Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

OVER-THE-ROAD-BUS INTELLIGENCE AWARENESS DAILY (OTRBIAD) REPORT

November 1, 2024

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) MONTH

Resolve To Be Resilient!

Each year, the Cybersecurity and Infrastructure Security Agency (CISA) leads the national recognition of Critical Infrastructure Security and Resilience (CISR) Month in November… As a nation, we are grappling with continued cyber and physical threats to critical infrastructure Americans rely on every day. We have seen increasing threats of violence targeted at faith-based organizations, election workers, and others; extended, record-breaking heat and destructive weather and fire events; global conflicts with ripple effects around the world, including civil disturbances at home; and rapid advances in technology that enable novel cybersecurity risks. The safety and security of the nation depends on the ability of critical infrastructure owners and operators to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. We must accept that it's a whole of community responsibility to prepare and secure the nation's critical infrastructure and protect the vital services it provides, so when something does happen, we are better able to respond to and recover from any impacts. We can do this by building resilience into our preparedness planning year around by understanding the threat landscape and assessing risks; creating and exercising actionable plans; and continually adapting and improving based on lessons learned.
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-security-and-resilience-month

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Manhunt Under Way In Berlin After Bag Of Explosives Left At Train Station
Reuters, 10/31/2024

[Berlin, Germany] German police are searching for a man who abandoned a bag of explosives at a Berlin train station and ran away after being stopped by federal officers, according to police. "We are investigating all possibilities," a police spokesperson told Reuters on Thursday, adding that authorities had not yet been able to identify the suspect. Police said they stopped the man in the German capital's Neukoelln station on Wednesday afternoon. He fled the scene and explosives were found in the bag he left behind, according to a post on social media platform X. The bag was brought to a nearby park where

a controlled explosion took place, the post said. The Bild newspaper reported that the bag had contained triacetone triperoxide, an unstable white explosive powder known as TATP and often used in extremist attacks on the public. Police could neither confirm nor deny the report on the type of explosive. https://www.reuters.com/world/europe/manhunt-under-way-berlin-after-bag-explosives-left-train-station-2024-10-31/

ANALYST COMMENTARY: At approximately 3:30 p.m. on 30 October 2024, German federal police conducting a "routine" check of a man at the Neukölln train station in southern Berlin, Germany discovered a cloth bag containing explosives. According to German officials, the police confronted the man and he began to flee. The police attempted to detain him by grabbing him, and the man shook the officer's grip, dropped his bag, and fled the scene by running across the train tracks. When police went through the bags contents they discovered an explosive device. A manhunt has been launched for the suspect, and bomb removal experts were called to the scene, and took the device to a nearby park where it was subjected to a controlled detonation. German officials have not said much about the device or provided any description of the suspect, though they did claim that "If this explosive device had gone off in the vicinity of a group of people, it would have had dramatic consequences." German media agencies have said that the explosive device appeared to be "a grey substance, a plastic bottle wrapped with wires and a paper bag with more cables." They have also speculated that the grey substance was triacetone triperoxide (TATP), which is an explosive compound commonly found in improvised explosive devices (IEDs) due to the widespread availability of the ingredients needed to synthesize it. TATP takes the form of a crystalline white powder. German politicians have been quick to suggest the incident is terrorism related; however, German law enforcement officials have made no such claims and German media agency dpa has said there are "no indications that a planned attack was foiled." It remains unclear why the suspect was transporting an explosive device and what his plans for it may have been. The incident is under investigation by the Berlin Police State Criminal Police Office responsible for explosives offences on behalf of the Berlin Public Prosecutor's Office. Of note, criminals in Germany have been using explosive devices to rob cash machines over the past few years. In October 2024, CNN reported that "in Germany – Europe's largest economy – thieves have been blowing up ATMs at a rate of more than one per day in recent years."

