Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

December 11, 2024

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Officers Shoot Man With Knife At Rosslyn Metro Station, Arlington Police Say
DC News Now, 12/10/2024

[Arlington, Virginia] A man was hospitalized after police shot him at the Rosslyn Metro Station on Tuesday afternoon. The Arlington County Police Department (ACPD) said the shooting happened at the Rosslyn Metro Station. An officer reportedly shot a suspect, according to a post that ACPD made on X shortly before 5 p.m. Police were dispatched to the area at about 3:45 p.m. after receiving a report about a suspicious person in a Safeway. ACPD said a man engaged employees in conversation, during which he took out a knife from his pocket and left. Officers found the suspect on the top floor of the Rosslyn Metro Station. During their encounter, a struggle reportedly ensued and one officer shot the man. The suspect was taken to a hospital with serious injuries. The two officers involved were also taken to the hospital – one with non-life-threatening injuries, and one for evaluation. There is no ongoing threat to the community, but people should expect an increased police presence in the area, ACPD noted. https://www.dcnewsnow.com/news/local-news/virginia/arlington-county/officers-shoot-suspect-at-rosslyn-metro-station-arlington-police-say/

2 Found Hurt On MAX Platform After Stabbing Call In NE Portland
FOX 12, 12/7/2024

[Portland, Oregon] Two people were found hurt at a northeast Portland TriMet Transit Center after a stabbing on Friday night, according to police. Just before midnight, officers with PPB responded to a stabbing call at the Gateway Transit Center on Northeast 99th Avenue. Police said there were no transit officers available at the time. Officers said they found two people with injuries on the MAX train platform, and any suspects had left the area before they arrived. Police also said the two victims did not cooperate with EMS. Eventually, one of the victims was taken by ambulance to the hospital, and the other eventually showed up to the hospital on their own. PPB said they are not sure if the assault happened on the platform or on a train, but said the victims would likely recover.
https://www.kptv.com/2024/12/08/2-found-hurt-max-platform-after-stabbing-call-ne-portland/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TERRORISM & EXTREMISM

US Says It Will Support New Syrian Leaders Who Protect Women And Renounce Terrorism
Associated Press, 12/10/2024

[Syria] The Biden administration said Tuesday it will recognize and support a new Syrian government that renounces terrorism, destroys chemical weapons stocks and protects the rights of minorities and women. Secretary of State Antony Blinken said in a statement that the U.S. would work with groups in Syria and regional partners to ensure that the transition from President Bashar Assad's deposed government runs smoothly. He was not specific about which groups the U.S. would work with, but the State Department has not ruled out talks with the main Syrian rebel group despite its designation as a terrorist organization. The qualified pledge of support for a post-Assad Syria comes as the Biden administration targets Islamic State fighters to try to prevent the group from reemerging as an international threat and maintains support for Israel as its forces conduct their own operations inside Syria. https://apnews.com/article/syria-united-states-assad-b02790878868ddb3d2f5bc887b66fd5e

SECURITY & SAFETY AWARENESS

Executive 'Hit Lists' And Wanted Posters: NYPD Warns About Threats To Executives
ABC, 12/10/2024

[New York] A New York Police Department bulletin issued Tuesday emphasized the heightened risk environment for health care executives following last week's brazen killing of United Healthcare CEO Brian Thompson. Viral posts online have listed the names and salaries of several health insurance executives, multiple "Wanted" signs featuring corporate executives have been posted throughout Manhattan and users on social media continue to celebrate Thompson's death, according to the bulletin. The warning signs come as a sea of social media posts indicate that shooting suspect Luigi Mangione might be viewed as a "martyr" who could inspire extremists to action.
https://abcnews.go.com/US/executive-hit-lists-wanted-posters-nypd-warns-threats/story

