Ganancias del Cibercrimen como Servicio

Profits at the dawn of Cybercrime-as-a-Service

Jorge Maestre Vidal
Indra, Digital Lab,
Madrid, España
jmaestre@indra.es

Marco Antonio Sotelo Monge,
Universidad de Lima, Perú
msotelo@ulima.edu.pe
Sergio Mauricio Martínez Monterrubio
Departamento de Ingeniería del Software e Inteligencia Artificial.
Universidad Complutense de Madrid. España
sergim13@ucm.es

Lorena Isabel Barona López, Ángel Leonardo Valdivieso Caraguay
Departamento de Informática y Ciencias de la Computación (DICC), Escuela Politécnica Nacional,
Quito, Ecuador
{lorena.barona, angel.valdivieso}@epn.edu.ec

Resumen — **El incremento de las Tecnologías de la Información en los últimos años ha derivado en sofisticadas formas de hacer negocio. En consecuencia, grupos criminales de todo el mundo han adaptado sus actividades a las nuevas tendencias en el área de la seguridad de la información. En este artículo se expone el problema del ciberdelito como un negocio rentable, conocido como Cibercrimen como Servicio (CaaS). Para ello se hace hincapié en una de las actividades que más beneficio ha generado, ransomware. Este tipo de software malicioso tiene la capacidad de bloquear o cifrar activos de los sistemas y de extorsionar a sus propietarios por medio de amenazas basadas en su eliminación o divulgación. En este sentido, se presenta un modelo del comportamiento del atacante y la víctima basado en la teoría de juegos. El modelo describe el proceso de extorsión realizado por el atacante sobre la víctima y establece la probabilidad de pago del rescate basado en los intereses de cada participante.**

Palabras Clave - CaaS; Cibercrimen; Malware; Ransomware.

Abstract — **The growing of Information and Communication Technologies (ICT) that has been experienced in recent years, has led to new and more sophisticated ways of doing business. Consequently, worldwide organized criminal groups have been able to adapt their activities to new trends in the area of information security. In this paper the problem of cyber-crime as a profitable business and the model Cybercrime-as-a-service (CaaS) are exposed. For this purpose, the ransomware, which is one of the threats that have generated more profit in the last two years, is analyzed. This kind of malware is able to block assets in the victim systems and blackmail their owners with their deletion, if they fail to pay a ransom. In this sense, a game theory model of the behavior of actors involved in a ransomware attack is proposed. The proposed model describes the extortion process between the attacker and victim and estimates the probability of payment of ransom.**

Keywords - CaaS; Cybercrime; Malware; Ransomware.

I. INTRODUCCIÓN

El importante aumento del número de delitos informáticos registrados en los últimos años, así como las grandes cantidades de beneficios generados por los cibercriminales, ha llevado a definir un nuevo modelo de negocio, conocido como Cybercrime-as-a-Service (CaaS) [1]. El CaaS es un modelo emergente, en el cada comerciante ofrece una serie de productos, tales como vulnerabilidades sin explotar, servicios bulletproof, servicios de phishing o blanqueo de capitales, que hoy en día resultan imprescindibles para que cualquier tipo de campaña maliciosa resulte efectiva. Una de las características más peligrosas del CaaS, es que presenta una relación de retroalimentación con la aparición de nuevas amenazas [9]. Por ejemplo, cuando la explotación de un espécimen de malware deja de ser rentable, sus desarrolladores ponen a la venta el código fuente. Esto deriva en la aparición de nuevas cepas que fortalecen los aspectos vulnerables de su esquema original y que añaden funcionalidades adicionales. Por lo tanto, el problema desencadenado por la muestra original aumenta exponencialmente. Esto también implica un incremento en las ventas de los diferentes servicios del mercado negro y potencia la demanda de nuevos productos. Con el fin de demostrar el problema que implica la expansión del CaaS, en este artículo se considera como objeto de análisis el software malicioso conocido como ransomware [8].

El término ransomware es aplicado a cualquier tipo de malware que al ejecutarse bloquea total o parcialmente el sistema de la víctima, o en su defecto cifra la información del dispositivo. Posteriormente demanda un pago a modo de rescate, tras el que restablece su funcionalidad original. El número de variantes ransomware se incrementó en los últimos años en un 46% y en el caso de WannaCry se contabilizó un total de 5.4 billones de ataques [3]. Tal y como afirma la Europol, es difícil calcular los beneficios totales que este tipo de ataque ha generado [5]. Por ejemplo, se estima que solamente Cryptolocker estafó hasta 3 millones de dólares en 9 meses de actividad, o el pago de 397 bitcoins ($1 millón) realizado por el web hosting Nayana [3]. Para entender la retroalimentación que existe entre este tipo de amenazas y el mercado negro, a lo largo del documento se describen todos los aspectos relacionados con el lanzamiento de sus campañas de distribución. Asimismo, se muestra la necesidad de la participación de terceras partes y los beneficios que obtienen a pesar de las grandes inversiones realizadas [16].

El objetivo final del atacante es obtener un beneficio económico por parte de la víctima, aprovechando su necesidad de recuperar la información que ha sido encriptada. Por su parte, la víctima es forzada a participar del ataque y consecuentemente evalúa diversos factores a la hora de ceder a un pago económico.

978-1-7281-4886-1/19/$31.00 ©2019 IEEE
DOI 10.1109/ICI2ST.2019.00017

En este sentido, el presente trabajo propone un modelo del proceso de extorsión y la decisión de la víctima basado en la teoría de juegos. El modelo toma en cuenta al atacante y víctima como participantes fundamentales. El atacante tiene como objetivo, entre otros factores, la ganancia económica, mientras que la víctima realiza una valoración de sus activos bloqueados. El modelo matemático propuesto identifica a los diferentes elementos que intervienen en un ataque ransomware (jugadores, objetivo, estrategia) e intenta contribuir en el entendimiento de los factores que intervienen en las decisiones tomadas por los atacantes y las víctimas.

