SAND2020-6431PE

# ADDSEC: IP Hopping

Adrian Chavez
Sandia National Laboratories

Artificial Diversity & Defense Security

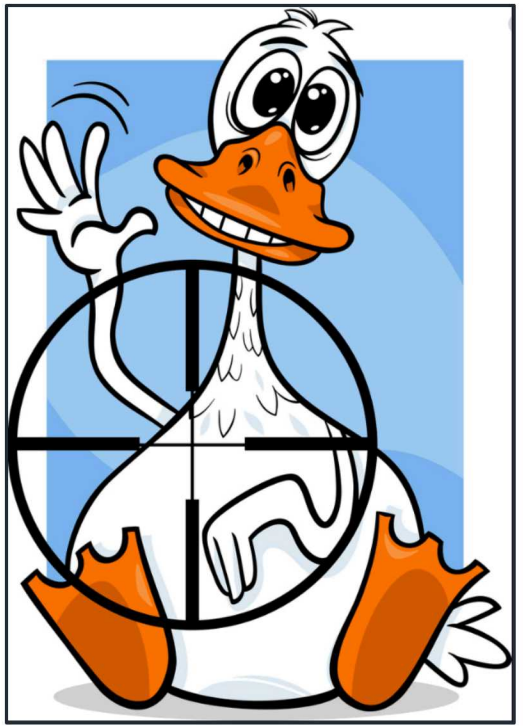
DOE PACT VIRTUAL SHOWCASE

# Business Problem



Static networks use predictable communications and static configurations, making them vulnerable to attack.

- Electrical grids
- Critical infrastructure environments
- Federal communications systems

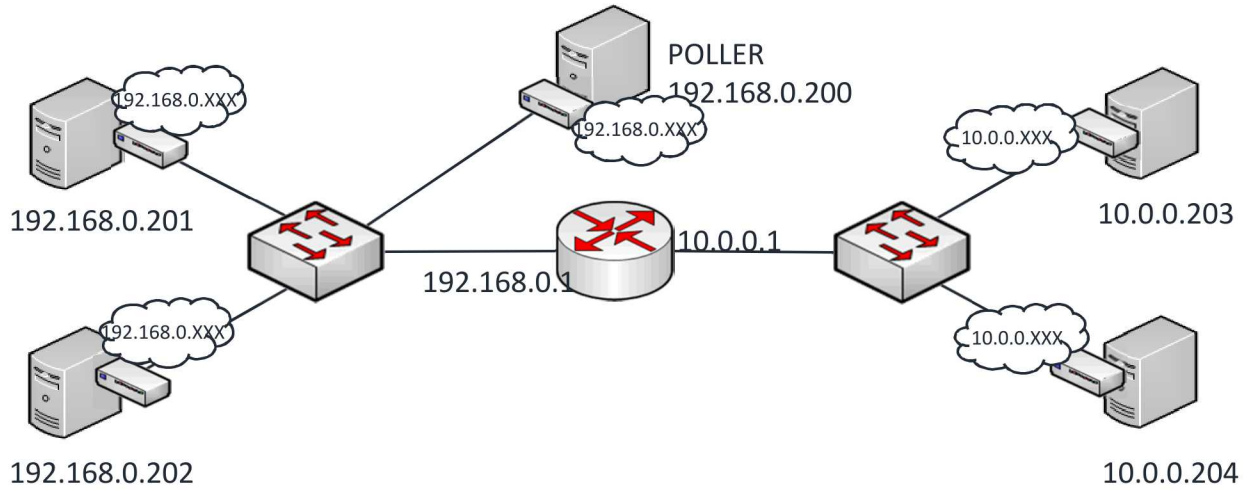


# Technical Challenge



How to create a moving target defense?

- Maintain continuity of network communications
- Maintain timing of network communications
- Broad-based detection needed



