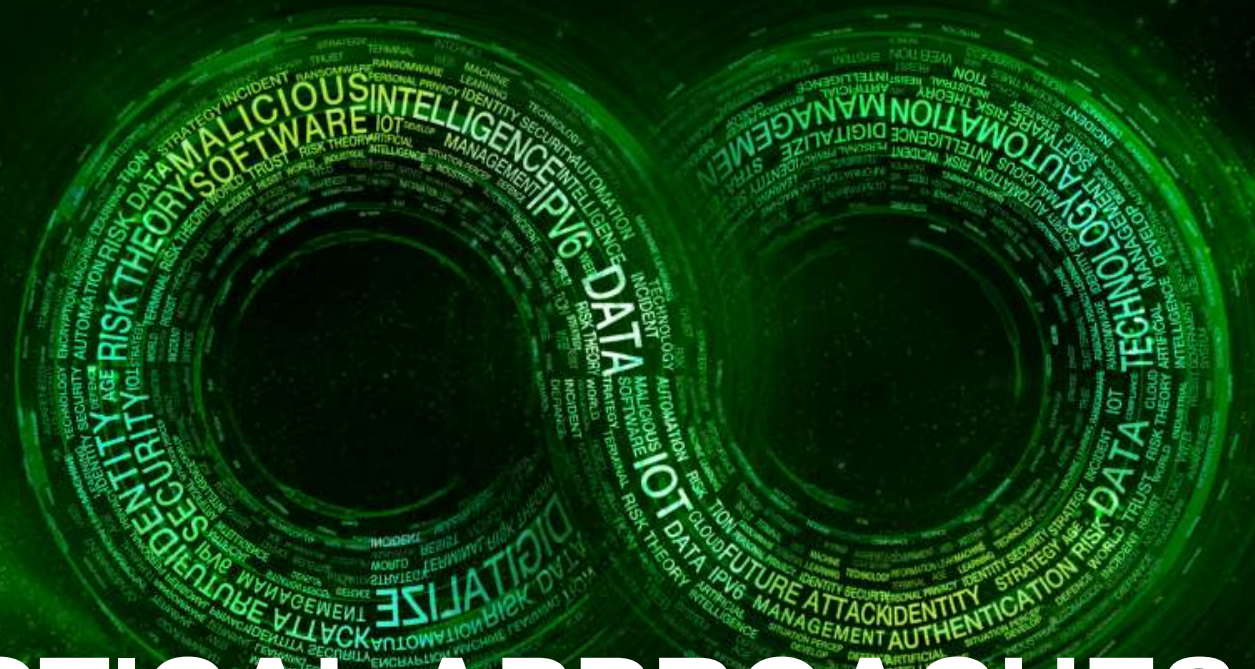


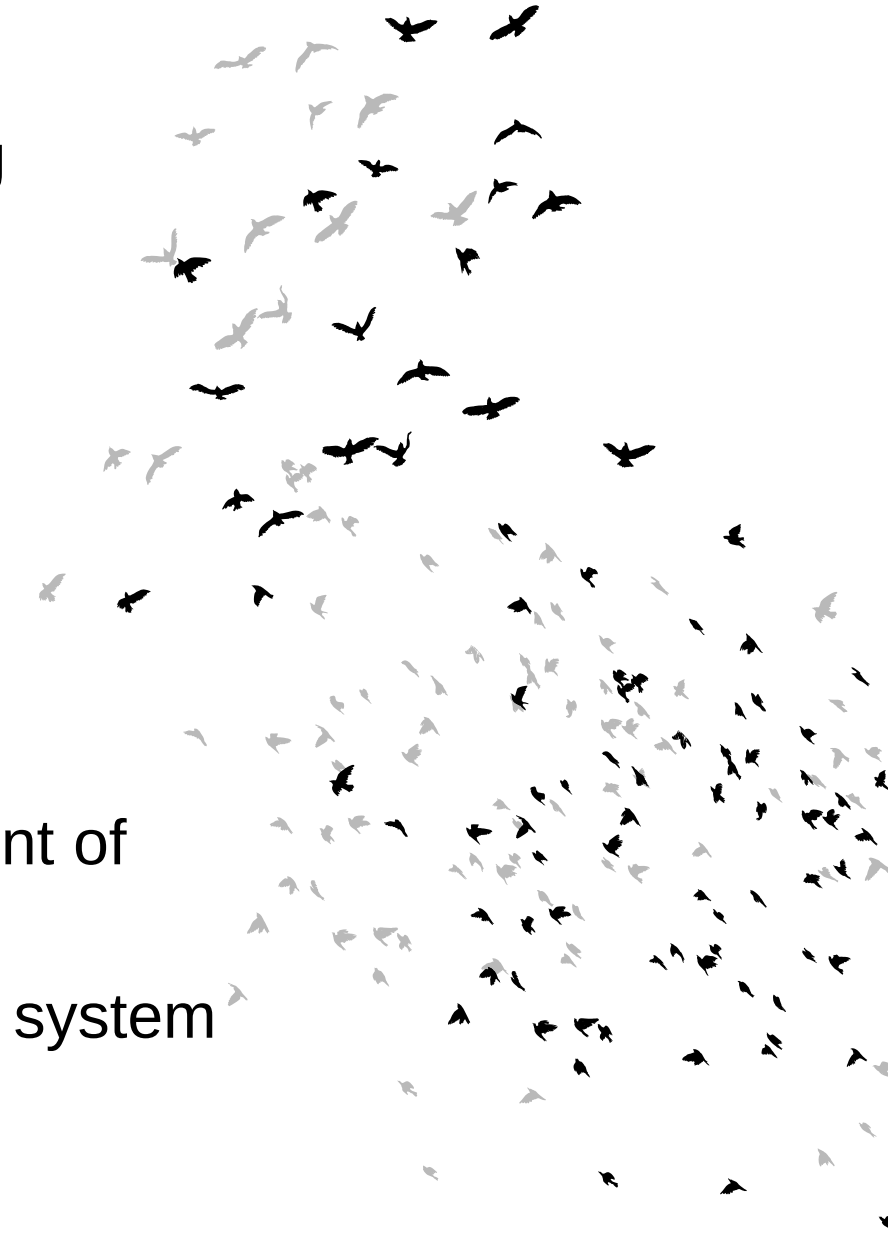
TACTICAL APPROACHES VS. SELF ORGANIZED SWARMBOTS

