RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: **LAW-T10**

HACK BACK FOR GOOD, NOT VENGEANCE: DEBATING ACTIVE DEFENSE FOR ENTERPRISES

MODERATOR: **Steven M. Bellovin**
Professor of Computer Science, Columbia University
@SteveBellovin

PANELISTS:

Salvatore J. Stolfo
Professor
Columbia University and Allure Security Technology, Inc.

Stewart Baker, Esq.
Steptoe & Johnson, LLP

Angelos D. Keromytis
DARPA, I2O

Hack back for Good, Not Vengeance:

Steven M. Bellovin

Columbia University

Hackback for Good, Not Vengeance:

Stewart Baker, Esq.

Steptoe & Johnson, LLP

The hackback problem

- Under US law, almost anything you do on a computer is unlawful if it isn’t “authorized”
- You know you’re authorized if you own the computer
- Otherwise, you’re in legal limbo
- Put another way, you’re hacking back
- This is dumb law and failed policy

Failed 1980s Policy

- If everyone just patched and defended their own systems
- Hackers would be deterred and we'd have security, rainbows, and unicorns

2017 Reality: Yeah, not so much

- Huddling behind walls doesn’t work
- What does?
  - Attribution
  - Threat Intelligence
  - Deterrence
- Someone has to do the attribution, collect the intelligence, and bring the deterrence

Why not let the government do that?

- Resources: Three or four top banks spend more on cyber security than all of DHS and FBI
- Agility:
  - In physical world, government forces respond to 911 intrusions and patrol the territory where criminals are active
  - On the internet, 911 calls emergency response firms, patrolling is done by CISOs – no government role or ability to respond quickly
- Yet in the physical world, no one leaves all policing to the government.
- Security guards, private investigators, bond bounty hunters, repo men – all have some additional (and regulated) quasi-governmental authority

Responsible hackback

- Government oversight/conditions
- Liability for destruction/loss on third party sites
- Sharing of information obtained with government
- Getting there
  - ACDC Act (Graves, Sinema)
  - CCIPS "No Action" Letters

Hack back for Good, Not Vengence: Debating Active Defense

Salvatore J Stolfo

Columbia University

Intrusion Detection Systems Lab

And

Allure Security Technology, Inc.

Optimal Goals of Active Defense

- Strengthen My Security Posture
  - Break the adversary/defender cycle that favors the attacker
  - Deter/Punish Adversaries (and feel good about it)
- Forget Attribution – its of no value
- Hack Back is viable depending upon how you define it and design it to avoid self inflicted wounds

Feasible Goals of Active Defense

- Respond to an attack to raise adversary costs
  - Response should be carefully designed to avoid inadvertent risks to the defender
- Risks due to adversary response, or inadvertent harm to bystanders may not be known, but perhaps can be “minimized” using non-lethal hackback
  - Knowledge attack: Decoy Technology

Deception and Decoy Technology is Knowledge Hack Back

- Focus on “fake” data they seek. HoneyX’s are detectors, and do not provide a Knowledge Hack Back
- Automated/Scalable Data Deception is feasible and legal
  - Bogus data generation to “poison” and trick adversary (eg., insiders)
  - Remote “beacons” to detect exfiltration and feed more bogus data
- Automated generation strategic placement of believable decoys such as documents within your security architecture
- A rich collection of decoy DATA types is feasible:
  - Cloud services
  - Mobile applications
  - Software
  - Voicemail

Hack Back and Active Defense
Take away…

Forget about Attribution

Forget About Legal Conundrums

Prepare for the adversary with fake data, decoys and beacons

Raise the **cost** to the adversary

____

Nonetheless, It may be wise to be prepared and capable of launching lethal hack back in extreme cases when it is necessary at least as a deterrent.

Hack back for Good, Not Vengeance:

Angelos D. Keromytis

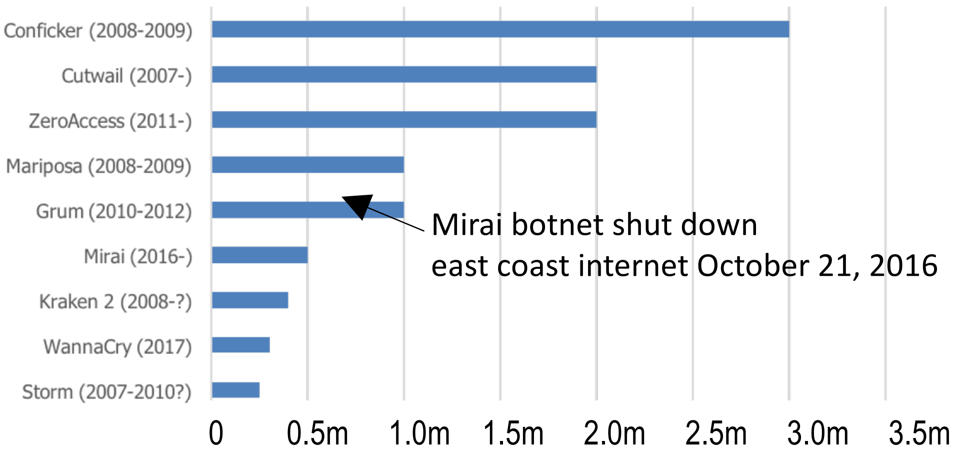
DARPA/I2O

HACCS Program Goal

Develop safe, reliable, and effective capabilities for conducting Internet-scale counter-cyber operations to deny adversaries' use of neutral (gray) systems and networks (e.g., botnets)