# Solution Architecture

ADDSEC

## Machine Learning Ensemble

- Threat detection

## Software Defined Networking

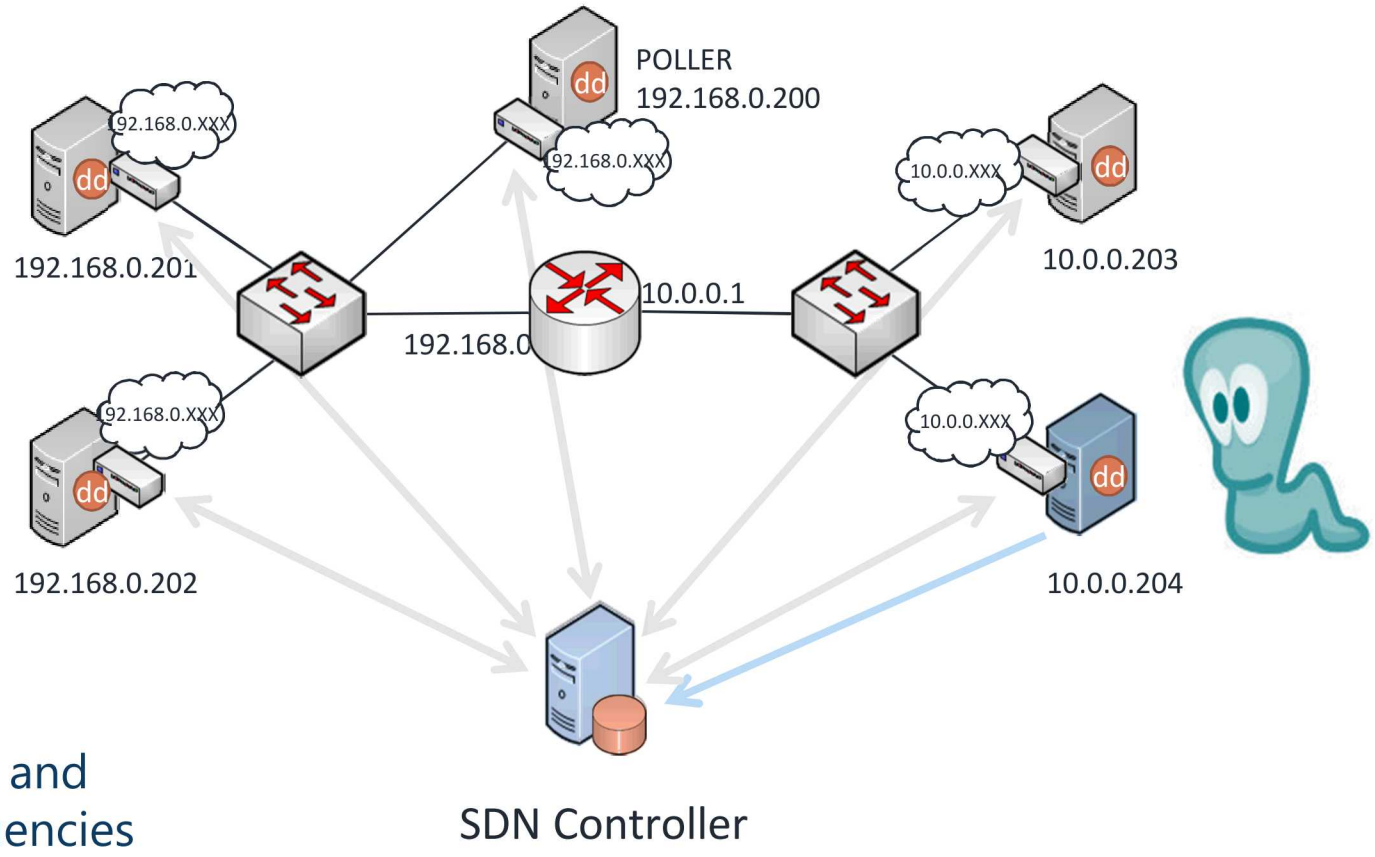
Network level engineering and management

- Transparent to hosts on network
- Open source software switch
  - No need to replace existing network hardware
- Scales with size of network nodes

## Moving Target Defense

Randomizes IP addresses, service port numbers, and communication paths at user configurable frequencies

*Dynamic Defense (dd) Machine Learning Algorithms Deployed*



# Development History & Results

ADDSEC

## Principal Investigator
Adrian Chavez

- Ph.D. Computer Science
  University of California, Davis
- Principal Member of Technical Staff
  Cybersecurity R&D

## Developmental History
**2014** Initial patent filing

**2018** US patent granted

**2019** R&D100 Award Winner (Software/Services)

## Funding History: 2015-Present
$3.8M, DOE CESER Office

Lead: Sandia National Laboratories

Partners: Washington Gas Energy Systems, Chevron, GRIMM, Lawrence Livermore National Laboratory, SEL Schweitzer Engineering Laboratories


## Research Team
Jason Hamlet
Erik Lee
James Obert
William Stout
Mitchell Martin

## Technology Readiness Level (TRL):
TRL 6/7 as of June 2020

## IP Protection
US Patent No. 9,985,984
*Dynamic Defense and Network Randomization for Computer Systems*

## Market Validation
**2017** Successful interoperability testing performed at SEL site (May)

**2018** Technology demonstrated DoD Ft. Belvoir microgrid

# Technical Requirements & Benefits

ADDSEC

## TECHNICAL REQUIREMENTS

- Supports both hardware and software implementations of Software Defined Networking
- Both network layer and edge ML detection

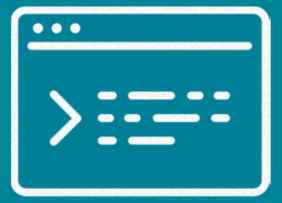
## BENEFITS

- Very low network load
- Improved cyber resilience
- Effective cyber attack detection