Shots Fired At Norfolk Southern Railway Police During Burglary Investigation In Fuller Park
ABC 7, 10/30/2024

[Chicago, Illinois] Chicago police said shots were fired at Norfolk Southern police on Wednesday morning. The shooting happened near 45th Street and Stewart Avenue in Fuller Park on at about 6:15 a.m. Railway police were on patrol inside unmarked squad vehicles when shots were fired in their direction, Chicago police said. Nobody was injured in the shooting. The suspects entered two vehicles and drove off in an unknown direction. No one is in custody and Area Detectives are investigating. https://abc7chicago.com/post/chicago-shooting-shots-fired-norfolk-southern-police-45th-street-steward-avenye-fuller-park-say/15488572/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

2 Shot Dead And 6 Injured In Downtown Orlando During Halloween Celebrations
NBC News, 11/1/2024

[Orlando, Florida] Two people are dead and at least six others are injured after a shooting in downtown Orlando, Florida, in the early hours of Friday morning as thousands enjoyed the city's Halloween celebrations, police said. Police arrested a 17-year-old boy on suspicion of carrying out the shooting. No motive has so far been established and the identities of those killed and injured have not been released, although police said the victims ranged in age from 19 to 39. https://www.nbcnews.com/news/us-news/2-shot-dead-6-injured-downtown-orlando-halloween-celebrations-rcna178356

Officer Injured As Riot Police Called To Edinburgh Fireworks Disorder
BBC, 11/1/2024

[Edinburgh, Scotland] A police officer has been injured and more than a dozen buses damaged in Edinburgh during a night of disorder on Halloween. Riot police were pelted with bricks and fireworks in the city's Niddrie area, with a female officer hurt when the window of her vehicle was shattered. An open-top bus carrying young people with disabilities was also targeted with fireworks outside the city's Dynamic Earth attraction. A 14-year-old boy was arrested and charged with fireworks offences. It came hours before an exclusion zone on fireworks in parts of the city came into force. Earlier officers seized a "quantity of fireworks" and two cans of petrol during a raid on a property in the Magdalene Gardens. Lothian Buses withdrew at least nine bus services due to anti-social behaviour. Police also responded to incidents at Moredunvale Road, Southhouse Road, Captain's Road and West Pilton Park, where a number of buses were targeted. Edinburgh city council leader Cammy Day said a total of 16 vehicles from the Lothian fleet were damaged. … He said: "It is despicable, the behaviour of a minority of people in certain areas of the city, attacking public service workers and bus drivers.
https://www.bbc.com/news/articles/c62lkw6qwy9o

Las Vegas Train Crash Injures 1, Leads To Closures On Sunset Road
Las Vegas Review Journal, 10/30/2024

[Las Vegas, Nevada] A train collision near Sunset Road and Decatur Boulevard left a man injured, the Metropolitan Police Department said. Around 7:05 p.m. Wednesday, a train struck an unoccupied truck parked on the tracks at 6420 Cameron St. After it was hit, the truck damaged fencing, which fell and hit several other vehicles. What appeared to be an unoccupied homeless camp was also hit, Metro Lt. Trish Heldt said in a text message. One man was injured and complained of neck pain, but he was stable. Heldt added that the crash was under investigation. A portion of Sunset Road near the crash will be closed until Thursday. Metro was also expecting a repair crew from California on Thursday.
https://www.reviewjournal.com/local/local-las-vegas/train-crash-injures-1-leads-to-closures-on-sunset-road-3203811

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TERRORISM & EXTREMISM

Suspect Faces Hate Crime, Terrorism Charges In Shooting Of Jewish Man On Chicago's North Side
CBS, 10/31/2024

[Chicago, Illinois] Authorities on Thursday announced terrorism and hate crime charges against the man accused of shooting an Orthodox Jewish man in the West Ridge neighborhood last weekend, and then opening fire on police and paramedics. Sidi Mohamed Abdallahi, 22, had already faced six counts of attempted first-degree murder, seven counts of aggravated discharge of a firearm, and aggravated battery. On Thursday, Police Supt. Larry Snelling announced Abdallahi also has been charged with one felony count of terrorism and one felony count of a hate crime. Police said Abdallahi shot a 39-year-old man in the 2600 block of West Farwell Avenue in the West Ridge, or West Rogers Park, neighborhood around 9:30 a.m. on Saturday. After first responders arrived at the scene, the suspect is alleged to have opened fire on them and struck an ambulance. No officers or paramedics were hit.
https://www.cbsnews.com/chicago/news/sidi-mohamed-abdallahi-hate-crime-charges-west-ridge-shooting/

