Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

December 13, 2024

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

More Than 100 MARTA Bus Shelters Vandalized In 1 Week
Atlanta Journal Constitution, 12/12/2024

[Atlanta, Georgia] MARTA is working to repair more than 100 bus shelters that were vandalized in a one-week period this month, causing at least $20,000 in damage, officials said. The bus shelters, many of them new and clustered around Memorial Drive, were graffitied with a liquid substance that etches glass, a MARTA spokeswoman said. The etching makes the graffiti impossible to remove without replacing an entire glass panel, each of which costs about $200. In some cases, the glass was completely shattered, leaving the shelters open to the elements. The spokeswoman said most of the vandalism took place between Dec. 3 and Dec. 10. https://www.ajc.com/news/crime/more-than-100-marta-bus-shelters-vandalized-in-1-week/SKSYQ2SFIVAE3D3P2TBQSTSUS4/

Woman Sought After Allegedly Attacking 63-Year-Old Woman At Bus Stop In Philadelphia's Center City
6ABC, 12/13/2024

[Philadelphia, Pennsylvania] Philadelphia police are asking for the public's help identifying a woman accused of assaulting another woman while waiting at a bus stop in Center City. Officials released video of the assault that happened around 11:45 a.m. on Wednesday in the 1100 block of Market Street. In the video, police say the 63-year-old victim waiting for the bus when she was approached by an unknown woman who appeared to be screaming. The suspect can then be seen hitting the victim with a closed fist on the left side of the face for an unknown reason, knocking the victim to the ground. The suspect was wearing a black hat, black jacket, blue jeans and tan boots at the time of the attack. https://6abc.com/post/woman-sought-after-allegedly-attacking-63-year-old-bus-stop-philadelphias-center-city/15650732/

Extreme Cold Causes Morning Delays On Metra, CTA Trains Due To Cracked Rails
CBS News, 12/12/2024

[Chicago, Illinois] Thursday's extreme cold impacted the morning commute for many people in the Chicago area, as trains on five Metra lines and one CTA line came to a temporary halt because of breaks or cracks in the rails. … That's what happened on five of Metra's 11 commuter lines Thursday morning, with the extreme cold causing cracked rails and switching issues. "One is kind of a pull-apart, where the joint between the rails kind of separates, and you have a gap between there; or you have just kind of a

tiny minute crack in the steel, enough to disrupt the track circuit. And what the track circuit is, it controls all the signals," said Metra spokesman Michael Gillis said. Gillis said Metra issues service advisories to notify commuters as soon as possible when trains are delayed. "Unfortunately, a lot of this happened in the moment of the rush hour, and there were trains with people on them that were caught up in this, and we apologize for that. It's just a function of Chicago weather," Gillis said. Metra inspects their tracks twice each week. So what's the solution for switch problems? Gas burners are placed near switches so crews can ignite flames to warm them when needed throughout the system.
https://www.cbsnews.com/chicago/news/track-conditions-suspend-cta-brown-line-service-kimball-southport/

TERRORISM & EXTREMISM

European Union Terrorism Situation and Trend Report 2024 (EU TE-SAT)
Europol, 12/12/2024

The European Union Terrorism Situation and Trend Report (EU TE-SAT) 2024 is a situational overview, presenting figures and trends in the terrorism landscape in the EU in 2023, based on qualitative and quantitative data provided by Member States on terrorist attacks, arrests and court decisions issued for terrorist offences. Europol publishes the EU TE-SAT on a yearly basis. With the purpose of informing policymakers, law enforcement and the wider public, the EU TE-SAT aims at protecting public safety and advancing regional stability, allowing the EU to continue responding to terrorism in an efficient manner and making Europe safer. https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat

ANALYST COMMENTARY: According to the Global Terrorism Index (GTI) produced by the Institute for Economics & Peace (IEP), the impact of terrorism in Europe is the lowest it has been since the index's inception. Altogether, the GTI 2024 report data reveals an 88% decline in fatalities from terrorism and a 63% percent decline in terrorist attacks across Europe over the past decade. Seventeen of the 36 countries in the region haven't recorded a single incident over the past five years. By contrast, the impacts of terrorism increased in the U.S., which accounted for 76% of terrorism-related deaths in Western democracies in 2023. GTI data indicates that North America and sub-Saharan Africa are the only regions where the impact was higher in 2023 than in 2013. The GTI 2024 report also noted a significant shift in the "epicenter" of terrorism from the Middle East to the Central Sahel region of sub-Saharan Africa, which now accounts for more than half of all deaths from terrorism. The terrorist threat became increasingly concentrated as well, with just ten countries accounting for 87% of total terrorism-related deaths. For more information, the GTI 2024 Report is available here: https://www.visionofhumanity.org/maps/global-terrorism-index/#/

This Is How Political Violence Goes Mainstream
The Atlantic, 12/11/2024

It is tempting to think of political extremists as those who have had their brain flambéed by a steady media diet of oddball podcasters, fringe YouTubers, and "do your own research" conspiracists. Dylann Roof, who killed nine people at a Black church in Charleston, South Carolina, in 2015, was known to hang out in white-supremacist forums. Robert Bowers frequently posted racist content on the right-wing site Gab, where he wrote "Screw your optics, I'm going in" just before murdering 11 people at a synagogue in Pittsburgh in 2018. Brenton Tarrant's manifesto explaining why he murdered 51 people in two mosques in Christchurch, New Zealand, in 2019 was filled with 4chan jokes and memes, suggesting that he had spent ample time on the platform. https://www.theatlantic.com/technology/archive/2024/12/luigi-mangione-political-violence-mainstream/680964/

ANALYST COMMENTARY: According to the Network Contagion Research Institute (NCRI), which is a nonprofit that focuses on online extremism, the targeted killing of UnitedHealthcare CEO Brian Thompson on 3 December 2024 may represent a shift in the way extremists promote their ideologies online. Historically, following a high profile violent event, extremists have shared content praising or promoting further violence primarily on "fringe" websites like 4chan and 8chan with "niche online subcultures", or amongst each other in private chat groups. In stark contrast to that, following the killing of Brian Thompson, the NCRI noted that six of the top 10 most viewed posts on X (formerly Twitter) that mentioned either Brian Thompson or UnitedHealthcare "either expressed explicit or implicit support for the killing or denigrated the victim." On one post, a user wrote "Are we starting now then?" which received over 1.8 million views and multiple users discussed a "Class War" in the comments section. These posts that "expressed explicit or implicit support" for the violence have generated millions of views, with hundreds of thousands of users 'liking' and sharing the content. According to Robert Pape, a University of Chicago professor who studies political violence, this most recent incident is just the latest underscoring what he calls the "normalization" of political violence in the U.S. Pape claims that other instances of high profile political violence that have evoked a polarized reaction from the general populace include the "insurrection at the Capitol on Jan. 6, 2021; the assault of former House Speaker Nancy Pelosi's husband, Paul Pelosi, in 2022; and a pair of assassination attempts on former President Donald Trump during the 2024 presidential campaign."

SECURITY & SAFETY AWARENESS

Beware Of Credit Card 'Skimming Devices At Gas Pump
The Mining Journal, 12/3/2024

[New York] With the holiday travel season at hand, state officials are recommending ways to avoid having unnecessary pain at the pumps. While gas prices are generally down across the U.S., scammers

have developed the means to still make filling up a more costly experience down the road. Consumers, drivers and visitors are advised to stay alert for potential credit card "skimming," where criminals use hidden devices inside fuel pump card readers to steal credit and debit card information, according to the Michigan Department of Agriculture and Rural Development, or MDARD. … Simple steps to protect yourself from card skimmers include — Choose the pump nearest the cashier. Criminals are less likely to install skimmers near a staff member; Inspect the card reader for tampering. Look for loose or discolored panels, exposed wires or unusual scuff marks-these could signal the presence of a skimmer; ≤ Always select the "credit" option when paying. This avoids entering a PIN that could be stolen by a skimmer. Instead, only a zip code will be needed, which is safer; Monitor bank accounts while traveling to catch fraudulent activity. https://www.miningjournal.net/opinion/editorial/2024/12/beware-of-credit-card-skimming-devices-at-gas-pump/

