Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

Public Transportation ISAC
Transit & Rail Intelligence Awareness Daily Report (TRIAD)

November 12, 2024

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) MONTH

Transportation Systems Sector Cybersecurity Framework Implementation Guide

The Transportation Systems Sector Cybersecurity Framework Implementation Guidance and its companion workbook provide an approach for Transportation Systems Sector owners and operators to apply the tenets of the National Institute of Standards and Technology Cybersecurity Framework to help reduce cyber risks. Specifically, organizations may use the implementation guidance to:

- Characterize their current cybersecurity posture.
- Identify opportunities for enhancing existing cyber risk management programs.
- Find existing tools, standards, and guides to support Framework implementation.
- Communicate their risk management issues to internal and external stakeholders

Organizations that lack a formal cybersecurity risk management program could use the guidance to establish risk-based cyber priorities.
https://www.cisa.gov/resources-tools/resources/transportation-systems-sector-cybersecurity-framework-implementation-guide

Additional Resources:

- National Institute of Standards and Technology Cybersecurity Framework http://www.nist.gov/cyberframework/
- Transportation Systems Sector Cybersecurity Framework Implementation Guide https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Man Shot At Boston MBTA Station, Red Line Service Affected
NECN, 11/9/2024

[Boston, Massachusetts] A man was shot on a platform at the MBTA Red Line's Broadway Station in Boston Friday evening, police said. The man is expected to survive the gunshot wound to his lower extremities, according to the MBTA Transit Police, which said it was investigating the shooting, reported about 5:30 p.m. The man was rushed to the hospital. A witness told NBC10 Boston the man was shot in

the leg. Transit police shut down rail service as they searched for the gunman. No arrests have been made. https://www.necn.com/news/local/boston-mbta-red-line-shooting/3384703/

Spirit Airlines Flight From Florida Hit By Gunfire While Trying To Land In Haiti
FOX News, 11/11/2024

[Haiti] A Spirit Airlines flight out of Florida was struck by gunfire on Monday while making a landing in Port-au-Prince in Haiti on Monday. A spokesperson for the airline told Fox News Digital Spirit flight 951 from Fort Lauderdale, Florida, was diverted to Santiago, Dominican Republic, where it landed safely after being hit by gunfire. After arriving in the Dominican Republic, an inspection found evidence of damage to the aircraft that was consistent with gunfire. While none of the guests on board were injured, one flight attendant on the aircraft reported minor injuries and was being evaluated by medical personnel. https://www.foxnews.com/us/spirit-airlines-flight-from-florida-hit-gunfire-while-trying-land-haiti

ANALYST COMMENTARY: On 11 November 2024, two U.S.-based airlines reported that their passenger jets sustained damage from gunfire while flying over Port-au-Prince, Haiti. A Spirit Airlines plane flying from Florida to Haiti was targeted while approaching the Haitian capital and diverted to the Dominican Republic where "an inspection revealed evidence of damage to the aircraft consistent with gunfire." The same day, Jet Blue announced that a post-flight inspection found bullet holes in one of their planes that had flown from Haiti to New York. Following the incidents, a notice to airmen (NOTAM) was published advising that the Port-au-Prince airport was closed to air traffic operations from 2 p.m. on 11 November to 18 November. Multiple U.S. airlines announced that they would be temporarily suspending service to Haiti citing safety concerns stemming from the ongoing civil unrest in the country. In 2020, two Haitian gang coalitions were formed, and since then, the coalitions have been fighting each other, vigilante groups, and government forces for territorial control which has resulted in a large-scale conflict. The conflict has left approximately 600,000 Haitians homeless and hundreds of thousands of other Haitians have fled the country. In February 2024, Haitian gangs launched a series of coordinated attacks and took control of Haitian airports, prisons, and government facilities, which they held on to until May 2024. The Haitian police are outnumbered and outgunned by the gangs, and while they have been successful in retaking airport and prison control from the gangs, they have been unable to retake control of the city as a whole. A United Nations report released in September 2024 claimed that Haitian gangs currently control 85 percent of Port-au-Prince.