# Technology Roadmap

ADDSEC

Collect target system requirements



Install ADDSec/SDN infrastructure

Pilot test and validate scalability of ADDSec

Collect metrics

Field test ADDSec

Bringing ADDSec to Market

# ADDSEC: IP Hopping

DOE PACT VIRTUAL SHOWCASE

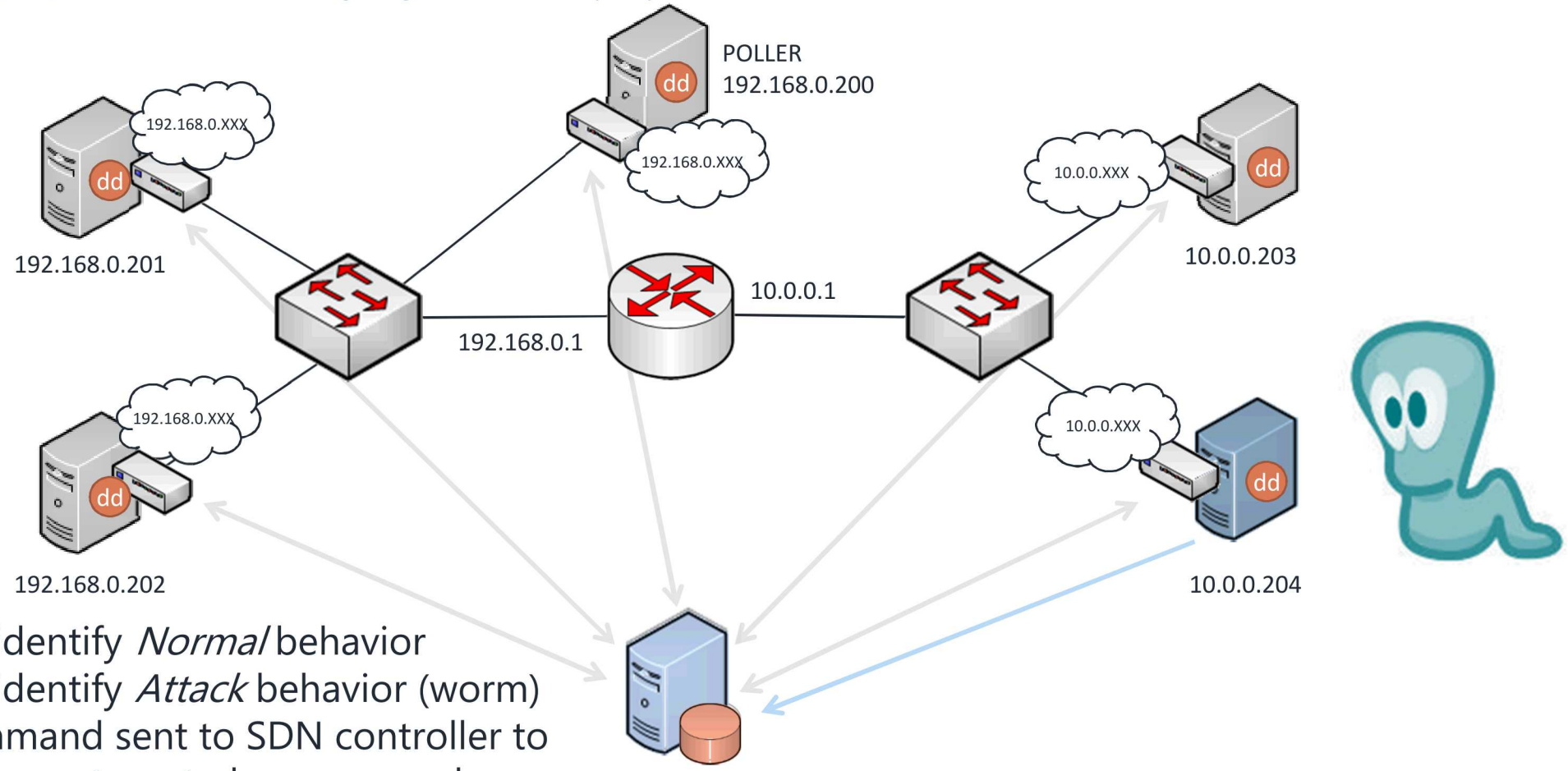
Artificial Diversity & Defense Security

DEMONSTRATION

# Solution Architecture



Dynamic Defense (dd) Machine Learning Algorithms Deployed

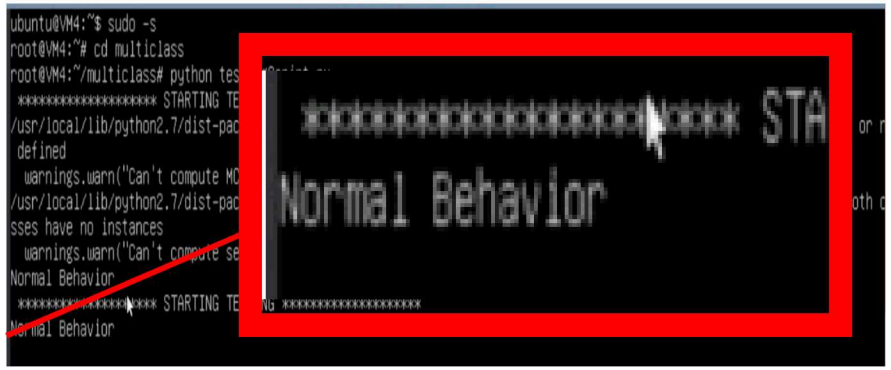



**Results:**

- ML Algorithms identify *Normal* behavior
- ML Algorithms identify *Attack* behavior (worm)
- IP Rotation command sent to SDN controller to change IP's (other automated responses also possible: port, path, and application library randomization)

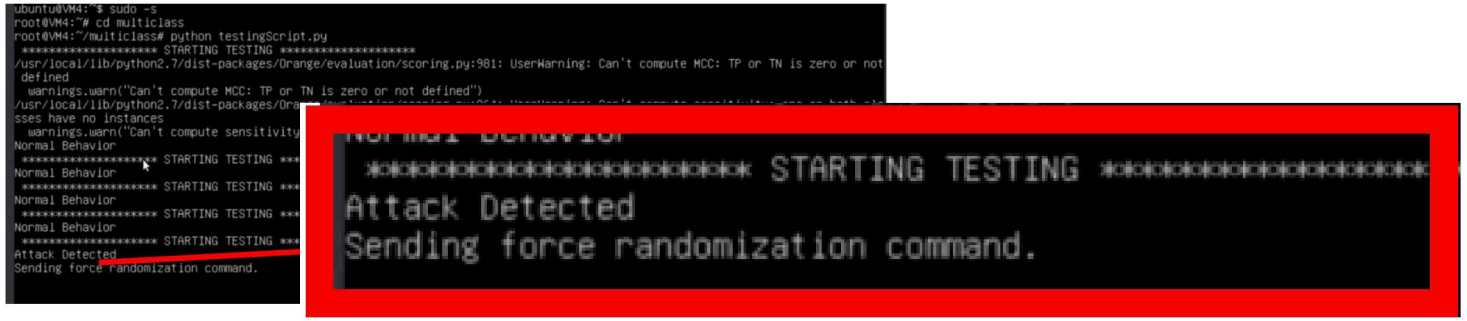
# System Responses Before, During, and After Attack

