NOTA DE ACTUALIDAD 16/2018
20 de diciembre 2018

*Loreto Machés Blázquez y Pilar Roig Minguell**

IOCTA 2018
Evaluación de Amenazas del Crimen Organizado en Internet 2018

IOCTA. Evaluación de Amenazas del Crimen Organizado en Internet 2018

El presente texto es una síntesis y del documento Internet Organised Crime Threat Assesment 2018

ÍNDICE

* Alumnas en prácticas del doble grado en Relaciones Internacionales (bilingüe) y Traducción e Interpretación, Universidad Pontificia de Comillas (ICADE), Madrid

SIGLAS Y ABREVIATURAS

- API→ Interfaz de programas de aplicación
- CSE→Explotación sexual de menores en línea
- CSEM→ Material de explotación sexual de menores
- DDoS→ Ataques de denegación de servicios
- DEA: Administración para el Control de Drogas
- EKs→ Kits de *exploit*
- EPC→ Consejo Europeo de Pagos
- GDPR→ Reglamento General de Protección de Datos
- IoT→ Internet de las Cosas
- LDCA→ Difusión en directo de abusos sexuales a menores
- IRSF→ Fraude internacional de coparticipación
- OCG→ Grupos de crimen organizado
- PBX→ centralita telefónica
- PoS→ Puntos de venta
- RATs→ Troyanos de acceso remoto
- RDP→ Protocolo de escritorio remoto
- SGEM→ Material explícito autogenerado

1. PREÁMBULO

Tengo el placer de presentar la Evaluación de Amenazas del Crimen Organizado en Internet 2018 de Europol (IOCTA), que ha sido y continúa siendo uno de los documentos estratégicos más emblemáticos de Europol. Proporciona una excepcional evaluación de las nuevas amenazas y las principales evoluciones en el campo de la ciberdelincuencia durante el último año, desde la perspectiva de las fuerzas de seguridad. Sin embargo, esto es únicamente posible gracias a las valiosas contribuciones de las fuerzas de seguridad europeos y al continuo apoyo que recibimos de nuestros socios en el sector privado, financiero y académico.

Cada año el informe resalta ciberataques de una magnitud y alcance sin precedentes. Este año no es diferente, lo que demuestra la creciente necesidad de una mayor cooperación y colaboración dentro de nuestra comunidad policial, un principio/aspiración que se encuentra en el corazón de la misión de Europol. El informe también nos hace reflexionar sobre amenazas anteriores que se subestimaron, como fraudes en telecomunicaciones, lo que demuestra la necesidad de una constante adaptación y desarrollo por parte de los servicios de seguridad, y un entrenamiento continuo en todos los aspectos de ciberdelincuencia. Este informe engloba las palabras clave de Europol: confianza, intercambio y cooperación.

Solo si los cuerpos de seguridad, el sector privado y el mundo académico trabajan en estrecha colaboración (colabora estrechamente), se podrá combatir la ciberdelincuencia de forma efectiva.

A pesar de que algunos ciberataques siguen apareciendo en titulares debido a su magnitud, otras áreas de la ciberdelincuencia también deben considerarse como amenazas o problemas.

El fraude en los pagos destaca las ganancias criminales y favorece la aparición de otros crímenes, así como las pérdidas económicas considerables, tanto para ciudadanos como para instituciones.

La explotación sexual de menores en línea representa una de las peores facetas de internet, y subraya el peligro constante hacia nuestros menores de aquellos que quieren explotarlos o abusar de ellos.

La lucha contra los crímenes aberrantes debe seguir adelante. Después de todo, todos los menores, donde quiera que se encuentren, tienen el derecho de crecer en un ambiente seguro.

El informe de este año también describe un número de desarrollos legislativos y tecnológicos claves, tales como la introducción de la Reglamento General de Protección de Datos (RGPD), la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (conocida como Directiva NIS) y la tecnología 5G. A pesar de su importancia, todos estos desarrollos tendrán un impacto en cierta medida en nuestra capacidad como funcionarios de policía para investigar de manera efectiva la ciberdelincuencia. Esto subraya la necesidad de un compromiso del cumplimiento de la ley con los políticos, legisladores e industria, para desempeñar un papel en la evolución de la sociedad.

El IOCTA también celebra los numerosos logros del cumplimiento de la ley en la lucha contra la ciberdelincuencia. Mientras que el cumplimiento de la ley en la Unión Europea siga creciendo, evolucionando y forjando nuevos lazos con socios internacionales en los sectores público y privado, confío en que podamos continuar informando de estos logros en los próximos años.

2. RECOMENDACIONES

Se desarrollan en cada punto.

3. INTRODUCCIÓN

La Evaluación de Amenazas del Crimen Organizado en Internet de Europol (IOCTA) tiene como objetivo informar a responsables en puestos estratégicos, políticos y tácticos en la lucha contra la ciberdelincuencia, con el propósito de dirigir la atención operativa entre todas las fuerzas y cuerpos de seguridad de la UE. La IOCTA de 2018 contribuye a definir las prioridades de la plataforma Multidisciplinar Europea contra las Amenazas Delictivas (EMPACT, por sus siglas en inglés), en tres subescalas de prioridades de cibercrimen: ataques cibernéticos, fraude de pago, explotación sexual de menores en línea, y factores transversales de delincuencia.

4. CRÍMENES CIBERDEPENDIENTES

Este tipo de crímenes se caracterizan por poder cometerse únicamente con ordenadores, redes o cualquier otro medio relacionado con las Tecnologías de la Información y la Comunicación (TIC).

4.1. Conclusiones principales

- El *ransomware* sigue siendo la principal amenaza tanto para las fuerzas de seguridad como para la cobertura industrial.

- Se espera que el *malware* de la minería de criptomonedas se convierta en una fuente de ingresos recurrente y de bajo riesgo para los ciberdelincuentes.

- El uso de kits de *exploit* (EKs por sus siglas en inglés) para dañar equipos informáticos sigue reduciéndose. Sin embargo, el *spam*, la ingeniería social y los métodos nuevos como el Protocolo de escritorio remoto (RDP por sus siglas en inglés) están comenzando a crecer.

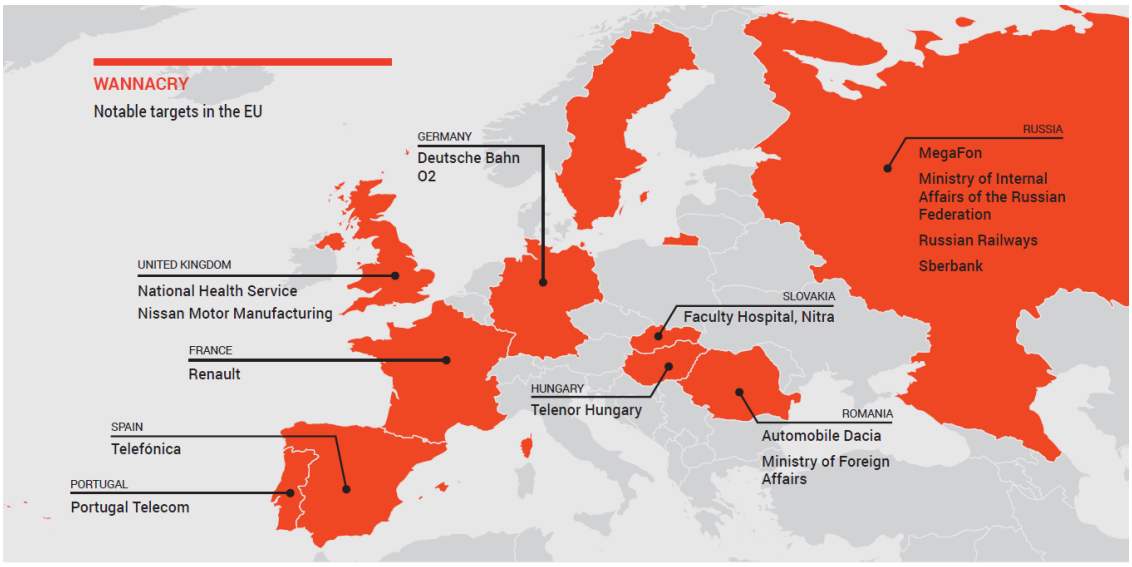
- Gracias a la nueva legislación contra la violación de datos personales, se espera que se denuncien más casos de incumplimiento de la ley y de ciberextorsión.

4.2. Malware

El *ransomware* sigue a la cabeza de las amenazas en todos los ámbitos de la comunicación durante 2017. Los ataques de WannaCry y *NotPetya* afectaron a más de 300 000 usuarios en 150 países. Dentro de la UE, estos ataques perjudicaron a numerosas industrias e infraestructuras, incluidos los servicios sanitarios, de telecomunicaciones, transporte o producción. A pesar de que existe una respuesta coordinada específica para estos ataques a nivel global, las fuerzas de seguridad europeas han denunciado muchos otros de distinta naturaleza.

La tendencia actual de los ataques de *ransomware* es que afectan cada vez más a pequeñas empresas y a objetivos más importantes -por las ganancias que suponen- y ya no solo a objetivos individuales. Sin embargo, los troyanos de banca y otras formas de *malware* financiero ya no constituyen un problema grave. Lo mismo sucede en el caso del *malware* móvil, ya que este tipo de actividades malignas suceden con más frecuencia en las regiones de África, Asia y América, en particular en Estados Unidos. Asimismo, los Troyanos de acceso remoto (RATs por sus siglas en

inglés) no predominan en los Estados miembros, aunque los casos en los que aparecen lo hacen tanto en los sectores público como privado.



El *cryptojacking* es un término inglés que se refiere a cualquier proceso que use un sistema para minar criptomonedas sin el permiso del usuario. En la mayoría de los casos, esto se consigue a través de la ejecución de un *script* del buscador que el usuario esté utilizando. Esta forma de minería de criptomonedas está comenzando a aumentar, debido en parte al proceso de legalización de las criptomonedas.

En 2014, este informe comunicó que más del 80% de las amenazas en línea estaban asociadas al uso de kits de *exploit*. En 2017, esta tendencia se ha reducido considerablemente y solo algunos Estados miembros ha informado de la existencia de esta actividad. Por el contrario, los ciberdelincuentes utilizan con más frecuencia métodos más consistentes de virus informáticos a través de ingeniería social, como el *spam* o el *phishing*.

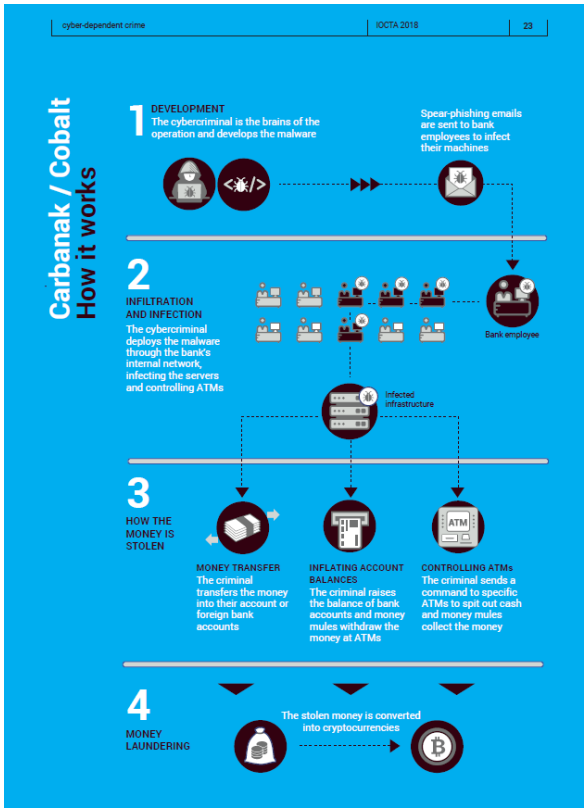
4.3. Ataques a infraestructuras importantes

Como ya se ha mencionado con anterioridad, los ataques de WannaCry o NotPetya no solo afectaron a usuarios sino también a infraestructuras importantes, en particular en los sectores de sanidad, transporte y telecomunicaciones. Uno de los desafíos que conllevan este tipo de ataques es la variabilidad de su naturaleza, y, por lo tanto, la dificultad de determinar un *modus operandi* para las fuerzas de seguridad.

4.4. Violaciones de datos y ataques a redes

En la actualidad, la protección de datos resulta crucial en cualquier sector de la sociedad. La mayoría de los ataques de violación de datos personales los llevan a cabo actores externos, y una minoría de actores internos perpetra los demás.

El patrón que más se repite en los Estados miembros es la adquisición ilícita de datos, aunque los datos de las víctimas no tienen tanto valor para los atacantes como los de las infraestructuras. Las organizaciones del sector sanitario parecen ser las más afectadas en los últimos años por este tipo de intrusiones.



Los ataques que predominan después de los de *malware* son los Ataques de denegación de servicios (DDoS por sus siglas en inglés). Una de las razones principales de este aumento es la facilidad de obtener herramientas y servicios que permiten incluso a usuarios sin muchas habilidades informáticas perpetrar este tipo de ataques. Por el contrario, los ataques en servicios del Internet de las Cosas (IoT) no se han producido en el año 2017.

Por último, la amenaza de la de la desfiguración de páginas web sigue prevaleciendo, a pesar de tener un menor impacto debido a las escasas habilidades informáticas de los ciberdelincuentes realizan este tipo de acciones.

4.5. Evolución y amenazas futuras

El *ransomware* seguirá creciendo, tal y como lo señala la industria y la cobertura de las fuerzas de seguridad. Esta expansión también demuestra el abuso activo de la criptografía por parte de los delincuentes. Sin embargo, la minería de criptomonedas podría superar al *ransomware* como amenaza principal, dado el bajo riesgo de los navegadores de minería de criptomonedas -muchos de ellos legales- y la "ventaja" de poder prescindir de víctimas individuales. Asimismo, el *malware* móvil podría aumentar, debido a la transición de los servicios de banca digital a banca móvil.

Desafortunadamente, resulta complicado predecir si otro ataque de la misma envergadura que los de WannaCry o NotPetya se producirá de nuevo. Como se ha destacado en informes anteriores, existe muy poca claridad en lo que a las herramientas y acciones de los ciberdelincuentes y delincuentes auspiciados por Estados se refiere.

Por otro lado, la Directiva NIS entrará en vigor en la Unión Europea en mayo de 2018, y gracias a ella se reforzará la ciberseguridad en una variedad de sectores que operan en industrias críticas. Sin embargo, la menor cantidad de datos disponibles y la rigidez de los controles de datos personales pueden hacer que esa información sea aún más valiosa para los ciberdelincuentes.

4.6. Recomendaciones

4.6.1. Cooperación

Resulta esencial que las fuerzas de seguridad trabajen en conjunto con la industria de la seguridad en internet para poder frenar los ataques de ciberdelincuencia y la minería de criptomonedas.

4.6.2. Cobertura de la ciberdelincuencia

Las fuerzas de seguridad de cada Estado miembro deberían identificar las consecuencias de la Directiva NIS en sus respectivos países y poner planes en práctica según estos resultados.

4.6.3. Investigación

Las fuerzas de seguridad deberían centrarse en los ciberdelincuentes que ofrecen servicios o productos de ciberataques con el objetivo de impedir a los ciberdelincuentes con menores habilidades que ejecuten ciberataques de gran magnitud.

5. EXPLOTACIÓN SEXUAL DE MENORES EN LÍNEA

La explotación sexual de menores en línea (CSE por sus siglas en inglés) sigue siendo el aspecto más perturbador de la ciberdelincuencia. Debido a la dimensión en línea de este delito, los agresores han podido comunicarse entre sí por internet y conseguir material de explotación sexual de menores (CSEM por sus siglas en inglés) en cantidades que habrían sido inimaginables hace diez años. El creciente número de niños cada vez más pequeños que tienen acceso a dispositivos con conexión a internet y redes sociales, permite que los agresores contacten con los mismo de una forma que sería imposible en un entorno sin conexión a internet.

5.1. Conclusiones principales

- El material de explotación sexual de menores encontrado en línea sigue aumentando, lo que dificulta los procesos de investigación y las tareas de identificación de las víctimas.

- Como las tecnologías son cada vez más fáciles de usar, el empleo de herramientas de anonimato y encriptación por parte de los agresores para evadir a las fuerzas de seguridad es cada vez más común.

- El creciente acceso a internet y redes sociales por niños cada vez más pequeños, provoca un aumento en los casos de coerción y extorsión sexual en línea hacia menores.

- El abuso sexual a menores en directo sigue siendo un delito difícil de investigar y la trasmisión en directo de material autogenerado ha aumentado considerablemente.

5.2. La disponibilidad y distribución en línea de CSEM

El material de explotación sexual de menores en línea sigue aumentando, con un 60% de los Estados miembros indicando un incremento de la distribución digital de CSEM. El aumento de los dispositivos móviles con acceso a internet y el fácil acceso de anonimato en línea, así como el uso de la red oscura (*darknet*) permite a los agresores guardar y compartir material con menor riesgo de ser detectados.

Una de las razones del aumento de CSEM en línea es la continua producción de material explícito autogenerado (SGEM por sus siglas en inglés) y el desconocimiento de los propios padres y menores sobre las repercusiones que tienen el compartir este tipo de material, que puede terminar en manos de agresores sexuales de menores en línea.

5.3. La organización en línea de los agresores

La explotación sexual de menores en línea no es un fenómeno de crimen organizado en el sentido tradicional de la palabra, los agresores suelen ser lobos solitarios y no suelen estar involucrados en grupos de crimen organizado (OCG por sus siglas en inglés). No obstante, los agresores sexuales sí se organizan con la ayuda de foros en internet donde no solo comparten CSEM, sino que también discuten técnicas y enseñan cómo evadir a las fuerzas de seguridad. Así mismo, comienzan a

formarse grupos más pequeños para compartir CSEM e información desde aplicaciones de mensajería móvil.

Con el uso de herramientas de anonimato y encriptación en línea como Virtual Private Networks (VPNs), Tor y los foros de la red oscura (*darknet*) para evitar ser rastreados, los agresores pueden trabajar en un entorno relativamente seguro para ellos.

5.4. Coerción y extorsión sexual en línea

La mayoría de los abusos sexuales a menores están cometidos por un familiar u otra persona próxima a la víctima. No obstante, sobre todo en el caso de niños más mayores y adolescentes, esta amenaza proviene de la explotación sexual en línea por alguien que nunca han conocido en persona.

Los agresores sexuales en línea pueden obtener material comprometido de distintas formas a través de la coerción y extorsión de los menores. En la mayoría de los casos la coerción y extorsión requiere que el agresor tenga en su posesión material comprometido de la víctima y amenace con publicar este contenido. Según datos, tanto las víctimas como los agresores en casos de extorsión sexual son cada vez más jóvenes.

5.5. Abusos sexuales a menores en directo

Una forma de explotación sexual de menores en línea especialmente compleja es la difusión en directo de abusos sexuales a menores conocido con el término LDCA (por sus siglas en inglés). Esta forma de explotación no solo está compuesta por transmisiones internacionales en directo, también se producen difusiones nacionales.

LDCA es la forma comercial (de pago), más frecuente de explotación sexual de menores en línea. Los métodos de pago suelen estar compuestos por servicios de pago en línea, transferencias de dinero y centros de pago locales. El uso de monedas virtuales como el *bitcoin* no se ha extendido todavía en este sector debido a problemas para retirar las criptomonedas.

Así mismo se ha registrado un aumento en la cantidad de material autogenerado trasmitido en directo a través de aplicaciones de redes sociales con la posibilidad de verlo en directo a través de Facebook o Instagram.

5.6. Evolución y amenazas futuras

Debido al creciente acceso a internet de alta velocidad en distintas partes del mundo, es probable que la trasmisión de abusos sexuales a menores, tanto la difusión como el material autogenerado trasmitido en directo, aumente en el futuro. Los agresores sexuales de menores en línea continúan buscando métodos para evadir a las fuerzas de seguridad y la red oscura (*darknet*) puede facilitar la comercialización de CSE.

5.7. Recomendaciones

5.7.1. Cooperación

Cooperar con el sector privado, financiero y académico. Proporcionar ayuda a personas que tengan un interés sexual hacia niños y puedan controlar su inclinación a llevar a cabo abusos. Continuar la colaboración de las fuerzas de seguridad con empresas de pago para restringir el CSEM y LDCA.

5.7.2. Investigación

Investigar a administradores de grades foros que fomentan la seguridad operativa.

5.7.3. Prevención y educación

Campañas de prevención y educación sobre los riesgos.

