Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

December 24, 2024

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Man Charged After Bus Roof Torn Off In Crash
BBC, 12/23/2024

[United Kingdom] A man has been charged after a double decker bus crashed into a railway bridge and had its roof torn off. Police confirmed a 34-year-old had been charged with a road traffic offence following the incident in Kilmarnock which involved a Stagecoach bus. Emergency services were called to Culzean Cresent in the town at about 13:55 on The Stagecoach bus was heading to Bellfield in Kilmarnock when it travelled under the bridge at Macphail Drive. The roof of the bus was completely torn off and remained behind while the vehicle passed through the tunnel. A Stagecoach West Scotland said investigations into the crash were ongoing and the bus company was working closely with police. The latest smash came after after a double-decker bus crashed into a railway bridge in Glasgow on Saturday 14 December. https://www.bbc.com/news/articles/cm2evrlj08ro

Cook County Men Arrested After Allegedly Assaulting, Robbing Man On CTA Train
FOX 32, 12/23/2024

[Chicago, Illinois] Two Cook County men were arrested Sunday after allegedly assaulting and robbing a man on a CTA train. Claude Elder, 44, of Chicago, faces one felony count of aggravated robbery, indicating that he was armed with a firearm and one felony count of aggravated battery to a transit employee. Christopher Owens, 19, of Lansing, faces the same charges. The charges stem from an incident around 8 a.m. Sunday when the two men allegedly beat and stole belongings from a 20-year-old man aboard a train in the 0-100 block of West Cermak. Officers located and arrested the men about 35 minutes later. https://www.fox32chicago.com/news/cook-county-men-charged-cta-train-robbery

TERRORISM & EXTREMISM

Germany: Man Arrested Over TikTok Christmas Market Threat
dw, 12/23/2024

[Germany] Police in the northern German port city of Bremerhaven arrested a man over an online threat to stab everyone with an "Arab or southern" appearance at the local Christmas market. The man was

released later on Monday after a psychiatric examination. A psychiatrist found the man did not pose a danger to others, broadcaster Radio Bremen reported. The arrest and release came after a man drove a car through the Christmas market in Magdeburg on Friday, killing five people. The individual in Bremerhaven, with long gray hair, a beard, and glasses, repeatedly says he will target people with Arab appearance and that he has nothing to lose. "I will go to the Christmas market here in Bremerhaven on the 25th and I'm going to stab anyone who looks Arab or southern — anyone. I'm taking enough knives with me." The man says it "must finally come to an end here in Germany." "This is no joke... I've got nothing to lose. I have no relatives. I am alone and I live alone. I could just as well be dead or in jail," the man says. https://www.dw.com/en/germany-man-arrested-over-tiktok-christmas-market-threat/a-71142398

Evaluating 'Transnationalism' as an Analytical Lens for Understanding REMVE Terrorism
Combatting Terrorism Center, 12/2024

This article explores the extent to which 'transnationalism' offers analysts a meaningful prism through which to analyze racially or ethnically motivated violent extremist (REMVE) terrorism or whether the term obscures more than it illuminates. The 'transnational' dimension of REMVE terrorism is often ill-defined and misunderstood, leading to misconceptions about the nature of such networks that in turn exaggerate their 'global' reach and distort our understanding of how they operate in practice. The digital revolution has internationalized far-right extremist networks, but many of these remain regional rather than truly transnational. Nevertheless, understanding the transnational dimension of social media and its role in the radicalization of lone-actor REMVE terrorists is increasingly important. Online REMVE communities rather than physical organizations per se serve as the medium through which violent ideologies are spread; where lessons from previous attacks are learned and internalized; where the perpetrators of violence are revered; and where further acts of violence are encouraged and incited—which, as this article demonstrates, has real-world effects. What this suggests is that, insofar as REMVE terrorism is concerned, 'domestic' terrorism is increasingly inseparable from tackling 'transnational' terrorism and that digital platforms have increasingly blurred the boundaries between the two. https://ctc.westpoint.edu/evaluating-transnationalism-as-an-analytical-lens-for-understanding-remve-terrorism/

