Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

December 12, 2024

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Metro Transit Police Arrest Armed Fare Evader On Metrobus
WTOP News, 12/11/2024

[Washington, D.C.] The Metro Transit Police Department arrested a person it said had a loaded shotgun on a bus in D.C. Plainclothes Metro police officers stopped the person after boarding an X2 route Metrobus without paying Wednesday, just after 10:30 a.m. The officers said the person was refusing to comply before they found a loaded gun under the rider's coat. "The shotgun was determined to be stolen out of Prince George's County, Maryland," a Metro transit police spokesperson said. Officials identified the man as 30-year-old Gerald Evans, who already has an open felony warrant in Anne Arundel County for theft. Evans has been charged with possession of a prohibited weapon, carrying a dangerous weapon, unlawful possession of a firearm, possession of unregistered ammunition, fugitive from justice and fare evasion, officials told WTOP. Metro has stepped up enforcement efforts on bus fare evasion after Thanksgiving, with increased officer visibility and plainclothes officers along service routes.
https://wtop.com/crime/2024/12/metro-transit-police-arrest-armed-fare-evader-on-metrobus/

Thousands Evacuated From Subway Trains In Brooklyn After Power Loss, MTA Says
CBS, 12/12/2024

[Brooklyn, New York] Thousands of subway riders had to be evacuated from two trains in Brooklyn on Wednesday evening after a power loss, the MTA said. According to the MTA, power was lost between the Jay Street-MetroTech and Hoyt-Schermerhorn Streets stations in Downtown Brooklyn just before 5:30 p.m. Two F trains got stuck and had to be evacuated, the MTA said. About 3,500 total riders were on the two trains and the evacuations took nearly three hours, according to the MTA. "The FDNY does train for this specifically. Of course, passenger safety is the most important issue here, particularly when the power's out underground. It's not only dark down there, but of course, there's always the possibility of the energy coming back on with the third rail," said Glenn Gorbett, a fire rescue expert and associate professor at John Jay College. According to the New York City Fire Department, at least one person had to be taken to a local hospital. The MTA said three other trains were "briefly" stuck, but were eventually able to move backward to return to the station they had left.
https://www.cbsnews.com/newyork/news/manhattan-brooklyn-subway-third-rail-power-loss/

Russia Detains German Citizen On Suspicion Of Railway Sabotage
Reuters, 12/10/2024

[Russia] Russia's Federal Security Service (FSB) said on Tuesday it had detained a dual Russian-German citizen on suspicion of preparing an act of sabotage on a railroad in Nizhny Novgorod, a city some 280 miles (450 km) east of Moscow. The FSB did not name the man, but said he was born in 2003. It said authorities had found an improvised explosive device (IED) at his home, as well as evidence he had corresponded with a member of Ukrainian special services. Ukraine's military intelligence and state security service did not immediately reply to requests for comment. Russian officials have linked pro-Ukrainian sabotage groups with numerous attacks on railways aimed at disrupting supplies to the battle front in Ukraine since the war began in February 2022. Ukraine's domestic spy agency has also been accused of detonating explosives on railway lines inside Russia.
https://www.reuters.com/world/europe/russia-detains-german-citizen-suspicion-railway-sabotage-2024-12-10/

TERRORISM & EXTREMISM

New Zealand Spy Agency Says Terror Attack Remains 'Realistic Possibility
Reuters, 12/9/2024

A terror attack in New Zealand remains a "realistic possibility" over the next year as evolving global and domestic security trends continue to drive extremist sentiment, the country's intelligence service said on Tuesday. Following its annual review of the national terror threat levels, the New Zealand Security Intelligence Service (NZSIS) said people were getting exposed to an increasingly diverse range of violent extremist narratives through online networks, raising the risk of radicalization and potential violence. "An attack is a realistic possibility amid what is a deteriorating global security environment," NZSIS Director-General of Security Andrew Hampton said in a statement. There is no change to the national threat level, which has remained at 'low' since November 2022, Hampton said. The NZSIS said it was severely concerned about the impact of the online networks on young people, "who are being exposed to and influenced by violent extremism in ways we haven't seen before."
https://www.reuters.com/world/asia-pacific/new-zealand-spy-agency-says-terror-attack-remains-realistic-possibility-2024-12-09/

