# Acronyms

|  |  |
| --- | --- |
| ILA | Independent Lone Actor |
| HR | Human Resources |
| TOO | Target of Opportunity  Engage as available, not all TOO targets need to be hit. |
| Eng (Abbr.) | Engineering |
| DMZ | Demilitarized Zone |
| Infra (Abbr.) | Infrastructure |
| DMZ | Demilitarized Zone |
| FTP | File Transfer Protocol |

# Day 2 – Independent Lone Actor

COA: Delete/destroy software from systems associated with mission critical systems to disrupt operations.

Motivation: ILA was fired from the co-op for cause, after multiple warnings about performance, harassment, and aggressive behavior.

Storyline: The ILA holds power utilities as key contributors to the issue of climate change/global warming. It is unlikely that this ideology was held by the ILA at the time of initial employment, instead having developed at some point during his employment. His contempt for power utilities is shared publicly via social media platforms such as X/Twitter and Facebook, where he interacts with a small community of activists who advocate for varying degrees of action. His grievances were exacerbated by his first formal write-up, which he felt was retaliatory, further justifying his perceived grievance. Subsequent write-ups led to further grievance and rumination, escalating the situation and progressing the stairway of violence.

Recently the ILAs social media accounts have been more active, posting original content and reposting content from other activists, advocating for activity in protest to a new natural gas plant in Chesterfield, Virginia. (Maybe add a second site in for the Finns)

Shortly after the above activities, the ILA got into heated argument with a co-worker at the co-op regarding the impact of natural gas power generation. The encounter escalated and was reported to HR, resulting in the termination of the employee. He was notified of his termination at the start of business this morning. He was told to return to his workstation and pack his belongings.

Specific Targets for Consideration:

* User-workstation06 🡨 Priority Target
  + Supports storyline. This is the workstation of the user he got in an argument with.
* Dmz-Web-Elcoop-1 🡨 Priority Target
  + Supports storyline. Consistent with ideologies.
* Dmz-dns-elcoop01 🡨 Priority Target
  + High-impact target.
* Infra-dc1 🡨 Priority Target
* Infra-file 🡨 TOO
* Eng-workstation01,02,04,06 🡨 TOO
* HR-workstation01,02,03,05,06,07,08 🡨 TOO
* User-workstation,02,030,04,05,06,07,08,09 🡨 TOO
* It-workstation01,02,03,04,05,07,08 🡨 TOO
* Fin-workstation01,02,03,04,05,06,07 🡨 TOO
* Dmz-ftp-elcoop01 🡨 TOO
  + Medium impact target
* Entire 10.0.5.0/24 subnet (rnd) 🡨 TOO
  + Medium to high impact target.

## Extra Scenario Information:

This scenario is different from the others, in that the state sponsor of the activity is not actually directly connected to the activity which disrupts the power cooperative.

The ILA is influenced by an Iranian IO operation. The IO campaign is a part of Iran’s strategic operations to decrease Western involvement in the Israel-Palestine conflict, maintain regional influence, and support Hamas in their attacks against Israel.

The operations used accomplish this this strategic goal are: Sponsoring Houthi attacks against maritime operations to increase frequency, sustained cyber warfare operations against U.S. aligned middle eastern countries and Europe, and a unique activity group specifically cyber operations against Israeli critical infrastructure in support of Hamas.

The IO campaign targeting the U.S. leveraged climate change caused by non-nuclear power generation, and the safety and environmental risks of nuclear power. The ILA established a connection with this campaign and was inadvertently influenced.

Aggravating factors in his life include: Getting written up on several occasions in the last year, financial hardship, no clear or evident support system or social circle outside of limited online engagement, working for an ‘environmentally oppressive system’ that he no longer believed in, and finally termination, resulting in his final escalation to violence.

The U.S. intelligence community has not predicted that U.S. critical infrastructure is likely to be attacked at the time of the scenario start; however, this is not because it is unlikely – this is a simulated failure in intelligence. Blue intel analysts should be able to find this was highly likely/almost certain, based on past incidents.

Past Incidents:

Iran campaign in other occurrences appeared to target financial institutions, power grid, transportation systems, and water/wastewater systems of other countries. This would be done using disruptive attacks and hack & leak attacks in the case of Israel. Activity in Germany and the United Kingdom would indicate that a U.S. attack is extremely likely, combined with one previous incidents from the Cyber Av3ngers, showing a demonstrated interest in attacking the west.

NOTES:

1. How do we make sure that forensics is possible? Maybe red team has a logic bomb that doesn’t go off.
2. Johns is working on alternative IO models for the Iran IO campaign.