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.

JOINT STATEMENT FROM THE EMBASSY OF THE UNITED STATES IN PARAGUAY AND THE MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGIES (MITIC)

U.S. Embassy - The Government of Paraguay, in collaboration with U.S. Southern Command, recently completed a joint cybersecurity review of Paraguayan government networks designed to strengthen the security of the nation's critical assets. During the review, cyber espionage actor Flax Typhoon - a People's Republic of China-based group with ties to the PRC government - was identified infiltrating Paraguayan government systems. Recent infiltrations of private telecommunications infrastructure in the United States demonstrate the importance of cooperation and strengthening critical infrastructure, especially in the cyber and communications realm, to reduce vulnerabilities.

DETAILED REPORT ON STATE CYBERSECURITY REQUESTED FROM MITIC - PARAGUAY

Deputies - At the request of Deputy Carlos Núñez Salinas (ANR-Central), the Chamber of Deputies, in its ordinary session yesterday, approved at the Sobre Tablas stadium, a draft resolution "Requesting a report from the Ministry of Information and Communication Technologies (MITIC), on management in the area of state cybersecurity." This request seeks to evaluate the planning and execution of resources allocated to the protection of critical infrastructure and sensitive State data.

GSI: NATIONAL CYBERSECURITY STRATEGY READY FOR APPROVAL - BRAZIL

Digital Convergence - Brazil's cyber defense is still awaiting political definition on the creation of a national agency specialized in the subject, as proposed by the Institutional Security Office. A breakthrough on the subject is scheduled. On December 4, the National Cybersecurity Committee will deliberate on the proposal, already prepared, for a National Cybersecurity Strategy. According to “In the next meeting, which will be on December 4, the report will be ready, the strategy proposal that will be voted on by the representatives, the working group has already finalized this process”, revealed the Secretary of Information and Cybersecurity of the GSI, André Luiz Molina.

TCU: WITH ONLY R$588 THOUSAND, THE GOVERNMENT DOES NOT PRIORITIZE CYBERSECURITY AND DOES NOT PROPOSE THE CREATION OF ANCIBER - BRAZIL

Digital Capital - The Federal Court of Auditors, after conducting an operational audit to evaluate the National Cybersecurity Policy (PNCiber), found low maturity in the cybersecurity policy in 254 federal government agencies (SISP). Due to these findings, the court recommended that the Civil House of the Presidency of the Republic manage risks and promote the creation of the National Cybersecurity Agency (ANCiber), which will execute the current National Cybersecurity Policy (PNCiber), whose budget in 2023 was only R$ 588 thousand.

THE NATIONAL ARTIFICIAL INTELLIGENCE STRATEGY 2024 - 2030 WAS APPROVED - URUGUAY

Gob.uy - On November 21, the Public Sector Strategic Committee for Artificial Intelligence and Data approved Uruguay's new Artificial Intelligence Strategy, with the aim of advancing a public policy of national scope, based on the development and ethical use of this technology. The review process of the National Artificial Intelligence Strategy was led and articulated by Agesic, in coordination with the Public Sector Strategic Committee for Artificial Intelligence and Data, in accordance with the provisions of article 74 of Law No. 20,212 of November 6, 2023. It had the technical cooperation of the Development Bank of Latin America and the Caribbean (CAF) and the United Nations Educational, Scientific and Cultural Organization (UNESCO).

GOVERNMENT ARRANGES NEW COMPOSITION OF THE NATIONAL CYBERSECURITY COMMITTEE - ECUADOR

News - President Daniel Noboa, through Executive Decree 464, ordered a new formation of the National Cybersecurity Committee, with the purpose of coordinating and articulating actions in this area in Ecuador. The document issued this Friday, November 22, 2024, reforms the general regulations of the Organic Law of Digital and Audiovisual Transformation. The purpose of the Committee will be "to coordinate and articulate actions in the field of cybersecurity, aimed at identifying potential risks, mitigating vulnerabilities, and the development, promotion, discussion, timely management and implementation of respective policies and regulations, with the aim of strengthening cybersecurity capabilities."

ORGANIZATIONS CALL FOR VETOING NEW LAWS ON CYBERSECURITY AND PERSONAL DATA FOR VIOLATING FREEDOM OF EXPRESSION AND PRESS - EL SALVADOR

Prensa Gráfica - Civil society organizations published a statement on November 25 in which they express their concern about "the almost unlimited power" that the State Cybersecurity Agency will have and ask President Nayib Bukele to observe or veto the decrees that gave life to the Cybersecurity and Information Security and Personal Data Protection laws. The statement that was published on social networks is signed by Citizen Action, the Association of Journalists of El Salvador (APES), Cristosal Foundation, TRACODA, the Central American Institute for Fiscal Studies (ICEFI) and the National Foundation for Development (FUNDE), which ask the President of the Republic to "observe or veto the decrees approved by the Legislative Assembly, for being an attack on the fundamental rights to freedom of expression and the press."

FOLLOWING HACKS AT ROSSI GROUP MEDICAL CENTERS, SPECIALISTS WARN OF A LACK OF INVESTMENT IN CYBERSECURITY IN THE HEALTH SECTOR - ARGENTINA

Forbes - A cyber attack paralyzed the operation of three of Argentina's main medical centers managed by the Rossi Group more than twenty days ago: the Rossi Center, Stamboulian Health Services, and the Hidalgo Laboratory. The attack had immediate consequences. The Hidalgo Laboratory suspended all its services, while medical procedures such as magnetic resonance imaging, CT scans, and ultrasounds continue to be performed at the Rossi Center, but without connection to the computer systems. At Stamboulian, the stoppage affected the laboratory, although the vaccination service continues to operate.

MICITT CONFIRMS CYBERSECURITY INCIDENTS AND CALLS ON THE POPULATION TO BE ALERT - COSTA RICA

MICITT - The Ministry of Science, Innovation, Technology and Telecommunications (MICITT) confirmed today that several institutions in the country have recently been affected by cybersecurity incidents, including the Costa Rican Oil Refinery (RECOPE), the Immigration and Foreign Affairs Directorate and a mass communication company. MICITT, through the Computer Security Incident Response Center (CSIRT-CR), is working closely with the affected institutions to contain the incidents and restore services. In the case of Immigration, it was an intrusion incident, which was contained when it was detected and work is now being done to implement measures to fortify the systems. It is important to note that in this case there was no impact on the institution's services as it was contained immediately.

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.