Bio-Inspired, host-based firewall

By: James Ballard, Kevin Hamilton, Jay Chow
Advisor: Dr Lanier Watkins
16th December 2019

Table of Contents

Introduction

- A firewall is security technology that deployed in networks, restricting network traffic between different segments in a network

- Creates a clear distinction between various divisions in an organization, separating trusted boundaries from untrusted boundaries (i.e DMZ and internet)

- Main functionalities include filtering data, redirecting traffic and protecting against network attacks such as DOS

Introduction(Cont'd)

- As networks attack have become more intricate, complex and sophisticated, firewalls are required to adapt to meet new challenges

- Our team focused on cell biology as there is a natural mapping between host-based firewalls and cell membranes; we wanted to push the firewall design in a new direction

- Biological-inspired cybersecurity is still in its infancy phase and there is more R&D that needs to be done at this stage

Introduction(Cont'd)

- Natural biological mechanisms that can be applied to increase the cybersecurity defense of a host-based system: endocytosis, active sites and ligand-gated channels for design inspiration

- Applied supervised and unsupervised machine learning algorithms to the brains of the classification engine

- Created a prototype, tested and evaluated our prototype on test data; solving this problem could scale massively in a distributed computing system

Look into modern firewalls

- Like many modern enterprise firewalls from Palo Alto and Fortinet , Cisco's Next-Generation Firewall is an application layer firewall that uses access control lists and Snort to inspect network traffic up to the application layer

- Capable of conducting real-time traffic analysis, packet logging on networks, performing protocol analysis, content searching and matching, detecting attacks and probes such as port scans, buffer overflows, CGI attacks, SMB probes and OS fingerprinting attempts

Look into modern firewalls(Cont'd)

- In Cisco's NGFW, snort can be used as a packet sniffer like tcpdump, a packet logger for network traffic debugging, and a network file logging device to capture files in real time from network traffic

- Cisco's NGFW could be managed on the same premise by Cisco Firepower Management Center or remotely by Cisco Cloud Defense Orchestrator

- Anomaly detection via machine learning is not primarily utilized due to high false positive rates that make the algorithms unreliable in real network environments

Problem Definition

- Signature-based firewalls have advantages such as the ability to map a specific threat to a malware signature, useful for threats that have seen before

- However, they struggle against zero-day attacks and encrypted traffic with TLS 1.3 being the most recent version of TLS now

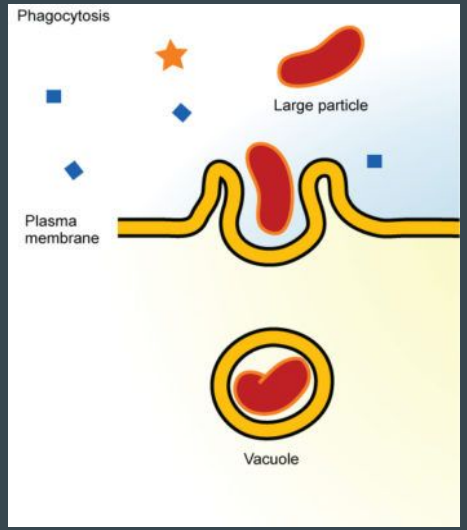
- We decided to make a system using biomimicry, the process of modeling a system off from biological entities

Project Scope

1) Our objective was to create a prototype firewall capable of giving a binary determination of benign or malicious network traffic after ingesting a certain number of TCP packets
2) Since creating a UI was out of the project's scope, the firewall must be started on the command line
3) We also performed analysis on TCP packets, not UDP packets
4) Firewall is only able to block IPs on linux machines

Endocytosis

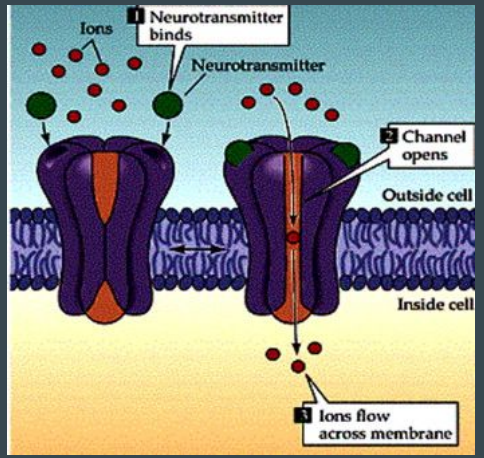
- Endocytosis is the process of actively transporting molecules into the cell by engulfing it with its membrane into a vacuole. [1]
- The immune system's purpose is to rid the body of any pathogens or foreign particulates that can cause disease. [1]



[2]

Ligand-Gated Ion Channels

- Ligand-gated ion channels are large receptors that form a membrane ion channel that, when open, allows the passage of certain molecules. [3]



[3]

Prototype Overview

Random Forest

- Derivative of the decision tree algorithm

$$entropy = - p_1 \log(p_1) - p_2 \log(p_2) - \cdots$$

- Functions well on a small amount of data
- Good with high dimensional datasets

K-Means Clustering

- Unsupervised learning that attempts to partition data into clusters
- Used as an additional feature for a Logistic regression model
- Can potentially help to mitigate our labeling issue

