



Automated Threat Information Generation

August 2022

Changing the World's Energy Future

Taylor Wayne McCampbell



INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Automated Threat Information Generation

Taylor Wayne McCampbell

August 2022

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

<http://www.inl.gov>

**Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517**

Automated Threat Information Generation



College of Engineering
and Applied Science
Computer Science

Taylor McCampbell | CEDAR Lab, University of Wyoming | Mentors: Rita Foster, Zach Priest, Rafer Cooley

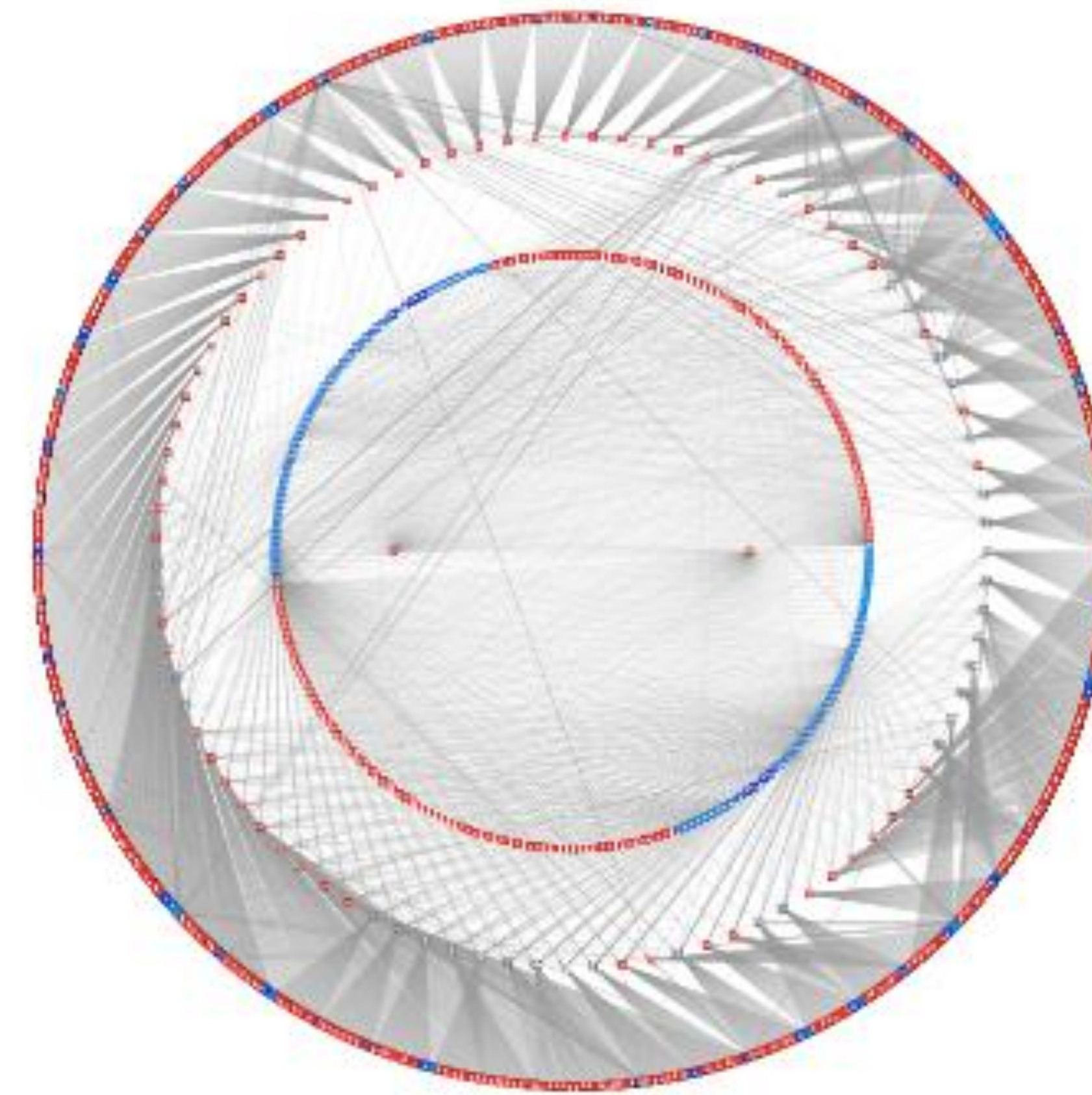


Introduction

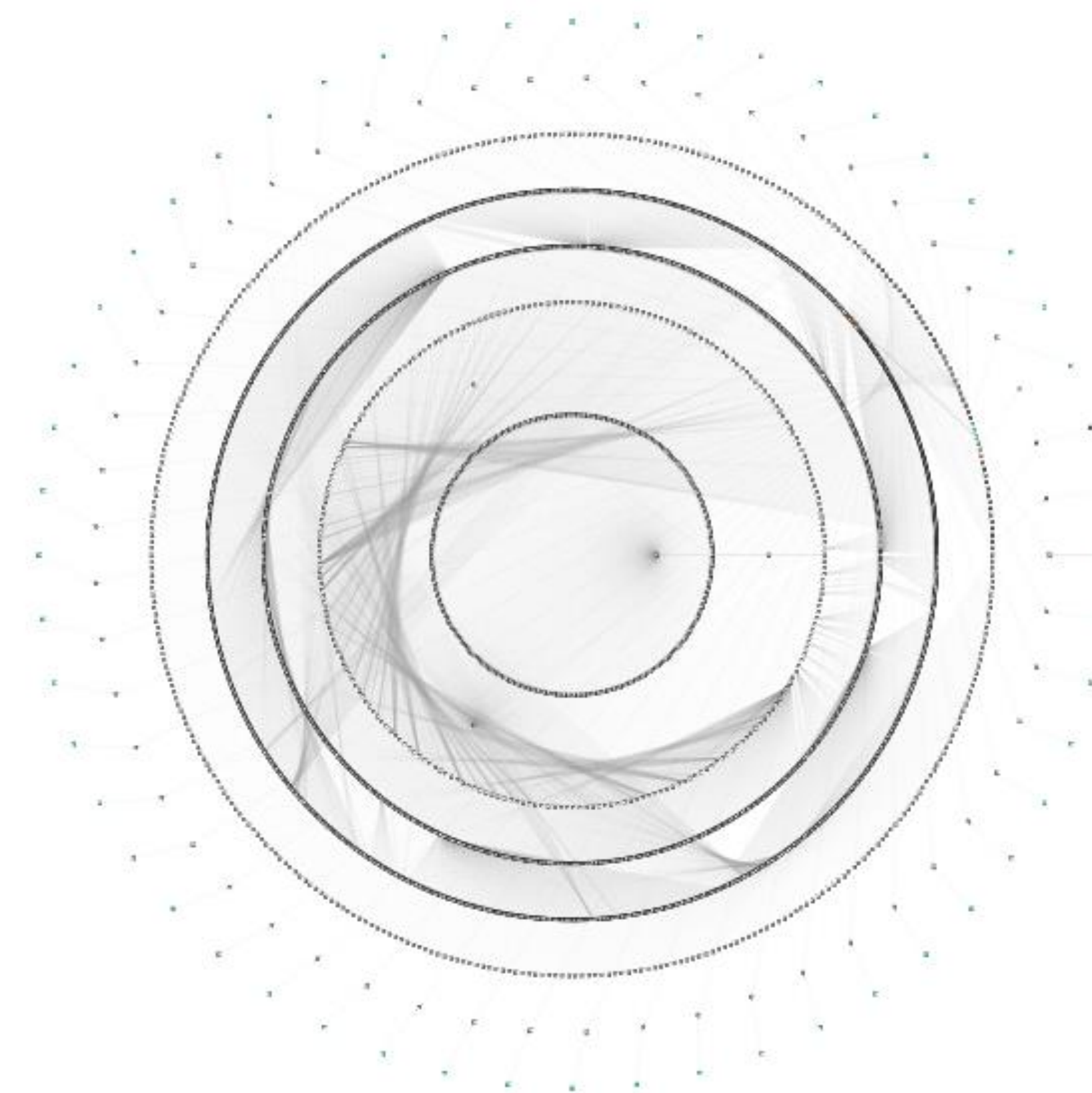
- Harvesting threat information manually is time consuming
- With hundreds of thousands of new malware samples being up uploaded to malware repositories every day, there is no way to manually stay up to date with emerging trends
- Automated threat information generation combats this problem by quickly analyzing, translating, and expressing threat intelligence in a computer readable, standardized language

Why Should You Care?

