Visualizar principales características y métodos de la delincuencia informática, a partir de la lucha mundial contra el COVID-19

To visualize the main characteristics and methods of computer crime, based on the global fight against COVID-19

Henry Gutiérrez-Oquendo

Universidad Nacional Abierta y a Distancia

Recibido: 20/10/2022 Aprobado 22/12/2022

Resumen

Mediante el objetivo planteado: visualizar las principales características y métodos de la delincuencia informática, a partir de la lucha mundial contra el COVID-19, se pretende demostrar en esta investigación, que, a mayor implementación de tecnologías en los hogares, empresas o sectores comerciales, mayores oportunidades para el cibercrimen. Es importante resaltar, que recopilamos información en sitios web reconocidos de entidades públicas y privadas que se dedican a datar sobre la trasformación digital, implementación de las tecnologías, índice de conectividad, destrezas y habilidades del usuario a la hora de navegar por el ciberespacio; por otra parte, documentan sobre los ciberataques más eficaces y continuos en los últimos años, y sus principales sectores de interés. Por último, nos centramos en predecir el grado de verdad de la hipótesis, utilizando una metodología experimental a partir de lo ya descrito y explicado; por lo cual, por medio de análisis estadístico, presentamos claramente el objeto de estudio y técnicas visualizadas en el proceso de investigación, además de centrar la discusión en las coincidencias de los resultados y proyectar los trabajos futuros enfocados en la comisión de delitos informáticos; más específicamente, delincuencia o criminalidad informáticas, donde las TIC son el medio por el cual se lanzan vectores de ataque.

Palabras clave: características y métodos de la delincuencia informática, cibercrimen, ciberespacio, ciberataques, delincuencia o criminalidad informática, vectores de ataque.

Abstract

By means of the proposed objective; to visualize the main characteristics and methods of computer crime, based on the global fight against COVID-19, we intend to demonstrate in this research, that the greater the implementation of technologies in homes, companies or commercial sectors, the greater the opportunities for cybercrime. It is important

Citación: Gutiérrez Oquendo, H. (2023). Visualizar principales características y métodos de la delincuencia informática, a partir de la lucha mundial contra el COVID-19. Publicaciones E Investigación, 17(1). https://doi.org/10.22490/25394088.5968

Bafim1420@gmail.com - https://orcid.org/000-0002-8300-2014

https://doi.10.22490/25394088.5968

to highlight that we collected information from recognized websites of public and private entities that are dedicated to data on digital transformation; implementation of technologies; connectivity index; user skills and abilities when navigating cyberspace; on the other hand, they document the most effective and continuous cyber-attacks in recent years, and their main sectors of interest. Finally, we focus on predicting the degree of truth of the hypothesis, using an experimental methodology from what has already been described and explained; therefore, by means of statistical analysis we clearly present the object of study and techniques visualized in the research process; besides focusing the discussion on the justification objectively in the coincidences of the results and project them to future works focused on the commission of computer crimes; more specifically, computer crime or delinquency, where ICT are the means by which attack vectors are launched.

Key words: *Characteristics and methods of computer crime, cybercrime, cyberspace, cyberattacks, computer crime, attack vectors.*

1. Introducción

Los gobiernos nacionales e internacionales, vienen abordando la ciberdelincuencia y fenómenos relacionados, a través de una reforma legislativa, de reorganización e implementación de distintos protocolos de seguridad. Es el caso del Convenio sobre la Ciberseguridad, también conocida como el Convenio de Budapest, (Consejo de Europa, 2001), el cual es un tratado internacional vinculante que otorga un marco para la adopción de medidas legislativas, con una clara vocación de universalidad, no solo para países pertenecientes al Consejo de Europa, sino también a otros, (Council of Europe, 2022); y la Decisión del Marco 2005/222/JAI, (Consejo de la Unión Europea, 2005)), relativa a los ataques contra sistemas informáticos.

Toda esta lucha, se ha visto afectada con la pandemia mundial y lucha contra el COVID-19, la tecnología pasó de ser un elemento necesario a convertirse en obligatorio, como lo indica el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), (Gobierno de España, 2020).. En consecuencia, es habitual hablar de cibersociedad, cibercomercio, cibereducación, ciberadministración, ciberelaciones y ante todo ciberdelincuencia, que sin lugar a duda repercute en las actividades humanas que tiene un reflejo en el ciberentorno.

Por otra parte, se hace imperante contar con peritos especialistas en delitos informáticos y una reforma legislativa del código penal que aborde la amplísima gama de conductas criminales en los referentes a la criminalidad informática. Concretamente, durante los años de pandemia, se registró un crecimiento en la implementación de las tecnologías en las empresas; conectividad; habilidades mínimas y avanzadas del usuario para navegar por el ciberespacio, como lo documenta el (DESI, 2021); y las ciberamenazas y tendencias de la ciberdelincuencia, documentadas por CCN-CERT IA-23/21, (Gobierno de España, 2021).

En suma y con los antecedentes descritos, se pretende demostrar que, a mayor implementación de tecnologías en los hogares, empresas o sectores comerciales, mayores oportunidades para el cibercrimen; de lo cual, planteamos el problema mediante el análisis de las bases de datos obtenidas en la recolección de información, visualizamos las principales características y métodos de la ciberdelincuencia a partir de la contingencia mundial, para sintetizar todo este enfoque en tablas y gráficos, que afirmen o refuten el propósito de nuestra verdad.

2. Método

2.1 Transformación digital

El 20 de marzo de 2020, se marcó un antes y un después; la Organización Mundial de la Salud (OMS), declara una lucha mundial contra el COVID-19. Esta lucha trajo consigo la trasformación digital que hizo que nuestra "normalidad", sea un constante movimiento por el ciberespacio, tanto en la vida personal como en la profesional.

Sustentando lo dicho, el informe elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI); asegura que 8 de cada 10 hogares disponen de ordenadores, frente a 4 de cada 10, en países en vías de desarrollo, (Gobierno de España, 2020, p. 11); por otra parte, el Índice de Economía y Sociedad Digitales (DESI), facilita bases de datos con unidad de medida de ponderación (0 a 100), sobre el desempeño digital de Europa, (DESI, 2021).

En consecuencia, el confinamiento, permitió que las empresas e instituciones integraran la tecnología digital, para que su personal pudiese trabajar a distancia y sus servicios permanecieran operativos. La Tabla 1, muestran datos que dan fe de la intensidad digital en países de Europa en el año 2021, así mismo la ponderación del desglose de las tecnologías digitales en las empresas y el comercio electrónico en esos mismos países, (DESI, 2021, párr. 8).

Tabla 1.
Implementación de las tenologias en las empresas

País	Intensidad digital	Tecnologías digitales para empresas	Comercio electrónico
Finlandia	12,5201	41,0983	5,87567
Dinamarca	12,6845	36,4486	8,79402
Suecia	11,3322	37,6093	7,39381
Malta	9,22556	36,0332	5,58569
Países Bajos	10,0151	34,2841	6,39914
Bélgica	10,0023	31,9659	7,80593
Irlanda	8,19136	28,9228	10,9065
Eslovenia	8,50012	27,8901	5,92951
Estonia	9,72902	26,3608	5,37286
Italia	8,71114	28,9145	3,82192
Austria	7,69352	26,9476	6,66249
Lituania	5,70444	27,9123	7,5928
Croacia	7,42908	25,3785	7,16162
Luxemburgo	7,8881	28,47	3,06549
Chequia	6,86908	23,5336	8,66975
España	7,47236	25,9096	5,36879
Unión Europea	7,03112	25,3338	5,20364
Portugal	5,14718	25,6211	5,8059
Alemania	7,43468	22,8303	5,28473
Francia	5,97026	24,4557	4,3407
Chipre	4,87646	21,7002	3,96234
Eslovaquia	5,43728	19,0381	4,61636
Grecia	3,75435	22,3362	2,43473
letonia	3,38078	19,9084	3,51005
Polonia	5,30502	16,8844	3,68685
Rumania	1,52224	18,0951	4,14207
Hungría	4,12792	15,4081	3,76351
Bulgaria	1,51826	17,0558	1,90991

Nota. Datos extraídos de DESI (2021).

Este nuevo escenario, insto rápidamente el incremento para establecer una mejor conectividad y migración masiva a infraestructuras en la nube. La Tabla 2, resume, los países de Europa que demandaron más conectividad, (DESI, 2021a, párr. 7).

Tabla 2.
Datos de conectividad, países de Europa

País	Conectividad
Dinamarca	10,0868
Países Bajos	10,0538
España	10,8012
Luxemburgo	11,0836
Suecia	11,8443
Alemania	9,42512
Irlanda	7,91001
Malta	9,77871
Eslovenia	7,40247
Rumania	7,12351
Austria	4,87661
Hungría	12,0795
Finlandia	3,52097
letonia	5,19057
unión Europea	7,55956
Portugal	10,2824
Bélgica	10,2961
Francia	7,8708
Estonia	7,0298
Eslovaquia	6,7886
Croacia	4,56732
Polonia	6,19958
Chequia	7,54568
Italia	4,76134
Chipre	7,27223
Lituania	5,05964
Bulgaria	2,88067
Grecia	4,79167

Nota. Datos extraídos de (DESI, 2021).

Lo anterior, presume una facilidad para que los ciberatacantes se aprovecharan del aumento de las vulnerabilidades de seguridad para sus actos delictivos utilizando medios informáticos; la Tabla 3, evidencia los ataques pasivos y activos que alteran los principales servicios de seguridad demandados, como son la confidencialidad, integridad, autenticación, control de acceso, el no repudio y la disponibilidad de la información. Importante resaltar que estos ataques son muy difíciles de destectar, ya que los pasivos no producen alteración.

Tabla 3.
Ataques activos y pasivos

Activos	Pasivos
Suplantación de identidad	Obtención de contenido de mensaje
Modificación de mensajes	
Repetición	Análisis de tráfico
Denegación de servicios	

Nota. Tabla extraída de Oquendo & Giraldo (2022, p. 6). La principal diferencia entre estos ataques reside en la intervención o no del atacante.

Un claro ejemplo de estos ataques, son los intentos de robar información sobre el desarrollo de las vacunas.

Tanto la implementación de las tecnologia como la conectividad, evidencia que el internet y todos los servicios alojados en la red, promueven unas habilidades mínimas y avanzadas para el usuario final, ya que la ciberpandemia, focalizaba un mercado rebosante de oportunidades para los cibercriminales que se han entrenado y perfeccionado; además de saber como explotar este mercado. La Tabla 4, muestra información relevante por países, de las habilidades que tienen usuarios a la hora de navegar por internet; también se muestran, habilidades avanzadas y de desarrollo que tuvieron que adquirir algunos usuarios, (DESI, 2021, párr. 6)

Es importante resaltar que (OWASP, 2017) de forma gratuita, especifica herramientas y estándares de seguridad en aplicaciones, libros completos revisados no solo en aplicaciones, sino además en desarrollo de código fuente; presentaciones y videos.

Tabla 4.
Habilidades del usuario en el uso de Internet

País	Habilidades del usuario de internet	Habilidades de desarrollo avanzado
Finlandia	38,2305	32,878
Suecia	36,0145	28,5409
Países Bajos	39,2354	22,3136
Dinamarca	35,4817	25,7172
Estonia	30,2154	27,702
Luxemburgo	31,3978	24,7862
Alemania	33,8654	21,3759
Irlanda	26,6679	27,4064
Austria	32,3794	20,9698
Bélgica	29,4622	21,3196
Malta	28,3866	20,7082
España	28,5461	19,7867
Eslovenia	26,9987	20,8045
Francia	27,6888	19,6707
Chequia	28,43	18,7231
Unión Europea	27,1965	19,8632
Croacia	27,0347	19,6876
Lituania	27,4068	18,7357
Portugal	25,8958	19,67
Eslovaquia	25,5389	18,2133
letonia	20,8585	20,2504
Grecia	24,0346	17,0067
Hungría	23,3018	17,1785
Chipre	21,8221	17,8519
Polonia	20,9058	16,7922
Italia	20,2178	14,8976
Rumania	14,0844	18,9668
Bulgaria	13,3506	19,3501

Nota. Datos extraídos de (DESI (2021).

2.2 Características y métodos de la ciberdelincuencia

La criminalidad informática se basa en gran medida en la existencia de la tecnología, las características y herramientas que los delincuentes informáticos operan a través del Internet, tanto a nivel internacional como nacional crece de forma exponencial a un ritmo alarmante. Un claro ejemplo es la inmersión de la educación 4.0 en los últimos años que se dio a través de la contingencia mundial; esta trajo aparejada una profunda transformación del proceso enseñanza – aprendizaje, discurriendo en la vida cotidiana e interacciones personales, con independencia académica y múltiples formas de vectores de ataque que pueden sufrir desde cualquier zona del planeta (Oquendo & Giraldo, 2022)in the digital educational society, in which the citizen was subjected through the global contingency that we live in today. For this purpose, we focused on a qualitative research that considers the conditions and characteristics of education 4.0; in addition to the probabilities of security incidents, materialization of threats regarding the media that occur in the teaching-learning process.\nHowever, we carried out the analysis method, oriented in Open Web Security Project (OWASP.

Esta delincuencia, a diferencia de los que buscan un renombre en el mundo hacker, no se vanaglorian de sus hazañas y la notoriedad, fijan su objetivo en lo económico (enriquecimiento rápido); político o religiosos (ideas tendenciosas). También, en la fácil comisión, que son de elemento internacional; por otra parte, que se centra en un número muy elevado de víctimas; que los resultados pueden manifestarse de manera inmediata; pasan desapercibidos ya que, en los fraudes online junto con los delitos contra el honor, es donde existe mayor incidencia de cifra negra; así mismo, que cuentan con la facilidad de complicar la investigación policial y judicial.

En lo referente a los principales sectores de interés que focaliza la delincuencia informática, la observamos a continuación, (Gobierno de España, 2021,, p. 13).

- Gubernamental
- Defensa
- Industria armamentista
- Salud e industria farmacéutica
- Centros de investigación
- Tecnologías de la información y las comunicaciones
- Energía
- Telecomunicaciones
- Inversión financiera
- Comercio internacional

1. Empleo de las Bonet

El Bonet, hace referencia a una red de ordenadores, robots, bots o zombis, que están infectados por un malware, y controlados de forma remota y coordinada por un botmaster y proyectado a un número muy elevado de víctimas.

El aumento del desarrollo de las redes informáticas y las infraestructuras asociadas en su efecto, las redes bots, representan una gran amenaza y se utilizan ampliamente para muchos delitos en Internet (Hoque *et al.,* 2015). Dicho de otra forma, "Las botnets son amenazas emergentes con miles de millones de hosts en todo el mundo infectado. Los bots pueden propagarse por miles de computadoras en una velocidad muy alta, como lo hacen los gusanos" (Liu *et al.*, 2009, p. 2).

Básicamente, el botmaster establece un tipo de red, estableciendo finalidad y medios técnicos a utilizar, como puede ser un keylogger; se puede focalizar en la creación de cuentas administrativas para escalar privilegios, ejecución remota de comandos, captura de pantalla, descarga y trasferencia de ficheros, etc.

La Figura 1, muestra cómo se puede realizar la ejecución remota de comandos de tipo, PDF, Word, Excel, etc.) por un Botmaster.

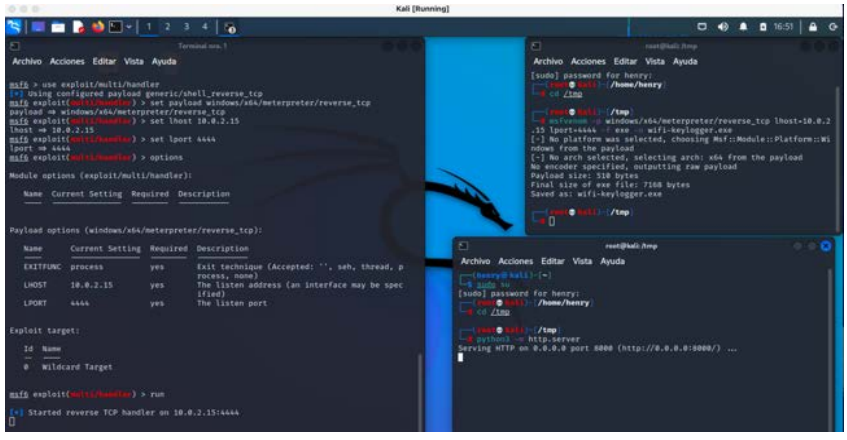

Figura 1. Ejecución remota de comandos. Producción propia.

Nota. Para mayor comprensión de esta práctica se puede observar en Maestro Rromani (2022).

Importante resaltar, que los dispositivos IoT son un foco de ataque para la delincuencia informática.

