South American Publishing

SAP Netnography. 2024; 2:69
doi: 10.62486/net202469

ORIGINAL

Criminal Behavior Analysis of Cybercriminals: Profiles, Motivations, and Trends in Cybersecurity

Análisis del Comportamiento Criminal del Ciberdelincuente: Perfiles, Motivaciones y Tendencias en la Ciberseguridad

Cecilia Elizabeth Checchia[1], Francisco Gabriel Bolzan[1]

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

Cite as
Checchia CE, Bolzan FG. Criminal Behavior Analysis of Cybercriminals: Profiles, Motivations, and Trends in Cybersecurity. SAP Netnography. 2024; 2:69. https://doi.org/10.62486/net202469

Publication History
Submitted: 03-05-2023
Revised: 10-08-2023
Accepted: 01-01-2024
Published: 02-01-2024

ABSTRACT

Within the vast territory of the digital world, a challenge has emerged in recent years, that of the cybercriminal. This agent, with perplexing technical skills, transcends physical borders, threatening the security and privacy of individuals, businesses, and institutions alike. In this context, the need to unravel the mysteries surrounding their behavior becomes evident. Thus, this research becomes a source of knowledge in the midst of this complex digital environment by addressing the modus operandi of these malicious actors and, in doing so, aspiring to understand their psychological profiles, motivations, and patterns of action within the broad field of cybersecurity. Through the exploration of cases that have occurred in our country and the analysis of literature, this study aims to provide a comprehensive overview of how these figures maneuver in the virtual space. The goal is not only to observe their actions but also to decipher the background of their intentions. As we investigate this scenario, the need to implement both preventive and corrective approaches that are effective in mitigating their impact becomes evident. This research represents a commitment to expanding the spectrum of knowledge regarding criminal behavior in the digital realm. The objective is undoubtedly to strengthen the sphere of cybersecurity through the substantial contribution it makes to the understanding of these actors and, consequently, to the development of mitigation strategies. However, its implications go beyond lines of code and security protocols. By providing a solid foundation of understanding, the aim is to protect not only systems but also individuals, organizations, and institutions facing these digital threats. The convergence of psychology, criminology, and cybersecurity provides us with a more comprehensive view that goes beyond the purely technical and delves into underlying motivations. This union, at its core, aims to establish a robust defense in this ongoing digital battlefield. This study presents itself as a concrete effort to explore the most enigmatic aspects of the interaction between humans and machines, where malice, intention, and vulnerability intertwine. Through this research, we embark on a journey toward understanding and, consequently, toward preparing for a safer coexistence in the digital environment.

Keywords: Cybercrime; Cybersecurity; Cybercriminal Profiles; Cybercrime Motivations; Cybersecurity Trends.

RESUMEN

En el inmenso territorio del mundo digital, surge un desafío que en los últimos años ha cobrado un notable crecimiento, hablamos del ciberdelincuente. Este agente con habilidades técnicas desconcertantes trasciende las fronteras físicas, amenazando la seguridad y privacidad de individuos, empresas e instituciones por igual. En esta coyuntura, surge la necesidad de desentrañar los misterios que rodean su comportamiento. De este modo, esta investigación se convierte en una fuente de conocimiento en medio de este entorno digital complejo al abordar el modus operandi de estos actores maliciosos y, con ello, aspirar a comprender sus perfiles psicológicos, motivaciones y patrones de actuación dentro del amplio campo de la ciberseguridad. A través de la exploración de casos ocurridos en nuestro país y el análisis de bibliografía, este estudio tiene por objeto presentar una panorámica completa de cómo estas figuras maniobran en el espacio virtual. Se busca no solo observar sus acciones, sino también descifrar el trasfondo de sus intenciones. A medida que investigamos este escenario, se hace evidente la necesidad de implementar enfoques tanto preventivos como correctivos que sean efectivos en la mitigación de su impacto. Esta investigación, representa un compromiso con la ampliación del espectro del conocimiento en lo que respecta al comportamiento criminal en el ámbito digital. La meta es, sin lugar a duda, reforzar la esfera de la ciberseguridad a través del aporte sustantivo que brinda al entendimiento de estos actores y, por ende, al desarrollo de estrategias de mitigación. No obstante, sus implicaciones trascienden las líneas de código y protocolos de seguridad. Al proporcionar una base sólida de comprensión, se busca proteger no

© 2024; 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.

solo sistemas, sino también a individuos, organizaciones e instituciones que se enfrentan a estas amenazas digitales. La convergencia de la psicología, la criminología y la ciberseguridad nos proporciona una visión más integral, que va más allá de lo puramente técnico y se adentra en las motivaciones subyacentes. Esta unión, en su esencia, tiene como objetivo establecer una defensa sólida en este continuo campo de batalla digital. Este estudio se presenta como un esfuerzo concreto para explorar los rincones más enigmáticos de la interacción entre humanos y máquinas, donde se entrelazan malicia, intención y vulnerabilidad. Mediante esta investigación, emprendemos un viaje hacia la comprensión y, por ende, hacia la preparación para una convivencia más segura en el entorno digital.

Palabras clave: Ciberdelito; Ciberseguridad; Cibercrimen; Perfiles de Ciberdelincuentes; Motivaciones del Ciberdelito; Tendencias de Ciberseguridad.

INTRODUCCIÓN

En la actualidad, el campo de la ciberseguridad se ha convertido en un terreno cada vez más complejo y desafiante. La creciente dependencia de la tecnología y la interconexión global de sistemas informáticos han dado lugar a la aparición de un tipo de delincuencia que trasciende las fronteras físicas, este es el ciberdelito.[1,2,3] Esta forma de actividad criminal, llevada a cabo por individuos conocidos como ciberdelincuentes, plantea amenazas significativas tanto para individuos como para organizaciones de diversa índole, que van desde gobiernos hasta empresas y usuarios comunes. Este fenómeno requiere una atención y una respuesta adecuada para resguardar la seguridad en el entorno digital.[4,5,6]

La evolución tecnológica ha impulsado cambios que han reconfigurado nuestras rutinas diarias, nuestro entorno laboral y nuestras formas de comunicarnos. A pesar de las ventajas y facilidades que esta evolución ha aportado, también ha dado origen a un ámbito digital en el cual operan personas con un alto dominio técnico. Estos individuos emplean sus destrezas para llevar a cabo acciones ilícitas, dando lugar al fenómeno conocido como ciberdelincuencia.[7,8,9]

La ciberdelincuencia opera en un entorno altamente sofisticado y en constante evolución, lo que plantea desafíos continuos en su detección y prevención. Este entorno dinámico requiere una respuesta igualmente ágil y avanzada para garantizar la seguridad en el mundo digital.[10,11,12]

Es esencial comprender en profundidad el comportamiento de los ciberdelincuentes para poder desarrollar estrategias efectivas de ciberseguridad y contrarrestar sus actividades.

La relevancia de esta investigación se hace evidente en un entorno digital en constante evolución, donde las amenazas cibernéticas pueden tener consecuencias devastadoras en términos de pérdida de datos, interrupción de servicios críticos y violación de la privacidad. Comprender quiénes son los ciberdelincuentes, qué los impulsa y cómo operan, es fundamental para minimizar los riesgos asociados con la tecnología.[13,14,15]

A lo largo de estas páginas, se examinarán los resultados de un análisis riguroso de información, identificación de perfiles de ciberdelincuentes, sus motivaciones, así como las tendencias emergentes en el ámbito de la ciberseguridad, como por ejemplo el uso de la IA (Inteligencia Artificial).[16,17,18]

El enfoque de esta investigación implica la intersección de campos como la psicología, la criminología y la ciberseguridad. A través de esta perspectiva integral, se busca obtener una visión completa de la mente del ciberdelincuente y los factores que influyen en sus acciones.[19,20,21]

Esta investigación aspira a contribuir al conocimiento existente en el campo de la ciberseguridad y servir como una herramienta valiosa para los profesionales, investigadores y responsables de la formulación de políticas que buscan abordar el desafío constante de proteger el ciberespacio en un mundo cada vez más interconectado. Los hallazgos y conclusiones aquí presentados no solo enriquecerán la comprensión de la ciberdelincuencia, sino que también brindarán orientación para el desarrollo de estrategias efectivas de prevención y respuesta en la era digital.[22,23,24]

En el primer capítulo, se presenta el contexto y la justificación de esta investigación. Se destaca la importancia de analizar el comportamiento del ciberdelincuente en el marco del panorama actual de ciberseguridad y se subraya la necesidad de abordar este desafío desde una perspectiva multidisciplinaria ofreciendo un sólido fundamento para el abordaje de este tema.[25,26,27]

En el segundo capítulo, se construye el marco teórico necesario, que nos proporcionará un entendimiento completo y unificado de la ciberdelincuencia y la ciberseguridad en el análisis del comportamiento criminal.[28,29,30,31]

Los siguientes capítulos profundizan en las múltiples facetas del comportamiento delictivo de los ciberdelincuentes. Se examinan los perfiles psicológicos típicos, las habilidades técnicas que distinguen a estos individuos malintencionados y los factores que influyen en su selección de objetivos. Además, se analizan las variadas motivaciones que impulsan sus acciones, que abarcan desde incentivos financieros hasta motivaciones ideológicas, políticas y el simple deseo de enfrentar desafíos. Este análisis proporciona una comprensión más completa de la complejidad de la ciberdelincuencia.[32,33,34,35,36]

El cuarto capítulo nos introduce en el análisis de las tendencias y patrones de comportamiento que emergen de los ciberataques y cómo estos delincuentes evaden la detección mediante el uso de técnicas de ingeniería social y manipulación psicológica. A través del estudio de casos de ciberataques reales, se proporciona una visión detallada de las estrategias utilizadas por estos individuos.[37,38,39,40,41]

En el quinto capítulo, exploraremos la conexión entre la ciberdelincuencia y el ciberterrorismo. Analizaremos cómo ciertos ciberdelincuentes pueden verse influenciados por el proceso de radicalización en línea, lo que los lleva a involucrarse en actividades con motivaciones terroristas claramente definidas. Este análisis enriquecerá nuestra comprensión de la intersección entre estos dos campos y sus repercusiones tanto en el ámbito académico como en el profesional.[42,43,44,45,46]

Por último, el sexto capítulo aborda estrategias de prevención y mitigación para enfrentar el comportamiento criminal del ciberdelincuente. Se destacan enfoques de fortalecimiento de la ciberseguridad, educación y concientización, así como la importancia de la colaboración entre el sector público y privado para abordar este desafío de manera integral.[47,48,49,50,51]

Con este análisis se pretende mejorar el entendimiento sobre el comportamiento criminal de los ciberdelincuentes.[52,53,54] Se busca brindar herramientas efectivas para robustecer la ciberseguridad y resguardarnos de las embestidas cibernéticas. En el proceso, nos sumergimos en las complejidades de sus perfiles, motivaciones y patrones, trazando un camino hacia un entorno digital más seguro y resiliente para todos los que participamos en este constante intercambio de información y poder.[55,56,57,58]

Contexto y Justificación

En la actualidad, nos encontramos inmersos en una era de transformación digital que ha tenido un gran impacto en nuestra vida cotidiana. La digitalización y la interconexión global de sistemas informáticos han impulsado una revolución tecnológica que ha permeado todos los aspectos de nuestra existencia: cómo vivimos, cómo trabajamos y cómo nos comunicamos. Si bien este cambio tecnológico ha aportado innumerables beneficios y comodidades, también ha planteado una serie de desafíos complejos y diversos. Entre estos desafíos, uno que se destaca por su creciente urgencia es el rápido aumento de la ciberdelincuencia. Este fenómeno requiere una atención especial y una respuesta eficaz por parte de la sociedad y la comunidad académica.[59,60]

La ciberdelincuencia es un concepto que abarca una amplia y diversa gama de actividades criminales que se ejecutan en el amplio y complejo territorio del ciberespacio.

“Son conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas.

Consiste en estafas, robos de datos personales, de información comercial estratégica, suplantación de identidad, fraudes informáticos, ataques como cyberbulling, grooming, phishing cometidos por ciberdelincuentes que actúan en grupos o trabajan solos.”

Antecedentes: A lo largo de los años, se han documentado numerosos incidentes y tendencias alarmantes en el ámbito de la ciberseguridad que respaldan la urgente necesidad de abordar este fenómeno. Según estadísticas recientes de ESET en su informe “Security Report Latinoamérica 2023”, los ataques cibernéticos se han multiplicado y diversificado, causando pérdidas económicas significativas a nivel global. Organizaciones y ciudadanos comunes han experimentado el impacto directo de la ciberdelincuencia en forma de robos de datos, extorsiones, ataques de ransomware y otros delitos cibernéticos.[61,62,63,64]

Investigaciones e informes anteriores en el campo de la ciberseguridad, han proporcionado claridad sobre los diferentes aspectos de este problema, desde la identificación de vulnerabilidades en sistemas informáticos hasta la implementación de soluciones técnicas. No obstante, a pesar de los esfuerzos sostenidos en esta dirección, perduran desafíos de naturaleza multifacética en lo que respecta a la prevención y atenuación de las amenazas tecnológicas.[65,66,67]

Aquí, en este entorno digital sin fronteras físicas, los ciberdelincuentes despliegan sus conocimientos técnicos avanzados con el propósito de cometer una variedad de actos ilegales. Sus acciones oscilan desde el robo de datos confidenciales y la extorsión.[68]

cibernética, hasta el sabotaje de infraestructuras críticas y la ejecución de operaciones de espionaje. Los ciberdelincuentes, en su mayoría invisibles para el ojo humano, operan en un espacio virtual donde las fronteras se desvanecen, y las jurisdicciones se superponen y se despliegan en cuestión de milisegundos.

A medida que nuestra sociedad ingresa en una era cada vez más conectada y dependiente de la tecnología, las amenazas aparecen como un problema de seguridad de alcance global. Esta preocupación abarca a una variada gama de actores, desde multinacionales hasta los organismos gubernamentales responsables de resguardar la seguridad, y hasta el ciudadano común y corriente que confía su vida digital a plataformas en línea. El ciberdelito, en su esencia, no solo tiene el potencial de causar pérdidas económicas significativas, sino que también plantea amenazas mucho más grandes, incluida la vulnerabilidad de nuestra seguridad, la pérdida de la privacidad y la integridad de datos críticos que sustentan el funcionamiento de nuestra sociedad actual.[69,70,71]

El problema central que abordamos en esta tesis reside en la urgente necesidad de comprender y analizar de manera detallada el comportamiento de los ciberdelincuentes. A pesar de los esfuerzos continuos y sostenidos en el campo de la ciberseguridad, la identificación y mitigación de las amenazas persisten como un desafío perpetuo y multifacético. Para enfrentar de manera eficiente y eficaz el ciberdelito en todas sus dimensiones, es imperativo descifrar la compleja dinámica de quiénes son estos actores, qué impulsa sus acciones ilegales en línea y cómo evolucionan y adaptan sus tácticas y estrategias a lo largo del tiempo.[72,73,74]

El comportamiento de los ciberdelincuentes se presenta como una pieza esencial en el intrincado rompecabezas de la ciberseguridad. ¿Quiénes son realmente estos individuos que operan detrás de las pantallas? ¿Cuáles son los factores, motivaciones y desencadenantes subyacentes que los llevan a cometer actos criminales en el ciberespacio? ¿Cómo se organizan y coordinan en este mundo digital aparentemente sin límites ni fronteras definidas? ¿Qué tendencias emergentes en el ciberdelito debemos monitorear y entender a fondo para anticiparnos y enfrentar las amenazas que se perfilan en el horizonte? Estas son solo algunas de las preguntas fundamentales que esta investigación se propone abordar con la mayor profundidad y meticulosidad.[75,76,77]

El conocimiento adquirido acerca del comportamiento delictivo de los ciberdelincuentes no solo resulta fundamental para la prevención activa y la respuesta efectiva frente a los ciberataques en curso, sino que también tiene una importancia fundamental en la formulación y ejecución de políticas y estrategias de ciberseguridad sólidas y proactivas. Al comprender las motivaciones, así como las dinámicas sociales que subyacen en las acciones de los ciberdelincuentes, podemos crear estrategias más efectivas para desalentar, prevenir y disuadir su actividad delictiva.[78,79,80]

La comprensión y la caracterización del comportamiento delictivo de los ciberdelincuentes son importantes para garantizar la seguridad, la integridad y la confianza en un mundo digital que se encuentra en constante evolución. Esta investigación aspira a

contribuir al conocimiento y al diseño de estrategias efectivas para afrontar el ciberdelito, trascendiendo las limitaciones actuales y forjando un futuro más seguro en el entorno digital. La confianza en la tecnología se muestra como un elemento esencial para la adopción generalizada de innovaciones tecnológicas. Para que la sociedad continúe aprovechando los innumerables beneficios de la tecnología, es imperativo mantener la confianza en las plataformas y sistemas digitales.[81,82,83]

Objetivos de la investigación

Objetivo General

El objetivo general de esta investigación es profundizar en la comprensión de la ciberdelincuencia y la ciberseguridad con el propósito de fortalecer la seguridad en línea y contribuir al conocimiento en este campo.