6. FRAUDE EN LOS PAGOS

6.1. Conclusiones clave

- El *skimming* sigue prevaleciendo, dado que la banda magnética de las tarjetas se sigue utilizando.

- El abuso de los terminales de Puntos de venta (PoS por sus siglas en inglés) toma distintas formas: desde la manipulación de dispositivos hasta la adquisición fraudulenta de terminales nuevos.

- El fraude en las telecomunicaciones es un delito ya establecido, aunque sigue constituyendo un reto para las fuerzas de seguridad.

6.2. Fraude de tarjetas de pago

El *skimming* y el *shimming* siguen representando una amenaza, aunque tiene lugar con una frecuencia considerablemente menor gracias a la puesta en práctica de medidas de bloqueo geográfico. Las herramientas que se utilizan para llevar a cabo estas prácticas fraudulentas cada vez son más sofisticadas. Algunos Estados miembros han comunicado que la amenaza principal se produce en los países de Europa oriental y los Balcanes.

Los criminales siguen robando información de tarjetas de crédito en centros turísticos y en áreas geográficas donde no existe Europay, MasterCard o Visa (EMV). Estos ataques se producen en cajeros automáticos cuando los clientes desconectan la medida de bloqueo geográfico para asegurarse de que su tarjeta de crédito funciona en el extranjero.

Una vez ya se ha obtenido la información de las tarjetas de crédito, se suele vender en tiendas de tarjetas (ACS por sus siglas en inglés) o en mercados de la *darknet*.

Un gran número de Estados miembros ha comunicado que los criminales también utilizan tarjetas con origen en Estados Unidos o India para ejecutar cobros múltiples en un periodo de tiempo relativamente corto.

Otra cuestión importante en 2017 ha sido el fraude en teléfonos móviles. En mayo, la Policía Nacional española y la Guardia Civil interceptaron a 24 individuos durante una operación internacional de fraude en teléfonos móviles que afectaba a España y Francia.

En cuanto al abuso de terminales de PoS, los criminales utilizan distintos *modus operandi*. El más conocido es la manipulación del terminal para captar los datos personales de los clientes, mientras que un método alternativo que las fuerzas de seguridad han denunciado es la creación de empresas falsas para registrar PoS.

6.3. Fraude fuera de tarjetas de pago

A medida que las transacciones en línea dentro del ámbito del comercio electrónico (*e-commerce*) han aumentado, también lo han hecho los abusos de datos personales de las tarjetas en el fraude fuera de tarjetas de pago. Así lo indican también informes del Consejo Europeo de Pagos (EPC por sus siglas en inglés).

La presencia de un gran número de casos desconocidos sigue resultando una amenaza para realizar una cobertura exacta de la prevalencia del problema. Muchas víctimas suelen denunciar estos casos a las instituciones financieras en lugar de a las fuerzas de seguridad.

En relación con los diferentes sectores en los que se localiza el fraude fuera de tarjetas de pago, la cobertura de los Estados miembros está fragmentada, lo que impide que se pueda dar una respuesta conjunta a este tipo de casos. En el sector de la hostelería, algunos Estados miembros han comunicado niveles estables de fraude, así como en el sector del transporte el fraude relacionado con billetes de avión.

6.4. Otros tipos de fraude en los pagos

Como se mencionó en el anterior informe, se han detectado varios intentos de ataques a cajeros automático, tales como el método "jackpot" y los ataques a la "black box", aunque la mayoría no suelen culminar. El primero de estos ataques permite extraer dinero de un cajero automático sin necesidad de utilizar una tarjeta de crédito o débito a través del robo de datos de sus propietarios, mientras que en el segundo los delincuentes conectan un dispositivo al cajero automático para enviar comandos al dispensador sin tener que introducir una tarjeta.

El fraude en las telecomunicaciones, que existe desde hace tiempo, había pasado desapercibido para las fuerzas de seguridad hasta este momento. Agencias como la Asociación del control del fraude en las comunicaciones (CFCA por sus siglas en inglés) han alertado sobre el Fraude internacional de coparticipación (IRSF por sus siglas en inglés), un ataque donde se interceptan las tarjetas SIM o los sistemas de centralitas telefónicas (PBX por sus siglas en inglés) y el atacante recibirá una parte de los ingresos de las tasas de terminación móvil del dueño. En la actualidad, agencias y servicios de telecomunicaciones han comenzado a cooperar para terminar con este tipo de ataques.

6.5. Evolución y amenazas futuras

En enero de 2018, la Directiva de Servicios de Pago 2 (PSD 2) entró en vigor, e introdujo nuevas oportunidades para luchar contra las amenazas cibercriminales. Esta directiva obliga a las instituciones financieras a conceder acceso a sus cuentas bancarias a terceras personas siempre que tengan el permiso de sus clientes. Esto se conseguirá a través de una Interfaz de programas de aplicación (API por sus siglas en inglés), que, sin embargo, puede concluir en escenarios peligrosos como solicitudes fraudulentas de terceras personas para recibir datos bancarios.

6.6. Recomendaciones

A pesar de su presencia desde hace años, el fraude en las telecomunicaciones puede representar una nueva área de cibercrimen para las fuerzas de seguridad. Para investigar este tipo de ataques se requerirá la colaboración y formación adicional de la industria de las telecomunicaciones.