ANALYST COMMENTARY: In 2021, the Office of the Director of National Intelligence (ODNI) produced a product titled "Domestic Violent Extremism (DVE) Poses Heightened Threat in 2021" in which the intelligence community (IC) assessed that "racially or ethnically motivated violent extremists (RMVEs) and militia violent extremists (MVEs) present the most lethal DVE threats with RMVEs most likely to conduct mass-casualty attacks against civilians and MVEs typically targeting law enforcement and government personnel and facilities" in the United States. While RMVEs are generally considered DVEs in the U.S. because the perpetrators target their fellow countrymen at venues within their shared homeland, some counterterrorism researchers have challenged the definition because it suggests the perpetrators do not have any kind of transnational nexus despite evidence suggesting that many RMVEs consume foreign RMVE media online, which has a hand radicalizing the perpetrators to

violence. Instead, researchers argue that some RMVEs are better described as homegrown violent extremists (HVEs), which differ from DVEs in that, according to DHS, DVEs are categorically "not inspired by and do not take direction from a foreign terrorist group or other foreign power" whereas HVEs are. Regardless of their inspiration, both HVEs and DVEs remain a persistent threat to the U.S., and while successful terrorist attacks within the U.S. are relatively few and far between, potential attackers are frequently thwarted by law enforcement. According to Anti-Defamation League (ADL), between 2021 and 2023, the ADL tracked "six Islamist-related terror incidents in the U.S., compared to 30 incidents with far-right perpetrators and five incidents with far-left or other perpetrators within that same timeframe." Oftentimes, law enforcement investigations into these potential attackers begin through suspicious activity reports provided by the public. For additional information on threat indicators and suspicious activity reporting, visit: https://www.dhs.gov/see-something-say-something.

SECURITY & SAFETY AWARENESS

Man Charged After Woman Lit On Fire, Killed On Subway In Brooklyn
PIX 11, 12/23/2024

[Brooklyn, New York] Police charged a man after a woman was lit on fire and burned to death on the subway in Brooklyn over the weekend. Sebastian Zapeta-Calil, 33, was charged on Monday with murder in the first and second degree and arson, police said. The NYPD is still working to identify the victim. She was burned so severely that she will likely be identified through dental records, according to authorities. The gruesome attack happened on an F train near the Coney Island-Stillwell Avenue subway station around 7:30 a.m. Sunday, police said. A man lit the sleeping woman's clothing on fire, according to the NYPD. The man then left the subway car when the train pulled into the station and sat on a platform bench nearby, watching the woman burn to death before leaving the station, according to authorities. Investigators don't believe there were any verbal exchanges or interactions before the attack. The crime was caught on surveillance camera, according to the MTA. https://pix11.com/news/local-news/man-charged-after-woman-lit-on-fire-killed-on-subway-in-brooklyn/

Push For Stronger Bus Shields Intensifies After Fatal Stabbing Of Metro Bus Driver Shawn Yim
KREM2, 12/23/2024

[Seattle, Washington] A retired King County Metro bus driver who was knocked unconscious in a 2010 attack is calling for better safety measures after the murder of operator Shawn Yim. … Yim died early Wednesday morning after a passenger stabbed him in Seattle's University District. The suspect in the stabbing Richard Sitzlack, was arrested early Saturday morning. Police said the public should not approach Sitzlack if spotted, as he is considered armed and dangerous. … "Metro is the employer. It's no different than a parent taking care of their children. The transit operators are Metro's responsibility to make safe. When you're a parent, you don't necessarily need their opinion. You need to know they're

safe. You do whatever it takes to make them safe," she said. Specifically, Batey has been pushing for stronger, more secure shields between drivers and passengers. "The shop threw some shields together, put them on the buses and took a survey of all the drivers to see what they felt about it and they said the drivers voted it down. Metro said they didn't want to give a bad impression making people think the buses aren't safe. Well, when the drivers aren't safe, nobody is safe," said Batey. https://www.krem.com/article/news/local/retired-bus-driver-assaulted-in-2010-pushes-for-safety-upgrades-after-murderf-shawn-yim/281-4a3da266-2f02-4be6-9d7c-d54133a4d352

