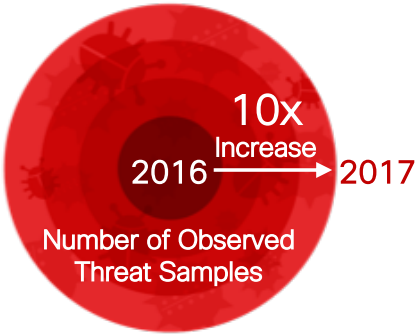
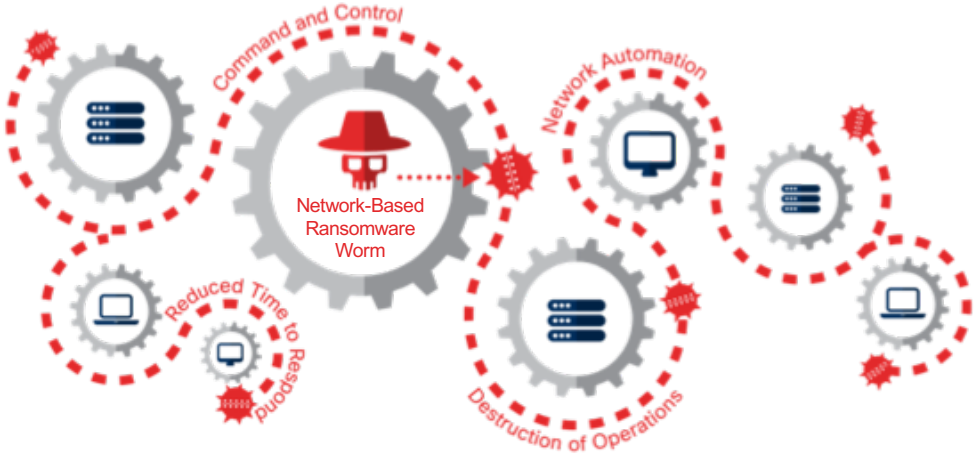
Agent-Based Modeling and Simulation in Cybersecurity

Petr Cernohorsky
Advanced Threat Solutions, Cisco Security
April, 2018

Evolving Threat Landscape …





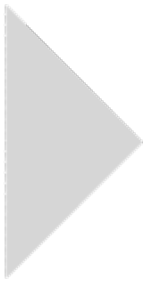
Attackers use encrypted C&C, cloud, ransomware worms, IOT/DDoS

Source: 2018 Annual Cybersecurity Report

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Evolving Threat Landscape Requires Automation!

Attackers
use encrypted C&C, cloud, ransomware worms, IOT/DDoS



Defenders
employ automation, AI/ML, behavioral analytics

Source: 2018 Annual Cybersecurity Report; Over 30% surveyed organizations are completely reliant on AI/ML.

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

AI/ML is Gaining Traction in Cybersecurity

Success Criteria

Balance between
unsupervised & supervised
methods

Reinforcing cycle of
input data and
continuous learning

Availability of labeled data

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

ML & Simulations: Reduced Need for Labeled Data

Machine Learning algorithms can be trained via Simulation *

Labeled data challenge *: supervised machine learning requires labeled data (imagine 100's hours of work for every simple task)

Digital Twin *: virtual model facilitating analysis of a complex system, e.g. Agent-based Modeling and Simulation (ABMS)

*) Source: http://usblogs.pwc.com/emerging-technology/top-10-ai-trends-for-2018

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Learning Through Simulation

Car Racing
Computer Game

Autonomous
Car

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Complexity Science

Cyber Systems (IT, networks, humans) are **Complex Adaptive Systems (CAS)**

Emergent phenomena, adaptation, distributed artificial intelligence

Inspired by social sciences, economics, epidemiology

Sources:

http://www.bcs.org/content/conWebDoc/55148

https://hbr.org/2013/06/embrace-the-complexity-of-cybe

http://bit.ly/wiki-abms; *https://www.santafe.edu/engage/learn/courses/introduction-agent-based-modeling*

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Complexity Science

Agent-Based Modeling and Simulation (ABMS)

Approach to studying systemic issues in cybersecurity

Simulations

Cybersecurity: simulation allows for scenario testing (risk free environment)

Dreams: evolution's mechanism to prepare the mind for new events / "nightmare"

