícil de detener o detectar siendo que además siempre están en constante innovación para asegurarse el pago del rescate aumentando la presión en la victima amenazándola de todo lo que podrían hacer con su información.

En los últimos años se ha visto una transición en los ataques de ransomware porque pasaron de ser ataques masivos (que apuntaban a un gran número de personas y solicitaban sumas modestas de rescates) a ser ataques dirigidos a sectores específicos, exigiendo montos mucho mayores a grupos de víctimas más pequeños. Estas víctimas elegidas tienen bolsillos más grandes y miembros que no pueden permitirse perder el acceso o el control de sus datos.[5]

Para poder dimensionar la profundidad con la que actúan tanto técnica como psicológicamente los ataques ransomware sobre las victimas hay que saber que existen distintos tipos como los de bloqueo, denegación de servicio (como los DDoS) y los de cifrado, es fácil guiarse por los nombres acerca de que pueden hacer cada uno de estos tipos, pero no es muy sencillo predecir los efectos que dejan en sus víctimas.

Mas allá de las dificultades técnicas que los ciberdelincuentes dejan a su paso después del ataque son los "virus residuales" en los equipos o la mera presencia de estos en el ciberespacio provocando conmoción como es el caso del print bombing, que consiste en la infección y utilización de impresoras disponibles en la red objetivo para imprimir mensajes exigiendo el rescate.

La sanción de la ley 26.388[3] conocida como "la ley de los delitos informáticos" sancionada en el 2008 introdujo nuevos tipos penales en relación al uso de la tecnología. Entre todos los nuevos tipos penales y artículos añadidos por esta ley se encuentra el articulo 10 incorporado por dicha ley el cual pena alteración, destrucción o inutilización de los datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. Este articulo y las características de las conductas que describe son las que encuentran en los delitos informáticos de tipo ransomware.

Un ejemplo de cómo el delincuente se adapta a los cambios para cometer el delito lo podemos ver en este "nuevo" tipo de delito, el delito informático, algunos optan por este camino mientras otros eligen la delincuencia "convencional" como el robo con o sin violencia. Esto visto desde una perspectiva general y teniendo en cuenta el paso de generación y la evolución de las tecnologías. Pero, y si, ¿en un caso particular el delincuente no tiene la posibilidad de delinquir convencionalmente por que se encuentra encerrado en su casa como el resto de los ciudadanos?

Esta situación se dio en la pandemia de COVID-19 en donde toda la población argentina se vio obligada a permanecer en cuarentena en su casa debido a la amenaza biológica, en esta situación ninguna persona con actividad delictiva activa podía salir para ejercer sus actividades sin ser detenida por las autoridades.

Es bajo estas condiciones que el delincuente debido a factores externos aprende y se adapta usando las TIC como nueva herramienta para delinquir aprovechando que buena parte de la población usaba internet, de acuerdo con el INDEC para el último trimestre del año 2020, el 86 % de los habitantes de nuestro país utilizaba internet, lo que representa un aumento de 5,6 puntos porcentuales con respecto al año anterior. Según el Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia,[6] en el transcurso del año 2019 se recibieron un total de 2 369, lo que equivale a aproximadamente 6,5 reportes diarios sin distinción de días hábiles y no hábiles, mientras que, para el año 2020, el número ascendió a 11 396, un 381 % más, lo que equivale a alrededor de 31 reportes por día. Se aclara que estos datos fueron tomados teniendo de muestra a la población de CABA.

Entre las modalidades que se dieron en ese periodo con más frecuencia se encuentran fraude en línea, difusión no autorizada de imágenes, acoso y ransomware.

El ataque Ransomware a Telecom argentina el 18 de julio de 2020.[7] Este ataque se produjo globalmente, el ransomware de 0-day basado en el malware Sodinokibi. Se le dice 0-day si un hacker logra vulnerar la seguridad antes de que los desarrolladores de software puedan encontrar una solución a esa vulnerabilidad de seguridad.

Afortunadamente en este caso se detectó el problema a tiempo lo cual afecto solo el 5 % de los equipos informáticos de la empresa, no se vieron afectados ni los servicios, ni las bases de datos de la compañía. Tampoco fue afectado ningún cliente corporativo.

Un ejemplo de que pasa cundo no se paga un rescate de un ataque ransomware y al mismo tiempo la organización afectada es una organización gubernamental, él 27 de agosto de 2020 la Dirección Nacional de Migraciones informo que fue víctima de un ataque ransomware, perdiendo datos y este resultando encriptados, la banda llamada "Netwalkers" exigió el pago del rescate por cuatro millones de dólares.

El día del ataque diferentes puntos fronterizos notificaron problemas de sistema, en pos de preservar los datos y evaluar la situación se solicitó desactivar el SICAM (Sistema Integral de Captura Migratoria), se cerraron los cinco pasos fronterizos terrestres

sumados los aeropuertos de Ezeiza y Buquebus y durante cuatro horas no hubo movimientos migratorios consecuencia de la desactivación del SICAM.

El ataque tuvo repercusiones por que no era normal que un ataque de esas características paralizara las actividades de todo un país y desemboco en la dimisión del director de Sistemas de Migraciones que en ese momento llevaba dos décadas y el inicio de sumarios judiciales. En medio de todos los ciberdelincuentes pusieron fecha límite para pagar el rescate de los datos secuestrados, el estado se negó y esto resulto en la publicación de todos los datos

¿Qué contenían las carpetas? Según Clarin "Información de los años 2015 y 2016 vinculada a inteligencia criminal, vinculadas a temas de seguridad, cédulas o alertas de Interpol".

El ataque al cuerpo legislativo del senado a principio del año 2022, siendo también un caso de ransomware que bloqueo el acceso a los senadores, restringiendo correos electrónicos personales y paralizando las funciones del mismo.

Otro caso sucedió aproximadamente a mitad del año 2022, en Córdoba, un ataque ransomware al poder judicial que provocó la caída de los servicios de el mismo, paralizando las actividades de este organismo debido a la imposibilidad de los usuarios para acceder a expedientes electrónicos, correos oficiales, uso temporal del expediente físico y con riesgo de que se filtren datos sensibles. (8)

En este caso es el sucedido el 9 de octubre del 2021, donde el estado argentino fue víctima de un hackeo en la base de datos privados de las personas (Renaper), base de datos que contiene todos los registros privados de los habitantes del país. Se filtraron números de documento, domicilios, números de tramites (que sirven para los créditos online, fechas de nacimientos, fechas de nacimiento y números de celular en algunos casos.

El estudio de estos delitos supone vincular múltiples factores, desde la practica individual o colectiva de estos delitos y sus modos, el contexto social-político- económico de la/las victimas (siendo político en los casos en donde el país entero se ve afectado o un gran número de personas y personalidades).

A los fines del presente manuscrito, resulta importante contextualizar la problemática de los ciberataques en los organismos privados y gubernamentales, ubicándonos en la Provincia de Córdoba, sus casos, abordaje, intervenciones y estudios sobre el tema. Por ello se buscará determinar las acciones gubernamentales tendientes al abordaje del análisis de la conducta.

Por lo tanto, el objetivo general del presente trabajo será:

- Describir y explicitar las acciones gubernamentales en el análisis criminal de cibercrímenes ransomware llevado adelante por el Tribunal Superior de Justicia de la Provincia de Córdoba.

Por otro lado, los objetivos específicos son:

- Indagar sobre la posible implementación del análisis operativo de casos en ciberdelitos ransomware en caso de que se hayan implementado.
- Explicitar casos emblemáticos de ciberdelitos ransomware en la provincia de Córdoba.
- Desarrollar y explicitar modalidades de ciberdelitos y cibercrímenes y su diferencia
- identificar y especificar modus operandi, firmas, patrones de los delitos informáticos para realizar una aproximación a una perfilación criminal.
- Profundizar sobre el accionar de la Justicia local sobre los ciberdelitos de tipo ransomware.

MÉTODO

Diseño

Para esta investigación se realizó una investigación con un alcance descriptivo y explicativo. Esto es así porque se busca describir cómo fueron y se presentaron las conductas, situaciones y eventos ocasionados por ataques ransomware en la Argentina en general y explicar en la provincia de Córdoba en específico para describir variables, fenómenos, contextos y casos para la comprensión del fenómeno.

El enfoque elegido es cualitativo, es decir que no habrá mediciones ni análisis numéricos o en análisis estadísticos, únicamente fuentes documentales y recolección de datos. No es el objetivo refutar o comprobar hipótesis

Por último, será de tipo no experimental, ya que no hubo manipulación deliberada de variables, observando los hechos tal y como se presentan para su análisis

Unidad de análisis

La unidad de análisis es la de fuentes documentales. Siendo de diferentes tipos como artículos e informes periodísticos, papers académicos, testimonios en las causas, entre otros. La elección de los casos encuentra justificación en características delictuales y geográficas acorde al tema de investigación propuesto

Instrumentos

Para alcanzar los objetivos señalados los instrumentos utilizados fueron de tipo documental, por lo que se consultaron fuentes escritas, entrevistas ya hechas y publicadas para corroborar los datos de los fenómenos.