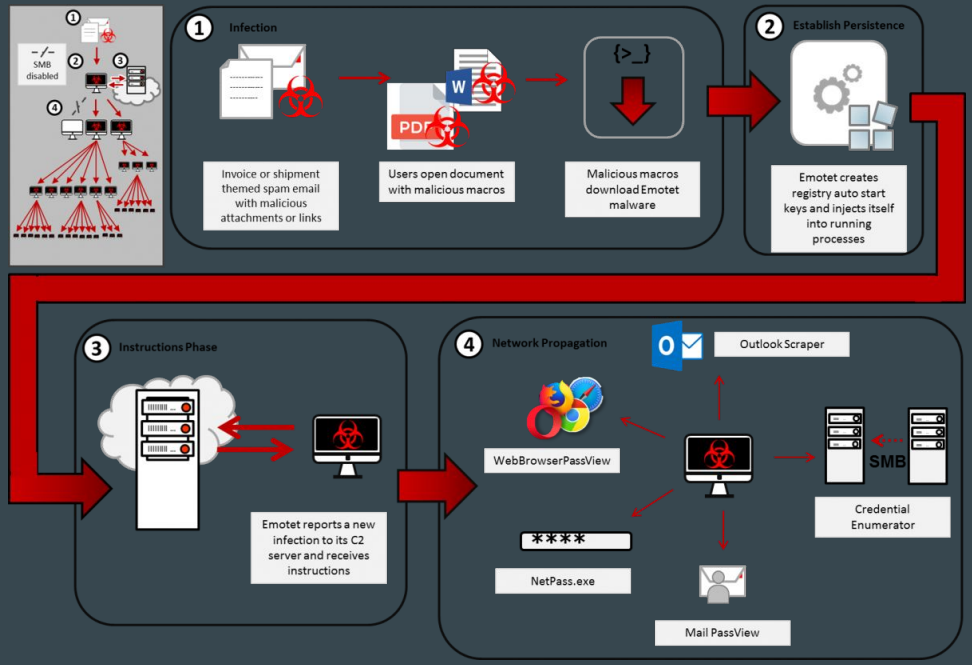
Gathering Data

- Lack of good publically available well-vetted datasets
  - KD99 is almost old enough to enroll in this program
- MalwareBytes
  - Source for all of the malware packet traces
- Stratosphere Labs
  - Czech cyber security firm with a large repository of network traffic

Malware Background

- Aside from ransomware banking trojans are one of the most costly forms of malware in recent history
    - Zeus, ZeusGameOver, ... etc
- Chosen because high impact and high popularity meant data availability
- A very jack-of-all-trades style of malware
- For the test set Emotet, Hancitor and, Trickbot were chosen

Malware Execution



Feature Selection and Extraction

- Three categories of features: Size, Timing, and TCP/IP
- Forward or Backward portion of the connection
- Various statistical transforms of the data ie std dev, mean, etc
    - 29 features in total

Prototype Design

- Ingress
  - Waiting until the amount of “activator sites” are full
- Extraction
  - Determine the “protein folds” of the subject connection
- Evaluation
  - Compare the “folding” to known sample and give a determination
- Action
  - Accept the protein if good and reject and block if malicious

Experimental Setup

- Completely fresh data from the same sources as the training data
- Also two additional captures were created:
  - Homemade network capture and CobaltStrike
- Using tcpreplay the pcap files can be replayed for the firewall operating on a host
- Log is kept tracking which connections, if any, are blocked
- Varied between the model and activator sites through the tests

Results

- For normal traffic this worked very well

Model	Receptors	Packet Capture	TPR	FPR	TNR	FNR	Malicious Connections
Supervised	10	Normal (4073 flows)		0.01%	99.99%		4
Unsupervised	20	Normal		0.00%	99.998%		1
Supervised	20	Homemade (183 Flows)	N/A		100.00%		0

Results cont.

- Struggled somewhat with identifying malicious connections

Model	Receptors	Packet Capture	TPR	FPR	TNR	FNR	Malicious Connections
Supervised	10	Attack (43 Flows)	50%	N/A	N/A	50%	23
Supervised	20	Attack	30.40%	N/A	N/A	69.60%	14

- But it is entirely likely that the detector is operating properly and the labeling scheme is misguided

Cobalt Strike

- Only notion for this data was that all of the HTTPS traffic contained was malicious
- Correctly identified 77% of malicious connections

Limitations

- Dataset
- Challenge of balancing biology with trying to create strong results
- Black box nature of algorithms used
- Only surveyed one algorithm in supervised and unsupervised learning

Conclusion

- Procured dataset
- Prototype firewall that can be retrained

Future Work

- Expand past a single cell model
- Add fuzzy logic model
- Add confidence interval or third class for greyware
- Quality of life fixes

Acknowledgements

- Kevin Klous, Cisco Systems
- Ayenson Mika, JHUAPL

Any Questions?

Thank you

References

[1] "*Endocytosis*". Accessed on: Nov. 24, 2019. [Online]. Available: https://biologydictionary.net/endocytosis/

[2] "*Cell Membranes*". Accessed on: Nov. 24, 2019. [Online]. Available: https://courses.lumenlearning.com/suny-wmopen-biology1/chapter/endocytosis-and-exocytosis/

[3] Pacheco, Mary A. "Receptor Types and Subtypes." pp. 1-5. 2017

[4] Ding, Lei "Data Science Basics and Decision Tree Models" Lecture. Johns Hopkins University September 16, 2019

[5]"Emotet Malware: CISA." Emotet Malware | CISA. Accessed December 15, 2019. https://www.us-cert.gov/ncas/alerts/TA18-201A.

[6] Garcia, Sebastian. Malware Capture Facility Project. Retrieved from https://stratosphereips.org