Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

December 23, 2024

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Man Arrested Over Death Of Woman Set On Fire On New York Subway
BBC, 12/23/2024

[New York] A man has been arrested in New York in connection with the death of a woman who was set on fire on a subway train in Brooklyn. Police Commissioner Jessica Tisch described Sunday's incident as "one of the most depraved crimes one person could possibly commit against another human being". She said the woman was on a stationary F train when she was approached by a man who used a lighter to ignite her clothing - which became "fully engulfed in a matter of seconds". Although officers extinguished the flames, the victim died at the scene. Police are still working to establish a possible motive for the attack. No charges have yet been filed. https://www.bbc.com/news/articles/clygk48nxgzo

ANALYST COMMENTARY: At approximately 7:30 a.m. on 22 December 2024, a man murdered a woman riding the F Train that was idling at Coney Island-Stillwell Avenue station in New York during a random arson attack. According to New York City Police Department (NYPD) Commissioner Jessica Tisch, "As the train pulled into the station, the suspect calmly walked up to the victim, who was in a seated position at the end of a subway car … and used what we believe to be a lighter to ignite the victim's clothing, which became fully engulfed in a matter of seconds." The suspect remained at the scene and watched the woman burn to death even while transit officers responded and attempted to save her. He then left the scene by train and was arrested later after a witness phoned in a tip. The NYPD has credited both tips from witnesses and the Metropolitan Transportation Authority's (MTA) robust security camera infrastructure as being invaluable during the hunt for the suspect. No motive for the killing has been released. This incident is the second high-profile murder on a major transit system in the past two years where the assailant used fire as a murder weapon. In Toronto, Canada in 2022, a man set a 28-year-old woman on fire while they both rode a city transit bus. In that case, the suspect asked the victim if she was a Tibetan, and when she said yes, he poured an accelerant (a mason jar full of lighter fluid) on her and ignited it. Officials claimed the crime was random in nature and initially suspected that the crime was motivated by hate because the two individuals were strangers to each other; however, during the attacker's two-year long trial, the Canadian judicial system ruled that he could not be held criminally responsible because he had schizophrenia and "had delusions that the Tibetan community hated him." He was remanded to psychiatric care where he will remain until he is no longer considered a threat to public safety.

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Subway Stabbing That Killed 1, Injured Another Was In Self Defense, Queens District Attorney Finds
ABC 7, 12/23/2024

[Queens, New York] A 69-year-old man who stabbed two men attempting to rob him on a subway train in Queens, killing one, appears to have been acting in self-defense and was not charged. The man was sleeping on the Manhattan-bound No. 7 train when a group of men took his bags early Sunday around 12:30 a.m. in Woodside. He woke up and tried to get his bags back. During the struggle, the man pulled a knife and stabbed two of the men. A 32-year-old man was stabbed in the chest and pronounced dead at Elmhurst Hospital. A second man was slashed in the face and is being treated at the hospital. The Queens District Attorney's Office declined to prosecute the man. He is believed to have been acting in self-defense. https://abc7ny.com/post/subway-crime-stabbing-killed-1-injured-another-7-train-was-defense-during-robbery-queens-da-finds/15695846/

5 Injured After Fleeing Driver Crashes Into JCPenney At Texas Mall; Suspect Fatally Shot: Police
ABC 7, 12/21/2024

[Killeen, Texas] A man drove into a Texas mall after a 19-mile police pursuit, striking four people before he was fatally shot by responding law enforcement officers, according to the Texas Department of Public Safety. A trooper shot and killed the suspect after the chase led them into the mall, Texas Department of Public Safety Sgt. Bryan Washko said at a Saturday news conference. A Texas Highway Patrol Trooper attempted to stop a pickup truck around 5 p.m. Central Time, Washko said. The man driving the vehicle was called in as possibly driving while intoxicated, Washko said. After the suspect exited the highway, he entered the Killeen Mall parking lot, where he drove through the glass doors of a JC Penney store's main entrance, according to Washko. https://abc7ny.com/post/killeen-shooting-today-5-injured-after-fleeing-driver-crashes-jcpenney-texas-mall-suspect-fatally-shot-police-say/15688397/

Amtrak Service Resuming With Delays Between New York And Philadelphia
ABC 7, 12/22/2024