Objetivos Específicos

- Identificar y categorizar los perfiles psicológicos que caracterizan a los ciberdelincuentes, a través de un enfoque multidisciplinario que integre elementos de psicología y criminología.
- Investigar las diversas motivaciones que impulsan a los ciberdelincuentes a cometer delitos en línea, abarcando incentivos financieros, objetivos políticos e ideológicos, entre otros.
- Analizar tendencias y patrones de comportamiento emergentes mediante el estudio detallado de casos reales de ciberataques, con el fin de identificar secuencias repetitivas de acciones y tácticas utilizadas por los ciberdelincuentes.
- Desarrollar estrategias efectivas de prevención y mitigación de ataques cibernéticos, basadas en el entendimiento adquirido sobre el comportamiento de los ciberdelincuentes, que incluyan medidas técnicas y buenas prácticas de seguridad.
- Contribuir al conocimiento en el campo de la ciberseguridad y la prevención de la ciberdelincuencia mediante la presentación de nuevos datos, enfoques y perspectivas que enriquezcan la base de conocimientos existente.
- Promover la colaboración y la conciencia en ciberseguridad, destacando la importancia de la cooperación entre diversos actores involucrados en la seguridad en línea y fomentando la toma de conciencia sobre las amenazas cibernéticas para abordar este desafío de manera conjunta y efectiva.

MÉTODO

La presente investigación se llevará a cabo utilizando una metodología cualitativa. Se busca obtener una visión integral y enriquecedora que permita explorar tanto los aspectos psicológicos y motivacionales de los ciberdelincuentes como las tendencias y patrones de comportamiento que surgen de sus acciones en línea.

A continuación, se describen las principales etapas de la metodología que se seguirá:

- Revisión bibliográfica: se realizará una revisión de la literatura científica y técnica relacionada con la ciberdelincuencia, la ciberseguridad y la psicología criminal. Esta revisión permitirá obtener una comprensión sólida de los conceptos fundamentales y las teorías relevantes en el campo de estudio.
- Análisis de casos prácticos: se llevará a cabo un examen detallado de casos reales de ciberataques, así como de las actividades llevadas a cabo por ciberdelincuentes, con el fin de estudiar sus tácticas, técnicas y procedimientos. Estos casos servirán como ejemplos para comprender las motivaciones que impulsan estos ataques y cómo los ciberdelincuentes evaden la detección.
- Recomendaciones: los resultados obtenidos a partir del análisis serán utilizados para formular recomendaciones que aborden eficazmente la ciberdelincuencia y fortalezcan la ciberseguridad. Se propondrán estrategias de prevención y mitigación basadas en el análisis del comportamiento criminal del ciberdelincuente.

DESARROLLO

Ciberdelincuencia y ciberseguridad

La ciberdelincuencia y la ciberseguridad son conceptos estrechamente relacionados que desempeñan un papel esencial en el entorno digital. A pesar de su importancia, la conceptualización precisa de estos términos aún no ha alcanzado un consenso universal. Por este motivo, se ha recurrido a diversas definiciones propuestas por expertos en el campo, con el objetivo de aproximarnos a una comprensión más precisa a través de la interpretación de sus enfoques y perspectivas. A continuación, se describen ambos términos:

Ciberdelincuencia

La ciberdelincuencia es un término que abarca una variedad de conceptos y acepciones, lo que puede hacer que su definición sea un tanto compleja. Para comprenderlo mejor, es útil desglosarlo en términos de a quién va dirigido, quién lo origina y la naturaleza del delito en cuestión.

En términos generales, podemos definir la ciberdelincuencia como el conjunto de acciones llevadas a cabo a través de sistemas informáticos o bienes digitales que resultan en actos considerados ilícitos. En otras palabras, es una extensión del crimen tradicional que se vale de las nuevas tecnologías para expandirse y desarrollarse de manera amplia.

Para profundizar un poco más en esta definición, podemos considerar como ciberdelictivas aquellas acciones que ponen en riesgo la confidencialidad, integridad y disponibilidad de sistemas informáticos, redes y datos, así como el uso fraudulento de dichos sistemas. Esta definición se basa en el Convenio sobre Cibercriminalidad de Budapest del 23 de noviembre de 2001, que establece un marco internacional para abordar los delitos cibernéticos.

Aunque gran parte de la ciberdelincuencia gira en torno a la obtención de información confidencial con fines no autorizados, es

importante reconocer que este fenómeno también engloba actos criminales que son familiares en el mundo no digital. Hablamos de delitos como robos, suplantación de identidad, fraude, acoso y una serie de otros actos delictivos que, considerando esto, se realizan a través de la Internet.

La ciberdelincuencia no se limita únicamente a la esfera de la tecnología, sino que abarca una amplia gama de actividades ilegales que pueden tener consecuencias graves tanto en el mundo virtual como en el mundo real. La evolución constante de las amenazas en línea hace que sea crucial abordar esta problemática de manera integral.

Tomando como referencia la información brindada por el Ministerio de Justicia y Derechos Humanos5, los ciberdelitos y contravenciones más comunes representan una serie de actividades delictivas que se llevan a cabo en el entorno digital y que abarcan diversas formas de intrusión y manipulación de datos informáticos con el propósito de obtener ganancias económicas y causar daño. Estas acciones, que se caracterizan por su carácter ilícito, pueden ser agrupadas en varias categorías:

- Ataques a la navegación: estos ataques consisten en la redirección de navegadores web hacia sitios maliciosos que pueden infectar los sistemas con malware, como virus, gusanos y troyanos. Los efectos de tales programas incluyen la eliminación de datos, la infección de dispositivos, la activación no autorizada de cámaras y micrófonos, así como la extracción de información confidencial.
- Ataques a servidores: los ciberdelincuentes pueden dirigir sus esfuerzos a servidores con el propósito de dañar o robar datos, así como de negar el acceso legítimo a la información almacenada en dichos servidores.
- Corrupción de bases de datos: esta modalidad de ciberdelincuencia implica interferir en bases de datos, tanto públicas como privadas, para generar información falsa o sustraer datos sensibles.
- Virus informáticos: los virus informáticos cifran archivos, bloquean sistemas, y hasta roban dinero mediante el envío de mensajes de texto fraudulentos que aparentan ser de empresas legítimas.
- Programas de espionaje: estos programas tienen la capacidad de acceder y utilizar cámaras y micrófonos en dispositivos sin autorización, además de recopilar información personal de manera secreta.

En la ejecución de estos ciberdelitos, se emplea frecuentemente la ingeniería social como medio para engañar, amenazar y obtener datos personales o información sensible de individuos u organizaciones, lograr beneficios económicos, suplantar identidades, acosar digitalmente o cometer agresiones sexuales en línea. Algunos ejemplos de estas prácticas son:

- Phishing o vishing: ciberdelincuentes se hacen pasar por entidades legítimas, como empresas de servicios o instituciones gubernamentales, con el fin de obtener información personal para suplantar identidades y llevar a cabo actividades ilícitas en cuentas bancarias, perfiles en plataformas digitales y redes sociales, así como en servicios en línea.
- Ciberbullying: el acoso en línea, conocido como ciberbullying, se manifiesta en la persecución, el acoso y la difamación de individuos a través de mensajería instantánea y redes sociales, con el objetivo de afectar su integridad moral y su reputación.
- Grooming: en este caso, adultos intentan obtener imágenes o videos sexuales de menores de edad de manera oculta, con fines de chantaje o abuso sexual posterior.
- Sextorsión: implica la solicitud de dinero a cambio de no difundir imágenes generadas en el contexto de un intercambio erótico consensuado.
- Ciberodio: comprende contenidos inapropiados que vulneran a las personas, como la promoción de violencia, odio, xenofobia, racismo, discriminación y maltrato animal.
- Pornografía infantil: Se refiere a la explotación sexual de menores y la producción y comercialización de contenido explícito relacionado con estos actos.

Además de las mencionadas categorías de ciberdelitos, existe otra dimensión que involucra la violación de la privacidad de las personas, que incluye:

- Espionaje ilícito de comunicaciones privadas ciudadanas.
- Violación de la intimidad por parte de proveedores de servicios de internet sin consentimiento del usuario, para obtener información sobre sus preferencias y facilitar la venta agresiva de productos y servicios relacionados.
- Acceso no autorizado a las comunicaciones privadas de empleados, como correos electrónicos y perfiles en redes sociales.

El crecimiento de la ciberdelincuencia ha sido notorio en los últimos años, impulsado de manera significativa por el imparable avance de la tecnología y la creciente interconexión de nuestros sistemas, los ciberdelincuentes han demostrado una capacidad de adaptación asombrosa, no solo para aprovechar las nuevas tecnologías, sino también para perfeccionar sus tácticas, volviéndolas cada vez más sofisticadas y difíciles de detectar.

La inteligencia artificial (IA) se ha convertido en una herramienta clave tanto para los ciberdelincuentes como para los profesionales de la ciberseguridad. Los actores maliciosos utilizan la IA para automatizar tareas, como la identificación de vulnerabilidades en sistemas y redes, el phishing y la generación de malware altamente personalizado. Esta automatización agiliza sus operaciones y les permite escalar sus ataques de manera eficiente.

La complejidad y la gravedad de los ciberdelitos siguen en aumento. Los ataques ransomware, por ejemplo, han evolucionado hacia una forma aún más peligrosa, conocida como “doble extorsión”, en la que los atacantes no solo cifran los datos de la víctima, sino que también amenazan con divulgar información confidencial si no se paga un rescate. Esto agrega una dimensión adicional de

presión sobre las víctimas. Los ciberdelincuentes también se han vuelto más selectivos al elegir sus objetivos.

Las organizaciones gubernamentales, las grandes empresas y las infraestructuras críticas son blancos populares debido al potencial impacto económico y social de sus ataques.

Dentro de este escenario, la promoción de la educación y la concienciación en temas de ciberseguridad se torna imperativa. Las personas y las organizaciones deben comprender las amenazas que enfrentan y adoptar prácticas de seguridad sólidas, como el uso de contraseñas seguras, la autenticación MFA y la actualización regular de software y sistemas.

Ciberseguridad

La ciberseguridad abarca un conjunto de medidas, tecnologías y estrategias destinadas a resguardar los sistemas informáticos, redes y datos de amenazas cibernéticas y actos delictivos en línea. Su propósito fundamental radica en preservar la integridad, confidencialidad y disponibilidad de la información digital, al tiempo que asegura la protección de los activos y recursos en el entorno digital.

En el ámbito de la ciberseguridad, se implementan diversas medidas para proteger sistemas y datos sensibles. Estas estrategias incluyen:

- Sistemas de Detección y Prevención de Intrusiones: se instalan sistemas que pueden detectar y prevenir intrusiones no autorizadas en las redes y sistemas informáticos, proporcionando una defensa activa contra posibles amenazas.
- Firewalls y Protección contra Malware: se utilizan cortafuegos y software de protección contra malware para filtrar el tráfico de red y evitar que software malicioso infecte los sistemas.
- Autenticación y Cifrado: se aplican métodos de autenticación sólidos y cifrado robusto para resguardar el acceso a información confidencial, garantizando que solo las personas autorizadas puedan acceder a ella.
- Capacitación y Concienciación: se brinda formación al personal en prácticas seguras en línea, promoviendo la concienciación sobre los riesgos cibernéticos y la importancia de mantener la seguridad digital en el lugar de trabajo.
- Colaboración y Compartir Información sobre Amenazas y Vulnerabilidades: La cooperación entre diferentes actores, es esencial para intercambiar información sobre amenazas cibernéticas y vulnerabilidades, permitiendo una respuesta más efectiva.

También, es fundamental considerar otras prácticas de ciberseguridad, como:

- Copia de Seguridad de Datos: resguardar datos críticos en ubicaciones seguras y garantizar la capacidad de restaurar copias probadas en caso de pérdida o corrupción de archivos.
- Hábitos Cibernéticos Seguros: evitar abrir enlaces o archivos adjuntos inesperados en correos electrónicos o mensajes de texto, incluso si provienen de remitentes de confianza, para prevenir posibles ataques de phishing.
- Mantenimiento de Software Actualizado: actualizar sistemas operativos, aplicaciones y navegadores con las últimas revisiones y correcciones proporcionadas por los fabricantes, reduciendo así las vulnerabilidades explotables.
- Contraseñas Fuertes y Únicas: utilizar contraseñas robustas con al menos 14 caracteres, evitar palabras en inglés y evitar su reutilización en múltiples cuentas, fortaleciendo así la seguridad en línea.
- Autenticación Multifactor: activar la autenticación multifactor siempre que sea posible, añadiendo una capa adicional de seguridad tanto en entornos domésticos como laborales.
- Bloqueo de Dispositivos: configurar dispositivos para requerir una contraseña, PIN o autenticación biométrica, como huellas dactilares o reconocimiento facial, para acceder a ellos, reduciendo el riesgo en caso de pérdida o robo.

Estas prácticas, cuando se aplican de manera constante y eficiente, contribuyen significativamente a fortalecer la ciberseguridad y a proteger los activos digitales.

Por otra parte, los expertos en ciberseguridad también han adoptado la inteligencia artificial como una herramienta invaluable en la lucha contra la ciberdelincuencia. La aplicación de algoritmos de aprendizaje automático les permite analizar patrones de tráfico en busca de actividades sospechosas, identificar comportamientos inusuales y anticipar posibles amenazas. La inteligencia artificial juega un rol esencial en la detección y mitigación de ataques en tiempo real, lo cual se ha convertido en una necesidad indispensable en un entorno digital en constante evolución.

Con la tecnología avanzando constantemente y la ciberdelincuencia representando una amenaza persistente, la ciberseguridad se mantiene en un estado de continua evolución y adaptación para enfrentar los desafíos y amenazas emergentes.

Conceptos fundamentales en el análisis del comportamiento criminal

En el análisis del comportamiento criminal, se destacan conceptos esenciales que desempeñan un papel fundamental en la comprensión de las motivaciones, patrones y rasgos distintivos de los delincuentes. Estos conceptos, establecen una sólida base teórica que respalda la investigación en el ámbito del comportamiento delictivo, abarcando incluso el comportamiento criminal de los ciberdelincuentes. A continuación, se expondrán algunos de los conceptos más destacados en este campo de estudio:

Motivaciones: en el análisis del comportamiento criminal, es esencial explorar las razones que impulsan a una persona a cometer un acto ilícito. La comprensión de estas motivaciones desempeña un papel fundamental en esta disciplina. Estas motivaciones pueden ser diversas, abarcando aspectos económicos, sociales, políticos, así como impulsos personales y emocionales. En el caso específico de la ciberdelincuencia, las motivaciones pueden incluir la búsqueda de ganancias económicas, el deseo de reconocimiento, la adhesión a una ideología política o el interés por superar desafíos técnicos.

https://doi.org/10.62486/net202469

Perfiles Psicológicos: los perfiles psicológicos representan descripciones detalladas de las características, personalidad y patrones de comportamiento típicos de un determinado tipo de delincuente. En el ámbito del análisis del comportamiento criminal, el objetivo es identificar tendencias recurrentes en la conducta de los delincuentes que ayuden a comprender sus motivaciones y estrategias delictivas. Estos perfiles pueden incluir información sobre la edad, género, nivel educativo, antecedentes penales y otras características que puedan estar relacionadas con el comportamiento delictivo.

Ciclo Delictivo: el concepto de ciclo delictivo se refiere a las diversas etapas o fases que un delincuente puede atravesar, desde la concepción de un delito hasta su ejecución, y en algunos casos, la reincidencia. Estas etapas pueden abarcar la planificación, la selección del objetivo, la ejecución del delito y la huida. Comprender el ciclo delictivo proporciona información valiosa para prevenir y reducir los delitos, así como para entender cómo los delincuentes se preparan y llevan a cabo sus acciones, tanto en el contexto tradicional como en el ciberespacio.

Técnicas de Ingeniería Social: las técnicas de ingeniería social comprenden estrategias empleadas por individuos delictivos con el propósito de manipular a personas con el fin de obtener información confidencial o acceder de manera no autorizada a sistemas y datos. Estas tácticas se basan en la comprensión de la psicología humana, incluyendo aspectos como la confianza, el temor y la curiosidad, para inducir a las víctimas a cometer errores que permitan alcanzar sus objetivos ilícitos. En el contexto del análisis del comportamiento criminal de los ciberdelincuentes, la investigación de estas técnicas es de gran relevancia, dado que son ampliamente utilizadas en ataques cibernéticos.

Al analizar estas dimensiones, se puede obtener una visión más completa de los factores que impulsan a los delincuentes a cometer delitos y, en consecuencia, diseñar estrategias más efectivas para prevenir y enfrentar la ciberdelincuencia.