Sources:
http://www.bcs.org/content/conWebDoc/55148
https://hbr.org/2013/06/embrace-the-complexity-of-cybe
http://bit.ly/wiki-abms; https://www.santafe.edu/engage/learn/courses/introduction-agent-based-modeling

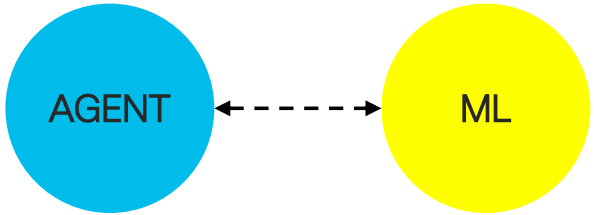
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Machine Learning (ML) meets Agent-Based Modeling and Simulation (ABMS)

Option: #1

Interact with the world and other agents

Observe the world & learn optimum agent behavior



Population of Agents
(network nodes, users, admins, attackers)

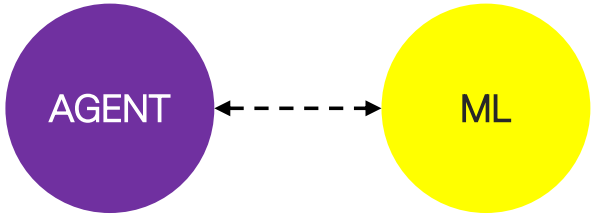
Source: *https://ccl.northwestern.edu/papers/agent2006rand.pdf*

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Machine Learning (ML) meets Agent-Based Modeling and Simulation (ABMS)

Option: #2

Feed threat detection classifiers with
combination of
REAL & SIMULATED DATA



Population of Agents
(… simulate effects of attacks and policies …)

Source: *https://ccl.northwestern.edu/papers/agent2006rand.pdf*

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Agent-based Simulation for Assessing Network Security Risk due to Unauthorized Hardware

MIT Lincoln Laboratory: Neal Wagner, Richard Lippmann, Michael Winterrose, James Riordan, Tamara Yu and William W. Streilein

ABMS

- Captures emergent system behaviors among network agents
- Agents = users, administrators, attackers, defenders
- Models
  - Attack and defense model
  - Network environment model
  - User model

Simulation

- Cost effective evaluation of network policies
- Quantifies effectiveness of strategies for unauthorized devices prevention

Source: *https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2015-04-Wagner-ACM.pdf*

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

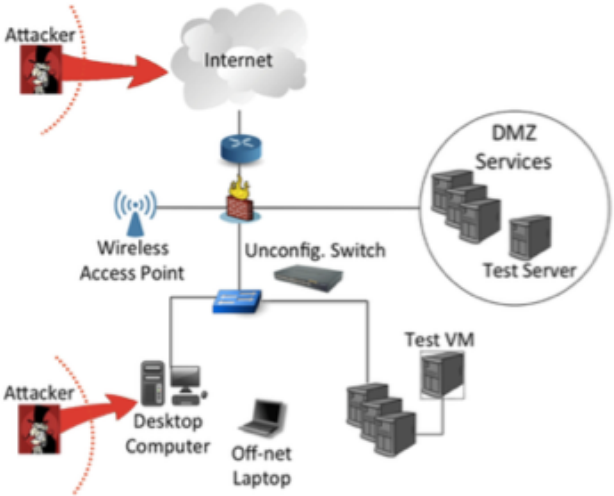
Agent-based Simulation for Assessing Network Security Risk due to Unauthorized Hardware

MIT Lincoln Laboratory: Neal Wagner, Richard Lippmann, Michael Winterrose, James Riordan, Tamara Yu and William W. Streilein

Attack and Defense Model

- SANS Critical Control 1 (CC1)
- Attacker scans a network either internally or externally looking for vulnerabilities.
- Opportunistically compromises devices.
- **Unauthorized devices**

  Unmanaged or improperly managed devices (un-configured, unpatched, not-updated devices, personal devices, VMs).



Network Model (Vulnerability & Asset Val.)

