Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

December 19, 2024

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

King County Metro Bus Driver Fatally Stabbed In Seattle's U District
The Seattle Times, 12/18/2024

[Seattle, Washington] A King County Metro bus driver was fatally stabbed in Seattle's University District early Wednesday, marking the first killing of a Metro driver on the job in 26 years and the latest example of violence that is shaking confidence in the regional transit system. Shawn Yim, 59, was stabbed in the chest just before 3 a.m. on a bus at 15th Avenue Northeast and Northeast 41st Street, during an altercation with a passenger, according to Seattle police and Metro. Officers responding to reports of the stabbing found Yim on the ground. They provided aid but could not save him. No arrests have been made. https://www.seattletimes.com/seattle-news/law-justice/king-county-metro-bus-driver-fatally-stabbed-in-seattles-u-district/

Texas Train Derails After Hitting Tractor-Trailer, Barreling Into City Building: Video
FOX News, 12/19/2024

[Pecos, Texas] A train derailment in Pecos, Texas, left one person dead and four others injured on Wednesday. Pecos City Manager Charles Lino said the incident began when a train struck a tractor-trailer on the railroad tracks on Wednesday evening. The collision caused the train to derail, ultimately hitting the Chamber of Commerce building. It was not noted if the victims were inside the building or not. Three of the cars were carrying potentially hazardous materials at the time of the accident, but they were contained. Three of the victims were treated at Reeves Regional Health, while the fourth had more serious injuries and was transported to an Odessa hospital for treatment.
https://www.foxnews.com/us/texas-train-derails-after-hitting-tractor-trailer-barrels-city-building-video

Teenager Charged For Allegedly Threatening To Shoot, Stab Passenger On MTA Bus
WSMV 4, 12/18/2024

[Nashville, Tennessee] A young woman was arrested after an MTA bus driver witnessed her threaten to shoot another passenger on the bus on Tuesday. Officers with the Metro Nashville Police Department were flagged down by a bus driver at the MTA station who reported witnessing a woman threaten to shoot another woman on her bus. The arrest affidavit states the officers located 18-year-old Brookelin

NOT FOR PUBLIC DISSEMINATION

WARNING: THIS DOCUMENT IS UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). IT CONTAINS INFORMATION THAT MAY BE EXEMPT FROM PUBLIC RELEASE UNDER THE FREEDOM OF INFORMATION ACT (5 U.S.C. 552). IT IS TO BE CONTROLLED, STORED, HANDLED, TRANSMITTED, DISTRIBUTED, AND DISPOSED OF IN ACCORDANCE WITH DHS POLICY RELATING TO FOUO INFORMATION AND IS NOT TO BE RELEASED TO THE PUBLIC, THE MEDIA, OR OTHER PERSONNEL WHO DO NOT HAVE A VALID "NEED-TO-KNOW" WITHOUT PRIOR APPROVAL OF AN AUTHORIZED TSA OFFICIAL. NO PORTION OF THIS REPORT SHOULD BE FURNISHED TO THE MEDIA, EITHER IN WRITTEN OR VERBAL FORM. PLEASE REFER TO EACH DOCUMENT'S U//FOUO WARNING FOR FURTHER HANDLING INSTRUCTIONS THAT MAY APPLY.

Jackson, who the driver identified as the suspect in the incident. According to the affidavit, the female victim told officers that Jackson had stolen her child's cell phone and she was attempting to get it back when Jackson reached into her backpack and threatened to shoot and stab the woman. The officers searched Jackson's bag and found a large silver and black blade, along with the cell phone she allegedly stole from the child. Jackson was arrested and given a medical evaluation before she was booked on an aggravated assault with a deadly weapon charge. https://www.wsmv.com/2024/12/18/teenager-charged-allegedly-threatening-shoot-stab-passenger-mta-bus/

Eight Injured During Crash Involving MTA Bus In Brooklyn: Officials
PIX 11, 12/17/2024

[Brooklyn, New York] Multiple people were injured during a motor vehicle accident involving a MTA bus in Brooklyn Tuesday afternoon, officials say. The incident was reported near Flushing Avenue and Nostrand Avenue at around 2:27 p.m. Four individuals were treated on scene and four others were taken to local hospitals with minor injuries. https://pix11.com/news/local-news/brooklyn/eight-injured-during-crash-involving-mta-bus-in-brooklyn-officials/

TERRORISM & EXTREMISM

FBI Agents Search Home Of Los Angeles Deputy Mayor Who Allegedly Made Bomb Threat: Mayor's Office
ABC News, 12/18/2024