7. MERCADOS CRIMINALES EN LA RED

Los mercados criminales en la red, tanto en la *surface web* como en la *dark web*, brindan a los proveedores criminales la oportunidad de facilitar todo tipo de materiales ilícitos.

7.1. Conclusiones principales

- El ecosistema del mercado de la *darknet* es muy inestable. Si bien las fuerzas de seguridad cerraron tres principales mercados en 2017, al menos nueve más tuvieron que cerrar, bien forma espontánea o porque el administrador huyó con el dinero almacenado del mercado.

- El inevitable cierre de grandes mercados globales de la *darknet* ha generado un aumento de tiendas al por menor y mercados secundarios dirigidos a nacionalidades específicas.

7.2. Mercados en la red oscura (darknet)

Los mercados criminales en la red permiten un fácil acceso a una amplia gama de productos y servicios ilícitos que, a su vez, son factores clave para el desarrollo de otros crímenes.

El año pasado, las fuerzas de seguridad cerraron tres grandes mercados de la *dark web* que comprendían el 87% de la actividad total en el mercado de la *darknet*. Se llevaron a cabo dos operaciones importantes dirigidas por el FBI, la Administración para el Control de Drogas (DEA por sus siglas en inglés) y la Policía Nacional de Países Bajos, y la colaboración de Europol y otras fuerzas de seguridad. AlphaBay era uno de los mercados más grandes hasta la fecha, contando con drogas ilegales, químicos tóxicos, documentos y productos falsos, *malware*, armas de fuego y servicios fraudulentos. El segundo y tercer mercado más grandes en la *darknet* eran RAMP y Hansa respectivamente.

Debido al cierre de mercados en la *darknet*, vendedores y consumidores buscan otros mercados, no obstante, el nivel de actividad a decrecido. Como resaltan algunos Estados miembro, otra consecuencia del cierre de estos grandes mercados es el aumento de mercados secundarios. Así mismo, el comercio en línea de drogas continúa dominando los mercados en la *darknet*, mientras que el comercio de productos falsificados continúa estando en la *surface web*. Por último, el comercio de armas comienza a florecer en la *dark web*.

7.3. Evolución y amenazas futuras

En años anteriores hemos sugerido que las continuas y eficaces medidas de las fuerzas de seguridad contra los mercados en Tor, forzarán a que estos mercados cambien a otro tipo de red descentralizada como I2P o Freenet. No obstante, incluso con el cierre de los tres mercados más grandes, la voluntad o la necesidad de cambiar del territorio familiar de Tor a otro entorno digital posiblemente más seguro no parece estar presente.

7.4. Recomendaciones

7.4.1. Coordinación

Una medida de respuesta eficaz consiste en una respuesta horizontal coordinada con la participación de expertos.

7.4.2. Estrategia global

Es preciso desarrollar una estrategia global para abordar el mercado ilícito en la *dark web*.

8. LA CONFLUENCIA DEL CIBER Y EL TERRORISMO

8.1. Conclusiones clave

- El Estado Islámico sigue utilizando internet para propagar y motivar a personas a que cometan actos terroristas.

- Las fuerzas de seguridad y la acción de la industria han llevado a los seguidores del ISIS a utilizar aplicaciones de mensajería encriptada que ofrecen grupos privados y cerrados, la *dark web* y otras plataformas que no están lo suficientemente capacitadas para interrumpir su actividad.

- A pesar de que los seguidores del ISIS han demostrado su disposición para adquirir herramientas y servicios de ciberdelincuencia de la economía sumergida, su capacidad interna es limitada.

8.2. El uso de internet por grupos terroristas

Durante los últimos años, la campaña de que han llevado a cabo las fuerzas de seguridad junto con los proveedores de servicios digitales (OSP) ha obligado a los seguidores del ISIS a esconderse. En el año 2016, se observó una transición de plataformas como Twitter o Facebook hacia plataformas de mensajería encriptadas como Threema, Signal o Telegram. Como parte de la lucha armada contra el ISIS, las agencias de las fuerzas de seguridad han desplegado ciberoperaciones proactivas contra el alcance de estos grupos en la red.

El ISIS es más sofisticado tecnológicamente que otros grupos terroristas anteriores, y ha contactado con expertos en tecnología para reclutarlos. Los seguidores del ISIS han compartido videos tutoriales que ofrecen consejos sobre la encriptación o que tocan temas como el alcance de la vigilancia de gobiernos hostiles. Además, también han luchado contra el cierre masiva de las cuentas seguidores del ISIS a través de voluntarios que han creado un conjunto de cuentas en Facebook, Twitter, Gmail e Instagram.

A pesar de la preocupación que ha surgido en estos últimos años sobre los posibles ciberataques que podrían realizar grupos terroristas, los hackers del ISIS y sus herramientas tecnológicas siguen siendo limitadas y los seguidores del ISIS solo han llevado a cabo un pequeño número de ataques de desfiguración.

Las criptomonedas representan una oportunidad de mover fondos a través de fronteras para los grupos terroristas, para evitar el escrutinio tradicional de los bancos. A finales del año 2017, los seguidores del ISIS iniciaron una campaña masiva de donaciones de criptomonedas tanto en páginas web del grupo como en sus chats para apoyar su causa.

Sin embargo, a pesar de su potencial, ninguno de los ataques que se perpetraron en terreno europeo parece haber sido financiado con criptomonedas. El uso de estas por grupos terroristas solo ha incluido transacciones de bajo nivel, ya que sus principales fuentes de financiación siguen proviniendo de los servicios bancarios y el envío de dinero.

8.3. Recomendaciones

Los grupos terroristas seguirán utilizando las plataformas digitales y las redes sociales para distribuir su propaganda, reclutar a nuevos simpatizantes, obtener fondos y organizar ataques. A pesar de que resulta imposible eliminar la propaganda terrorista en internet, sí que se puede

minimizar su impacto. Para ello se deben llevar a cabo dos estrategias separadas, aunque muy relacionadas:

Por un lado, se deben contrarrestar las operaciones de reclutamiento y de propaganda en internet. Esto requerirá una coordinación y un intercambio de información mayores dentro de las agencias de fuerzas de seguridad, así como una cooperación mejorada dentro del sector privado.

Por otro lado, se debe investigar más la capacidad de los grupos terroristas para llevar a cabo ciberataques.

Estas dos estrategias se refuerzan la una a la otra, ya que alterar los intentos de propaganda en internet dificultará el acceso terrorista a la experiencia técnica humana, la financiación y a las herramientas ciber.

9. FACTORES TRANSVERSALES DE LA DELINCUENCIA

Los factores transversales de la delincuencia son aquellos que afectan, facilitan o, por el contrario, contribuyen en numerosas áreas de delincuencia, pero estos no son necesariamente delictivos. Algunos incluyen elementos como los métodos de comunicación, finanzas, encriptación, internet de las cosas e ingeniería social.

9.1. Conclusiones principales

Estafadores de África Occidental han adoptado nuevas técnicas de fraude, incluyendo aquellas con un aspecto técnico más sofisticado como BEC (*business email compromise*). El *phishing* continúa aumentando y se mantiene como la forma principal de ingeniería social. Muchas de las estafas tradicionales como la estafa de soporte técnico, la estafa de pago por anticipado o la estafa romántica, todavía continúan afectando a un número considerable de víctimas. El aumento de los protocolos de encriptación HTTPS por páginas *phishing* consigue engañar a las víctimas para que crean que la página web es legítima y segura. Los ciber ataques que habitualmente se centraban en instrumentos financieros tradicionales están atacando ahora comercios y usuarios de criptomonedas. A pesar de que la cuota del *bitcoin* está disminuyendo en el mercado de las criptomonedas, sigue siendo la cirptomoneda predominante en las investigaciones sobre ciberdelincuencia.

9.2. Ingeniería social

Los ataques de ingeniería social pueden adoptar muchas formas. Por un lado, pueden ser ataques que creen un pretexto para convencer a las víctimas de divulgar información o actuar de forma inusual. Por el otro, pueden ser un componente clave de un ataque mucho mayor en el que las víctimas instalan inconscientemente un *malware* al abrir el enlace de un correo electrónico malicioso o un link de una página web maliciosa. Estos tipos de ataques incluyen el *phishing* (por correo electrónico) que se mantiene como la principal metodología, el *vishing* (por teléfono) y el *smishing* (por SMS). Así mismo, el BEC abarca tanto el delito ciber dependiente como el delito cibernético. A pesar de que la mayoría de los ataques mencionados son relativamente nuevos, la ingeniería social no es una amenaza nueva y continúa utilizando formas de fraude tradicionales como estafa de soporte técnico, la estafa de pago por anticipado o la estafa romántica.

9.3. Finanzas criminales

Ahora, los usuarios de criptomonedas también son víctimas de hackers.

El aumento de la demanda de criptomonedas ha resultado en la proliferación de servicios de tipo de cambio operando a escala mundial. Estas entidades no solo mantienen los fondos de sus propias criptomonedas para el comercio, sino que con frecuencia también mantienen los fondos de compradores de criptomonedas. Estas entidades son sin lugar a duda un blanco perfecto para delincuentes con intereses económicos. El *bitcoin* continúa siendo la forma de pago más extendida para servicios ilícitos en el ámbito de la ciberdelincuencia, aunque otros métodos de pago se siguen utilizando como monedas virtuales centralizadas, sistemas basados en bonos, sistemas de tarjetas o tarjetas de prepago. A su vez, las mulas de dinero siguen siendo un componente principal en el blanqueo de capitales de origen ilícito.

9.4. Desafíos comunes para las fuerzas de seguridad

El desafío más importante al que nos vamos a enfrentar es la pérdida de datos. En primer lugar, la tecnología 5G de la nueva generación de teléfonos móviles inhibirá la atribución e interpretación legal. En segundo lugar, la base de datos WHOIS no cumple con las normas establecidas por la GDPR de la UE y las medidas temporales dificultan la identificación e investigación del crimen online. Desde el 25 de mayo de 2018 las fuerzas de seguridad necesitan iniciar un proceso legal y conseguir una autorización especial de un fiscal o juez para obtener información de registrantes de nombres de dominio.

9.5. Evolución y amenazas futuras

A pesar de que el uso de kits de *exploit* está en declive o en disminución en comparación con años anteriores, continúa estando presente y lo más seguro es que permanezca así mientras haya vulnerabilidades que se puedan explotar.

