SAND2016-6651D

iSAFE
Interns for Security, Arms control and Force protection Engineering

# Network Forensic Analyzer

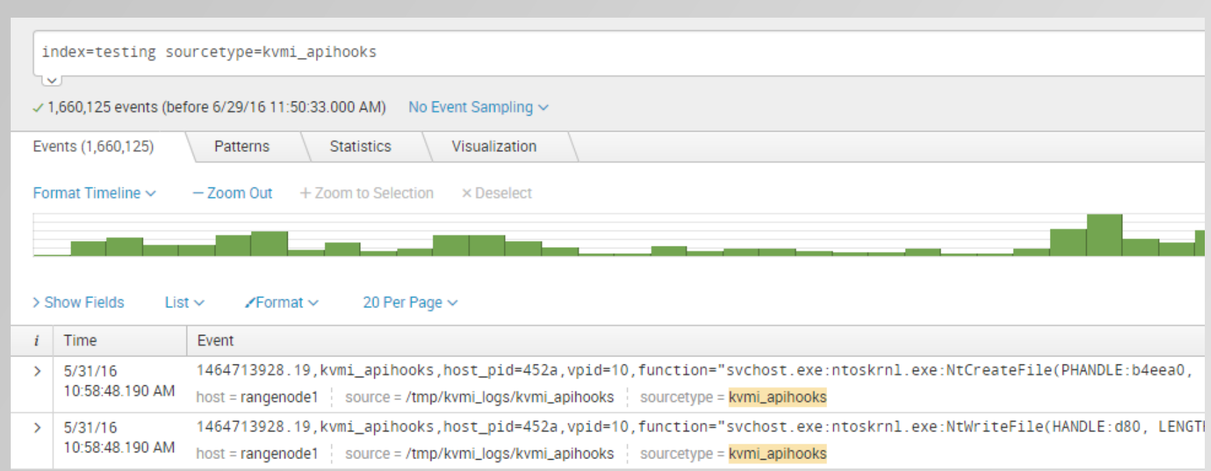
Manager:
Shawn Taylor
6613

Christopher Goes
University of Idaho
M.S Computer Science, May 2017

Project Mentors:
Vincent Urias, 9526
William Stout, 5629

**Currently, analysts reconstructing a network intrusion have to sift through millions of log events, taking even experienced analysts hours or days to fully understand an intrusion. This project will greatly simplify this process using a web-based visualization tool. It will allow analysts to quickly get a "big-picture" view of an intrusion, rapidly find events of note, and drill down into the details needed to respond or report.**

Deception Networks are virtualized environments designed to deceive an adversary into thinking they're undetected, while collecting detailed log data. This data includes SDN flows, firewall logs, and VM introspections. It is collected using Splunk, a robust log aggregator and parser.




Data is extracted from Splunk and fed into a data processor written in Python. The processor extracts key features from the data, cleans them, and hands them to the analyzer.

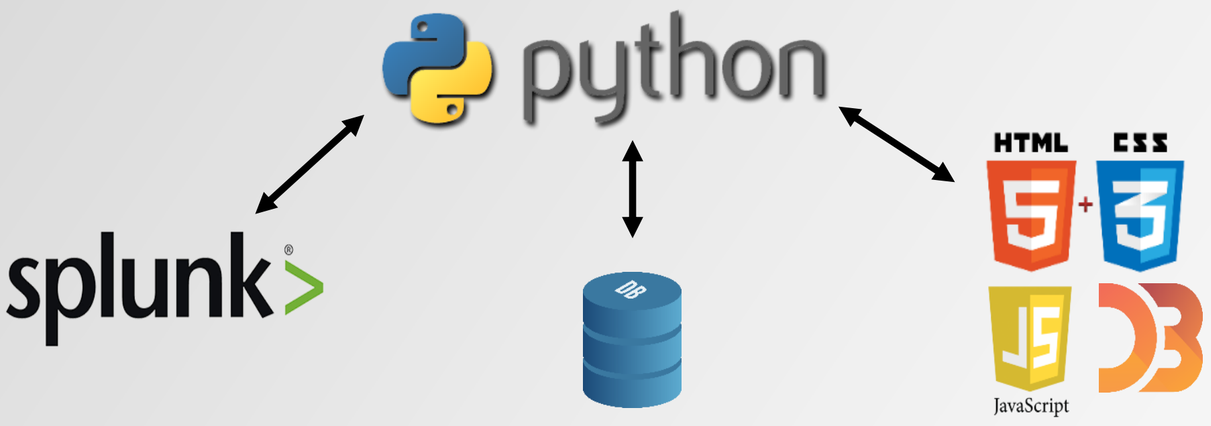
1464713812.27,kvmi_newproc,host_pid=3eee,vpid=4,eproc_hva=7fcf834f06a0,peb_hva=7fcf40ccf000,peb64=7fffffdf000,peb32=0,cr3=1068c8000,pid=b2c,wow64=0,name="bad.exe",user="unknown_user",commandline="bad.exe --do-evil 'evil IP'"

**Process "bad.exe"**
Exe: bad.exe
Args: "--do-evil", "evil IP"
User: unknown_user
Process ID: b2c

The analyzer determines if events are related using features such as:

- IP address
- process name
- filenames
- host
- username

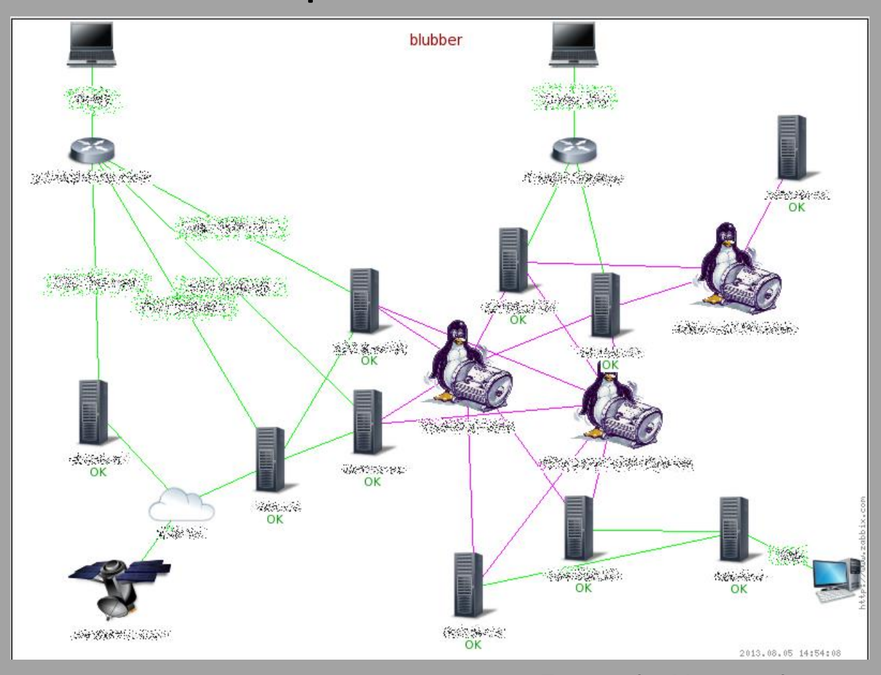
It then labels and inserts them into a database, used by a Python web server to serve display requests.




Navigation is performed in a web interface by clicking on these objects, which will display data objects related to the clicked object.

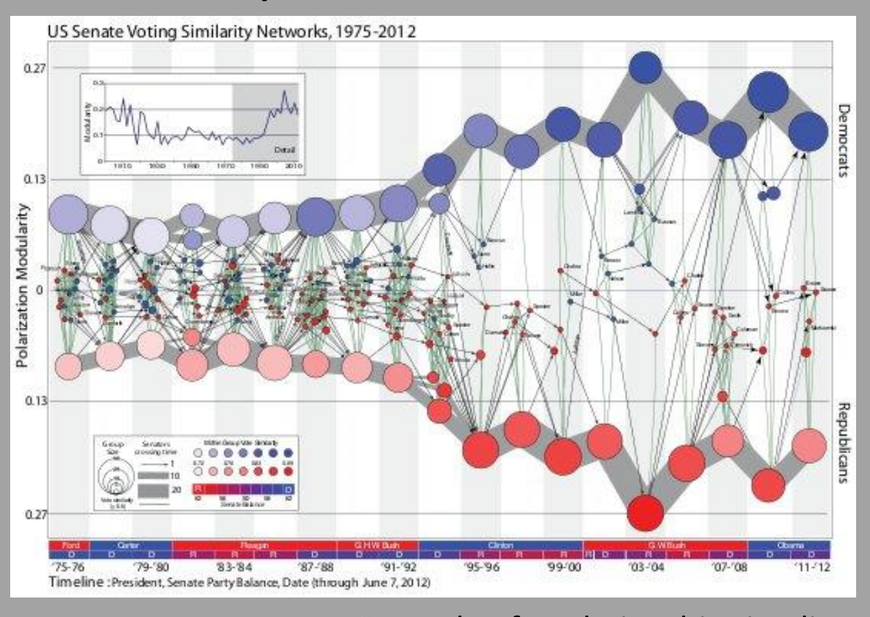
Data objects are displayed as:

1. Network map



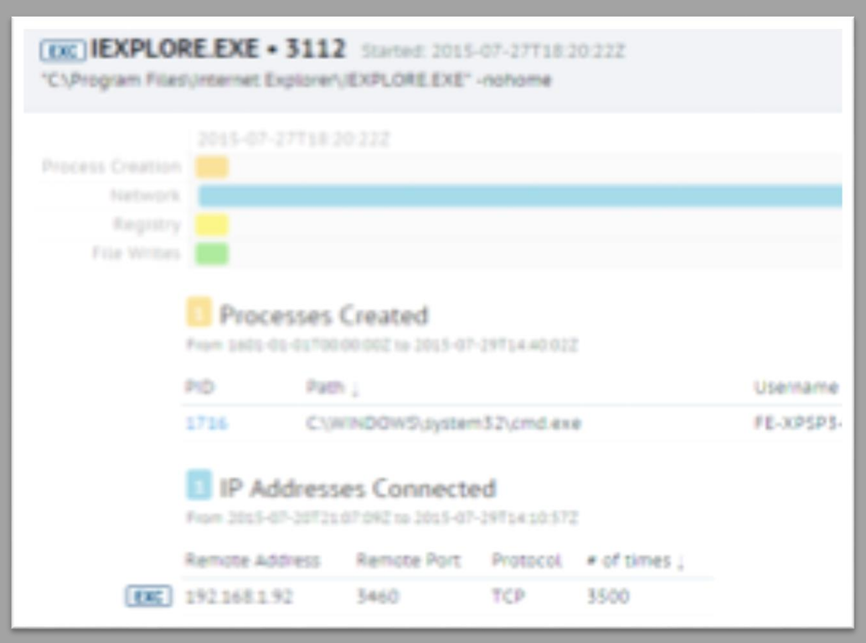

Example Network map

2. Relationship timeline of events




Example of a relationship timeline

3. Text buttons and lists




FireEye's HX Triage interface

Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

U.S. DEPARTMENT OF ENERGY