PERFILES PSICOLÓGICOS DEL CIBERDELINCUENTE Y MOTIVACIONES

El análisis del comportamiento criminal de los ciberdelincuentes implica la evaluación de perfiles psicológicos que caracterizan a estos individuos involucrados en actividades delictivas en el entorno digital. Es relevante destacar que los perfiles psicológicos pueden ser diversos, y no es posible aplicar un único patrón a todos los ciberdelincuentes. Sin embargo, se han identificado ciertas características comunes que proporcionan una visión más completa del comportamiento delictivo en línea. A continuación, se exponen algunos de los perfiles psicológicos que han sido observados en determinados ciberdelincuentes, iniciando por el perfil conocido como hacker ya que es importante conocer que no todos los hackers son ciberdelincuentes.

Perfil del Hacker

Un hacker es un individuo altamente habilidoso y versado en la informática y la tecnología de la información, cuyo enfoque principal es la exploración, comprensión y manipulación de sistemas y redes informáticas. Los hackers emplean sus conocimientos técnicos para identificar vulnerabilidades en sistemas informáticos, desarrollar soluciones creativas para problemas técnicos y, en algunos casos, para eludir restricciones de seguridad.

White Hat Hacker: el Hacker Ético, también conocido como "White Hat Hacker" o "Hacker de Sombrero Blanco," es un individuo altamente capacitado en seguridad informática que utiliza sus habilidades con un propósito ético y legal. Su principal enfoque es identificar y corregir vulnerabilidades en sistemas, redes y aplicaciones para proteger la integridad y la seguridad de la información.

Los Hacker Éticos se adhieren a un código ético estricto que prohíbe el uso de sus habilidades para fines maliciosos. Están comprometidos con la legalidad y la integridad en su trabajo. Poseen un profundo conocimiento de sistemas informáticos, programación y protocolos de red. Esto les permite identificar y comprender las vulnerabilidades de seguridad.

Hacker Motivado por el Desafío Técnico: Los hackers motivados por el desafío técnico, a menudo llamados "hackers aficionados" o "hackers por diversión", son individuos que se dedican a actividades de hacking principalmente por el interés en explorar y superar desafíos técnicos. Estos hackers están motivados por la curiosidad y el deseo de aprender sobre sistemas, redes y tecnología en general.

La principal motivación de los hackers motivados por el desafío técnico es su curiosidad por la tecnología. Disfrutan de la exploración de sistemas informáticos, la resolución de problemas y la comprensión de cómo funcionan las cosas.

Ven el hacking como una forma de aprendizaje continuo y autodidacta. Creen que, al desafiar sus habilidades técnicas, pueden mejorar constantemente y mantenerse actualizados en un campo en constante evolución.

A menudo, los hackers motivados por el desafío técnico operan dentro de límites éticos. No tienen la intención de causar daño o infringir la ley, sino que buscan explorar sistemas y redes de manera responsable y ética.

Estos hackers pueden participar en actividades como la configuración de laboratorios de pruebas, el análisis de vulnerabilidades en aplicaciones y sistemas, y la participación en competencias de hacking ético o CTFs (Capture The Flag) con el objetivo de resolver desafíos técnicos.

A menudo se involucran en comunidades en línea o grupos locales de hacking donde comparten conocimientos, colaboran en proyectos técnicos y discuten temas relacionados con la seguridad y la tecnología.

Aunque su motivación principal es el desafío técnico, estos hackers pueden hacer contribuciones valiosas a la comunidad de seguridad informática. Su habilidad para identificar vulnerabilidades y debilidades en sistemas puede ayudar a mejorar la seguridad en general.

Black Hat Hacker: los hackers maliciosos, comúnmente referidos como Black Hat Hackers o sombreros negros, son individuos que emplean sus habilidades informáticas con fines ilícitos y maliciosos. A diferencia de sus contrapartes éticas y de sombrero gris, estos hackers se dedican a actividades que infringen las leyes y a menudo buscan obtener beneficios personales o causar daño a

individuos, organizaciones o sistemas.

Algunas de las motivaciones de los Black Hat Hackers son intereses económicos. Su objetivo principal puede ser el robo de información financiera, como números de tarjetas de crédito o contraseñas de cuentas bancarias, con la intención de vender esta información en el mercado negro o cometer fraudes financieros.

Algunos hackers maliciosos se dedican a causar daño a sistemas informáticos, redes o sitios web. Utilizan diversas técnicas, como ataques de denegación de servicio (DDoS), inserción de malware o ransomware en sistemas vulnerables, o el robo y destrucción de datos valiosos.

La obtención de información confidencial, secretos comerciales o datos gubernamentales es otra motivación común para los Black Hat Hackers. Esta información puede ser utilizada con fines de espionaje o para obtener ventajas competitivas.

En ocasiones, los hackers maliciosos buscan venganza personal. Utilizan sus habilidades informáticas para causar daño como represalia por motivos personales, profesionales o ideológicos.

Los hackers de sombrero negro emplean una amplia gama de técnicas y herramientas para llevar a cabo sus actividades ilegales. Esto incluye el uso de malware (como virus, troyanos y ransomware), la explotación de vulnerabilidades en el software o los sistemas, el phishing para engañar a las personas y obtener acceso a sus cuentas, así como la ingeniería social para manipular a las personas y obtener información confidencial.

Grey Hat Hackers (Hackers de Sombrero Gris): los hackers de sombrero gris son individuos que operan en un espacio intermedio entre los hackers éticos (White Hat Hackers) y los hackers maliciosos (Black Hat Hackers). Su enfoque se caracteriza por una mezcla de intenciones, lo que hace que su posición sea menos clara en términos éticos. Algunas de sus motivaciones pueden ser por ejemplo el descubrimiento de vulnerabilidades, los hackers de sombrero gris comparten con los hackers éticos la motivación de descubrir vulnerabilidades y debilidades en sistemas y aplicaciones. Sin embargo, a diferencia de los hackers éticos, pueden realizar estas actividades sin el consentimiento explícito de las organizaciones afectadas.

A menudo, los hackers de sombrero gris buscan exponer las vulnerabilidades que descubren para que los propietarios de los sistemas puedan tomar medidas correctivas. Esto se conoce como "divulgación responsable" y tiene el propósito de mejorar la seguridad cibernética en lugar de explotar las vulnerabilidades.

Algunos hackers de sombrero gris pueden solicitar recompensas o reconocimiento por la divulgación de vulnerabilidades. Esto puede incluir recompensas monetarias o menciones públicas por su contribución a la seguridad.

Los hackers de sombrero gris pueden tener límites éticos variables. Aunque su intención principal es mejorar la seguridad, la ambigüedad en sus acciones puede llevar a ciertas controversias éticas.

Utilizan técnicas similares a las de los hackers éticos para identificar vulnerabilidades en sistemas y aplicaciones. Esto puede incluir escaneo de seguridad, pruebas de penetración y análisis de código.

La legalidad de las acciones de los hackers de sombrero gris puede variar según la jurisdicción y las circunstancias específicas. Mientras algunos pueden operar dentro de los límites de la ley, otros pueden estar en una zona gris legal.

A pesar de la ambigüedad ética, los hackers de sombrero gris desempeñan un papel importante en la mejora de la seguridad. Su capacidad para identificar y señalar vulnerabilidades ayuda a las organizaciones a fortalecer sus defensas cibernéticas y a proteger a los usuarios finales.

Hacktivistas: los hacktivistas son individuos o grupos que combinan habilidades de hacking con motivaciones políticas, sociales o éticas para llevar a cabo acciones en línea que buscan promover un cambio social o político. El término "hacktivismo" se deriva de la combinación de las palabras "hacking" y "activismo".

Se muestran motivados por una variedad de causas, que pueden incluir la libertad de expresión, la privacidad en línea, la lucha contra la censura, la justicia social, la transparencia gubernamental y muchas otras. Sus acciones en línea suelen estar alineadas con sus creencias y objetivos políticos o sociales.

Utilizan una variedad de técnicas de hacking para lograr sus objetivos, que pueden incluir el desfiguramiento de sitios web, la divulgación de información confidencial, la realización de ataques de denegación de servicio (DDoS) y otras acciones que buscan llamar la atención sobre sus causas.

Los hacktivistas a menudo se comunican públicamente a través de canales en línea, como sitios web, foros, redes sociales y comunicados de prensa, para explicar sus motivaciones y objetivos. También pueden usar el hacktivismo como una forma de llamar la atención de los medios de comunicación y generar discusión pública sobre los temas que les preocupan.

Algunos grupos de hacktivistas notables incluyen Anonymous, WikiLeaks y LulzSec. Estos grupos han llevado a cabo acciones en línea notorias que han tenido un impacto en la política y la seguridad en línea.

El hacktivismo es un campo controvertido, ya que las acciones de los hacktivistas pueden ser vistas como ilegales y éticamente cuestionables por algunos, mientras que otros los consideran defensores de la libertad y la justicia. La percepción de la legitimidad del hacktivismo varía según las circunstancias y las perspectivas individuales.

Los hacktivistas pueden enfrentar consecuencias legales por sus actividades, incluyendo cargos de hacking, robo de datos, vandalismo en línea y otros delitos cibernéticos.

Perfil del ciberdelincuente organizado

El Ciberdelincuente Organizado es un perfil que se destaca en el mundo de la ciberdelincuencia por su participación en grupos delictivos con una estructura organizativa definida y por su enfoque en la obtención de ganancias financieras a través de actividades ilícitas en línea.

En contraste con los actores cibernéticos individuales o amateurs, el Ciberdelincuente Organizado se integra en grupos delictivos

que suelen tener una estructura jerárquica. Estos grupos cuentan con líderes, especialistas en distintas áreas y miembros que desempeñan roles específicos en las operaciones cibernéticas.

La principal motivación que impulsa a estos ciberdelincuentes es el lucro económico. Realizan actividades ilegales en línea con el propósito de obtener beneficios económicos significativos. Esto puede abarcar desde el robo de datos financieros y el fraude en línea hasta el uso de ransomware, la extorsión en línea y la comercialización de información robada en el mercado clandestino.

Los Ciberdelincuentes Organizados emplean una diversidad de tácticas cibernéticas para lograr sus objetivos. Esto incluye la utilización de técnicas de ingeniería social, la creación de malware avanzado, ataques de phishing dirigidos, fuerza bruta en contraseñas y más.

Estos grupos operan con gran discreción y buscan mantener su anonimato. Aplican técnicas destinadas a ocultar sus huellas digitales y evadir la detección por parte de las autoridades y las empresas especializadas en seguridad en línea.

Muchos de estos grupos de Ciberdelincuentes Organizados operan a nivel global y pueden llevar a cabo sus ataques desde diversas ubicaciones dispersas por todo el mundo. Esto les permite sortear las restricciones legales nacionales y dificulta su rastreo y persecución.

Perfil del ciberdelincuente Insider Threat

El "Insider Threat" (Amenaza Interna) representa un perfil de ciberdelincuente particularmente complejo, ya que involucra a empleados o exempleados que poseen acceso privilegiado a sistemas y redes de una organización. Estos individuos cometen actos delictivos desde dentro de la entidad, lo que a menudo los hace difíciles de detectar. Las motivaciones que impulsan a los Insider Threats pueden ser diversas. Algunos pueden cometer actos delictivos por razones financieras, como el robo de datos confidenciales o la venta de información a terceros. Otros pueden tener motivaciones personales, como la venganza contra la organización o los colegas.

La amenaza interna es especialmente desafiante de detectar, ya que estos individuos a menudo evitan llamar la atención. Sus actividades ilícitas pueden parecer legítimas a primera vista, lo que dificulta su identificación hasta que el daño ya está hecho. Los Insider Threats suelen abusar de la confianza que la organización ha depositado en ellos. Esto puede incluir el uso indebido de información sensible, la manipulación de datos o la creación de vulnerabilidades intencionadas.

La prevención y la mitigación de las amenazas internas requieren de estrategias específicas, como la supervisión adecuada de los privilegios de acceso, la implementación de políticas de seguridad sólidas y la formación del personal en la identificación de comportamientos sospechosos.

Perfil del Ciberdelincuente Motivado por Lucro Económico

Los ciberdelincuentes motivados por el lucro económico son individuos o grupos que realizan actividades delictivas en línea con el objetivo principal de obtener ganancias financieras. Estos ciberdelincuentes utilizan una variedad de técnicas y estrategias para llevar a cabo sus actividades ilegales y generar ingresos.

La motivación central de los ciberdelincuentes motivados por el lucro económico es obtener beneficios económicos. Buscan oportunidades para robar dinero, datos financieros o información valiosa que puedan vender en el mercado negro.

Estos ciberdelincuentes pueden participar en actividades como el robo de identidad, donde obtienen información personal y financiera de víctimas para cometer fraudes financieros, como el uso no autorizado de tarjetas de crédito o préstamos fraudulentos.

El ransomware es una táctica común utilizada por ciberdelincuentes motivados por el lucro. Cifran los datos de las víctimas y exigen un rescate a cambio de la clave de descifrado.

Los ciberdelincuentes pueden llevar a cabo estafas en línea, como esquemas de phishing, donde engañan a las personas para que divulguen información confidencial, como contraseñas o números de tarjetas de crédito.

Utilizan una variedad de técnicas y herramientas, como malware, troyanos, virus y botnets, para llevar a cabo sus actividades delictivas en línea. Estas herramientas les permiten infiltrarse en sistemas, robar datos y realizar ataques cibernéticos.

Los ciberdelincuentes motivados por el lucro a menudo venden la información robada en el mercado negro en línea. Este mercado incluye datos personales, información de tarjetas de crédito, credenciales de inicio de sesión y otros activos digitales valiosos.

Estas actividades son ilegales y pueden llevar a consecuencias legales graves si los ciberdelincuentes son identificados y capturados por las autoridades. Las leyes de ciberdelincuencia varían según la jurisdicción, pero a menudo se aplican cargos por robo de identidad, fraude, acceso no autorizado a sistemas y otros delitos relacionados con la ciberseguridad.

Perfil del Ciberdelincuente Vengativo

Los ciberdelincuentes vengativos son individuos o grupos que realizan actividades cibernéticas maliciosas con el objetivo principal de vengarse de una persona, empresa o entidad específica. Estos ciberdelincuentes buscan causar daño, perturbación o perjuicio a sus objetivos, y una de las tácticas más perniciosas y perjudiciales que algunos de estos ciberdelincuentes emplean es la "pornografía de venganza".

La pornografía de venganza implica la difusión no consensuada de material sexualmente explícito que involucra a la víctima, a menudo con la intención de dañar su reputación, intimidad y bienestar emocional. Este material generalmente se comparte en línea a través de sitios web, redes sociales o foros, y a menudo incluye información personal de la víctima, como su nombre completo, dirección o detalles de contacto. Esta práctica, además de ser inmoral y de dudosa legalidad en muchos lugares, puede tener graves consecuencias emocionales y psicológicas para la víctima.

La motivación central de los ciberdelincuentes vengativos es la venganza. Pueden sentirse agraviados por una acción o evento

previo y buscan perjudicar al responsable de alguna manera, ya sea un individuo, una organización o una entidad gubernamental.

Los ciberdelincuentes vengativos a menudo perciben que han sido tratados injustamente o que han sufrido daños o pérdidas debido a las acciones de otra parte. Consideran que sus acciones son una forma de equilibrar la balanza.

Utilizan diversas tácticas y acciones cibernéticas para llevar a cabo su venganza. Estas pueden incluir la divulgación de información confidencial, el robo de datos, el vandalismo en línea, los ataques de denegación de servicio (DDoS) y otros métodos diseñados para causar perjuicio o daño a sus objetivos.

Los objetivos de los ciberdelincuentes vengativos pueden ser diversos. Pueden dirigirse a individuos, empresas, organizaciones o incluso a figuras públicas, dependiendo de su motivo y percepción de la injusticia.

Perfil del Ciberdelincuente Basado en el Ciberterrorismo

Los ciberdelincuentes basados en el ciberterrorismo son individuos o grupos que realizan acciones cibernéticas con la intención de causar terror, pánico, disrupción o daño significativo a nivel político, económico o social. Estos ciberdelincuentes utilizan la tecnología y las tácticas cibernéticas para lograr sus objetivos terroristas.

La motivación central de los ciberterroristas es causar miedo y alarma en la sociedad o en un grupo específico. Buscan sembrar el caos y la inseguridad a través de sus acciones cibernéticas.

Los ciberdelincuentes basados en el ciberterrorismo a menudo tienen motivaciones políticas, ideológicas o religiosas. Sus ataques pueden estar destinados a promover sus creencias o agendas, y a menudo buscan desestabilizar gobiernos u organizaciones.

También pueden estar motivados por el deseo de causar daño económico a través de ataques a infraestructuras críticas, empresas o instituciones financieras.

Utilizan tácticas cibernéticas avanzadas, como ataques de denegación de servicio (DDoS), intrusiones en sistemas críticos, sabotaje cibernético y la propagación de malware, para lograr sus objetivos.

