**El malware común desplaza al ransomware como principal ciber-amenaza**

*Entre abril y junio los ataques tipo troyano supusieron el 20% del total, afectando principalmente a los sectores de telecomunicaciones, educación y salud, según Cisco Talos*

**Madrid, 27 de julio de 2022.** – Por primera vez en los últimos 18 meses, el ransomware ha dejado de ser la principal ciber-amenaza para las empresas, pasando a suponer del 25% del total de amenazas al 15% entre abril y junio del presente año.

Así se desprende del último informe trimestral de Cisco Talos, la mayor organización privada de inteligencia frente a ciber-amenazas del mundo. El ‘commodity malware’[[1]](#endnote-1) se convirtió en la amenaza más frecuente a la que respondió Cisco Talos Incident Response durante el segundo trimestre, acaparando el 20% frente al 15% del ransomware.

Los datos también desvelan que los ciber-delincuentes dirigieron el malware a una amplia gama de sectores como transporte, fabricación y administración pública, siendo telecomunicaciones el más atacado y seguido por educación y salud.

**Factores del cambio**

Según la investigación de Cisco Talos, es probable que este cambio se deba a diversos factores, como el cese de actividad de algunos grupos de ransomware -ya sea por fractura interna o por las acciones de las fuerzas de seguridad- y el resurgimiento de ciertos troyanos basados en e-mail como Remcos, Vidar, Redline y Qakbot/Qbot (este último un conocido troyano bancario). Phishing, Business Email Compromise y las amenazas persistentes avanzadas (APTs) completan la lista de malware destacado.

A pesar del descenso de actividad, los grupos de ransomware como servicio (RaaS) de alto perfil incluyendo Conti -probablemente rebautizado como ‘Black Basta’- y BlackCat han seguido actuando, dirigiéndose a organizaciones supuestamente capaces de afrontar grandes pagos. De hecho, el ransomware LockBit lanzó una nueva versión que incluye más opciones de pago en criptomoneda.

Cisco Talos también ha seguido detectando técnicas de ingeniería social para incitar a los usuarios a hacer clic o ejecutar un enlace o archivo determinado. Y aunque el principal país objetivo de los ciber-delincuentes sigue siendo Estados Unidos, se mantiene la actividad de ciber-ataques dirigidos a empresas y administraciones en Europa, Asia, Norteamérica y Oriente Medio.

Accede [aquí](https://blog.talosintelligence.com/2022/07/quarterly-report-incident-response.html) a la información completa sobre el informe.

**Acerca de Cisco**

Cisco (NASDAQ: CSCO) es el líder mundial en tecnología para Internet. Cisco inspira nuevas posibilidades reinventando las aplicaciones corporativas, protegiendo a las organizaciones, transformando su infraestructura y facilitando el trabajo colaborativo para avanzar hacia un futuro global e inclusivo. Descubre más en [news-blogs.cisco.com/emear/es](https://news-blogs.cisco.com/emear/es/) / [The Network](https://newsroom.cisco.com/) <http://cisco.mwnewsroom.com/es/es> y síguenos en [twitter.com/cisco\_spain](https://twitter.com/cisco_spain) y [twitter.com/Cisco](https://twitter.com/Cisco).

Cisco y el logotipo de Cisco son marcas comerciales o marcas registradas de Cisco y/o sus filiales en Estados Unidos y otros países. Puede encontrarse un listado de las marcas comerciales de Cisco en [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Las marcas comerciales de terceros mencionadas son propiedad de sus respectivos dueños. El uso de la palabra partner no implica una relación de asociación entre Cisco y cualquier otra empresa.

**Para obtener más información:**

[Cisco España](http://www.cisco.com/c/es_es/index.html)

Ariadna Hernández, Directora de Comunicación

[ariahern@cisco.com](mailto:ariahern@cisco.com)

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

Juan Ortiz

Tel: 91 926 67 05

E-mail: [juan.ortiz@teamlewis.com](mailto:juan.ortiz@teamlewis.com)

1. Malware ampliamente disponible para su compra o descarga gratuita, no personalizado y utilizado por diversos tipos de ataque. [↑](#endnote-ref-1)