**¿Qué pretenden hacer los ciber-delincuentes con el dinero obtenido ilícitamente?**

*Sophos revela cómo consideran blanquearlo en negocios legítimos, actividades sospechosas y otras ilegales, incluyendo start-ups, plataformas pornográficas y esquemas piramidales*

**MADRID, España — 14 de agosto de 2025 –** Los ciber-delincuentes están considerando blanquear sus ganancias ilícitas invirtiendo tanto en negocios legítimos como en actividades sospechosas o ilegales. Así se desprende de un informe de Sophos, que desvela cómo los cibercriminales están adoptando diversas prácticas para integrarse en la economía, ocultar sus actividades y aumentar su capital.

Titulado ‘*Beyond the Kill Chain: What Cybercriminals Do with Their Money,* y elaborado por Sophos X-Ops (el grupo de trabajo conjunto de investigación y respuesta frente a amenazas avanzadas de Sophos), el estudio analiza partes de foros en los que los actores de amenazas debaten cómo y dónde invertir el dinero obtenido a través de ciber-delitos con motivaciones económicas.

La rentabilidad del ransomware (y otros ciber-delitos con fines financieros) crea, irónicamente, un complejo desafío financiero para las operaciones delictivas. Por ejemplo, cuando las fuerzas del orden desmantelaron la infraestructura del ransomware LockBit, la organización [poseía](https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-has-over-110-million-in-unspent-bitcoin/) bitcoins sin gastar por un valor superior a 110 millones de dólares, mientras ALPHV/BlackCat [recibió](https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/) 22 millones de dólares en un solo pago de rescate.

*“Los criminales no sólo operan en las sombras de Internet, sino que también abusan de identidades legales y redes de negocio*”, afirma **John Shier, Field CISO en Sophos**. *“Sus discusiones implican crear una apariencia de legitimidad con el capital robado*”.

**Una red global de empresas legales**

Sophos X-Ops dedicó meses a analizar foros de la darknet para identificar cómo los actores de amenazas discutían sobre el blanqueo y la inversión de capitales. Las conversaciones abarcan operaciones desde Asia hasta Europa Occidental, mencionando países como Reino Unido, Suiza, Emiratos Árabes Unidos, Estados Unidos, China, Corea del Sur y Gibraltar.

Algunas opciones de inversión mencionadas por los ciber-delincuentes son startups de ciberseguridad y TI, proyectos inmobiliarios y activos refugio (como oro y diamantes), así como restaurantes, bares y negocios de hostelería. También se mencionaron ONGs y empresas de alcohol y tabaco, posiblemente debido a su flujo de caja.

**El lado oscuro del emprendimiento**

Además de estos ‘nuevos’ negocios legales, la investigación de Sophos señala conversaciones de inversión en negocios sospechosos y en actividades abiertamente criminales que combinan lo digital con lo físico, lo legal con lo criminal y lo visible con lo invisible.

Entre ellas se incluyen plataformas pornográficas y juegos de azar on line, donde es difícil rastrear el origen del capital. Otras actividades mencionadas incluyen servicios ilegales de generación de documentos, esquemas piramidales, evasión fiscal y venta de productos farmacéuticos.

*“La profesionalización del cibercrimen es una realidad. Ya no vemos a los hackers simplemente presumiendo de sus lujos en redes sociales; ahora se comportan como inversores, desarrollando planes de negocio y buscando la rentabilidad a largo plazo”,* continúa el directivo de Sophos. “*Lo más preocupante es que, al invertir en sectores tradicionales o infraestructuras críticas, pueden influir en mercados legítimos mientras siguen operando en la clandestinidad digital”.*

Esta convergencia entre el cibercrimen y la economía real plantea desafíos para gobiernos, autoridades reguladoras, agencias tributarias, bancos y empresas privadas. El dinero de origen delictivo no sólo alimenta la ciber-delincuencia, sino que también puede distorsionar los mercados, competir deslealmente con empresas legítimas o financiar nuevos ataques desde estructuras aparentemente legítimas.

*“El cibercrimen no termina con un ataque. La única manera de abordar esta amenaza es mediante la cooperación internacional, la colaboración entre analistas de ciber-amenazas y el sector público, y una mayor vigilancia para detectar patrones financieros y actividades económicas sospechosas, especialmente en sectores de alto riesgo”*, concluye Shier.

**Acerca del informe**

El informe ‘*Beyond the Kill Chain: What Cybercriminals Do with Their Money’* se basa en una extensa investigación que abarca debates en foros de la darknet. Consta de cinco capítulos e incluye análisis detallados de las conversaciones entre actores de amenazas, así como las implicaciones y oportunidades relacionadas para la industria de la seguridad, los investigadores criminales y la sociedad en general. Puedes acceder aquí:

* [Parte 1](https://news.sophos.com/en-us/2025-05-15/beyond-the-kill-chain-what-cybercriminals-do-with-their-money-part-1)
* [Parte 2](https://news.sophos.com/en-us/2025-05-15/beyond-the-kill-chain-what-cybercriminals-do-with-their-money-part-2)
* [Parte 3](https://news.sophos.com/en-us/2025-05-15/beyond-the-kill-chain-what-cybercriminals-do-with-their-money-part-3)
* [Parte 4](https://news.sophos.com/en-us/2025-05-15/beyond-the-kill-chain-what-cybercriminals-do-with-their-money-part-4)
* [Parte 5](https://news.sophos.com/en-us/2025-05-15/beyond-the-kill-chain-what-cybercriminals-do-with-their-money-part-5)

**Acerca de Sophos**

Sophos es un líder mundial e innovador en soluciones de seguridad avanzadas para combatir los ciberataques. La compañía adquirió Secureworks en febrero 2025, uniendo a dos proveedores pioneros que han redefinido el sector de la ciberseguridad con sus innovadores servicios, tecnologías y productos nativos optimizados para IA. Sophos es actualmente el mayor proveedor especializado en servidos de Detección y Respuesta Gestionadas (MDR), dando soporte a más de 28.000 empresas. Además de MDR y otros servicios, el completo porfolio de Sophos incluye seguridad líder en el sector para terminales, redes, correo electrónico y la nube, que interoperan y se adaptan para defender a través de la plataforma Sophos Central.

Secureworks ofrece el innovador Taegis XDR/MDR, líder del mercado, detección y respuesta frente a amenazas de identidad (ITDR), funcionalidades SIEM de última generación, gestión de riesgos y un completo conjunto de servicios de consultoría. Sophos comercializa todas estas soluciones a través de su red de distribuidores, proveedores de servicios gestionados (MSPs) y proveedores de servicios de seguridad gestionados (MSSPs) en todo el mundo, protegiendo a más de 600.000 organizaciones a escala global del phishing, ransomware, robo de datos y otros ciberdelitos cotidianos e incluso patrocinados por estados. Las soluciones se basan en la información histórica y en tiempo real sobre amenazas de Sophos X-Ops y la recién incorporada Unidad de Contraamenazas (CTU, Counter Threat Unit). Sophos tiene su sede en Oxford, Reino Unido. Para obtener más información, visita [www.sophos.com](https://www.sophos.com/en-us) / <https://www.sophos.com/es-es>.

**Para obtener más información:**

[**TEAM Lewis**](http://www.teamlewis.com/es)

Nina Janmaat

[nina.janmaat@teamlewis.com](mailto:nina.janmaat@teamlewis.com)

Tel: 91 926 62 82