El resto del artículo está estructurado de la siguiente manera: en la sección 2 se explica el modelo de negocio CaaS. En la sección 3 se detallan los principales aspectos del ransomware y sus campañas de distribución. En la sección 4 se analiza la relación entre el mercado negro y el ransomware. En la sección 5 se realiza un análisis de las decisiones económicas que realizan los actores de este tipo de CaaS, considerando la teoría de juegos. En la sección 6 se realiza un caso de estudio y finalmente, se indican las conclusiones y las propuestas para trabajos futuros en la sección 7.

II. CIBERCRIMER COMO SERVICIO (CAAS)

Desde sus inicios en los años 80, el cibercrimen ha evolucionado alcanzando un alto nivel de organización, de tal manera que se ha convertido en un negocio muy rentable [3]. La similitud que presenta su funcionamiento con el modelo de distribución software como un servicio, del inglés, *Software-as-a-Service (SaaS)*, ha llevado a la popularización del término cibercrimen como servicio, del inglés, *Cybercrime-as-a-Service (CaaS)*. El paradigma SaaS ofrece la posibilidad de alquilar productos de software a terceras partes, con el fin de ahorrar los costes de las licencias y simplificar las tareas de implementación. Esto permite que cualquier empresa pueda recurrir a los diferentes conjuntos de aplicaciones, sin perder demasiada rentabilidad en sus negocios. El CaaS opera de manera similar: ofrece servicios ilegales para el desarrollo de campañas delictivas [23]. A continuación, se describen algunos de los principales aspectos de este mercado negro, destacando a sus participantes, su modelo de distribución y los servicios ofertados.

A. Vendedores y clientes

El principal punto de compra-venta de productos CaaS son los underground *(foros ocultos)* y determinados servicios en redes anónimas, similares al Black Market (*mercado negro digital*) y Silk Road *(la ruta de la seda digital)* [18], desplegados en dominios del tipo .onion sobre la red Tor. Dada la garantía de anonimato [15] que ofrecen y su difícil trazabilidad de las formas de pago actuales, el comprador no requiere de conocimientos técnicos avanzados para acceder a ellos [16]. En este sentido, la inversión debe ser alta para que una campaña de propagación de malware produzca beneficios. Por lo tanto, sus autores deben asumir importantes gastos iniciales y costes de mantenimiento, aún a riesgo de que el producto final no genere beneficios. En otras palabras, detrás de este tipo de acciones se encuentran involucradas importantes organizaciones criminales. En [22] se analiza el perfil de las organizaciones responsables de la mayor parte de los ciberdelitos con la habilidad de causar impacto a gran escala. Estos son grupos de criminales convencionales, cibercriminales y grupos con motivaciones ideológicas o políticas.

Por un lado, las organizaciones criminales clásicas han actualizado su negocio a las nuevas tecnologías. El desarrollo de nuevas variantes normalmente requiere de componentes comprados a terceras partes. Se sabe que, por ejemplo, el ransomware Reveton, *(virus de la policía)* expandido principalmente entre 2009 y 2011, tuvo su origen en la mafia rusa [5] y se tiene la misma sospecha de Cryptolocker en el año 2014. Por su parte, ataques más recientes se basan en el uso de criptomonedas [4] tal es el caso del ransomware WannaCry. Aunque no se puede determinar el origen de esta variante se estima que, desde su aparición en 2017, WannaCry ha infectado alrededor de 200,000 computadores en 150 países, siendo los casos más mediáticos los ataques a Telefónica-España, el sistema de salud de Inglaterra (NHS), FedEx en Estados Unidos, entre otros [20]. Por otro lado, el negocio del ciberdelito ha llevado a la creación de una asociación de delincuentes que habitualmente operarían de manera individual. Dicha asociación se realiza con el fin de poder asumir gastos, distribuir e incluso la especialización en la carga de trabajo. Estos grupos actúan únicamente por beneficios económicos. Al finalizar la campaña, normalmente intentan sacar un beneficio extra vendiendo las herramientas que desarrollaron [1]. Finalmente, existen organizaciones unidas en base a una motivación común de carácter ideológico o religioso. En este caso su objetivo no suele ser ganar dinero, sino conseguir visibilidad o boicotear a las víctimas. Este es caso de grupos hacktivistas como Anonymous o Lulzsec [6]. Finalmente, los servicios del mercado negro también pueden ser contratados por grupos terroristas para encubrir actividades relacionadas con el reclutamiento o su financiación. En el peor de los casos pueden llegar a ser piezas indispensables para completar ciberataques contra infraestructuras, por ejemplo, hospitales [17].

B. Modelo de Distribución

Huang et al. [9] identifican dos tipos de actividades que añaden valor a CaaS: i) actividades primarias y ii) actividades de soporte. Por un lado, las actividades primarias se relacionan con el descubrimiento de la vulnerabilidad, el desarrollo del software de explotación, la selección del objetivo y la parte operacional del ciclo de vida del ataque. Por otro lado, las actividades de soporte se enfocan en el marketing y la entrega del servicio, el lavado de dinero, el reclutamiento y entrenamiento, es decir la distribución del servicio como tal.

En [23] se propone un modelo de distribución del CaaS basado en tres perfiles de participantes: operadores, anunciantes y clientes. El modelo define a los operadores como usuarios con grandes conocimientos técnicos, capaces de desarrollar los productos maliciosos y el framework necesario para su gestión. A menudo también se encargan de la ocultación de huellas y del blanqueo de los beneficios. Por otro lado, se define a los anunciantes como los elementos intermedios entre operadores y clientes. Su labor es localizar nuevos clientes y participar a modo de enlace en los procesos de negociación. Finalmente, los clientes son los que adquieren los servicios CaaS. Como indicaron sus propios autores, en ocasiones un mismo individuo puede ejercer de operador y anunciante. Con el fin de adaptar el modelo a las campañas de ciberdelitos, se ha incluido un nuevo

perfil al modelo: los patrocinadores. Se define como patrocinadores a aquellos individuos u organizaciones propietarios del dinero que se mueve en el mercado negro. De este modo, operadores y clientes pasan a ser conexiones de las entidades que verdaderamente promueven este tipo de negocios. Los patrocinadores habitualmente pertenecen a cualquiera de las organizaciones descritas en la subsección anterior. También es posible que un mismo individuo ejerza a la vez de operador y patrocinador, o de cliente/usuario y de patrocinador. En la Figura 1 se muestra el modelo descrito.

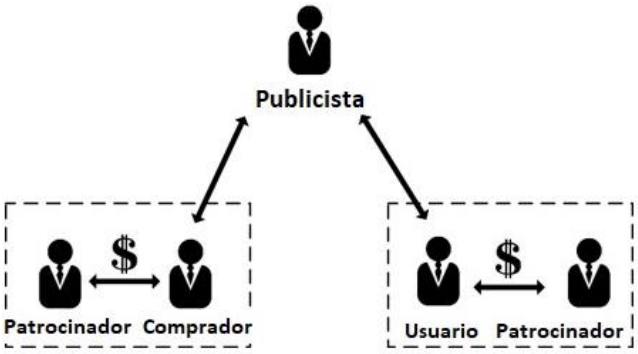

Figura 1 – Modelo de distribución de CaaS.

C. Servicios Ofertados

A continuación, se describen los servicios ofrecidos como CaaS con mayor demanda.

1. **Sistemas comprometidos**. Se relaciona con la venta y el alquiler de botnets, así como el software necesario para gestionarlas [24]. Normalmente se destinan a la generación de ataques de denegación de servicio (DoS) y a la propagación de malware y spam. En [9] se muestran algunos precios relacionados con este tipo de servicios, como los de alquiler de bots (aprox. 100$ cada 1000 unidades), o los de contratación de spam (aprox. $40 cada 20,000 emails. Los servicios extra se cobran por separado, por ejemplo, los bots pueden incluir un módulo basado en SpyEye para el blanqueo de dinero ($500-10.000) o exploit kits ($1000-$200).
2. **Vulnerabilidades**. En el mercado negro se ofrecen vulnerabilidades sin explotar y sin ser solucionadas (vulnerabilidades día cero). Tal y como se indica en [19], su demanda cada vez es mayor, y sus precios como CaaS a menudo son superiores que los que ofrecen las propias desarrolladoras para su mitigación. Por ejemplo, con una inversión de $10,000 USD se podría llegar a generar beneficios de entre $50,000 a $250,000 USD.
3. **Código**. Es frecuente que los autores de ciberdelitos ofrezcan el código fuente y frameworks para su edición como CaaS. En el caso del Toolkit Mpack, su precio en el mercado negro osciló entre $500 a $1000 USD [12]. En [23] se presentan los precios aproximados asociados a kits de desarrollo de botnets. Habitualmente se venden componentes o empaquetados, y éstos varían en base a su funcionalidad.
4. **Infraestructura e información**. En CaaS también se ofrece la infraestructura y la información necesarias para perpetrar cualquier tipo de campaña. Un ejemplo claro se encuentra en los productos relacionados con las suplantaciones de identidad o Phishing [3]. Entre ellos se incluye el alquiler de servidores SMTP para el envío de correos fraudulentos (aprox. $15-30 USD), la aplicación que automatiza su envío (aprox. $20-25 USD), el uso de páginas web falsificadas (aprox. $15-$20 USD) y listas de correo de usuarios.
5. **Servicios Profesionales**. Para afrontar una campaña maliciosa con éxito a menudo es necesario la contratación de expertos en campos muy concretos. Por ejemplo, en [13] se menciona la posibilidad de contratar asistencia técnica a modo de guía en la instalación de sistemas C&C de botnets (aprox. $350-400 USD). En [14] la empresa de seguridad McAfee advierte de la existencia de sitios donde es posible contratar cibercriminales para que cometan cualquier tipo de delito a la carta.
6. **Ofuscación de malware**. Consiste en modificar el código fuente de un programa, con el fin de que no se parezca a su versión original. Este tipo de técnicas permiten que el malware evite los sistemas de detección de intrusiones, facilitando de este modo su propagación [21]. En los casos más complejos, la ofuscación puede llevarla a cabo un profesional de manera manual. Sin embargo, lo habitual en el mercado negro es contratar servicios de ofuscación web, en los que basta con subir el espécimen original a una aplicación, para obtener la muestra transformada.
7. **Servicios Bulletprof**. Este nicho de mercado contiene las ofertas relacionadas con la protección de la campaña maliciosa y la ocultación de huellas (para garantizar la inmunidad de los criminales). Entre sus servicios se encuentra el alquiler de direcciones IP legítimas, protección de dominios, protocolos de seguridad, tunelaje, detección de intrusiones, entre otras.
8. **Otros**. Por ejemplo, el alquiler de tarjetas de crédito (aprox. $4-$12 USD), la venta de datos del cliente y sus direcciones de correo (aprox. $6-$40 USD), etc [23]. Se sabe que organizaciones rumanas han contratado hablantes en lengua inglesa para que, al suplantar identidades, no se note su acento.

Además de estos servicios, el inicio de una campaña maliciosa debe contar con la infraestructura adecuada. Por ejemplo, Cryptolocker llegó a infectar hasta 500,000 sistemas. Es evidente que para garantizar su operabilidad se debió de disponer de los sistemas apropiados, tales como servidores, cortafuegos, proxies etc. En ocasiones, este tipo de productos también son adquiridos en el mercado negro.

III. RANSOMWARE

Ransomware es un tipo de software malicioso que encripta o bloquea parte del sistema víctima o sus archivos, y exige un pago a modo de rescate. Algunas de sus caracterizas hacen que sea muy diferente del malware convencional [11], por ejemplo, no necesita extraer información de la víctima. Su objetivo únicamente es conseguir que pague el rescate. Además, es

visible ya que, una vez realizada la infección, avisa directamente a la víctima. En [3] se atribuye su rápida proliferación a la existencia de métodos de pago anónimo, la calidad de los servicios ofrecidos como CaaS para respaldar sus campañas de propagación y la falta de formación de las víctimas.

A. Evolución

El ataque tipo ransomware no es una amenaza nueva. Las primeras variedades de malware con capacidad de bloquear y de extorsionar a la víctima aparecieron en los años 80. Uno de los primeros ejemplares fue el conocido AIDS Trojan [2]. Se propagaba vía correo electrónico y funcionaba como una bomba lógica: después de iniciar 90 veces el equipo, cifraba el disco duro por medio de un sencillo esquema de sustitución mono alfabético, exigiendo un pago de $189 o $378 por su recuperación. En los años 90s este tipo de amenazas captó la atención de la comunidad investigadora. En [25] se acuñó el término "Cryptovirology" para designar a la criptografía aplicada en el desarrollo de malware malicioso. La mayor parte de su aplicación se enfocó en la implementación de crypto-ransomware. A pesar de su variedad, este tipo de amenaza no ganó en sofisticación hasta llegar el siglo XXI. En efecto, las primeras campañas importantes procedieron de países que pertenecieron a la antigua unión Soviética [2] y se desarrollaron entre los años 2005 y 2006. Las estrategias de cifrado aplicadas eran simétricas, y los métodos de pago muy sencillos; vía SMS o con llamadas a teléfonos de pago.

Posteriormente, el ransomware ganó complejidad cuando en el año 2011 se descubrió la campaña del espécimen Reveton el cual tenía la capacidad de bloquear el acceso al sistema mostrando un mensaje de pago a las supuestas fuerzas de orden [3]. En el año 2011 apareció el primer espécimen que aplicaba criptografía asimétrica: Cryptolocker. Su complejidad, facilidad de propagación y esquema de cifrado prácticamente inquebrantable, permitieron que infectara al menos 50,000 equipos. El éxito que obtuvo animó a otros cibercriminales a emprender campañas similares o a nuevas variantes. Hoy en día varias variantes son ofrecidas en el mercado negro como CaaS, permitiendo a sus compradores modificarlo en función de sus necesidades. También han aparecido cepas que afectan a diferentes arquitecturas y sistemas operativos, tal es el caso de dispositivos móviles [26].

B. Modus Operandi

En términos generales, el ransomware opera en tres etapas: propagación, bloqueo de activos y extorsión, tal como se muestra en la Figura 2.

En la etapa de **propagación** se utilizan algunas técnicas, entre las más conocidas la aplicación de phishing sobre correos electrónicos y servicios web. También es frecuente el uso de banners que explotan vulnerabilidades en tecnologías web tales como flash y java, y que además pueden redirigir a la víctima a páginas con contenido malicioso [10]. Las versiones actuales pueden afectar a los servicios de volcado de archivos o infectar los respaldos de los activos originales. Finalmente, el atacante puede utilizar herramientas para identificar sistemas cuyos servicios de control remoto sean vulnerables o presenten contraseñas por defecto. Por su parte, en durante la segunda etapa, el ransomware opera en segundo plano **bloqueando** o cifrando el contenido del disco duro. En sus orígenes se cifraba completamente, sin embargo, las versiones modernas realizan un cifrado selectivo, eligiendo archivos con determinadas extensiones [3], tales como .docx, .xls, .ppt, .avi, .jpg, .rar, .c, etc.

Finalmente, en la etapa de **extorsión** se notifica al usuario acerca del estado del sistema y se negocia su rescate. Por ejemplo, Wannacry muestra un mensaje en donde pide un pago de $300 USD en un plazo de 72 horas para desencriptar sus archivos. El mensaje juega con la psicología de la víctima, mostrando un reloj con la cuenta atrás. Pasado ese tiempo, da una segunda posibilidad de realizar el pago, pero esta vez aumentando su cantidad.

IV. INTERDEPENDENCIA ENTRE RANSOMWARE Y CAAS

Como se indicó en la sección anterior, para que el ransomware sea efectivo necesita desplegarse sobre una infraestructura de apoyo que reúna características técnicas muy avanzadas. Esta es habitualmente adquirida en el mercado negro como CaaS. A continuación, se mencionan algunos de sus componentes típicamente adquiridos a terceras partes.

1. **Código fuente del espécimen original y código fuente del malware** cuyo vector de ataque se aplica en la infección, incluyendo scripts para distinguir el tipo de sistema víctima o la contratación de servicios de ofuscación.
2. **Vulnerabilidades y exploit kits** para su propagación (proceso de infección).
3. **Equipos comprometidos** para su instalación y el inicio de su distribución.
4. Dado que la mayor parte de **especímenes se propagan** vía correo electrónico, se requiere de servidores, envío de spam, y elementos relacionados con el phishing, tanto para su distribución como para extorsión.
5. **Bulletproof services** tales como fast flux, tunelaje para el C&C y servidores capaces de soportar tráfico cifrado.
6. **Servicios relacionados con el blanqueo de capitales**, como el alquiler de tarjetas de crédito, y la automatización de los procesos de blanqueo.

Figura 2 - Etapas de un ataque ransomware

A la vista de la necesidad de estas adquisiciones, las grandes campañas requieren del gasto de una importante cantidad de dinero en el mercado negro. A esto debe añadirse el coste inherente asociado a la creación y mantenimiento de cualquier tipo de producto de las tecnologías de la información, como el salario de los trabajadores o el mantenimiento de la infraestructura básica. Por lo general, el gasto en el mercado negro puede distribuirse en tres etapas: inversión inicial, mantenimiento y blanqueamiento [7]. El coste inicial del proyecto malicioso involucra la compra del código fuente de las aplicaciones, las vulnerabilidades, exploit kits, y los gastos iniciales de contratar el resto de la infraestructura. Por otro lado, el coste de mantenimiento es el que se produce día a día por seguir utilizando los servicios contratados, y de este modo mantener la campaña activa [28]. Cuando su valor es superior al de los beneficios aportados, el negocio deja de ser rentable. Finalmente, en la etapa de blanqueamiento se incluyen gastos asociados a la compra de información bancaria, y las tasas de las entidades intermedias que participan.

En conclusión, emprender una campaña maliciosa como las mencionadas en los ejemplos expuestos a lo largo del artículo, requiere de la realización de una inversión grande en CaaS. Los vendedores del mercado negro conocen esta situación, motivo por el cual cada vez hay más oferta y de mayor calidad. Adicionalmente, el éxito de las campañas realizadas incentiva a nuevos cibercriminales a cometer negocios similares. Esto compensa el incremento de la oferta de CaaS, con un incremento en su demanda. Como consecuencia, el modelo de negocio permanece estable y en constante crecimiento [3]. Esto también supone un beneficio para las campañas de distribución de Ransomware y puede comprobarse en la aparición de nuevos especímenes cada vez más complejos que sus versiones originales. Además, el miedo y la falta de formación hacen de la extorsión una de las mayores garantías de recuperar rápidamente el dinero invertido. De este modo, los cibercriminales se arriesgan a asumir la compra de cada vez mejores servicios CaaS, produciéndose una realimentación beneficiosa para ambos lados, como se muestra en la Figura 3.

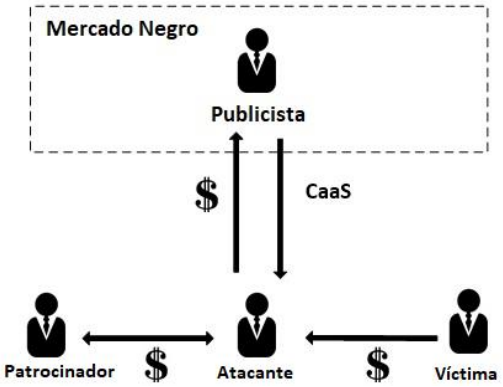

Figura 3 - Caas y Ransomware

V. MODELADO DE LA RETRIBUCIÓN DE RANSOMWARE

La efectividad de los mecanismos de extorsión del ransomware puede llegar a comprenderse a partir del estudio de las decisiones económicamente racionales que realizan los actores que participan en su desarrollo. Para ello se basan en la consideración de sus necesidades y los recursos disponibles con el fin de optimizar sus beneficios. Por lo tanto, se trata de un caso de estudio fácilmente adaptable a las características de la teoría de juegos. En esta sección se analiza un esquema de juego en el que participan un único criminal y una única víctima. De este modo es posible entender la naturaleza del proceso de extorsión.

A. Modelo de extorsión

El proceso de extorsión inicia una vez que el software malicioso ha infectado a la víctima. La primera decisión del juego, es definida como la decisión binaria:

$$\begin{cases} Act = 0, & no\ activación\ de\ bloqueo \\ Act = 1, & activación\ de\ bloqueo \end{cases}$$

Donde la elección racional $Act = 0$ conserva el beneficio $noAct_{prof}$ para el criminal, asociado a continuar con el sistema infectado, sin mostrar indicadores de actividad maliciosa. Estos beneficios proceden de situaciones como la de ofrecer su alquiler como CaaS, o de la capacidad de propagar el software malicioso a nuevos anfitriones. Sin embargo, al decidirse $Act = 1$, la víctima conoce el estado del sistema. Esto puede llevar a su aislamiento, produciendo la perdida para el criminal $-noAct_{prof}$ asociada a su estado de ocultación. La elección $Act = 1$ también da pie al proceso de negociación, en el cual el ransomware muestra un mensaje en el que exige un rescate inicial valorado en R a cambio de devolver la funcionalidad al

sistema. La reacción de la víctima ante dicha notificación depende de diferentes factores. Por un lado, esta valora los activos bloqueados en una cantidad C de dinero. Por lo tanto, cuando C<R considera que el rescate exigido es mayor que el valor de los activos confiscados, por lo que se negará categóricamente a su pago. En el caso de C≥R considera que el valor de los activos es superior o igual a R, lo que le llevará a decidir si realizará el pago. En este caso, aún existe la probabilidad P_{eth} de que a pesar de todo, elija no pagar.

El valor P_{eth} representa tres características de la víctima: en primer lugar, el condicionamiento ético de la víctima asociado a la decisión de negociar con delincuentes. También involucra su temor a que, una vez realizada la transacción, los activos no sean restablecidos. Por último, tiene en cuenta su preocupación a la hora de asumir futuros riesgos. Entre ellos, el más común es que la infección prevalezca en estado latente. Esto daría lugar a futuros chantajes similares, o al uso del sistema comprometido como elemento de propagación del malware, tal y como se ha repetido en múltiples casos reales [13]. La relación entre P_{eth} y los valores C y R da lugar al establecimiento del factor α. Este representa la probabilidad total de que la víctima pague el rescate. Por lo tanto, tiene en consideración la diferencia entre el rescate pedido R y el coste de los activos C; evidentemente, cuanto mayor sea C respecto a R, mayor es la probabilidad de pago. A esto le añade la probabilidad P_{eth} de negarse a cooperar, simplificándose la relación, en la función lineal:

$$\alpha = P_{eth} - \frac{R}{C}P_{eth} \quad = P_{eth}(1 - \frac{R}{C})$$

Adicionalmente se considera la probabilidad β de que, una vez realizado el pago, el atacante no libere el bloqueo, y la probabilidad ɣ de que la víctima sea capaz de eliminar completamente la infección. Estos valores dependerán de lo malvado que sea el atacante y de la habilidad del administrador del sistema de IT victima encargado de restaurar el sistema. Nótese que se asume que la víctima no es capaz de desbloquear los activos por sus propios medios. Ésta precondición se apoya en la complejidad de los esquemas de cifrado de los especímenes actuales.

B. Reglas y pagos esperados

En la Tabla 1 se muestran los beneficios y pérdidas del cibercriminal (jugador P1) y la víctima (jugador P2), tras la elección de las distintas estrategias de juego (*payoffs*).

Tabla 1 – Pagos de cada jugador

Decisiones				Pago (Payoff)	
(P1) Chantajea	(P2) Paga	(P1) Elimina activos	(P2) Elimina Infección	Cibercriminal	Víctima
No	---	---	---	0	0
Si	Si	Si	No	R	$-R-C$
Si	Si	Si	Si	$R - noAct_{prof}$	$-R-C$
Si	Si	No	No	R	$-R$
Si	Si	No	Si	$R - noAct_{prof}$	$-R$
Si	No	Si	No	0	$-C$
Si	No	Si	Si	$-noAct_{prof}$	$-C$

La Figura 4 resume el proceso de decisión.

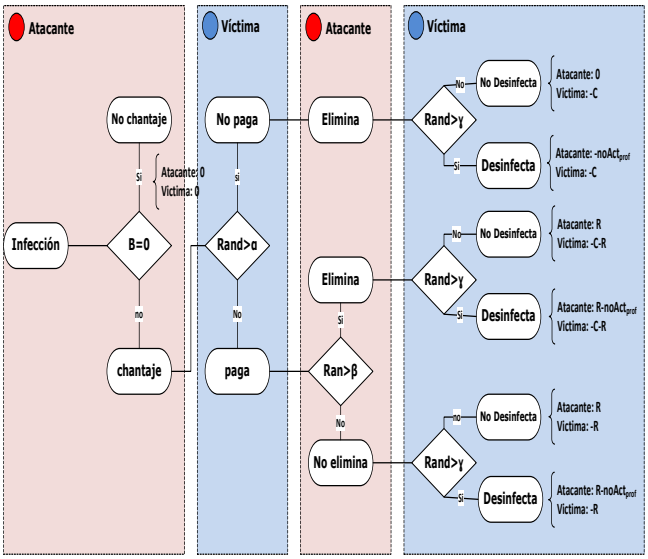

Figura 4 – Desarrollo de juego individual

A continuación, se describen las reglas del juego:

1. Del atacante decide si se inicia el proceso de chantaje, es decir, $Act = 0$ o $Act = 1$
2. Si $Act = 1$, el atacante tiene que anunciar la cantidad de dinero R del rescate.
3. La víctima valora los activos bloqueados en una cantidad de dinero C. La combinación de C su perfil de comportamiento P_{eth}, determinan la probabilidad α de que decida pagar el rescate. La probabilidad β indica con qué frecuencia el atacante elimina los activos pese a recibir el pago, y la tasa ɣ define la probabilidad de que la víctima consiga eliminar completamente la infección tras el chantaje.
4. La víctima decide si pagar el chantaje o no. En el primer caso, el atacante añade a sus beneficios el rescate R, y la víctima pierde ese dinero –R
5. Si la víctima se niega a pagar el rescate, el atacante no añade dinero a sus beneficios. Sin embargo, la víctima pierde los activos secuestrados -C.
6. Cuando el atacante cobra el rescate, existe una probabilidad β de que ejecute su amenaza. En ese caso, la víctima pierde también los activos secuestrados -C (en total acumula -C-R). En el caso contrario, no sufre pérdidas adicionales (en total acumula -R).
7. Una vez concluida la negociación, la víctima podría eliminar la infección. En ese caso el atacante pierde el control sobre su sistema $-noAct_{prof}$.

Dado que no se trata de un juego de suma 0, en cada elemento de la matriz que representa los pagos se aplica un vector bidimensional, siendo su primera posición la del atacante y la segunda la de la víctima. La Tabla 2 resume su contenido:

Tabla 2. Representación de pagos

		Víctima			
		Paga (α) y Limpia (ɣ)	Paga (α) y no Limpia (1-ɣ)	No paga (1-α) y Limpia (ɣ)	No paga (1-α) y no Limpia (1-ɣ)
Atacante	Liberaría (1-β)	A: $R-noAct_{prof}$ V: $-R$	A: R V: $-R$	A: $-noAct_{prof}$ V: $-C$	A: 0 V: $-C$
	No Liberaría (β)	A: $R-noAct_{prof}$ V:$-R-C$	A: R V: $-R-C$	A: $-noAct_{prof}$ V: $-C$	A: 0 V: $-C$

Por lo tanto, la matriz del juego es la siguiente:

$$\begin{pmatrix} (R-noAct_{prof},-R) & (R,-R) & (-noAct_{prof},-C) & (0,-C) \\ (R-noAct_{prof},-R-C) & (R,-R-C) & (-noAct_{prof},-C) & (0,-C) \end{pmatrix}$$

Y el pago (*payoff*) esperado del atacante es:

$$\begin{aligned} \mathrm{P(Atacante)} = {} & \big((\mathrm{R}-\mathrm{noAct_{prof}})(\alpha(1-\beta)\gamma)\big) \\ & + \Big((\mathrm{R})(\alpha(1-\beta)(1-\gamma))\Big) \\ & + \Big(\big(-\mathrm{noAct_{prof}}\big)\big((1-\alpha)(1-\beta)(\gamma)\big)\Big) \\ & + \Big(\big(\mathrm{R}-\mathrm{noAct_{prof}}\big)(\alpha\beta\gamma)\Big) \\ & + \Big(\big(\mathrm{R}\big)\big(\alpha(\beta)(1-\gamma)\big)\Big) \\ & + \big((-\mathrm{noAct_{prof}})((1-\alpha)(\beta)(\gamma))\Big) \end{aligned}$$

Y el de la víctima es:

$$\begin{aligned} \mathrm{P(Víctima)} = {} & \big((-\mathrm{R})(\alpha(1-\beta)\gamma)\big) + \Big((-\mathrm{R})\big(\alpha(1-\beta)(1-\gamma)\big)\Big) + \\ & \Big((-\mathrm{C})\big((1-\alpha)(1-\beta)\gamma\big)\Big) + \Big((-\mathrm{C})\big((1-\alpha)(1-\beta)(1-\gamma)\big)\Big) + \\ & \big((-\mathrm{R}-\mathrm{C})(\alpha\beta\gamma)\big) + \Big((-\mathrm{R}-\mathrm{C})\big(\alpha\beta(1-\gamma)\big)\Big) + \Big((-\mathrm{C})\big((1- \\ & \alpha)\beta\gamma\big)\Big) + ((-\mathrm{C})((1-\alpha)\beta(1-\gamma)))\end{aligned}$$

De este modo, el modelo permite calcular la probabilidad de pago de un rescate, una vez que la infección del ransomware en el sistema ha sido exitosa. Es claro que la precisión de los resultados dependerá en gran parte de la estrategia utilizada para la estimación del valor de determinadas variables del juego. En este sentido, es importante utilizar estadísticas actualizadas con el fin de ubicar el daño potencial de la amenaza en su situación temporal. Es decir, el grado de amenaza se reduce gradualmente una vez que estrategias de mitigación han sido creadas.

VI. CASO DE ESTUDIO

Para comprobar el modelo, se ha realizado un caso de estudio sobre un ataque real en una empresa, que, por motivos de confidencialidad, se guarda su nombre. Dicha empresa recibió un ataque del tipo CaaS por medio de un ransomware el cual ataco la base de datos de sus clientes cifrando dicha información y pidiendo un rescate de $15,000 USD. El dueño de la empresa decide contratar a un experto en seguridad informática muy reconocido en España [27]. Después de un laborioso día de investigación, concluye que dicho ataque no es similar a ninguno que se haya visto anteriormente y que, dado a la naturaleza de la inflexión era más barato la negociación con el estafador que buscar una vacuna para contrarrestar el ataque. En ese momento, el dueño de la empresa solicita al experto en seguridad informática que sea el mediador entre el estafador y la empresa. Al mismo tiempo decide dar parte a la policía quien solicita a la empresa que no se deje estafar. En la negociación para tener un menor precio, el estafador se percata de la trampa y deja bloqueado el sistema huyendo sin el pago, pero haciendo el perjuicio a la empresa. La empresa solicita ayuda a la policía quien junto con el experto en seguridad logran descifrar el sistema en un mes, lo que conlleva a perdidas a dicha empresa por más de $100,000 USD. En este caso el criminal dejó un rastro, pero no fue posible localizarlo. Por lo que dicho crimen sigue impune, pero se ha agregado a una base de datos de la policía de diferentes países para una detención en el caso de que nuevamente ocurra dicho incidente y capturar al cyber criminal. En el modelo propuesto en este artículo, se representó el comportamiento del atacante y la victima utilizando teoría de juegos y tomando como base los intereses de cada participante. Se simuló en el sistema las diferentes probabilidades de dicho escenario logrando obtener un 98% de precisión.

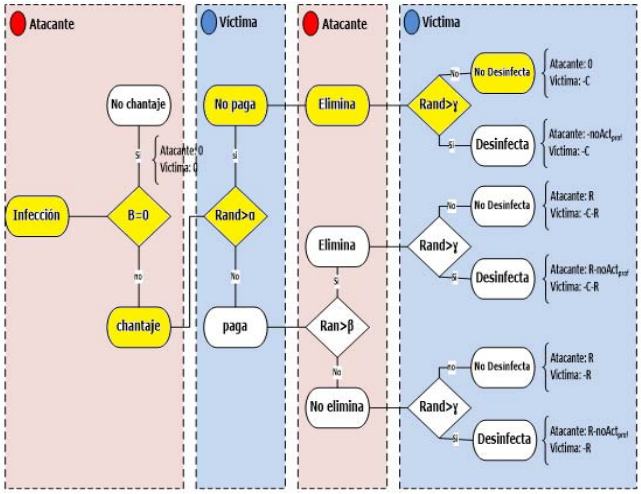

Figura 5 – Desarrollo de juego del caso de estudio.

VII. CONCLUSIONES

El presente artículo analiza la retroalimentación que existe entre el mercado negro y el ransomware. Con este fin se han descrito los aspectos más característicos del modelo de negocio CaaS. De igual manera, se ha mostrado la evolución de ransomware y las principales diferencias que presenta con el malware convencional. A la vista de las observaciones realizadas, este problema conlleva una amenaza creciente y en constante evolución. La complejidad de la tecnología ofrecida en el mercado negro hace que la mitigación de las campañas de distribución de malware sea cada vez más difícil. Para contribuir en la mitigación de este tipo de amenazas se ha presentado un modelo del comportamiento del atacante y la victima utilizando teoría de juegos y tomando como base los intereses de cada participante. Para la ejemplificación del modelo se elaboró un caso de estudio de una actividad maliciosa real logrando resultados muy favorables con el modelo de teoría de juegos. Se propone como trabajo futuro analizar en mayor profundidad el modelo de negocio CaaS en otros escenarios y aprovechar la relación entre el malware distribuido y los componentes obtenidos de terceras partes. De igual manera, se propone ampliar el modelo de teoría de juegos con el fin de incluir más escenarios empresariales, en donde el número de variables, tipo de activos y participantes se incrementa.

AGRADECIMIENTOS

Este trabajo ha sido posible gracias al apoyo de SECTEI (Subsecretaría de Ciencia, Tecnología e Innovación de la Ciudad de México) para el autor Sergio Martínez durante sus estudios postdoctorales en la Universidad Complutense de Madrid.

REFERENCIAS

[1] An, J., Kim, H. W. A data analytics approach to the cybercrime underground economy. IEEE Access, 6, 1-17, 2018.

[2] Bajpai, P., Sood, A. K., Enbody, R. A Key-management-based Taxonomy for Ransomware. In Proceedings of APWG Symposium on Electronic Crime Research, CA, USA, 1-12, May 2018.

[3] Cleary, G., Cox, O., Lau, H., Nahorney, B., Gorman, B., O'Brien, D., Wallace, S., Wueest, C. Internet Security Threat Report Symantec, 80-89, 2018.

[4] Conti, M., Gangwal, A., & Ruj, S. On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective. Computers & Security, 79, 162–189, 2018.

[5] Europol. Police Ransomware Threat Assessment 2014. Retrieved from: https://www.europol.europa.eu/content/police-ransomware-multimillion-euro-business, 2014.

[6] Goode, L. Anonymous and the Political Ethos of Hacktivism. Popular Communication, 13 (1), 74-86, 2015.

[7] Hernandez - Castro, J., Cartwright, E., Stepanova, A. Economic Analysis of Ransomware. Retrieved from: http://dx.doi.org/10.2139/ssrn.2937641, 2017.

[8] Herrera, J, Barona, L, Valdivieso., L., & Hernández-Álvarez, M. A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. Remote Sensing, 11 (10), 1-17, 2019.

[9] Huang, K., Siegel, M., & Stuart, M. Systematically Understanding the Cyber attack business: A survey. ACM Computing Surveys (CSUR), 51 (4), 1-36, 2018.

[10] Kim, D., Yan, P., & Zhanf, J. Detecting Fake Anti-virus Software Distribution Webpages. Computers & Security, 49, 95-106, 2015.

[11] Kolodenker, E.; Koch, W.; Stringhini, G.; Egele, M. PayBreak: Defense against Cryptographic Ransomware. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. ACM, Abu Dhabi, UAE, 599–611, April 2017.

[12] Kshetri, N. Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current Status and Key Drivers. Crime, Law and Social Change, 60 (1), 39-65, 2013.

[13] Manky, D. Cybercrime as a Service: a very Modern Business. Computer Fraud & Security, 2013 (6), 9–13, 2013.

[14] McAfee. The Economic Impact of Cybercrime No Slowing Down, McAfee white paper. Retrieved from: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf, 2017.

[15] Me, G., & Pesticcio, L. Tor Black Markets: Economics, Characterization and Investigation Technique. Cyber Criminology, 119–140, 2018.

[16] Naqvi, S. Challenges of Cryptocurrencies Forensics: A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals. In Proceedings of the 13th International Conference on Availability, Reliability and Security, ACM, New York, NY, USA, 1-5, August 2018.

[17] Naseir, M. A. B., Dogan, H., Apeh, E., Richardson, C., & Ali, R. Contextualising the National Cyber Security Capacity in an Unstable Environment: A Spring Land Case Study. In Proceedings of 2019 World Conference on Information Systems and Technologies. Springer, Galicia, Spain, 373-382, March 2019.

[18] Phelps, A., & Watt, A. I shop online – recreationally! Internet anonymity and Silk Road enabling Drug Use in Australia. Digital Investigation, 1 (4), 261-272, 2014.

[19] Ring, T. Why Bug Hunters are Coming in from the Wild. Computer Fraud & Security, 2014 (2), 16-20, 2014.

[20] Schirrmacher, N. B., Ondrus, J., Tan, F. T. C. Towards a Response to Ransomware: Examining Digital Capabilities of the WannaCry Attack. In Proceedings of Pacific Asia Conference on Information Systems, 1-9, Yokohama, Japan, June 2018.

[21] Schrittwieser, S., Katzenbeisser, S., Kieseberg, P., Huber, M., Leithner, M., Mulazzani, M., Weippl, E. Covert Computation — Hiding code in code through compile-time obfuscation, Computers & Security, 42, 13-26, 2014.

[22] Snader , R., Borishov, N. Improving Security and Performance in the Tor Network through Tunable Path Selection. IEEE Transactions on Dependable and Secure Computing, 8 (5), 728-741, 2012.

[23] Sood, A. K., & Enbody, R. J. Crimeware-as-a-service—A Survey of Commoditized Crimeware in the Underground Market. International Journal of Critical Infrastructure Protection, 6 (1), 28-38, 2013.

[24] Wainwright, P., & Kettani, H. An Analysis of Botnet Models. In Proceedings of the 2019 3rd International Conference on Compute and Data Analysis. ACM, New York, USA, 116-121, March 2019.

[25] Young, A., & Yung, M. Cryptovirology: Extortion-based Security Threats and Countermeasures. In Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, USA, 129-140, May 1996.

[26] Zavarsky, P., & Lindskog, D. Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization. Procedia Computer Science, 94, 465-472, 2016.

[27] "Security Watch: The Crimeware-As-A-Service Reality." Sunday Business Post, N/a, 2013.

[28] Dupont, Benoit. "Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation As a Way to Control Large-Scale Cybercrime." Crime, Law and Social Change : An Interdisciplinary Journal, vol. 67, no. 1, 2017, pp. 97–116., doi:10.1007/s10611-016-9649-z.