RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: HT-W02

ORDER VS. MAD SCIENCE ANALYZING BLACK HAT SWARM INTELLIGENCE

Derek Manky

Global Security Strategist
Fortinet, Office of CISO
/in/derekmanky

FORTINET®

WAR GAMES

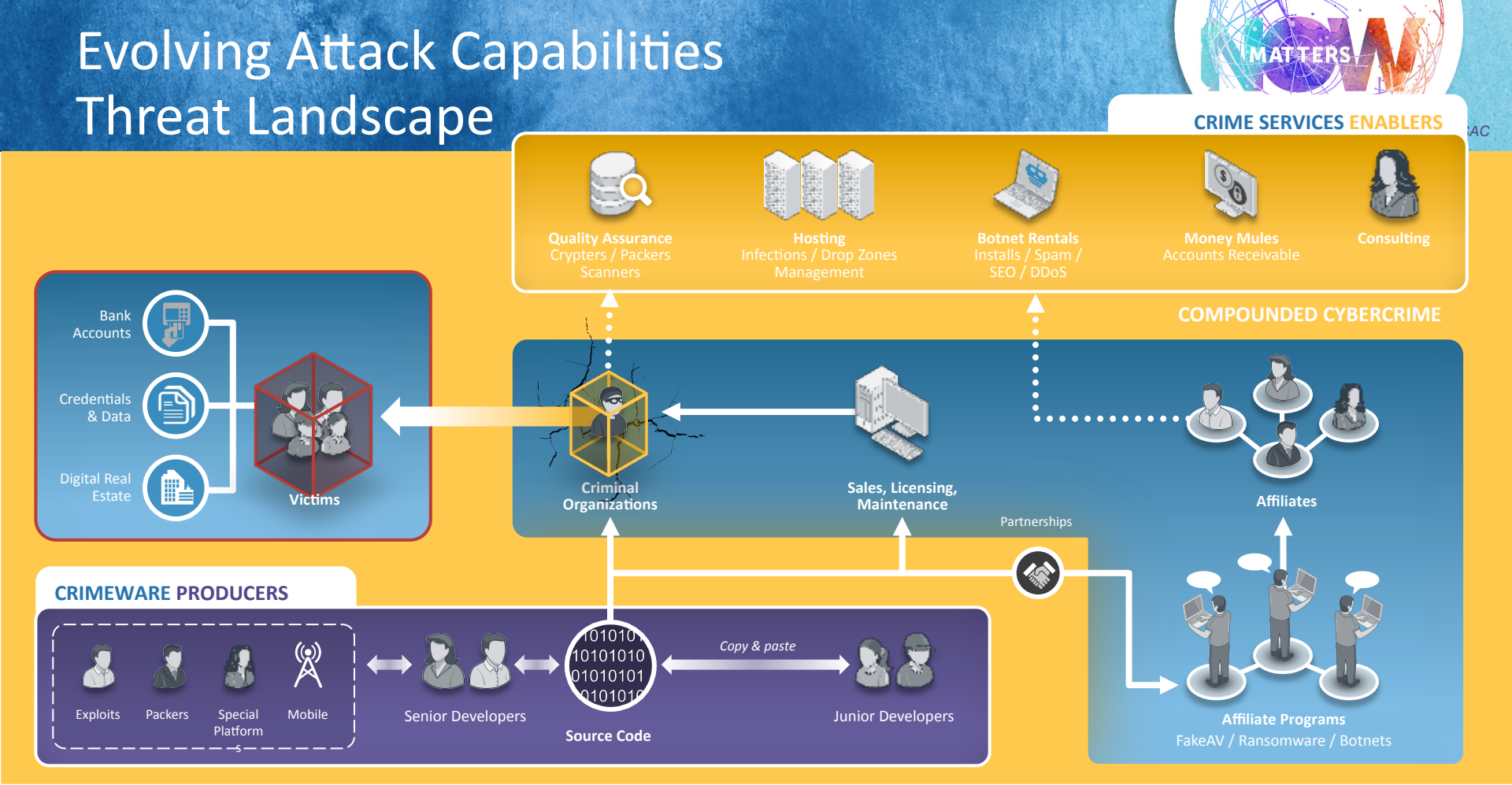
The Rise of the Machines

1971: Creeper – The First Computer Virus

- Experimental self-replicating program
- Written in **1971** to demonstrate a ‘mobile’ application
- Infected DEC PDP-10 computers running TENEX OS
- Just 1 year after Unix ‘Epoch Time’ began
- ‘Reaper’ worm created in ‘72 to delete it

