RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: AIR-T08

Flash War: Tapering an Accelerating Attack Chain

Derek Manky
Chief of Security Insights, Global Threat Alliances
Fortinet

ABOUT ME

- Software & reverse engineering (Threat Analysis) background
- 20 years experience in IT
- 14 years experience at Fortinet (FortiGuard)

- Visionary role – threat forecasting and roadmap
- Chief liaison for threat intelligence partnerships & industry
  - Sit on steering committee of Cyber Threat Alliance
  - Pioneered founding efforts, bylaws

- Designed, Created & Lead Cyber SEAL Team (FortiGuard)
  - Seasoned, global threat expertise team
  - Incident response to breaking events
  - Proactive threat research & intelligence
  - Consult to C-Suite worldwide including Fortune 500
  - Train talent & capacity

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

Agenda

- Current Landscape – Offensive Automation
- Traditional Challenges we Face
- Strategic, Agile & Scalable Approaches
- Future Weaponization of AI
- Flash War Summary – Takeaways

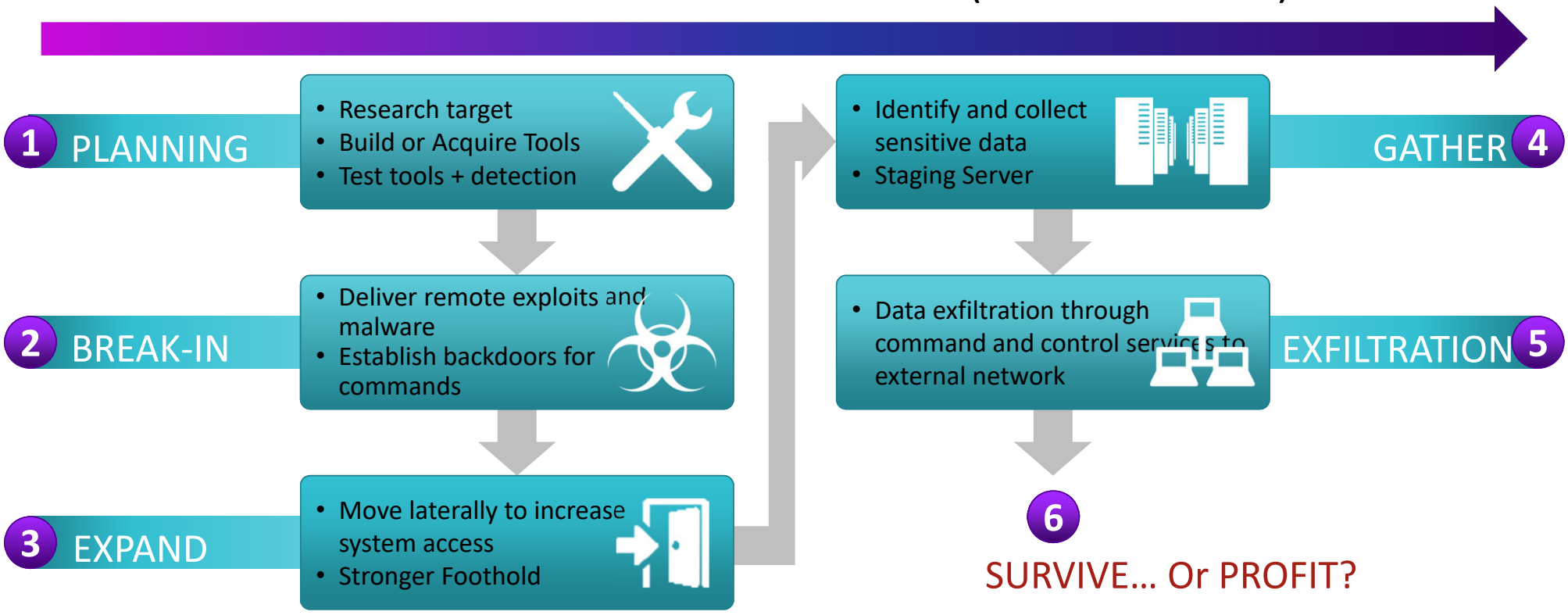
RSAConference2019

The Now – Offensive Automation

Precursors of Offensive AI, Swarm Technology

THE ACCELERATED ATTACK CHAIN

Automation & Swarm Decrease TTB (Time to Breach)



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

AUTOSPLOIT – BUILDING SWARMS

- Shodan is a search engine that indexes open ports and services
- Attacker Queries Shodan
- Attacker uses a list of known exploits to attack known IoT and other systems based on indexed queries given by Shodan
- Attackers then attacks IoT or vulnerable systems directly bypassing per miter security features gaining a foothold into internal networks.