ANALYST COMMENTARY: On 10 December 2024, following the murder of the UnitedHealthcare CEO last week, the New York City Police Department (NYPD) posted a bulletin advising companies to increase precautions and safety measures for their public facing executives. In the wake of last week's murder, a surge in calls for violence against corporate executives – especially those in healthcare fields – has increased dramatically, and has been accompanied by "growing negative sentiment around conglomerates, the wealthy, and executive staff at private and public organizations." The bulletin goes on to claim that "Both prior to and after the suspected perpetrator's identification and arrest, some online users across social media platforms reacted positively to the killing, encouraged future targeting of similar executives, and shared conspiracy theories regarding the shooting." The NYPD bulletin warns

that this growing sentiment has the "capability to inspire a variety of extremists and grievance-driven malicious actors to violence." Since the murder occurred, multiple organizations, including healthcare insurance companies, have scrubbed their corporate websites and deleted images of their executives, with some organizations removing executive profile pages entirely.

Recent Road Rage Deaths Heighten Las Vegas Traffic Safety Concerns
FOX 5, 12/9/2024

[Las Vegas, Nevada] Southern Nevada roads can be a dangerous place to be, and recent road rage incidents are heightening concerns for drivers. Most recently, a man was killed in a road rage shooting in Henderson Friday night. "My first reaction is that people's anger is getting completely out of control in Las Vegas," said Erin Breen, director of the Road Equity Alliance Project at UNLV's Transportation Research Center. Another fatal shooting at a shopping center in Henderson Friday added to a list of road rage-related deaths on Southern Nevada roads. Just two weeks ago, an Uber driver was killed in a road rage shooting on the Strip. "We've had so many of these in the last month, you know, a couple that have been fatal, high profile, you know that shootout in the middle of Las Vegas Boulevard," said Breen. … "If you have an altercation with someone, stay in your car," Breen said. "This getting out of the car and confronting the other person where you're at, whether you're actually pulling a gun or you're showing that you have a gun, you have no idea if the person behind the wheel of the car also has a gun. You have no idea what their level of fright is." https://www.fox5vegas.com/2024/12/09/recent-road-rage-deaths-heighten-las-vegas-traffic-safety-concerns/

ANALYST COMMENTARY: According to an analysis of Gun Violence Archive data conducted by The Trace in April 2024, road rage shootings in the U.S. surged by 400 percent from 2014 to 2023. The Trace claimed that from 2014 to 2023, a total of 3,095 people were shot during road rage incidents which is approximately one person each day, and 777, or approximately 25 percent, of the individuals shot died from their injuries. The number of road rage shootings peaked in 2022 at 502, though it did not fall much in 2023, with 456 still reported. According to The Zebra, an insurance comparison firm, approximately 96 percent of drivers have witnessed at least one road rage incident in the U.S. in 2024 and 82 percent of drivers admit to having road rage or aggressive driving tendencies. The Zebra also found that only 10 percent of drivers reported having called the cops to report road rage incidents. Techniques that can be used to mitigate road rage incidents and mitigate escalation can be found at: https://www.defensivedriving.org/dmv-handbook/avoiding-road-rage-12-ways-you-can-escape-aggressive-driving/

To Solve Light Rail Crime, Start With Agents On Every Train
Minnesota Star Tribune, 12/10/2024

[Minnesota] … Right now, the question for Twin Cities transit users is: Will anyone of authority be on your train if something happens? In transit agencies around the country, there used to be. For decades,

conductors were a mainstay of public transit. They opened doors, announced stops, sometimes collected fares and most importantly enforced a code of conduct. The same is true today on the Northstar commuter rail, as well as on Amtrak — carry-overs from the age of rail travel where, for better or worse, conductors in some states had police powers. With the advent of automatic stop announcements and reassigning door-opening to motorpersons, cities like Boston and Chicago got rid of their conductors. That meant a huge savings in salaries, but at the cost of safety. One analysis shows crime on Chicago's system has doubled since conductors were dismissed in 2000. https://www.startribune.com/to-solve-light-rail-crime-start-with-agents-on-every-train/601193454

Saskatoon Transit Safety Staff 'Afraid To Ride The Bus,' Union Says
Saskatoon StarPhoenix, 12/10/2024

[Saskatoon, Canada] The union representing Saskatoon Transit staff says stressful conditions continue on city buses in spite of a new program designed to increase the safety of passengers and drivers. Fire Community Safety Workers, formerly called Community Safety Officers, were introduced in June in an effort to address violence and aggression on city buses. "We're seeing weapons, we're seeing bear spray, knives, machetes, hammers, drywall saws. Pretty much anything you can think of is happening on the bus," said Darcy Pederson, president and business agent for Amalgamated Transit Union local 615. … "The reports I'm getting back is (the fire community support workers) are actually afraid to ride the bus," Pederson said. City council expects to receive more information about the program next year in an annual report on its progress. Saskatoon Transit director Mike Moellenbeck said social disorder incidents on city buses, including intoxication and verbal abuse, have increased, but assaults on bus drivers have declined over the last year after protective barriers were installed and security and supervisory staff were added. https://thestarphoenix.com/news/local-news/saskatoon-transit-safety-staff-afraid-to-ride-the-bus-union-says

New Jersey State Senator Calls For 'Limited State Of Emergency' Over Mysterious Drone Sightings
ABC News, 12/10/2024

[Oakland, California] A New Jersey state senator is calling for a limited state of emergency over the mysterious drones that have been seen flying over New Jersey in recent weeks. "The State of New Jersey should issue a limited state of emergency banning all drones until the public receives an explanation regarding these multiple sightings," Republican state Sen. Jon Bramnick said in a statement Tuesday. The call came amid numerous recent drone sightings reported across New Jersey in recent weeks. The drones are larger than the type typically used by hobbyists, officials and eyewitnesses have said. The source and reason for the drones remains unknown as local, state and federal investigators look into the matter. The Picatinny Arsenal in New Jersey -- a military research and production facility in Morris County -- has reported 11 confirmed sightings by a police officer or security guard in response to a report since Nov. 13. https://abcnews.go.com/US/new-jersey-state-senator-calls-limited-state-emergency/story

TSA Rule Would Require Cyber Risk Management For Railroads, Buses, And Pipeline Operators
JD Supra, 12/10/2024

On November 6, 2024, the Transportation Security Administration (TSA) published a Notice of Proposed Rulemaking (NPRM) that would mandate cyber risk management and reporting requirements for certain surface transportation owners and operators. TSA's NPRM would impose cybersecurity requirements on designated critical surface transportation sectors—including pipelines, freight railroads, passenger railroads, and bus operators—adapted from the cybersecurity framework developed by the National Institute of Standards and Technology and the cross-sector cybersecurity performance goals developed by the Cybersecurity and Infrastructure Security Agency (CISA). https://www.jdsupra.com/legalnews/tsa-rule-would-require-cyber-risk-1283120/

Atmospheric River-Fueled Storm Threatens To Knock Out Power And Cause Travel Trouble In The Northeast
CNN, 12/11/2024

A wide-reaching storm boosted by an atmospheric river is drenching the entire East Coast Wednesday and its heaviest rain and strongest winds are still to come as it strengthens considerably throughout the day. The storm's worst sloppy mess of heavy rain and strong winds will be in the Northeast and make for treacherous travel and a miserable day. Winds gusting 50 to 60 mph in the afternoon and evening could also knock out power across the region, including in New York City and Boston. "Damaging winds could blow down trees and power lines. Widespread power outages are possible. Travel could be difficult, especially for high profile vehicles," such as buses and trucks the National Weather Service office in Boston warned. … Experts are saying this will be the most moisture-rich system in the Northeast since last December when widespread flooding killed several people and caused significant damage to roads in Maine. https://www.cnn.com/2024/12/10/weather/northeast-storm-atmospheric-river-climate/index.html

CYBERSECURITY

At Least $100,000 In Transit Fare Revenue Lost From Cyberattack On Oahu Transit Services
Transit Talent, 11/27/2024