Deadly Explosion in Athens Apartment Sparks Anti-Terrorism Investigation
Greek City Times, 10/22/2024

[Athens, Greece] A fatal explosion rocked an apartment in Athens on Thursday, claiming the life of a man and seriously injuring a woman. Authorities have launched an anti-terrorism investigation into the incident, according to fire brigade and police officials. Preliminary assessments by Greece's anti-terrorism police unit suggest that the explosion was triggered by an explosive device, intensifying concerns over possible terrorist activity. The blast occurred in the Ampelokipi district, severely damaging the apartment and causing extensive harm to the entire residential building. Emergency responders successfully evacuated the injured woman, who was subsequently hospitalized. The identity of the deceased man remains unknown at this time. Greece experienced a surge in bomb and arson attacks during its 2009-18 debt crisis, primarily targeting politicians, judges, and businesses. Although such incidents have declined in recent years, this latest explosion has revived fears and prompted heightened security measures. https://greekcitytimes.com/2024/11/01/deadly-explosion-in-athens-apartment-sparks-anti-terrorism-investigation/

SECURITY & SAFETY AWARENESS

METRO Police Chief Responds To Videos Showing Violent Incidents Along Rail Line
ABC 13, 10/29/2024

[Houston, Texas] The Chief of the METRO Police Department is reacting to videos showing violent incidents on rail platforms. A METRO insider shared the videos with ABC13, claiming they expose problems within the department. Chief Vera Bumpers says they show officers doing their jobs.

All the videos are from the Northline Transit Center. In two of them, officers are struggling with suspects and have to use their Tasers. At times, bystanders step in to help. … According to METRO's website, major crimes, which include sex assaults, have nearly tripled over the last two fiscal years, from 460 in 2022-2023 to 1,279 in 2023 to 2024. https://abc13.com/post/crime-metro-rail-platforms-triples-videos-released-violent-attacks-where-officers-showed-delayed-response/15486656/

ANALYST COMMENTARY: Houston, like most major metropolitan areas, struggles with crime in its transit system which causes fear among riders. The prevalence of personal cellular devices enables many crimes to be captured on video which are then shared on social media channels. Short video clips that are absent of context or complete details can contribute to a jaded view of police actions or perceived inactions in responding to crime. Metro Police Chief Vera Bumpers points out that some of the videos depict police doing what they are supposed to do. ABC News reports that according to METRO's website, "major crimes, which include sex assaults, have nearly tripled over the last two fiscal years, from 460 in 2022-2023 to 1,279 in 2023 to 2024." Chief Bumpers stated they are working to address public safety concerns and are adding 20 new police officers in addition to increasing security guards throughout the system. Metro is also leveraging technology by adding emergency call buttons to MetroRail stations and adding video surveillance to all buses, trains, rail station platforms, Park and Ride lots and transit centers. The Metro Police web site points out that given the volume of passengers in the millions, METRO averaged approximately one major crime for every 133,155 rides total across the services. Major crimes include robbery and grand theft where no injuries result. In the time period from October 2023 to September 2024, Metro logged 73 million rides and reported 1,279 major crimes which is an average of 1 major crime for every 57,067 rides.

NYPD Drones Save More Than 100 Subway Surfers In NYC: Mayor Adams
PIX 11, 10/31/2024

[New York] Hundreds of drones have helped save more than 100 young people, including a 9-year-old, who were subway surfing on New York City trains in the past year, according to Mayor Eric Adams. "Subway surfing is not a game," Adams said at a press conference Thursday. The mayor said there have been 900 NYPD drones deployed that have caught and stopped 114 riders, including one that was just 9 years old. The average age of subway surfers is 14. The oldest was 33. The drones are used to monitor the most popular subway lines used for the dangerous activity, including the No. 7 train. The NYPD used 911 calls to send drones and officers to the necessary areas. https://pix11.com/news/local-news/nypd-drones-save-more-than-100-subway-surfers-in-nyc-mayor-adams/

ANALYST COMMENTARY: The draw to social media is so strong that many people engage in risky behavior to gain attention for themselves by posting videos on various platforms. Recently in New York City, two teenage boys were killed while subway surfing (riding on top of the trains while they are in motion). The boys were engaging in the behavior due to a "TikTok Challenge." On 27 October 2024, two teenage girls fell off the top of a moving subway train, killing one and critically injuring the other.

