Mexico Ransomware Task highlights value of disrupting criminal infrastructure, commits to public awareness campaign

The Mexico RTF recommends a public-private effort to disrupt criminal infrastructure and create a national repository of resources for use in ransomware attacks

MEXICO CITY, CA, MEXICO, August 13, 2026 /EINPresswire.com/ -- Yesterday, the 40+ members of the México Ransomware Task Force endorsed a set of actionable recommendations for the Mexican multistakeholder community to combat the threat of ransomware. The recommendations highlight that, while ransomware poses a serious and growing threat to Mexico's economic and national security, there are actionable steps that citizens, companies, and the government can take to protect and defend against it. The México Ransomware Task Force emphasizes that the recommendations made by the task force are a cohesive and mutually reinforcing set of actions. Together, they provide a comprehensive approach to strengthening Mexico's resilience against ransomware.

The task force, led by the non-profit Institute for Security and Technology alongside a coalition of global and local partners, brings together leaders from government, industry, civil society, and academia in pursuit of practical recommendations for strengthening Mexico's resilience against the threat of ransomware and other cybercrime. It is modeled after IST's flagship Ransomware Task Force, which developed 48 recommendations to combat ransomware in the United States and worldwide in 2021 and has since observed preliminary or significant progress on 91 percent of those recommendations.

The recommendations made today are the result of months of preparatory work, culminating in a day-long conference hosted at Mastercard's Mexico City office. At the conference, members of the initiative articulated specific recommendations for the Mexican multistakeholder community in order to achieve four complementary goals:

- Deter ransomware attacks
- Disrupt the ransomware business model
- Help organizations prepare for ransomware attacks
- More effectively respond to ransomware attacks

Working groups for each of these goals were chaired by FTI Consulting and a member of civil society for Deter; Chainalysis and Mastercard for Disrupt; Microsoft and Scitum for Prepare; and

Delta Protect for Respond. Organizations that participated include the following: AMITI; Bitso; Capa8; CrowdStrike; Delta Protect; GNP Seguros; KIO IT Services; Mifel Bank; the Technological Institute of Monterrey; the Mexico Office of the United Nations Office on Drugs and Crime (UNODC); the Secretariat of Security and Citizen Protection (SSPC); and the University of Guadalajara.

Each working group has articulated concrete, actionable recommendations for how Mexican society can tackle the scourge of ransomware. Recommendations affirmed during the conference include the following:

- Reinforce national measures for accountability and increase attribution capabilities / Fortalecer medidas nacionales para la rendición de cuentas e incrementar capacidades de atribución
- Launch a national campaign to disrupt criminal infrastructure / Lanzar una campaña nacional para la disrupción de infraestructura criminal
- Develop a public awareness plan to promote ransomware readiness / Generar una estrategia de comunicación para promover la preparación ante el ransomware
- Develop and publish an executive guide for ransomware response / Desarrollo y publicar una Guía Ejecutiva de Respuesta ante Ransomware.

The group will continue to collaborate as they finalize the formal process of the México Ransomware Task Force. Coming out of today's conference, working group co-chairs and members are going to begin the hands-on process of implementation, with formal collaboration under the RTF banner continuing through the end of 2026. In November 2026, IST and working group co-chairs will publish a report with more specifics on each of the recommendations and pathways towards implementation. Critically, the connections forged between government, civil society, and industry will continue to pay dividends long after the formal process has concluded.

The México Ransomware Task Force reflects a shared commitment to strengthening public-private collaboration and enhancing national resilience against cyber threats. IST is honored to partner with the Mexican and global multistakeholder community to share these recommendations with Mexican society, and to support efforts to implement them over the coming months. Convened by the Institute for Security and Technology, a non-profit, non-partisan organization, the initiative is made possible through the support of Mastercard, Microsoft, and Sophos.

Sophia Mauro
Institute for Security and Technology
email us here

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.