Derek Manky Chief, Security Insights - Fortinet

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原中国互联网安全大会）

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



Original 1986 BOID Life Simulation Model

1989: Swarm Intelligence is Coined

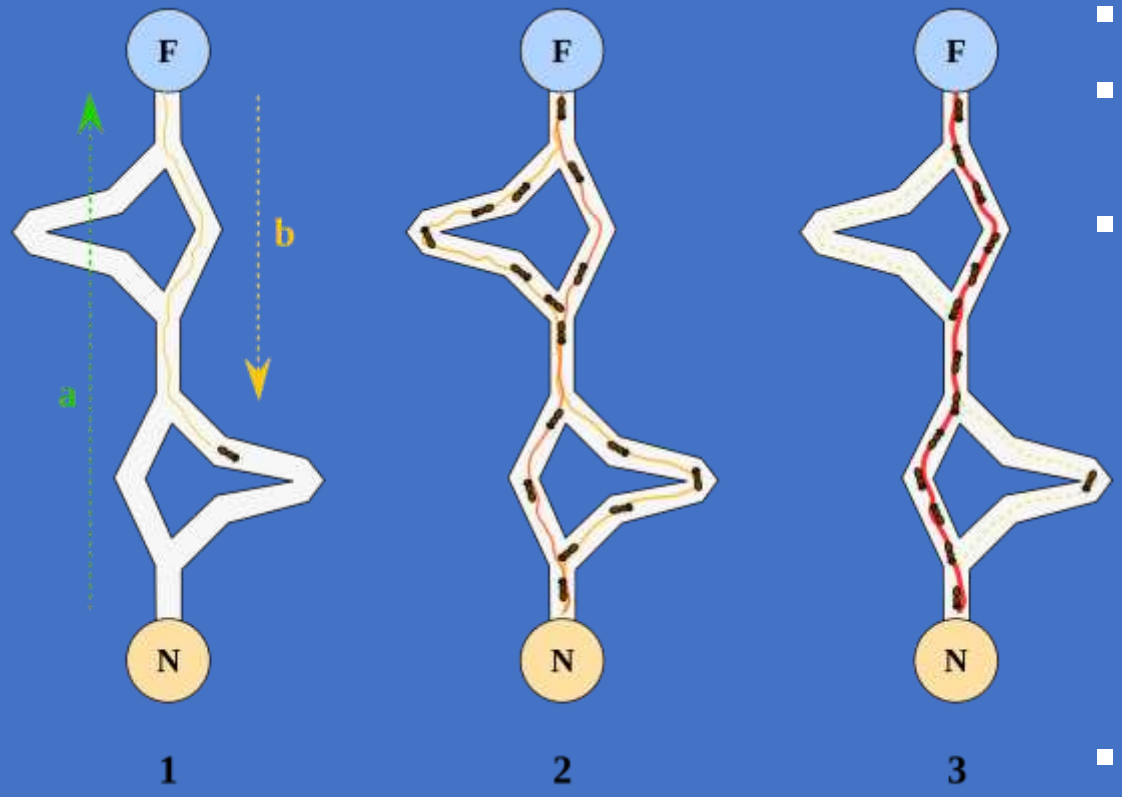
DR. GERARDO BENI

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

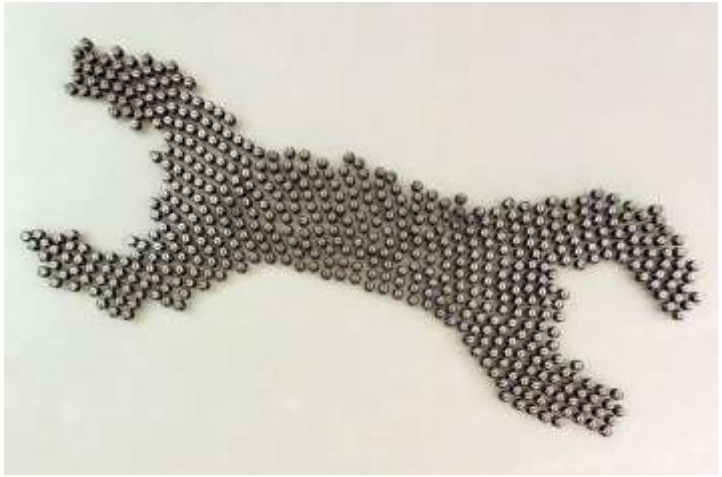