1 January 1970 00:00:00 GMT → Epoch timestamp 0

Evolving Attack Capabilities
Threat Landscape



SPEED KILLS: SWARM BOTNETS

Accelerating the Attack Chain

Hit Me With Your Best Shot – Fire Away

Swarm – Individual Survival Using the Group

Collective behavior exhibited by entities, particularly animals

Similar size or same species

Aggregate together, usually moving together in some direction

Other Biomechanical Examples of Swarm Behavior

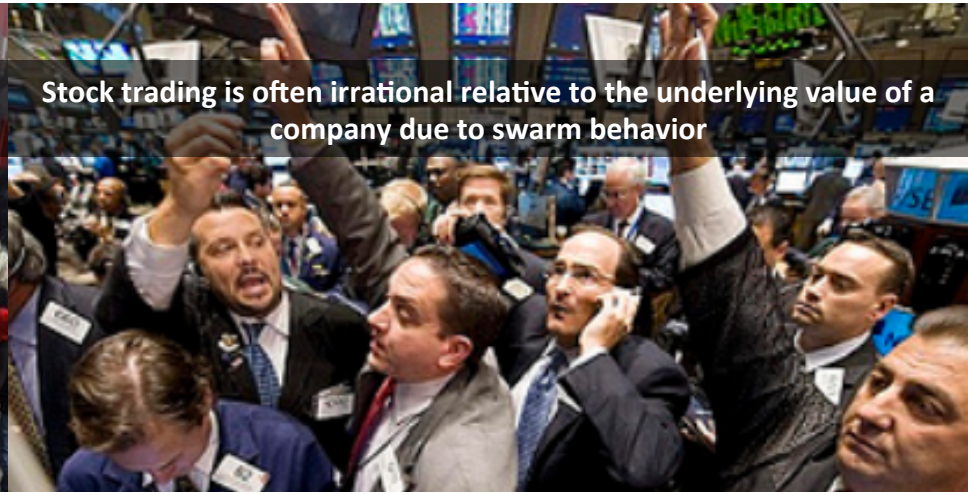
Humans also Behave in Swarm Fashion

Old saying – a person is smart, a crowd is not

Tend to exhibit swarm behavior depending on situation

Aggregate and size of grouping determines behavior

Group behavior can be radically different from individual behavior



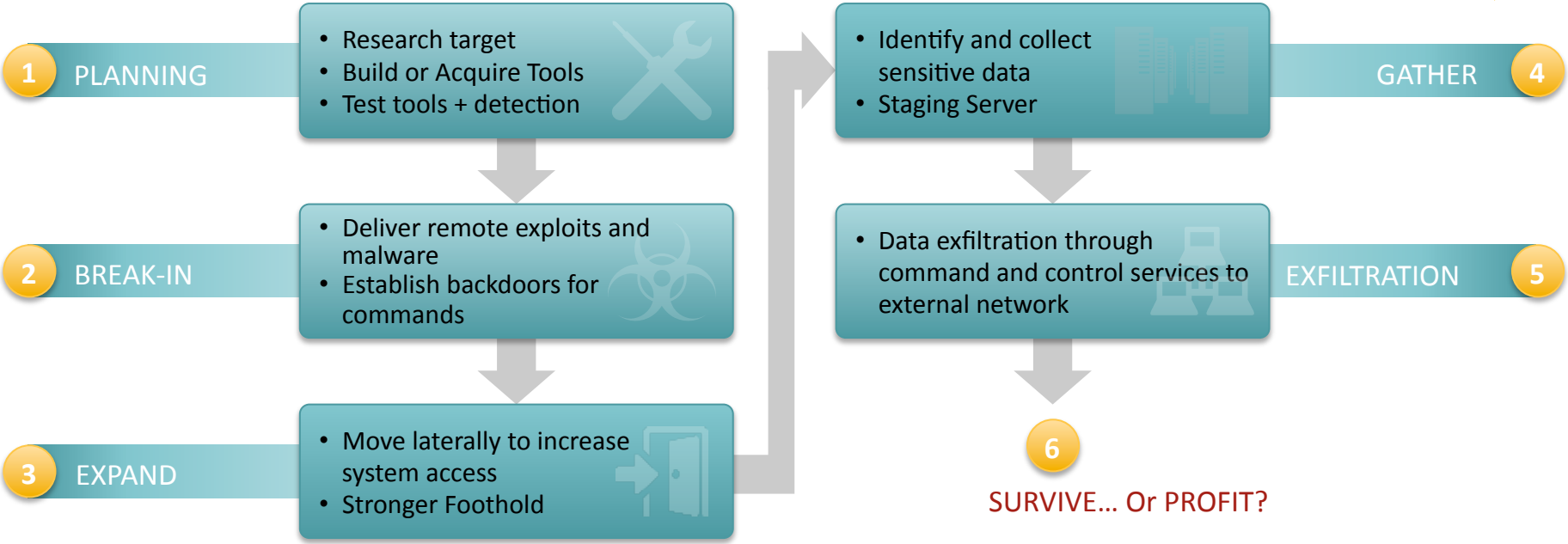
Stock trading is often irrational relative to the underlying value of a company due to swarm behavior

PREDICTION:

THE RISE OF SELF-LEARNING HIVENETS AND SWARMBOTS

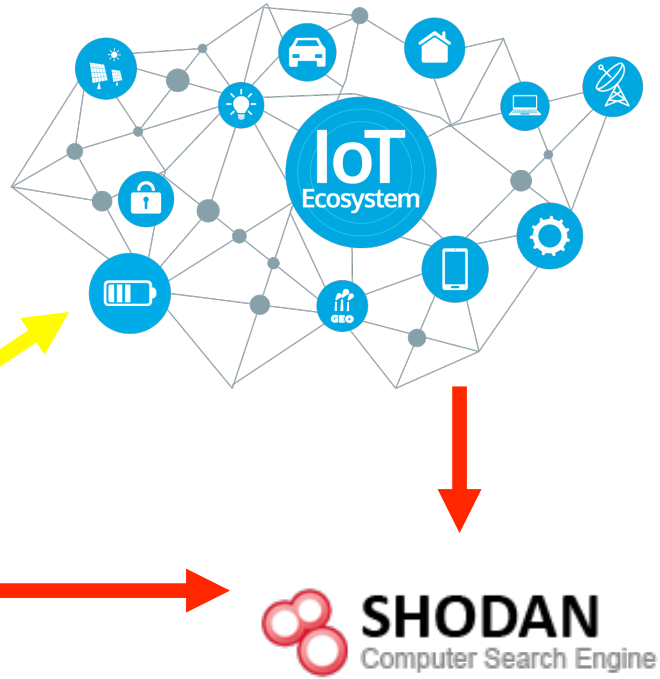
The Accelerated Attack Chain

Automation & Swarm Decrease TTB (Time to Breach)

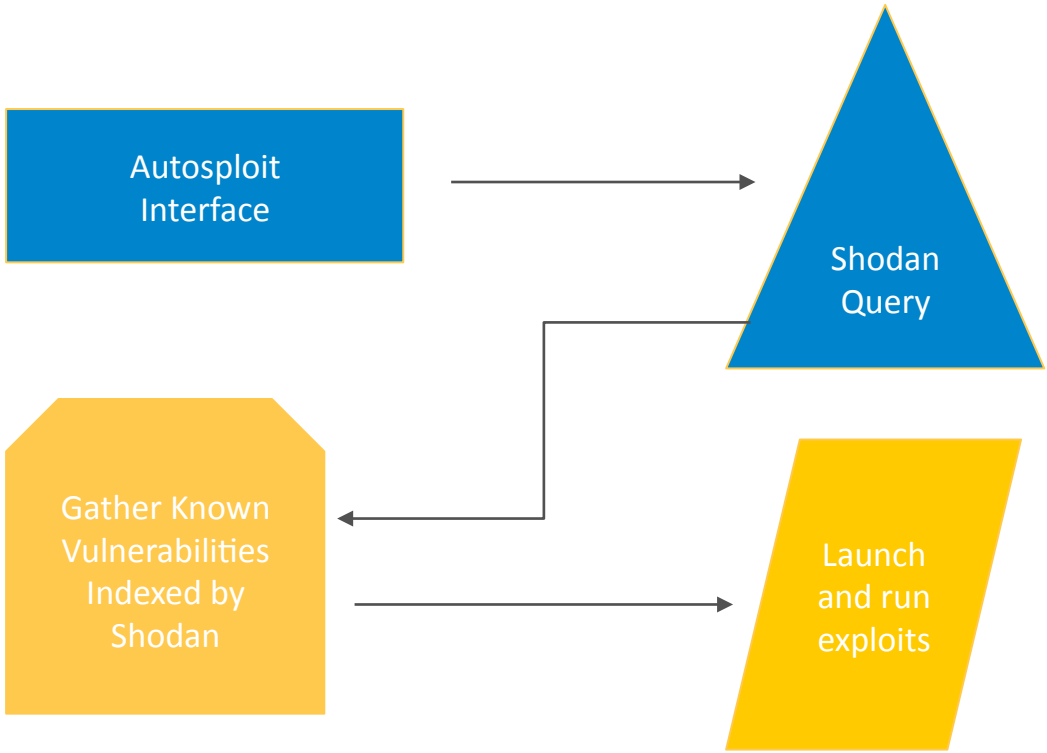


Autosploit – Building Swarms

- 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.



Autosploit Workflow



1. Attacker launches Autosploit script

2. Autosploit queries Shodan for known exploits

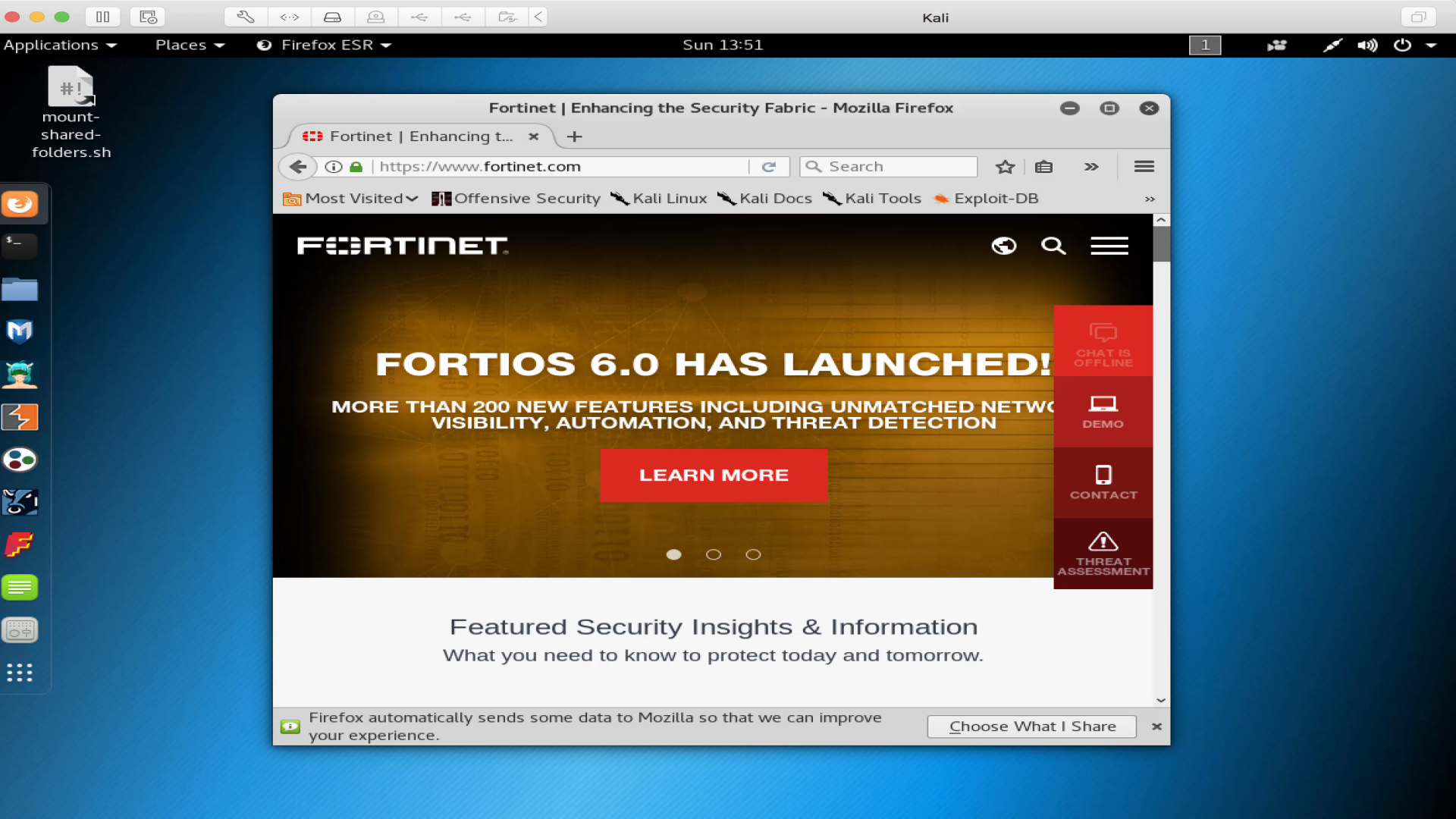
3. Autosploit uses intelligent matching (optional) to match additional exploits to ports and services

4. Autosploit configures metasploit as a "reverse listener" to launch an attack to a victim.

5. Victim connects back to the attacker's Autosploit, allowing (many times) for the attacker to bypass security measures

Problems with Autosploit

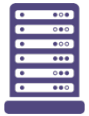
- **Easy to launch**
  - No real skills needed
  - No discrimination between hosts
  - Uses dangerous exploits that may crash/destroy sytems
- **Shodan**
  - Shodan uses hive functions by looking for similar systems with similar functions
  - Categorizes vulnerabilities
  - Allows users to search for vulnerable systems that are live


Kali
Applications
Places
Firefox ESR
Sun 13:51
mount-shared-folders.sh
Fortinet | Enhancing the Security Fabric - Mozilla Firefox
Fortinet | Enhancing t...
https://www.fortinet.com
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
FORTINET
FORTIOS 6.0 HAS LAUNCHED!
MORE THAN 200 NEW FEATURES INCLUDING UNMATCHED NETWO
VISIBILITY, AUTOMATION, AND THREAT DETECTION
LEARN MORE
CHAT IS OFFLINE
DEMO
CONTACT
THREAT ASSESSMENT
Featured Security Insights & Information
What you need to know to protect today and tomorrow.
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share

Botnet Building Blocks

Typical Botnet Components

Attacker
(botmaster, herder)

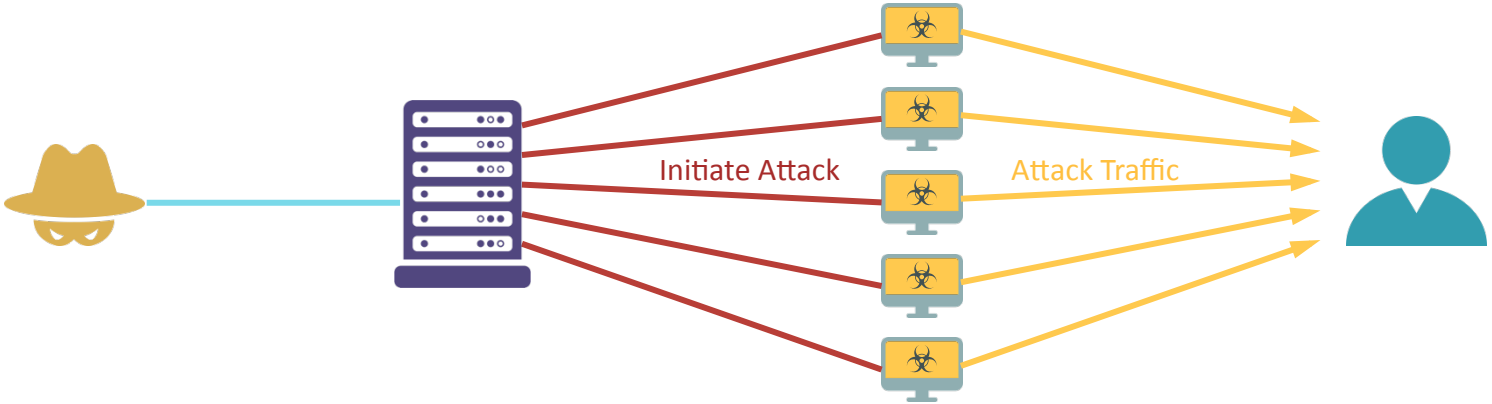


C&C Server

Zombies

Victim / target

Communications
channels



Blackhat Swarms – Removing the C2

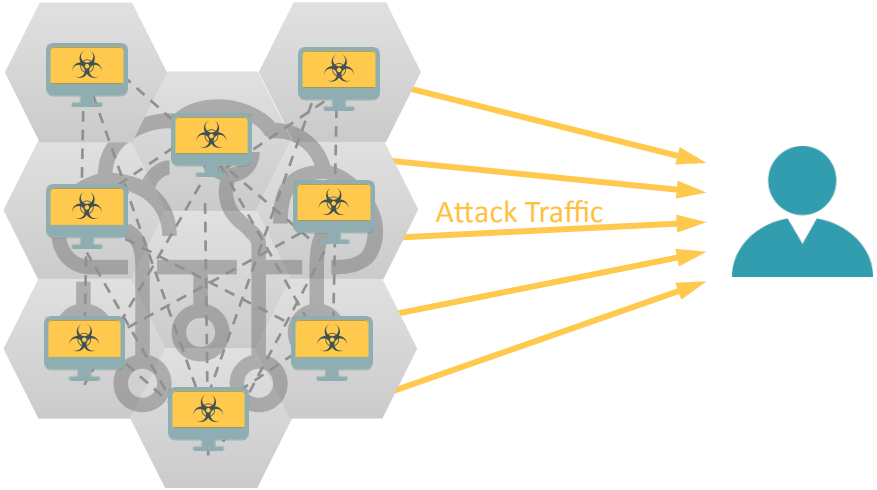
Next Generation Botnet 3.0: Swarm

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)