[Los Angeles, California] FBI agents searched the home of a Los Angeles deputy mayor this week over a bomb threat he allegedly made against Los Angeles City Hall earlier this year, the mayor's office said. The FBI was at the home of Brian Williams, the deputy mayor for public safety, on Tuesday "as part of an investigation into a bomb threat he allegedly made against City Hall earlier this year," a spokesperson for the mayor's office said in a statement on Wednesday. Williams was "immediately" placed on administrative leave, according to spokesperson Zach Seidl. "The Mayor takes this matter very seriously," Seidl said in a statement. "When the threat was reported, LAPD investigated and determined there was no immediate danger." https://abcnews.go.com/US/los-angeles-deputy-mayor-brian-williams-fbi-search-bomb-threat/story

ANALYST COMMENTARY: According to the Los Angeles Police Department (LAPD), the Los Angeles Deputy Mayor for Public Safety, Brian Williams, is believed to be responsible for a bomb threat that was called into the Los Angeles City Hall earlier this year. Deputy Mayor Williams oversees the police department and previously served for seven years as the executive director of the Los Angeles County Civilian Oversight Commission which "Works to facilitate public transparency and accountability with respect to the Sheriff's Department," according to their website. False bomb threats and false reports to the police of an emergency are often used to disrupt operations at government facilities such as

courthouses, state capitals, and federal buildings. The effort to resolve the threat is enormously labor-intensive and expensive which adds to the damage caused by false reporting. The trend of making false reports has gained in popularity over the last few years and is now known as "swatting," which is described as "the false reporting of an emergency to public safety by a person for the intent of getting a ('SWAT team') response to a location where no emergency exists." When doing this, the callers often make other false statements to lend credibility to their report, such as saying they are directly involved in the incident or, that they are currently witnessing an incident. To evoke a larger response, fraudulent callers have often claimed the incident involves a hostage or active shooter to attempt to solicit the largest law enforcement response possible as quickly as possible. In many cases, law enforcement responds in significant numbers and ends up confronting unsuspecting victims before realizing that the incident was fabricated. While many of these swatting incidents and bomb threats do not involve an explosive, law enforcement cannot risk assuming the threat is not credible. According to an FBI statement in 2020, approximately one percent of bomb threats are deemed credible, meaning an explosive device is found or detonated at the reported location. The Bureau of Alcohol, Tobacco, Firearms and Explosives (BATFE) operates the U.S. Bomb Data Center and each year they produce an explosives incident report. According to the BATFE, in 2023, there were 3,203 reported bomb-threat incidents in the U.S., which was a 26 percent increase from 2022. An analysis of those threats revealed that the top three targets of bomb threats were: education facilities (1,123), office and business locations (503), and public assembly locations (353). Law enforcement continues to investigate the incident involving Williams, who has been relieved of his duties pending the outcome.

Neo-Nazi With Home 'Armoury' Jailed For 10 Years
BBC, 12/19/2024

An extremist who amassed an "armoury" at his home and discussed launching an attack on a local LGBT group has been jailed for 10 years. A court heard Alan Edward, 55, from Falkirk who had nearly 28,000 followers on social media, believed in white supremacy and openly expressed racist, homophobic and anti-Semitic views. He denied all the offences, but a jury found him guilty of charges under the Terrorism Act, racism, anti-semitism, holocaust denial and breach of the peace. Edward will also be supervised for five years following his release, and monitored for 30 years under the terms of the Terrorism Act.
https://www.bbc.com/news/articles/c7864zqx84no

SECURITY & SAFETY AWARENESS

Study: Traffic Congestion Added $108.8B In Costs To Trucking Industry In 2022
Transportation Today, 12/19/2024

According to a new study by the American Transportation Research Institute (ATRI), traffic congestion added $108.8 billion in costs to the trucking industry in 2022. The Cost of Congestion study said the

highway performance measurement is a new record for costs due to traffic congestion across the country. Using a variety of data sources, including its truck GPS database, ATRI calculated the impact of trucking delays on major roadways. The total hours of congestion decreased slightly the study found, but the cost of operating a truck increased at a much greater rate, leading to the overall cost of congestion increasing by 15 percent. https://transportationtodaynews.com/news/34570-study-traffic-congestion-added-108-8b-in-costs-to-trucking-industry-in-2022/