[Honolulu, Hawaii] A crippling cyberattack that targeted TheBus and The -Handi-Van earlier this year wound up costing the city $100,000 or more in lost fare revenue, Honolulu officials indicate. Nearly a half-year later, Oahu Transit Services Inc., the private company that manages the city's bus and paratransit system, said it's still working on implementing cybersecurity measures to protect its fleet as well as its ridership. Over several days in mid-June, OTS said, thebus.org website, HEA (also known as Honolulu Estimated Arrival) and related GPS services were inoperable due to the cyberattack. The city Department of Transportation Services said on June 18 that there was a "cyber breach" and that OTS

was working with the "proper authorities to investigate and handle the situation." HOLO card readers on TheBus and TheHandi-Van were also affected. https://www.transittalent.com/articles/index.cfm?story=Lost_Fare_Revenue_In_Cyberattack_on_Oahu_Transit_Services_11-29-2024

ANALYST COMMENTARY: In June 2024, Oahu Transit Services (OTS) suffered a ransomware attack from DragonForce Ransomware (DFR). OTS is a contractor that manages Honolulu, Hawaii's bus and paratransit system. OTS is the primary bus service on the island of Oahu, managing over 100 routes that connect customers to major destinations such as Honolulu, Waikiki, Kapolei, and Pearl Harbor. The attack impacted the organization's phone systems, GPS services, and left its websites offline for four days. Additionally, DFR listed OTS on its leak site claiming to have stolen 800,000 records containing customers' sensitive personal information. OTS President and General Manager Robert Yu told the City Council's Public Infrastructure and Technology Committee in mid-November that the attack cost the service $100,000 or more in lost fare revenue. The initial point of access was not confirmed by Yu, but DFR most commonly gains initial access through phishing attacks, particularly spearphishing with malicious attachments such as Word documents, Excel files, or ZIP archives containing JavaScript files, to trick users into executing malware. The group is also known to gain access by exploiting vulnerabilities in Remote Desktop Protocols (RDP) and Virtual Private Network (VPN) solutions. Yu noted that the breach has resulted in "training our employees on the importance of looking" at emails and "making sure it's the proper email that you recognize the sender."

Hackers Use Corrupted ZIPs and Office Docs to Evade Antivirus and Email Defenses
Hacker News, 12/4/2024

Cybersecurity researchers have called attention to a novel phishing campaign that leverages corrupted Microsoft Office documents and ZIP archives as a way to bypass email defenses. "The ongoing attack evades #antivirus software, prevents uploads to sandboxes, and bypasses Outlook's spam filters, allowing the malicious emails to reach your inbox," ANY.RUN said in a series of posts on X. The malicious activity entails sending emails containing ZIP archives or Office attachments that are intentionally corrupted in such a way that they cannot be scanned by security tools. These messages aim to trick users into opening the attachments with false promises of employee benefits and bonuses. In other words, the corrupted state of the files means that they are not flagged as suspicious or malicious by email filters and antivirus software. https://thehackernews.com/2024/12/hackers-use-corrupted-zips-and-office.html

ANALYST COMMENTARY: This phishing campaign is a clever evolution of traditional techniques, exploiting corrupted file formats to bypass antivirus tools and email filters. By sending intentionally damaged Office documents or ZIP archives, attackers evade automated scanning mechanisms, which fail to analyze such files. The brilliance of this method lies in its reliance on the built-in recovery features of common applications like Microsoft Word and WinRAR. These programs can repair and

open corrupted files, effectively enabling the payload to execute without raising suspicion. This tactic highlights a gap in current security solutions, as these files are flagged neither as malicious nor as unusable, slipping past many defenses. The inclusion of QR codes in the booby-trapped documents adds another layer of social engineering. Scanning these codes redirects victims to phishing websites or initiates malware downloads, furthering the attackers' objectives of stealing credentials or compromising systems. This attack underscores the critical need for organizations to educate employees about the dangers of unsolicited attachments and emphasize scrutinizing the sources of such files, regardless of perceived legitimacy. For security teams, this campaign is a wake-up call to enhance detection methods for non-standard file behaviors and corrupted formats. Sandboxing solutions should simulate recovery scenarios to assess the true intent of files, and endpoint defenses must monitor for unusual file repair activities. It's a reminder that attackers are adept at identifying and exploiting overlooked system behaviors, pushing defenders to stay proactive and vigilant.