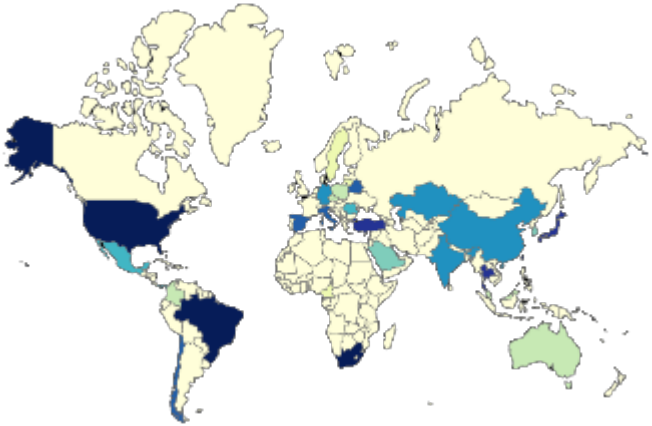


Frankenstein Malware

- Localized swarm behavior – code building blocks from legitimate running processes
- Semantic Blueprint contains malware goals
- Malware scans for existing underlining code in memory
- Malware uses pieces of code from various programs to create new malware
- Lua gives flexibility, add code
  - Debug in real-time

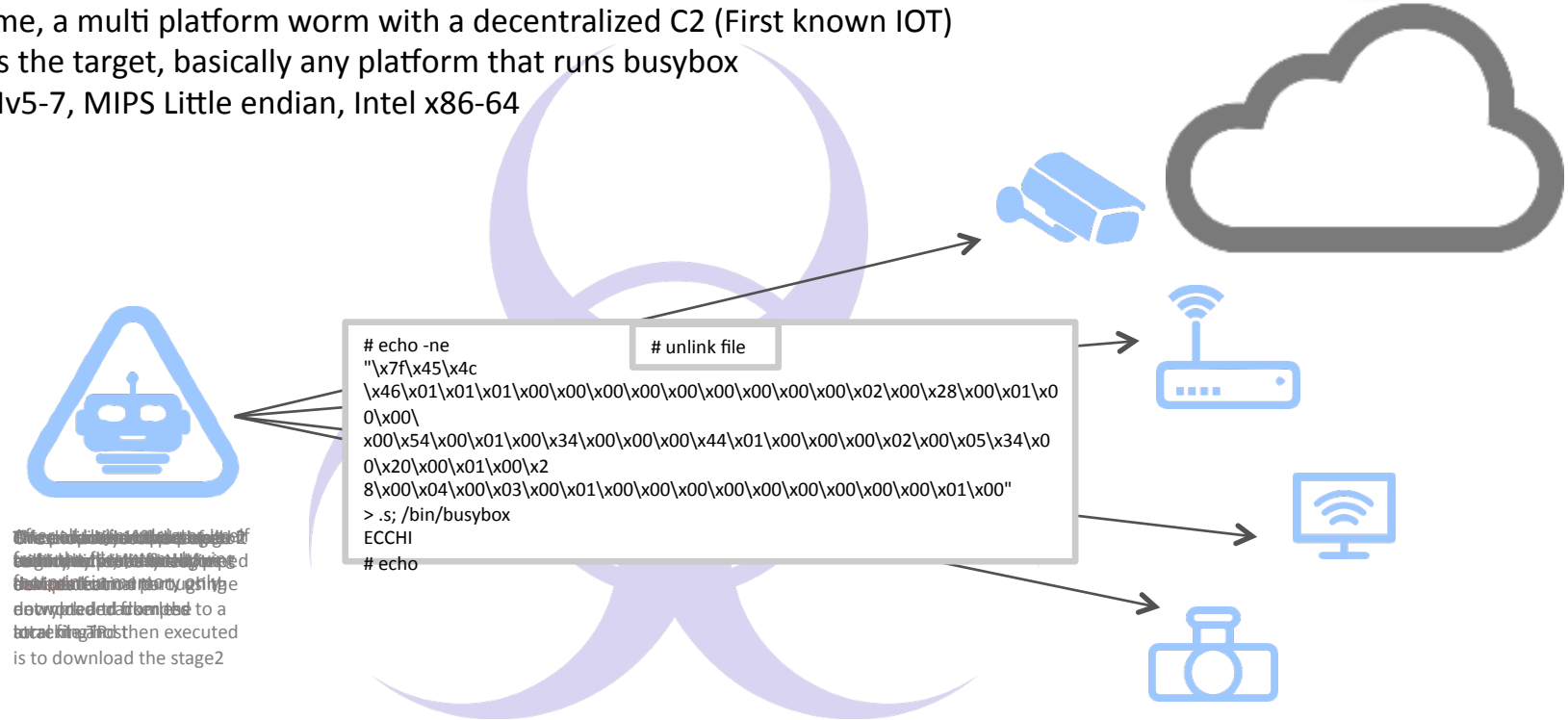
Hajime Precursor

- Intelligent IOT Botnet – Nine Platforms + x86
- TR-069 Exploit (MSSP/Telco Control)
- First detected October 25, 2016
- 30,000+ detections per day (FortiGuard)