África Occidental tiene una larga historia de fraudes de ingeniería social y la ciberdelincuencia está aumentando.

Los propios bancos se están familiarizando con el uso de criptomonedas y estas propias entidades están siendo víctimas de ataques a manos de hackers. A pesar de que el *bitcoin* es la criptomoneda más usada en la mayoría de los delitos cibernéticos, no se descarta el uso de otras monedas con más privacidad.

9.6. Recomendaciones

9.6.1. Educación

La mejor defensa contra la ingeniería social es educar a las posibles víctimas. Las fuerzas de seguridad deberán por lo tanto continuar apoyando las campañas de prevención y sensibilización con el objetivo de concienciar sobre las amenazas.

9.6.2. Cooperación

Debido a la ingeniería social de fraude por parte de grupos de crimen organizado en África Occidental que amenazan a los ciudadanos de la UE, la cooperación con estados de África Occidental es imprescindible para combatir estas amenazas.

9.6.3. Prevención y Concienciación

Se deberán adaptar las campañas de prevención y concienciación para incluir información de cómo pueden proteger los usuarios de criptomonedas sus datos y carteras.

9.6.4. Relaciones de confianza

Las fuerzas de seguridad deberán entablar relaciones de confianza con cualquier empresa que esté usando criptomonedas en su jurisdicción.

9.6.5. Herramientas de investigación y entrenamiento

Los Estados miembros deberán invertir en herramientas de investigación y entrenamiento para combatir delitos cibernéticos.

10. LA DISTRIBUCIÓN GEOGRÁFICA DE LA CIBERDELINCUENCIA

10.1. América

En América, en particular en Estados Unidos, no solo se originan numerosos ciberataques a gran escala, sino que también se producen ciberataques con base nacional o internacional. La cobertura industrial demuestra que Estados Unidos y hasta cierto punto Canadá son dos países contra los que se producen ataques de *ransomware*.

En América Latina también se ha detectado una falta de ciberseguridad. En el caso de Brasil, la falta de legislación sobre la ciberdelincuencia ha provocado que este país sea el primer objetivo y la principal fuente de ciberataques en América Latina (un 54% de los ataques tienen origen nacional). Asimismo, México es el país que más ciberataques está sufriendo en los últimos años después de Brasil.

La amenaza más importante que se origina en el continente americano desde una perspectiva de las fuerzas de seguridad consiste en los numerosos aspectos relacionados con el fraude en los pagos.

10.2. Europa

La mayoría de las amenazas ciber que afectan a Europa siguen surgiendo dentro de sus fronteras. El énfasis actual en el uso del correo electrónico como medio de ataque se demuestra en las tendencias que resalta la industria. En Austria, Alemania, Hungría, Italia, Rusia, España y el Reino Unido se perpetran la mayoría de los ataques con correos electrónicos maliciosos que contienen *malware*. Por otro lado, Irlanda, Noruega y Suecia han sufrido las mayores cifras mundiales de correos electrónicos con URL maliciosos. Países Bajos, Hungría, Portugal y Austria son los países que más han sufrido el phishing en los correos electrónicos.

Estos ataques también demuestran que una proporción significante de los ataques mundiales que se originan en dispositivos electrónicos vienen de Europa. Las fuerzas de seguridad han resaltado una amplia variedad de ciberataques que emanan de otros países de la región, aunque también se ha hecho hincapié en aspectos relacionados con el fraude en los pagos. En este último tema, Bulgaria y Rumanía desempeñan un papel clave.

10.3. Oriente Medio y África

En los informes de años anteriores, se ha resaltado la creciente importancia de África como fuente de ciber y de delitos ciberdependientes. Estas tendencias las han reiterado Estados miembros al resaltar la importancia de los Grupos del Crimen Organizado (OCG por sus siglas en inglés) y la sofisticación de sus ciberataques. A pesar de que las estafas de ingeniería social “tradicionales” todavía prevalecen los delitos asociados con esta región, la ingeniería social combinada con los

ataques que incluyen *malware* ha aumentado exponencialmente. Por último, se ha detectado también el creciente fraude en los métodos de pago, así como el Material de Explotación Sexual de Menores (CSEM) en la región de África.

10.4. Asia

Teniendo en cuenta la cobertura industrial, los ciberataques que se han dirigido hacia los países asiáticos siguen un perfil y metodologías distintas comparados con los que se perpetran en Europa. A pesar de que los correos electrónicos con adjuntos maliciosos siguen prevaleciendo en muchos países del sudeste asiático, el uso de los URL maliciosos apenas tiene lugar. Sin embargo, se observan tendencias altas de *phishing* en esta región, y en China se dan numerosos casos de *spam*. En definitiva, la región asiática constituye una de las más susceptibles a ciberataques; a pesar de que Estados Unidos figure como el primer objetivo, siete países asiáticos aparecen en los diez más susceptibles de ataques.

10.5. Oceanía

Como aparece en varios informes anteriores, a pesar de que Oceanía todavía sigue sufriendo ciberataques a nivel nacional, no suele aparecer en investigaciones de la Unión Europea. Los ciberataques más importantes que se dan en esta región reflejan aquellos de la UE: *ransomware*, *malware* para el robo de datos, DDoS, PBX o ingeniería social entre otros.