ADDSEC
DEMONSTRATION



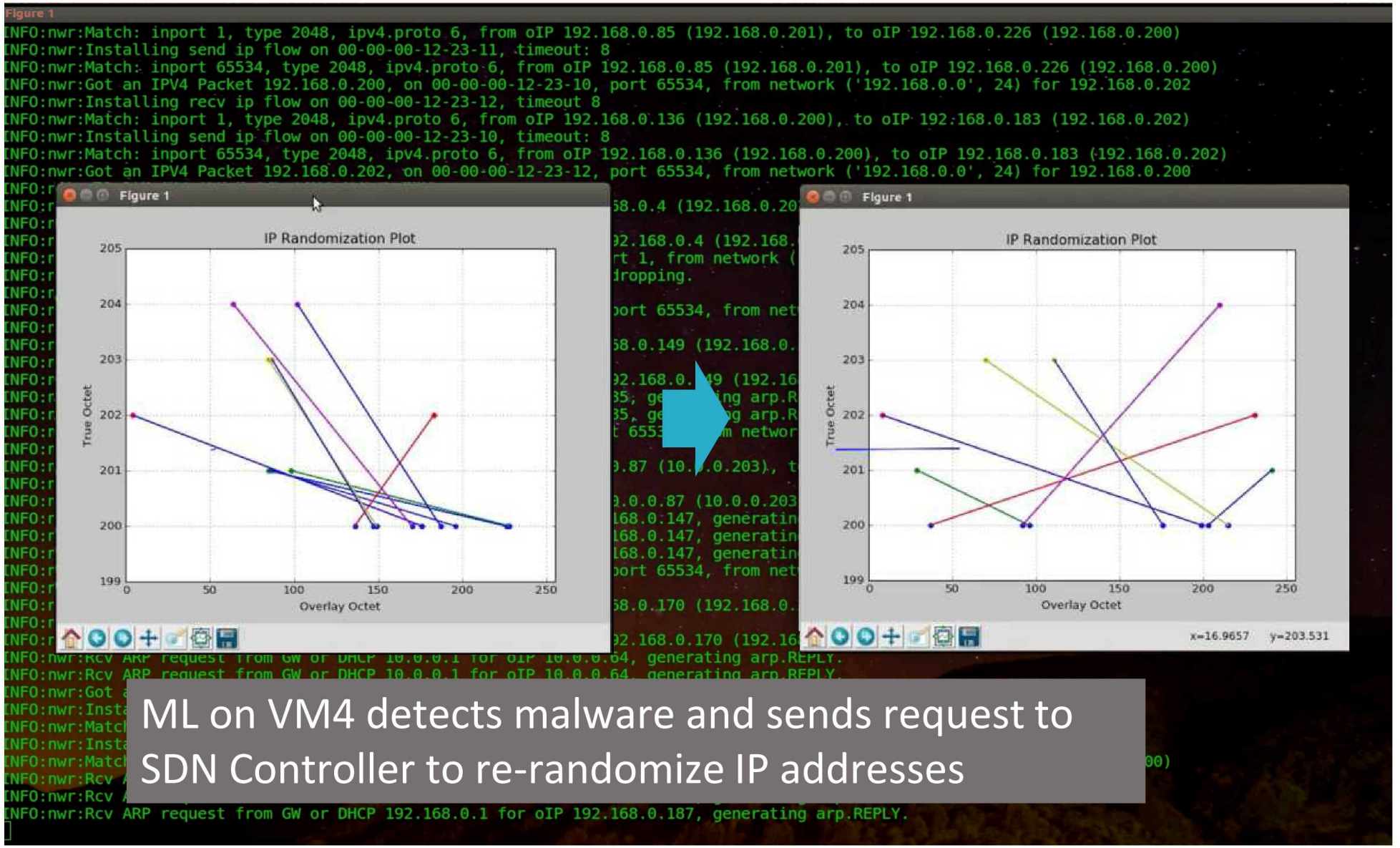

Normal Behavior Detected BEFORE Attack


Malware Worm Scans Network to Propagate




Machine Learning Algorithms Detect Malware Worm Scan

# All Hosts Continue to Communicate, Now, with Randomized IP Addresses

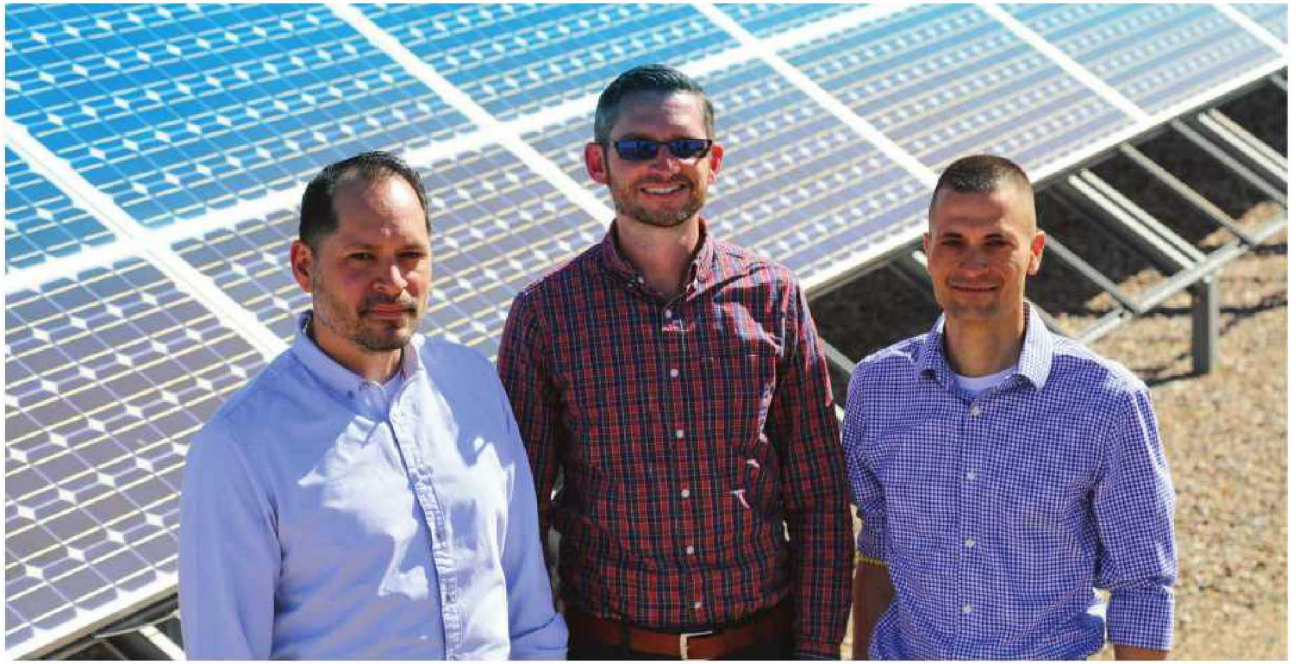


# Reserve Slides

# Business Problem

ADDSEC