SHODAN
Computer Search Engine

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

Hide and Seek

```
arg = (char *)v4[1];
_arg = *arg;
if ( *arg == 'k' )                      // kill by port
{
  port = strtol(arg + 1);
}
else if ( *arg > 'k' )
{
  if ( _arg == 'l' )                    // use specified udp port
  {
    sp_port = strtol(arg + 1);
  }
  else if ( _arg == 's' )               // load file to mem
  {
    v2 = 0;
    loadfpath(arg + 1);
  }
}
else if ( _arg == 'a' )                 // add ip port to list
{
  sub_40B9B1((__int64)(arg + 1), 0);
}
else if ( _arg == 'e' )                 // add ip port to scanner target
{
  v7 = sub_40E480((unsigned __int64 *)qword_5127E8, 16LL * (unsigned int)(dword_5127F0 + 1));
  qword_5127E8 = v7;
  if ( v7 )
  {
    sub_401346(arg + 1, v7 + 16LL * (unsigned int)dword_5127F0);
    ++dword_5127F0;
  }
  else
  {
    dword_5127F0 = 0;
  }
```

2) Target is identified by swarm

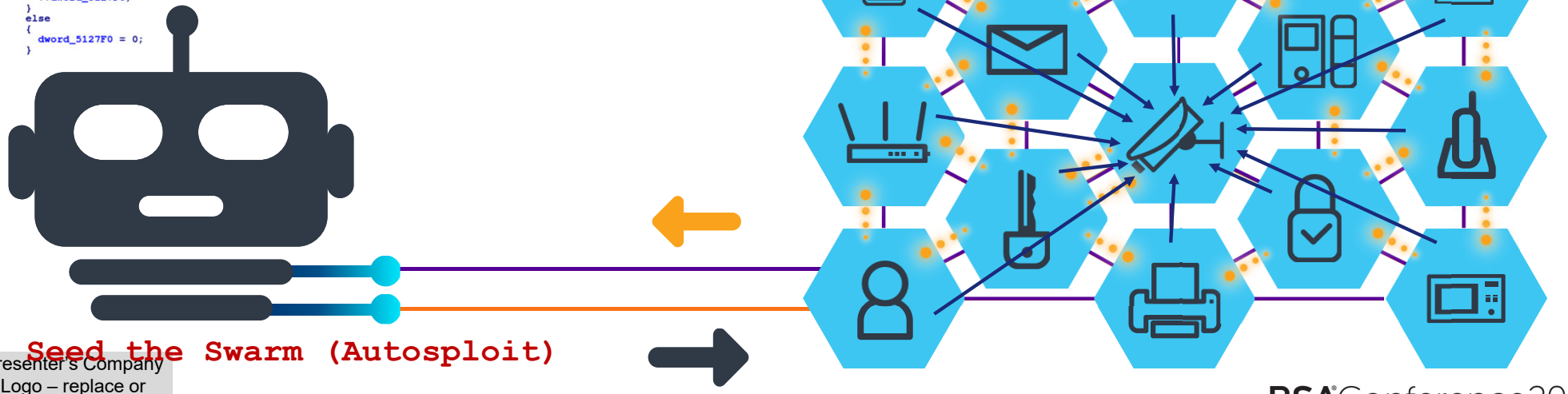
3) Target is swarmed, penetrated

4) File information leaked through swarm (IP, etc)

READ FILE ——
ADD NEW TARGET ····
GATHERED DATA ——

'e's++IP:PORT

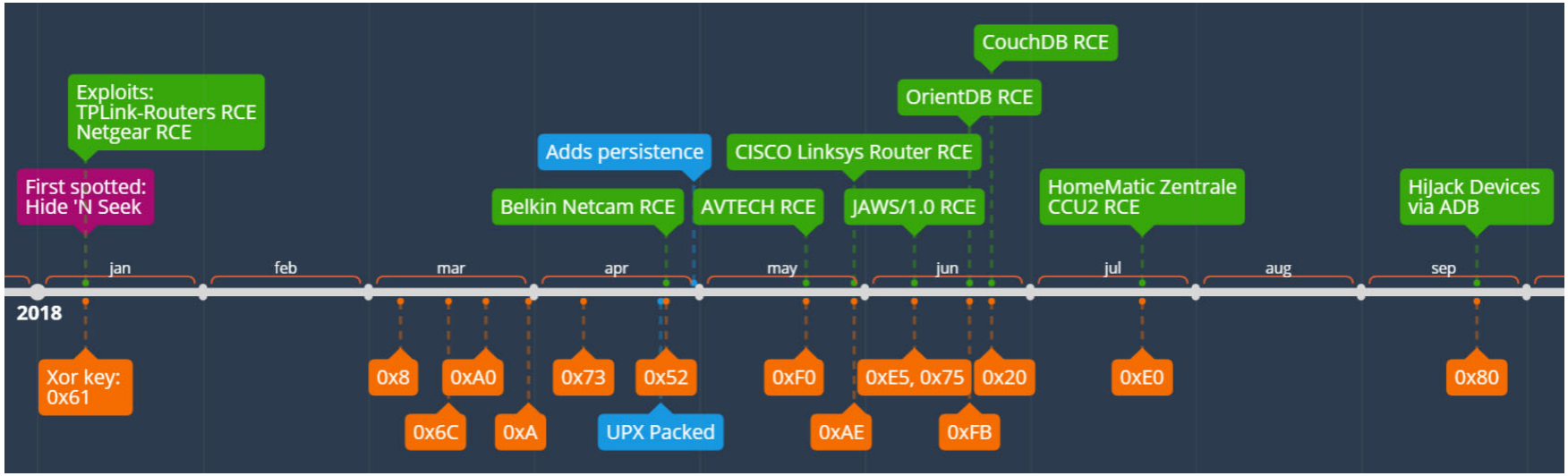
'm<data' ←→ Y<data>'