Los objetivos de los ciberterroristas pueden variar ampliamente e incluir instituciones gubernamentales, infraestructuras críticas (como centrales eléctricas o sistemas de agua), empresas, organizaciones religiosas o políticas y cualquier entidad que consideren relevante para sus objetivos.

Las acciones de los ciberterroristas pueden tener consecuencias graves, como apagones eléctricos, pérdida de datos críticos, interrupciones en servicios públicos esenciales, daño económico y, en casos extremos, pérdida de vidas humanas.

La lucha contra el ciberterrorismo a menudo implica la cooperación entre agencias de seguridad y organismos gubernamentales de diferentes países. La colaboración internacional es esencial para abordar amenazas cibernéticas de gran envergadura.

Características comunes y habilidades técnicas

Las características comunes y habilidades técnicas son aspectos distintivos que suelen encontrarse en el perfil de numerosos ciberdelincuentes. Estas particularidades y destrezas les habilitan para llevar a cabo sus acciones ilícitas en línea con una mayor eficacia y un grado más elevado de sofisticación.

Por lo general, poseen un sólido conocimiento en informática y tecnología, que abarca desde la comprensión de sistemas operativos hasta redes, protocolos de Internet y software afín. Además, es común que cuenten con habilidades en programación y desarrollo de software.

Uno de sus principales objetivos es mantener su identidad y ubicación en el anonimato, para lo cual hacen uso de técnicas de ocultamiento. Para ello, recurren a herramientas como redes privadas virtuales (VPN), proxies y servicios de anonimato con el fin de ocultar su dirección IP y dificultar su rastreo.

En ocasiones, algunos ciberdelincuentes pueden adquirir conocimientos en hacking ético y emplear estas habilidades de manera no ética.

La ingeniería social constituye una técnica recurrente utilizada por estos individuos para manipular a las personas y obtener información confidencial o acceso no autorizado a sistemas. Se destacan por ser expertos en el arte de engañar a sus víctimas mediante tácticas psicológicas para alcanzar sus objetivos.

El arsenal de herramientas y software especializados que emplean es diverso e incluye malware como virus, troyanos, ransomware y botnets, entre otros. Estas herramientas les permiten infiltrarse en sistemas, sustraer información o causar daño.

Son altamente adaptables y no escatiman en cambiar sus tácticas y técnicas con el fin de evitar la detección y mantenerse un paso adelante de las medidas de seguridad.

Asiduamente, se encuentran en búsqueda de nuevas vulnerabilidades en el software y sistemas que puedan ser explotadas para obtener acceso no autorizado o causar daño.

Algunos ciberdelincuentes forman parte de comunidades en línea donde comparten conocimientos, herramientas y estrategias. Estas comunidades pueden funcionar como entornos de aprendizaje y colaboración para perfeccionar sus habilidades y técnicas.

Es importante mencionar que no todos los ciberdelincuentes poseen estas características en el mismo grado, y algunos pueden contar con habilidades más especializadas que otros. Además, con la constante evolución de la tecnología y el ciberespacio, las habilidades y tácticas de los ciberdelincuentes se adaptan y evolucionan para hacer frente a nuevas circunstancias y desafíos. También, es relevante destacar que la inteligencia artificial se ha convertido en un aliado que potencia sus ataques y les permite perfeccionar sus técnicas.

Factores que influyen en su elección de objetivos

Los ciberdelincuentes pueden seleccionar sus objetivos en línea basándose en diversos factores que les ofrecen oportunidades

para llevar a cabo sus ataques de manera exitosa o que se ajustan a sus motivaciones específicas.

La ciberdelincuencia es un campo dinámico y diverso, y los factores que influyen en la elección de objetivos pueden variar dependiendo del tipo de delito y de las motivaciones individuales de los ciberdelincuentes.

Algunos de los factores que influyen en su elección de objetivos son:

Valor de la Información: buscan objetivos que alberguen información valiosa, como datos personales, financieros o comerciales. Empresas, organizaciones gubernamentales y sitios web de comercio electrónico suelen ser objetivos atractivos debido a la cantidad de datos confidenciales que manejan.

Vulnerabilidades Técnicas: buscan explotar vulnerabilidades en sistemas y redes para obtener acceso no autorizado. Objetivos con sistemas desactualizados o con falta de medidas de seguridad son más susceptibles a ataques.

Potencial de Lucro: muchos ciberdelincuentes están motivados por beneficios económicos y, por lo tanto, eligen objetivos que les brinden oportunidades para obtener ganancias financieras. Esto puede incluir sitios web de comercio electrónico, bancos en línea o sistemas de pago en línea.

Motivaciones Ideológicas o Políticas: algunos pueden tener motivaciones políticas o ideológicas y seleccionar objetivos que estén relacionados con sus creencias o que consideren representativos de una causa en particular. En estos casos, pueden apuntar a sitios web gubernamentales, corporativos o de organizaciones específicas.

Impacto y Reconocimiento: pueden elegir objetivos que les brinden la posibilidad de causar un impacto significativo o que les otorguen reconocimiento dentro de la comunidad hacker. Ataques a sitios web populares o sistemas críticos pueden aumentar su reputación entre sus pares.

Oportunidades de Extorsión: algunos utilizan ransomware para secuestrar datos o sistemas y luego exigir un rescate para su liberación. Eligen objetivos que puedan pagar el rescate y que tengan información o sistemas críticos que las víctimas necesiten recuperar urgentemente.

Búsqueda de Información Sensible: pueden buscar información específica, como secretos comerciales, propiedad intelectual o datos confidenciales que puedan vender o utilizar para chantajear a la víctima.

Riesgo y Probabilidad de Detección: evalúan el riesgo asociado con sus objetivos y seleccionan aquellos que tienen una probabilidad más baja de ser detectados y rastreados por las autoridades o expertos en ciberseguridad.

Motivaciones de Hacktivismo: los objetivos pueden ser seleccionados con el objetivo de promover una causa o hacer una declaración política. Pueden dirigir sus ataques contra sitios web o sistemas relacionados con instituciones gubernamentales, corporaciones o grupos que consideren en desacuerdo con sus ideologías.

Diferencias y similitudes con otros tipos de delincuentes

Las características y motivaciones de los ciberdelincuentes pueden diferir significativamente de otros tipos de delincuentes que operan en el mundo físico. A continuación, se presentan algunas diferencias y similitudes entre los ciberdelincuentes y otros tipos de delincuentes tradicionales:

Diferencias

Ámbito de Operación: los ciberdelincuentes operan principalmente en el ciberespacio, utilizando tecnologías y redes informáticas para llevar a cabo sus ataques. Por otro lado, los delincuentes tradicionales suelen cometer delitos en el mundo físico, como robos, asaltos o vandalismo.

Identidad y Anonimato: los ciberdelincuentes pueden ocultar su identidad y ubicación mediante técnicas de anonimato en línea, lo que dificulta su rastreo por las autoridades. En contraste, los delincuentes tradicionales están sujetos a ser identificados y arrestados más fácilmente por la policía.

Escala y Alcance: los ciberdelincuentes pueden operar a escala global y llevar a cabo ataques masivos que afectan a un gran número de víctimas en diferentes partes del mundo. Los delincuentes tradicionales, en cambio, tienden a operar localmente y afectar a un número más limitado de víctimas en una ubicación específica.

Naturaleza del Delito: los ciberdelincuentes suelen cometer delitos de forma virtual, como robo de datos, fraude en línea, ataques de ransomware, entre otros. Los delincuentes tradicionales cometen delitos físicos, como robos a mano armada, agresiones, vandalismo, etc.

Habilidades Técnicas: los ciberdelincuentes requieren habilidades técnicas en informática y tecnología para llevar a cabo sus ataques en línea. Los delincuentes tradicionales, por otro lado, pueden depender más de su fuerza física o de tácticas tradicionales para cometer delitos.

Similitudes

Motivaciones Criminales: a pesar de las diferencias en la naturaleza de los delitos, tanto los ciberdelincuentes como los delincuentes tradicionales pueden estar motivados por obtener beneficios económicos, poder, reconocimiento, venganza, entre otras razones.

Adquisición de Beneficios: tanto los ciberdelincuentes como los delincuentes tradicionales buscan obtener beneficios de sus acciones delictivas. Estos beneficios pueden ser económicos, sociales o emocionales.

Búsqueda de Oportunidades: tanto los ciberdelincuentes como los delincuentes tradicionales buscan oportunidades para cometer delitos. Los ciberdelincuentes buscan vulnerabilidades en sistemas y redes, mientras que los delincuentes tradicionales buscan momentos y lugares adecuados para cometer sus acciones.

Riesgo y Probabilidad de Detección: tanto los ciberdelincuentes como los delincuentes tradicionales evalúan el riesgo asociado con sus acciones y seleccionan objetivos y métodos que minimicen la probabilidad de ser detectados y capturados.

A pesar de que existen diferencias importantes entre los ciberdelincuentes y los delincuentes tradicionales, ambos grupos comparten ciertas motivaciones criminales y estrategias para lograr sus objetivos. La ciberdelincuencia es una forma de delito que se ha vuelto cada vez más prominente en la era digital, y su naturaleza en constante evolución presenta desafíos únicos para las autoridades encargadas de hacer cumplir la ley y los expertos en ciberseguridad.

Tendencias y patrones de comportamiento

Las tendencias y patrones de comportamiento en la ciberdelincuencia son dinámicos y cambiantes debido a la evolución constante de la tecnología, las políticas de seguridad y la respuesta de las autoridades. Sin embargo, existen algunas tendencias y patrones generales que han sido observados en el mundo de la ciberdelincuencia en los últimos años:

Aumento del Cibercrimen Financiero: el cibercrimen con motivaciones financieras sigue siendo una de las principales tendencias en la ciberdelincuencia. Los ataques dirigidos a robar datos financieros, realizar fraudes en línea, distribuir ransomware y llevar a cabo estafas continúan en aumento debido a su potencial lucrativo.

Ciberataques a Infraestructuras Críticas: Ha habido un aumento significativo en los ciberataques dirigidos a infraestructuras críticas, como sistemas de energía, transporte, salud y gobierno. Estos ataques pueden tener consecuencias devastadoras para la seguridad nacional y la economía.

Aumento de Ataques de Ransomware: los ataques de ransomware han experimentado un crecimiento considerable. Los ciberdelincuentes utilizan el ransomware para bloquear sistemas y exigir rescates en criptomonedas a cambio de la liberación de datos o sistemas secuestrados.

Uso de Inteligencia Artificial y Automatización: los ciberdelincuentes están empleando cada vez más tecnologías de inteligencia artificial y automatización para llevar a cabo ataques más sofisticados y extensos. La IA puede ser utilizada para identificar vulnerabilidades, automatizar ataques de phishing y adaptar estrategias en función de la respuesta de la víctima. Esto crea un desafío adicional para la seguridad cibernética, ya que las defensas también deben hacer uso de la IA para combatir estas amenazas.

Amenazas de Ingeniería Social La ingeniería social sigue siendo una de las tácticas más efectivas en el arsenal de los ciberdelincuentes. El uso de técnicas de manipulación psicológica para engañar a las personas y obtener acceso a información confidencial o contraseñas sigue siendo una preocupación importante.

Expansión de Internet de las Cosas (IoT): la creciente adopción de dispositivos conectados a Internet, como cámaras, termostatos y electrodomésticos inteligentes, ha abierto nuevas posibilidades para ataques de IoT y la creación de botnets.

Ataques a la Nube: con la migración masiva de datos y servicios a la nube, los ciberdelincuentes también están enfocando sus ataques en plataformas en la nube.

Falsificación de Identidad y Suplantación de Identidad: La suplantación de identidad y el uso de datos personales robados para cometer delitos siguen siendo una amenaza significativa para individuos y organizaciones.

Enfoque en Vulnerabilidades Zero-Day: los ciberdelincuentes están cada vez más interesados en la explotación de vulnerabilidades zero-day, que son fallas de seguridad desconocidas para el fabricante y, por lo tanto, no tienen un parche de seguridad disponible.

Top risks by region

Top 10 risks in Argentina

Source: Allianz Global Corporate & Specialty

Figures represent how often a risk was selected as a percentage of all responses for that country
Respondents: 17. Figures don't add up to 100% as up to three risks could be selected

Rank		Percent	2022 rank	Trend
1	Cyber incidents *(e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties)*	41%	*2 (32%)*	↑
2	Climate change *(e.g. physical, operational and financial risks as a result of global warming)*	24%	*5 (19%)*	↑
2	Energy crisis *(e.g. supply shortage/outage, price fluctuations)*	24%	NEW	↑
2	Fire, explosion	24%	*3 (29%)*	↑
5	Business interruption *(incl. supply chain disruption)*	18%	*1 (58%)*	↓
5	Political risks and violence *(e.g. political instability, war, terrorism, civil commotion, strikes, riots, looting)*	18%	*3 (29%)*	↓
5	Shortage of skilled workforce	18%	NEW	↑
8	Changes in legislation and regulation *(e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration)*	12%	*7 (16%)*	↓
8	Macroeconomic developments *(e.g. inflation, deflation, monetary policies, austerity programs)*	12%	NEW	↑
8	Natural catastrophes *(e.g. storm, flood, earthquake, wildfire, extreme weather events)*	12%	*5 (19%)*	↓

Figura 1. Riesgos en Argentina

https://doi.org/10.62486/net202469

En el informe de riesgo de Allianz donde clasifican las preocupaciones corporativas más importantes, "clasificado por 2712 expertos en gestión de riesgos de un récord de 94 países y territorios", las preocupaciones principales para las empresas a nivel global, por segundo año consecutivo, se centran en los incidentes cibernéticos y las pérdidas de beneficios, ambas representando un 34 % de todas las respuestas.

Entre los principales riesgos de nuestro país se identifican los ciberdelitos como nro. 1 del ranking en dicho informe.

Análisis de casos de ciberataques

El análisis de casos de ciberataques es una parte fundamental para comprender cómo operan los ciberdelincuentes y qué técnicas utilizan para llevar a cabo sus acciones. Estudiar casos reales de ciberataques permite identificar patrones, vulnerabilidades explotadas y posibles medidas de mitigación. A continuación, se presentan algunos ejemplos de casos de ciberataques notorios que han ocurrido en el pasado:

Hackeo a la Dirección Nacional de Migraciones

En septiembre de 2020, la Dirección Nacional de Migraciones (DNM) de Argentina fue objeto de un ciberataque que utilizó un tipo de malware conocido como ransomware Netwalker. Este malware cifró los sistemas de la DNM y exigió un rescate inicialmente de 76 millones de dólares, que posteriormente fue reducido a 2 millones y luego a 4 millones de dólares, solicitando el pago en bitcoins, una criptomoneda que permite transacciones no rastreables. En lugar de ceder a las demandas de los atacantes, la DNM optó por presentar una denuncia ante las autoridades judiciales.

Como resultado del ciberataque, los ciberdelincuentes hicieron públicas una veintena de carpetas robadas en la "Deep Web". A pesar de que algunos de los nombres de archivo sugirieron la posible presencia de información delicada, la DNM negó que la filtración comprometiera la seguridad de la Agencia Federal de Inteligencia (AFI) u otras agencias gubernamentales. La Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) colaboró en las labores de investigación destinadas a identificar a los responsables del ataque.

El incidente suscitó diversas hipótesis, incluyendo la posibilidad de que el ataque estuviera destinado a exponer vulnerabilidades, manipular o dañar datos, o facilitar la comisión de un delito convencional. Además, se especuló sobre la existencia de posibles deficiencias en la seguridad del sistema o la implicación de un empleado desleal en la introducción del ransomware, aunque hasta ese momento no existían pruebas concluyentes en este sentido.

Los archivos sustraídos abarcaban una variedad de información, incluyendo documentos relacionados con embajadas como la de Estados Unidos, México y Rumania, así como datos de Interpol y solicitudes de la AFI. La DNM aseguró que, antes de la filtración, había notificado a las agencias pertinentes acerca de la información que podría divulgarse y que esta no representaba una amenaza para la seguridad de la inteligencia.

Hackeo al Renaper

En octubre de 2021, se produjo una preocupante filtración de datos personales que involucra a ciudadanos argentinos, donde un usuario accedió a la base de datos del Registro Nacional de las Personas (Renaper) y publicó información sensible, incluyendo documentos con fotos y números de trámite. Este individuo afirmó tener en su poder datos de los 45 millones de argentinos. Aunque el Gobierno identificó accesos no autorizados a la base de datos del Renaper desde un usuario del Ministerio de Salud, aún no ha confirmado si se descargó toda la información.

El archivo que contiene estos datos se encuentra en formato "json" y se publicó en un foro online utilizado por ciberdelincuentes para transacciones de información robada. Hasta el momento, ha recibido alrededor de 15 000 visualizaciones. El usuario también demostró que poseía información de documentos de personalidades famosas, como políticos y celebridades, y compartió estos datos en una cuenta de Twitter.