Análisis de Datos

En este apartado se dará definición a palabras y conceptos fundamentales para entender de lo que se habla. Con relación al plan de trabajo, se distinguen tres etapas: La primera etapa consistió en un análisis bibliográfico para la elaboración y construcción

del marco teórico. En la segunda, se planteó un relevamiento de datos de tipo documental. Se realizó una recolección, selección y análisis de fuentes documentales según los objetivos planteados, tales como, papers académicos, informes de fuentes oficiales (gubernamentales y no gubernamentales), fuentes jurisprudenciales, entrevistas, leyes, libros, entre otras.

La tercera etapa estuvo centrada en el análisis de los datos obtenidos, el cual se realizó con un enfoque cualitativo, su sistematización de acuerdo con los objetivos planteados, el análisis y descripción de la información relevada desde el marco de referencia elaborado.

El análisis de los datos se realizó en torno a la creación de categorías, las mismas son:

- Cibercrimen: es toda conducta antijuridica cuya modalidad de acción es realizada a través de dispositivos electrónicos y redes sociales o ciberespacio, siendo el componente fundamental la tecnología que forma parte de este "nuevo" proceso delictivo.
- Cibercriminalidad: Modus operandi en la comisión de un delito usando principalmente las TIC.
- Ramsomware: Es un tipo de malware o software malintencionado desarrollado para bloquear el dispositivo y encriptar sus datos para luego pedir una recompensa para la posterior reintegración de los datos y la habilitación del equipo.[1]
- Análisis operativo de casos: es el análisis de la estructura, naturaleza y características de casos para elaborar un perfil de los autores, evaluar riesgos, confrontar casos, investigar sus causas y analizar la influencia del contexto social y cultural.
- Ingeniería social: Son las diferentes técnicas de manipulación que utilizan los ciberdelincuentes, haciéndose pasar r otra persona con el objetivo de apropiarse de datos de valor como contraseñas o cuentas
- TIC: Las tecnologías de la información y comunicación, como su nombre lo indica, son aquellas tecnologías que se necesitan y usan para la gestión y transformación de la información. Siendo en particular los ordenadores y programas que permiten ordenar, almacenar, modificar y proteger la información.
- Marco legal: el marco legal es el conjunto de leyes, normas y reglamentos en el que se apoyara este escrito, siendo la ley 26.388 más específicamente en el art 10 de esta ley.[3]
- Hacker: Persona con conocimientos informáticos dedicada u obsesionada a encontrar fallos en la seguridad informática de los organismos.
- Ciberespacio: el ciber espacio o mundo virtual NO es un espacio físico donde cualquier persona puede comunicarse y compartir a través de los medios que permiten su acceso, estos son los denominados TIC. Álvaro Écija[9] afirma "es ya el quinto entorno estratégico, tras tierra, mar, aire y espacio".

RESULTADOS

Indagar sobre la posible implementación del análisis operativo de casos en ciberdelitos ransomware en caso de que se hayan implementado:

No se encontraron fuentes que afirmen que se haya implementado el método de análisis operativo de casos en la provincia de Córdoba para analizar ciberataques con uso de la metodología de ransomware. Según los datos recabados se concluyó que el método permite su aplicación a la tipología delictual estudiada, ya que los autores son conocidos por buscar constantemente la vulnerabilidad en los sistemas de seguridad informática o el error humano mediante el uso de ingeniería social en las organizaciones, si bien pueden ser innovadores a la hora de cambiar la estrategia o el código malicioso una vez fueron rechazados estos usaran la misma técnica hasta que no le resulte más útil y al no ser diferentes en muchos de los casos se cuenta con la característica de serialidad, como afirmo en una entrevista en particular hecha por Todo Noticia[10] a un experto en ciberseguridad, en donde dice "son de tipo común, silvestres, hay criminales que escanean miles de servidores por día y cuando encuentran una vulnerabilidad obviamente la atacan".