1) Seed the Swarm (Autosploit)

Hide and Seek Development Timeline

- Recap of Attack Chain/HNS/Swarm



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

1986: CRAIG REYNOLDS CREATES BOIDS AI SIM

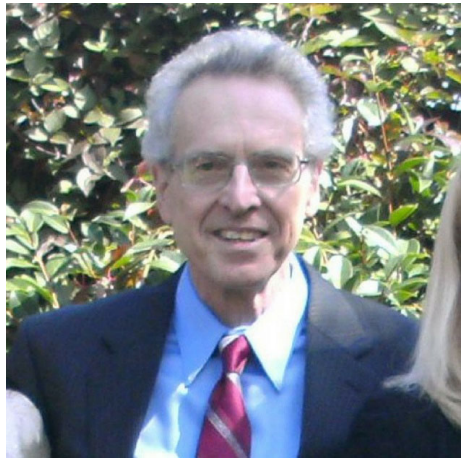
- Worked on Disney's 1982 Tron scene programming
- Artificial Life Simulation Program (1986)
- Program follows three simple rules
  - Collision Avoidance
  - Velocity Matching
  - Flock Centering Rules
- Used in computer modeling for video games,
  eg. 1998 Half-Life flying birds
- 2014: Algorithm adopted for autonomous deployment of
  Micro Aerial Vehicles (MAVs)
  - Aims for collision free, autonomous surveillance system

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

ORIGINAL 1986 BOID LIFE SIMULATION MODEL

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

1989: SWARM INTELLIGENCE IS COINED

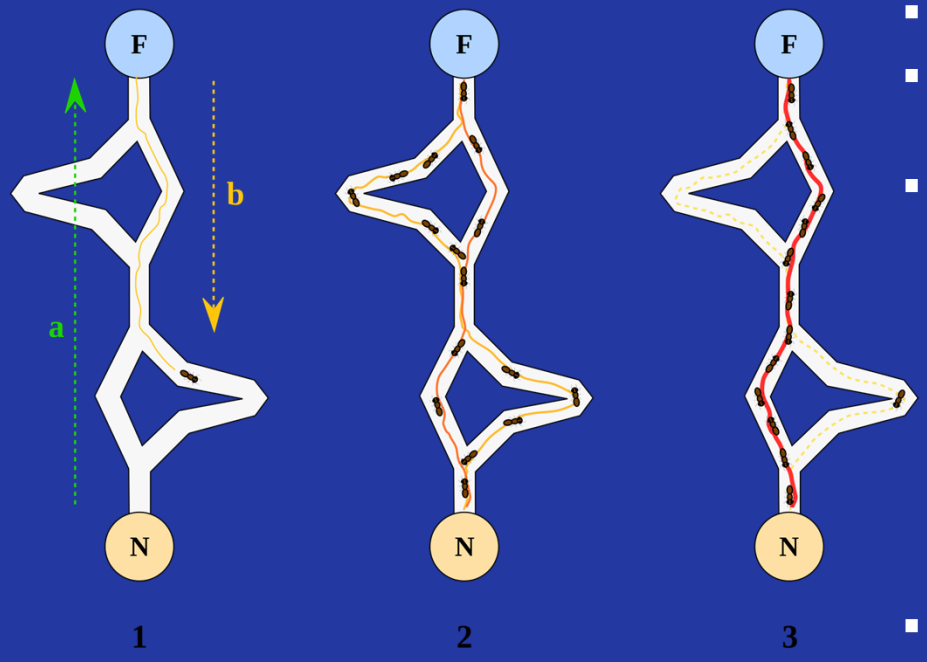


DR. GERARDO BENI
Distinguished Technical Staff Member,
AT&T Bell Labs 1983

- Dr. Gerardo Beni & Jing Wang (1989) coined the term at NATO Advanced Workshop on Robots & Biological Systems
- Member of Editorial Board “Swarm Intelligence”
- 1993: From Swarm Intelligence to Swarm Robotics
  - Paper on Swarm Intelligence in Cellular Robotic Systems (Beni)
- Self Organized Systems Research Groups now Exist

ANT COLONY OPTIMIZATION

Form of Swarm Intelligence



- **Shortest Path Between Nest and Food**
- **Traveling Salesman Problem**
- **Nodes lay synthetic pheromones along edges of their paths**
- History
  - 1959: Stigmergy theory invented, behavior of nest building in termites
  - 1989: Ant Colony Optimization algorithm is born
    - Food behavior model implemented
  - 1994: British Telecommunications Plc publishes first application of ACO to telecommunication networks
- Applications include emergency vehicle response systems, planning & logistics, microchip manufacturing