ANALYST COMMENTARY: Nationally, the rate of reported "major assaults" against transit workers more than quadrupled between 2011 and 2023, reaching a 15-year high, according to an Associated Press analysis of Federal Transit Administration (FTA) data. Surveys suggest fear of on-the-job violence contributes to operator shortages. In addition to passing new laws, deploying additional security personnel, implementing stiffer penalties for attacks against transit employees, revising fare enforcement policies and procedures, and providing de-escalation training to frontline personnel, many agencies are installing various physical barriers to protect drivers. However, implementation can be costly; existing bus designs can prevent the installation of complete operator compartments, and many partial shields offer minimal protection. Some drivers oppose their implementation as well. The increase in assaults prompted the FTA to issue "General Directive 24-1" in September 2024, requiring every transit agency subject to their Public Transportation Agency Safety Plans (PTASP) to conduct a risk assessment on its transit vehicles and stations and issue a detailed "data-driven" report on how they're monitoring and mitigating those risks. Responses are due by December 26, 2024. For more information on General Directive 24-1, visit: https://www.transit.dot.gov/assaults. The PTASP Technical Assistance Center (TAC) is also available at https://www.transit.dot.gov/PTASP-TAC.

MTA To Order 80 More 'Open Gangway' Subway Cars, Plans To Deploy Some On G Train
Gothamist, 12/15/2024

[New York] The MTA plans to order dozens more "open gangway" subway cars and redeploy some of the airy cars the agency already owns to the G line, transit officials announced Monday. The modern cars do not have doors between them, offering riders roomier commutes as they can walk freely throughout their trains. The MTA last year received its initial purchase of 20 of the cars — enough for two 10-car trains — and rolled them out on the C line. On Wednesday, the agency's board is set to approve the purchase of 80 more of the open gangway models as part of a larger $1.3 billion order of 435 new train cars that are scheduled to be delivered by 2028, officials said. And early next year, 10 of the door-less cars currently running on the C line will be moved over to the G train. That's enough to cover two trains on the Crosstown Line, which uses shorter, five-car sets. "It's going to be 'OG' on the G: open gangway on the G train," MTA Chair Janno Lieber told reporters Monday. The redeployment of open gangway cars to the G train will still leave enough to run a single 10-car door-less train on the C line. https://gothamist.com/news/mta-to-order-80-more-open-gangway-subway-cars-plans-to-deploy-some-on-g-train

Intel Officials Warned Police That US Cities Aren't Ready for Hostile Drones
Wired, 12/17/2024

The Department of Homeland Security issued warnings to state and local law enforcement agencies this summer regarding the "growing illicit use" of commercial drones, internal documents show. Among the recommended steps was to conduct "exercises to test and prepare response capabilities." A DHS memo from August, which has not been previously reported, paints US cities as woefully underprepared for the "rising" threat of weaponized drones. The capabilities of unmanned aircraft systems (UAS) are "progressing faster" than available countermeasures offered under "federal prevention frameworks," the memo says, adding that it's common for state and local authorities to observe "nefarious" and "noncompliant" flights but still lack the authority to intervene. The memo states that violent extremists in the US are increasingly searching for ways to modify "off-the-shelf" drones to ferry dangerous payloads, including "explosives, conductive materials, and chemicals," with major advancements in the area being propelled largely by rampant experimentation on foreign battlefields, including those in Ukraine. https://www.wired.com/story/intel-officials-police-us-cities-drones-dhs/

Feature Article: Bomb Technicians Train On Trains
Department of Homeland Security, 12/12/2024

[Philadelphia, Pennsylvania] Philadelphia, Pennsylvania, will host several high profile and heavily attended events in the next few years, including the International Federation of Football Association World Cup soccer games, the Homecoming 250 Navy and Marine Corps celebration, and the U.S. Semiquincentennial commemorating the 250th anniversary of the signing of the Declaration of Independence. … As part of the preparations for these events, the Protective Security Advisor for the Southeast Pennsylvania District invited the Science and Technology Directorate's (S&T) Response and Defeat Operations Support (REDOPS) program to assist with their response planning. REDOPS conducted joint exercises in the Philadelphia area earlier this year with the Southeastern Pennsylvania Transportation Agency (SEPTA) Transit Police, and the Philadelphia (PA) State, and Montgomery County (PA) bomb squads, to ensure regional response agencies are ready for any possible scenarios. The exercises focused on two different events: a bomb threat underground in the mass transit system and a bomb threat at a power generation or distribution point. https://www.dhs.gov/science-and-technology/news/2024/12/12/feature-article-bomb-technicians-train-trains

CYBERSECURITY

Investigation Underway After Pittsburgh Regional Transit Alerts Riders Of Cybersecurity Incident
4WTAE, 12/23/2024

