Physical & Cyber Security Intelligence & Information Threat Report

Issue – October 18, 2022

I. *Cyber*

US Airports in Cyberattack Crosshairs for Pro-Russian Group Killnet[1]

Killnet calls on other groups to launch similar attacks against US civilian infrastructure, including marine terminals and logistics facilities, weather monitoring centers, and healthcare systems. Hot on the heels of attacks against US state government websites, pro-Russian threat group Killnet on Monday disrupted the websites of multiple US airports in a series of distributed denial-of-service (DDoS) attacks. It also called on similarly aligned groups and individuals to carry out DDoS attacks on other US infrastructure targets, in what appears to be an escalation of a recent campaign protesting the US government's support for Ukraine in its war with Russia. Airport websites that were affected by Killnet's DDoS attacks included Los Angeles International Airport (LAX), Chicago O'Hare, Hartsfield-Jackson Atlanta International Airport, and the Indianapolis International Airport. While the DDoS attacks made some of the sites inaccessible for several hours, they do not appear to have had any impact on airport operations.

As Ransomware Attacks Increase, New Algorithm May Help Prevent Power Blackouts[2]

Millions of people could suddenly lose electricity if a ransomware attack just slightly tweaked energy flow onto the U.S. power grid. No single power utility company has enough resources to protect the entire grid, but maybe all 3,000 of the grid's utilities could fill in the most crucial security gaps if there were a map showing where to prioritize their security investments. Purdue University researchers have developed an algorithm to create that map. Using this tool, regulatory authorities or cyber insurance companies could establish a framework that guides the security investments of power utility companies to parts of the grid at greatest risk of causing a blackout if hacked.

[1] https://www.darkreading.com/attacks-breaches/us-airports-cyberattack-crosshairs-pro-russian-group-killnet

[2] As ransomware attacks increase, new algorithm may help prevent power blackouts - Elmore Family School of Electrical and Computer Engineering - Purdue University

II. *Threat Reporting*

Domestic Threat Reporting

Terrorgram Collective Publications Focus on Sabotaging Critical Infrastructure

The Terrorgram Collective, an alias used by a transnational network including racially or ethnically motivated violent extremists (RMVEs), on July 14 released a 261-page publication titled The Hard Reset on Telegram that promotes accelerationism and contains information on attacking critical infrastructure along with suggestions for other targets and attack methods. The Hard Reset encourages RMVEs and antigovernment or antiauthority violent extremists (AGAAVEs) to take violent action against the US and other governments that the authors argue are facilitating the replacement of the white race in the US with nonwhite minority groups. Structured similarly to some earlier Terrorgram releases—as well as Make It Count, an associated publication released in June on Telegram —The Hard Reset includes short passages promoting the ideological motivations of RMVE actors worldwide, how-to chapters for waging terror attacks, and corresponding stylized graphics. The publication's content also similarly contains a large subsection aiming to inspire and provide guidance—which NCTC assesses to be of widely varying detail, accuracy, and potential impact—on attacks and sabotage across multiple categories of critical infrastructure, including:

- Highlighting power grids as attractive targets, suggests using power tools, arson, and explosives to destroy transformers and substations, and advocates finding substations by using publicly available indexed maps and Google Street View.

- Advising how to locate, shoot, burn, or collapse 5G-capable telecommunications towers, encouraging saboteurs to destroy guyline tension cables stabilizing cell towers by cutting them with cordless grinders or placing thermite charges at their base, and providing advice on attacking fiber-optic cable networks, junction boxes, servers, and satellite dishes.

- Encouraging readers to target water processing and distribution infrastructure through arson, noting that chlorine used in the water treatment process can cause intense and uncontrollable fires, and encouraging research to find and sabotage "choke points within grids" by using fires, gunfire, explosives, electrical shorts, or thermite, citing civilian deaths from "bad water" in the Bosnian War as an example. The publication provides several detailed diagrams of water treatment facilities, including a named sanitary district in Ohio.

- Encouraging followers to attack the food and agriculture sector, including farms, ranches, and restaurants, and describing tactics to contaminate farmland with salt; destroy crops by releasing wild boars into the fields, driving vehicles through fields, or use machinery to rip up crops; burn fertilizer plants or barns or plant explosives at grain silos. The publication also advocates attacks that contaminate food at restaurants, or making false claims of poor food quality at restaurants and food delivery services to cause economic damage.

- Recommending sabotaging roads, bridges, and highways by dropping nails or motor oil onto them; compromising them with sledgehammers, power tools, or explosives; and targeting bridge tension cables and stabilizing brackets with thermite. In addition, the publication recommends disrupting freight routes by damaging freight-capable trucks, especially those displaying nonwhite religious or cultural symbols on their exterior, and calling in threats to depots on major retail holidays.

- Offering detailed instructions and guidance on planning, preparing, and executing attacks against railroad infrastructure, augmented by graphic illustrations depicting the steps necessary to implement the recommended tactics, including using derailing devices, smashing junction boxes, melting tracks with thermite, tampering with brakes, and removing rail components.

- Recommending targeting commercial facilities, including warehouses, retail establishments, banks and "degenerate" small businesses, and offering methods for sabotage, including instructions for making effective Molotov cocktails. The publication defines degenerate businesses as LGBTQ+ bars, strip clubs, and nightclubs, and specifically calls on attackers to sabotage natural gas lines or HVAC systems commonly used in commercial facilities to cause explosions.

- Advocating attacks against "race traitors," Jews, abortion clinics, an identified US billionaire, and government officials, including "cops" (for protecting females and minorities), a named US government official, and an identified foreign leader, among others.

- In addition, the publication contains numerous articles on constructing bombs, including one called "Fumigate the Cities," which contains an alleged dirty-bomb recipe. The article instructs readers to purchase uranium ore online and "with basic precautions and proper [personal protective equipment], you could easily incorporate a radiological payload into a conventional bomb or incendiary device." Such devices are unlikely to cause illness because uranium ore is only harmful if ingested or inhaled in large quantities and is not radioactive enough to cause a health hazard.

International Threat Reporting

Europe ramps up energy security after suspected sabotage[3]

European companies are ramping up security around pipelines and energy prices are climbing again as the suspected sabotage of two pipelines that deliver natural gas from Russia underscored the vulnerability of Europe's energy infrastructure and prompted the EU to warn of possible retaliation.

Some European officials and energy experts have said Russia is likely to blame for any sabotage — it directly benefits from higher energy prices and economic anxiety across Europe — although others cautioned against pointing fingers until investigators are able to determine what happened.

[3] https://madison.com/news/national/govt-and-politics/europe-ramps-up-energy-security-after-suspected-sabotage/article_449dc650-7965-53b6-b3b1-978f769466c0.html