Explicitar casos emblemáticos de ciberdelitos ransomware en la provincia de Córdoba

Los casos de ciberataque a organismos ya sean públicos o privados tienen la "mala costumbre" de no ser muy públicos. Esto es debido a que en parte no existen regulaciones sobre denuncias de ciberataque como en otros países o por razones de impacto y otras cuestiones no son públicas, por ejemplo, una empresa llamada Globant hizo público un ataque que sufrió y sus acciones cayeron un 13 % en Wall Street. Es por eso que las compañías tratan de que ese tipo de información no se haga pública, lo mismo podría decirse de los gobiernos que lo sufren al querer mantener todo bajo control y la población afectada no entre en pánico.

Aun así, existe un caso emblemático mencionado anteriormente ocurrido en la provincia de Córdoba, aunque se presume hay más y ocurren diario, que sucedió a mitad del año 2022. Este ataque paralizo las actividades judiciales por un tiempo determinado, varios mails fueron interceptados y se corrió el peligro de que el backup o copia de respaldo se perdiese, obligo a que se sustituyese el expediente electrónico por el físico, alcanzo a unos 8 000 usuarios y los cerca de 25 mil abogados matriculados en la provincia.

En una entrevista hecha por un canal local de Córdoba a un experto en ciberseguridad, dijo: "Normalmente este tipo de acciones son hechas por grupos que desean generar algún pánico en la sociedad".

Desarrollar y explicitar modalidades de ciberdelitos y cibercrímenes y su diferencia

Los ciberdelitos se encuentran las actividades de los ciberdelincuentes, actividades genéricas y poco graves, haciendo un daño mínimo a la población civil afectando a un solo individuo o a un grupo de la comunidad. Algunas de estas conductas son Fraudes informático, falsificación, scammer, extorsión, acoso, grooming, ilícitos contra la propiedad intelectual, hacking, corrupción de menores, crímenes contra la moralidad y el pudor, distribución de contenidos ilegales, trata de personas. Todas estas modalidades con excepción de algunas no requieren de una experiencia previa en el manejo de las TIC y suelen usar medios de comunicación habituales como WhatsApp, Facebook o correos electrónicos para su comisión otras técnicas usan la ingeniería social y el engaño para conseguir lo que buscan. Siempre siendo el objetivo el ciudadano promedio que cae ya sea por ignorancia u oportunismo.[11,12]

El cibercrimen es un escalón en los delitos informáticos donde estos son más graves, provenientes de ciber terroristas, su modalidad de actuación es a través de las tecnologías de la comunicación para intimidar, acosar o coaccionar a grupo sociales para causar daños, todo esto con finalidades político-religiosas y o persiguiendo fines adquisitivos.[13]

Ambos fenómenos se presentan con características similares con sus respectivas técnicas de vulneración en la seguridad de los sistemas informáticos, pero con distintos fines a perseguir.

Identificar y especificar modus operandi, firmas, patrones de los delitos informáticos ransomware

Cundo hablamos de delitos informáticos y sus modos de operar nos encontramos con un amplio número de firmas y patrones que se dejan o demuestran al proceder con el ciberdelito, todo dentro de las mencionadas TIC. Pero en los casos de ataques ransomware estos modos, firmas y patrones son visibles en las distintas modalidades en las que los delincuentes se hicieron para conseguir engañar a las personas que fueron víctimas. Correos, mensajes, gusanos informáticos entre otros métodos son utilizados en los ciberataques para la vulneración de la seguridad y posterior acceso y encriptación de los datos para luego solicitar su rescate buscando a veces la seguridad de una moneda o activo que sea difícil de rastrear como las criptomonedas.[14,15]

Por lo menos el patrón parece claro, es secuencial y metódico vulneración seguido de robo y encriptación para luego proceder a la demanda y si no se cumple la demanda el castigo.

La firma parece ser algo fácil de obtener ya que muchas bandas de cibercriminales optan por plasmar de alguna manera el nombre de dicho grupo, aunque, el mismo grupo podría actuar bajo muchos nombres, pero un solo malware o viceversa.

Profundizar sobre el accionar de la Justicia local sobre los ciberdelitos

La justicia debe optar por reforzar la actuación de la fiscalía especializada en delitos informáticos para la capacitación de personal especializado en la prevención o detección de ataques ransomware, reforzar su propia infraestructura ya que han sido objetivo de ataque y los sistemas de seguridad debido a que han sido eludidos en ciertas ocasiones, y capacitar al personal existente para actuar en el pos-delito descartando o dejando como último recurso el pago del rescate, ya que habrá una tendencia alcista de estos delito, opciones a barajar podrían ser el uso e dispositivos analógicos o sistema de conexión local para resguardar la información en círculos cerrados de ordenadores sin conectarse a la red impidiendo el acceso de terceros, solo personal autorizado para manejar esos equipos.