El crecimiento de los dispositivos IoT es masivo en la actualidad. Sin embargo, la seguridad se está convirtiendo en un gran desafío con este crecimiento. Los ataques, como los ataques de botnets basados en IoT, son cada vez más frecuentes y se han vuelto populares entre los atacantes (Ali *et al.*, 2020, p. 1)

2. *Uso del Ransomware*

Otra característica de esta delincuencia es que el delito se lleva de forma instantánea y con resultados también instantáneos, como es el caso del uso de ransomware (variante de software malicioso). Este software, bloquea los sistemas informáticos o determinados archivos, exigiendo que se pague una determinada cantidad de dinero (rescate), afecta, no solo pequeñas empresas y administraciones públicas locales,

sino, además, a grandes corporaciones con sistemas de defensa y cierta madurez de las TIC.

Esta modalidad de ataque es una de las más eficientes y sencillas en la comisión de delito, debido a la aparición de exploit kits (funcionalidades empaquetadas), con programas informáticos destinados a ejecutar, como se evidencia en la Figura 1. No obstante, este ataque, conlleva a detener actividades ante la amenaza de pérdida total del sistema. "Como respuesta a estas situaciones, el CCN-CERT ha publicado durante el año diferentes informes de código dañino tipo ransomware, como RobbinHood, Avaddon, NetWalker, Maze, Snake locker y Vcript". (Gobierno de España, 2021, p. 16).

Importante resaltar, que el ciberdelincuente, para cobrar el rescate del sistema, archivo o documento secuestrado, emplea el método de la criptomoneda, ya que es difícil de rastrear.

3. El Phishing

El robo de identidad informático es un delito en el cual se utilizan los datos de un usuario para navegar, inyectar algún script, spyware u otro tipo de malware; estas acciones, logran infectar el sistema, robar datos personales o transformarlos en miembro de un Bonet. Conviene subrayar, que uno de los principales inconvenientes que enfrenta el ciudadano informático, es la gran cantidad de mensajes e-mails que se reciben a diario, como no se presta mucha atención a su contenido se facilita la labor del atacante para la simulación de ser otra persona (Pacheco & Jara, 2009, p. 49).

En pocas palabras, estos sitios fraudulentos simulan ser entidades financieras o de compras online, para solicitar datos personales al usuario y poder robar su identidad y en su efecto realizar estafas masivas como el phishing. La página de Ciberseguridad, indicar que el phishing, se produce cuando se intenta engañar a los usuarios (2021, párr. 8).

La Figura 2, muestra la facilidad para clonar y simular, la existencia a de una entidad reconocida como Facebook; el link obtenido (página fraudulenta) se puede enviar a miles de usuarios (red Bot) por medio de ingeniería social.

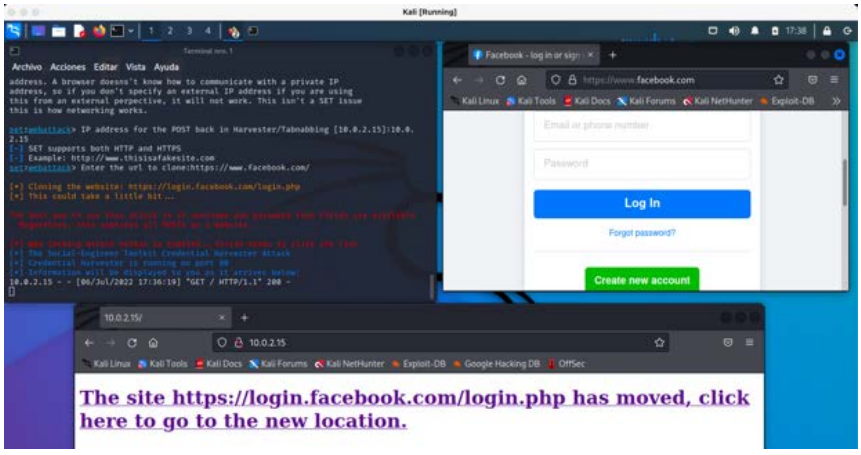

Figura 2. Clonar un sitio (link) para simular ser una entidad y capturar información confidencial. Producción propia.

Sumado a esto, surge el BEC (Business Email Compromise) o phishing corporativo, que es uno de mecanismos de ciberataque empleado especialmente en pandemia (teletrabajo), esto por el aumento de objetivos potenciales; el supuesto de la falta de los controles de seguridad, que no mitigan las amenazas y vulnerabilidades de los vectores de ataque; usuarios no familiarizados con la tecnología y que tiene que usar a diario por su trabajo.

En su estudio de Palo Alto Network (2021) y como se citó en RedZone (2021), concluyeron que el

teletrabajo ha hecho que los ataques de phishing crezcan, las causas en gran parte es que las redes domésticas no están protegidas por firewall, utilizan equipos informáticos personales sin protección.

4. El hacktivismo

Básicamente son protestas trasladadas al Internet con conflicto político, religioso, étnico o cultural, conocidas como hacktivismo; personas que buscan hacer una declaración sin buscar ganancias financieras (piratear por una causa), (Ciberseguridad, 2021c).

No obstante, este acto delictivo disminuyó durante los últimos años, pero se siguen utilizando las mismas tácticas y procedimientos (TTP) registradas en años anteriores. "Los hacktivistas atacan utilizando una plétora de métodos de piratería que les permiten obtener acceso a computadoras personales, donde pueden tomar el control y obtener información privada", (CFI, 2022).

Conviene resaltar, que a los hacktivistas no les interesa obtener beneficios económicos. Por otra parte, los daños causados son visibles como ataques de Denegación de Servicios (DoS y DDoS) dirigidos principalmente a sitios web del Gobierno; defacements (desconfiguraciones de sitios web); inyecciones SQL (SQLi) para exfiltrar información de la base de datos y publicarla; doxxing (obtener máxima información privada), (Gobierno de España, 2021, p. 18).