[New York] Amtrak service is resuming with delays between New York Penn Station and Philadelphia after an earlier issue with downed overhead wires. The railroad says two of Amtrak's four tracks along the route have been returned to service and that trains are moving at reduced speeds in and out of NY Penn Station. Amtrak says continuing delays should be expected up and down the Northeast Corridor: This incident has impacted trains operating from Washington Union Station (WAS) to Boston South Station (BOS). Customers traveling along the Northeast Corridor should expect delays of at least 30 minutes to 60 minutes. We will update you when the service is fully restored. We appreciate your patience. https://abc7ny.com/post/amtrak-suspended-between-nyc-and-philadelphia/15690816/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TERRORISM & EXTREMISM

Questions Mount In Germany Over Deadly Christmas Market Attack As Suspect Appears In Court
CNN, 12/22/2024

Authorities in Germany face growing accusations they could have done more to prevent a deadly Christmas market attack as a judge ordered the suspect to be held in pre-trial detention following a late-night court appearance on Saturday. Taleb Al Abdulmohsen is accused of ramming a car into a busy market in the city of Magdeburg, killing five people and injuring more than 200. The motive for the attack is unclear but the suspect is a 50-year-old Saudi citizen who has lived in Germany for more than a decade and worked to help Saudis leave his home country. On social media, he has been a fervent critic of Islam and prosecutors suggested he may have become embittered with how Germany treats Saudi refugees. Recent messages grew increasingly threatening. One says, "if Germany wants to kill us, we will slaughter them, die, or go to prison with pride." "The magistrate ordered pre-trial detention for five counts of murder, several counts of attempted murder and several counts of dangerous bodily harm," a statement from police early Sunday said. https://www.cnn.com/2024/12/22/europe/german-market-attack-suspect-court-intl/index.html

ANALYST COMMENTARY: Numerous deadly incidents and disrupted plots demonstrate that mass gatherings and other populated public spaces remain attractive targets to extremists seeking to maximize casualties and/or amplify the secondary impact of their attacks. Individuals espousing a broad range of ideologies continue to employ relatively rudimentary tactics and readily available implements – including vehicles, guns, improvised explosives, and edged weapons – to attack densely populated areas. In response, security professionals urge vigilance and prompt reporting of suspicious activity to authorities. Based on day-to-day experience and familiarity with their surroundings, residents, patrons, and employees are particularly well-placed to identify suspicious items or behavior that could indicate an emerging or imminent threat. Once aware of a potential concern, personnel should promptly report what was seen, when, and where in the greatest detail possible. Organizations should also define their perimeter, evaluate areas that may require access control for pedestrians and vehicles, deploy permanent and temporary barriers to establish clear standoff zones around buildings and outdoor spaces frequented by people, and ensure that fences, gates, and barriers are appropriately sized, sufficiently anchored, adequately reinforced, and fully functional. For additional information on vehicle ramming attacks, a comprehensive analysis including attacker statistics and mitigation techniques can be found in the Mineta Transportation Institute's (MTI) "Smashing Into Crowds" report at: https://transweb.sjsu.edu/research/SP1119-Vehicle-Ramming-Update. The MTI also has a related analysis regarding vehicle attacks against U.S. protestors that can be found at: https://transweb.sjsu.edu/sites/default/files/SP1020-Metal-Against-Marchers.pdf.

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY & SAFETY AWARENESS

Trolley And Bus Riders Say They Feel Safer, A Year After Security Boost. Here's What Else A New Survey Found.
San Diego Union Tribune, 12/20/2024

[San Diego, California] A new survey finds people riding the San Diego trolley and local buses feel safer a year after security got beefed up and enforcement officers got more power to issue citations for crimes such as battery and indecent exposure. Metropolitan Transit System officials say making people feel safe can boost ridership, which could be crucial as new high-rise housing development makes transit a more practical transportation option. When asked whether they feel safer than they did a year ago, nearly four times as many riders who were surveyed said yes as said no. And trolley riders — who typically express more concerns about safety than bus riders — expressed greater confidence in their safety than bus riders did. https://www.sandiegouniontribune.com/2024/12/20/trolley-and-bus-riders-say-they-feel-safer-a-year-after-security-boost-heres-what-else-a-new-survey-found/

Chinese National Charged With Acting As Beijing's Agent In Local California Election
Associated Press, 12/20/2024

