Ground Truth: Coordinated Cyber Attacks

The New Independence Group

Attack Type

Three-pronged custom cyber-attack consisting of 1) ransomware against Critical National Infrastructure (CNI) digital assets in the transportation and energy sectors, 2) mass spearphishing disinformation campaign against electricity customers to simultaneously increase electricity usage and surge the Eastern Interconnection electricity grid leading to blackouts, and 3) a Telephony Denial of Service (TDoS) attack against emergency services to cause havoc after the blackouts and initial disruption. Despite Christmas Day being one of the most electricity-intensive days in the calendar, the syndicate opted to act in summer to coincide with increased temperatures and exploit the high demand air cooling systems put on the grid. As with the years preceding it, a dangerous heatwave lingered across America that summer.

Actors and Background

Although the actors themselves claim no name, the media has labelled them the 'New Independence Group' – a radical group of eco-activists with formidable technology skills. Led by their founder, Julia, a veteran of the US Army, the sixteen person strong syndicate work in secret, and contribute to their mission of brining the US fossil fuel industry to a halt. Despite the electricity grid being the primary target – which consists of some renewable sources – their aim is to try and reset the whole energy industry and infrastructure. By hitting the electricity grid, cascading consequences would occur and disrupt all other CNI sectors. The Eastern Interconnection electricity grid is targeted as this would see the greatest impact due to the greater population density compared to the rest of America.

Overall Impact and Outcome

In the aftermath of the event, investigators found that in the first 72 hours alone, the coordinated attack directly resulted in 562 preventable deaths from heat-related illness due to electrical cooling capabilities being impaired. The majority of these were elderly or vulnerable members of society. 38 people were killed by private security or armed vigilantes for attempting to sabotage or steal from private property. 70 people died in total across seven hospitals due to a lack of critical medical resources including refrigerated medicine, defibrillators, and not staff being unable to access vitally needed digital patient records. 126 people lost their lives in traffic incidents in the minutes following the attacks, 57 of which were onboard a train that derailed due to the signal system - which was impacted by the ransomware - showing falsely safe signals.

Political Impacts

Aside from the political embarrassment of suffering such a catastrophic cyber incident, local and federal government agencies are left in disarray as they scramble to understand the extent of the impact, get critical services back online, and to find those responsible. Due to the aggressors of this incident not wanting fame, believing it would distract from the movement, the US Government and its intelligence/law enforcement agencies have to consider hostile foreign state's as the threat actors. This worsens extant geopolitical tensions as a blame game begins before official attribution. US signals intelligence finds that foreign adversaries are seeking to exploit the situation America finds

itself in by acting on goals in their geographic spheres of interest. They know the US cannot respond quickly, or at least gain much public support for foreign operations until the situation at home is resolved.

Economic Impacts

The economic impact of the coordinated cyberattack is astronomical. Businesses, houses, and public services such as hospitals cannot operate as usual unless they have emergency backup power capabilities such as diesel generators. Imports and exports on the eastern seaboard are halted causing supply chain disruptions both domestically and internationally. Cascading consequences are seen throughout the country including most refrigerated food stocks and prescription drugs being thrown away as refrigerators are down. If the electricity outage lasts more than a week, there are fears of bacterial infections spreading through overcrowded commercial aviaries containing turkeys and chickens as standard antibiotic supplies become held up in the logistical backlog. The financial market is suspended but only after the economic uncertainty caused stock prices to plummet. The revenue lost from no trading will impact businesses for years to come. Some companies hit by the ransomware try paying the ransom in a desperate attempt to regain access to their data and systems, but the decryption keys never arrive.

Social Impacts

Over 180 million people are left without power for at least 5 days amidst a record-breaking heatwave. This causes panic and looting of shops for essential resources. Minority groups seize the opportunity to loot non-essential goods and vandalise cities. Crime rates of all types soar, especially given the disruption in policing abilities and mistrust over 911 calls' authenticity. Those with generators become attractive targets for those desperate for electricity. The combination of ransomware on the transport networks and key strategic fuel providers means that energy supplies for local generators will not last long amid the chaos. Many State Governors deploy the Army National Guard to maintain law and order. Armed militias take to the streets adding to the chaos. A backlog of several months accumulates for medical appointments. All commercial flights East of the Rocky Mountains are suspended due to cascading safety and communication technology issues.

Technological Impacts

Once power is attained again, the computer systems impacted with ransomware still remain unusable until backups are loaded. Severe and long lasting reputational damage occurs for companies impacted and without strong business continuity plans. There is widespread mistrust for AI usage after this incident, meaning other countries overtake America in the AI development race and opportunities to use AI for good are forgone.

Environmental Impacts

The sudden uptake in fossil fuel powered generators causes temporary and localised spikes in pollution. Some sewerage treatment plants are accidentally hit by the ransomware worm and leads to unsafe sewerage discharge into public waterways. Other extreme eco-activists seize the opportunity to add to the chaos by physically damaging poorly secured energy generation and transmission infrastructure. This prolongs recovery. Some of these sabotage attempts are met with armed force from vigilantes and private security trying to defend private property.