INL/EXT-21-63816-Revision-0

STIG_EKANS

December 2022

Tarek Mohamed Elagaty

Changing the World's Energy Future

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.

INL/EXT-21-63816-Revision-0

STIG_EKANS

Tarek Mohamed Elagaty

December 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

Using Structured Threat Intelligence Graph (STIG) to protect our critical infrastructure against cyber attacks

Idaho State University

Intro about STIG and its uses with STIX

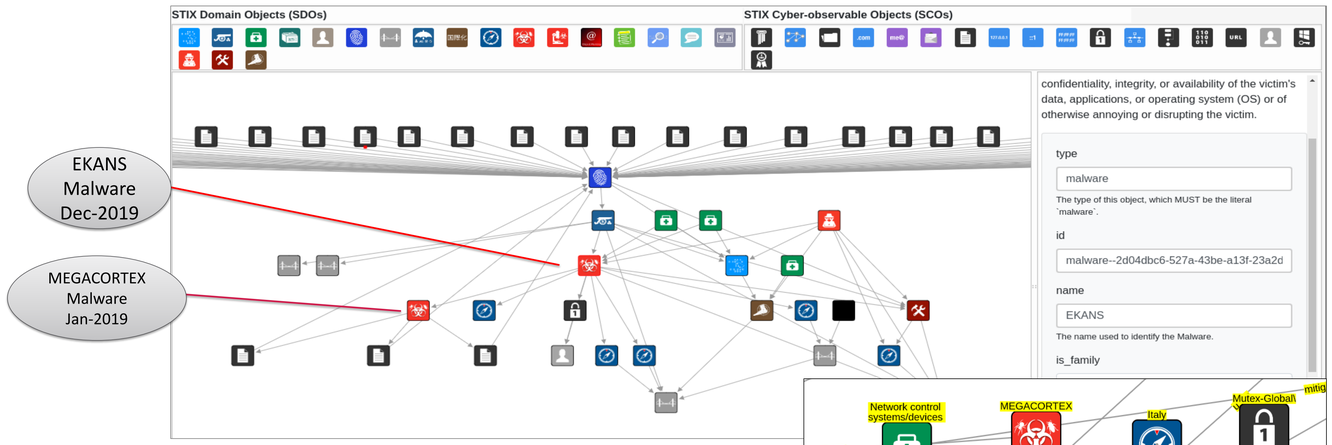
- STIG, is a revolutionary cybersecurity tool developed by researchers at the U.S. Department of Energy's Idaho National Laboratory and it is a software that allows utility owners and operators to easily visualize, share, create, and edit cyberthreat intelligence information.
- STIG uses Structured Threat Information eXpression (STIX) and converts complex data on cybersecurity vulnerabilities into a visualization that is easy to understand and act on.
- With STIG, utility owners and operators have a common system for sharing threat intelligence information, thus increasing the chances of detecting and mitigating cyber exploits before they lead to a cyberattack.

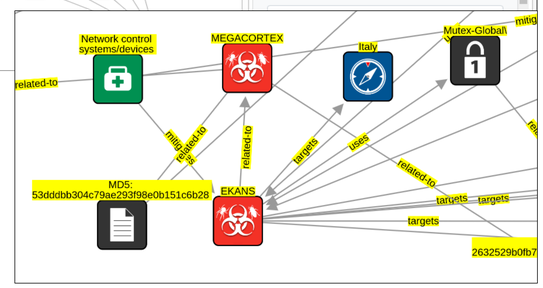
OrientDB

OrientDB

OrientDB was selected to be used with STIX because of its great features. OrientDB is an open-source Multi-Model NoSQL DBMS with the support of Native Graphs, Documents Full-Text, Reactivity, Geo-Spatial and Object-Oriented concepts. It's written in Java and it's amazingly fast: it can store 220,000 records per second on common hardware.

Using STIG to analyze EKANS ransomware





EKANS ransomware analysis (December 2019)

- EKANS ransomware is written in **Golang** and includes a static "kill list" that will stop numerous antivirus and Industrial Control Systems (ICS) processes and services. One way to identify an EKANS infection is by looking for the hexadecimal string of EKANS at the end of the file, which is added by the ransomware.
- Malware objects are compared as for **EKANS** has the following characteristics:
  File Name: update.exe
  MD5: 3d1cc4ef33bad0e39c757fce317ef82a
  SHA1: f34e4b7080aa2ee5cfee2dac38ec0c306203b4ac
  SHA256: e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60
- **MEGACORTEX** sample that also references ICS processes has the following characteristics:
  MD5: 53dddbb304c79ae293f98e0b151c6b28
  SHA1: 2632529b0fb7ed46461c406f733c047a6cd4c591
  SHA256: 873aa376573288fcf56711b5689f9d2cf457b76bbc93d4e40ef9d7a27b7be466
- **STIG** helped us to determine that EKANS represents an obfuscated, hardened ransomware variant based on prior MEGACORTEX activity. Both Malwares have some similarities as they both target ICS- related processes with Process kill activity similar to each other plus their hashes have some in common

- In the graph above, is shows us how we could relate more than one malware with others. In this process, each malware observables are compared with others to determine how much they match in order to identify the attacker & patterns in order to implement the appropriate mitigations.
- **STIG** helps create or find relations between the information related to threats such as code source, language used & country.

- All these data gets saved in a database for future references and could be possibly shared with others to help them detect threats and protect their properties from cyber attacks.

Tarek Elagaty
Mentors: Rita Foster & Zachary Priest
www.inl.gov

Idaho National Laboratory