LaSEI
School of Economic Intelligence & International Relations
Escuela de Inteligencia Económica y RRII
Universidad Autónoma de Madrid
2021
Vol. 3, n 3, pp. 25 - 34
ISSN: 2659-9805
Editor in-Chief: Javier Oubiña
JOURNAL OF ECONOMIC & BUSINESS INTELLIGENCE
Universidad Autónoma de Madrid UAM

CRIME-AS-A-SERVICE: INTELIGENCIA COMPETITIVA EN EL LADO CIBERCRIMINAL PARA LA ERA POST-COVID19

Eva Moya[1] y Leticia Lanuza[2]

Resumen

Fruto de la observación del ecosistema cibercriminal con fines profesionales, llegamos a la conclusión de la existencia de un esquema que llamamos "Cadena de Valor Cibercriminal" basado en el modelo de negocio del Crime-as-a-Service (CaaS). Siendo el cibercrimen, uno de los sectores que más ha crecido durante la pandemia, consideramos analizar su éxito para obtener las mejores prácticas que puedan ser aprovechadas en los negocios legítimos.

Palabras clave: Crime-as-a-Service, prácticas competitivas, crisis, post- Covid-19.

Abstract

As a result of observing the cyber-criminal ecosystem for professional purposes, we came to the conclusion that there is a scheme we call "Cyber-criminal Value Chain" based on the Crime-as-a-Service (Caas) business model. As cyber-crime is one of the sectors that has grown the most during the pandemic, we considered analyzing its success in order to obtain the best practices that can be used in legitimate businesses.

Keywords: Crime-as-a-Service, competitive practices, crisis, post-Covid-19.

1.Introducción

Hace ya varios años que se acuñó el término Crime-as-a-Services (CaaS) como concepto para definir un nuevo tipo de relaciones cibercriminales que están mucho más cerca del mundo de los negocios legítimos que de las relaciones sórdidas y oscuras propias del imaginario de la Deep Web y Darknet.

Relaciones regidas por los mecanismos más duros derivados de la oferta y la demanda, y el liberalismo más extremo; a través de los cuales, cada cibercriminal realiza un análisis de riesgos para determinar cuál será finalmente su exposición al delito.

[1] Eva Moya. Risk & Fraud Analysis Manager. MNEMO, Madrid, España. Contacto: moya.eva@gmail.com
[2] Leticia Lanuza. Risk & Fraud Analyst. MNEMO, Madrid, España. Contacto: laelanuza@gmail.com

Durante diez años, hemos estado observando el comportamiento cibercriminal y su evolución. Esta observación, fruto de la necesidad profesional de defender a nuestros clientes nos ha permitido diseñar un esquema de comportamiento basado en la evolución del CaaS. Inspiradas en la definición del profesor Porter sobre la Cadena de Valor como ventaja competitiva, hemos decidido bautizar este esquema como la "Cadena de Valor Cibercriminal". El hecho de que hayamos considerado escribir sobre ello ahora, está en relación con el aumento exponencial de los ciberataques y la aparición de nuevos actores en este sector, como consecuencia de la transformación digital a la que se ha visto sometido el mundo con la pandemia de la covid-19. Sin duda, el cibercrimen ha sido uno de los sectores que más ha crecido al respecto. Por ello, hemos querido analizar cuáles podrían ser las claves más relevantes para este despegue y reflexionar si alguno de sus mecanismos son lo suficientemente innovadores como para desvelar aspectos que pudieran ser aprovechados bajo los parámetros de la inteligencia competitiva y bajo el amparo del marco legal.

Somos conscientes de que esta reflexión puede herir sensibilidades y esperamos que se comprenda su finalidad como un ejercicio de análisis de inteligencia cuyo objetivo persigue el apoyo a la supervivencia de las empresas en este periodo tan difícil.

Para la elaboración de nuestra cadena de valor cibercriminal, nos hemos centrado única y exclusivamente en los delitos económicos y fraude. Por supuesto, las conclusiones se mantienen siempre dentro del amparo legal, pues reiteramos que no es objeto de esta reflexión extrapolar las prácticas delictivas como unas buenas prácticas para los negocios legítimos.

2.Crime-as-a-Service (CaaS)

2.1 El punto de partida.

El crimen en modo servicio es un término acuñado oficialmente por Europol en 2014 para referirse a una nueva modalidad de cibercrimen basada en el intercambio de servicios entre cibercriminales[3]. Si bien es cierto que ya aparece mencionado en blogs de especialistas del sector en 2013. Sea como fuere, ya han pasado siete años desde que se identificó este modelo de negocio surgido en la Deep Web y Darknet.

Con los inicios de Internet, en los años 90, aparecieron los primeros delitos digitales realizados por lobos solitarios y bandas organizadas especializadas que disponían de todos los recursos, conocimientos y capacidades para cometerlos. En esta época de la denominada web 1.0 era imprescindible ser experto en todos los aspectos de los ataques informáticos, con un altísimo grado de conocimiento en las técnicas de ingeniería social, que adaptaban los mecanismos tradicionales de las estafas al ámbito digital.

La evolución desde uno de los primeros virus informáticos de mayor impacto, "I love you"[4], hasta las conocidas cartas nigerianas[5] fue realmente rápida y abrió a los criminales un océano azul[6] de oportunidades que apenas habían empezado a aprovechar.

Así, conforme Internet y los dispositivos que lo soportan han ido evolucionando, los cibercriminales han potenciado el I+D+I con la intención de ser mucho más eficientes en sus ataques, así como para descubrir nuevas oportunidades vinculadas al desarrollo de sus negocios.

La transformación digital a la que asistimos hoy día ha acelerado el interés de los cibercriminales por intensificar su explotación del negocio. Si bien, el CaaS era la adaptación lógica a la explotación de un negocio digital creciente, hoy día se ha convertido en la clave del desarrollo del mismo y augura en los próximos años una explosión en la generación de beneficios.

Así pues, lo frecuente ya no es que un grupo cibercriminal invierta todos sus recursos en el diseño, elaboración y ejecución de un ataque o robo, sino que la subcontratación de tareas, servicios y tecnología a otros criminales se convierte

[3] https://www.europol.europa.eu/newsroom/news/organised-crime-groups-exploiting-hidden-internet-in-online-criminal-service-industry

[4] Este conocido virus inundó las redes en 2000, llegando a ser capaz de infectar a más de 50 millones de ordenadores. Su creador, un estudiante filipino, lo lanzó como venganza porque la universidad había suspendido su tesis, en la que investigaba este tipo de desarrollos.

[5] Las cartas nigerianas son intentos de estafa a través de la internet. El estafador se hace pasar por una víctima en apuros y solicita la ayuda del receptor del email. La situación de desamparo es muy variada, pero el objetivo siempre es el mismo: pedir dinero para salir del apuro. En los últimos tiempos, los estafadores se hacen pasar por gente del entorno de la víctima con la intención de aportar más credibilidad a la estafa.

[6] La estrategia del océano azul fue publicada en 2005 de manos de W. Chan Kim y Renée Mauborgne. Esta estrategia pone el foco de atención en cómo los avances tecnológicos y la innovación permite crear nuevos negocios que todavía no se han explorado, reduciendo así los esfuerzos por competir en aquellos modelos tradicionales donde se hace muy complejo obtener rendimientos.

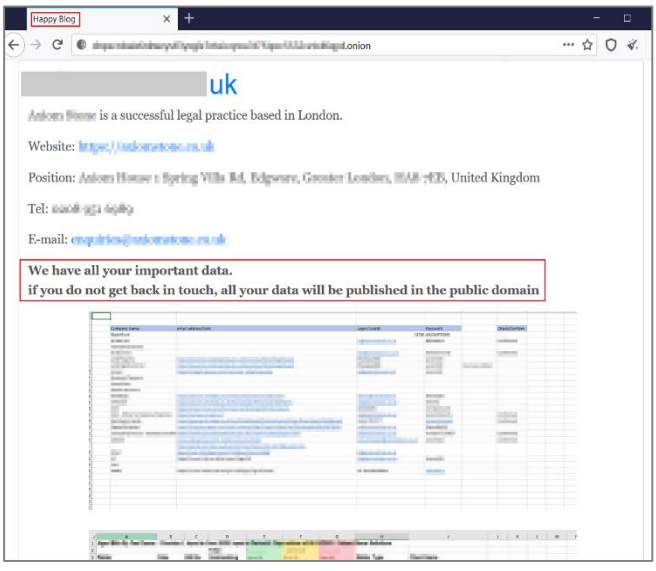
en la clave de la eficacia y eficiencia de sus procesos de negocio, minimizando además los riesgos derivados del mismo. En este nuevo entorno y bajo este esquema se hace posible estructurar los trabajos y relaciones, pudiendo llegar a establecer algunos paralelismos sorprendentes con el mundo de los negocios legítimos. En términos generales, así sería la cadena de valor cibercriminal del CaaS hoy en día:

2.1.1 Ejecución

Desarrollada por los cibercriminales que ejecutan directamente las campañas de ataque para monetizar la operación, es decir, representan a los "ladrones virtuales del dinero".

Ataques	Descripción	Equivalente legal
Secuestro de datos y/o la operación.	Se cifran los datos y/o los procesos de la operación de la víctima a cambio de un rescate.	La ejecución de los cibercriminales se corresponde con las operaciones de cualquier compañía.
Chantaje.	Dos opciones principales: • Por interrupción continuada de la operación, bloqueando los sistemas hasta que se pague (DDoS). • Disponen de información sensible que si sale a la luz puede destruir personal y/o profesionalmente a los involucrados.	
Fraude.	Robo directo a las víctimas a través de la cuenta bancaria, la tarjeta, mediante estafas online, etc.	

Imagen 1: Blog de REvil para mostrar su chantaje



En los últimos meses ha aparecido una nueva modalidad que combina varios tipos de ataque, como es el caso de uno de los grupos criminales que se está haciendo más conocido: REvil. Este grupo combina el secuestro de datos con el chantaje de hacerlos públicos a través de su blog en la Deep Web.

En un caso típico llevado a cabo por el grupo REvil, los actores accederían a la red interna de la víctima (independientemente de su tamaño o sector) aprovechándose de vulnerabilidades de software cómo puede ser el CVE 2019-115107 o desarrollando una campaña de phishing con una ingeniería social elaborada que atrajera a las víctimas a interactuar con el correo electrónico malicioso.

Una vez dentro de la red interna, los actores buscan información relevante de la víctima que les sirva en un futuro para extorsionar a la organización afectada. Cuando los cibercriminales consideran iniciar su ataque, empiezan secuestrando la operación y/o datos a cambio de un rescate. Paralelamente, en su blog de la Deep Web, Happy Blog, los cibercriminales exponen a sus víctimas y el chantaje.

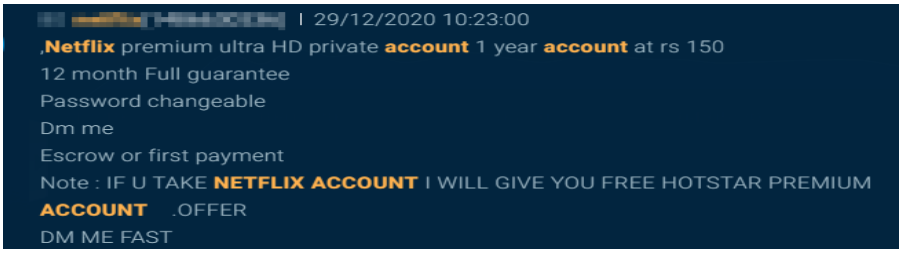
7 www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2019-11510

2.1.2 Venta de datos y/o información

Uno de los activos más valiosos para los cibercriminales son los datos y/o información, pues con ellos elaboran las campañas de ejecución que permitirá la monetización. Este tipo de criminales gana dinero poniendo a la venta los datos obtenidos. En el pasado, ganaban "al peso", pero hoy día se valora mucho más la calidad, hasta tal punto que los grupos criminales empiezan a utilizar indicadores para determinar la calidad de sus productos y poder diferenciarse de la competencia. Algunos de los más relevantes son los siguientes:

Tipo de dato	Descripción	Equivalente legal
Credenciales.	Robo de usuario y contraseña a través de ataques a grandes filtraciones de bases de datos.	Documentalistas y gestores de la información que manejan y mantienen las bases de datos que contienen el conocimiento de las compañías.
Tarjetas y credenciales bancarias.	A través de técnicas de phishing y/o robo de bases de datos de tiendas virtuales. Es uno de los negocios de mayor auge con la transformación digital.	
Documentos.	Especialmente vinculados a espionaje, como por ejemplo relacionados con la vacuna contra la COVID-19.	
Acceso a servicios.	Por ejemplo, robo de cuentas de servicios como Netflix.	
Configuraciones técnicas.	Ya sea para disponer información para futuros ataques, o para emular las medidas de seguridad biométricas, basadas en fingerprint.	