El Gobierno sospecha que el acceso indebido se realizó mediante credenciales de VPN (Virtual Private Network) entre el Renaper y el Ministerio de Salud, lo que llevó a descartar la hipótesis de un hackeo masivo en favor de considerar un acceso no autorizado con fines ilícitos. En respuesta, se bloqueó el acceso desde el Ministerio de Salud a la base de datos del Renaper.

La investigación interna apunta a un número limitado de personas con credenciales de alto nivel de seguridad, aunque no se descarta la posibilidad de un acceso remoto desde fuera del Ministerio de Salud utilizando una IP enmascarada.

El usuario que robó los datos amenazó con publicar más información y ofreció vender toda la base de datos por una suma considerable en bitcoins. Este caso es significativamente más amplio que la filtración a la Dirección Nacional de Migraciones ocurrida el año anterior.

Hackeo a Rapipago

Dos empresas vinculadas a Rapipago, Gire Soluciones y Ducit, sufrieron ataques cibernéticos del tipo "ransomware". Gire Soluciones, dedicada a la gestión de pagos de empresas y dueña de Rapipago, informó que detectaron la activación de un malware el 7 de diciembre de 2022. Este malware afectó principalmente los sistemas utilizados para prestar servicios a entidades financieras y encriptó datos sensibles.

Los atacantes exigieron un rescate para devolver el control de la información secuestrada, una práctica común en este tipo de situaciones. Aunque Gire Soluciones aseguró que no hubo indicios de fuga de datos y que cuentan con métodos de encriptación para resguardar información crítica, el riesgo persiste.

Los expertos en ciberseguridad desaconsejan el pago de rescates, ya que no garantizan la recuperación de los datos y pueden

llevar a pagos adicionales. En cambio, se recomienda restaurar la seguridad de la red vulnerada para prevenir futuros ataques.

Ciberataque a farmacias afecta a millones en Argentina

Un ciberataque informático extorsivo afectó al sistema que valida los descuentos en medicamentos en farmacias de Argentina, dejando a millones de usuarios en una situación complicada. El ataque se dirigió al sistema que maneja las transacciones de prepagas y servicios de validación en línea a través de Farmalink, impactando a más de 20 obras sociales. La empresa responsable, Bizland, reportó que aunque no se comprometieron datos sensibles de los usuarios, la operatividad de su red de comunicaciones resultó afectada, impidiendo la validación en línea de los consumos de salud.

Aunque se esperaba una pronta solución, el sistema no se ha restablecido completamente. Esto ha llevado a que los beneficiarios de programas sociales no puedan recibir los descuentos correspondientes en sus medicamentos. A pesar de que no todas las prepagas y obras sociales se vieron afectadas, algunas de las más grandes en el Área Metropolitana de Buenos Aires experimentan dificultades. La Cámara de Farmacias de Córdoba ha proporcionado instrucciones para garantizar la continuidad del servicio de forma manual hasta que se resuelva la situación.

Bizland logró recuperar el sistema de almacenamiento sin comprometer los datos de los pacientes. En este contexto, los farmacéuticos se ven obligados a registrar las transacciones de forma manual y posteriormente solicitar el reconocimiento de los descuentos a las farmacias por parte de los prestadores de servicios de salud. La magnitud del ciberataque pone de relieve la vulnerabilidad de los sistemas de salud ante las amenazas cibernéticas, y la situación sigue siendo objeto de investigación por parte de las autoridades pertinentes.

Hackeo al INTA

El Instituto Nacional de Tecnología Agropecuaria (INTA) ha sido objeto de un ciberataque significativo que comenzó a fines de abril 2023. Este ataque de ransomware, donde los piratas informáticos bloquearon el acceso a los sistemas del INTA y exigieron un rescate de 2,5 millones de dólares, ha tenido graves repercusiones en las operaciones de la institución.

Las autoridades del INTA tomaron medidas inmediatas para abordar la situación. Se activaron protocolos de seguridad y se formó un equipo de gestión de contingencia en colaboración con expertos en seguridad informática y la Dirección Nacional de Ciberseguridad de la Jefatura de Gabinete de la Nación. Se destaca que este no es el primer ataque de esta naturaleza que enfrenta el INTA; uno similar tuvo lugar en marzo del año anterior, aunque esta vez se ha manifestado de manera más agresiva y ha afectado múltiples servicios.

La gravedad del incidente ha llevado al INTA a tomar la decisión de suspender todos sus servicios informáticos institucionales hasta que la situación esté completamente bajo control y se garantice la seguridad. Esta medida es comprensible, dado que el INTA es una institución compleja que presta servicios a una vasta red de más de 400 puntos en todo el país y a aproximadamente 7000 personas.

El ataque informático al INTA es un reflejo de la creciente amenaza de ciberataques en Argentina y la región. Según informes recientes, Argentina lidera la región en términos de ciberataques, con un promedio de 2 052 ataques semanales. Este incidente destaca la importancia de la ciberseguridad y la necesidad de una mayor colaboración entre los sectores público y privado para abordar eficazmente las amenazas cibernéticas en la actualidad.

Ciberataque a la CNV

En un hackeo a la Comisión Nacional de Valores (CNV), la organización de hackers Medusa robó 500 000 archivos confidenciales que incluyen datos de bancos, empresas y trámites internos. Este robo se realizó a través de una operación de ransomware en la que se secuestraron 1,5 terabytes de datos de la CNV y se solicitó un rescate de $500 000. La información filtrada, que ahora está disponible en la "dark web," contiene expedientes, correos electrónicos, sanciones, multas y detalles de campañas de seguridad informática y se ha compartido a través de mensajes en redes sociales, especialmente Telegram. La CNV había denunciado el ataque y afirmado que había conservado toda su información gracias a medidas de prevención contra ciberataques. La información filtrada incluye bases de datos internas, documentos financieros, denuncias, grabaciones de audiencias y documentos privados de empleados de la CNV. A pesar de la amenaza inicial de vender la información por partes, Medusa finalmente la hizo pública. La CNV presentó una denuncia ante la Unidad Fiscal Especializada en Ciberdelincuencia y aún no ha ampliado la denuncia ni proporcionado más detalles debido a la naturaleza sensible de la investigación.

Estos son solo algunos ejemplos de casos de ciberataques que han tenido un impacto significativo en la seguridad y la privacidad de individuos y organizaciones de nuestro país. El análisis de estos casos, junto con otros incidentes cibernéticos, permite a los expertos en ciberseguridad y a las autoridades comprender las tácticas empleadas por los ciberdelincuentes y desarrollar estrategias para prevenir y mitigar futuros ataques.

Métodos de evasión y elusión de la detección

Indudablemente, los ciberdelincuentes emplean diversas estrategias con el fin de eludir la detección por parte de sistemas de seguridad y herramientas de ciberseguridad. Estas tácticas se despliegan con el propósito de mantener un perfil bajo, prolongar su presencia en sistemas comprometidos y obstaculizar la identificación y atribución de sus ataques. Entre los métodos más recurrentes de evasión y elusión de la detección, destacan:

- Ofuscación de Código: recurren a técnicas de ofuscación con el objetivo de complicar la comprensión del código malicioso por parte de herramientas de detección y análisis. La ofuscación tiene la capacidad de modificar la apariencia y la

estructura del código con el propósito de encubrir su verdadero propósito.

- Polimorfismo y Metamorfismo: estas estrategias conllevan la alteración de la apariencia o el comportamiento del malware en cada instancia de infección, lo que complica su detección y análisis por parte de soluciones de seguridad que se basan en firmas predefinidas.
- Uso de Tecnologías de Anonimato: pueden emplear tecnologías como redes privadas virtuales (VPN), redes de cebolla (como Tor) y servicios de proxy para enmascarar su ubicación y dirección IP, dificultando así su rastreo e identificación.
- Uso de Botnets: los ciberdelincuentes pueden aprovechar redes de bots (botnets) con el propósito de ejecutar ataques distribuidos y dispersar la actividad maliciosa a través de diversos dispositivos y ubicaciones, lo que complica considerablemente su detección.
- Ataques de Zero-Day: los ataques de día cero aprovechan vulnerabilidades previamente desconocidas tanto para los fabricantes como para la comunidad de seguridad. Al hacer uso de estas vulnerabilidades no identificadas previamente, los delincuentes cibernéticos evitan ser detectados por soluciones de seguridad convencionales que carecen de medidas de protección para dichas debilidades.
- Ataques Dirigidos y Spear Phishing: los ataques dirigidos se diseñan de manera personalizada para objetivos específicos, lo que complica su detección por parte de soluciones de seguridad más genéricas. Por otro lado, el spear phishing se focaliza en individuos o empleados concretos dentro de una organización, con el propósito de engañarlos y obtener acceso a sistemas de alta sensibilidad.
- Enmascaramiento de Tráfico: para eludir la inspección de contenido malicioso por parte de soluciones de seguridad, los ciberdelincuentes recurren a técnicas de enmascaramiento de tráfico, como la cifra de las comunicaciones, con el fin de dificultar la detección del contenido nocivo en las transmisiones.
- Uso de Credenciales Robadas: en su estrategia, los ciberdelincuentes pueden hacerse con credenciales robadas, tales como nombres de usuario y contraseñas, con el propósito de acceder a sistemas sin levantar sospechas y sortear las medidas de seguridad.

La continua evolución de las tácticas y técnicas empleadas por los ciberdelincuentes subraya la necesidad imperante de establecer una estrategia de ciberseguridad integral. Dicha estrategia debe abarcar la actualización y parcheo regular de sistemas, la capacitación de los usuarios en prácticas seguras, así como la implementación de herramientas de detección avanzadas y soluciones de seguridad basadas en el comportamiento. Además, es crucial fomentar la colaboración entre la comunidad de seguridad, las organizaciones y las autoridades, dado que esta colaboración resulta esencial para hacer frente a la creciente sofisticación de la ciberdelincuencia.

Uso de técnicas de ingeniería social y manipulación psicológica

El empleo de tácticas de ingeniería social y manipulación psicológica constituye una estrategia frecuente y efectiva utilizada por los ciberdelincuentes con el propósito de obtener información confidencial, acceder de manera no autorizada a sistemas y persuadir a individuos a llevar a cabo acciones que beneficien a los atacantes. Estas tácticas se fundamentan en la explotación de la confianza, la curiosidad, el temor y otros aspectos psicológicos de las personas. Algunos ejemplos de técnicas de ingeniería social comprenden:

- Phishing: los ciberdelincuentes envían correos electrónicos fraudulentos que se hacen pasar por entidades legítimas, como bancos, servicios en línea o empresas conocidas. Estos correos electrónicos suelen contener enlaces maliciosos o adjuntos con malware, y buscan persuadir a los destinatarios para que divulguen información personal o credenciales de inicio de sesión.
- Ingeniería Social en Redes Sociales: Los ciberdelincuentes pueden utilizar información obtenida de perfiles de redes sociales para personalizar sus ataques de phishing o para realizar ataques dirigidos. También pueden crear perfiles falsos para establecer relaciones de confianza con víctimas potenciales.
- Pretexting: los ciberdelincuentes inventan una situación o escenario falso para obtener información de una persona o para hacer que realice ciertas acciones. Pueden hacerse pasar por colegas, proveedores o autoridades para obtener datos confidenciales o acceso a sistemas protegidos.
- Vishing: esta técnica implica la manipulación de personas a través de llamadas telefónicas. Los ciberdelincuentes pueden hacerse pasar por representantes de servicios legítimos para obtener información personal o financiera de las víctimas.
- Spear Phishing: esta forma de phishing está dirigida a individuos específicos o grupos pequeños, lo que lo hace más difícil de detectar por soluciones de seguridad automatizadas. Los correos electrónicos y mensajes de spear phishing se personalizan para parecer legítimos y se adaptan a los intereses y roles de las víctimas.
- Baiting: los ciberdelincuentes dejan dispositivos de almacenamiento infectados, como unidades USB, en lugares donde las víctimas potenciales los encontrarán. La curiosidad lleva a las personas a conectar estos dispositivos a sus computadoras, lo que permite que el malware se propague.
- Quid Pro Quo: los ciberdelincuentes ofrecen algo valioso a cambio de información o acceso. Por ejemplo, pueden ofrecer asistencia técnica o descuentos para obtener credenciales de inicio de sesión.

Estas técnicas de ingeniería social y manipulación psicológica muestran cómo los ciberdelincuentes pueden explotar aspectos humanos para lograr sus objetivos. Es importante que las personas estén conscientes de estas tácticas y se eduquen sobre cómo identificar y evitar ser víctimas de ataques de ingeniería social. La concienciación y la formación en seguridad cibernética son fundamentales para protegerse contra estas amenazas.

Ciberterrorismo y radicalización en línea

El ciberterrorismo y la radicalización en línea son fenómenos preocupantes y estrechamente relacionados que han surgido con la creciente dependencia de la tecnología y las redes sociales en la sociedad actual. Estos dos conceptos tienen un impacto significativo en la seguridad y la estabilidad global y merecen una atención especial, son temas que requieren un enfoque multidisciplinario para abordarlos adecuadamente. Los esfuerzos para combatirlos deben incluir medidas de ciberseguridad para prevenir ataques, así como estrategias para contrarrestar la propaganda y la desinformación que propagan los extremistas en línea. A continuación, se explica cada uno de estos términos:

Ciberterrorismo

En el ámbito del ciberespacio, al igual que con la definición de ciberdelito, no se ha logrado alcanzar un consenso universal en cuanto a la comprensión de los conceptos de terrorismo y ciberterrorismo, esta definición también se encuentra sujeta a diversas interpretaciones.

El término ciberterrorismo ha evolucionado desde un enfoque más amplio, que incluye cualquier actividad terrorista en línea, hasta concepciones más específicas. Estas variaciones en la conceptualización han sido objeto de debate en la comunidad académica y de seguridad. Algunos expertos se refieren a la noción más restringida de ciberterrorismo como "ciberterrorismo puro".

Esta definición más restringida considera el ciberterrorismo como un acto delictivo que se apoya en la tecnología digital y tiene como objetivo fundamental generar temor, intimidar o coaccionar a un Gobierno o a una población específica, con la intención de causar o amenazar con causar daño físico o material, como el sabotaje.

El ciberterrorismo abarca el empleo de la tecnología y el ciberespacio con el propósito de llevar a cabo actos terroristas o respaldar, promover y facilitar actividades de índole terrorista. Los ciberterroristas emplean tácticas cibernéticas que incluyen ataques a sitios web, perturbaciones en servicios en línea, difusión de propaganda terrorista y la infiltración de sistemas informáticos críticos. Su finalidad principal es instigar el temor, el pánico o causar daño a individuos o comunidades.

Características del Ciberterrorismo

El ciberterrorismo se caracteriza por las siguientes facetas:

Utilización de Técnicas Cibernéticas para Difundir Ideología y Propaganda Terrorista: los ciberterroristas aprovechan las herramientas digitales para promover y difundir su ideología y propaganda terrorista, llegando a una audiencia global a través de plataformas en línea.

Ataques a Infraestructuras Críticas: se dirigen hacia infraestructuras vitales, como las redes eléctricas, sistemas financieros o redes de transporte, con el fin de interrumpir sus operaciones y causar daño significativo a la sociedad.

Uso de Medios en Línea para Reclutamiento y Radicalización: las plataformas en línea se utilizan para reclutar nuevos seguidores y radicalizar a individuos, propagando así las creencias extremistas y terroristas.

Coordinación y Planificación en Plataformas en Línea: Los ciberterroristas se valen de medios en línea para coordinar y planificar actividades terroristas, lo que les permite operar de manera más encubierta y organizada.

Radicalización en línea

La radicalización en línea es el proceso mediante el cual individuos adoptan ideas y creencias extremistas o violentas a través de plataformas en línea y redes sociales. Los extremistas emplean las redes sociales y otros espacios virtuales para propagar propaganda, reclutar seguidores y facilitar la radicalización de individuos en diferentes partes del mundo.

Características de la Radicalización en Línea

La radicalización en línea se caracteriza por las siguientes facetas:

Utilización de Propaganda y Mensajes Persuasivos: se recurre a la propagación de propaganda y mensajes persuasivos para atraer y radicalizar a individuos vulnerables, aprovechando la influencia de estos contenidos en línea.

Creación de Cámaras de Eco en Línea: se generan comunidades en línea que refuerzan y validan las creencias extremistas, creando un entorno en el que los individuos radicalizados se sienten respaldados y justificados en sus creencias.

Difusión de Contenido Radical en Plataformas de Redes Sociales: las plataformas de redes sociales se utilizan como medios de difusión para contenido radical y extremista, lo que permite alcanzar una audiencia amplia y diversa.

Uso de Técnicas de Ingeniería Social: los extremistas emplean técnicas de ingeniería social para atraer y reclutar seguidores, manipulando la psicología de los individuos y explotando sus vulnerabilidades.