ANALYST COMMENTARY: The American Transportation Research Institute (ATRI), found that in 2022, commercial vehicles stuck sitting in traffic due to urban congestion was "equivalent to greater than 430,000 commercial drivers sitting idle for an entire year." The cost of this lost time to owner-operators and shipping companies is staggering and affects the entire supply chain. The Texas A&M Transportation Institute studied this issue in their state and on 27 June 2024, released the 2025 Unified Transportation Program (UTP) Development plan to mitigate congestion issues. Texas A&M found that the network of seriously congested roadways spans 9,922 miles, causes annual delays of 408,197,108 hours, wastes 105,961,544 gallons of gas and costs the state and local governments an additional $10,820,999,295. There is a similar negative impact on surface transportation, as trucks are delayed by 27,112,540 hours, waste 23,375,200 gallons of fuel, and incur $1,687,678,633 in additional costs each year. In September 2024, Streetlight released a case study called "The State of Vehicle Miles Traveled (VMT) and Congestion – Measuring Five Years of VMT." According to Streetlight's report, "NYC leads the country in both worsening vehicle miles traveled and traffic congestion among large downtowns. Metrowide, New York City saw congestion worsen faster than the next 47 most populated cities." This occurred even though NYC has a robust public transportation system. The Streetlight report can be obtained from: https://learn.streetlightdata.com/vmt-congestion-report-2024.

Transportation Safety Board Of Canada Determines Broken Rail Was Cause Of October 2023 CN Derailment
RT&S, 12/17/2024

[Canada] The Transportation Safety Board of Canada has determined that the derailment of a CN freight train traveling on the Sussex Subdivision in October 2023 was caused by a broken rail. Here are some excerpts from the investigation report: "On 30 October 2023, Canadian National Railway Company freight train L59411-30 was traveling westward on the Sussex Subdivision at approximately 38 mph when a train-initiated emergency brake application occurred at about 1310 Atlantic Daylight Time. The conductor inspected the train and discovered that the last 4 cars had derailed around Mile 32.7, near Dunsinane, New Brunswick. There were no injuries or fires. Approximately 2000 liters of methanol leaked from the 46th car. https://www.rtands.com/track-construction/track-structure/transportation-safety-board-of-canada-determines-broken-rail-was-cause-of-october-2023-cn-derailment/

How Cargo Thieves Capitalize On Holiday Shipping Rush
Supply Chain Brain, 12/18/2024

The approaching Christmas holiday brings an increased risk of cargo theft for shippers, with criminal groups often planning their activity around a period when they know that resources are strained and security is minimal. According to data from fleet management software company Pedigree Technologies, cargo thefts increased by 68% in the fourth quarter of 2023 compared to the previous year. Pedigree notes that more products get moved on tighter deadlines ahead of Christmas, leading to lapses in security as companies bring on less experienced seasonal workers to manage an influx of high-value items like electronics, luxury clothing, and alcohol. Supply chain security company Overhaul also points out that over long holiday weekends, distribution centers and warehouses are known to operate with reduced staffing, offering attractive targets to would-be thieves, and a larger window of time before thefts can be detected. https://www.supplychainbrain.com/articles/40859-how-cargo-thieves-capitalize-on-holiday-shipping-rush

Safeguarding Freight And Logistic Business Amidst Rising Cargo Crime
Gallagher, 12/18/2024

Cargo theft is a rising concern in the UK, particularly in the freight and logistics sector. According to reports, there was a 7% increase in cargo crime incidents between 2022 and 2023, resulting in an estimated £68 million loss. The spike in cargo crime has put intense pressure on the UK's logistics sector, necessitating identifying and mitigating such threats as soon as possible. Reasons behind rising cargo thefts: The Road Haulage Association (RHA) reports that the UK witnessed over 5,000 cases of cargo crime in 20232. Various factors are contributing to the increase in cargo theft: Easy targets with higher rewards, Lack of secure parking facilities, Organized and sophisticated networks, Rising demand for essentials, and Global supply chain disruptions. https://www.ajg.com/uk/news-and-insights/safesguarding-freight-and-logistics-business-amidst-rising-cargo-crime/

