DIGI AMERICAS ALLIANCE MEMBERS

WHITE HOUSE: CHINESE TELECOM HACKS HAVE BEEN IN MOTION FOR YEARS

CyberScoop - A White House official says the Salt Typhoon hack has impacted eight telecom companies in the United States, with dozens of other countries also affected, and has been in motion for as long as two years. The information comes as U.S. administration officials said earlier this week that the hacking group, linked to the Chinese government, is still believed to be in U.S. telecom networks. The government began investigating the breach this past spring, and are continuing to assess its full scope.The spying efforts targeted officials from both presidential campaigns, including the phone of President-elect Donald Trump.

COMUNICADO CONJUNTO DE LA EMBAJADA DE LOS ESTADOS UNIDOS EN PARAGUAY Y EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (MITIC)

U.S. Embassy - El gobierno del Paraguay, en colaboración con el Comando Sur de los Estados Unidos, completaron recientemente una revisión conjunta de ciberseguridad de las redes del gobierno paraguayo diseñada para fortalecer la seguridad de los activos críticos de la nación. Durante la revisión, se identificó al actor de ciberespionaje Flax Typhoon -un grupo basado en la República Popular China con vínculos con el gobierno de la RPC- infiltrándose en los sistemas del gobierno paraguayo. Infiltraciones recientes a la infraestructura privada de telecomunicaciones en los Estados Unidos demuestran la importancia de la cooperación y el fortalecimiento de la infraestructura crítica, especialmente en el ámbito cibernético y de comunicaciones, para reducir las vulnerabilidades.

PIDEN INFORME DETALLADO SOBRE CIBERSEGURIDAD ESTATAL AL MITIC - PARAGUAY

Diputados - A instancias del diputado Carlos Núñez Salinas (ANR-Central), la Cámara de Diputados, en su sesión ordinaria de ayer, aprobó en el estadio de Sobre Tablas, un proyecto de resolución “Que pide informe al Ministerio de Tecnologías de la Información y Comunicación (MITIC), sobre la gestión en materia de ciberseguridad estatal”. Mediante esta solicitud, se busca evaluar la planificación y ejecución de los recursos destinados a la protección de la infraestructura crítica y los datos sensibles del Estado.

GSI: ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA ESTÁ PRONTA PARA APROVAÇÃO - BRASIL

Convergencia Digital - A defesa cibernética do Brasil ainda aguarda a definição política sobre a criação de uma agência nacional especializada no tema, como proposto pelo Gabinete de Segurança Institucional. Um avanço no tema tem data prevista. No próximo 4 de dezembro, o Comitê Nacional de Cibersegurança vai deliberar sobre a proposta, já pronta, para uma Estratégia Nacional de Segurança Cibernética. Segundo “Na próxima reunião, vai ser dia 4 de dezembro, já está pronto o relatório, a proposta de estratégia que vai ser votada pelos representantes, o grupo de trabalho já finalizou esse processo”, revelou o secretário de Segurança da Informação e Cibernética do GSI, André Luiz Molina.

TCU: COM APENAS R$ 588 MIL, GOVERNO NÃO PRIORIZA SEGURANÇA CIBERNÉTICA E NEM PROPÕE CRIAÇÃO DA ANCIBER - BRASIL

Capital Digital - O Tribunal de Contas da União após a realização de uma auditoria operacional para avaliar a Política Nacional de Cibersegurança (PNCiber), constatou baixa maturidade na política de segurança cibernética em 254 órgãos integrantes do governo federal (SISP). Por conta desses achados, o tribunal recomendou que a Casa Civil da Presidência da República gerencie riscos e promova a criação da Agência Nacional de Cibersegurança (ANCiber), que executará a atual Política Nacional de Ciber Segurança (PNCiber), cujo orçamento em 2023 foi de apenas R$ 588 mil.

SE APROBÓ LA ESTRATEGIA NACIONAL DE INTELIGENCIA ARTIFICIAL 2024 - 2030 - URUGUAY

Gob.uy - El 21 de noviembre, el Comité Estratégico del Sector Público para la Inteligencia Artificial y Datos aprobó la nueva Estrategia de Inteligencia Artificial de Uruguay, con el objetivo de avanzar en una política pública de alcance nacional, con base en el desarrollo y uso ético de esta tecnología. El proceso de revisión de la Estrategia Nacional de Inteligencia Artificial fue liderado y articulado por Agesic, en coordinación con el Comité Estratégico del Sector Público para la Inteligencia Artificial y Datos, de acuerdo con lo establecido en el artículo 74 de la Ley N° 20.212 de 6 de noviembre de 2023. Contó con la cooperación técnica del Banco de Desarrollo de América Latina y el Caribe (CAF, por su sigla en inglés) y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, por su sigla en inglés).

GOBIERNO DISPONE NUEVA CONFORMACIÓN DEL COMITÉ NACIONAL DE CIBERSEGURIDAD - ECUADOR

Primicias - El presidente Daniel Noboa, a través del Decreto Ejecutivo 464, dispuso una nueva conformación del Comité Nacional de Ciberseguridad, con el propósito de coordinar y articular acciones en este ámbito en Ecuador. El documento expedido este viernes, 22 de noviembre de 2024, reforma al reglamento general a la Ley Orgánica de Transformación Digital y Audiovisual. El Comité tendrá como propósito "coordinar y articular acciones en el ámbito de la ciberseguridad, orientadas a la identificación de riesgos potenciales, la mitigación de vulnerabilidades, y el desarrollo, promoción, discusión, gestión oportuna e implementación de políticas y regulaciones respectivas, con el objetivo de fortalecer las capacidades de ciberseguridad".

