Cyber Operations Analysis and Research Group
Risk and Infrastructure Science Center
Global Security Science Division

Argonne NATIONAL LABORATORY

CYBER REPORTING TREND ANALYSIS TOOL

Cyber Incident Report Trending

SUMMARY

Owners and operators report cyber risk information to the US Government via multiple sources. This includes US-CERT reporting, ICS-CERT reporting, and reporting through I&A. The mixture of these self-reported datasets contain a mixture of data elements and at times duplicate reported incidents.

Last year, Argonne National Laboratory's Cyber Operations Analysis and Research team created a disparate database structure and tool that ingested these datasets on a quarterly basis, and merged them on common fields to produce a simple filterable report.

Data was initially tracked with the following fields: Sector, Sub-Sector, Category of Incident, Sub-Category, Access Vector, Asset, Sub-Asset, Actor, Intent, and if the attack was successful.

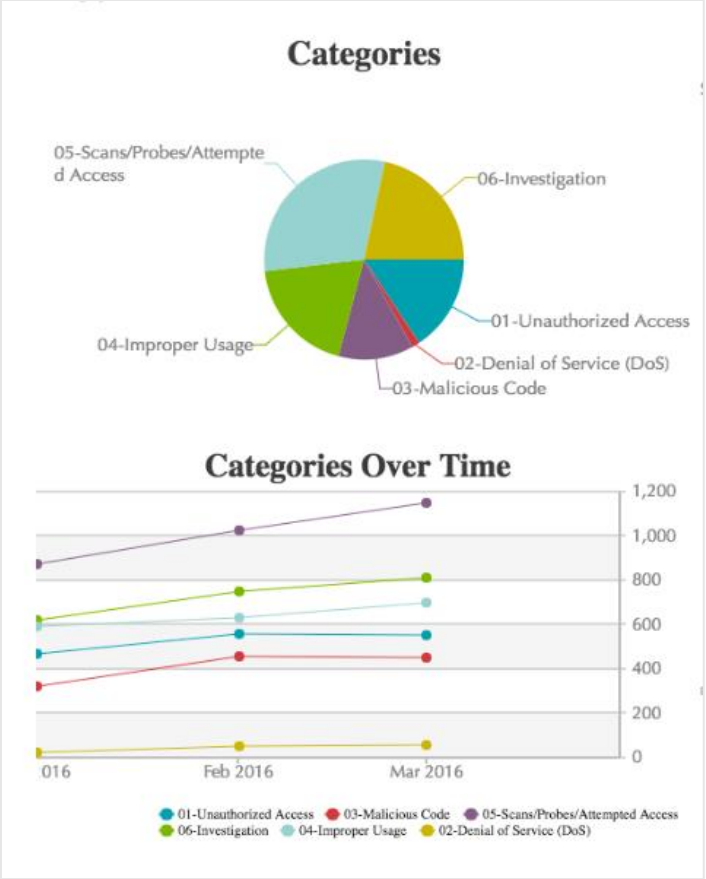
Argonne would like to continue this work; ingesting more data feeds including potential real-time feeds like US-CERT's Einstein or the Cyber Federated Model. Argonne looks to spend additional time to build a reporting engine in order to add a historical element to this tracking would be valuable for analysts looking at self-reported incidents.

LONG TERM GOAL

The ability to perform trend analysis and real-time incident tracking of critical infrastructure across the Nation as they report it to the US Government would allow for timely analysis of impacts.

PROPOSED DELIVERABLES

- Task Option 1: Update the tool and add in more data on a quarterly basis from ICS-CERT, US CERT and I&A. Produce more reports allowing for historical searching.
- Task Option 2: Add in an ability to ingest data feeds in real-time including ICS-CERT, US CERT and I&A as well as potential new real time data feeds from Einstein or the Cyber Federated Model.
- Task Option 3: Automate reporting engine to alert on specific critical infrastructure sectors, producing regular automated reports
- Task Option 4: Create a mapping element to regionalize incidents based on the data in the database



Trend Chart Reporting

incident identification incident_id	affiliation affiliation
INC000010045908	Federal Government
INC000010045909	Federal Government
INC000010045910	Federal Government
INC000010045911	Federal Government
INC000010045912	Federal Government
INC000010045913	Federal Government
INC000010045915	Federal Government

Report Filtering

THE UNIVERSITY OF CHICAGO
U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.

Contact: Nathaniel Evans
Phone: 630-252-3733
Email: nevans@anl.gov
https://coar.risc.anl.gov