Hajime Precursor

- Hajime, a multi platform worm with a decentralized C2 (First known IOT)
- IoT is the target, basically any platform that runs busybox
- ARMv5-7, MIPS Little endian, Intel x86-64



Hide and Seek

- **Second known decentralized P2P IOT botnet**
- ***Swarm characteristics***
- Known exploit to spread to TP Link routers
- Confirmed Capabilities
  - AMD x64, ARM
  - Brute force attacks
  - Target addition to random list
  - File retrieval commands through P2P nodes
- **Peer request-response model**
  - ‘i’ request → ‘I’ response
  - ‘h’ request → ‘H’ response
  - ‘z’ request → ‘O’ response
  - ‘~’ request → ‘^’ response

Hide and Seek


```
File  Edit  View  Search  Terminal  Help
                    :~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:15495

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
                    :~$
```

Fig 1: HNS Adds firewall rule to allow traffic on UDP port for P2P

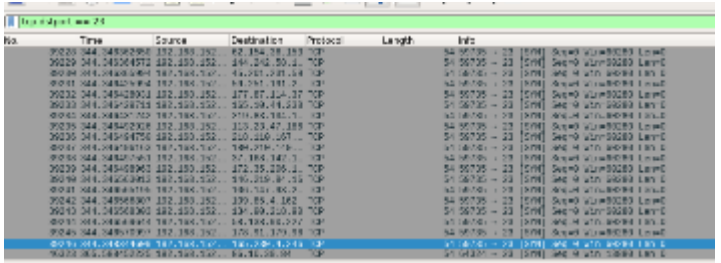


Fig 2: Scanning for next victims

Fig 3: P2P communication traffic captured, retrieving ELF files

```
if ( command == 'h' )
{
  if ( (_DWORD)a2 == 5 )
  {
    v5 = _byteswap_ulong(dword_5129C1);
    if ( v5 <= (unsigned int)sub_40A8E9(a2, a3) )
    {
      v3 = 5;
      v4 = 4;
      byte_512BA0 = 'H';
      dword_512BA1 = sub_40A89D(qword_512978);
      goto LABEL_105;
    }
    v4 = 4;
    sub_40C0AF(a3, v5);
    goto LABEL_111;
  }
  goto LABEL_93;
}
if ( (unsigned __int8)command <= 'h' )
{
  if ( command == 'G' )
  {
    if ( (_DWORD)a2 == 2 )
    {
      v3 = 0;
      v4 = 2;
      if ( (_BYTE)dword_5129C1 != byte_512950 )
        return 0;
      goto LABEL_105;
    }
  }
  else
  {
    if ( (unsigned __int8)command <= 'G' )
    {
      if ( command == 'H' && (_DWORD)a2 == 5 )
      {
        v4 = 4;
        v6 = _byteswap_ulong(dword_5129C1);
        if ( v6 > (unsigned int)sub_40A8E9(a2, a3) )
          sub_40C0AF(a3, v6);
        goto LABEL_111;
      }
      goto LABEL_93;
    }
    if ( command == 'Y' )
    {
      if ( (unsigned int)a2 > 4 )
      {
        v3 = sub_40C582(a2, a3);
LABEL_94:
```

Fig 4: List of supported run time commands

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

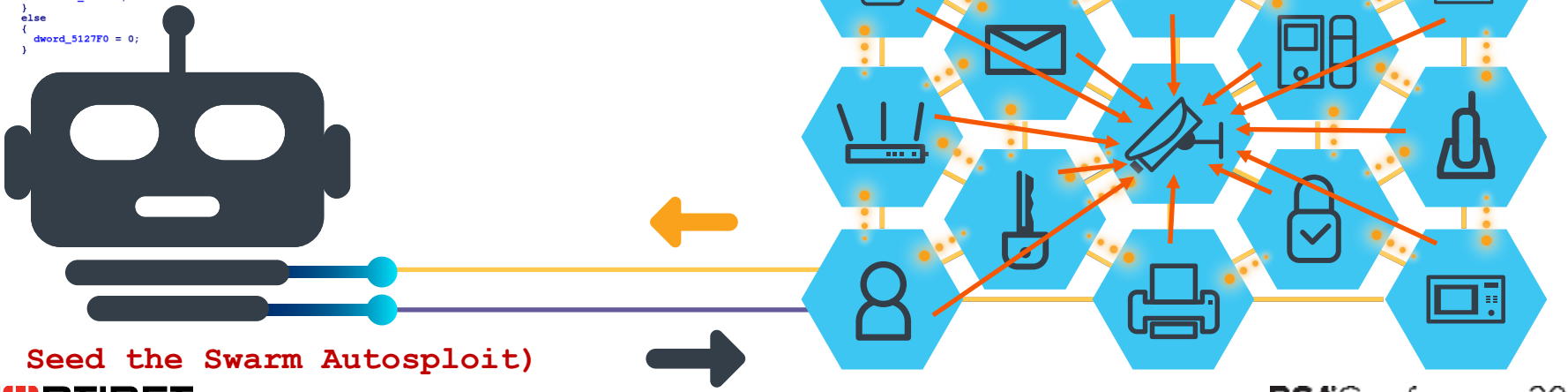
3) Target is swarmed, penetrated

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

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

'e's++IpatDRT

'm<data' ←→ Y<data>'



1) Seed the Swarm Autosploit)