ORGANIZACIONES PIDEN VETAR NUEVAS LEYES DE CIBERSEGURIDAD Y DATOS PERSONALES POR ATENTAR CONTRA LIBERTAD DE EXPRESIÓN Y PRENSA - EL SALVADOR

Prensa Gráfica - Organizaciones de la sociedad civil publicaron este 25 de noviembre un comunicado en el que expresan su preocupación por "el poder casi ilimitado" que tendrá la Agencia de Ciberseguridad del Estado y piden al presidente Nayib Bukele que observe o vete los decretos que dieron vida a las leyes de Ciberseguridad y Seguridad de la Información y de Protección de Datos Personales. El comunicado que se publicó en redes sociales es firmado por Acción Ciudadana, la Asociación de Periodistas de El Salvador (APES), Fundación Cristosal, TRACODA, el Instituto Centroamericano de Estudios Fiscales (ICEFI) y la Fundación Nacional para el Desarrollo (FUNDE) las cuales piden al presidente de la República que "observe o vete los decretos aprobados por la Asamblea Legislativa, por ser atentatorios de los derechos fundamentales a la libertad de expresión y de prensa".

TRAS HACKEOS A CENTROS MÉDICOS DEL GRUPO ROSSI, ESPECIALISTAS ALERTAN POR LA FALTA DE INVERSIÓN EN CIBERSEGURIDAD EN EL SECTOR SALUD - ARGENTINA

Forbes - Un ciberataque paralizó hace más de veinte días el funcionamiento de tres de los principales centros médicos de Argentina y administrados por el Grupo Rossi: el Centro Rossi, Stamboulian Servicios de Salud y el Laboratorio Hidalgo. El ataque tuvo consecuencias inmediatas. El Laboratorio Hidalgo suspendió toda su atención, mientras que en el Centro Rossi continúan haciéndose procedimientos médicos como resonancias magnéticas, tomografías y ecografías, pero sin conexión a los sistemas informáticos. En Stamboulian, la paralización afectó al laboratorio, aunque el servicio de vacunación sigue funcionando.

MICITT CONFIRMA INCIDENTES DE CIBERSEGURIDAD Y LLAMA A LA POBLACIÓN A ESTAR ALERTA - COSTA RICA

MICITT - El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) confirmó hoy que varias instituciones del país han sido afectadas recientemente por incidentes de ciberseguridad, entre ellas la Refinadora Costarricense de Petróleo (RECOPE), la Dirección de Migración y Extranjería y una empresa de comunicación masiva. El MICITT, a través del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR), trabaja en estrecha colaboración con las instituciones afectadas para contener los incidentes y restaurar los servicios. En el caso de Migración se trató de un incidente de intrusión, el cual logró ser contenido al detectarse y ahora se trabaja en la aplicación de medidas para fortificar los sistemas. Es importante destacar que en este caso no hubo afectación a los servicios de la institución pues se contuvo de forma inmediata.

INTERPOL BUSTS AFRICAN CYBERCRIME: 1,006 ARRESTS, 134,089 MALICIOUS NETWORKS DISMANTLED

Hacker News - An INTERPOL-led operation has led to the arrest of 1,006 suspects across 19 African countries and the takedown of 134,089 malicious infrastructures and networks as part of a coordinated effort to disrupt cybercrime in the continent. Dubbed Serengeti, the law enforcement exercise took place between September 2 and October 31, 2024, and targeted criminals behind ransomware, business email compromise (BEC), digital extortion, and online scams. The participating nations in the operation were Algeria, Angola, Benin, Cameroon, Côte d'Ivoire, Democratic Republic of the Congo, Gabon, Ghana, Kenya, Mauritius, Mozambique, Nigeria, Rwanda, Senegal, South Africa, Tanzania, Tunisia, Zambia, and Zimbabwe.

BARBADOS SIGNS US$500 MILLION MOU WITH USEXIM BANK

Barbados Today - Barbados and the U.S. Export-Import Bank (USExim Bank) have signed a US$500 million Memorandum of Understanding (MOU) to improve critical sectors, including renewable energy, cybersecurity, water and sanitation, and maritime domain awareness. The agreement, signed on Monday by Prime Minister Mia Amor Mottley and USExim Bank Chairwoman Reta Jo Lewis, will finance U.S.-made goods and services for government projects that align with the island's push for 100 per cent renewable energy by 2030 and enhanced digital security.

COLLABORATION IS KEY TO TACKLING CYBERCRIME. RECENT TAKEDOWNS SHOW WHY

WEF - Cybercrime is on the rise. In particular, cyber-enabled financial fraud has emerged as a boom industry for transnational crime. In 2024, scammers stole over more than $1 trillion from victims, according to the Global Anti-Scam Alliance. However, collaboration between law enforcement and experts drawn from the private sector and non-profits is demonstrating how it can be disrupted. This year saw a string of successful disruption campaigns targeting cybercrime groups that could be a blueprint for tackling the problem. In November 2024, for example, INTERPOL announced that an operation dubbed Operation Serengeti led to the arrests of more than 1,000 suspected cybercriminals responsible for 35,000 victims in 19 countries across all regions of Africa.

HOW TO PROTECT THE GLOBAL SUPPLY CHAIN FROM PHISHING SCAMS

WEF - The supply chain is a highly interconnected ecosystem of suppliers, manufacturers, logistics, retailers and finally, consumers. The exchange of goods and the flow of transportation between all of these various groups is the backbone of our global economy. But if disrupted, our interconnected world could face all types and levels of chaos – from stolen Christmas presents to empty shelves in grocery stores or hospitals being unable to get their hands on life-saving supplies.