Vínculos entre ciberdelincuencia y ciberterrorismo

Los vínculos entre la ciberdelincuencia y el ciberterrorismo están en constante evolución debido a la naturaleza dinámica del ciberespacio y las actividades que se realizan en él. Aunque la ciberdelincuencia y el ciberterrorismo tienen objetivos y motivaciones diferentes, existen áreas de superposición y posibles conexiones que requieren una comprensión detallada para abordar de manera efectiva los riesgos y amenazas cibernéticas. Algunos de los vínculos y conexiones entre ambas áreas son:

Uso de Técnicas y Herramientas Similares: tanto los ciberdelincuentes como los ciberterroristas utilizan técnicas similares, como el uso de malware, ataques de phishing, ingeniería social y otras tácticas cibernéticas para lograr sus objetivos. Ambos grupos pueden aprovechar vulnerabilidades en sistemas y redes para obtener acceso no autorizado.

Financiamiento y Recursos: la ciberdelincuencia puede proporcionar fuentes de financiamiento y recursos a los grupos

ciberterroristas. Los ciberdelincuentes pueden realizar actividades ilegales, como robos de datos o extorsión, para obtener fondos que luego pueden ser utilizados para financiar actividades terroristas.

Radicalización y Propagación de Ideas: algunos ciberdelincuentes pueden ser reclutados o radicalizados en línea, lo que los convierte en partidarios o miembros activos de grupos ciberterroristas. Además, la ciberdelincuencia puede ser utilizada para propagar la ideología extremista y la propaganda de grupos terroristas en línea.

Amenazas Híbridas: existe la posibilidad de que grupos terroristas recurran a ciberdelincuentes para llevar a cabo operaciones cibernéticas en su nombre, aprovechando su experiencia técnica y conocimiento en el ciberespacio.

Ciberterrorismo como Medio de Ataque: algunos ciberterroristas pueden utilizar ataques cibernéticos como parte de sus estrategias de terrorismo, apuntando a infraestructuras críticas, sistemas financieros o redes de comunicaciones para causar pánico, interrupción y daño.

Mas allá de que puede haber conexiones entre la ciberdelincuencia y el ciberterrorismo, ambos fenómenos son distintos y deben ser abordados por separado.

Cómo se radicalizan los ciberdelincuentes

La radicalización de ciberdelincuentes es un proceso complejo que puede implicar varios factores y circunstancias. No todos los ciberdelincuentes se radicalizan, y la radicalización puede variar dependiendo de cada individuo y su contexto. Sin embargo, algunos factores comunes que pueden contribuir a la radicalización de ciberdelincuentes incluyen:

Ideología Extremista: algunos ciberdelincuentes pueden ser atraídos hacia ideologías extremistas que promueven la violencia o la subversión. La exposición a discursos y propaganda radical en línea puede influir en su forma de pensar y actuar.

Búsqueda de Reconocimiento y Pertenencia: para algunos ciberdelincuentes, la radicalización puede estar relacionada con la búsqueda de reconocimiento y pertenencia a un grupo o comunidad en línea. El sentimiento de ser parte de algo más grande puede llevarlos a adoptar ideologías extremistas y participar en acciones delictivas para ganar reconocimiento dentro de ese grupo.

Descontento Social o Político: los ciberdelincuentes pueden sentirse descontentos con la sociedad o el sistema político y utilizar la ciberdelincuencia como una forma de expresar su frustración y desafiar el statu quo.

Influencia de Pares: la interacción con otros ciberdelincuentes o extremistas en línea puede desempeñar un papel importante en la radicalización. La influencia de pares puede reforzar y validar creencias extremas y fomentar la participación en actividades delictivas.

Búsqueda de Aventura o Emoción: algunos ciberdelincuentes pueden verse atraídos por la emoción y el desafío de llevar a cabo actividades delictivas en línea. La ciberdelincuencia les proporciona una salida para probar sus habilidades técnicas y sentirse empoderados por el anonimato que ofrece el ciberespacio.

Factores Psicológicos: ciertos ciberdelincuentes pueden tener vulnerabilidades psicológicas que los hacen más susceptibles a la radicalización. La búsqueda de un propósito y una identidad en línea puede satisfacer necesidades emocionales y psicológicas insatisfechas.

La radicalización de ciberdelincuentes no siempre sigue un patrón lineal y puede variar en cada caso. Además, las redes sociales y las plataformas en línea pueden desempeñar un papel crucial en la propagación de ideas extremistas y la radicalización de individuos.

Implicaciones para la seguridad nacional e internacional

Las implicaciones de la radicalización de ciberdelincuentes para la seguridad nacional e internacional son significativas y multifacéticas. La convergencia entre la ciberdelincuencia y el extremismo ideológico plantea desafíos complejos y requiere una respuesta integral y coordinada a nivel global.

Algunas de las implicaciones incluyen:

Amenaza para la Seguridad Cibernética: la radicalización de ciberdelincuentes puede llevar a un aumento en el número y la sofisticación de los ataques cibernéticos. Los ciberterroristas y extremistas pueden utilizar sus habilidades técnicas para llevar a cabo operaciones cibernéticas que tengan como objetivo infraestructuras críticas, redes de comunicaciones y sistemas financieros, lo que representa una amenaza para la seguridad cibernética de los países y organizaciones.

Ataques Híbridos: la combinación de habilidades cibernéticas y motivaciones extremistas puede dar lugar a ataques híbridos, donde los ciberdelincuentes buscan combinar acciones en línea y fuera de línea para maximizar el impacto y la propagación de su mensaje.

Radicalización Transfronteriza: el ciberespacio permite que las ideas extremistas se propaguen más allá de las fronteras nacionales. La radicalización en línea puede cruzar fácilmente las barreras geográficas y llevar a la creación de células terroristas y seguidores en diferentes partes del mundo.

Dificultad en la Atribución: la naturaleza anónima y descentralizada del ciberespacio hace que la atribución de ataques y actividades extremistas sea más desafiante. Identificar a los responsables detrás de las operaciones cibernéticas y las actividades radicales puede requerir una cooperación internacional sólida y la utilización de herramientas de inteligencia avanzadas.

Impacto en la Estabilidad y las Relaciones Internacionales: los ataques cibernéticos y las actividades extremistas en línea pueden tener un impacto significativo en la estabilidad política, social y económica de los países y pueden generar tensiones entre naciones.

Desafío para la Cooperación Internacional: la lucha contra la radicalización de ciberdelincuentes y el ciberterrorismo requiere una cooperación estrecha entre países y organizaciones internacionales. El intercambio de información y la colaboración en la aplicación de la ley y la inteligencia son esenciales para abordar estos desafíos a nivel mundial.

Protección de la Privacidad y Libertad de Expresión: mientras se toman medidas para prevenir la radicalización en línea, es

importante equilibrar la seguridad con la protección de la privacidad y la libertad de expresión en el ciberespacio. Es crucial garantizar que las soluciones adoptadas no restrinjan indebidamente los derechos y libertades de los ciudadanos.

Estrategias de prevención y mitigación

Para hacer frente al ciberdelito, el ciberterrorismo y sus repercusiones en la seguridad nacional e internacional, es imperativo implementar estrategias integrales de prevención y mitigación. Estas estrategias deben abordar tanto los aspectos técnicos como los sociales y educativos.

En este sentido, promover la concienciación y la educación pública acerca de los riesgos relacionados con la radicalización en línea y la ciberdelincuencia adquiere un rol fundamental. Las campañas de sensibilización tienen el potencial de informar a las personas sobre las tácticas empleadas por los extremistas en línea, alentando al mismo tiempo el uso seguro y responsable del ciberespacio.

La colaboración estrecha entre gobiernos y plataformas en línea resulta esencial para abordar la difusión de contenido extremista en Internet. Trabajar en conjunto para identificar y eliminar contenido radicalizado puede contribuir significativamente a prevenir la radicalización y el reclutamiento.

En este contexto, los servicios de inteligencia desempeñan un papel crucial al monitorizar las actividades en línea de posibles ciberdelincuentes y extremistas, detectando indicios de radicalización temprana y de planificación de ataques. Esta vigilancia posibilita una respuesta rápida y proactiva frente a posibles amenazas.

Asimismo, la capacitación de ciudadanos y empleados de organizaciones en seguridad y concienciación sobre el ciberdelito puede prevenir la caída en trampas de ingeniería social y proteger contra ataques en línea.

La cooperación a nivel internacional es fundamental para abordar los retos transnacionales asociados con la radicalización y la ciberdelincuencia. El intercambio de información, la colaboración en la aplicación de la ley y la colaboración en investigaciones son elementos cruciales en la lucha efectiva contra estos problemas.

Para prevenir la radicalización en primer lugar, es esencial abordar las causas subyacentes, como la exclusión social, la discriminación y la desigualdad. Promover la inclusión y brindar oportunidades para todos los ciudadanos puede reducir las vulnerabilidades a la radicalización.

La aplicación de tecnologías avanzadas, como el análisis de datos y la inteligencia artificial, puede ser de gran utilidad para identificar patrones de radicalización en línea y prever posibles amenazas antes de que se materialicen.

Fomentar el diálogo y el debate abierto y constructivo sobre cuestiones políticas y sociales puede ofrecer un medio para abordar el extremismo y la radicalización de manera pacífica y democrática.

Al implementar estrategias de prevención y mitigación, es esencial salvaguardar la privacidad y las libertades civiles de los ciudadanos. Las medidas de seguridad no deben comprometer indebidamente los derechos y las libertades fundamentales.

En última instancia, abordar el cibercrimen y sus consecuencias para la seguridad nacional e internacional exige una respuesta coordinada y multidisciplinaria que involucre a gobiernos, organizaciones, comunidades en línea y ciudadanos. Trabajando en conjunto, es posible construir un ciberespacio seguro y resiliente frente a los desafíos planteados por la ciberdelincuencia y el extremismo en línea.

Fortalecimiento de la ciberseguridad y medidas de protección

El fortalecimiento de la ciberseguridad y la implementación de medidas de protección son aspectos cruciales para mitigar los riesgos asociados a las amenazas cibernéticas en general.

Una práctica esencial es mantener los sistemas operativos, aplicaciones y software actualizados con los últimos parches de seguridad. Esto cierra vulnerabilidades conocidas y evita que los ciberdelincuentes aprovechen brechas de seguridad.

Para resguardar redes y sistemas informáticos, herramientas como firewalls y sistemas de detección de intrusos son fundamentales. Además, los sistemas de prevención de intrusiones tienen la capacidad de bloquear ataques cibernéticos conocidos y desconocidos en tiempo real, impidiendo la infiltración y propagación de malware.

El monitoreo del comportamiento de usuarios y sistemas a través de soluciones de seguridad puede detectar actividades anómalas y potencialmente maliciosas, contribuyendo a prevenir ataques cibernéticos.

La encriptación de datos confidenciales y su almacenamiento seguro son medidas efectivas para evitar la exposición de información sensible en caso de una brecha de seguridad.

La educación sobre las mejores prácticas de seguridad cibernética, incluyendo la identificación de ataques de ingeniería social y el uso seguro de contraseñas, es esencial para prevenir la ciberdelincuencia.

Es igualmente vital contar con un plan de respuesta a incidentes cibernéticos, que permita una acción rápida y coordinada en caso de una violación de seguridad.

Realizar análisis de vulnerabilidades y pruebas de penetración de manera regular puede identificar debilidades en los sistemas y corregirlas antes de que sean explotadas por ciberdelincuentes.

La protección de infraestructuras críticas, como redes eléctricas, sistemas de transporte y servicios de emergencia, es de suma importancia debido a las graves consecuencias que su interrupción podría conllevar.

La colaboración entre organizaciones y gobiernos, junto con el intercambio de información sobre amenazas cibernéticas y tácticas empleadas por los ciberdelincuentes, es esencial para estar mejor preparados y protegerse.

Finalmente, la inversión en ciberseguridad y la implementación de mejores prácticas son inversiones que ayudan a reducir el riesgo y proteger tanto la infraestructura como los datos críticos.

Rol de la educación y concienciación en la prevención de ataques

La promoción de la concienciación y la educación desempeña un papel crucial en la prevención de ataques cibernéticos y la lucha contra el cibercrimen. Una población bien informada y consciente de los riesgos, así como de las mejores prácticas en seguridad cibernética, se convierte en un escudo eficaz contra las amenazas en línea.

A través de programas de formación, las personas pueden aprender a identificar señales de posibles amenazas cibernéticas, como correos electrónicos de phishing, sitios web maliciosos y comportamientos en línea sospechosos.

Estos programas ofrecen valiosas lecciones sobre cómo proteger la información personal y la privacidad en línea, haciendo hincapié en el uso de contraseñas seguras, la autenticación de dos factores y la verificación de la autenticidad de los sitios web antes de compartir información personal.

La educación sobre ingeniería social capacita a las personas para detectar intentos de manipulación y persuasión por parte de ciberdelincuentes que buscan obtener información confidencial o acceso no autorizado.

Asimismo, se destaca la importancia de compartir información responsablemente en las redes sociales y se evita la exposición innecesaria de datos personales que podrían utilizarse en ataques de ingeniería social.

Es esencial que las personas comprendan la importancia de resguardar sus datos personales y entender cómo se utilizan y comparten en línea.

Además, se ofrece formación sobre ciberterrorismo y la radicalización en línea, lo que permite a las personas comprender cómo los extremistas emplean el ciberespacio para difundir sus ideas y atraer seguidores.

La concienciación sobre ciberseguridad desempeña un papel crítico en las organizaciones al fomentar una cultura de seguridad entre los empleados y proteger los datos y activos de la empresa.

Tanto la educación como la concienciación motivan a las personas a informar sobre actividades sospechosas o incidentes de ciberdelincuencia a las autoridades y colaborar con la comunidad en la prevención de ataques.

La promoción de estas medidas debe ser un esfuerzo colaborativo que involucre a gobiernos, instituciones educativas, organizaciones y el sector privado, con el objetivo de crear una sociedad más informada y resiliente ante las amenazas cibernéticas.

Colaboración entre el sector público y privado

La cooperación entre el sector público y privado desempeña un papel fundamental en el enfrentamiento de desafíos relacionados con la ciberseguridad, la prevención de ataques y la lucha contra el cibercrimen. Estos dos ámbitos cuentan con habilidades y recursos complementarios que, cuando se combinan, pueden reforzar de manera significativa la protección cibernética y la capacidad de respuesta ante amenazas.

Esta colaboración facilita el intercambio de información sobre amenazas y vulnerabilidades cibernéticas en tiempo real. Las empresas privadas, al estar al tanto de diversos ataques y tácticas empleadas por ciberdelincuentes, pueden compartir dicha información con agencias gubernamentales para mejorar la inteligencia y la respuesta a incidentes.

En este sentido, el sector público puede aprovechar la experiencia del sector privado en el análisis de inteligencia y la identificación de patrones de ataque, permitiendo la detección de tendencias y amenazas emergentes.

La colaboración en respuesta a incidentes conduce a una coordinación más eficiente. Las empresas privadas pueden notificar con prontitud a las agencias gubernamentales sobre ataques, lo que agiliza una respuesta más efectiva.

Además de esto, la cooperación entre ambos sectores puede ser el catalizador para el establecimiento de prácticas óptimas y estándares de seguridad cibernética que tengan un alcance más amplio, abarcando diferentes sectores y organizaciones.

El sector privado puede también desempeñar un papel activo en la capacitación y educación en seguridad cibernética en la comunidad empresarial, aumentando la conciencia sobre la importancia de la ciberseguridad y la prevención de ataques. Además, puede impulsar la investigación y el desarrollo conjunto de tecnologías y soluciones de ciberseguridad más avanzadas y efectivas.

En el ámbito de la protección de infraestructuras críticas, como redes eléctricas, sistemas financieros y servicios de emergencia, la colaboración entre el sector público y privado es esencial, dado que ambos comparten la responsabilidad de su operación y protección.

Para fomentar esta colaboración, los gobiernos pueden ofrecer incentivos y reconocimientos a las empresas privadas que adopten prácticas de ciberseguridad sólidas y contribuyan activamente a la protección cibernética.

Es imperativo destacar que esta colaboración debe ser un esfuerzo continuo y sostenible que involucre a todas las partes interesadas, desde pequeñas y medianas empresas hasta grandes corporaciones y agencias gubernamentales. El intercambio de información, la coordinación en la respuesta a incidentes y el desarrollo conjunto de soluciones son esenciales para fortalecer la ciberseguridad y proteger de manera efectiva a la sociedad y la infraestructura crítica contra las amenazas cibernéticas y la radicalización de ciberdelincuentes.