SECURITY & SAFETY AWARENESS

Metro Transit Expanding Use Of Unarmed Presence To Address Crime, Fare Evasion
KSTP, 12/11/2024

[New York] For the second time in a year, Metro Transit is doubling down on a plan to increase its uniformed presence on light rail trains and buses across the Twin Cities. The agency announced

Wednesday that its unarmed agents and community service officers conducted more than 450,000 fare inspections this year — twice the number of checks performed in 2023. The increase coincides with a state law that decriminalized fare evasion and replaced $180 misdemeanor fines with $35 citations. At a news conference in St. Paul, Metro Transit shared that its agents have handed out more than 2,000 of those citations so far. Jeremiah Collins, a former train operator, is now among nearly 60 agents interacting with riders as part of the Transit Rider Investment Program. … The overall effort has contributed to what Metro Transit says is a 8.4% drop in reported crime on transit in the first three quarters of 2024, compared to the same time period a year ago. https://kstp.com/kstp-news/top-news/metro-transit-expanding-use-of-unarmed-presence-to-address-crime-fare-evasion/

Northern California Man Arrested for Allegedly Flying Drone Over and Photographing Vandenberg Space Force Base
Department of Justice, 12/11/2024

[California] A Northern California man has been arrested on a federal criminal complaint for allegedly flying a drone over and taking photographs of Vandenberg Space Force Base, the Justice Department announced today. Yinpiao Zhou, 39, of Brentwood, is charged with failure to register an aircraft not providing transportation and violation of national defense airspace. Zhou was arrested Monday at San Francisco International Airport prior to boarding a China-bound flight and made his initial appearance Tuesday in United States District Court in San Francisco. … According to an affidavit filed on December 8 with the complaint, on November 30, 2024, drone detection systems at Vandenberg Space Force Base in Santa Barbara County detected a drone flying over the base. The drone systems detected that the drone flew for nearly one hour, traveled to an altitude of almost one mile above ground level, and originated from Ocean Park, a public area next to the base. Base security personnel went to the park, spoke to Zhou and another person accompanying him, and learned that Zhou had a drone concealed in his jacket – the same one that flew over the base. https://www.justice.gov/usao-cdca/pr/brentwood-man-arrested-allegedly-flying-drone-over-and-photographing-vandenberg-space

Weeks Of Unexplained Drone Sightings Raise Fears And Frustrations In New Jersey
CNN, 12/12/2024

[New Jersey] Weeks of mysterious drone sightings across New Jersey are prompting heightened security concerns – and mounting frustrations – from residents, military personnel and federal, state and local officials. While the state's governor says there's no threat to public safety, other state officials and local mayors are alarmed. Law enforcement has not identified the origin or landing sites of the drones, Mayor Michael Melham of Belleville Township said in a Facebook video update on Wednesday. … "One of the takeaways today was that these drones statewide are hovering and appearing to be surveilling New Jersey's critical infrastructure," Melham said. … During a US Homeland Security Committee hearing Tuesday, Robert Wheeler, assistant director of the FBI's Critical Incident Response Group, called the

phenomenon “concerning” but said “there is nothing that is known” that would lead him to identify a public safety risk. https://www.cnn.com/2024/12/11/us/new-jersey-drone-sightings-investigation/index.html

Arkansas Lawmakers Push To Fight Human Trafficking At Interstate Truck Stops
ABC 7, 12/10/2024

Monday, Arkansas lawmakers filed a bill that would provide incentives to truck drivers who provide information to either take down human trafficking perpetrators or rescue victims. State Rep. Steve Unger is partnering with Arkansas lawmakers to help fight human trafficking in Arkansas. A hot spot for the crime is truck stops along interstates. In the proposed bill, any Arkansas resident truck driver who reports a tip on human trafficking can possibly get this incentive. "Could be sex trafficking, could be any sort of forced labor that leads to either a rescue or an arrest," said Unger (R) AR-19. "We will give you a lifetime hunting and fishing license.” Unger said during his time volunteering with the National Child Protection Task Force, it was clear human trafficking is prevalent everywhere, but especially at truck stops. https://katv.com/news/local/lawmakers-push-to-fight-human-trafficking-at-interstate-truck-stops-with-driver-incentives-representative-steve-unger-senator-joshua-bryant-national-child-protection-task-force-operation-arkansas-state-police-matthew-foster-missouri-incentive-game-fish