ANALYST COMMENTARY: On 6 December 2024 the U.S. Attorney's Office for the Middle District of Florida announced that a 29-year old man from Miami, Florida had pled guilty to conspiracy, wire fraud, and aggravated identity theft for his role in a series of crimes stemming from placing credit card skimmers on fuel pumps. According to prosecutors, the man and his co-conspirators placed credit card skimmers on fuel pumps at gas stations to obtain credit and debit card account numbers used to purchase fuel at the compromised pumps, then made counterfeit credit and debit cards with the stolen numbers. They then distributed the cards amongst each other and purchased large amounts of fuel at gas stations around Florida, which they would pump into vehicles containing large internal fuel bladders, then leave the scene and deposit the fuel into a 9,500 gallon fuel truck. Once the fuel truck was full, they would sell the stolen fuel, that had been paid for with stolen credit cards, back to a gas station associated with one of the co-conspirators. This marks the second co-conspirator in the scheme to plead guilty, and three others are still awaiting trial. To recognize fuel skimming devices at fuel pumps, it is important to check tamper seals and make sure the credit card reader housing on the pump matches others before inserting any form of payment. Most gas stations will have tamper tape and safety seals across dispenser doors to protect against internal skimming devices. Do not use a pump if the tape or seal has been broken, and do not use a pump if the credit card reader housing is loose or appears to vary in design from other pumps at the same station. More information on fuel theft, vehicles used to steal fuel, and fuel skimmers and how to recognize them can be found at: https://www.tdlr.texas.gov/fcic/pdf/Current%20TX%20Trends%20Fuel%20Theft%20and%20Skimming.pdf

TriMet Awards Contract To STV To Enhance Safety And Security
Mass Transit Magazine, 12/12/2024

[Oregon] STV has entered into two new contracts with TriMet. The agency selected STV to enhance safety and security throughout its transit network by developing an operations plan for its new Security Operations Center (SOC); and separately, STV will help expand TriMet's cloud-based transit signal priority (TSP) system, a tool that prioritizes buses and light rail vehicles at traffic signals to improve

traffic flow and transit on-time performance. STV is creating a concept of operations, a dynamic framework for how the security center functions within TriMet's entire system. As part of the concept of operations, STV is helping TriMet integrate the new incident management software with the agency's overall operations. "We're thrilled to build on our decade-long partnership with TriMet as the agency expands both its security operations and a future system-wide, next generation TSP," said STV Western Director of Mobility Technologies Adrian Pearmine. "Our local team's deep understanding of TriMet's transit system, coupled with our expertise with security and advanced transit technology, will help create more safe, efficient and reliable transit options for riders." https://www.masstransitmag.com/safety-security/press-release/55249201/stv-group-inc-trimet-contracts-stv-to-enhance-safety-and-security

Denver Police Fight Crime With New Parking Lot Lighting Rules
CBS, 12/12/2024

[Denver, Colorado] Denver has always required that public parking lots have "proper illumination." However, until now, there was no clear guidance on what that meant. On Wednesday, the city released new guidance to help reduce auto thefts, break-ins, and crime in the parking lots. The goal is to make the community safer. For nine months, police studied crime patterns in parking lots and garages across downtown Denver, finding more than 700 thefts. While the number was higher in previous years, authorities said addressing the issue now is critical. "Lighting is the number one way to reduce crime," said Kayla Knabe, a community resource officer with the Denver Police Department. Knabe explained that requiring proper lighting in public parking lots is part of a strategy called Crime Prevention Through Environmental Design. … "Crime of opportunity often occurs in dark areas, so it's important to illuminate these spaces." The city's new guidelines for proper illumination include the use of security lighting, prohibition of glare, and the implementation of full cutoff lighting fixtures. Parking lot owners will now be required to upgrade their lighting when renewing their operating licenses.
https://www.cbsnews.com/colorado/news/denver-police-fight-crime-new-parking-lot-lighting-rules/

Billie Davis Receives 6-Year Sentence For Stabbing IU Student In Hate Crime
Indiana Public Media, 12/10/2024