NYPD is using a multi-pronged approach in trying to curb the practice including public information campaigns, enforcement efforts and appealing to social media companies to scrub these videos from their sites. The use of surveillance cameras and unmanned arial surveillance systems (UAS) (AKA drones), is helping the NYPD to spot and engage subway surfers before they hurt themselves. When the NYPD is alerted to a subway surfer, a drone is launched to the area to capture what is taking place in real time. The responding police and the train operator can work together to mitigate the issue. NYPD reports that "Officers have apprehended 41 people who have been arrested more than once for subway surfing," according to PIX 11. MTA CEO Janno Lieber said that NYPD analysts are checking every day to ensure the videos are being deleted from social media, in an attempt to remove the incentive.

NYS Thruway Planning To Ban Drivers Who Already Don't Pay Tolls
CDL Life, 10/30/2024

[New York] The New York State Thruway has announced new measures banning some drivers from using the thruway. A spokesperson for the New York State Thruway told ABC 7. That the new regulation would ban drivers who haven't paid tolls from using the Thruway. The regulation would be enforced through license plates. Many drivers employ the use of fake license plates to avoid paying the tolls. "If you don't feel you can pay, just don't drive on it," said truck driver Mark Nemerow, who has been trucking for 50 years. The NYS Thruway Authority is missing $40 million in unpaid fees from drivers who have failed to pay the tolls. 90% of the Authority's revenue comes from tolls. https://cdllife.com/2024/nys-thruway-planning-to-ban-drivers-who-already-dont-pay-tolls/

CYBERSECURITY

New Attack Lets Hackers Downgrade Windows To Exploit Patched Flaws
HackRead, 10/26/2024

In a recent research, SafeBreach Labs researcher Alon Leviev exposed a new attack technique that could compromise the security of fully patched Windows 11 systems. This technique, dubbed Windows Downdate, involves manipulating the Windows Update process to downgrade critical system components, effectively resurrecting previously patched vulnerabilities. The attack was initially reported in August 2024 at Black Hat USA 2024 and DEF CON 32. Researchers have now published additional details to enhance public understanding of the attack. One such vulnerability is the "ItsNotASecurityBoundary" Driver Signature Enforcement (DSE) bypass, which allows attackers to load unsigned kernel drivers. This bypass allows attackers to replace a verified security catalogue with a malicious version, enabling the loading of unsigned kernel drivers. https://hackread.com/hackers-downgrade-windows-exploit-patched-flaws/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ANALYST COMMENTARY: The *Windows Downdate* attack technique, developed by SafeBreach Labs' Alon Leviev, targets fully patched Windows 11 systems by exploiting the Windows Update process to revert components to previous, vulnerable versions. Introduced at Black Hat USA 2024, this attack resurrects critical vulnerabilities by downgrading OS files. A primary vulnerability used in this technique is the *"ItsNotASecurityBoundary"* Driver Signature Enforcement (DSE) bypass, allowing attackers to replace legitimate security catalogues with malicious versions and load unsigned kernel drivers. The root cause is a new vulnerability class called *False File Immutability (FFI)*, which enables modifications to supposedly "immutable" files by clearing system working sets. This method affects Virtualization-Based Security (VBS) configurations, even those with UEFI locks, marking the first known bypass without physical access. Attackers can disable VBS features by adjusting registry settings or invalidating *SecureKernel.exe*. However, the VBS "Mandatory" flag with UEFI lock provides some resistance. The *Windows Downdate* attack facilitates installing custom rootkits, bypassing security controls, and maintaining stealth access. To mitigate this risk, experts recommend maintaining updated systems, deploying robust endpoint detection (EDR) tools, and applying strong network security measures. Enabling VBS with UEFI lock and the "Mandatory" flag is also advisable for organizations seeking enhanced protection against this downgrading threat.