Suspect Arrested In String Of At Least 10 Stabbing Attacks In Seattle
CBS News, 11/9/2024

[Seattle, Washington] A man has been arrested in connection with a spate of random stabbings over two days in Seattle, in which a woman and nine men were injured — five of them on Friday afternoon, police said. Suspect Roland J. Lee appeared in court on Saturday to face at least five counts of assault in the first degree, the King County Prosecutor's Attorney Office said. The court set bail at $2 million. "This incident

was apparently one individual over a 38-hour period of time committing random assaults," Deputy Chief Eric Barden said at the scene Friday. The stabbings on Friday afternoon took place in a roughly four-block area in Seattle's Chinatown-International District. https://www.cbsnews.com/news/seattle-stabbing-attack-suspect-arrested/

ANALYST COMMENTARY: On 8 November 2024, Seattle police arrested Roland J. Lee, age 37, in connection with a series of random stabbings that occurred in Seattle, Washington over 38 hours. On 7 November 2024, Seattle police responded to four different stabbings in the vicinity of the Chinatown-International District between 12 a.m. and 11 p.m. that they believe were perpetrated by Lee. At approximately 2 p.m. on 8 November, five more people were stabbed in the Chinatown-International District. A witness who saw the 8 November attacks claims they saw a man "calmly" walk up to a victim, stab them in the back, then walk down the street and stab three other random people waiting on a street corner. Police responded to the scene and arrested Lee after a short chase. According to the King County Senior Deputy Prosecutor Ian Michels-Slettvet, Lee has an "extreme" criminal history with nine felony convictions in the past 10 years and had a warrant out for his arrest at the time of the stabbings. Lee is currently in jail with a $2 million bail, though no charges have been announced against him yet. Most of the victims were stabbed in the upper body or neck, some multiple times. While none of the victims were killed during the stabbings, three remain in serious condition. Police are investigating the incident and believe that the attacks were random. Three knives used in the stabbings were recovered from the scenes.

Arrest Made In Tuskegee University Shooting That Left 1 Dead, 16 Injured
NPR, 11/10/2024

[Tuskegee, Alabama] Authorities are investigating a shooting that happened early Sunday during homecoming celebrations on the Tuskegee University campus in the city of Tuskegee, Ala., that left one person dead and 16 injured, according to the Alabama Law Enforcement Agency. Jaquez Myrick, a 25-year-old from Montgomery, Ala., was found leaving the scene of the shooting and carrying a handgun with a machine gun conversion device, the agency said in a statement. Myrick has been arrested and federally charged with possession of a machine gun. The university said law enforcement has secured the scene and the ALEA's Bureau of Investigations is investigating. https://www.npr.org/2024/11/10/nx-s1-5185988/tuskegee-university-shooting-homecoming-alabama

TERRORISM & EXTREMISM

Financial Action Task Force Identifies Jurisdictions With Anti-Money Laundering, Combating The Financing Of Terrorism, And Counter-Proliferation Finance Deficiencies
FinCEN, 10/30/2024

[Washington D.C.] The Financial Crimes Enforcement Network (FinCEN) is informing U.S. financial institutions that the Financial Action Task Force (FATF), an intergovernmental body that establishes international standards for anti-money laundering, countering the financing of terrorism, and countering the financing of proliferation of weapons of mass destruction (AML/CFT/CPF), updated its lists of jurisdictions with strategic AML/CFT/CPF deficiencies at the conclusion of its plenary meeting this month. U.S. financial institutions should consider the FATF's stance toward these jurisdictions when reviewing their obligations and risk-based policies, procedures, and practices. On October 25, 2024, the FATF added Algeria, Angola, Côte d'Ivoire, and Lebanon to its list of Jurisdictions Under Increased Monitoring and also removed Senegal from the list. https://www.fincen.gov/news/news-releases/financial-action-task-force-identifies-jurisdictions-anti-money-laundering-1

ANALYST COMMENTARY: On 23-25 October 2024, 200 global jurisdictions met in Paris, France as part of the Financial Action Task Force (FATF) to discuss the integrity of the monetary system and protections against money laundering, terrorism financing and nuclear/weapons of mass destruction (WMD) proliferation financing. The Financial Crimes Enforcement Network (FinCEN) which represents the United States, issued a report regarding the outcome of the meeting. The FATF's list of High-Risk Jurisdictions Subject to a Call for Action remains the same, with Iran, the Democratic People's Republic of Korea (DPRK), and Burma subject to calls for action. Iran and DPRK are still subject to the FATF's countermeasures, while Burma is still subject to the application of enhanced due diligence, but not countermeasures. FinCEN also emphasized that U.S. financial institutions are required to have "appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to enable the covered financial institution to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed in the United States for a foreign financial institution (FFI). The DPRK and Iran are causing trouble for the global financial system and as identified high-risk jurisdictions, U.S. financial institutions must comply with the extensive U.S. restrictions and prohibitions against opening or maintaining any correspondent accounts, directly or indirectly, for North Korean or Iranian financial institutions.