[Indiana] Billie Davis, 57, of Bloomington was sentenced to six years in prison and three years of probation for stabbing an Indiana University student. Judge Tanya Walton Pratt sentenced Davis on Wednesday in federal court in Indianapolis. Davis pleaded guilty to attacking the victim, then 18, because of her Chinese descent, which is a federal hate crime. The crime happened Jan. 11, 2023. The student was seen on surveillance standing to exit a Bloomington Transit bus when Davis, who was sitting behind her, stabbed her seven to 10 times in the head with a folding knife. Davis and the victim did not know each other and did not speak to each other before the attack. The victim survived her injuries, which required sutures and staples. According to an FBI press release, Davis described the victim to police as "some Asian" followed by profanity. She said she attacked the victim because she was of

Chinese descent and so there was "one less enemy." https://indianapublicmedia.org/news/billie-davis-receives-6-year-sentence-for-stabbing-iu-student.php

The Era of Supply Chain Spy Wars Is Here
Foreign Policy, 12/10/2024

The sabotage this year of Hezbollah's communications devices, apparently by Israel, was undoubtedly spectacular, but, as a matter of espionage, it was anything but new. Intelligence agencies have long targeted and exploited supply chains both for intelligence and sabotage purposes. From the 20th century Cold War to today's geopolitical clash with Russia and China, infiltrating supply chains has always offered the opportunity to acquire valuable information about an adversary, or to disrupt critical sectors of its economy. Western officials are now busily assessing their own strategic and tactical supply chain vulnerabilities. Hardly a D.C. conference goes by without mention of the CHIPS Act and semiconductor supply chains. The United States is funneling billions of dollars towards the development of ecosystems for high tech manufacturing and critical materials processing to support microelectronics both domestically (e.g., Intel in Arizona) and in partner countries (Mexico, the Philippines, and others). https://foreignpolicy.com/2024/12/10/the-era-of-supply-chain-spy-wars-is-here/

CYBERSECURITY

"aiocpa" Python Package Exposed as Cryptocurrency Infostealer
HackRead, 12/5/2024

The machine learning-based threat-hunting system of leading threat intelligence and cybersecurity firm ReversingLabs (RL) recently detected malicious code in a legitimate-looking package, "aiocpa." According to RL's investigation, shared with Hackread.com, this package was designed to compromise cryptocurrency wallets. Through differential analysis of two package versions, RL was able to determine how these attackers carried out their distinctive campaign. The package, a synchronous and asynchronous Crypto Pay API client, has been downloaded 12,100 times. While probing, researchers identified what makes this campaign unique. Unlike most attacks targeting open-source repositories like npm and PyPI, in this campaign, the threat actors published their own crypto client tool to gradually build trust with a growing user base. Then, they struck. An apparently harmless update to the aiocpa package (version 0.1.13 and later) injected malicious code. https://hackread.com/aiocpa-python-package-cryptocurrency-infostealer/

ANALYST COMMENTARY: The discovery of malicious code in the "aiocpa" Python package shows the evolution of supply chain attacks targeting open-source ecosystems like PyPI. Threat actors behind this campaign deviated from common tactics; instead of injecting malware into popular, existing packages, they created their own tool to build credibility over time before injecting malicious code. The attack leveraged obfuscation techniques and targeted sensitive cryptocurrency wallet data, demonstrating

how open-source repositories remain vulnerable despite traditional application security measures. The malicious update, undetectable by conventional AST tools due to its absence from the referenced GitHub repository, the limits of surface-level code reviews and the critical need for advanced behavioral analysis tools like ReversingLabs' Spectra Assure. This incident also highlights the broader risks of package name takeovers, where attackers exploit the dependency on familiar or abandoned projects to inject malicious updates. Such tactics make it imperative for developers to pin dependencies, use hash-based verification, and regularly review third-party code. The attack emphasizes the importance of proactive threat-hunting systems powered by machine learning, which can analyze patterns and behaviors in ways that surpass traditional methods. With over 12,000 downloads, the scale of potential impact demonstrates why securing the software supply chain must be a priority for both developers and the platforms hosting these packages.