Software Examples: Swarm Robotics

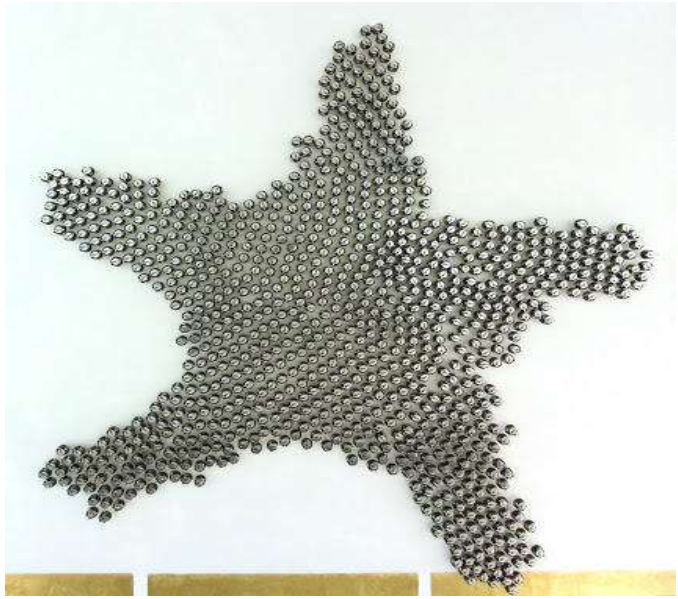
Self Organizing Systems Research Group

Kilobots: Headless swarm, no leaders

Follow solutions based approach

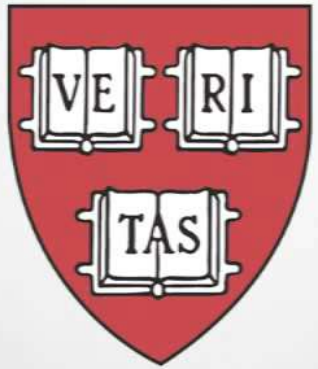
Work by communication through peer nodes





HARVARD

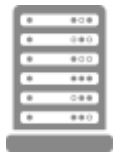
UNIVERSITY



Botnet Building Blocks

Typical Botnet Components

Attacker
(botmaster, herder)