No dejar todo completamente automatizado porque eso buscan, una vez infectado un equipo este al estar conectado a toda la red servirá como efecto contagio esparciéndose a otros ordenadores. Educar adecuadamente a la población y prioritariamente será la población de mayores de edad, ya que estos en su mayoría se encuentran en una posición de vulnerabilidad debido poca adaptabilidad que tienen algunos a las nuevas tecnologías, siendo fácilmente manipulados.

DISCUSIÓN

Como resultado de la investigación, el gobierno argentino y por extinción el de Córdoba, así como los habitantes conocen poco sobre los riesgos y consecuencias que produjo el avance de las tecnologías de información y comunicación, siendo más vulnerables o propensos a ser víctimas de cualquier tipo de delito que se pueda producir a través de estas herramientas. Si analizamos el modo en el que operan las organizaciones o los individuos que perpetúan este tipo de actividades podemos observar que son personas constantes en la búsqueda de alguna vulnerabilidad, distracción o desliz por parte de la víctima o víctimas, se los puede considerar oportunistas o insistentes dependiendo del ciberdelito que se observe, buscan el error y el provecharse de la ignorancia de sus víctimas y ese es uno de los ejes donde podría moverse la justicia para fortalecer y prevenir a la ciudadanía y a sus propios organismos de sufrir hackeos o vulneraciones en sus sistemas o redes. A lo largo de la investigación el planteamiento del problema, así como los objetivos fueron cambiando, la poca información que se tiene sobre antecedentes relacionados con la provincia de Córdoba son pocos y se buscó un planteamiento del problema mixto, es decir revelar antecedentes de todo u otras partes del territorio argentino además de Córdoba.[16]

Una de las limitaciones de este trabajo fue los pocos antecedentes referidos a la ciudad de Córdoba considerando este escrito como un aporte más y necesario para el análisis criminal de estas conductas y para la comprensión de las motivaciones atrás de estas personas que buscan la oportunidad, satisfacción, el dinero, entre otros. Una línea de seguimiento podría ser, no quedarse solo en el ámbito del ciber espacio,

CONCLUSIONES

El objetivo de esta investigación fue describir y explicitar las acciones gubernamentales que aborden el análisis de la conducta criminal ciber delictiva tendiente a los ransomware llevada adelante por el Tribunal Superior de Justicia de la Provincia de Córdoba. Cabe mencionar que en las fuentes documentales consultadas para responder a esta pregunta de investigación se logró encontrar evidencia que nos permita inferir que el análisis de la conducta criminal se puede utilizar para analizar casos que presenten estas características específicas. Pero no se hallaron investigaciones previas que analicen la casuística de dichos hechos desde la perspectiva del análisis operativo de caso. Estos tipos de análisis son posibles porque los mismos cumplen con las características esenciales que deben tener para poder ser abordados por dicho método, la serialidad y autor/es desconocido. Pese al alcance de índole descriptivo y explicativo la convierten en un aporte sumamente necesario para el crecimiento del estudio, conocimiento del tema y la construcción de posibles líneas de investigación y también de nuevos métodos de análisis delictual. Ya que, junta las variables de ataques focalizadas en la provincia de Córdoba, para vincularlas específicamente con el método de análisis operativo de casos, lo que aporta una respuesta novedosa a las principales preguntas que constituyen la esencia del manuscrito. Dentro de los factores sociales y culturales que influyen en la conducta de los ciberdelincuentes, los resultados hallados se relacionan

principalmente a la estructura del ciberespacio y como los delincuentes interactúan con este, que demuestra cómo se adaptan y prenden a utilizar esos conocimientos para delinquir. Las humillaciones y degradaciones que padecen las victimas en el proceso demuestra la vulnerabilidad y la poca respuesta con la que quedan después del ataque, dejando en evidencia la impunidad y libertad con la que se manejan los ciberdelincuentes. Ya que, a pesar de que el estado tiene el control de los medios de comunicación o por lo menos los medios telemáticos, le es imposible controlar el tráfico y volumen de información que hay y le es complicado la prevención por medio de concientización.

FINANCIACIÓN

Ninguna.