[California] A Chinese national was arrested Thursday on charges of acting as an illegal agent for Beijing when serving as the campaign manager for an unnamed politician elected to a city council in Southern California two years ago. The arrest of Yaoning "Mike" Sun, 64, came at a time of rising concerns that the Chinese government has cultivated a network of operatives to influence local elections in the U.S. to install politicians who are friendly to Beijing and can help promote Chinese interests. According to a complaint filed Tuesday in the U.S. District Court for the Central District of California, Sun is accused of conspiring with Chen Jun, who was sentenced to 20 months last month for acting as an illegal agent of the Chinese government. Chen, 71, also a Chinese national, pleaded guilty in July to using Chinese money to bribe federal agents to undermine the anti-Beijing spiritual group Falun Gong. The charge against Sun shows that Chen also conspired to interfere with local elections.
https://apnews.com/article/china-election-interference-california-yaoning-mike-sun-194aaaa29afea6dda9b55e8cb1cd0c44

ANALYST COMMENTARY: On 19 December 2024, law enforcement authorities arrested a Chinese national who was serving as a campaign manager for an Arcadia, California city councilwoman on suspicion of conspiracy and acting as an illegal foreign agent for China. Multiple media outlets have also reported that the Chinese national charged, Yaoning "Mike" Sun, was also engaged to the city councilwoman. According to authorities, from 2022 to 2023, Sun had been conspiring with another individual, Chen Jun, who has since plead guilty to being an illegal foreign agent of China. The two men are believed to have been receiving funding and direction from the Chinese government to elevate certain persons in the U.S. to U.S. political offices, as long as those people have political goals

Timely reporting to the **TSA Transportation Security Operations Center** is essential. Reports are made by telephone at **866-615- 5150** and by e-mail at **TSOC.ST@tsa.dhs.gov.**

and policies that the Chinese government finds favorable. It is unclear if the city councilwoman Sun worked to install was aware of Sun's Chinese government involvement and she has not been charged. The actions of the suspected Chinese agent in California are not unprecedented and have been making headlines often in recent months – in September 2024, a former aide to two New York governors was also charged as acting as an illegal foreign agent of China and is accused "using her positions to subtly advance Beijing's agenda." Chinese espionage in California is also a recurring theme, though the foreign agents are not limited to conspiring to install "favorable" politicians to political offices. In the 1990s and early 2000s, the U.S. claimed that Chinese operatives had infiltrated Lawrence Livermore National Laboratory (LLNL) on multiple occasions and had successfully obtained top-secret nuclear and rocket technology blueprints that were turned over to the Chinese government at least once. In the 1990s, some of the information was allegedly solicited from or provided by students working at the labs. LLNL and the University of California, Berkely's Lawrence Berkeley National Laboratory (LBNL) focus on nuclear research and often collaborate closely with each other, and U.S. officials have raised concerns that the Chinese government might specifically try to install foreign agents at California colleges with the goal of infiltrating the academic and research communites for the national security information the labs may contain. The threat has remained persistent, and in 2019, the U.S. intelligence community openly warned in their annual threat assessment that Chinese actors were assessed to be exploiting "the openness of American society, especially academia and the scientific community, using a variety of means."

MTA's Subway Camera Bet Pays Off In Arrest After Fatal F Train Fire
Gothamist, 12/23/2024

[New York] New York Gov. Kathy Hochul spent Sunday morning discussing various state issues, including the installation of surveillance cameras on every New York City subway car. The MTA has finished installing 13,000 cameras on its 6,455 subway cars — an effort that complements the 10,000 cameras already in place across the city's subway stations, Hochul said. The project, which the governor originally championed in 2022, was completed ahead of schedule, with the governor noting that it was part of a broader initiative to improve safety and boost confidence in the subway system. Ridership has increased by 148% since January 2021, while crime has decreased by 42% during the same period, according to the governor. Speaking on "Up Close with Bill Ritter" on ABC7, Hochul emphasized the impact of the finished $5.5 million program, which had been accelerated in response to rising subway ridership.
https://gothamist.com/news/mtas-subway-camera-bet-pays-off-in-arrest-after-fatal-f-train-fire

Kalamazoo, MI, Using AI To Respond To Non-Emergency Calls
Firehouse, 12/21/2024

[Kalamazoo County, Michigan] The Kalamazoo County Consolidated Dispatch Authority is now using an artificial intelligence (AI) system to respond to some calls that come in through a non-emergency line. The calls will now be processed by Ava, the dispatch center's new virtual assistant. The tech is powered

by Aurelian, a Seattle-based software company, the Kalamazoo County dispatch center said in a news release while announcing the AI on Thursday, Dec. 19. Ava is quick to react to requests and respond to questions. It speaks multiple languages, officials said. The AI is "very smart," the agency said. The company advertises the technology as "a powerful Voice AI that doesn't just route callers, but actually solves their needs." The AI agent is designed specifically for emergency communications centers, including routing calls appropriately and collecting information for public safety resources to be dispatched, the the news release states. The dispatch center encourages callers to provide as much detail as possible to the AI to get the fastest response to non-emergency requests. https://www.firehouse.com/technology/cad-dispatch-systems/news/55251230/kalamazoo-mi-using-ai-to-respond-to-non-emergency-calls