Imagen 2: ejemplo de venta de datos



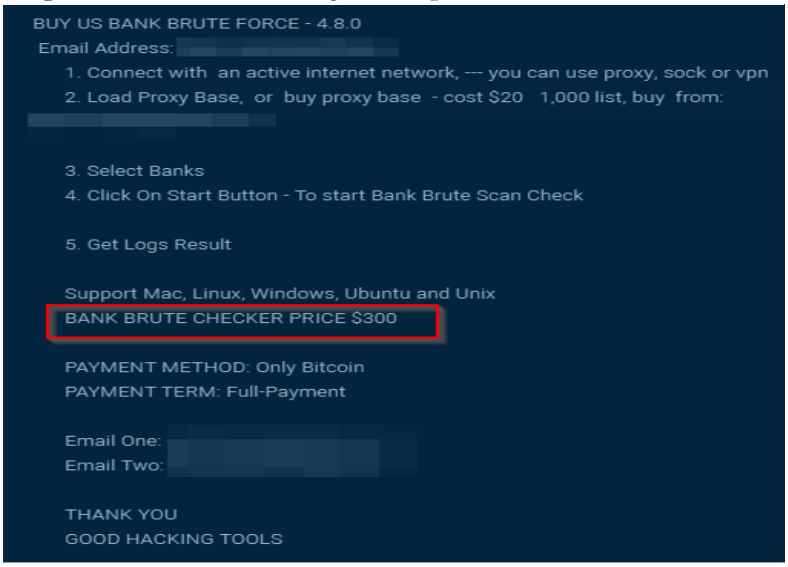
2.1.3 Desarrollo tecnológico e infraestructura

Desarrolladores informáticos e ingenieros especializados en crear toda la tecnología e infraestructura necesaria para llevar a cabo los ciberataques con éxito. Los más relevantes a día de hoy son:

Tipos	Descripción	Equivalente legal
Desarrolladores de malware y/o exploits para vulnerabilidades.	Especialistas en el desarrollo de malware avanzado y/o kits de consumo fácil por parte de ejecutores que no tengan conocimiento alguno. A día de hoy, son programas tan sencillos, que prácticamente permiten lanzar una campaña sólo con pulsar un botón.	Ingenieros y técnicos de sistemas. Incluye un alto componente de desarrollo de I+D+I.
Alojamiento para páginas fraudulentas.	Grandes granjas de servidores especializados en alojar páginas fraudulentas para phishing, estafas y cualquier vehículo necesario para cometer el delito. Son difíciles de localizar y	Servicios de alojamiento de páginas web.

	más aún de desactivar, pues suelen estar en regiones con legislaciones laxas.	Servicios de centralita y atención al cliente externalizados.
Call Center fraudulentos.	Desde hace un tiempo se han vuelto a poner de moda las llamadas telefónicas fraudulentas, ya sea para el fraude al CEO o para campañas masivas contra los ciudadanos, cada vez más se hace necesario disponer de servicios falsos de "atención al cliente".	

Imagen 3: anuncio de venta de kit para conseguir accesos a cuentas bancarias



Ejemplo de venta de un desarrollo de fuerza bruta contra cuentas bancarias.

En este anuncio, además se puede observar cómo el kit resulta de sencillo manejo, ya que en cinco pasos y con unos pocos conocimientos se puede conseguir el acceso a una cuenta bancaria.

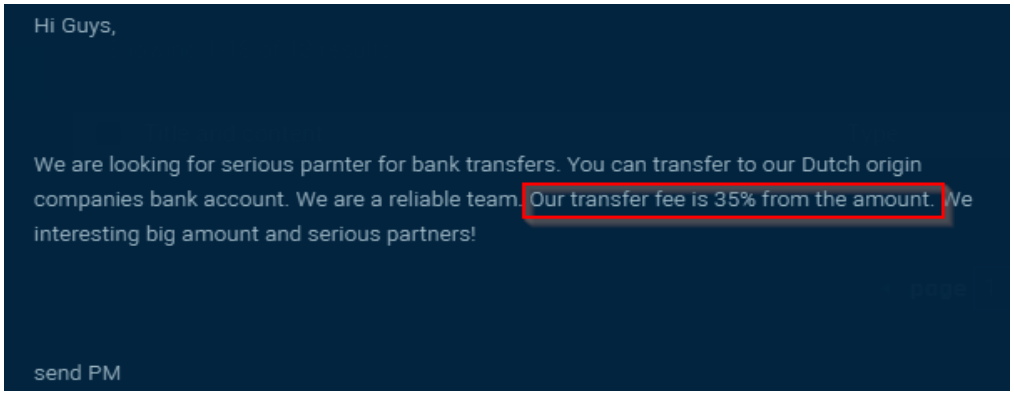
Por otro lado, añaden la versión de la herramienta, para futuros desarrollos y actualizaciones de la misma, igual que cualquier herramienta legítima a la venta.

2.1.4 Gestión del talento

Son aquellos cibercriminales especializados en buscar talento necesario para configurar los grupos de trabajo o los ataques puntuales.

