SAND2018-7461D

The Center for Cyber Defenders

Expanding computer security knowledge

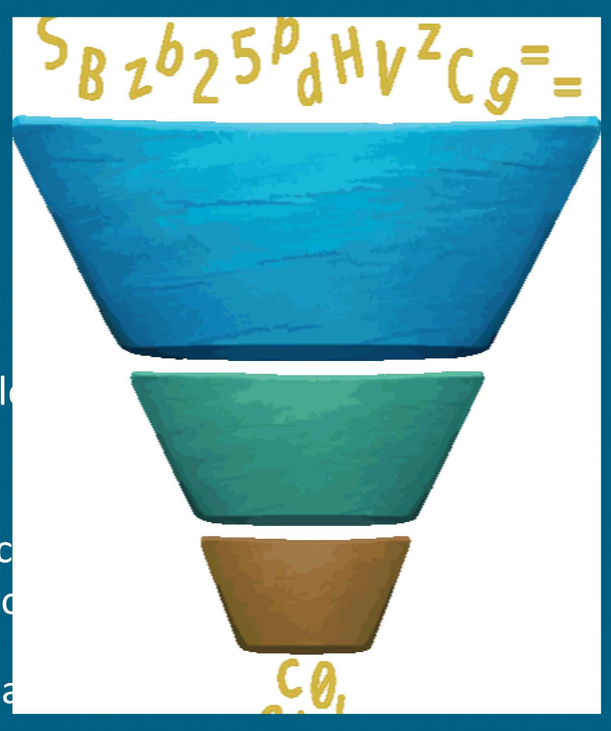
POSSE Mining

Preventing Outlawed and Surreptitious Sessions Engaged in Mining

Ken Goss

Jeremy Gin

- Problem Statement:
  - Cryptocurrency mining in enterprise networks generates potentially massive costs in resource use and infrastructure strain.
  - Benefits in payments are shunted off to corrupt individuals running miners.
  - Additionally, insecure mining scripts may increase the attack surface for other external adversarial threats.
  - Can also indicate that a compromise has already occurred



- Objectives and Approach:
  - Explore trends of mining activities through inspection of known mining network traffic records
  - Define static and dynamic criteria by which this type of traffic may be identified and filtered using Tamizar, diagrammed above
  - Study mining behaviors. These include unreferred DNS requests, unusual imbalances in data flow, uncommon specific TCP flagging, as well as a strong periodic flows.
  - Test static and dynamic criteria to validate efficacy in identifying mining traffic and ensure a low false positive rate for known mining traffic
  - Test on live enterprise network data streams to confirm results from static testing

- Results – Efficiency Tradeoffs
  - Static - A protocol level common byte signature was identified that occurs in all major messages for cryptocurrency mining, efficient but vulnerable to protocol alteration. This signature is, in hexadecimal format:

226D6574686F64223A20226D696E696E672E

  - If this byte string occurs in a payload, the Stratum mining protocol is being used. This is the sole protocol in heavy use currently.
  - Dynamic – Behaviors that indicate a high probability of mining traffic were discovered. An intersection of these individual criteria indicates a high probability of mining activity.
  - Specifically the individual indicators are, unreferred traffic with the TCP PSH flag set, more data leaving a client than arriving, and low standard deviation w.r.t. average packet interarrival times.
  - This is resilient against protocol change, but much more computationally expensive.

- Impact and Benefits:
  - The choice of the best criteria for a particular setting will ensure that no mining activities are sustainable, thus removing profitability for the miner, and incentive to mine.
  - The result is that the enterprise will save considerably in costs, and remain safe from more external threats.

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration