DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 26, 2024

DIGI AMERICAS ALLIANCE MEMBERS

PRELIMINARY POST INCIDENT REVIEW - CROWDSTRIKE

CrowdStrike - On Friday, July 19, 2024 at 04:09 UTC, as part of regular operations, CrowdStrike released a content configuration update for the Windows sensor to gather telemetry on possible novel threat techniques. These updates are a regular part of the dynamic protection mechanisms of the Falcon platform. The problematic Rapid Response Content configuration update resulted in a Windows system crash. Systems in scope include Windows hosts running sensor version 7.11 and above that were online between Friday, July 19, 2024 04:09 UTC and Friday, July 19, 2024 05:27 UTC and received the update. Mac and Linux hosts were not impacted. The defect in the content update was reverted on Friday, July 19, 2024 at 05:27 UTC. Systems coming online after this time, or that did not connect during the window, were not impacted.

GLOBAL IT OUTAGE: THE CYBER RESILIENCE ALARM HEARD AROUND THE WORLD

WEF - Last week, one of the largest IT outages in history disrupted businesses and governments around the world. The incident, which affected 8.5 million Microsoft Windows devices, led to widespread disruptions of airlines, banks, broadcasters, healthcare providers, retail payment terminals and cash machines globally. The cost of the outage is estimated to top $1 billion. The disruption was caused by a flawed update to a cloud-based security software of CrowdStrike, one of the global top cybersecurity companies. The update to the Falcon software triggered a malfunction that disabled parts of the computer systems and software like Microsoft Windows. Three days after the incident, CrowdStrike reported that a significant number of the devices are back online and operational.

SP PM SEIZES MOBILE CYBERCRIME UNIT - BRAZIL

CISO Advisor - The Military Police of São Paulo discovered, in a patrol action in the Capital, a vehicle equipped with an improvised “stingray”: a stingray is a portable device that transmits a cellular network signal, causing nearby cellular devices to connect to it as if you were connecting to an ERB antenna (radio base station) from a telecommunications operator. The arrest took place on the night of July 23rd, Tuesday of this week, on Avenida Professor Luiz Ignácio Anhaia Mello, in the East zone. The vehicle was a white Jeep Renegade, which was stopped because it aroused suspicion among the police when it was traveling with the lights off.

ESPERIDIÃO AMIN HIGHLIGHTS PUBLIC HEARING ON CYBERSECURITY - BRAZIL

Senate - Senator Esperidião Amin (PP-SC) highlighted, in a speech this Tuesday (16), a public hearing held by the Permanent Subcommittee on Cyber Defense (CREDC), last week, to debate international risks in cyber security and the importance of a national digital security agency in Brazil. The parliamentarian, who is president of the collegiate, highlighted that the World Economic Forum estimates that cybercrimes are affecting more than 10% of the gross domestic product (GDP) of Western countries.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 26, 2024

THEY WARN OF THE RELEASE OF “SENSITIVE INFORMATION” FROM THE DATABASE OF BOLIVIAN CITIZENS

El Deber - The Hacking Bolivia page warned that a “threat actor” is releasing the database of Bolivian citizens that contains “sensitive information” and that could be used by digital scammers. In addition, this same account assured that there was 'possible unauthorized access' to government systems and services. An expert explained that there are risks for an ordinary citizen if their private and personal information is accessed.

CYBERATTACK PARALYZED THE SYSTEMS OF A MUNICIPALITY ON THE COAST OF THE URUGUAY RIVER

El Entrerios - The Municipality of Paysandú suffered a cyber attack on Wednesday afternoon that inactivated a good part of the operations it usually carries out using Internet networks and services. The municipality described it as “a cybersecurity incident that affects the normal functioning of its systems”, which have not yet functioned normally. The Secretary General of the Municipality, Fermín Farinha, confirmed that “they are working together with CERTuy” , the National Computer Security Incident Response Center of Uruguay, made up of cybersecurity specialists from the Electronic Government and Knowledge Information Society Agency (Agesic).

IN ONE WEEK THE POLICE CYBERCRIME NETWORK INTERVENED IN NEARLY 50 CASES - ARGENTINA

El Territorio - Recently the Misiones Police put into operation a network of 30 agents specialized in Cybercrime, who are working in the 15 Regional Units. Since its inception, they have received numerous requests for advice from neighbors, as well as private and public entities, on measures to avoid scams and cybercrimes. The training of the officers, provided by the Cybercrime Directorate, focused on addressing the most common computer crimes, such as scams, hacking, phishing, grooming, preservation and kidnapping of devices, as well as extractions of film sequences in homes and shops for judicial evidentiary analysis.

PCM CARRIED OUT FIRST INTERNATIONAL CYBER ATTACK DRILL WITH 102 PUBLIC AND PRIVATE ENTITIES - PERU

Gob.pe - The Presidency of the Council of Ministers (PCM), through the Secretariat of Government and Digital Transformation, carried out the First International Cyber Attack Drill to reinforce the digital security capabilities of the country's public and private entities. For four hours in a row, 364 specialists from 102 entities were connected simultaneously, who faced a series of attack simulations in different digital scenarios designed by the National Digital Security Center, to observe the actions of the response teams in response to security incidents. digital security.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 26, 2024

NATIONAL GUARD INAUGURATES CYBERSECURITY DAY 2024 "SECURE INTERNET FOR ALL" - MEXICO

Gob.MX - With the aim of raising awareness and sensitizing society about the importance of the responsible use of information technologies, as well as promoting the culture of reporting crimes in the digital environment, the National Guard, through of the General Scientific Directorate, inaugurated the 2024 Cybersecurity Conference "Secure Internet for everyone". This is a joint effort between authorities and public and private service institutions, as well as civil society organizations, linked to the use of new technologies, who carry out a series of conferences, panels and interviews, aimed at preventing and confront new cybersecurity crimes, such as e-commerce fraud, identity theft, online sexual harassment or human trafficking, among others.

THEY PROMOTE CYBERSECURITY IN COMPANIES AND INSTITUTIONS IN GUANAJUATO - MEXICO

Mexico Industry - During the first quarter of 2024, Mexico experienced a 28 percent increase in cyberattacks compared to the same period in 2023, according to Check Point Research. Faced with these challenges, IDEA GTO and the companies ho1a Innovación and MetroCarrier of Megacable, through an alliance, will provide tools, knowledge and cybersecurity strategies for companies and institutions with the aim of promoting a culture of digital security that guarantees the protection of their information, networks and systems, in the face of environmental risks and threats.

WOMEN FROM COLOMBIA WILL BE ABLE TO TRAIN FOR FREE IN ARTIFICIAL INTELLIGENCE AND CYBERSECURITY - MINTIC

MINTIC - The ICT Ministry promotes the participation of the female gender in the technology industry, hence in alliance with the Hacker Girls community, it launches the 'Women Training Series' program, which will provide training, connection spaces and promote better job opportunities for 1,000 women who will be able to train for free in Artificial Intelligence and Cybersecurity. "We are working to encourage the participation of women in the technology sector and close the gender gap. That is why, with the Hacker Girls initiative, we support education spaces and job opportunities in areas associated with information technology We extend a very special invitation to all women in Colombia to be trained in these topics, which are increasingly becoming more relevant," said the ICT Minister, Mauricio Lizcano.

HUMAN RIGHTS ORGANIZATIONS WARN ABOUT THE RISKS OF THE CYBERCRIME TREATY TO BE DISCUSSED AT THE UN

Derechos Digitales - Human rights, digital rights and press freedom organizations met this July 24 with the media to address the risks of the UN treaty on Cybercrime. The treaty presents serious risks for the exercise of human rights and gender equality, as pointed out by the experts, Tirana Hassan, executive director of Human Rights Watch, Paloma Lara-Castro, public policy coordinator of Digital Rights, Katitza Rodriguez, director of Global Privacy Policy at the Electronic Frontier Foundation and Khadija Patel, president of the International Press Institute.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 26, 2024

NASA'S SCIENCE MISSION SPACECRAFT ARE AT RISK FROM HACKERS, BUT A NEW LAW COULD HELP PROTECT THEM

The Conversation - Nasa's missions are some of the most technologically advanced and critically important endeavours. From the Mars Rover explorations to the Artemis missions to the Moon, the space agency's projects push the boundaries of science and technology. However, these missions are also prime targets for cyber-attacks. In a bold move to counter the escalating threat of these attacks, US congressmen Maxwell Alejandro Frost and Don Beyer have proposed the Spacecraft Cybersecurity Act. If passed, the legislation would mandate the US space agency Nasa to overhaul the way it procures and builds its spacecraft.

THE NEED FOR A STRATEGIC APPROACH TO DISINFORMATION AND AI-DRIVEN THREATS

Rusi - Recent changes in governments across NATO countries – with the potential for more in the near future – have unfolded as several countries commit to increased levels of defence spending. UK Prime Minister Keir Starmer went even further by declaring his government's intention to reach a 2.5% commitment and announcing plans to publish a 2025 strategic defence review. The shift in support of defence spending is driven in part by concerns that a potential second Trump presidency will lead to a US retreat from NATO countries that fail to meet the 2% GDP defence spending threshold. Additionally, the current threat of kinetic warfare on the European continent – unprecedented since the Second World War – has compelled many European countries to enhance their military capabilities and bolster their defence institutions more broadly. This includes investing in modern, more technology-enabled capability, boosting weapons production, and launching extensive armed forces recruitment programmes.

RUSSIA'S CYBER CAMPAIGN SHIFTS TO UKRAINE'S FRONTLINES

Rusi - With the main thrust of Russia's anticipated summer offensive underway, it is an opportune moment to take stock of the significant and underappreciated changes that have taken hold in Moscow's approach to cyber operations in Ukraine. Much Western analysis to date has fixated on Russia's highly visible opening cyber offensive, the merits of its approach, and the potential for a renewed destructive campaign of a similar nature against Ukrainian critical infrastructure. This focus is misplaced, however, and has anchored Western understanding of the war's cyber dimensions to Russia's countervalue strategy to amass societal pressure via the widespread sabotage of computer networks – an approach that has not seen primacy since the invasion's first year when assumptions about a short war still guided Russia's theory of victory.