Colo. Transit System Deploys K-9s To Improve Safety
Police1, 12/22/2024

[Denver, Colorado] The Regional Transportation District is deploying more counterterrorism dogs for station sweeps and inspections on buses and trains, the latest effort to ramp up security and encourage riders to return. Three new K-9 team members, Belgian Malinois dogs, include Milo, born and bred in Hungary, who RTD transit police officer Corey Averill describes as extremely focused and motivated. "Milo lives for his job," Averill said. "If he was a house pet, he would go nuts. He wants to work." The expanded K-9 capacity — RTD previously had one dog — is part of a security campaign to boost security on public transit around metro Denver as violence has spilled into RTD buses and trains. RTD's annual ridership has decreased from 106 million in 2019 to around 65 million. https://www.police1.com/k-9/colo-transit-system-deploys-k-9s

House Approves Security Screening Legislation
Bulk Transporter, 12/23/2024

The U.S. House of Representatives unanimously passed the Transportation Security Screening Modernization Act on Dec. 18, simplifying the vetting process for commercial drivers delivering vital commodities throughout the country. The bill now heads to President Biden's desk to be signed into law. National Tank Truck Carriers and American Trucking Associations spearheaded the efforts to consolidate the application process for Hazardous Materials Endorsement (HME) for commercial driver's licenses and the Transportation Worker Identification Credential (TWIC) required for many hazmat operators. This legislation will save money and synchronize the expiration dates of the HME and TWIC credentials, which removes another barrier to attracting necessary workers to the trucking industry. https://www.bulktransporter.com/regulations/article/55251435/house-passes-transportation-security-screening-bill

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

CYBERSECURITY

Remcos RAT Malware Evolves with New Techniques
InfoSecurity Magazine, 12/12/2024

A sharp increase in cyber-attacks involving the Remcos remote access Trojan (RAT) has been identified in Q3 2024. The malware, delivered through phishing emails and malicious attachments, enables attackers to control victim machines remotely, steal data and carry out espionage. McAfee Labs researchers have analyzed two distinct Remcos RAT variants, each leveraging unique methods for delivery and execution. The first variant employs a highly obfuscated PowerShell script triggered by a VBS file. This script downloads files from command-and-control (C2) servers and injects malicious code into RegAsm.exe, a legitimate Microsoft executable. By using multi-layer obfuscation, it avoids detection by mimicking legitimate system paths and directories. The second variant spreads via spam emails containing malicious Microsoft Office Open XML (DOCX) attachments. These files exploit CVE-2017-11882, a remote code execution vulnerability. Upon execution, an embedded script downloads additional malware payloads, ultimately leading to the deployment of Remcos RAT. https://www.infosecurity-magazine.com/news/remcos-rat-malware-evolves-new/

ANALYST COMMENTARY: The resurgence of Remcos RAT reflects a broader trend in the evolution of evasive malware, with attackers increasingly leveraging old vulnerabilities like CVE-2017-11882 alongside sophisticated obfuscation techniques. This hybrid approach maximizes their reach while complicating detection. Organizations should consider this an urgent call to retire outdated software dependencies, particularly for older Office formats, as these remain low-hanging fruit for attackers. The use of PowerShell scripts, Base64 encoding, and in-memory execution further signals the growing reliance on "living-off-the-land" techniques, where attackers exploit legitimate tools to camouflage malicious activity. While McAfee's IOCs provide a strong starting point for identifying these threats, organizations must adopt proactive strategies. This includes advanced endpoint detection and response (EDR) solutions capable of behavioral analysis and anomaly detection, which can identify the hallmarks of malicious PowerShell or process injection. Additionally, isolating email attachments via sandboxing, combined with real-time threat intelligence feeds, can thwart initial infection attempts. User education remains pivotal, but it's worth integrating phishing simulations to test and improve awareness continuously. Beyond patch management and awareness, organizations should also invest in network segmentation and enforce least-privilege policies to limit the lateral movement of such malware. As these tactics evolve, having a comprehensive incident response plan to deal with breaches is just as critical as the defenses designed to prevent them.