Networks and systems that monitor our grid or other critical infrastructure environments use predictable communications and static configurations, making them vulnerable to attack.

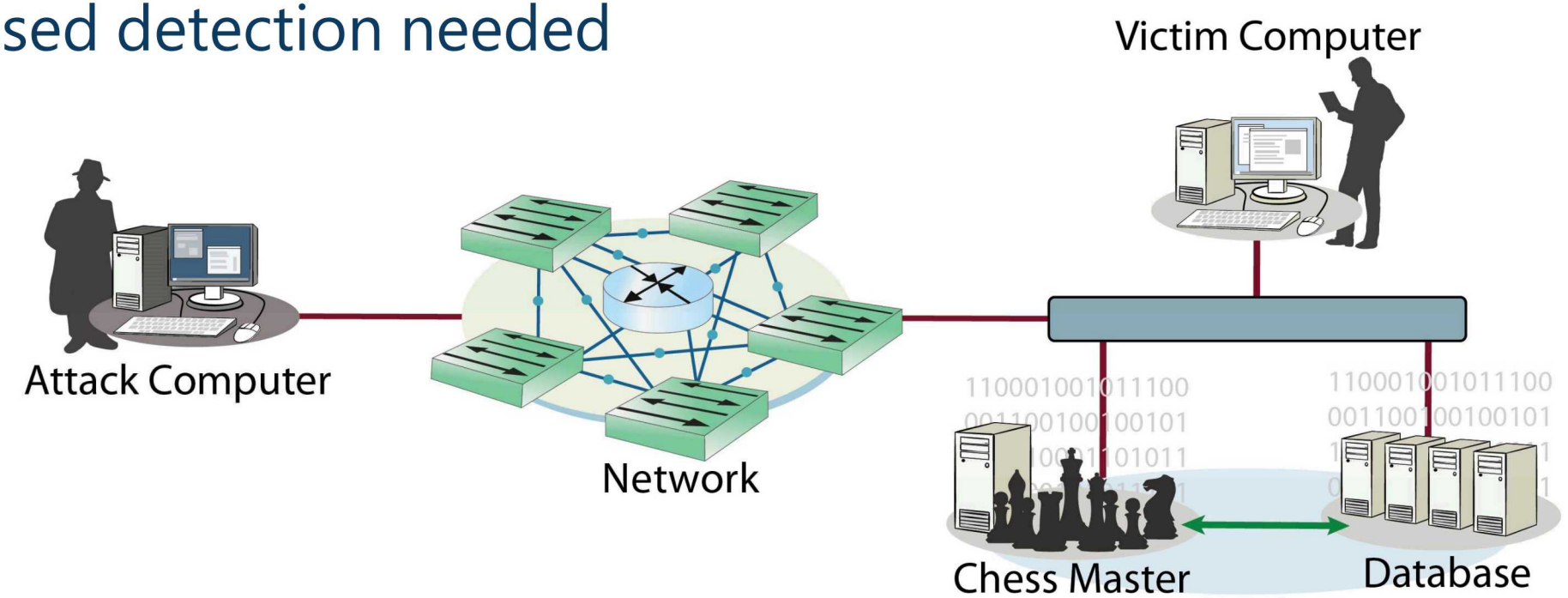


# Technical Challenge



How to create a moving target defense?

- Maintain continuity of network communications
- Maintain timing of network communications
- Broad-based detection needed