Cyber Attackers Can Muster Massive Botnets

Botnet Sizes Observed on the Internet, in millions of compromised devices



Mirai botnet shut down
east coast internet October 21, 2016

State and non-state adversaries can compromise and conscript large numbers of gray (neutral) networks and systems

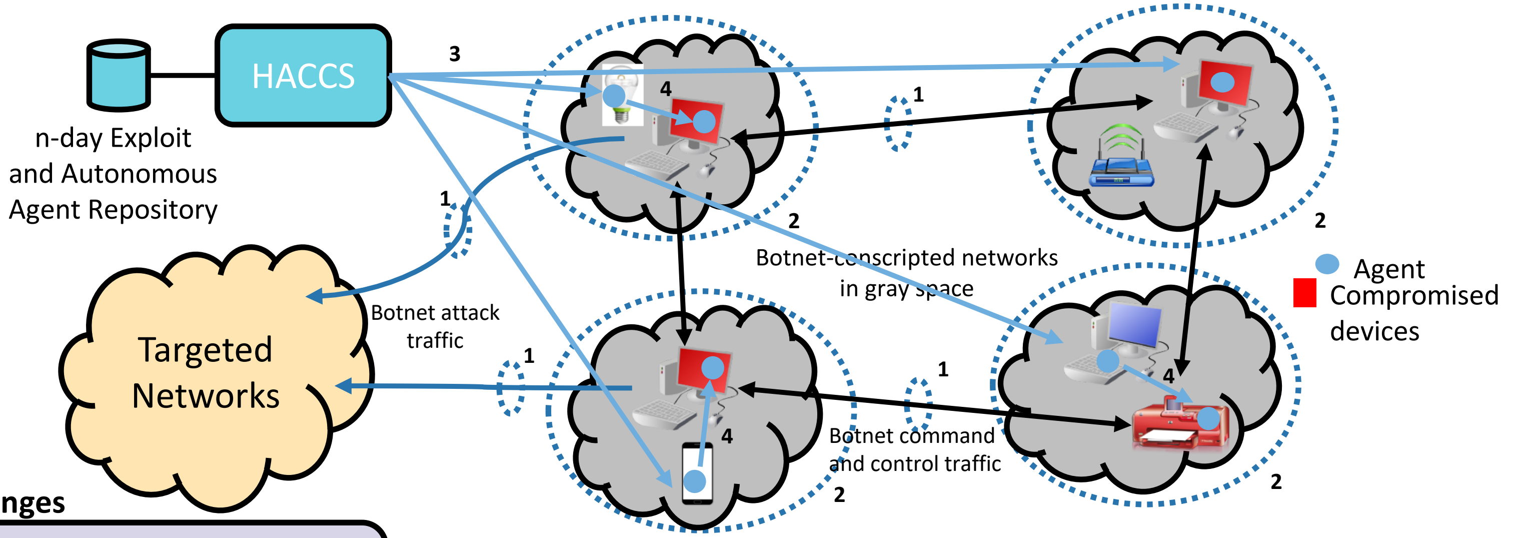
- Gradual or rapid buildup through compromise and purchase of resources
- “Botnet for hire” services
- Botnets can DDoS networks, provide pivot points for operations, impede the flow of information, circumvent defenses, and amplify influence operations via social media

Presenter’s Company Logo – replace or delete on master slide

Harnessing Autonomy for Counter Cyber Systems

#RSAC

Develop safe and reliable autonomous agents that can used in gray networks at scale to counter botnets/implants



HACCS
n-day Exploit and Autonomous Agent Repository
3
4
1
1
2
2
Botnet-conscripted networks in gray space
Botnet attack traffic
Targeted Networks
1
1
4
4
Botnet command and control traffic
2
2
● Agent
🟥 Compromised devices

Challenges

1. Find botnet-conscripted networks — **TA1**
2. Fingerprint botnet-conscripted networks — **TA1**
3. Exploit n-day vulnerabilities to insert agents — **TA2**
4. Identify and safely neutralize botnet implants at scale, according to verified rules of operation — **TA3**

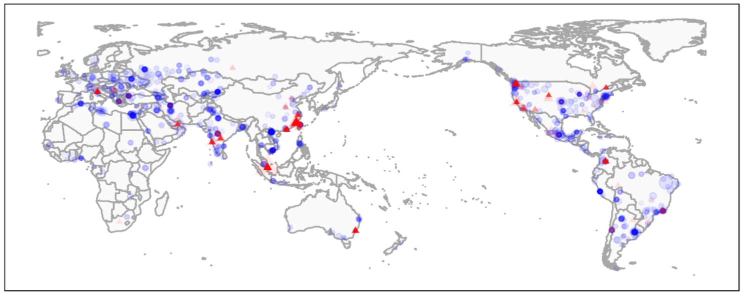
Why Now?
Recent Technical Advances in:

1. Multi-dimensional network analytics
2. Cyber Reasoning Systems
3. Autonomous software agents leveraging AI

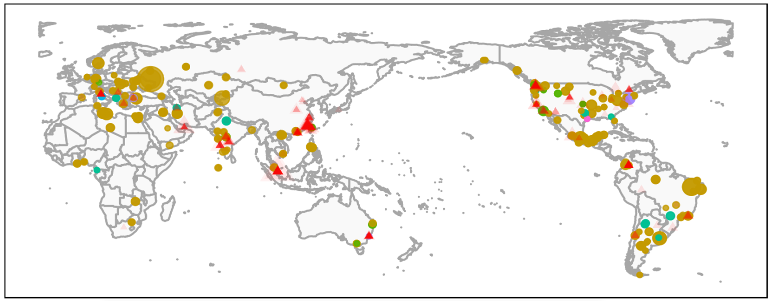
RSAConference2018

DARPA

TA1: Find and Fingerprint Botnet Infrastructure



Hidden Cobra (DPRK)



Hidden Cobra co-resident IoT devices

Key Research Challenges

1. Internet-scale real-time botnet detection in the presence of evasive/covert C2
2. Accurate fingerprinting of devices and software in compromised networks

Possible Approaches

1. Automated traffic analysis using disparate and noisy data sources
2. Efficient and scalable black-box characterization of device network behavior
3. Precise white-box analysis of network-observable software behavior using information flow

Metrics

- Accuracy
- Percentage of devices characterized across the Internet
- Speed/work factor of fingerprinting new device/software

TA2: Insert Autonomous Agents Into Gray Networks

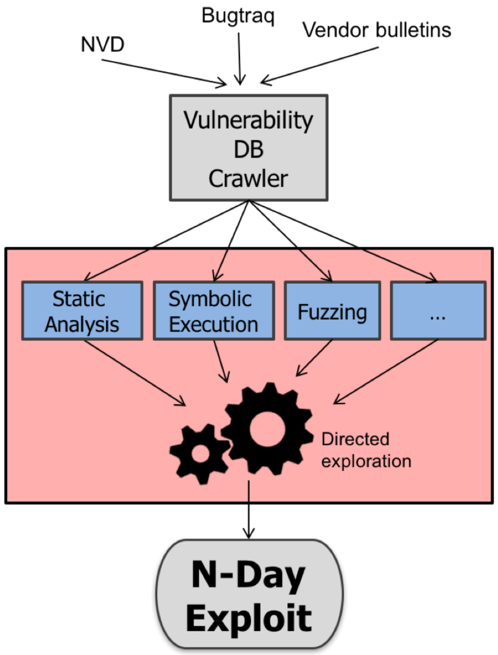
Primary approach: Exploit known (n-day) vulnerabilities

Key Research Challenges

1. Automated generation of n-day exploits for agent insertion
2. Development of IoT- and cloud-specific agent insertion techniques

Possible Approaches

1. Focus Software Reasoning Systems (SRS) analysis on known vulnerable code
2. Extend SRS analysis beyond memory corruption vulnerabilities



Metrics

- Number of exploits
- Vulnerability class coverage
- Stability of exploits

Presenter's Company Logo – replace or delete on master slide

DISTRIBUTION A. Approved for public release: distribution unlimited.

TA3: Identify and Neutralize Botnet Implants

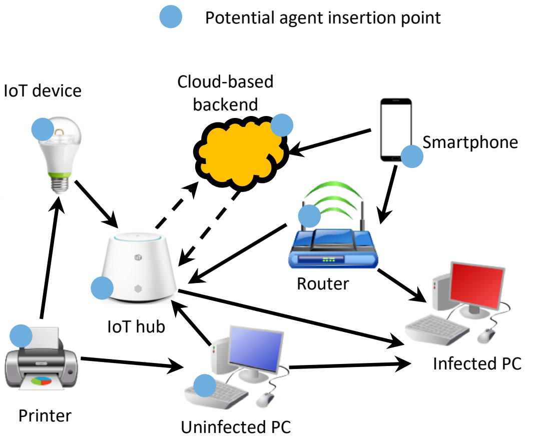
Develop software agents that autonomously navigate within each gray network toward infected devices to safely neutralize the malicious botnet implant

Key Research Challenges

1. Autonomous lateral movement in partially known environments
2. Correctness of agent implementation
3. Correctness of rules of operation

Possible Approaches

1. Learn and generalize from human operators in cyber-exercises, adversary activities, and similar sources
2. Correct-by-construction techniques and tools applied to agent generation
3. Contract-based programming



Metrics

- Success rate and speed in navigating topologies
- Fraction of code proven correct

DISTRIBUTION A. Approved for public release: distribution unlimited.