FORTINET

RSAConference2018

ORDER: HIVE NETWORKS (HIVENETS)

All Your Bots are Belong To Us

Building a Cohesive Security Fabric

Hive – Group Survival Using the Individual

Decentralized, multicomponent mind	Displayed by social insects and some animals	Individual is the lowest cell unit	Quickly dies if individual becomes separated	Many animals display forms of this behavior…

Elephants, Meercats, and even humans acting as a corporation

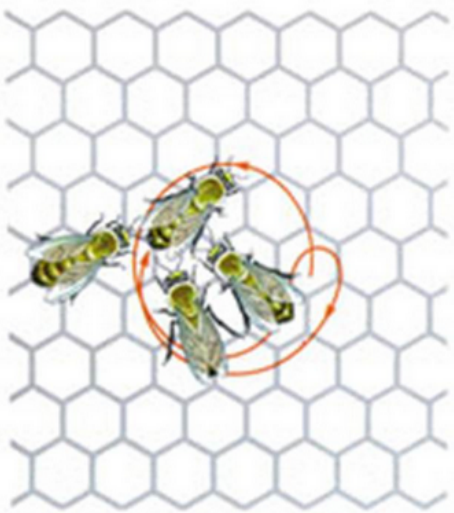
Hive – Group Survival Using the Individual

Bees: individual = simplistic

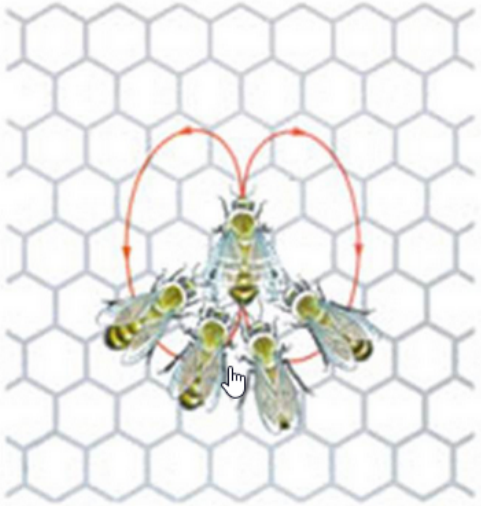
- As a group the intelligence rises
- Individuals responsible for jobs
- Complex communication and rituals
- Sub-groups have specific roles such as food gathering, digging, feeding pupae, cleaning
- All will act in defense of attack

Example – complex sub-group communications

Circular = nearby food



Tail wag = far away food



Is Cloud a Hive?