Necesidad	Descripción	Equivalente legal
Identificación de partners.	Para localizar aquellos grupos que puedan ofrecer los mejores servicios que necesita el cibercriminal. Suelen actuar como enlaces a cambio de una comisión.	Gestor de proveedores Captación de talento. Recursos Humanos.
Selección de talento para el grupo.	Encargados de localizar a los mejores recursos para un proyecto concreto o para formar un grupo estable. Lo realizan a través de redes de confianza o anuncios directos.	
Gestión de mulas.	Tener una buena red de mulas es imprescindible para el lavado de dinero. En este sentido, pueden llegar a disponer incluso de decenas de mulas gestionadas a través de falsas páginas de ofertas de empleo. Con un solo clic, pueden activar a la mula rápidamente. En otras ocasiones, simplemente ofrecen sus servicios de mula mediante anuncios directos.	

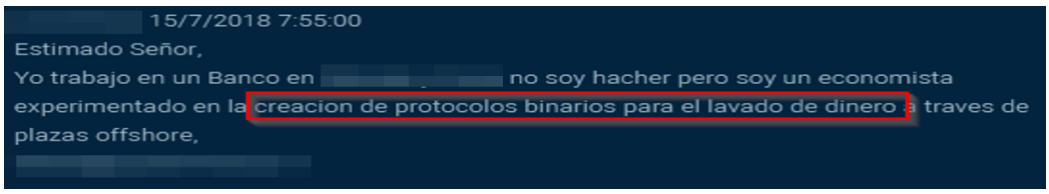
Imagen 4: anuncio de búsqueda de parters para mover gran volumen de dinero



2.1.5 Lavado de dinero

Criminales o cibercriminales que ofrecen sus servicios a otros grupos para el lavado de dinero y "cobro" seguro de las ganancias derivadas del delito.

Imagen 5: anuncio de oferta para lavado de dinero



2.2 Subservicios especializados (XaaS).

Debido al aumento y especialización cada vez más creciente del CaaS, han aparecido subservicios más especializados según las técnicas de ataque utilizadas para el robo del dinero. En este sentido se pueden encontrar grandes servicios, entre otros, como:

- **Malware-as-a-Service (MaaS).** Entendido como la venta de diferentes tipos de malware a medida del consumidor. Los cibercriminales desarrollan constantemente malware que ponen a la venta para obtener un beneficio económico de su trabajo sin exponerse a la realización de un ciberataque.
- **Ransomware-as-a-Service (RaaS).** Comprendido dentro del MaaS, el RaaS es una de las modalidades de cibercrimen al servicio que más ha crecido en los dos últimos años. En este sentido, los desarrolladores de ransomware han creado incluso programas de afiliación permitiendo a terceros expandir el malware a cambio de una suscripción mensual. [8]
- **Data-as-a-Service (DaaS).** Este es el servicio más extendido en el panorama cibercriminal y es que comprende la puesta en venta de todo tipo de información, ya sea personal (DNIs, fotos, correos electrónicos etc.) bancaria (tarjetas de crédito y débito), confidencial (documentos internos de empresas) entre otros.
- **Money-Laundry-as-a-Service (MLaaS).** Dentro del ecosistema de fraude, los cibercriminales ponen al servicio mulas que realicen los procesos de blanqueo de dinero, bien sea de forma física u online a través de transferencias bancarias.
- **Hacking-as-a-Service (HaaS).** Uno de los servicios más peligrosos que se pueden encontrar son los de hackeo al servicio del consumidor. Si bien puede comprender algo sencillo como el compromiso de una cuenta de correo electrónico, los grupos organizados que ofrecen estos servicios tienen altas capacidades para llegar a crear un vector de entrada en la entidad que el consumidor desee a cambio de un alto precio. Ejemplo de uno de estos anuncios en la Deep Web.

[6] unaaldia.hispasec.com/2020/04/el-ransomware-lockbit-toma-ejemplo-de-revil-y-maze-para-mantenerse-actualizado.html

2.3 Tipos de organizaciones cibercriminales.

Actualmente existe un reflejo similar en la estructura organizacional de los negocios criminales al comportamiento de los negocios legales. Una adaptación que cada vez se asemeja más y aprovecha toda la flexibilidad de las distintas organizaciones.

Flexibilidad es la palabra clave para el éxito de las organizaciones cibercriminales. Ya sean grandes o pequeñas, cibercriminales independientes o colaboradores; la adaptabilidad al entorno y los cambios de negocio, junto con una gran flexibilidad en el desarrollo del mismo les permite optimizar al máximo los esfuerzos, a la vez que reducen los riesgos.

Incluso en el caso de los grupos cibercriminales creados o financiados por estados de países no democráticos, mantienen cierta flexibilidad derivada de cierta independencia en el desarrollo de sus operaciones.