ANT COLONY OPTIMIZATION

Pheromones Laid for Optimal Path in Maze

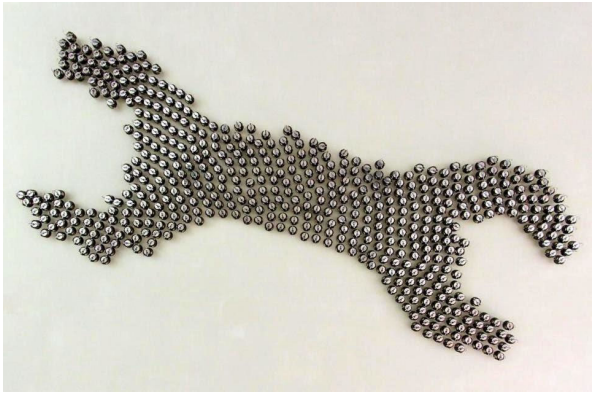
SOFTWARE EXAMPLES: SWARM ROBOTICS

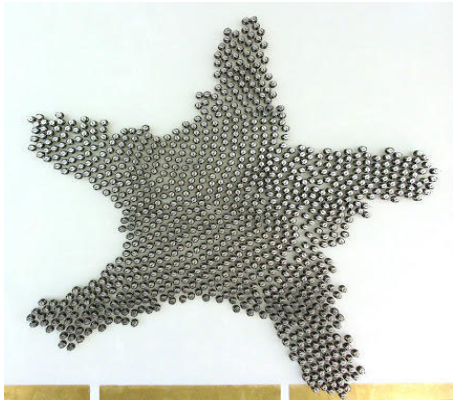
Self Organizing Systems Research Group

Kilobots: Headless swarm, no leaders

Follow solutions based approach

Work by communication through peer nodes

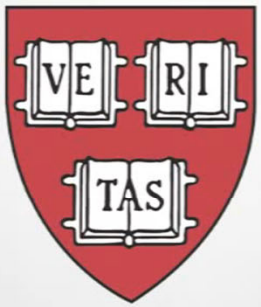




Presenter's Company Logo – replace or delete on master slide

HARVARD

UNIVERSITY



BOTNET BUILDING BLOCKS

Typical Botnet Components

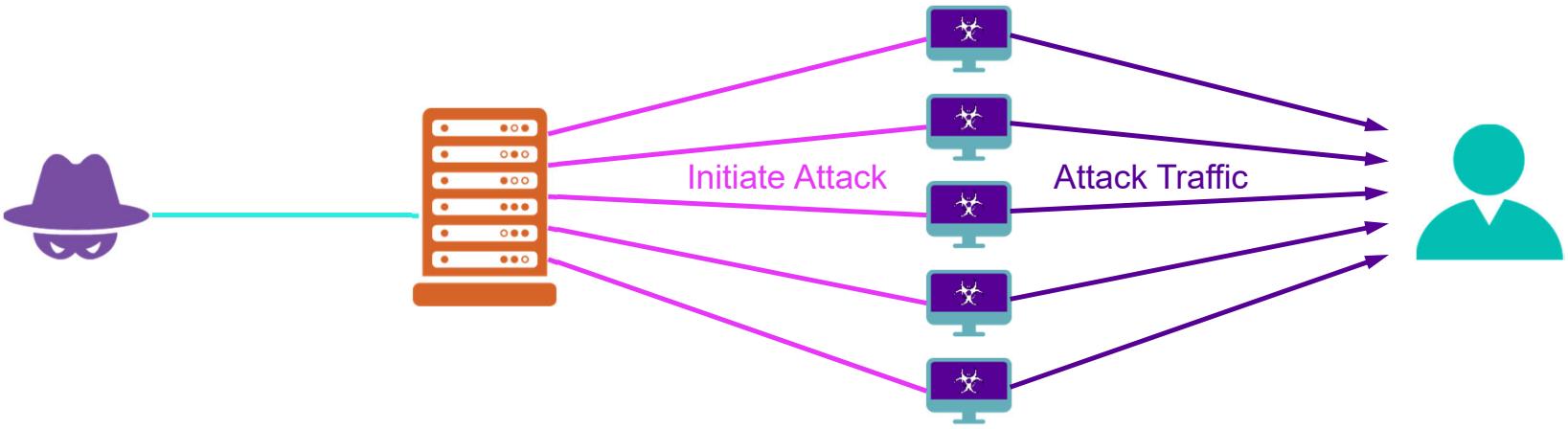
Attacker
(botmaster, herder)

C&C Server

Zombies

Victim / target

Communications
channels



BLACKHAT SWARMS – REMOVING THE C2

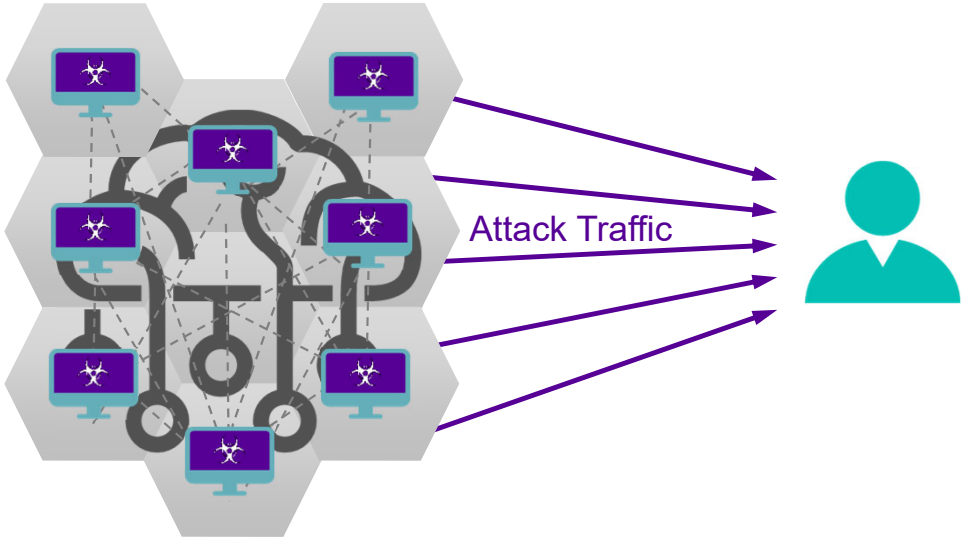
Next Generation Botnet 3.0: Swarm

What if Botnets could utilize swarm intelligence?

- Largely Accelerated Attack Chain
  - **Human Out of Loop**
- Strengthened Blackhat Hive

Satori Botnet example

- If camera is hacked or under stress it skips the system if better targets are found (pheromones)

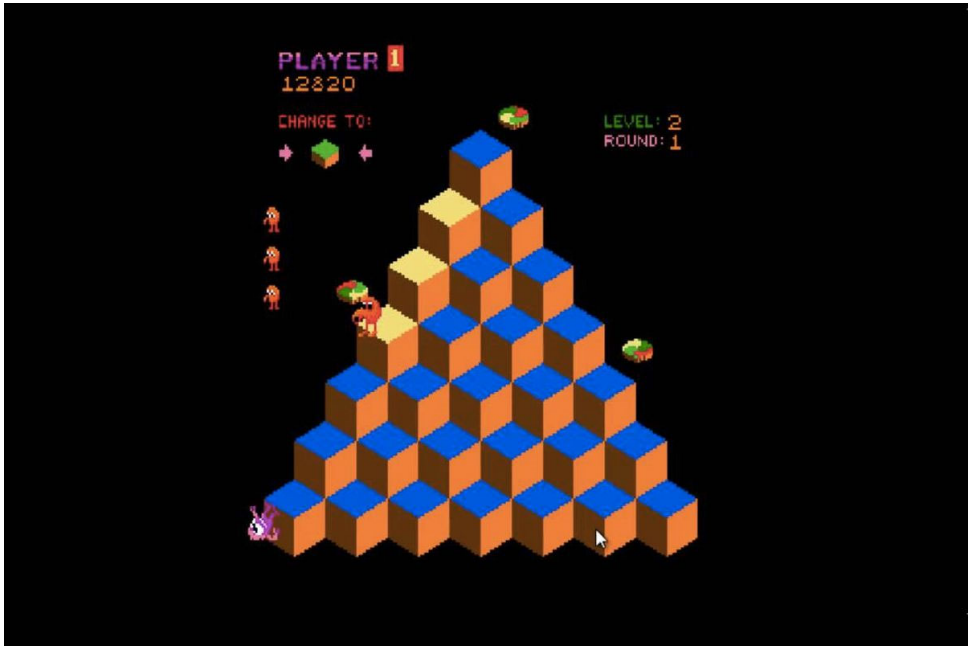


Presenter's Company Logo – replace or delete on master slide

INTENT BASED SOLUTIONS: SWARM NETWORKS

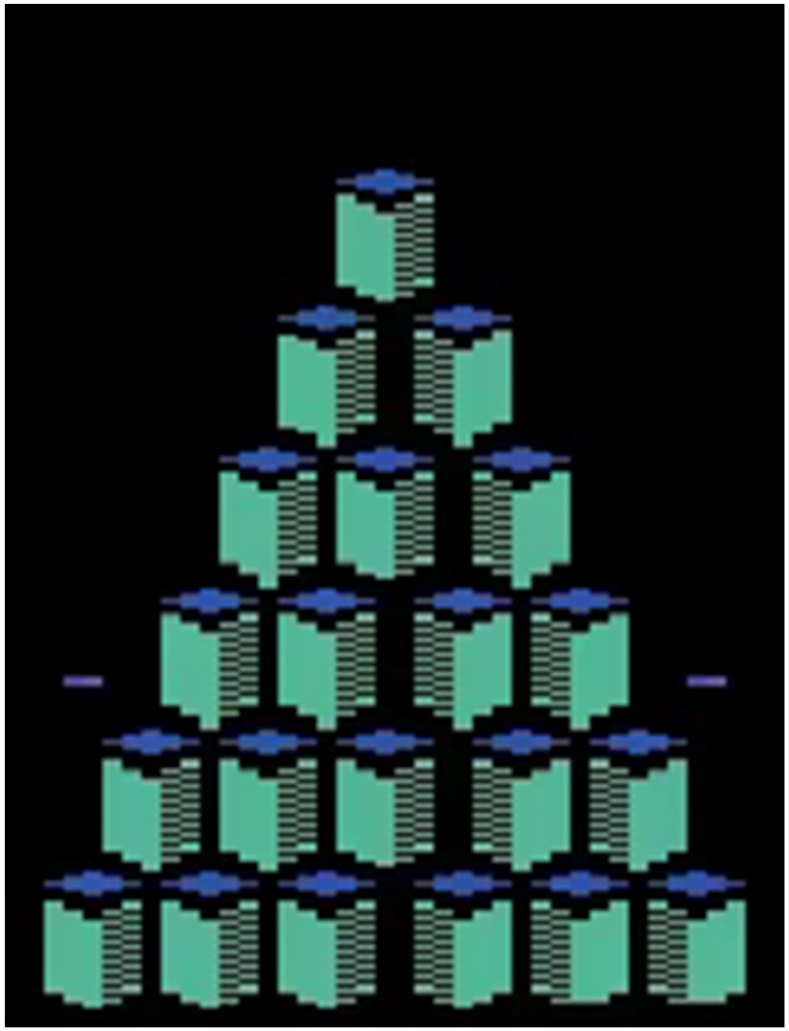
Mar 2018: Canonical ES Exploits Q*Bert

Intent Based AI: Get More Points	Q*Bert Designer Never Observed This Before	Swarm Attacks Will Follow This Path



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

MAR 2018: CANONICAL ES EXPLOITS Q*BERT



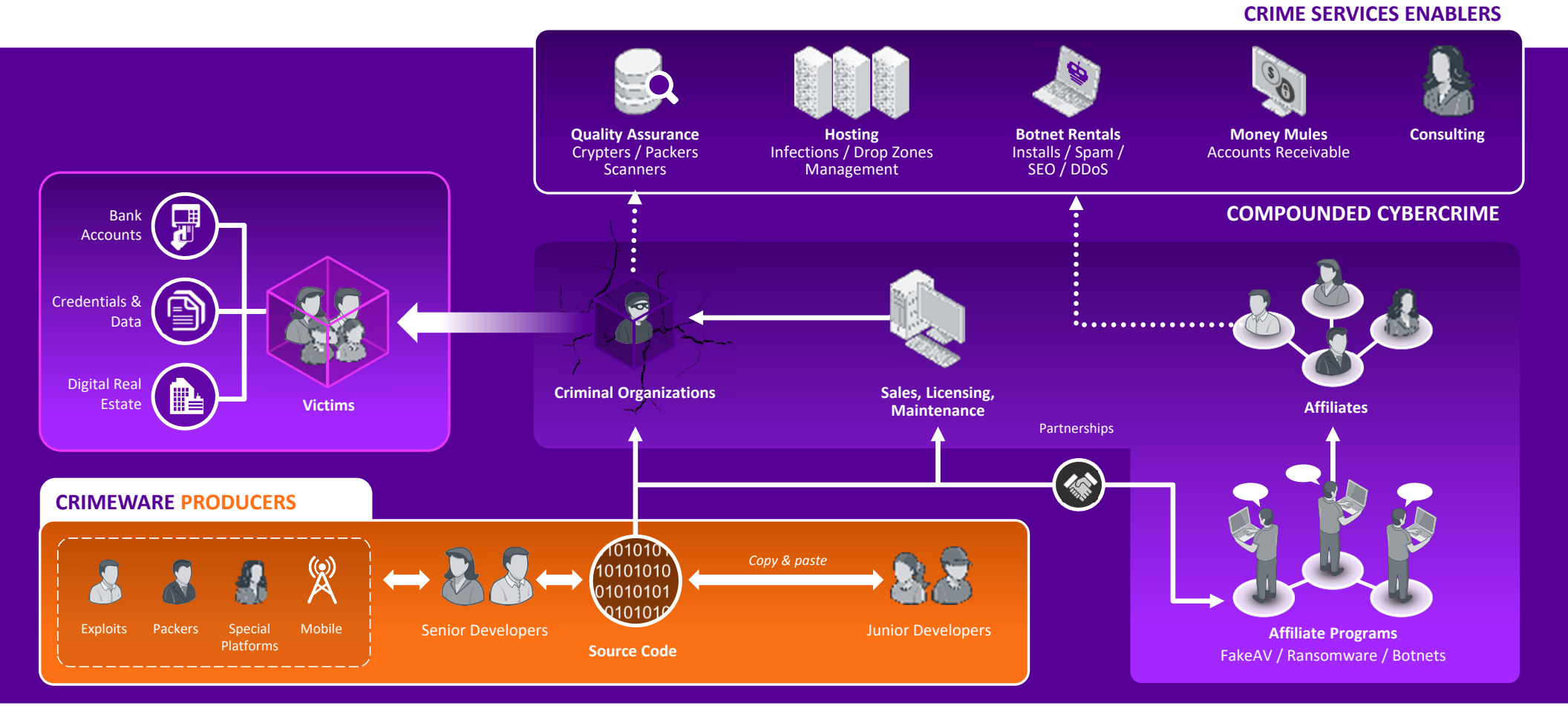
Presenter's Company Logo – replace or delete on master slide

RSAConference2019

Current Challenges

Humans are Slow – Gap in Cyber Security Resources

EVOLVING ATTACK CAPABILITIES THREAT LANDSCAPE



WIP

- Skills Gap Shortage
- Humans are Slow
- Data Vetting Problem

RSAConference2019

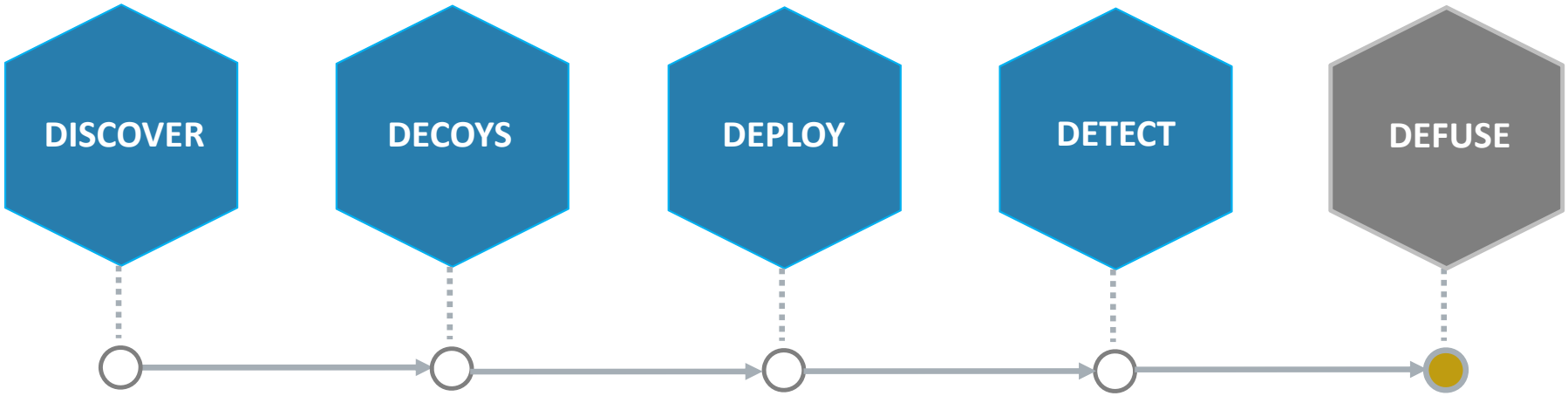
Strategic, Agile & Scalable Approaches

Viable Solutions to a Growing Problem

Prediction: Advanced Deception Tactics

Integrating deception techniques into security strategies that introduce network variations built around false information will force attackers to continually validate their threat intelligence, expend time and resources to detect false positives, and ensure that the networked resources they can see are actually legitimate.

Deception Based Approach



- Automatically discover network and assets
- Config. monitoring IPs

- Build decoy profiles
- Real OS and services indistinguishable from real assets

- Automatically places decoys in the monitored networks
- Install tokens (breadcrumbs) in real assets

- Real-time alerts from decoy access
- Analyze and correlate of threat activities

- Automatically quarantine or block attacks

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

Protect. Disrupt. Elevate.

CYBER THREAT ALLIANCE

For more information on becoming a CTA member, reach out to:
newmember@cyberthreatalliance.org

CYBER THREAT ALLIANCE

Michael J. Daniel – CEO & President

Board of Directors - Founding Members

Check Point SOFTWARE TECHNOLOGIES LTD.

CISCO

FORTINET

intel Security

paloalto NETWORKS

Symantec

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

Who We Are

Our members include some of the leading cybersecurity providers from around the world, representing many different approaches and points of view.

Charter Members

Check Point SOFTWARE TECHNOLOGIES LTD
cisco
FORTINET
McAfee
paloalto NETWORKS
Symantec

Affiliate Members

DRAGOS
Eleven Paths
INTSIGHTS
JUNIPER NETWORKS
NEC
NTT Security
RAPID7
SAINT SECURITY
SK infosec
SOPHOS

Contributing Members

ALIEN VAULT
lastline
radware
REVERSING LABS

Presenter's Company Logo – replace or

Data Quality

Our members include some of the leading cybersecurity providers from around the world, representing many different approaches and points of view.

- CTA Data Quality Working Group Discussion
- TODO: Add CTA Results for Data Vetting / Quality Program for CTA Platform Automation, Sharing of IOCs

Magellan Collaborative Platform Slide

Slide on Industry Experience Moving from STIX v1.2 to STIX v2.0

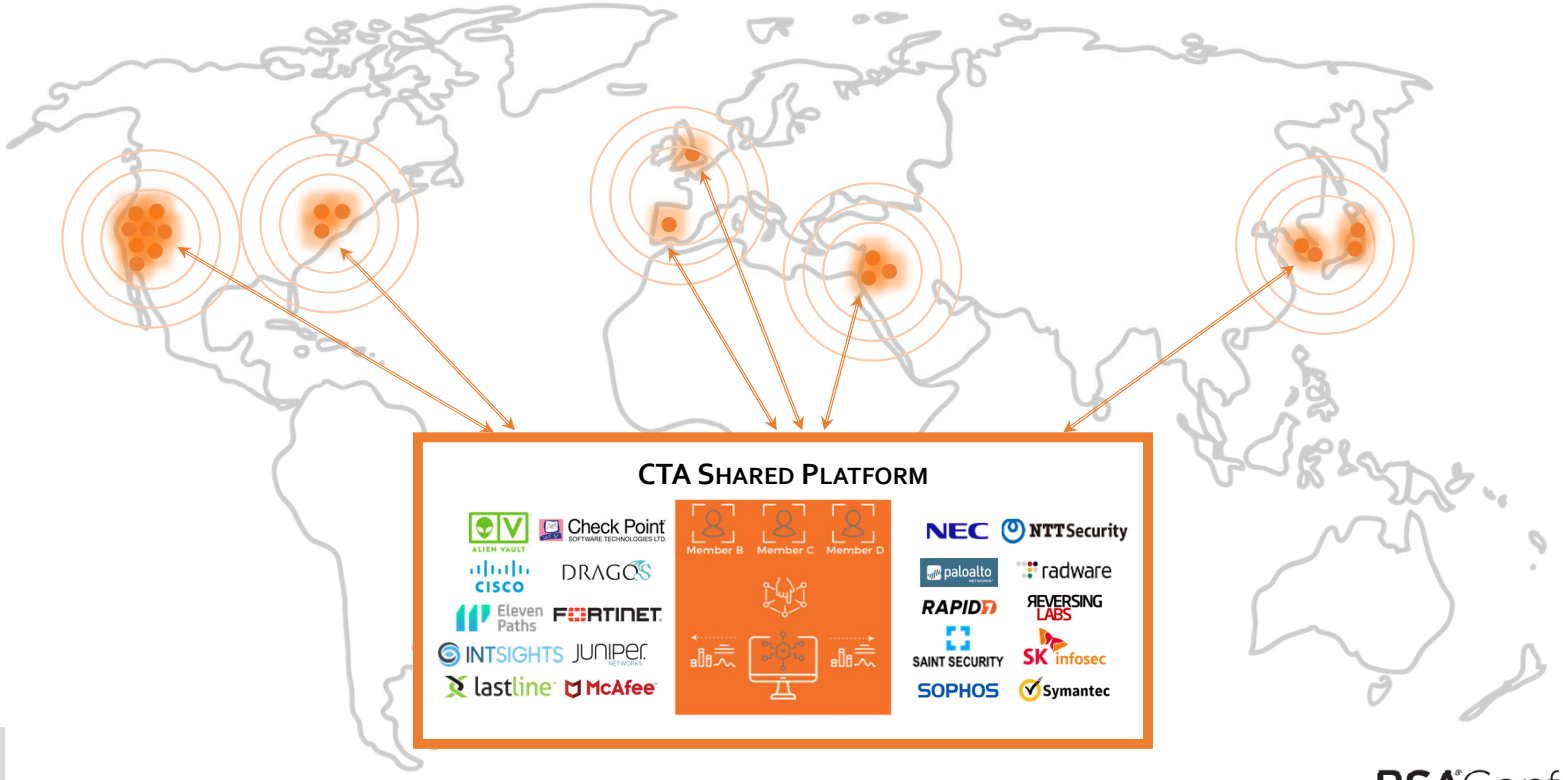
- CTA Has Used STIX to Map Killchain, Reward Speed
- Evolution Discussion from Norman Framework -> STIX 1.2 -> STIX 2.0
- MITRE ATT&CK Usage with CTA
- Early Access Automation – STIX v2 Embargo Concept & Implementation Discussion

Presenter's Company Logo – replace or

Protect End-Users

Global Impact

CTA is the industry's first formally organized group of cybersecurity practitioners that work together in good faith to share threat information and improve global defenses against advanced cyber adversaries; ultimately, protecting customers in real-time.



Presenter's Company Logo – replace or

ABOUT CTA

RSAConference2019

Future Weaponization of AI

2019 and Beyond: Building Blocks of a Flash War

Prediction: Artificial Intelligence Fuzzing (AIF)

Machine learning to study code for vulnerabilities via fuzzing, and automate subsequent exploitation.

Prediction: Zero-Days and AIF

Zero-day supply will increase, market value will decline.

Zero-Day Mining Using AIF

Zero-Day Mining-as-a-Service

Prediction: Poisoning Machine Learning

Machine learning data sets can be tainted to subvert AI defensive solutions.

RSAConference2019

Flash War Summary – Key Takeaways

It Does Not Have To Be Complex

Key Takeaways

- Humans need to be *repurposed* not *replaced*
  - Think about existing cycles that can be replaced with simple automation & orchestration
- Deception can be simple
  - Start with deployment of decoy systems within network
- Strengthen your kill chain, *taper the attacker*
  - Run automated red tests and evaluate time to breach window
  - Refactor and repeat tests, attempt to increase window

RSAConference2019

THANK YOU

/in/derekmanky