5. Ciberespionaje

El COVID-19, fundamentó las tendencias geopolíticas del ciberespionaje, con la mira de obtener información y el hecho de ser los primeros en disponer de una vacuna. "Sobre AstraZeneca se ha publicado que ha sufrido estos intentos de ataque. Asimismo, datos relativos a las vacunas de Pfizer fueron robados de la EMA (European Medicines Agency). Moderna tampoco se ha salvado de los intentos de intrusión", (Gobierno de España, p. 24).

De lo anterior, la tendencia más inquietante al ciberespionaje es la utilización de ransomware para ocultar sus huellas, dificultar la distribución y crear distractores. "Los dos grupos de actividad de hacking, analizados por Secureworks son "Bronze Riverside" (APT41) y "Bronze Starlight" (APT10), ambos utilizan el cargador HUI para desplegar troyanos de acceso remoto, PlugX, Cobalt Strike y QuasarRAT", (Nicola, 2022).

6. Doble extorsión

Consiste en cifrar los datos con un software malicioso, para que los ciberdelincuentes puedan acceder a robar información confidencial y amenazar con su publicación, (Life, 2021); así mismo se resalta que la familia de ransomware que iniciaron la tendencia de extorsión en Maze, se han involucrado en ciberataques al LG o Xerox, RagnarLocker o WastedLocker.

En la lectura, se puede apreciar que, "Las cifras del ransomware dirigido que usan la doble extorsión durante 2020 aumentó un 767 % con respecto al periodo anterior", (Life, 2021, p. 1).

7. Fraude del CEO

Este ataque se focaliza en el contable de la empresa o el empleado del rango alto, reciben un correo de su jefe, ya sea su CEO, presidente o director de la empresa; le piden ayuda urgente para transacciones financieras confidenciales. Este tipo de engaño es conocido como whaling (pesca dirigida), por tratarse de phishing dirigido a peces gordos, (INCIBE, 2017).

El fraude del CEO es la táctica BEC (Business Email Compromise) o phishing corporativo, más habitual en los últimos años, ya que suplanta a un superior para engañar al empleado.

8. Cryptojacking

El cryptojacking o también conocido como criptominería de criptomonedas maliciosas; consiste en instalar malware en el ordenador o celular, para ejecutar minería o script en segundo plano y extraer criptomonedas, como Bitcoin y Litecoin que son seudónimas, sin el consentimiento del propietario por medio del cryptojacking.

> Cryptojacking es una forma más sutil de robar criptomonedas. Si bien el phishing y el ransomware es un juego de números en el que los usuarios deben ser engañados o amenazados para entregar

> sus activos virtuales, el software de criptominería solo necesita un simple clic para instalar en secreto en segundo plano y comenzar a minar, sin que el usuario lo sepa. (Ciberseguridad, 2021)2021

9. Medio principal de cometer el delito informático

La red TOR implementa una técnica llamada onion routing (enrutado de cebolla), ésta diseña con vista a proteger las comunicaciones, lo que significa que cambia el modo de enrutado tradicional de Internet para garantizar el anonimato y la privacidad de los datos. Los datos son aviados, no de forma directa (solo el primero y último nodos sabe de dónde parte y hacia donde se dirige el mensaje o paquete de datos).

> La red TOR tiene como objetivo proporcionar anonimato a aquellos usuarios de Internet que no quieran revelar su identidad cuando navegan por determinados contenidos. TOR está compuesto por un conjunto de enrutadores que hacen uso de la criptografía para aplicar varias capas de encriptación a los paquetes, ocultando así la dirección IP del usuario pero también la relación entre el usuario y el servidor, y los contenidos a los que accede. (Ballesteros Lopez, 2018)

Por otra parte, las redes sociales son un medio de promocionar actos delictivos, ya que permiten llegar a una gran audiencia a nivel mundial, "En julio de 2020, Twitter sufrió uno de sus mayores ataques hasta la fecha, quedando expuesta información de personas muy influyentes y de diferentes cuentas de empresas". (Gobierno de España, 2021, p. 19)

10. Otras motivaciones del cibercrimen

Teniendo presente que muchos delitos pasan desapercibidos para la misma víctima, lo que implica una cifra negra, al no presentar denuncia por falta de la misma conciencia de la tipificación del delito, quedan una comisión de delitos no denunciados como:

- Smishing: SMS fraudulentos.
- Vishing: llamadas fraudulentas.
- Pharming: alteración de DNS.
- Skimming: clonación de tarjetas
- Etc.

3. Resultados

De acuerdo con los datos entregados por la Organización Mundial de la Salud (OMS) y el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), el confinamiento social a través de la lucha mundial contra el COVID-19, acrecentó la integración de las tecnologías en el sector empresarial.

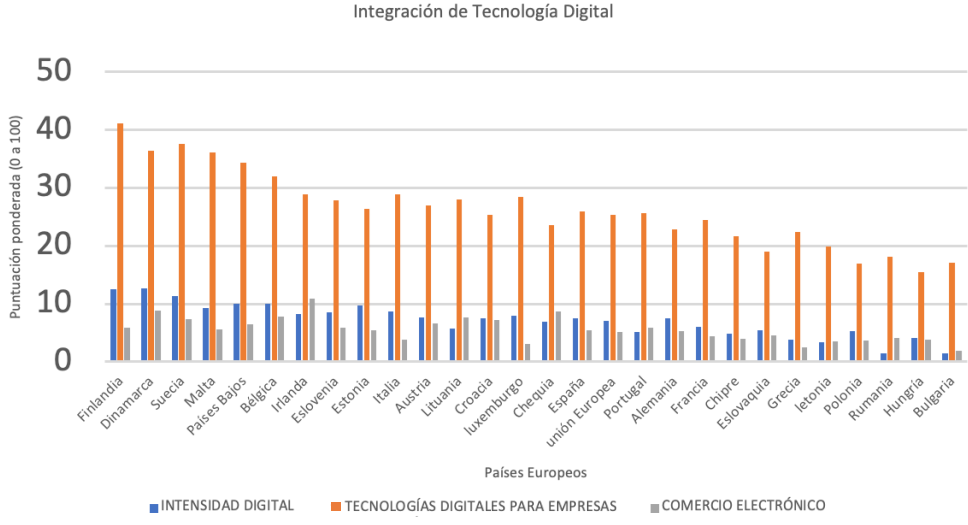

Figura 3. Integración de las tecnologías en países de Europa.
Producción propia.