Pittsburgh Regional Transit is alerting riders after a ransomware attack was detected Thursday. In a statement Monday, PRT said an investigation has been launched to determine if any information has

been compromised. "Upon discovering the incident, PRT immediately launched an investigation, activated its Cyber Incident Response Team, notified law enforcement, and engaged nationally recognized third-party cybersecurity and data forensics experts," the statement said. PRT said rail service experienced temporary disruptions Thursday morning due to the issue, but transit services are currently operating as normal. Some rider services, however, have remained negatively impacted, according to the statement. https://www.wtae.com/article/pittsburgh-regional-transit-alerts-cybersecurity-attack/63268341

ANALYST COMMENTARY: On 23 December 2024 a Pittsburgh Regional Transit (PRT) spokesperson disclosed that the PRT discovered that they had been targeted by a cyber attack on 19 December 2024. The PRT spokesperson claimed that following the detection of the attack, "PRT immediately launched an investigation, activated its Cyber Incident Response Team, notified law enforcement and engaged nationally recognized third-party cybersecurity and data forensics experts." The full scope of the attack remains unclear; however, the agency has claimed that the attack appeared primarily "to affect communications in our light-rail center for a couple of hours" on 19 December which "briefly disrupted dispatchers from tracking vehicles on its light-rail line." The PRT spokesperson "declined to elaborate and wouldn't comment on what hackers accessed, whether they demanded a ransom or what data they might have taken." Despite the attack, transit services are operating normally. Transportation organizations are increasingly targeted by cyber threat actors and make attractive targets because of the frequent exchange of financial information that occurs over their ticketing systems and the amount of personal data they store. Some also have an increased number of attack surfaces as they undergo digital transformations and adopt new systems while phasing old systems out. More information regarding cyber attack trends impacting the transportation sector can be found at: https://cloudsecurityalliance.org/blog/2024/12/17/threats-in-transit-cyberattacks-disrupting-the-transportation-industry

New Glutton Malware Exploits Popular PHP Frameworks Like Laravel and ThinkPHP
Hacker News, 12/16/2024

Cybersecurity researchers have discovered a new PHP-based backdoor called Glutton that has been put to use in cyber attacks targeting China, the United States, Cambodia, Pakistan, and South Africa. QiAnXin XLab, which discovered the malicious activity in late April 2024, attributed the previously unknown malware with moderate confidence to the prolific Chinese nation-state group tracked Winnti (aka APT41). "Interestingly, our investigation revealed that Glutton's creators deliberately targeted systems within the cybercrime market," the company said. "By poisoning operations, they aimed to turn the tools of cybercriminals against them – a classic 'no honor among thieves' scenario." Glutton is designed to harvest sensitive system information, drop an ELF backdoor component, and perform code injection against popular PHP frameworks like Baota (BT), ThinkPHP, Yii, and Laravel. The ELF malware also shares "near-complete similarity" with a known Winnti tool referred to as PWNLNX.
https://thehackernews.com/2024/12/new-glutton-malware-exploits-popular.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ANALYST COMMENTARY: The emergence of the Glutton backdoor reflects a fascinating, albeit concerning, evolution in cyber tactics. The malware's dual-purpose design—targeting both traditional victims and cybercriminals—highlights an escalating trend in adversarial adaptation within the cybercrime ecosystem. This self-cannibalizing strategy not only disrupts the tools of competing threat actors but also amplifies the overall threat landscape by repurposing compromised resources. The use of PHP-based frameworks like Baota, ThinkPHP, Yii, and Laravel as attack vectors indicates a growing focus on exploiting widely used development platforms, emphasizing the need for robust patching and code hygiene in software supply chains. The lack of obfuscation and encrypted communications in Glutton may initially appear as a vulnerability for defenders to exploit. However, this "unpolished" approach could serve as a smokescreen, lowering the profile of the attack and disguising its affiliation with highly sophisticated groups like Winnti. This aligns with broader tactics seen in nation-state campaigns, where different operational layers are used to test new tools without jeopardizing primary assets. Organizations should prioritize monitoring for anomalous PHP process activity and implement strict access controls, particularly around internet-exposed systems running PHP frameworks. The recursive use of cybercriminal resources against their operators, combined with tools like HackBrowserData, signifies that even malicious actors are not immune to supply chain risks. Defenders must adopt similar recursive thinking, leveraging adversary TTPs (Tactics, Techniques, and Procedures) to form proactive defenses. Sharing insights across security communities about modular malware trends like Glutton can be pivotal in mitigating future campaigns.