Source: *https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2015-04-Wagner-ACM.pdf*

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Agent-based Simulation for Assessing Network Security Risk due to Unauthorized Hardware

MIT Lincoln Laboratory: Neal Wagner, Richard Lippmann, Michael Winterrose, James Riordan, Tamara Yu and William W. Streilein

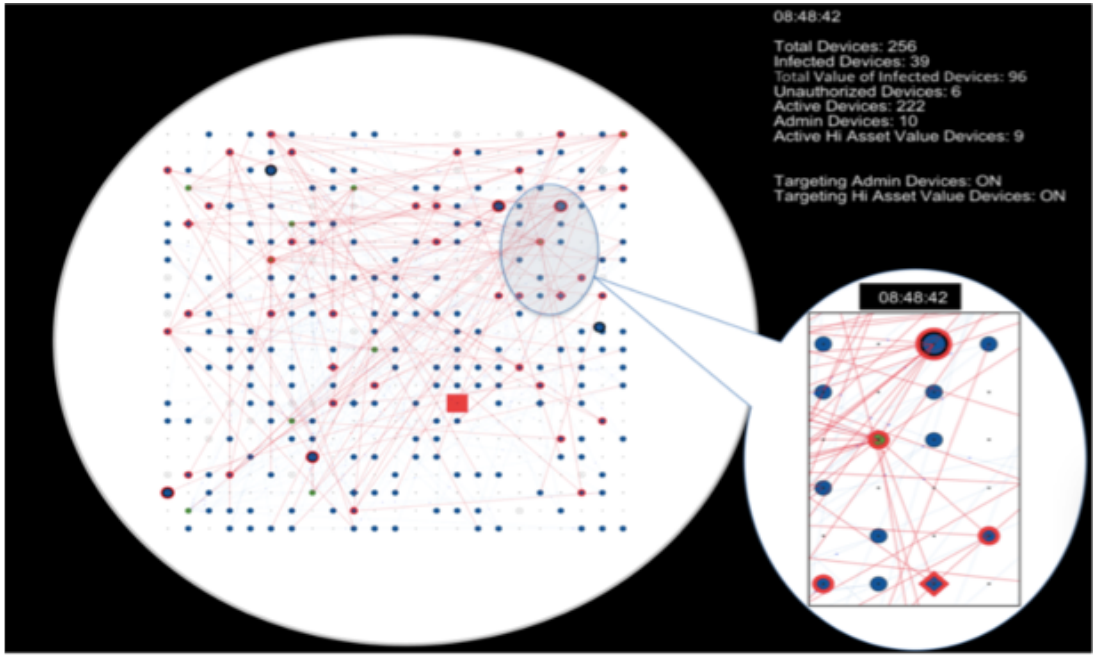
1

Experiments

- Goal is to minimize "Network Value" that was compromised.
- Tracing the infection (infected device, lateral spreading, escalating admin privilege)

Results

- Quantification of strategies (User trainings, NAC, # of admins, scan rates, …)



Source: https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2015-04-Wagner-ACM.pdf

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Agent-Based Simulation in Support of Moving Target Cyber Defense Evaluation

MIT Lincoln Laboratory: Ben W. Priest, Era Vuksani, Neal Wagner, Brady Tello, Kevin M. Carter and William W. Streilein

Goal: Evaluate effects of particular Moving Target (MT) techniques.

Model

- Network with mission-critical and non-mission-critical users and traffic.
- Cyber attacks sent by malicious actors.
- MT technique = multi-compiler to introduce software diversity

Experiments

- Interactions between attackers, MT system, and network operations.
- Measures effects, security posture, and performance.

Source: http://www.nealwagner.org/research/articles/springsim2015-NCS.pdf

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Behavioral Simulations: Using Agent-Based Modeling to Understand Policyholder Behaviors

PWC: Louis Lombardi, Mark Paich, and Anand Rao

Application: Insurance Industry

Behavioral Economics

- Study of actual (as opposed to rational) decision making by consumers
- Takes into account their social, cognitive and emotional biases.

Model / Agents

- Policyholder, Underwriter, Advisor
- Insurance Company, Rating Agency, Regulators

Source: *https://www.soa.org/library/newsletters/product-development-news/2014/june/pro-2014-iss89-lombardi.pdf*

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Simulations in Cybersecurity: Conclusion

Two major areas of application

1. Cyber Risk Assessment / Cyber Insurance
2. Learning Through Simulation (ABMS Enhancing ML)

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO