Combatiendo el cibercrimen

Grupo de delitos telemáticos de la Guardia Civil

Vivimos permanentemente interconectados a través de ordenadores portátiles, tablets, smartphones... ajenos a una continua actividad delincuencial en la que somos objetivos, no sólo por nuestro dinero sino también por nuestra información personal, con la que se comercia. Sólo percibimos de vez en cuando algún funcionamiento anormal de nuestro equipo por algún "virus" o que recibimos correos electrónicos no deseados, pero la realidad esconde mucho más.

COMANDANTE ÓSCAR DE LA CRUZ
Jefe del Grupo de delitos telemáticos de la Guardia Civil

En un escenario globalizado en el que ya existen más de 10 mil millones de dispositivos conectados a Internet, utilizados por casi 3 mil millones de usuarios, no cabe duda que el cibercrimen se configura como una de las grandes amenazas ya consolidada y su dimensión crece exponencialmente según los ciudadanos, las empresas y las administraciones aumentamos nuestra superficie de exposición a diversos riesgos que se derivan del uso de las ya no nuevas tecnologías.

Independientemente de la consideración de la ciberdelincuencia en sentido estricto (aquellos delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs) o en sentido amplio (otros delitos tradicionales pero que en su actividad criminal se sirven de las ventajas que ofrecen las TICs) debemos tener en cuenta que si excluimos aquellos en los que la motivación tiene un claro componente sexual (distribución de contenidos con explotación sexual a menores, grooming, etc...), el común denominador que impulsa al resto de actividades delictivas en la red es el ánimo de lucro, sin lugar a dudas. Estudios recientes, cuantifican el impacto económico del cibercrimen a nivel global en unos 400 mil millones de dólares. Si tenemos en cuenta la elevada cifra negra en estas tipologías, y la dificultad de cuantificar económicamente los daños sufridos por algunos tipos de ciberataques (denegación de servicio, robos de información confidencial, pérdida de imagen y reputación...) es posible que estas estimaciones se queden cortas.

La implantación de lo que se conoce como "El Internet de las cosas" en donde cualquier tipo de dispositivo estará conectado a la red y

FIGURA 1. Ejemplo de mercado underground

FIGURA 2. Ejemplo de *Ransomware* con el que "secuestran" nuestro equipo

el creciente volumen de información que volcamos en la red (incluyendo datos de carácter personal e información bancaria) genera nuevos vectores de ataque, en los que se combinan elementos técnicos como pueda ser el malware (software malicioso) con ingeniería social, y que serán aprovechados por redes de delincuentes para obtener un beneficio económico de cualquier brecha de seguridad que encuentren y sean capaces de rentabilizar. Sin profundizar demasiado en la problemática inherente a la persecución de estos delitos, es necesario reseñar que debido a la complejidad de este entorno global donde los límites geográficos han quedado obsoletos, la interacción entre sujetos sometidos a distintas jurisdicciones y soberanías nacionales, genera disfunciones que son aprovechadas por los delincuentes para cometer sus actos a miles de kilómetros de distancia, a las que hay que sumar la utilización de sistemas de anonimización (VPNs, proxies, darknets...) con los que dificultar la investigación policial.

Existen pues auténticas organizaciones criminales dedicadas al ciberdelito como "modelo de negocio" con estructuras especializadas en diversas actividades y reparto de cometidos y funciones entre sus miembros. Organizaciones que al igual que en la delincuencia clásica tienen distinto nivel de profesionalización, y en el que podemos encontrar desde el envío de cartas nigerianas (correos en el que nos ofrecen una elevada suma de dinero por una supuesta herencia, premio de lotería, inversión) o "phishing" (página réplica de otra original, generalmente de un banco, servicio de correo o red social, para que introduzcamos nuestras credenciales de acceso y sean capturadas) que son muy básicos y fácilmente detectables, hasta otras que son capaces de acceder a los sistemas informáticos de grandes empresas y corporaciones para robar información por encargo mediante técnicas de hacking y la utilización de malware y exploits de día cero (vulnerabilidades de aplicaciones y sistemas desconocidas y por lo tanto no parcheadas, muy cotizadas en el mercado negro ya que permitirían a un atacante acceder de forma remota y tomar el control del sistema).

Sin embargo, en este continuo proceso de industrialización del cibercrimen ya no hace falta disponer de elevados conocimientos técnicos para el desarrollo de este tipo de actividades, ya que de ello se encargan otras organizaciones e individuos que son capaces de proveer productos y servicios previo pago en un modelo conocido como Caas (Crime as a service). No es complicado acceder a

un foro "underground", (ubicados en alguna darknet, siendo TOR la más popular), que se configura como un auténtico mercadillo digital. ¿Qué podemos encontrarnos? Venta de tarjetas de crédito, clasificadas por países y tipo, y con garantía, de tal forma que si vamos a realizar alguna transacción y su usuario legítimo ha denunciado, nos enviarán una nueva numeración en 24h sin coste adicional. Podemos adquirir un troyano para infectar y espiar a quien queramos de forma sencilla, ya que los paneles de control se diseñan de forma intuitiva para el usuario más inexperto. También podemos alquilar una botnet (red de ordenadores infectados que el administrador puede manejar y controlar a su antojo, hasta millones de equipos de forma simultánea) para realizar un ataque de denegación de servicio y dejar sin conexión a la competencia, aunque en denegaciones de servicio ya es posible contratarlo directamente a la carta, con precios por minuto, hora, día, semanas....

A estas estructuras criminales, se complementan otras encargadas del posterior blanqueo del dinero obtenido, ayudadas por el desarrollo de nuevos mecanismos de pago surgidos en la propia red y que dificultan la trazabilidad de dichas transacciones. Entre estos mecanismos, les resultan especialmente beneficiosos la utilización de tarjetas prepago anónimas, las criptodivisas (siendo la más popular Bitcoin) o la operativa en páginas de juego online, aprovechando aquellas ubicadas en países con deficiente o nula legislación sobre la materia y sin supervisión. Dichas estructuras también son aprovechadas por otras organizaciones criminales (narcotráfico, tráfico de armas, prostitución...) e incluso terroristas, ya que permiten como hemos visto el movimiento de capitales con sencillez, a nivel global, con bajas comisiones y poco control.

¿Hacia dónde evoluciona el cibercimen? No abandonan las actividades más tradicionales, que tienen una tasa de éxito cada vez más baja gracias a las campañas de concienciación, pero que son muy fáciles de llevar a cabo y consumen muy pocos recursos (fraudes y estafas simples, phishing, robos de información con infecciones masivas). Estas convivirán con otras tipologías más avanzadas técnicamente, como son los ataques dirigidos sobre objetivos seleccionados, el spear phishing y nuevas modalidades de extorsión asociadas a un pago a cambio de no revelar una información, un secreto, unas imágenes comprometidas... Sirva de ejemplo la evolución de las familias de malware conocidas como "Ransomware" debido al "secuestro" que sufre nuestro equipo informático.

Las primeras versiones, conocidas como "el virus de la policía" simulaban (a través del bloqueo del sistema y un pantallazo con logotipos policiales) haber sido detectado cometiendo actividades ilegales a través de ese equipo, hechos que podrían quedar en nada penalmente si se pagaba una multa de 100 euros. A pesar de lo incongruente del procedimiento sancionador, y de las campañas preventivas lanzadas en medios de comunicación, se estiman beneficios de millones de euros con este modus operandi. Pues bien, sin haber agotado este modelo de negocio, iniciaron otro con otras familias de Ransomware (Cryptolocker, Cryptowall, CTB-Locker) consistente en que la información del sistema queda cifrada, y por tanto inaccesible, a no ser que se abone una cantidad económica, muy superior en estos casos a los 100 euros de los ejemplos anteriores. La incidencia que está teniendo en Pymes y ciudadanos es asombrosa, y los daños producidos y afectación económica imposibles de cuantificar.

La especialización llega a niveles desconocidos, en los que se diseña malware específico para cajeros automáticos, para terminales de venta en los comercios, y en un futuro para todo aquello que esté conectado a la red y sobre el que alguien pueda obtener nuestro dinero de manera ilegal, incluidos nuestros electrodomésticos, vehículos, etc...

Ante este panorama, sólo cabe unir esfuerzos y luchar contra el cibercrimen de manera conjunta y coordinada desde todos los sectores. Desde la industria, es necesario contemplar la seguridad de los equipos y sistemas desde su desarrollo (el concepto de security by design) para reducir vectores de ataque y vulnerabilidades. Fundamental seguir trabajando en la concienciación y educación, desde las edades más tempranas, para conseguir una ciudadanía digital capaz de obtener todas las ventajas que nos aportan las TIC pero minimizando los riesgos. Y las administraciones, aprovechando la Estrategia de Ciberseguridad Nacional como vertebración de todos los recursos disponibles, sin olvidar el componente de cooperación internacional que es fundamental para que la lucha contra estas nuevas amenazas sea eficaz. ✱