ANALYST COMMENTARY: Security Boulevard reports that as of December 2024, "approximately 183,000 customers worldwide were affected by supply chain attacks" in 2024. The computer software industry experienced one supply chain attack approximately every 48 hours and cybersecurity threats increased 1,300 percent between 2020 and 2023. Most of these attacks were perpetrated by cyber threat actors and hackers who exploited third party vendors and software to evade detection by and gain access to a larger organization they intended to victimize. In the surface transportation and freight industries, supply chain attacks are increasing and getting harder to detect due to the ability to commit fraud and redirect loads remotely. Cloudflare recently reported a 400% rise in double-brokering complaints since 2022. Loss of shipments has a substantial up front monetary impact but can also impact operations and damage a company's reputation. For this reason, a loss of shipments may not always be reported and is sometimes handled internally. To increase awareness, industry stakeholders designated 15 October 2024 as the inaugural Freight Fraud Awareness Day to educate

policymakers and the logistics community and promote efforts to mitigate cargo-related crimes. Security Boulevard advises that best practices should involve ensuring that third-party suppliers are also following security guidelines to minimize the potential for supply chain disruption due to theft. There can be regulatory and legal consequences for failing to be proactive and making a diligent effort to protect an organization's infrastructure.

EPA Grants California's Nox Regulation Waiver
Fleet Owner, 12/18/2024

[California] The U.S. EPA granted a waiver for the California Air Resources Board to implement its Omnibus NOx regulation for heavy-duty vehicles. The move comes with just more than a month left in the Biden Administration's term. The waiver grants California federal permission to implement its latest NOx regulation for heavy-duty vehicles. The waiver is a significant development for regulating heavy-duty vehicle and engine manufacturers. It sets record-low NOx and particulate matter emissions standards for medium- and heavy-duty engines and vehicles. Under the Clean Air Act, California is the only U.S. state that can set its own emissions standards that exceed federal standards. California's emissions regulator, CARB, must receive a waiver for each regulation that exceeds federal standards. The regulation began with model year 2024 equipment, but CARB could not enforce the rule until EPA granted a waiver. https://www.fleetowner.com/emissions-efficiency/article/55250674/epa-grants-california-waiver-for-truck-nox-standards

CYBERSECURITY

Hackers Weaponize Visual Studio Code Remote Tunnels For Cyber Espionage
The Hacker News, 12/10/2024

A suspected China-nexus cyber-espionage group has been attributed to an attack targeting large business-to-business IT service providers in Southern Europe as part of a campaign codenamed Operation Digital Eye. The intrusions took place from late June to mid-July 2024, cybersecurity companies SentinelOne, SentinelLabs, and Tinexta Cyber said in a joint report shared with The Hacker News, adding the activities were detected and neutralized before they could progress to the data exfiltration phase. "The intrusions could have enabled the adversaries to establish strategic footholds and compromise downstream entities," security researchers Aleksandar Milenkoski and Luigi Martire said. "The threat actors abused Visual Studio Code and Microsoft Azure infrastructure for C2 [command-and-control] purposes, attempting to evade detection by making malicious activities appear legitimate." https://thehackernews.com/2024/12/hackers-weaponize-visual-studio-code.html

ANALYST COMMENTARY: Operation Digital Eye reflects an increasingly sophisticated trend among state-aligned threat actors: the exploitation of legitimate tools and infrastructure to blend into normal traffic and evade detection. The abuse of Visual Studio Code Remote Tunnels and GitHub for

command-and-control exemplifies this approach with cyber threat actors leveraging tools that are already trusted in IT environments. This strategy makes detection and mitigation difficult for defenders because blocking such tools outright may disrupt legitimate business operations. The attackers' reliance on SQLmap for initial access and a modified version of Mimikatz (mimCN) for pass-the-hash attacks further indicates the refinement and modularity of the tools used in China-linked operations. The use of a "digital quartermaster" or shared vendor for tool development adds a layer of complexity, enabling operational consistency across campaigns like Soft Cell and Tainted Love. This structured approach points to a well-resourced ecosystem that fosters both technical innovation and collaboration. For defenders, these findings emphasize the importance of proactive threat-hunting and zero-trust principles. Monitoring for unusual patterns in tools like Visual Studio Code or unexpected SSH activity can offer critical detection opportunities. Additionally, organizations should strengthen SQL injection defenses by prioritizing web application firewalls (WAFs) and rigorous input validation. Advanced endpoint detection, combined with behavior-based anomaly detection, is essential to catch these tactics early before lateral movement or data exfiltration occurs. Enhanced visibility into cloud environments, where these attackers often operate, is becoming non-negotiable for a robust defense.

***** FAIR USE NOTICE*****

This message contains copyrighted material whose use has not been specifically authorized by the copyright owner. The ST ISAC is providing this report to ISAC members who have expressed a prior interest in receiving information to advance their understanding of threat activities in the interest of protecting the national infrastructure of the United States. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner. For questions regarding this document, please contact the ST ISAC: 866.784.7221 or email st-isac@surfacetransportationisac.org