# Solution Architecture

ADDSEC

## Machine Learning Ensemble

- Threat detection

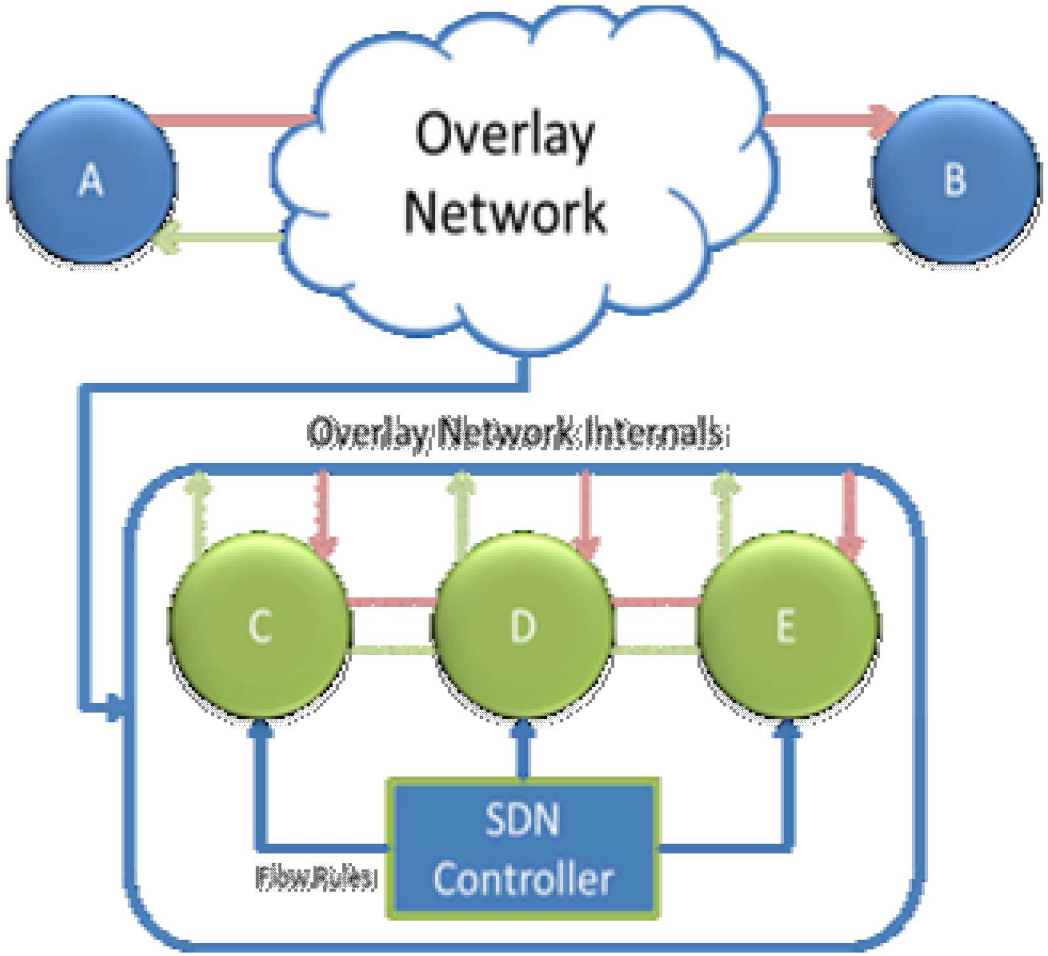
## Software Defined Networking

Network level engineering and management

- Transparent to hosts on network
- Open source software switch
  - No need to replace existing network hardware
- Scales with size of network nodes

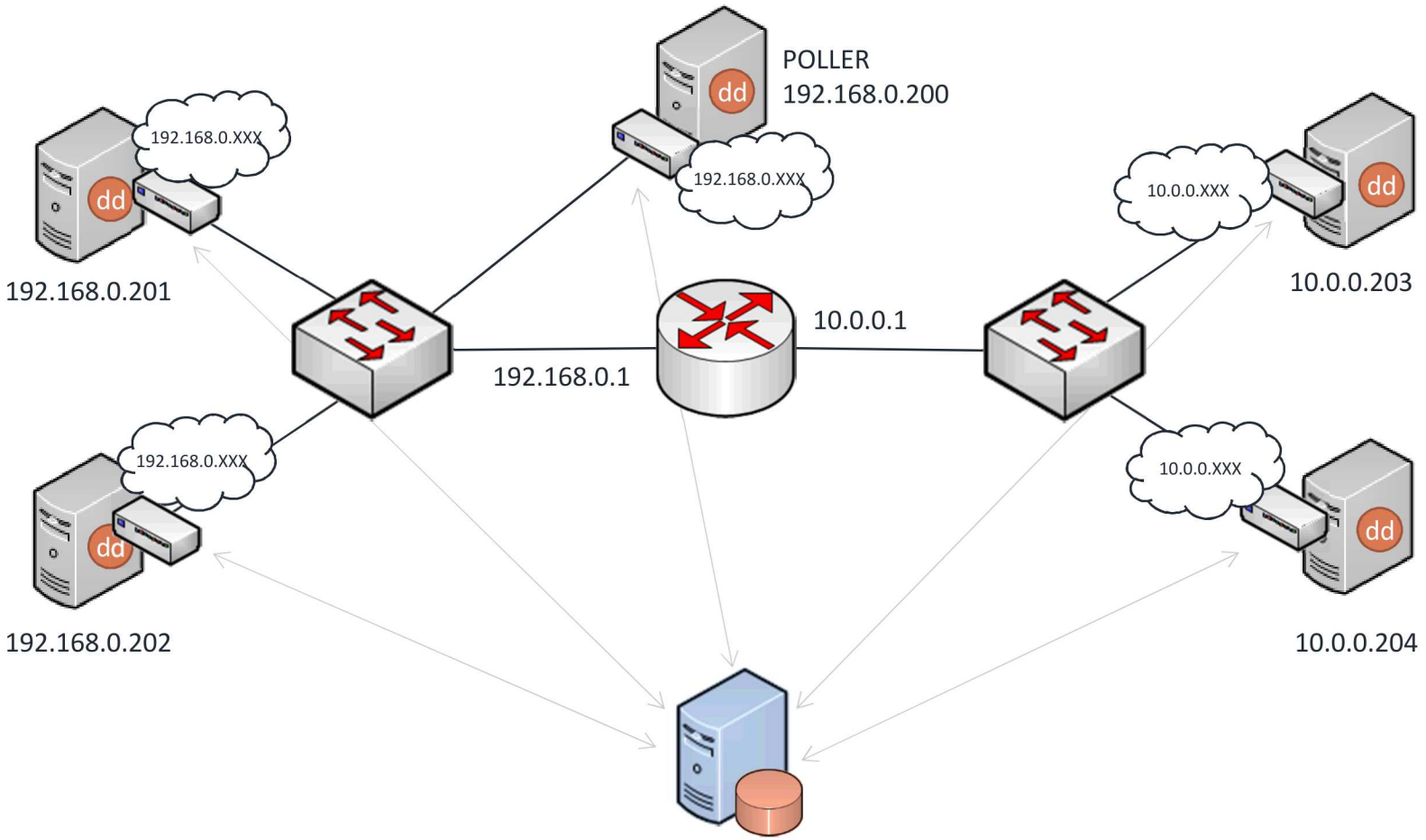
## Moving Target Defense

Randomizes IP addresses, service port numbers, and communication paths at user configurable frequencies