'Glorifying Terrorism' Charges – France Sentences Pro-Palestine Activist To Three Years
The Palestine Chronicle, 11/7/2024

[France] The founder of the 'De Nice a Gaza' (From Nice to Gaza) organization was handed a three-year prison sentence, with two years suspended and one year served under an electronic bracelet. A French

court has sentenced a nursing student to three years in prison for "glorifying terrorism" on social media, according to broadcaster France 3, cited by various news reports. Amira Zaiter, from the southern city of Nice, was arrested on September 19 for "promoting terrorism, glorifying crimes against humanity, and spreading hate speech online," the channel said. In 2021, France adopted the definition of antisemitism proposed by the International Holocaust Remembrance Alliance (IHRA), which deems criticism of Israel and Zionism and comparing Israel's practices to those of the Nazis forms of antisemitism, QNN reported. https://www.palestinechronicle.com/glorifying-terrorism-charges-france-sentences-pro-palestine-activist-to-three-years/

SECURITY & SAFETY AWARENESS

Putin Panic After Russian Rebels Blow Up Train Causing Massive Derailment
Express, 11/7/2024

[Russia] Russian rebels carried out a devastating attack on a rail line, causing a derailment of twenty-two carriages. The incident happened on November 3 in Bashkortostan, on a segment of the track between Dema and Chernikovka. An explosive device was placed under the carriage of a goods train that was transporting coal. Following the explosion, twenty-two carriages were derailed, blocking the line for hours afterwards. Russian police have arrested a 31-year-old man from the Stavropol region in connection with the attack. Russian railway lines have frequently been targeted by partisans, since Putin's full-scale invasion of Ukraine in February 2022. Rail relay cabinets have been set on fire on numerous occasions, causing major disruptions to trains. The attacks on transport infrastructure are part of a wider strategy by the internal Russian resistance to downgrade Putin's war machine. https://www.express.co.uk/news/world/1972827/putin-train-derailment-bashkortostan-russian-rebels

Delivering A Hawaii Transit Megaproject
Railway Age, 11/11/2024

[Honolulu, Hawaii] The Skyline rail project is a $10 billion, 20-mile, 21-station rail megaproject in Hawaii, spearheaded by the Honolulu Area for Rapid Transportation (HART). This elevated rail system will connect East Kapolei in West Oahu to Honolulu's dense urban core, addressing the city's significant traffic congestion issues. With limited space to expand roads, the Skyline project offers a sustainable solution. Stantec is providing construction engineering and inspection services for this groundbreaking project, which will feature electric and driverless cars – a first in the United States. This project has extensive and long-lasting benefits. It aims to reduce Hawaii's carbon footprint and dependence on imported oil, alleviate road congestion, stimulate the economy by creating jobs, and provide a safe mode of transportation. https://issuu.com/railwayage/docs/railway_age_november_2024/50

Schneider National Launches Mexico, US Southeast Intermodal Service
Freight Waves, 11/11/2024

Schneider National announced Monday the launch of an intermodal service providing "truck-like daily transit between the Southeast and Mexico." The Green Bay, Wisconsin-based multimodal transportation and logistics provider said the service will provide continuous rail transportation between locations in Mexico and Texas with points in the U.S. Southeast. The new lane is an offshoot of a deal struck by CSX and Canadian Pacific Kansas City, creating a Class 1 rail connection between the two carriers in Alabama. The service will provide shippers in states like Florida and Georgia with a seamless cross-border option that doesn't require a container handoff at the border as customs clearance is executed in transit. A news release said in addition to reducing delays, freight is less exposed to theft because it isn't stopped at the border. https://www.freightwaves.com/news/schneider-national-launches-mexico-us-southeast-intermodal-service

Crash Responder Safety Week 2024
National Operations Center of Excellence, 11/7/2024

The Federal Highway Administration (FHWA) Traffic Incident Management (TIM) Program invites all emergency medical service (EMS), fire and rescue, law enforcement, public works, towing and recovery, transportation, and other traffic incident response professions to participate in the National Kickoff webinar for CRSW. This kickoff event is hosted by FHWA Office of Transportation Operations will honor responders, provide an overview of activities taking place across the country, and connect all responder stakeholders to kickoff this important week. Additionally, the FHWA TIM Program Team (Jim Austrich, Paul Jodoin, and Joe Tebo) will share information regarding: The coordinated approach and unique strategies in promoting CRSW, Technologies for saving responder and all road user lives, Efforts towards better understanding the responder struck-by problem, A refresh for the National TIM Responder training debuting this month. https://transportationops.org/event/national-kickoff-webinar-crash-responder-safety-week-2024