ANALYST COMMENTARY: On 9 December 2024, Arkansas Representative Steve Unger filed a bill that would grant lifetime fishing and hunting licenses to Arkansan commercial truck drivers “for providing information that leads to the rescue of a trafficking victim or the arrest of a trafficker.” The trafficking does not need to have a nexus to Arkansas for the driver to be eligible; however, the driver does need to be an Arkansas resident. According to the National Human Trafficking Hotline, 9,619 human trafficking cases with 16,999 victims were identified in the U.S. in 2023. Of those cases, 3,233 venues for sex trafficking were also discovered, including 36 truck stops. While creating the bill, Representative Unger worked alongside Truckers Against Trafficking (TAT), which is a nonprofit that trains truckers to recognize and report instances of human trafficking. Resources specific to transportation sector personnel that can be used to identify and report human trafficking can be found at the TAT website at: https://tatnonprofit.org/.

More Alleged Participants Indicted in Staged Truck Accidents
Transport Topics, 12/11/2024

An indictment in a New Orleans-area scheme to stage crashes with tractor-trailers names two law firms, two individual attorneys and multiple participants in a sweeping conspiracy that included fraud, obstruction of justice, witness tampering and murder. The 10-count indictment, unsealed Dec. 9 by the U.S. attorney for the Eastern District of Louisiana, was the latest development in a yearslong federal investigation into a series of staged accidents with heavy trucks dating back as far as 2011. The new round of indictments brings to 63 the total number of individuals who have either been charged or

pleaded guilty to charges in connection with the ongoing FBI investigation, known as "Operation Sideswipe." https://www.ttnews.com/articles/indicted-staged-truck-accidents

ANALYST COMMENTARY: On 9 December 2024, the U.S. Department of Justice (DOJ) unsealed a 10-count indictment as the latest development in Operation Sideswipe, which is a substantial Federal Bureau of Investigation (FBI) investigation into accident fraud schemes in Louisiana dating back to at least 2011. The accident fraud schemes led to millions in fraudulent insurance claims, with one specific scheme in 2015 netting the fraudsters approximately $4.7 million. In the schemes, the fraudsters, some with the informal titles of "slammers" or "spotters," intentionally caused collisions with commercial trucks in order to litigate. The spotters would locate commercial trucks and relay information to the slammers, who would stage the accidents. In some cases, the slammers would switch positions inside the vehicles they intended to be involved in the "accidents" to ensure specific people were listed as driving for the subsequent paperwork. During the claims process, the fraudsters would fake injuries, with some going so far as to pay medical providers to perform unnecessary neck and back surgeries on them to increase their likelihood of large settlements. With the latest indictment, which charges multiple law firms, a total of 63 people have either been charged with or pled guilty to crimes associated with Operation Sideswipe, including fraud, obstruction of justice, witness tampering, and murder. It is unclear exactly how many people have participated in the scheme since 2011, though in 2021, a lawyer pled guilty to having arranged at least 31 fraudulent collisions with at least 77 plaintiffs involved.

Train Crashes Into Propane Truck Near US 290 In Northwest Harris County; 2 Injured
Click2Houston, 12/11/2024

[Houston, Texas] Two people were rushed to a hospital Wednesday following a crash involving a train and a propane truck in northwest Harris County, according to Harris County Sheriff Ed Gonzalez. The crash was reported at the entrance of Hot Wells at 24800 block of US 290. The eastbound feeder road was closed from Skinner to Barker Cypress roads. By the numbers: Texas leads nation in freight train accidents, Harris County ranks highest in state. The two occupants of the truck sustained non-life-threatening injuries and are in good condition at a hospital, according to deputies. Officials said there are no environmental hazards. The cause of the crash is being investigated. This is the second train crash this week. On Monday a Milby High School student was killed trying to cross a train track in southeast Houston. https://www.click2houston.com/news/local/2024/12/11/train-crashes-into-propane-truck-near-us-290-in-northwest-harris-county-1-person-injured/

CYBERSECURITY

Detailing the Attack Surfaces of the WolfBox E40 EV Charger
Zero Day Initiative, 12/3/2024