CONFLICTO DE INTERESES

Los autores declaran que no existe conflicto de intereses.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Curación de datos: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Análisis formal: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Investigación: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Metodología: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Administración del proyecto: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Recursos: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Software: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Supervisión: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Validación: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Visualización: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Redacción – borrador original: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Redacción – revisión y edición: Agustín Ramiro Manrique Aguad, María Belén Gauna.

REFERENCIAS BIBLIOGRÁFICAS

1. Sain G. Cibercrimen y delitos informáticos. Buenos Aires: Instituto de Pensamiento Penal; 2018. Disponible en: https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

2. Abogacía Española. Ransomware: una guía de aproximación para el empresario. Madrid: Consejo General de la Abogacía Española; s. f. Disponible en: https://www.abogacia.es/wp-content/uploads/2017/07/Guia_Ransomware.pdf

3. Ministerio de Justicia y Derechos Humanos. Ley 26.388. Delitos informáticos. Buenos Aires: Infoleg; 2008 jun 4. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

4. Moreno J, Rodríguez C, Leguias I. Revisión sobre propagación de ransomware en sistemas operativos Windows. 2019 mar 26. Disponible en: http://portal.amelica.org/ameli/jatsRepo/339/3391488005/3391488005.pdf

5. Secretaría de Innovación Tecnológica del Sector Público. El ransomware: el software malicioso usado para atacar a las organizaciones. Buenos Aires: Presidencia de la Nación Argentina; s. f. Disponible en: https://www.argentina.gob.ar/sites/default/files/2022/08/el_ransomware_el_software_malicioso_usado_para_atacar_a_las_organizaciones.pdf

6. Dirección Nacional de Ciberseguridad. Informe anual de incidentes de seguridad informática registrados en el 2021 por el CERT. Buenos Aires: Presidencia de la Nación Argentina; 2022 feb. Disponible en: https://www.argentina.gob.ar/sites/default/files/2022/02/informe_2_cert_2021_f_.pdf

7. Telecom Argentina. Información de Telecom sobre situación de ciberseguridad. Buenos Aires: Telecom Argentina; 2022 jul 20. Disponible en: https://institucional.telecom.com.ar/prensa/noticias/nota/informacion-de-telecom-sobre-situacion-de-ciberseguridad/415

8. El Doce. Por el ciberataque, la Justicia restringió sus actividades para el resto de la semana [video]. Córdoba: El Doce; 2022 ago 12. Disponible en: https://www.youtube.com/watch?v=Lg4wEBio3ts

9. Écijale Á. El ciberespacio: un mundo sin ley. s. f. Disponible en: http://ciberderecho.com/El_ciberespacio_un_mundo_sin_ley.pdf

10. Todo Noticias. Senado hackeado: denuncian un ciberataque al cuerpo legislativo [video]. Córdoba: TN; 2022 feb 1. Disponible

en: https://www.youtube.com/watch?v=tbt0bBGxhd8

11. Secretaría de Educación, Subsecretaría de Promoción de Igualdad y Calidad Educativa. Grooming. Córdoba: Gobierno de la Provincia de Córdoba; 2016. Disponible en: https://www.igualdadycalidadcba.gov.ar/SIPEC-CBA/publicaciones/2016-Docs/grooming%202016.pdf

12. Fusz LR. Los problemas de determinación del grooming [tesis de pregrado]. Córdoba (AR): Universidad Siglo 21; 2017.

13. Erreius. Cibercrimen y delitos informáticos. 2018. Disponible en: https://www.errepar.com/resources/descargacontenido/CIBERCRIMEN.PDF

14. Ucciferri L. La ciberseguridad en la era de la vigilancia masiva. Buenos Aires: Asociación por los Derechos Civiles; 2016. Disponible en: https://adc.org.ar/wp-content/uploads/2019/06/013-A-ciberseguridad-en-la-era-de-la-vigilancia-masiva-05-2016.pdf

15. González ML. La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado. 2017. Disponible en: http://www.seguridadinternacional.es/?q=es/content/la-cibercriminalidad-como-instrumento-para-la-expansi%C3%B3n-y-empoderamiento-del-crimen

16. Cybersecurity Hub. Los principales desafíos que enfrenta el sector de la ciberseguridad en Córdoba y la región. Córdoba: CorLab; s. f. Disponible en: https://corlab.cordoba.gob.ar/wp-content/uploads/2022/07/Publicacion-Ciberseguridad-Hub-vertical.pdf