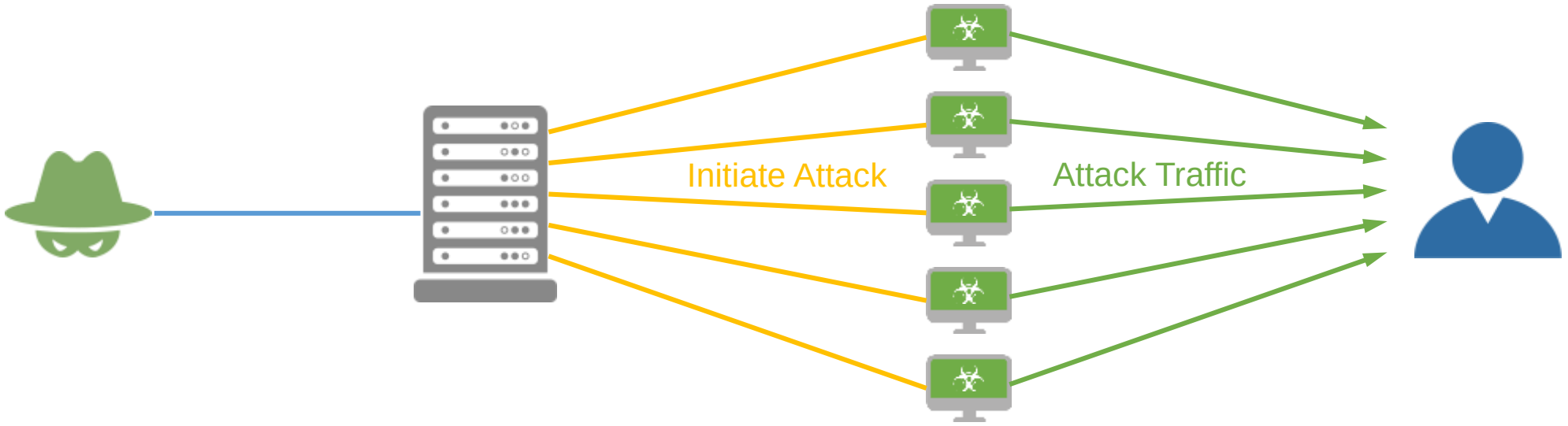


C&C Server

Zombies

Victim / target

Communications
channels



Blackhat Swarms – Removing the C2

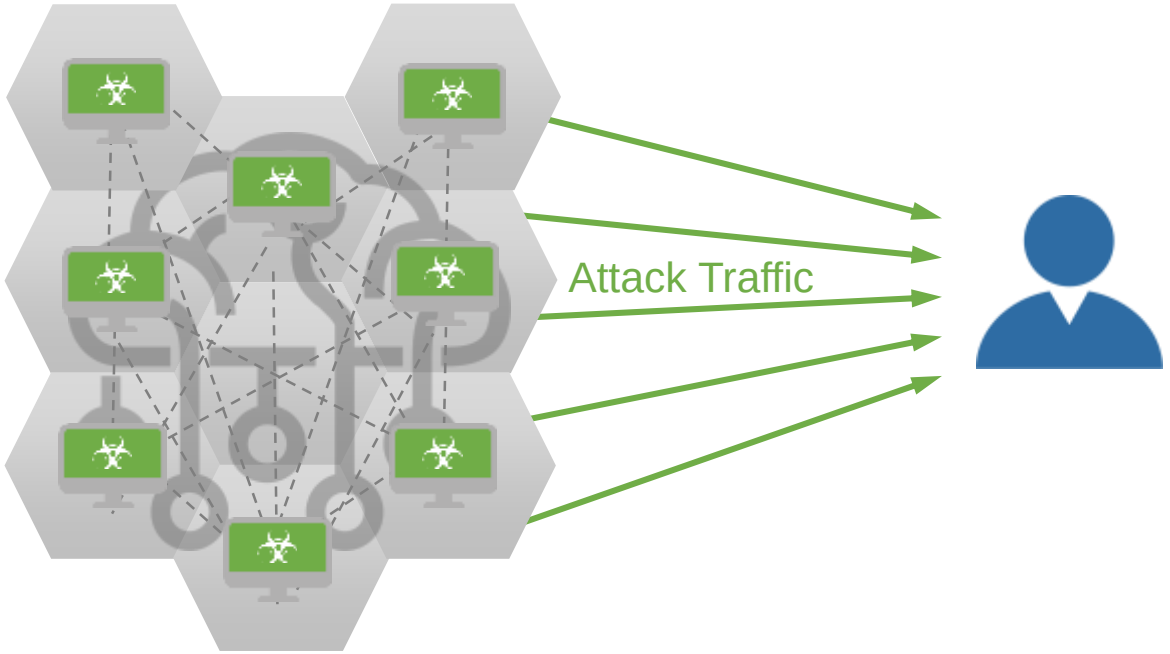
Next Generation Botnet 3.0: Swarm

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)



Botnet Attach Nodes

Victim

Hide and Seek

```
arg = (char *)v6[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 == 'a' )               // 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

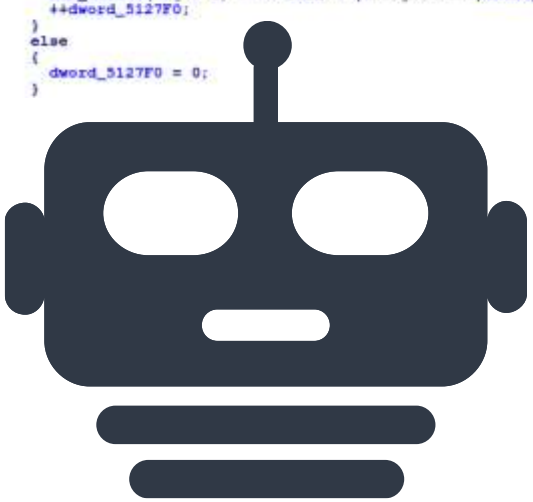
4) File information leaked through swarm (IP, etc)

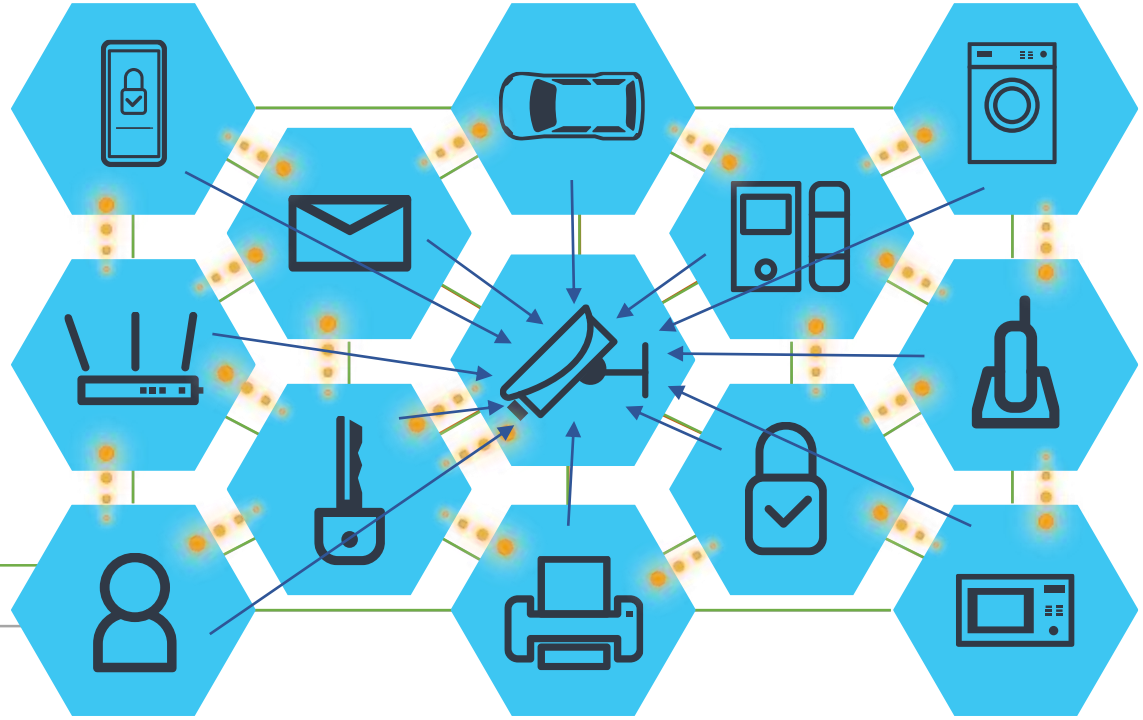
READ FILE

ADD NEW TARGET

GATHERED DATA

‘m<data>IP<PORT<data>’





1) Seed the Swarm (Autosploit)

ZERO TRUST SECURITY

Intent Based Solutions: Swarm Networks

Mar 2018: Canonical ES Exploits Q*Bert

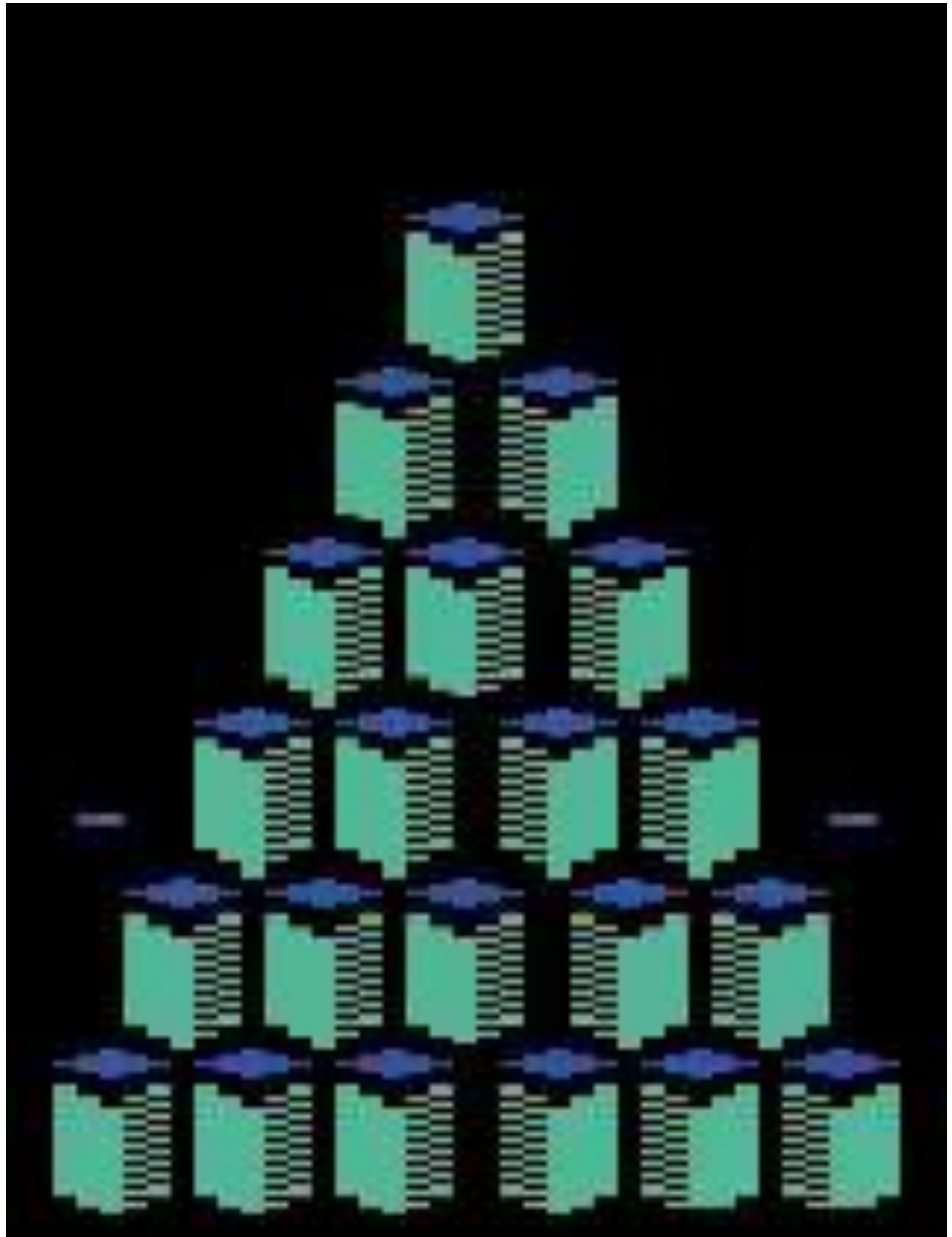
Intent Based AI: Get More Points

Q*Bert Designer Never Observed This Before

Swarm Attacks Will Follow This Path

S Exploits Q*Bert

Mar 2018: Canonical ES Exploits Q*Bert



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

McAfee Together is power.

paloalto NETWORKS

Symantec

Who We Are

Our members are 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

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

Contributing Members

radware, REVERSING LABS

CTA's Strategic Objectives