The WolfBox E40 is a Level 2 electric vehicle charge station designed for residential home use. Its hardware has a minimal user interface, providing a Bluetooth Low Energy (BLE) interface for configuration and an NFC reader for user authentication. Typical for this class of devices, the appliance employs a mobile application for the owner's installation and regular operation of the equipment. … The manufacturer distributes one application to configure and maintain the device. The application, named WolfBox EV, is available for both Android and iOS users. Interestingly, the application apparently allows pairing and managing with more than the expected EV charger devices; when attempting to add a new device, a list is presented that includes several other ostensibly known and accepted device types, such as lamps, switches, doorbells, mosquito repellent heaters, irrigators and battery packs, to name a few.
https://www.zerodayinitiative.com/blog/2024/12/2/detailing-the-attack-surfaces-of-the-wolfbox-e40-ev-charger

ANALYST COMMENTARY: TrendMicro researchers released a report, last week, detailing the attack surface of WolfBox E40 electric vehicle (EV) charge station. The EV charge station is designed for residential use and can be easily purchased on Amazon. The report did not discover particular vulnerabilities with the devices hardware, but did detail possible attack vectors through the chargers mobile application. Although there is no known active exploitation of vulnerabilities within thi EV mobile application, the attack surface detailing is meant to show possible vulnerabilities of at-home EV chargers. For instance, the hardware of the WolfBox E40 EV Charger "has a minimal user interface, providing a Bluetooth Low Energy (BLE) interface for configuration and an NFC reader for user authentication." BLE is a wireless communication technology designed for low power consumption, ideal for transferring data between the charger and the mobile application. Its hardware is also lightweight and affordable making it compatible with residential usage. However, BLE components are susceptible to unauthorized access. In past attacks, cyber criminals have been observed manipulating or intercepting data between the charger and its connected app, potentially controlling the device remotely. Additionally, weaknesses in the mobile app's encryption and its communication with the charger could be exploited by attackers, enabling them to disrupt charging or expose user information.

Mitel MiCollab Zero-Day And PoC Exploit Unveiled
Help Net Security, 12/4/2024

A zero-day vulnerability in the Mitel MiCollab enterprise collaboration suite can be exploited to read files containing sensitive data, watchTowr researcher Sonny Macdonald has disclosed, and followed up by releasing a proof-of-concept (PoC) exploit that chains together this zero-day file read vulnerability with CVE-2024-41713, which allows attackers to bypass authentication. In a blog post published on Thursday, Macdonald tells of watchTowr's quest to reproduce CVE-2024-35286, a MiCollab SQL injection

vulnerability fixed earlier this year, and their discovery of: CVE-2024-41713, an additional authentication bypass vulnerability (which Mitel subsequently patched in October), and an arbitrary file read zero-day still without a CVE number (a patch for which Mitel said would release in the first week od December 2024). The zero-day can only be exploited by authenticated attackers, hence it getting chained with CVE-2024-41713 in the PoC. But if that requirement is achieved, attackers can navigate to and access sensitive files such as /etc/passwd. https://www.helpnetsecurity.com/2024/12/05/mitel-micollab-zero-day-and-poc-exploit-unveiled/

ANALYST COMMENTARY: The discovery of a zero-day vulnerability in Mitel's MiCollab, combined with CVE-2024-41713, poses a significant risk to enterprises using the platform. The zero-day allows authenticated attackers to read arbitrary files, which could include sensitive system and user data. By chaining it with the CVE-2024-41713 authentication bypass, even unauthenticated attackers can exploit this flaw. Although Mitel patched CVE-2024-41713 in October, the zero-day remains unaddressed, leaving systems vulnerable until Mitel's promised fix in December 2024 is deployed. The critical takeaway is that this exploit can provide attackers with access to sensitive files such as `/etc/passwd`, potentially leading to broader system compromises. While the immediate mitigation involves upgrading MiCollab to version 9.8 SP2 (or applying the appropriate patches), organizations must also enforce strict network segmentation, restrict access to trusted IP ranges, and monitor for unauthorized access attempts. The fact that over 16,000 MiCollab instances are exposed online amplifies the urgency for action. Given MiCollab's role as a communication hub, compromising its functionality could lead to severe consequences, including unauthorized call routing, data theft via file sharing, and espionage through compromised desktop sharing. Organizations should prioritize patch management and implement layered defenses to mitigate the risk of exploitation until Mitel fully addresses the issue.