- Good data allows us to facilitate future research
- Automated data collection allows many different avenues for analysis which can help us better understand emerging trends, malware behavior, and our own security posture
- Automation allows us to gather data quickly so that we always have the most current dataset
- The quicker the response time and implementation of preventative measures, the more systems that are protected



ATIS Auto-Generated STIX based on VirusTotal Darkside Malware Report



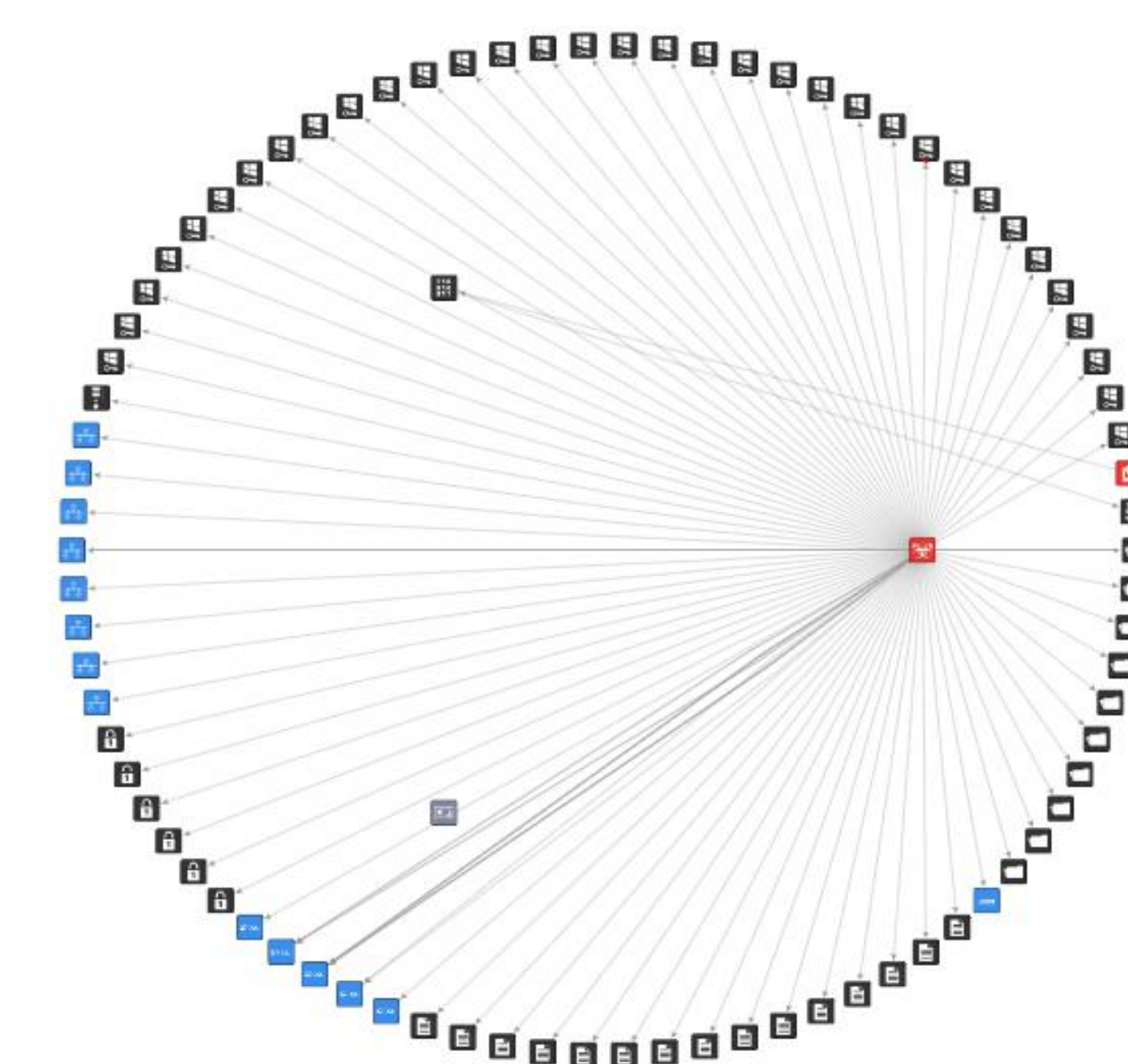
Autodiscover IX Toolset Auto-Generated STIX based on Odroid Board Scan

Contributions

- Use cases and development for the Autodiscover Infrastructure eXpression (IX) toolset
- Data analysis for the Cape2STIX toolset supporting Automated Malware Analysis (AMA) LDRD
- Creation and development of the Automated Threat Intelligence to STIX (ATIS) Software gathering from VirusTotal and Malware Bazaar supporting Deep Learning Malware.

Impacts

- Increased vendor security posture
- Detected trends in malware sample data
- ATIS framework allows for top level analysis and a quick understanding of new or specific samples



Cape2STIX Auto-Generated STIX based on PE Malware Sample