De esta manera se puede tener en cuenta los siguientes tipos de cibercriminales que operan en el entorno, siguiendo las definiciones de la Convención de las Naciones Unidas contra la delincuencia Transnacional[9].

- **Lobos solitarios o grupos estructurados**: vienen a ser el equivalente de los autónomos. Son cibercriminales que pueden participar en todas las actividades o colaborar puntualmente para un objetivo concreto. Al igual que sucede con los autónomos, en relación a la progresión dentro del negocio, y dado que el CaaS exige una reputación elevada para poder acceder a los mejores recursos, estos perfiles van desarrollándose poco a poco, primero con pequeños proyectos hasta demostrar su valía y llegar a ser requeridos por organizaciones más grandes. En el caso de los grupos estructurados conformados por cibercriminales independientes, simplemente se agrupan para un objetivo común, una vez conseguido se disuelven, por lo que no hay continuidad en el tiempo.
- **Pequeños y Grandes grupos organizados**: estos grupos son estables, es decir, se han formado con la intención de desarrollar el negocio criminal a largo plazo. Sus miembros pueden estar repartidos por todo el mundo y no tienen por qué conocerse físicamente. Dado que lo más importante en el ámbito cibercriminal es conseguir relaciones de confianza, este tipo de grupos limitan la rotación de sus miembros. Aunque en ocasiones, hemos asistido a pequeñas escisiones que se han separado para formar otros con otros objetivos.
- **Estados nación:** en ocasiones los servicios gubernamentales de diferentes países contratan o forman unidades específicas de cibercriminales que trabajan de forma coordinada y estructurada al servicio de los intereses del país en cuestión. Estos grupos suelen contar con altas capacidades técnicas para realizar intrusiones en entidades de países extranjeros, por lo que suelen estar categorizados como APT (Advanced Persistent Threat) y representan una de las ciberamenazas con más riesgo en la actualidad por su capacidad organizativa y las herramientas que tienen a su disposición. Existen diferentes motivaciones por las que estas unidades se crean, pudiendo encontrar grupos destinados a la obtención de un beneficio económico para el país (grupo Bluenoroff[10] proveniente de Corea del Norte), grupos dedicados al ciberespionaje (APT 41[11] proveniente de China) o grupos dedicados al sabotaje (APT 33[12] proveniente de Irán).

3.Fortalezas del negocio cibercriminal

Sin tener en cuenta la flexibilidad que permite trabajar al margen de la ley, hay algunos elementos destacables que se pueden analizar para una reflexión constructiva de "buenas prácticas" que inspiran la cadena de valor cibercriminal.

[9] www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

[10] apt.securelist.com/apt/bluenoroff

[11] www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

[12] www.cfr.org/cyber-operations/apt-33

3.1 Adaptación al entorno

Uno de los puntos fuertes del éxito cibercriminal es su capacidad para combinar tecnología, ingeniería social y una alta comprensión del entorno.

Esta inteligencia es aprovechada, no sólo para adaptarse a los acontecimientos previstos; sino que también disponen de la capacidad de adaptación frente a situaciones inesperadas.

Un ejemplo muy claro sobre cómo se preparan para acontecimientos previstos tiene que ver con el Black Friday. Al igual que las empresas se preparan para este tipo de eventos, los cibercriminales ponen en marcha toda la maquinaria que les permita obtener el mayor rendimiento posible. Así pues, por ejemplo, venimos observando en los últimos años cómo las semanas antes del evento, aumenta considerablemente el robo de tarjetas de pago online que se ponen a la venta días antes para ser aprovechadas durante este periodo de ofertas.

En la gráfica se observa dicho aumento. El primer pico corresponde a 15 días antes del Black Friday y el segundo a la semana durante la que tiene lugar.

Imagen 6: venta de tarjetas robadas para usar en el Black Friday en 2019

Por otro lado, en cuanto a la rápida capacidad de adaptación es cierto que, dado que este tipo de grupos no persigue una estrategia a largo plazo, dispone de una mayor capacidad para ser flexible, sin embargo esta adaptación ha sorprendido especialmente ante el reto de la pandemia COVID-19[13].

Dado el impulso a la transformación digital mundial a la que se ha visto sometido todo el tejido empresarial e industrial, los cibercriminales descubrieron un nuevo océano azul. Por ejemplo, hasta la fecha, las aplicaciones de videollamadas no eran objetivos tan relevantes como pasaron a serlo a raíz del aumento del teletrabajo, llegándose a crear nuevos tipos de ataques como el "Zoombombing".[14]

3.2 Vigilancia tecnológica e innovación.

Si en algo destacan los cibercriminales es en su constante monitorización de tecnología que les permita ser más eficaces y eficientes en sus ataques.

Este aumento creciente ha potenciado, sin duda, el desarrollo de la prestación de servicios vinculados al desarrollo de nuevas aplicaciones de la tecnología ya existente, e incluso de avances en la misma.

En cuanto a la aplicación de tecnología ya existente, sin duda el uso de los nuevos canales de comunicación como las redes sociales y el micro-chat son y seguirán siendo uno de los vehículos más interesantes para las estafas. También se adaptaron muy rápido cuando aparecieron los teléfonos móviles y los mercados de aplicaciones.

Cuanta mayor demanda hay de este tipo de servicios, más impulso cobran los desarrolladores. En este sentido se han visto ejemplos de ataques muy sofisticados, incluso utilizando inteligencia artificial para obtener el máximo rendimiento[15], algo que hasta la propia ENISA ha considerado como un escenario futuro a tener en cuenta[16].

13 www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

14 www.xataka.com/privacidad/zoombombing-nuevo-pasatiempo-internet-asi-incursiones-extranos-videollamadas-zoom-asi-difunden

15 retina.elpais.com/retina/2019/10/21/tendencias/1571641240_168585.html

16 www.enisa.europa.eu/publications/phishing

3.3 Creatividad: ejemplo de los programas de filiación.

Los cibercriminales han creado sus propios programas de afiliación para diversos malware como troyanos, botnets o ransomware, generando un nuevo modelo de negocio que permite a los usuarios participar de la distribución de estos ransomware. Esta tendencia se encuentra en incremento en los últimos años, habiendo sido adoptada por grandes grupos cibercriminales como los operadores de REvil.

Los programas de afiliación de un ransomware funcionan de manera similar a un programa de afiliación de cualquier marca:

- El desarrollador centra su actividad en actualizar y mantener las capacidades del malware y su infraestructura.
- Buscan afiliados, los cuales, por norma general, pagan una cuota inicial para ser incluidos en el programa.
- Los desarrolladores facilitan versiones del malware para que los afiliados se encarguen de modificar, adaptar y distribuir en diversas campañas.
- El beneficio resultado de los ciberataques es repartido en porcentajes entre el desarrollador y el afiliado, siendo la cifra más beneficiosa para el afiliado.

De esta manera, los desarrolladores reducen en gran medida el riesgo al que se exponen cuando se llevan a cabo los ciberataques, a cambio, reciben un menor porcentaje de los beneficios. Los operadores de REvil reparten los beneficios en un 30-70% a favor de los afiliados.

El afiliado será el encargado de distribuir el malware, lo que suele implicar acceder a subservicios del MaaS como alquileres de botnets, kits de explotación, herramientas de evasión de antivirus, herramientas de fuerza bruta o adquisición de listas de correos electrónicos.

Los afiliados son seleccionados cuidadosamente por los desarrolladores, habiendo diseñado unas condiciones o principios que se deben cumplir para acceder al programa de afiliados. De esto se desprende que los grupos que tienen programas de afiliación tienden a la sofisticación de sus procedimientos.

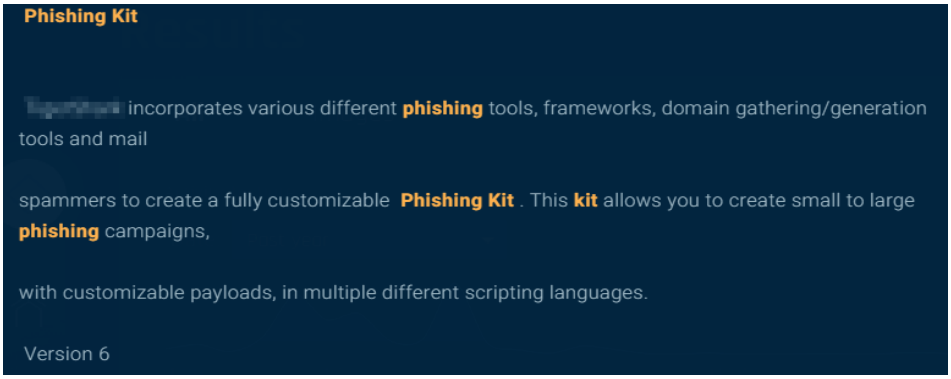
3.3 Soporte para *dummies*.

Otra clave del éxito de los ciberataques es la creación de entornos de soporte a los cibercriminales más novatos, lo que facilita el acceso a la realización de algunas campañas que no requieren de desarrollos excesivamente complejos.

En este sentido, por ejemplo, los desarrolladores preparan kits de malware con paneles de control cada vez más sencillos, donde el cibercriminal que va a ejecutar la campaña simplemente debe añadir la base de datos de emails que ha comprado a los vendedores de datos; así como aquellas imágenes que considere útiles para el engaño, y podrá poner en marcha la red de bots al instante.

Lo mismo sucede con los kits para montar phishing. En este caso, prácticamente se comportan como los constructores de páginas web legales que hay en el mercado, guiando al usuario sobre cada elemento que debe contener, así como ofreciendo consejos de cómo se puede optimizar para obtener el mejor rendimiento posible.

Imagen 7: anuncio de venta de kit sencillo para lanzar phishing



4. Conclusión: buenas prácticas de la cadena de valor cibercriminal

A lo largo de esta reflexión sobre los esquemas del Crime-as-a-Services (CaaS) y su cadena de valor cibercriminal, hemos podido llegar a la conclusión sobre una serie de elementos competitivos que permiten a unos cibercriminales tener más éxito comercial que otros:

- **Alto componente en I+D+I:** la innovación tecnológica está siempre presente. El aprovechamiento de los nuevos avances tecnológicos no se cuestiona y se analiza en profundidad cómo aprovecharlos.
- **Potenciación de los puntos fuertes y optimización de las palancas**: analizan cuáles son sus mejores capacidades y no desperdician ni un minuto en tareas ineficientes o intentos que no tienen claro. Van ajustando su capacidad y mejorando con cada movimiento. Analizan detenidamente cuáles son las palancas que llevan al éxito de sus operaciones con la intención de realizar el mínimo de movimientos que les exponga a mayores riesgos.
- **Establecimiento de relaciones óptimas con los mejores partners**: el principio básico del CaaS es que los cibercriminales ya no trabajan solos. La clave está en formar las mejores alianzas para el soporte, lavado de dinero, tecnología y fórmulas de ataque; de manera que el éxito sea mucho mayor.
- **Fortalecimiento de la reputación y gestión del talento:** cuanta mejor reputación, más capacidad de acceso a mejores relaciones, a mejor tecnología, etc. Resulta imprescindible también en el mundo cibercriminal. Por otro lado, se hace imprescindible una buena gestión del talento, procurando estabilidad para mejorar las relaciones de confianza.
- **Investigación actualizada sobre nuestro público objetivo, manteniendo flexibilidad ante los nuevos hábitos de consumo y necesidades demandadas**: una de las palabras estrella es la flexibilidad y capacidad rápida de adaptación al medio. Sin duda, una de las habilidades más necesarias para el entorno competitivo que viene. A raíz de la pandemia los hábitos sociales se han visto forzados a cambiar, el cibercrimen ha sido uno de los sectores más rápidos en adaptarse para obtener el máximo rendimiento.
- **Creatividad en el desarrollo de nuevos modelos de negocio**. En el nuevo ciclo económico que se inicia aparecerán océanos azules esperando a ser aprovechados. Pensamiento creativo y nuevas dinámicas de aproximación a los modelos de negocio serán imprescindibles para la supervivencia de las organizaciones.
- **Reducción de lo complejo a lo sencillo**. Uno de los mayores éxitos del CaaS es la capacidad que tienen todos los proveedores de reducir procesos y operaciones complejas a mecanismos sencillos y de rápida integración por parte de compradores potenciales. Siendo conscientes de que existen numerosos aspirantes a cibercriminales sin demasiados conocimientos técnicos, al abrirse a la expresión "para dummies" experimentan una ampliación exponencial del alcance y por tanto del negocio.

5. Referencias

Borum, R., & Sanders, R. (2015). *Cyber Intelligence: Preparing Today: for Tomorrow´s Threats*. INSA Online: Intelligence and National Security Alliance.

Carr, M. (2016). *Public-private Partnerships in National Cybersecurity Strategies*. Londres: Chatham House.

Cilluffo, F. (2015). *A Global Perspective on Cyber Threats*. Alabama (EEUU): Center for Cyber and Homeland Security.

Davis, P. K. (2014). Deterrence, Influence, Cyber Attack, and Cyberwar. *New York University Journal of International Law and Politics* 47(2): 327-355.

Denneson, K., Felker, J., Feyes, T. & Kern, S. (2014). *Strategic Cyber Intelligence*. INSA Online: Intelligence and National Security Alliance.

Hancock, G., Christian, A. & Kaffenberger, L. (2015). *Tactical Cyber Intelligence*. INSA Online: Intelligence and National Security Alliance.

Jensen, E. T. (2013). Cyber Attacks: Proportionality and Precautions in Attack. *International Law Studies* (89): 198-217.