Tree Branch That Penetrated Windshield Killed NJ Transit Light Rail Operator: NTSB
Trains, 11/8/2024

[Washington D.C.] A tree branch that penetrated the cab windshield struck and killed the operator of a train on NJ Transit's light rail River Line on Oct. 14, the National Transportation Safety Board said in its preliminary investigation report. The incident occurred at about 6:02 a.m. when the southbound diesel-powered light rail vehicle struck a downed tree near Florence, N.J. Twenty-three of the 41 passengers on board were also injured. The train was going 64 mph (track speed is 65 mph) when it rounded a curve in the dark and the tree was illuminated by the train's headlights. The operator operated the track brakes

and emergency brakes, and the train slowed for 430 feet before striking the tree. It came to a stop after another 880 feet. https://www.trains.com/trn/news-reviews/news-wire/tree-branch-that-penetrated-windshield-killed-nj-transit-light-rail-operator-ntsb/

CYBERSECURITY

Verizon Business Activates More Than 740 New Fixed Wireless Access Lines On TriMet Systems
Mass Transit, 11/8/2024

Verizon Business has activated more than 740 new fixed wireless access (FWA) lines on TriMet systems. The agency uses mobile data to support many key technologies, including allowing riders to pay fares using their mobile wallet or contactless payment card and providing connectivity and information to transit operators. In collaboration with regional traffic agency partners, TriMet is using mobile data to pioneer cloud-based transit signal priority that improves traffic flow efficiency, speeding up buses without causing delays for drivers, cyclists or pedestrians while improving safety and reducing carbon emissions. TriMet plans to use its enhanced mobile data in the future to further improve system performance and security. https://www.masstransitmag.com/technology/press-release/55241454/verizon-business-verizon-business-activates-more-than-740-new-fixed-wireless-access-lines-on-trimet-systems

Fake Lockbit, Real Damage: Ransomware Samples Abuse Amazon S3 To Steal Data
Trend Micro, 10/16/2024

From infostealer development to data exfiltration, cloud service providers are increasingly being abused by threat actors for malicious schemes. While in this case the ransomware samples we examined contained hard coded AWS credentials, this is specific to this single threat actor and in general, ransomware developers leverage other online services as part of their tactics. In line with this, we examined ransomware samples written in Go language (aka Golang), targeting Windows and MacOS environments. Most of the samples contained hard-coded AWS credentials, and the stolen data were uploaded to an Amazon S3 bucket controlled by the threat actor. By the tail end of the attack, the device's wallpaper is changed into an image mentioning LockBit.
https://www.trendmicro.com/en_us/research/24/j/fake-lockbit-real-damage-ransomware-samples-abuse-aws-s3-to-stea.html

ANALYST COMMENTARY: This analysis reveals the exploitation of AWS infrastructure and Amazon S3 Transfer Acceleration (S3TA) for ransomware deployment, highlighting how cloud services are being misused for rapid data exfiltration. The ransomware, developed in Go for cross-platform compatibility, targets both Windows and macOS, leveraging hard-coded AWS credentials to create an attacker-controlled S3 bucket. S3TA, designed to enhance data transfer speeds globally, is weaponized here to facilitate swift upload of encrypted victim data to the cloud. AWS Account IDs from such misuse can act as Indicators of Compromise (IOCs) for monitoring malicious activities, emphasizing the need for

vigilant cloud resource tracking. The ransomware's encryption process follows an AES-CTR method, with file encryption based on the MD5 hash of concatenated file names and a random master key. This master key is encrypted with an RSA public key, leaving only the attacker capable of decrypting the affected data. To obfuscate attribution, the ransomware alters the victim's wallpaper with images associated with the notorious LockBit ransomware, misleading victims toward a known, feared threat. Notably, AWS responded by suspending compromised accounts, underscoring cloud providers' role in incident mitigation. This attack underscores the importance of monitoring cloud credentials and account activity. Proactive steps, such as flagging suspicious account IDs and implementing rigorous IAM controls, are critical to defending against these increasingly sophisticated cloud-enabled threats. Enhanced detection tools and intelligence-sharing initiatives within cloud environments also play a vital role in counteracting cloud-based malware exploitation.