Mission Statement: CTA is a not-for-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field.

Protect End-Users

Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real time.

Disrupt Malicious Actors

We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

Elevate Overall Security

We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-users' resilience.

What Makes CTA Unique

The CTA Model

The CTA solution employs technology, incentives, and business rules to differentiate from traditional models. CTA's automated information sharing process enables members to share high volumes of data with context at machine speed.

THE CTA SOLUTION

- **An automated information sharing platform** that enables members to share more types of data, at higher volumes, more quickly
- **A scoring algorithm** that assigns points for submitting an indicator, providing context, and mutual validation of other members' submissions
- The scoring algorithm is designed to be **equitable for all members** and is regularly reviewed and updated based on information sharing trends
- Members are required to submit a minimum value of 10,000 points per day each day to **prevent the free-rider problem** prevalent in other information sharing organizations

OUR SHARING PROCESS

Step 1: Members enter linked intelligence into their local client using the API or web interface.

Step2: STIX formatted data transferred to central hub over TAXII/HTTPS.

Step 3: STIX package scored according to algorithm. Individual STIX elements stored in database back-end.

Step 4: Member systems poll central hub for new data, and sync the available information with their local database where it can be extracted and used.

Automated Sharing

Data Inputs

CTA's sharing process requires members to submit intelligence packages into a common format, runs it through a scoring algorithm, and enables members to extract the data most useful to them.

Platform Sharing Metrics

65,000 Average total packages per day shared across all members

85% Average percentage of packages with at least one observable, kill chain phase, and additional context / linked intelligence

1.5M Average total points per day across all members

Data Sharing

STIX Packages include a range of observables and TTPs across the kill chain

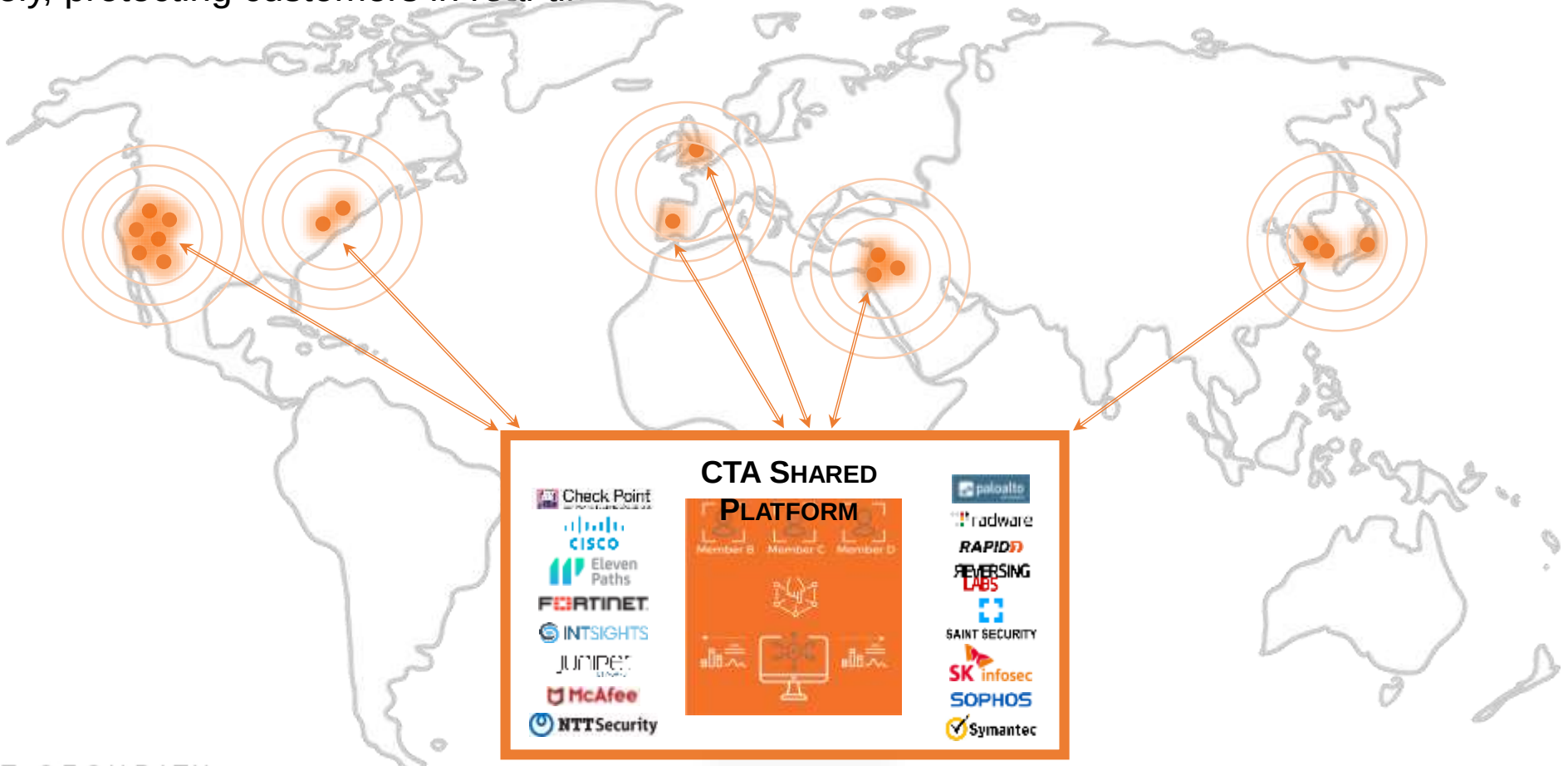
Observables: Files, URIs, Domain Names, and Addresses

TTPs: Over 50 TTPs from Mitre's CAPEC and ATT&CK frameworks

Protect End-Users

Global Impact

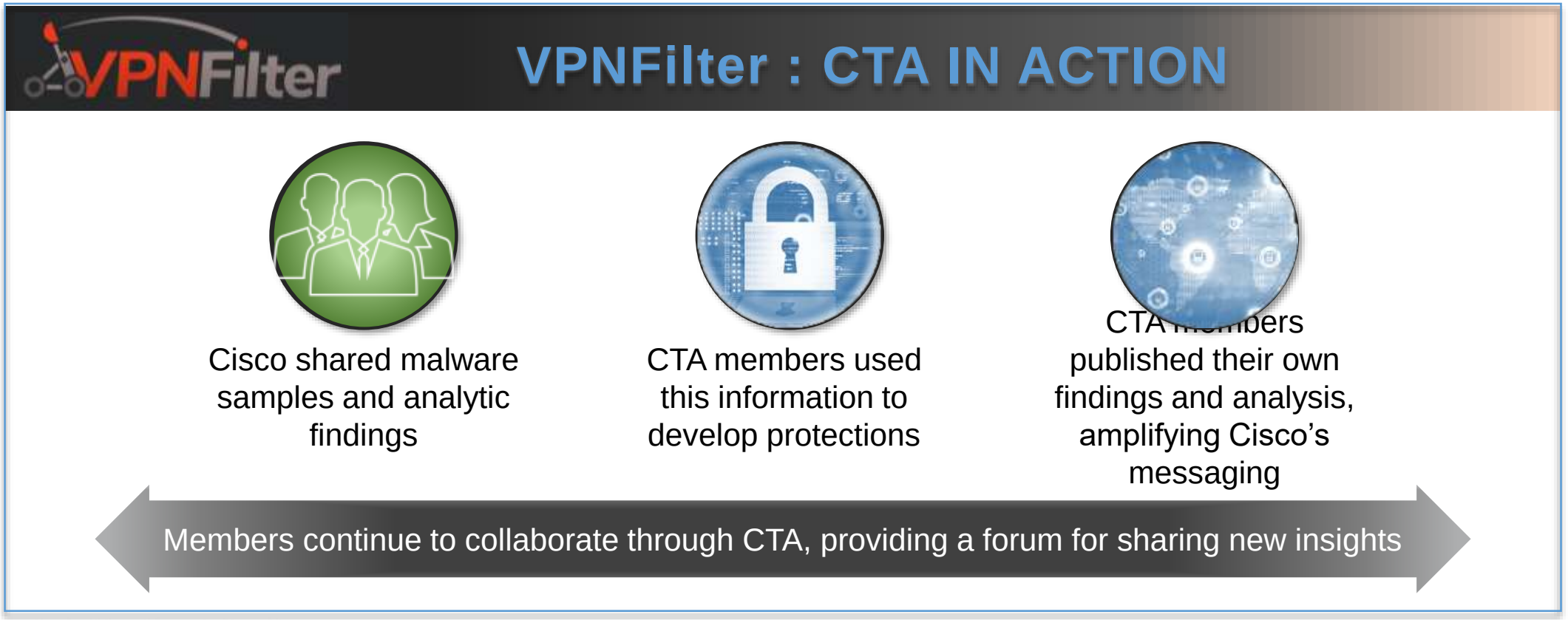
CTA is the industry's first formally organized group of cybersecurity practitioners that work together in good faith to share threat information and improve global defenses against advanced cyber adversaries; ultimately, protecting customers in real-time.



Disrupt Malicious Actors

Sharing information to enable more rapid deployment of protections

CTA enables members to share sensitive information on malicious activity, allowing members to bring together analytic insights on the activity, protect their customers as quickly as possible, and systematically disrupt adversary activity.



FLASH WAR: ARTIFICIAL INTELLIGENCE

FORTINET

THANKS

2018 ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原中国互联网安全大会）