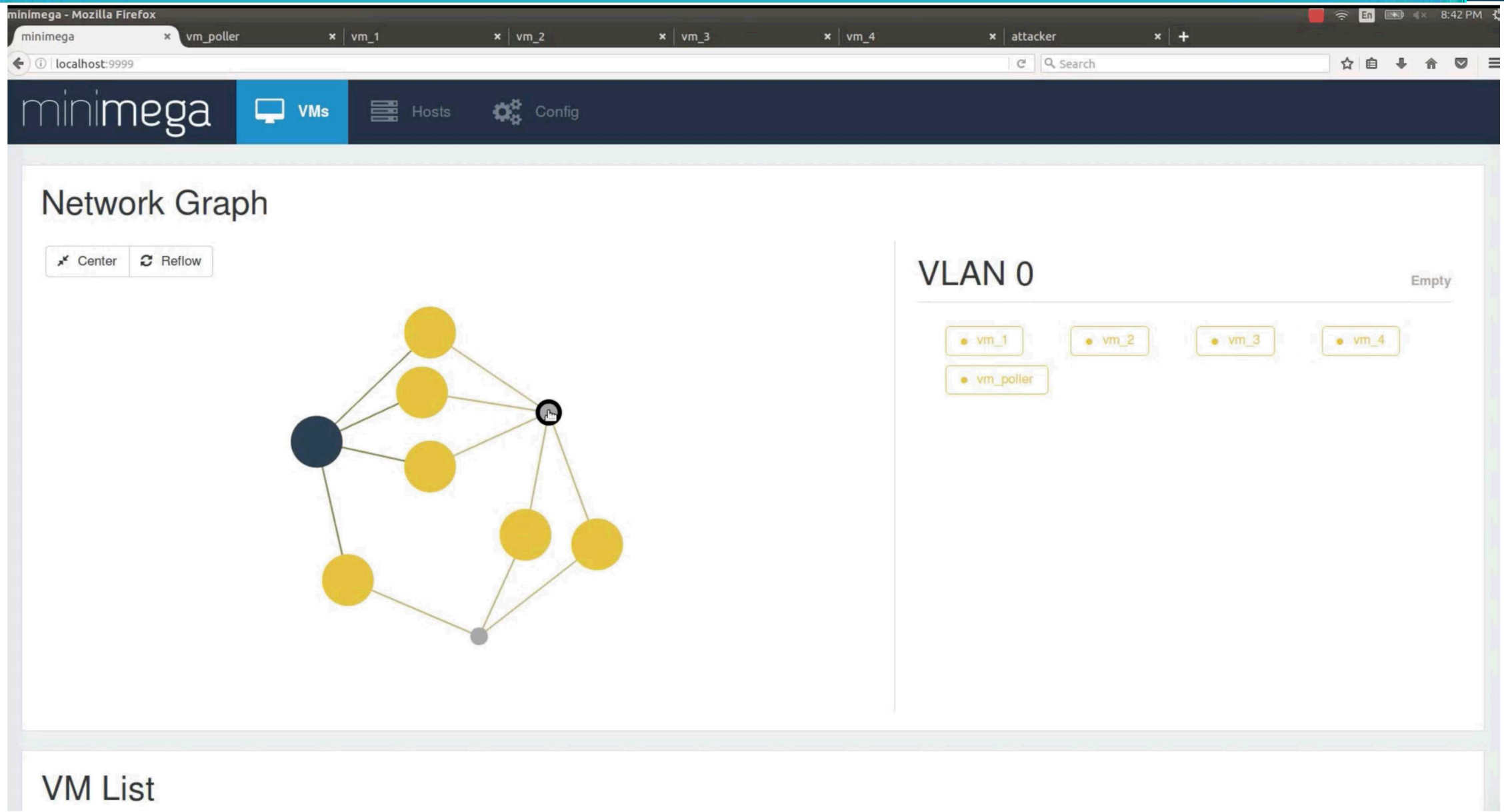
# Dynamic Defense (dd) Machine Learning Algorithms Deployed

ADDSEC



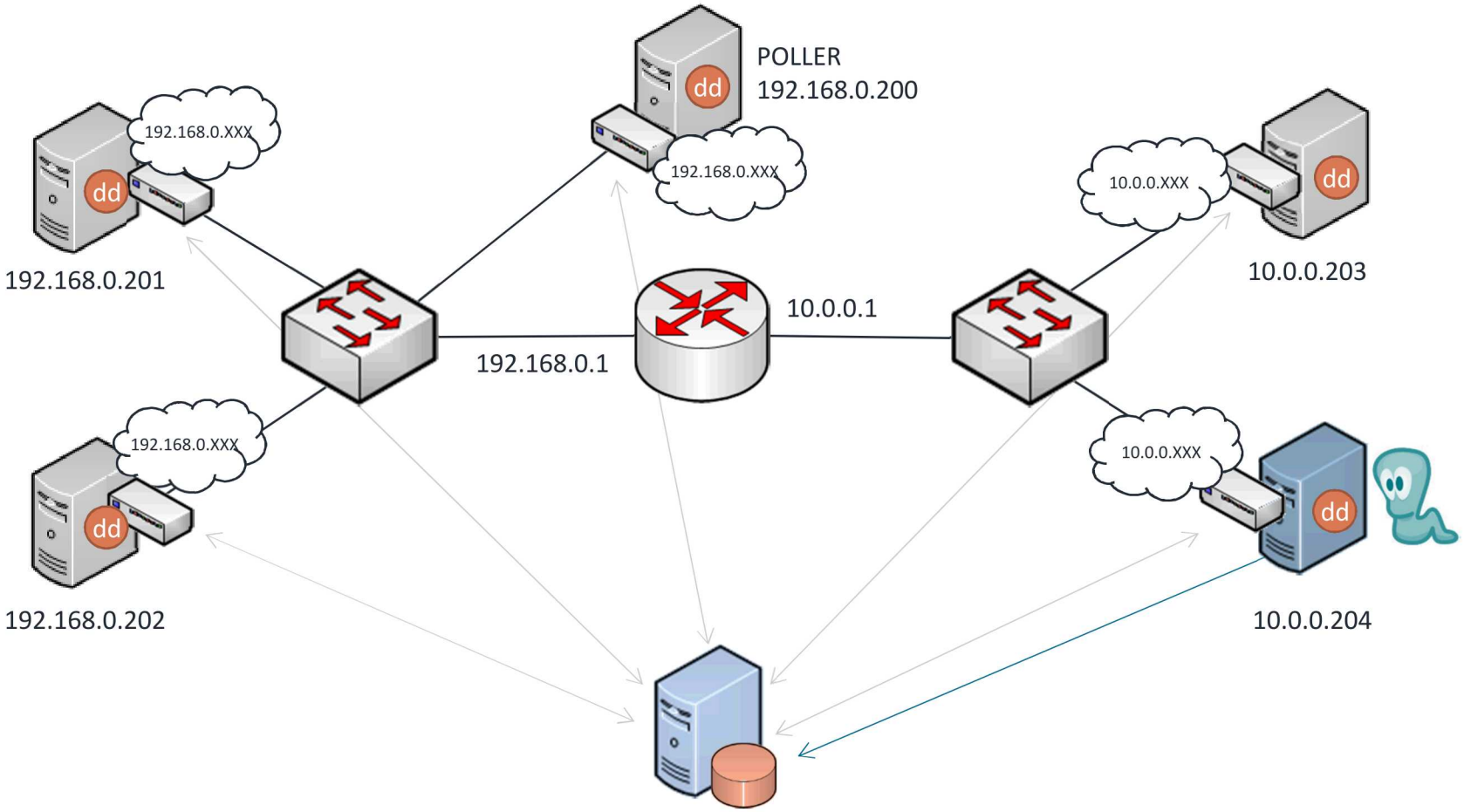
# Virtual Environment Deployment

ADDSEC



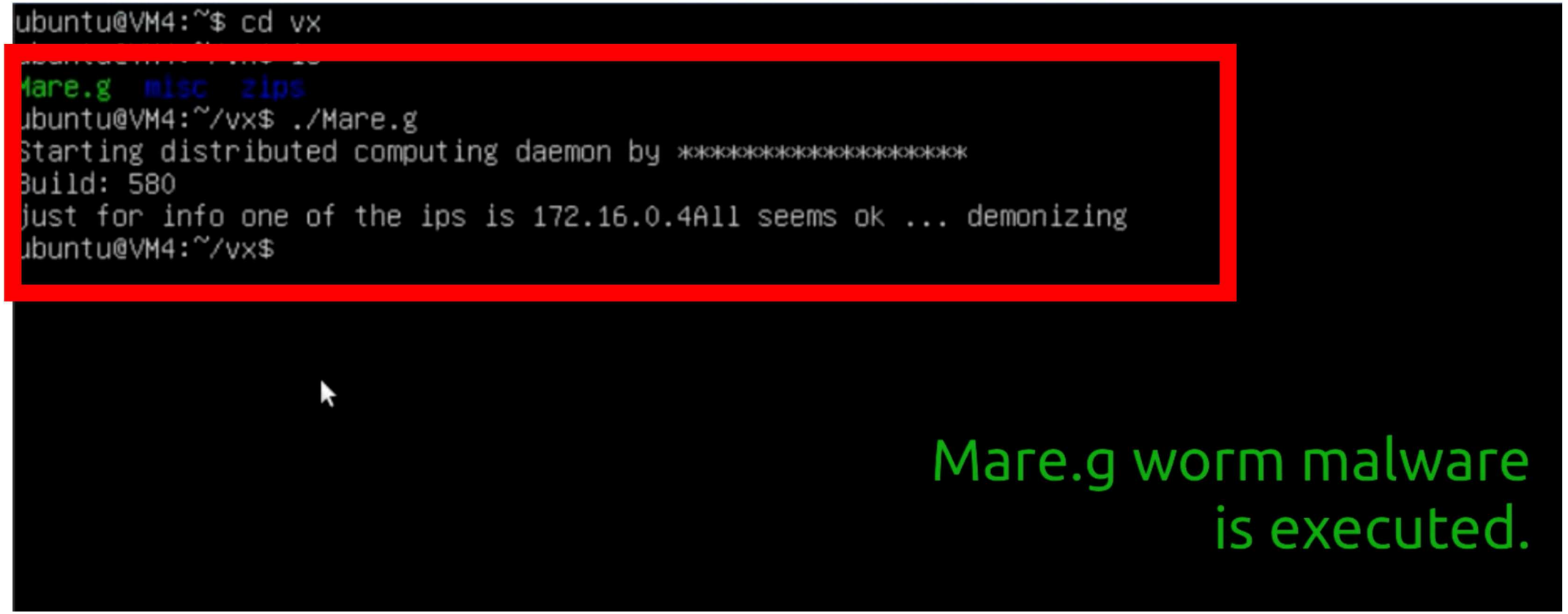
# Host Infected with Malware

ADDSEC



# Malware Worm Scans Network to Propagate

ADDSEC



# Machine Learning Algorithms Detect Malware Worm Scan

ADDSEC