La Figura 3, muestra un crecimiento significativo de las empresas, frente a la combinación de la intensidad digital y el comercio electrónico en su actividad comercial.

De igual forma, la Figura 4, evidencia los países europeos con mayor conectividad con la cual afrontaron la emergencia pandémica, estos son: España, Luxemburgo, Suecia y Hungría. Así mismo, los Países Bajos, Dinamarca, Portugal y Bélgica, que arrojaron una puntuación ponderada de 10.

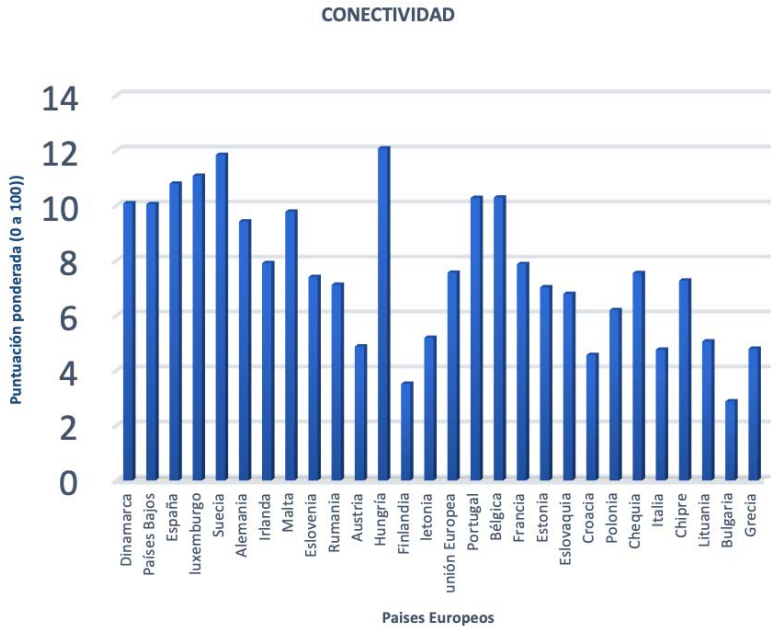

Figura 4. Conectividad en pandemia en países de Europa.

Conviene subrayar, que la lucha que enfrentaba la sociedad actual dentro su "normalidad" de vida, tanto personal como profesional en la navegación del ciberespacio, hace necesario capacitarse frente a temas de seguridad informática, para reconocer o en su efecto, salvaguardar los principales servicios de seguridad, como son: la confidencialidad, integridad, autenticación, control de acceso, el no repudio y la disponibilidad de la información; si bien, las habilidades del uso del Internet se acrecentaron en gran medida, no podemos omitir que las habilidades de desarrollo avanzado de las TIC no fueron a la par con las necesidades demandadas.

En definitiva, se observa con claridad, que el mercado de la ciberdelincuencia rebosaba de oportunidades para lanzar vectores de ataque al ciberespacio, por la necesidad de conexión de los miles de usuarios a nivel mundial.

No obstante, los países que apostaron más al desarrollo avanzado de las habilidades de usuario para el uso de las tecnologías, fueron: Rumania y Bulgaria, como se observa en la Figura 5. Conviene resaltar, que Rumania con 19.201.1662 de habitantes (considerado país intermedio) y una tasa de letalidad (fallecidos respecto a confirmados) es del 2,25 %, en comparación a otros países, (Expansión, s. f.). De igual forma, Bulgaria con 6.916.548 de habitantes (considerado país intermedio), y una tasa de letalidad (fallecidos respecto a confirmados) es del 3,18 %, (Expansión, s. f.a).

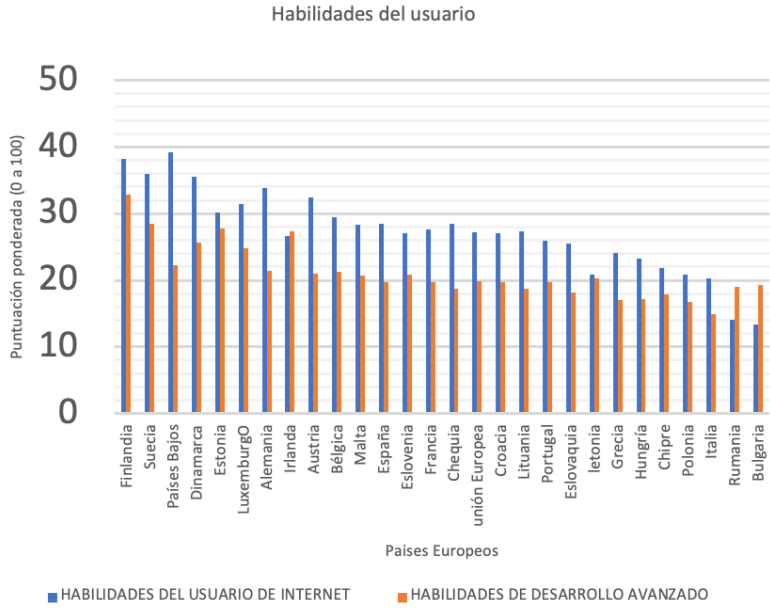

Figura 5. Habilidades del usuario en el uso de las TIC.
Producción propia.

Consecuentemente, el Instituto Nacional de Ciberseguridad (INCIBE) a través de INCIBE-CERT gestionó 133.155 incidentes de ciberseguridad durante el año 2020, de los cuales 106.466 hacen referencia a ciudadanos y empresas, 1.190 a operadores estratégicos y 25.499 a la Red Académica y de Investigación Española (RedIRIS).

Figura 6. Incidentes según criticidad de ataque.

Datos extraídos de (etl2020-cryptojacking-ebook-en-es.pdf, s. f.)

Así mismo, en el año 2019, las vulnerabilidades de software de almacenamiento en la nube aumentaron un 46 %, como se observa en la Figura 6, la cual muestra la distribución de estos incidentes según su criticidad.

Así mismo, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), constató, que los principales programas de malware de criptominería más importantes globalmente para los ciberataques son los evidenciados en la Figura 7.

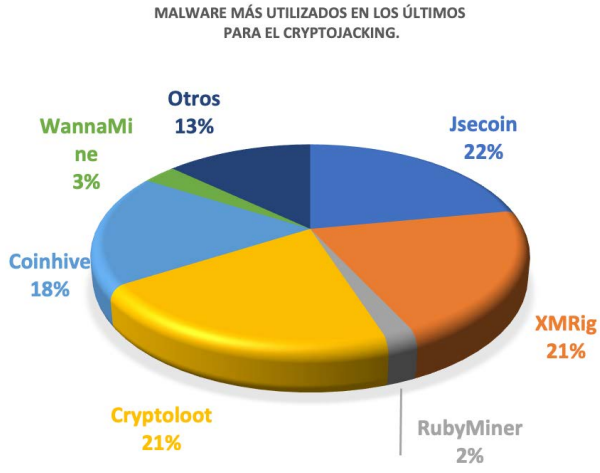

Figura 7. Malware más utilizados para realizar vectores de ataque.
Datos extraídos de (Enisa (2020)

Así mismo, señala que Coinhive (popular servicio de criptominería), cerró en marzo del 2019, por numerosos abusos por parte de la ciberdelincuencia que inyectaban códigos en sitios web, generando la criptomoneda Monero y desviar fondos.

En conclusión, la comisión de los delitos informáticos, en su mayoría son comercializados en la Dark web, como servicios contables (Malware as a Service (MaaS)), redes sociales, como difusión masiva de contenido y alojamiento en servidores informáticos sin resguardo de información. Todo esto, hace que los contenidos sean modificables, destruibles y que dificultan el proceso de investigación, lo que indica que las pruebas son difíciles de obtener, como bien lo señala Oquendo, en su investigación, al referirse a la dificultad de adquisición de contenidos probatorios en la memoria RAM en entonos virtuales que facilitan las técnicas antiforense. (2022, p. 9).

4. Discusión

Conviene subrayar, que el phishing sigue siendo uno de los vectores de ataque más utilizados para engañar actores internos de las organizaciones.

Así mismo, la adaptación de TTP en la ciberdelincuencia, hace que estos ciberataques sean más peligrosos que nunca; de igual forma, el ransomware, el BEC (Business Email Compromise) o phishing corporativo y el malware modular para cubrir superficies de ataque mayor, como se evidenció en la Figura 6 (Incidentes según criticidad de ataque) y la Figura 7 (Malware más utilizado para realizar vectores de ataque).

En coincidencia con este artículo, los ciberataques antes señalados, son posicionados por (Ciberseguridad, 2021a), como los métodos de ataques más significativos en la lucha mundial contra el COVID-19.

Además, los ataques de ransomware que se ha extendido hasta el año 2021, como lo fueron: el de DarkSite contra el oleoducto colonial (CP) de la infraestructura petrolera de EE.UU., cobrando un pago de 75 Bitcoin (aproximadamente $4,4 millones) para volver a su sistema. Ataque de DarkSite contra Toshiba; ingresaron a los sistemas produciendo robo de información. REvil dirigido a ACER; se produce el robo de datos y exigiendo un rescate de 214.151 XMR en criptomonedas (aproximadamente $50 millones). REvil compromete el acceso al sistema de JBS Foods; de lo cual se pagó $11 millones, para conectar de nuevo el sistema. Ataque a T-Mobile, filtrando información de más de 50 a proyhmillones de clientes y que se estaba vendiendo estos datos en la red oscura por una suma de 6 Bitcoins (aproximadamente $270.000).

Evil Corp contra CNA Financial, la aseguradora comercial más grande de los Estados Unidos; pagando un rescate de 40 millones de dólares. Escuelas públicas de Búfalo en Nueva York. Ataque a las tecnologías Applus. REvil contra el fabricante de computadoras portátiles de Apple, Quanta Computer. El Ejecutivo del Servicio de Salud de Irlanda (HSE); AXA; CD Projekt Red; IKEA; ataque al servidor de Microsoft Exchange y el de la Agencia Escocesa de Protección Ambiental (SEPA).

5. Trabajos futuros

Este artículo, enfatiza en la comisión de delitos informáticos; más específicamente, delincuencia o criminalidad informática, para que quede bien definida esta tipología delictiva en el Código Penal. En efecto, la ciberdelincuencia aprovechó las necesidades de la sociedad actual para atacar distintos bienes jurídicos en la que las TIC son el medio por el cual se lanzan vectores de ataque.