CONSIDERACIONES FINALES

Recapitulación de hallazgos

A lo largo de nuestra investigación sobre el análisis del comportamiento criminal del ciberdelincuente, hemos identificado hallazgos significativos que contribuyen a comprender la complejidad de este fenómeno emergente. Estos hallazgos son fundamentales para obtener una comprensión completa de la dinámica de la ciberdelincuencia y su relación con cuestiones de seguridad en un mundo cada vez más digital.[84,85]

Uno de los descubrimientos fundamentales es la creciente convergencia entre la ciberdelincuencia y el ciberterrorismo. La investigación reveló que algunos individuos involucrados en actividades ciberdelictivas pueden ser radicalizados en línea y

posteriormente utilizados por grupos terroristas para llevar a cabo operaciones cibernéticas. Esta conexión plantea nuevos desafíos para la seguridad global y subraya la necesidad de abordar de manera integral estos problemas.[86,87,88]

Los perfiles psicológicos de los ciberdelincuentes son increíblemente diversos. Sus motivaciones abarcan desde la búsqueda de ganancias financieras hasta impulsos ideológicos y el simple deseo de desafiar sistemas y organizaciones. Estos perfiles multifacéticos destacan la necesidad de comprender las diversas motivaciones detrás de los delitos cibernéticos para desarrollar estrategias efectivas de prevención y mitigación. La elección de objetivos por parte de los ciberdelincuentes se basa en una serie de factores complejos. Estos incluyen oportunidades financieras, la notoriedad que obtendrían al atacar a ciertas organizaciones o la satisfacción personal de superar sistemas de seguridad.[89,90,91]

Las motivaciones detrás de los ciberdelincuentes son variadas, abarcando desde la búsqueda de ganancias financieras hasta la promoción de ideologías extremistas o la búsqueda de desafíos técnicos. Estas motivaciones pueden influir en el tipo y la escala de los ataques cibernéticos.[92,93,94]

El uso generalizado de técnicas de ingeniería social es otro hallazgo clave. Los ciberdelincuentes recurren a la manipulación psicológica y a la ingeniería social para engañar a las personas y obtener acceso no autorizado a sistemas o información. Conocer estas tácticas es crucial para protegerse contra tales ataques.[95,96,97,98,99]

Nuestra investigación también destaca la importancia de la colaboración entre el sector público y privado. Este enfoque conjunto es fundamental para fortalecer la ciberseguridad y enfrentar con éxito las amenazas cibernéticas.[100,101,102,103] La colaboración permite el intercambio de información sobre amenazas y tácticas empleadas por los ciberdelincuentes, lo que resulta en una respuesta más efectiva.[104,105,106,107,108]

La educación y la concienciación en ciberseguridad son pilares fundamentales en la lucha contra la ciberdelincuencia.[109,110,111] Empoderar a las personas y organizaciones con conocimientos sólidos sobre cómo identificar y prevenir ataques cibernéticos es esencial. La concienciación se centra en el uso de contraseñas seguras, la autenticación de dos factores y la verificación de la autenticidad de los sitios web antes de compartir información personal.[112,113]

Para prevenir y mitigar ataques cibernéticos, el fortalecimiento de la ciberseguridad es imprescindible. Esto implica mantener sistemas y software actualizados con los últimos parches de seguridad, utilizar herramientas como firewalls y sistemas de detección de intrusos, y aplicar prácticas de encriptación para resguardar datos confidenciales.

Recomendaciones

Los hallazgos de esta investigación generan un conjunto de implicaciones y recomendaciones significativas tanto para la comprensión de la ciberdelincuencia como para la formulación de estrategias efectivas de prevención y mitigación. Estas implicaciones y recomendaciones se desprenden de la exploración de los perfiles de los ciberdelincuentes, sus motivaciones, la convergencia con el ciberterrorismo y las medidas para fortalecer la ciberseguridad.

Los resultados de esta investigación subrayan la importancia de que las políticas de seguridad, tanto a nivel nacional como internacional, deben estar actualizadas y reflejar las amenazas emergentes en el ciberespacio. Se necesita una adaptación constante para abordar las motivaciones cambiantes de los ciberdelincuentes y su capacidad en evolución.

Dada la convergencia identificada entre la ciberdelincuencia y el ciberterrorismo, se recomienda una mayor integración y cooperación entre las agencias encargadas de hacer cumplir la ley, la inteligencia y las instituciones gubernamentales responsables de la ciberseguridad y la lucha contra el terrorismo.

La investigación resalta la necesidad de campañas de educación pública y concienciación para empoderar a individuos y organizaciones a reconocer y responder a las amenazas cibernéticas. La alfabetización digital y la comprensión de las técnicas de ingeniería social son componentes esenciales de tales campañas.

La colaboración activa y continua entre el sector público y privado es esencial para mejorar la ciberseguridad. Se recomienda establecer asociaciones que faciliten el intercambio de información y la respuesta conjunta a incidentes cibernéticos.

Dada la rápida evolución de las tecnologías y las tácticas de los ciberdelincuentes, la investigación continua es fundamental para mantenerse al tanto de las amenazas emergentes. Se insta a la comunidad académica y a las instituciones de investigación a dedicar recursos a la exploración de estos temas.

La investigación subraya la importancia de proteger las infraestructuras críticas, como redes eléctricas y sistemas financieros. Se recomienda una mayor inversión en la ciberseguridad de estas áreas vulnerables.

En el desarrollo de políticas y estrategias de ciberseguridad, se debe garantizar un equilibrio entre la protección contra amenazas cibernéticas y el respeto de las libertades civiles y la privacidad de los ciudadanos.

Implicaciones para la ciberseguridad y el combate a la ciberdelincuencia

El análisis del comportamiento criminal del ciberdelincuente tiene implicaciones importantes para la ciberseguridad y el combate a la ciberdelincuencia. Mediante una combinación de medidas preventivas, colaboración entre diferentes actores, concienciación y desarrollo tecnológico, es posible fortalecer la defensa contra los ataques cibernéticos y proteger la sociedad y la infraestructura crítica contra las amenazas en línea.

La culminación de esta investigación ha revelado una serie de implicaciones significativas que tienen un gran impacto en el ámbito de la ciberseguridad y la lucha contra la ciberdelincuencia. Los hallazgos obtenidos proporcionan valiosas lecciones sobre cómo abordar las amenazas cibernéticas y fortalecer la seguridad en el entorno digital. A continuación, se presentan las implicaciones clave y las recomendaciones derivadas de este análisis:

Los hallazgos resaltan la necesidad de adoptar una perspectiva proactiva en la formulación de estrategias de ciberseguridad. En

lugar de reaccionar ante amenazas cibernéticas una vez que se manifiestan, es imperativo anticipar posibles escenarios y desarrollar estrategias que mitiguen los riesgos antes de que se materialicen.

La lucha efectiva contra la ciberdelincuencia exige un enfoque interdisciplinario que involucre a expertos en ciberseguridad, psicólogos, sociólogos y profesionales de la inteligencia. La comprensión de los perfiles psicológicos de los ciberdelincuentes y sus motivaciones es esencial para anticipar y prevenir sus actividades.

La educación y la concienciación pública sobre la ciberseguridad no deben ser eventos únicos, sino esfuerzos continuos. La capacitación constante y la actualización sobre las últimas amenazas y técnicas son esenciales para mantener a las personas y organizaciones al tanto de las amenazas en constante evolución.

La comprensión del comportamiento criminal del ciberdelincuente puede ayudar a identificar vulnerabilidades y mejorar las estrategias de ciberseguridad. Es crucial invertir en tecnologías y capacidades de defensa avanzadas para proteger sistemas y datos críticos contra ataques cibernéticos.

La colaboración entre el sector público y privado es un pilar fundamental para mejorar la ciberseguridad. La creación de alianzas sólidas y la comunicación fluida permiten compartir información sobre amenazas y tácticas, lo que fortalece la capacidad de respuesta y protección.

La inversión en investigación y desarrollo de tecnologías avanzadas, como la inteligencia artificial y el análisis de datos, es crucial. Estas tecnologías pueden utilizarse para identificar patrones de ciberdelincuencia en línea y prever amenazas antes de que se conviertan en incidentes graves.

La recopilación y el análisis de inteligencia sobre actividades ciberdelictivas pueden proporcionar información valiosa sobre tácticas, técnicas y procedimientos utilizados por los ciberdelincuentes. Esto puede ayudar a anticipar y prevenir futuros ataques.

Los avances en la ciberdelincuencia requieren marcos legales actualizados y sólidos que aborden de manera efectiva los delitos cibernéticos y faciliten la cooperación internacional en la persecución de ciberdelincuentes.

CONCLUSIONES

El análisis del comportamiento criminal del ciberdelincuente es un tema complejo y relevante en el mundo actual, donde la ciberdelincuencia y las amenazas cibernéticas han aumentado significativamente. A través de esta investigación, se ha explorado la intersección entre la ciberdelincuencia y la ciberseguridad, y cómo el estudio del comportamiento criminal de los ciberdelincuentes puede proporcionar información valiosa para prevenir y mitigar ataques en línea.

En el marco teórico, se destacaron conceptos fundamentales relacionados con la ciberdelincuencia y el análisis del comportamiento criminal, incluidas las teorías psicológicas que pueden ayudar a comprender las motivaciones detrás de las acciones delictivas en línea. Se analizaron los perfiles psicológicos de los ciberdelincuentes, sus características comunes y habilidades técnicas, así como los factores que influyen en su elección de objetivos.

Las motivaciones detrás del ciberdelincuente se exploraron en profundidad, desde las financieras hasta las ideológicas, y se destacó la importancia de comprender estos factores para desarrollar estrategias eficaces de prevención y mitigación.

Se discutieron las implicaciones para la seguridad nacional e internacional, donde se puso de relieve la necesidad de una colaboración estrecha entre el sector público y privado para abordar las amenazas cibernéticas y la radicalización de ciberdelincuentes. La educación y la concienciación también fueron identificadas como herramientas cruciales para empoderar a las personas y organizaciones en la protección contra ataques cibernéticos y la prevención.

Finalmente, se resaltó la importancia del fortalecimiento de la ciberseguridad y la implementación de medidas de protección, así como el análisis de casos de ciberataques y el uso de técnicas de ingeniería social y manipulación psicológica por parte de los ciberdelincuentes.

En conclusión, el análisis del comportamiento criminal del ciberdelincuente es un campo de estudio en constante evolución, pero es esencial para entender las motivaciones y tácticas detrás de las acciones delictivas en línea. Con un enfoque multidisciplinario, la colaboración entre diferentes actores y una educación sólida en seguridad cibernética es posible fortalecer la ciberseguridad y proteger a la sociedad contra las amenazas cibernéticas. Solo mediante un esfuerzo conjunto y proactivo podemos hacer frente a estos desafíos y asegurar un ciberespacio más seguro y resistente para todos.

FINANCIACIÓN

Los autores no recibieron financiación para el desarrollo de la presente investigación.

CONFLICTO DE INTERESES

Los autores declaran que no existe conflicto de intereses.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: Cecilia Elizabeth Checchia, Francisco Gabriel Bolzan.
Curación de datos: Cecilia Elizabeth Checchia, Francisco Gabriel Bolzan.
Análisis formal: Cecilia Elizabeth Checchia, Francisco Gabriel Bolzan.
Redacción – borrador original: Cecilia Elizabeth Checchia, Francisco Gabriel Bolzan.
Redacción – revisión y edición: Cecilia Elizabeth Checchia, Francisco Gabriel Bolzan.

REFERENCIAS BIBLIOGRÁFICAS

1. Amenazas Híbridas: Ciberseguridad, Ciberterrorismo y Ciberguerra. Cuadernos de Seguridad. 2022 Jul 28. https://cuadernosdeseguridad.com/2022/07/amenazas-hibridas-ciberseguridad-ciberterrorismo-y-ciberguerra/

2. Allianz Global Corporate & Specialty. Allianz Risk Barometer: Identifying the major business risks for 2023. The most important corporate concerns for the year ahead, ranked by 2,712 risk management experts from a record 94 countries and territories. 2023. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2023.pdf

3. Allianz Global Corporate & Specialty. Allianz Risk Barometer: Identifying the major business risks for 2023. The most important corporate concerns for the year ahead, ranked by 2,712 risk management experts from a record 94 countries and territories. 2023. p. 18. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2023.pdf

4. Ámbito Financiero. Hackeo de la CNV: el grupo hacker difundió información tras no recibir el pago de rescate. 2023. https://www.ambito.com/economia/hackeo-la-cnv-el-grupo-hacker-difundio-informacion-no-recibir-el-pago-rescate-n5757458

5. Barbería M. Ataque de hackers: una empresa vinculada a Rapipago que maneja información sensible sobre pagos online sufrió un secuestro virtual de datos. Infobae. 2022 Dec 13. https://www.infobae.com/economia/2022/12/13/ataque-de-hackers-una-empresa-vinculada-a-rapipago-que-maneja-informacion-sensible-sobre-pagos-online-sufrio-un-secuestro-virtual-de-datos/

6. BBVA. En la mente de un cibercriminal. https://www.bbva.com/es/innovacion/en-la-mente-de-un-cibercriminal/

7. Bertoia L. Los hackers publicaron finalmente la información robada a la Dirección Nacional de Migraciones. Página 12. 2020. https://www.pagina12.com.ar/291148-los-hackers-publicaron-finalmente-la-informacion-robada-a-la

8. Cárdenas MJ. Prevención y defensa ante el ciberterrorismo. Lisa News. 2023 Feb 23. https://www.lisanews.org/ciberseguridad/prevencion-y-defensa-del-ciberterrorismo/

9. Campus Ciberseguridad. Tipos de hackers. 2022. https://www.campusciberseguridad.com/blog/item/133-tipos-de-hackers

10. Cisco Umbrella. Top 10 Cybersecurity Tips. https://umbrella.cisco.com/blog/cisco-umbrella-top-10-cybersecurity-tips

11. Code42. 6 Types of Insider Threats. https://www.code42.com/glossary/types-of-insider-threats/

12. Comisión Económica para América Latina y el Caribe (CEPAL). Medidas de ciberseguridad informática. https://biblioguias.cepal.org/c.php?g=495473&p=4398100

13. ComputerWord. Evolucionan las técnicas de evasión de la ciberseguridad. 2017. https://cso.computerworld.es/cibercrimen/evolucionan-las-tecnicas-de-evasion-de-la-ciberseguridad

14. Consejo de Europa. Convenio sobre la ciberdelincuencia, Budapest. 2001 Nov 23. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

15. Derechodelared.com. Hacktivismo: Ciberactivismo ético. https://www.derechodelared.com/hacktivismo-ciberactivismo-etico/

16. Diccionario de la lengua española. Real Academia Española. https://dle.rae.es/

17. Diez R. Ciberseguridad: así atacan los hackers y estos son los ataques más comunes. La Vanguardia. 2022 Dec 19. https://www.lavanguardia.com/tecnologia/20221219/8529724/asi-atacan-hackers-estos-son-ataques-mas-comunes.html

18. DuraLex Sed Lex. Espionaje industrial: qué es y cómo evitarlo? 2021 Dec 30. https://www.duralexsedlex.eu/espionaje-industrial-que-es-y-como-evitarlo/

19. EducacionIT. Ciberdelincuencia y tipos de ciberdelincuentes. https://www.educacionit.com/temario/ciberdelincuencia-y-tipos-de-ciberdelincuentes

20. El Cronista. Amenazas informáticas: por qué las empresas deben invertir más en ciberseguridad. 2022 Nov 18. https://www.cronista.com/negocios/Amenazas-informaticas-por-que-las-empresas-deben-invertir-mas-en-ciberseguridad-20221118-0002.html

https://doi.org/10.62486/net202469

21. El Economista. Evolución y consecuencias del cibercrimen. 2021 Dec 27. https://www.eleconomista.com.mx/sectorfinanciero/Evolucion-y-consecuencias-del-cibercrimen-20211227-0019.html

22. El Orden Mundial en el Siglo XXI. Qué es el ciberespionaje? 2019 Jul 24. https://elordenmundial.com/que-es-el-ciberespionaje/

23. El País. El ciberespionaje al servicio de la geopolítica. 2020 May 21. https://elpais.com/tecnologia/2020-05-21/el-ciberespionaje-al-servicio-de-la-geopolitica.html

24. El País. Ciberespionaje y 'hackeo' en el conflicto israelí-palestino: el arma silenciosa de las agencias de inteligencia. 2021 May 13. https://elpais.com/internacional/2021-05-13/ciberespionaje-y-hackeo-en-el-conflicto-israeli-palestino-el-arma-silenciosa-de-las-agencias-de-inteligencia.html

25. El País. Ciberataque al Registro Nacional de Trabajadores Rurales y Empleadores. 2022 Dec 29. https://elpais.com.ar/ciberataque-al-registro-nacional-de-trabajadores-rurales-y-empleadores-n1667638

26. El Poder de la Palabra (E.P.D.L.P.). Definición de "ciberespionaje". https://www.epdlp.com/definicion.php?pal=ciberespionaje

27. El Español. Ciberterrorismo: el arma de destrucción masiva que se activa con un clic. 2020 Jul 22. https://www.elespanol.com/omicrono/tecnologia/20200722/ciberterrorismo-arma-destruccion-masiva-activa-clic/507348746_0.html

28. Europol. EU Cybersecurity Challenge. https://www.europol.europa.eu/activities-services-main/activities/eu-cybersecurity-challenge

29. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2020. 2020. https://www.europol.europa.eu/activities-services-main/reports/internet-organised-crime-threat-assessment-iocta-2020

30. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2021. 2021. https://www.europol.europa.eu/activities-services-main/reports/internet-organised-crime-threat-assessment-iocta-2021

31. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2022. 2022. https://www.europol.europa.eu/activities-services-main/reports/internet-organised-crime-threat-assessment-iocta-2022

32. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023. 2023. https://www.europol.europa.eu/activities-services-main/reports/internet-organised-crime-threat-assessment-iocta-2023

33. Fernández M. Evolución del cibercrimen: desde los primeros virus hasta el ransomware. 2021 Aug 10. https://www.abc.es/tecnologia/informatica/soluciones/abci-evolucion-cibercrimen-primeros-virus-hasta-ransomware-202108100124_noticia.html

34. Ferré J. Auge y caída de los grupos de ciberactivistas. 2019 Aug 16. https://retina.elpais.com/retina/2019/08/16/tendencias/1565966729_585119.html

35. Fuentes I. Amenazas informáticas: un análisis de los riesgos más graves para la ciberseguridad. OpenAI. 2022 Jan 25. https://openai.com/research/amenazas-informaticas-riesgos-ciberseguridad

36. García F. Guerra cibernética: el nuevo campo de batalla. 2017 Sep 14. https://www.dw.com/es/guerra-cibern%C3%A9tica-el-nuevo-campo-de-batalla/a-40501843

37. García JA. Hacktivismo: el ciberactivismo en la red. 2022 Jan 18. https://www.muycomputer.com/2022/01/18/hacktivismo-ciberactivismo/

38. García JJ. Hacktivismo: una forma de activismo digital. 2022 May 23. https://www.huffingtonpost.es/jorge-jimenez-garcia/hacktivismo-una-forma-de-activismo-digital_b_19740188.html

39. Garriga L. La ciberseguridad en la empresa: una necesidad imprescindible. 2019 Jul 29. https://www.abc.es/espana/comunidad-valenciana/abci-ciberseguridad-empresa-necesidad-imprescindible-201907290217_noticia.html

40. Gestión. Los principales ciberataques que afectaron a empresas y gobiernos en 2022. 2022 Jun 9. https://gestion.pe/mundo/los-principales-ciberataques-que-afectaron-a-empresas-y-gobiernos-en-2022-noticia/

41. Global Guardian. Understanding the Differences Between Hacktivism and Cyberterrorism. 2022 Jan 21. https://www.globalguardian.com/blog/understanding-the-differences-between-hacktivism-and-cyberterrorism

42. Goiburu M. Ciberespionaje: cómo funcionan los ataques de espionaje a través de Internet. 2017 Jul 13. https://www.elconfidencial.com/tecnologia/2017-07-13/ciberespionaje-hackers-espionaje-internet_1417513/

43. González G. Qué es el hacktivismo: cómo influye en la sociedad. 2020 Oct 21. https://somoslibros.net/que-es-el-hacktivismo/

44. Gómez M. Ciberterrorismo: el nuevo peligro en el ciberespacio. 2022 Jan 21. https://okdiario.com/tecnologia/ciberterrorismo-nuevo-peligro-ciberespacio-11383616

45. Grupo de Delitos Telemáticos de la Guardia Civil. Cyber Terrorism. https://www.gdt.guardiacivil.es/webgdt/pinformatica/terrorismo_cibernetico/index.html

46. Hidalgo H. Ciberdelincuencia: qué es, tipos, consecuencias y prevención. 2019 Mar 6. https://concepto.de/ciberdelincuencia/

47. Inkrypt. Hacktivismo y la ciberseguridad. https://inkrypt.co/blog/hacktivismo-y-la-ciberseguridad/

48. Insight. Evolución del cibercrimen: desde los primeros virus hasta el ransomware. 2021 May 13. https://www.insight.com/es_ES/content-and-resources/2021/08/evolucion-del-cibercrimen.html

49. Insight. Tipos de ciberataques y cómo protegerse de ellos. 2022 Sep 28. https://www.insight.com/es_ES/content-and-resources/2022/09/tipos-de-ciberataques.html

50. Inteco-Cert. Tipos de ciberdelincuentes. https://www.incibe-cert.es/faqs/incibe-cert/tipos-ciberdelincuentes

51. Internet Society. Qué es el hacktivismo? https://www.internetsociety.org/issues/internet-censorship/hacktivism/

52. Internet Society. Understanding the Modern Hacktivist: Money, Mayhem, or Mischief? 2020 Nov 10. https://www.internetsociety.org/blog/2020/11/understanding-the-modern-hacktivist-money-mayhem-or-mischief/

53. Kaspersky. La historia de los ciberataques: desde los gusanos hasta el ransomware. https://www.kaspersky.com.mx/resource-center/threats/history-of-cyber-attacks

54. Kaspersky. Cibercrimen: concepto, historia, tipos y prevención. 2021 Dec 21. https://www.kaspersky.com.mx/resource-center/threats/what-is-cybercrime

55. Kaspersky. Hacktivismo: concepto, historia, ejemplos y riesgos. 2022 Sep 20. https://www.kaspersky.com.mx/resource-center/threats/what-is-hacktivism

56. La Tercera. Espionaje industrial, la amenaza que acecha a las empresas. 2018 May 30. https://www.latercera.com/pulso/noticia/espionaje-industrial-la-amenaza-que-acecha-a-las-empresas/171475/

57. Larsson L. Cyberspace, Hacktivism, and Civil Disobedience. Science and Engineering Ethics. 2017;23(3):781-797. https://link.springer.com/article/10.1007/s11948-015-9710-6

58. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, núm. 294. 2018 Dec 6. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

59. Mauri L. Ciberseguridad y ciberdelincuencia: retos y desafíos en la era digital. ESADEgeo. 2021 Nov 23. https://www.esadegeo.com/es/ciberseguridad-y-ciberdelincuencia-retos-y-desafios-en-la-era-digital

60. Mauri L. La lucha contra la ciberdelincuencia. ESADEgeo. 2022 Jan 6. https://www.esadegeo.com/es/la-lucha-contra-la-ciberdelincuencia

61. Merkow MS, Breithaupt J. Computer Security Assurance. Journal of Information Systems. 2006;20(2):85–101. https://doi.org/10.2308/jis.2006.20.2.85

62. Ministerio de Asuntos Económicos y Transformación Digital. **¿Qué es el** ciberespionaje? https://www.mineco.gob.es/stfls/MICM/Menu/Areasdetrabajo/Ciberseguridad/Ciberespionaje.pdf

63. Molina C. La ciberseguridad en España: retos y amenazas. 2019 Nov 7. https://www.eleconomista.es/investigacion-eleconomista/noticias/10148209/11/19/La-ciberseguridad-en-Espana-retos-y-amenazas.html

64. Molina C. Ransomware: qué es, cómo actúa y cómo protegerse de él. 2020. https://www.eleconomista.es/tecnologia/noticias/10524413/05/20/Ransomware-que-es-como-actua-y-como-protegerse-de-el.html

65. Molina C. Phishing: qué es y cómo evitar caer en sus redes. 2021 Jun 7. https://www.eleconomista.es/tecnologia/noticias/11269536/06/21/Phishing-que-es-y-como-evitar-caer-en-sus-redes.html

66. Molina C. DDoS: el ataque que tumba los servicios digitales. 2022 Aug 23. https://www.eleconomista.es/tecnologia/noticias/11552270/08/22/DDoS-el-ataque-que-tumba-los-servicios-digitales.html

67. Molina C. Qué es el malware y cómo protegerse de él. 2022 Sep 28. https://www.eleconomista.es/tecnologia/noticias/11815666/09/22/Que-es-el-malware-y-como-protegerse-de-el.html

68. Molina C. Vulnerabilidades de seguridad: qué son y cómo protegerse de ellas. 2022 Oct 18. https://www.eleconomista.es/tecnologia/noticias/11916273/10/22/Vulnerabilidades-de-seguridad-que-son-y-como-protegerse-de-ellas.html

69. Myers MD. Qualitative research in business and management. Sage; 2013.

70. Naciones Unidas. Resolución 75/273 de la Asamblea General. 2021. https://undocs.org/A/RES/75/273

71. Nations Encyclopedia. Cybercrime. https://www.nationsencyclopedia.com/WorldStats/Crime-Statistics-Cybercrime.html

72. Núñez E. Qué es un hacker y cuántos tipos de hackers existen? 2020 Dec 21. https://www.muycomputer.com/2013/12/12/hacker/

73. OCDE. Informe sobre la ciberdelincuencia. 2020. https://www.oecd.org/internet/Informe-sobre-la-ciberdelincuencia.pdf

74. Paredes G. Ciberdelincuencia y ciberseguridad: diferencias y cómo prevenir ataques. 2022 Jan 5. https://www.genbeta.com/seguridad/ciberdelincuencia-ciberseguridad-diferencias-como-prevenir-ataques

75. PC Magazine. Qué es un ataque DDoS (Distributed Denial-of-Service)? https://www.pcmag.com/es/que-es/ataque-ddos-distributed-denial-of-service

76. Pew Research Center. The State of Privacy in America. 2017 Jan 26. https://www.pewresearch.org/internet/2017/01/26/the-state-of-privacy-in-america/

77. Pittaluga F. Ciberdelincuencia y ciberseguridad: diferencias y cómo prevenir ataques. 2022 Jan 5. https://www.genbeta.com/seguridad/ciberdelincuencia-ciberseguridad-diferencias-como-prevenir-ataques

78. Poza JJ. Qué es el ransomware, cómo funciona y cómo evitarlo? ABC. 2020 Jan 21. https://www.abc.es/tecnologia/informatica/soluciones/abci-ransomware-como-funciona-y-como-evitarlo-202001211226_noticia.html

79. Rex D. Cibercrimen y ciberdelincuencia: concepto, tipos y ejemplos. 2019 Dec 8. https://concepto.de/cibercrimen/

80. Rodríguez M. Ciberseguridad y ciberdelincuencia: retos y desafíos en la era digital. ESADEgeo. 2021 May 3. https://www.esadegeo.com/es/ciberseguridad-y-ciberdelincuencia-retos-y-desafios-en-la-era-digital

81. Sabadell B. Principales riesgos de seguridad informática para empresas y cómo prevenirlos. 2023. https://www.bancsabadell.com/cs/Satellite/SabAtl/Principales-riesgos-de-seguridad-informatica-para-empresas-y-como-prevenirlos/6000048086006/es/

82. Secretaría de Estado de Seguridad. Ciberterrorismo. https://www.interior.gob.es/web/servicios-al-ciudadano/ciberterrorismo

83. Security Art Work. Ciberterrorismo. 2019. https://www.securityartwork.es/2019/01/17/ciberterrorismo/

84. SegurInfo. Ciberseguridad. https://www.segurinfo.com/index.php/es/

85. Serrano A. Amenazas en la red: tipos de malware y cómo combatirlos. El País. 2018 Sep 13. https://elpais.com/tecnologia/2018/09/12/actualidad/1536772189_270775.html

86. Smith KW, Rogers MK. The Impact of Terrorism on the Global Economy: Statistical Evidence. Studies in Conflict & Terrorism. 2018;41(3):158–175. https://www.tandfonline.com/doi/full/10.1080/1057610X.2016.1264599

87. Solución Individual. Qué es la ciberdelincuencia y cómo protegerse de ella? https://www.solucionindividual.com/ciberdelincuencia/

88. Suárez-Tangil G, Egele M, Brumley D. Cc: identifying content-foraging malware. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. 2015. p. 226–246. https://link.springer.com/chapter/10.1007/978-3-319-20550-2_11

89. Tange A. Writing a doctoral thesis using LATEX: Tips, tricks and a template. Studies in Computational Intelligence. 2013;519:19–44. https://link.springer.com/chapter/10.1007/978-3-642-14058-7_2

90. Techopedia. Hacktivism. https://www.techopedia.com/definition/6522/hacktivism

91. Torres JA. Ciberespionaje: técnicas y tácticas utilizadas por los ciberespías. 2022 Aug 15. https://www.muyseguridad.net/2012/08/15/ciberespionaje-tecnicas-tacticas-utilizadas-ciberespia/

92. Unidad de Investigación Tecnológica. Ciberterrorismo. https://www.policia.es/ujit/ciberterrorismo.html

93. UNODC. Comprehensive Study on Cybercrime. 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

94. U.S. Department of Justice. National Strategy for Countering Domestic Terrorism. 2022. https://www.justice.gov/ag/page/file/1495171/download

95. U.S. Department of State. Country Reports on Terrorism 2018. 2019 Apr 25. https://www.state.gov/wp-content/uploads/2019/04/2018-Country-Reports-on-Terrorism-Full-Report.pdf

96. U.S. Department of State. Country Reports on Terrorism 2020. 2021 Apr 20. https://www.state.gov/wp-content/uploads/2021/04/Country-Reports-on-Terrorism-2020.pdf

97. U.S. Department of State. Country Reports on Terrorism 2021. 2022 Mar 31. https://www.state.gov/wp-content/uploads/2022/03/Country-Reports-on-Terrorism-2021-FINAL-2022.03.31.pdf

98. Valdés A. Ciberterrorismo: una amenaza en aumento. 2022 Jan 6. https://www.tekcrispy.com/2022/01/06/ciberterrorismo-amenaza-aumento/

99. Vila A. Qué es el ransomware? Claves, tipos y cómo protegerse. Xataka. 2019 Dec 16. https://www.xataka.com/basics/que-es-ransomware-claves-tipos-como-protegerse

100. Vila A. Phishing: cómo funciona, cómo protegerse y a quién recurrir si has sido víctima. Xataka. 2021 Jun 23. https://www.xataka.com/basics/phishing-como-funciona-como-protegerse-a-quien-recurrir-si-has-sido-victima

101. Vila A. Cibercrimen: qué es, cómo funciona y cómo protegerse. Xataka. 2022 Feb 16. https://www.xataka.com/basics/cibercrimen-que-es-como-funciona-como-protegerse

102. Vila A. DDoS: qué es un ataque de denegación de servicio y cómo protegerse. Xataka. 2022 Mar 28. https://www.xataka.com/basics/ddos-que-es-ataque-denegacion-servicio-como-protegerse

103. Vila A. Malware: qué es, cómo funciona y cómo protegerse de los distintos tipos. Xataka. 2022 May 16. https://www.xataka.com/basics/malware-que-es-como-funciona-como-protegerse-diferentes-tipos

104. Vila A. Vulnerabilidades: qué son, cómo se explotan y cómo protegerse. Xataka. 2022 Jun 29. https://www.xataka.com/basics/vulnerabilidades-que-son-como-se-explotan-como-protegerse

105. Walker G, Akdeniz Y. Cybercrime and the Law: Challenges, Issues, and Outcomes. In: Adimola MI, Ismaila O, Adekunle O, Oluwasegun T, editors. A Reader on Cybercrime and Information Security. African Books Collective; 2014. p. 1–36.

106. Wall DS. The Role of Policing in Cyberspace. Policing & Society. 2001;11(1):55–73. https://www.tandfonline.com/doi/

full/10.1080/10439460120050192

107. Ward D. The State of Cybersecurity in the Wake of the SolarWinds Attack. OpenAI. 2021 Nov 24. https://openai.com/research/cybersecurity-solarwinds

108. Weimann G. Terrorist Migration to the Cloud. Studies in Conflict & Terrorism. 2016;39(4):347–356. https://www.tandfonline.com/doi/full/10.1080/1057610X.2015.1120099

109. Zerdoumi D, Kechadi MT, Crosbie M. An Empirical Study of the Classification of Malware Families. International Journal of Electronic Security and Digital Forensics. 2009;2(4):334–349. https://www.inderscienceonline.com/doi/abs/10.1504/IJESDF.2009.032716

110. Zheng Y, Zhuang W, Shao J. Comprehensive Model for Cyberterrorism Preparedness. Information Systems Frontiers. 2012;14(4):905–920. https://link.springer.com/article/10.1007/s10796-011-9335-0

111. Zhuang W, Zheng Y. A Framework for Cyberterrorism Preparedness. Information Systems Frontiers. 2011;13(4):483–496. https://link.springer.com/article/10.1007/s10796-011-9261-1

112. Zimmermann P, Haas S, Düring M. Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking. Digital Investigation. 2014;11(1):S1–S10. https://www.sciencedirect.com/science/article/abs/pii/S1742287614000623

113. Zittrain J. Introduction: Exploring Anti-Circumvention. Berkeley Technology Law Journal. 2014;29(2):1229–1234. https://www.jstor.org/stable/24117960