



Physical & Cyber Security Intelligence & Information Threat Report

Issue – November , 2022

I. Cyber

U.S. watchdog seeks cybersecurity strategy for offshore energy infrastructure¹

A U.S. watchdog in a report made public on Thursday asked the federal regulator of offshore oil and gas infrastructure to come up with a cybersecurity strategy for the more than 1,600 facilities under its oversight. The Government Accountability Office (GAO) report highlighted that offshore facilities increasingly use technology to remotely monitor and control equipment, making them vulnerable to cyberattacks and risking environmental harm and supply disruptions. A successful cyberattack could wreak damage resembling the effects of 2010 Deepwater Horizon disaster, the report said. The report mentioned China, Russia and Iran among actors that may pose significant threats.

Microsoft: Hackers Are Using This ‘Concerning’ Tactic to Dodge Multi-Factor Authentication²

“Microsoft says token theft attacks are on the rise. Here's what you need to do to protect yourself. Microsoft has outlined several mitigations to protect against attacks on multi-factor authentication that will unfortunately make life more difficult for your remote workers. Three years ago, attacks on multi-factor authentication (MFA) were so rare that Microsoft didn't have decent statistics on them, largely because few organizations had enabled MFA. But with MFA use rising as attacks on passwords become more common, Microsoft has seen an increase in attackers using token theft in their attempts to sidestep MFA. In these attacks, the attacker compromises a token issued to someone who's already completed MFA and replays that token to gain access from a different device. Tokens are central to OAuth 2.0 identity platforms, including Azure Active Directory (AD), which aim to make authentication simpler and faster for users, but in a way that's still resilient to password attacks.”

II. Threat Reporting

Domestic Threat Reporting

¹ <https://www.reuters.com/business/energy/us-watchdog-seeks-cybersecurity-strategy-offshore-energy-infrastructure-2022-11-17/>

² <https://www.zdnet.com/article/microsoft-hackers-are-using-this-concerning-tactic-to-dodge-multi-factor-authentication/>



Insider threats accounted for more than a third of unauthorized access incidents in Q3³

The pandemic saw a great number of employees seeking new opportunities as the workforce shifted to remote and hybrid models. The threat of insider risk, however, also increased along with the so-called “Great Resignation” of 2021 and 2022.

According to a report by security risk management firm Kroll, insider threats peaked to its highest quarterly level to date in Q3 of 2022, accounting for nearly 35% of all unauthorized access threat incidents.

International Threat Reporting

'Close call' in shelling near nuclear reactor on Ukraine's frontline⁴

Ukraine narrowly escaped disaster during fighting at the weekend that rocked Europe's largest atomic power plant with a barrage of shells, some falling near reactors and damaging a radioactive waste storage building, the U.N. nuclear watchdog said.

Canada police charge Hydro-Quebec employee with China espionage⁵

The Royal Canadian Mounted Police (RCMP) arrested Yuesheng Wang, 35, on Monday and charged him with espionage.

Mr Wang "obtained trade secrets to benefit the People's Republic of China, to the detriment of Canada's economic interests," police said in a statement.

He will appear in court in Longueuil, Quebec, on Tuesday to face four criminal charges.

The resident of Candiac, a suburb south of Montreal, is accused of obtaining trade secrets, unauthorised use of a computer, breach of trust by a public officer and fraud for obtaining trade secrets.

Philly AntiCapitalist Blog Posts Unverified Claim of Blockading a 'High Frequency Railway' with Purported Intent of Inspiring “Many More and Frequent Blockades”⁶

AAR has been notified of a railway blockade claim posted this afternoon in a ‘Solidarity Action Communique’ on the Philly Anti-Capitalist blog – a self-proclaimed anarchist website.

³ <https://www.scmagazine.com/news/insider-threat/insider-threats-accounted-for-more-than-a-third-of-unauthorized-access-incidents-in-q3>

⁴ <https://www.reuters.com/world/europe/playing-with-fire-un-warns-team-inspect-damage-ukraine-nuclear-plant-2022-11-21/>

⁵ <https://www.bbc.com/news/world-us-canada-63631933>

⁶ Railway Alert Network (RAN) Notification – November 18, 2022



An anonymous source submits that a “small group” reportedly blockaded a railway “chokepoint”, allegedly leaving materials on an unidentified rail line with the purported intent of inspiring “many more and frequent railway blockades”.

The act was reportedly conducted to demonstrate “solidarity” against drilling in the “Wet’suwet’en...Wedzin Kwa” region and to oppose “colonial capitalist development and infrastructure across all Turtle Island and the World!”

The validity or reliability of this claim is not yet established; available incident reporting within the past few weeks does not indicate railroads have discovered materials on the tracks or impeded rail operations.

That said, there is seeming alignment in the claim on Philly Anti-Capitalist and recently posted protest activity earlier on November 4, 2022 on the New Westminster subdivision in British Columbia, Canada.

- A post online depicted a video of approximately three to four protesters under a pop-up tent at the side of a rail crossing holding a sign that stated “#KilltheDrill”.
- The post also stated “Come out and find us just off Renfrew Skytrain station. We're shutting Canada down. This is not a drill.”
- No reported trespass on rail property nor disruptions to rail traffic occurred in the area cited.

Both reference drilling, maintained a purported small number of participants, and touted the statement to “Shut down Canada”. That said, no direct linkage between the two events has been made.