Ahora bien, para ampliar esta investigación se recomiendan los siguientes trabajos a futuro y así poder compactar esta evaluación, esto es:

- Establecer un seguimiento de delitos informáticos en la Darck web.
- Concientización de seguridad informática en redes sociales, para actores internos y externos de las empresas.
- Análisis de ransomwares más eficaces y peligrosos en la criptomineria.
- Análisis actual, sobre la reforma legislativa contra la lucha de la ciberdelincuencia.

Referencias

Ali, I., Ahmed, A. I. A., Almogren, A., Raza, M. A., Shah, S. A., Khan, A., y Gani, A. (2020). Systematic Literature Review on IoT-Based Botnet Attack. *IEEE Access*, *8*, 212220-212232. https://doi.org/10.1109/ACCESS.2020.3039985

Ballesteros López, I. (2018). *Análisis de seguridad de la red TOR*. https://upcommons.upc.edu/handle/2117/123445

CFI. (2022). *Hacktivism*. Corporate Finance Institute. https://corporatefinanceinstitute.com/resources/knowledge/other/hacktivism/

Ciberseguridad. (2021). Minería de criptomonedas—Cryptojacking. https://ciberseguridad.com/amenzas/cryptohacking/

Ciberseguridad. (2021a). Los 15 ciberataques más importantes en 2021. *Ciberseguridad*. https://ciberseguridad.com/ciberataques/mas-importantes-2021/

Ciberseguridad. (2021b). Phishing. *Ciberseguridad*. https://ciberseguridad.com/amenzas/phishing/

Ciberseguridad (2021c). Hacktivismo. https://ciberseguridad.com/amenzas/hacktivismo/Consejo de Europa (2001). Convenio sobre la ciberdelincuencia. *Serie de tratados europeos, 185.* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

Consejo de la Unión Europea (2005). Decisión marco de 2005. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ES:PDF

Council of Europe. (2022). *Full list*. Treaty Office. https://www.coe.int/en/web/conventions/full-list

DESI. (12 de noviembre de 2021). *Acerca de: Índice de Economía y Sociedad Digital*. https://virtuoso.digital-agenda-data.eu/describe/?url=http://semantic.digital-agenda-data.eu/dataset/DESI

DESI (2021). *DESI by components—Digital Scoreboard—Data & Indicators*. https://digital-agenda-data.eu/charts/desi-components#chart={%22indicator%22:%22desi_conn%22,%22breakdown-group%22:%22desi_conn%22,%22unit-measure%22:%22pc_desi_conn%22,%22time-period%22:%222021%22}

DESI (12 de noviembre de 2021a). Índice de Economía y Sociedad Digital. *DESI — Cuadro de indicadores digital—Datos e indicadores*. https://digital-agenda-data.eu/datasets/desi/indicators

Enisa (2020). *Crypto-jacking.* https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-cryptojacking-ebook-en-es.pdf

Gobierno de España (2021). *Ciberamenazas y tendencias.* https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html

Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications Surveys & Tutorials*, *17*(4), 2242-2270. https://doi.org/10.1109/COMST.2015.2457491

INCIBE. (19 de enero de 2017). *Fraude del CEO*. INCIBE. https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fraude-del-ceo

Expansión (s.f.). Rumanía - COVID-19 - Crisis del coronavirus 2022, *Datosmacro.com.* de https://datosmacro.expansion.com/otros/coronavirus/rumania

Expansión (s. f.a). Bulgaria - COVID-19 - Crisis del coronavirus 2022. *Datosmacro.com*. https://datosmacro.expansion.com/otros/coronavirus/bulgaria

Gobierno de España (2020). *La sociedad en red transformación digital en España Informe Anual 2019.* Edición 2020 https://www.ontsi.es/sites/ontsi/files/2020-11/InformeAnualLaSociedadEnRed2019Ed2020.pdf

Life, B. (2021, abril 27). *El ransomware con doble extorsión crece un 767% en 2020*. Bit Life Media. https://bitlifemedia.com/2021/04/ransomware-los-ciberataques-extorsion-aumentaron-767-en-2020/

Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., y Zhang, J. (2009). Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. *EURASIP Journal on Wireless Communications and Networking*, *2009*(1), 692654. https://doi.org/10.1155/2009/692654

Maestro Rromani. (2022, enero 28). *Creación de un ejecutable con un payload: Ingeniería Social*. https://www.youtube.com/watch?v=Z9J8TVp9FJ4

Nicola, M. D. (2022). *Ciberdelincuentes chinos, utilizan el ransomware como señuelo para el ciberespionaje | Ciberseguridad LATAM*. https://www.ciberseguridadlatam.com/2022/06/26/ciberdelincuentes-chinos-utilizan-el-ransomware-como-senuelo-para-el-ciberespionaje/

Oquendo, H. G. (2022). Evaluación de herramientas de software libre, para el sistema operativo Windows, en la adquisición de evidencias de la memoria RAM. *Publicaciones e Investigación*, *16*(1), https://doi.org/10.22490/25394088.5567

Oquendo, H. G., & Giraldo, L. O. (2022). Análisis de riesgos y vulnerabilidades en la educación 4.0 del proceso de enseñanza – aprendizaje. *Publicaciones e Investigación*, *16*(1), https://doi.org/10.22490/25394088.5615

OWASP (s. f.). OWASP Top 10 2017. https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Palo Alto Network. (2021). *Informes técnicos*. Palo Alto Networks. https://www.paloaltonetworks.es/resources/whitepapers

Pacheco, F. G. & Jara, H. (2009). Hackers al descubierto. *Users.* https://manualdehacker.com/wp-content/uploads/2018/06/91-Hackers-al-Descubierto-pdf.pdf

RedZone. (2021). *El teletrabajo aumenta uno de los peores ataques de seguridad*. RedesZone. https://www.redeszone.net/noticias/seguridad/teletrabajo-aumento-ataques-phishing/