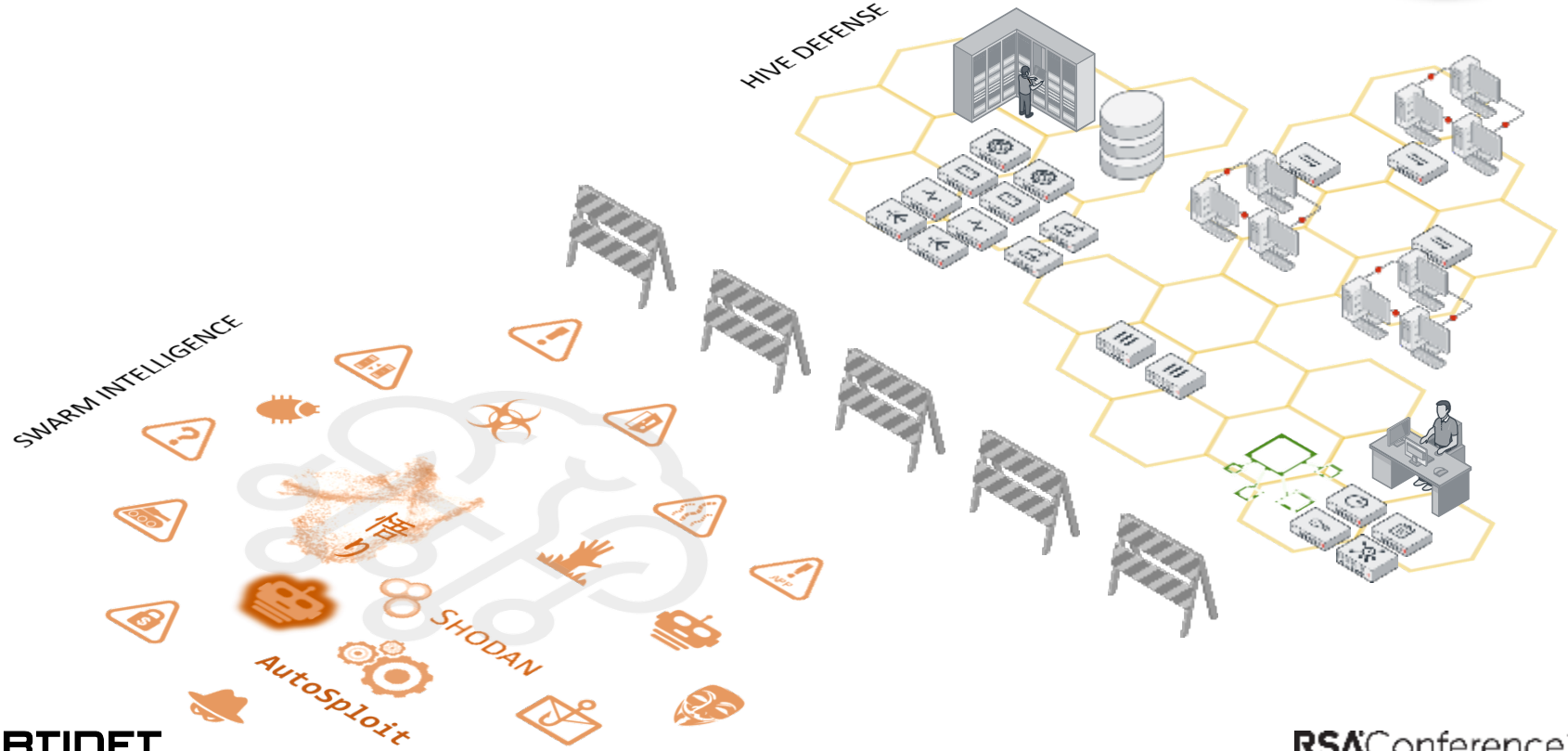
Hive

- Decentralized, multicomponent
- Group is intertwined through individuals
- Individual is the lowest cell unit
- Unable to act sufficiently as a stand-alone Quickly

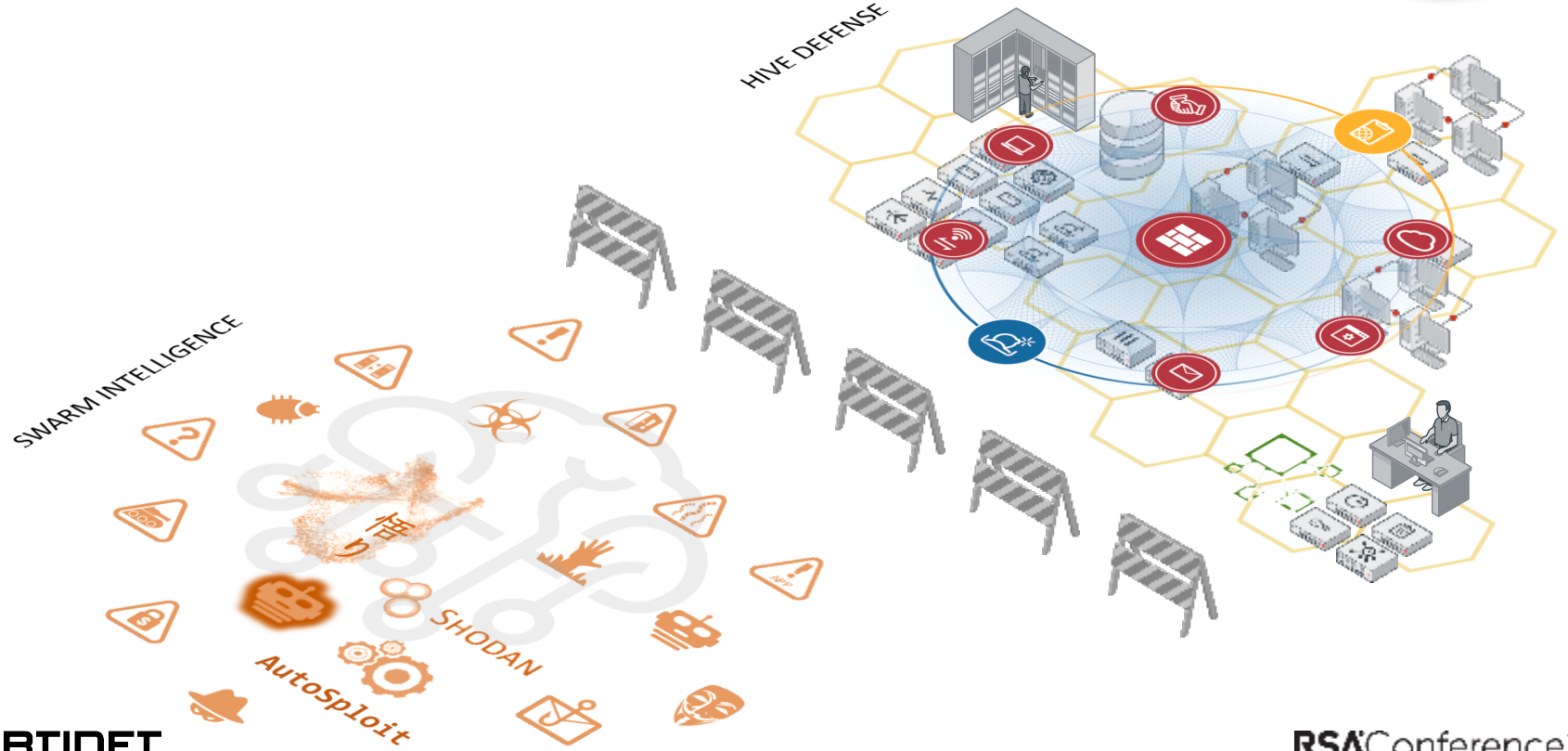
Cloud

- More of an extension of the hive
- As a component it is often like a sub-group
- Serves a function to infrastructure, resources
- Connects worker nodes and extends functionality
- Example: cloud-based security solutions such as sandbox, web content filtering, others

Hive Defense Strategy



Hive Defense Strategy



Cyber Threat Alliance

Integration of CTA Intelligence into Multiple Vendors (Swarm)

FOUNDING MEMBERS

Check Point SOFTWARE TECHNOLOGIES LTD.
cisco
FORTINET
McAfee Together is power.
paloalto NETWORKS
Symantec

AFFILIATE & CONTRIBUTING MEMBERS

Intsights
RAPID7
RSA
SOPHOS
SAINT
SK infosec
REVERSINGLABS
Eleven Paths

"The best way to combat the negative impact of cybercriminals and best protect our customers is through cooperation and partnership based on actionable intelligence from diverse sources."

Ken Xie, founder, chairman of the board and CEO, Fortinet

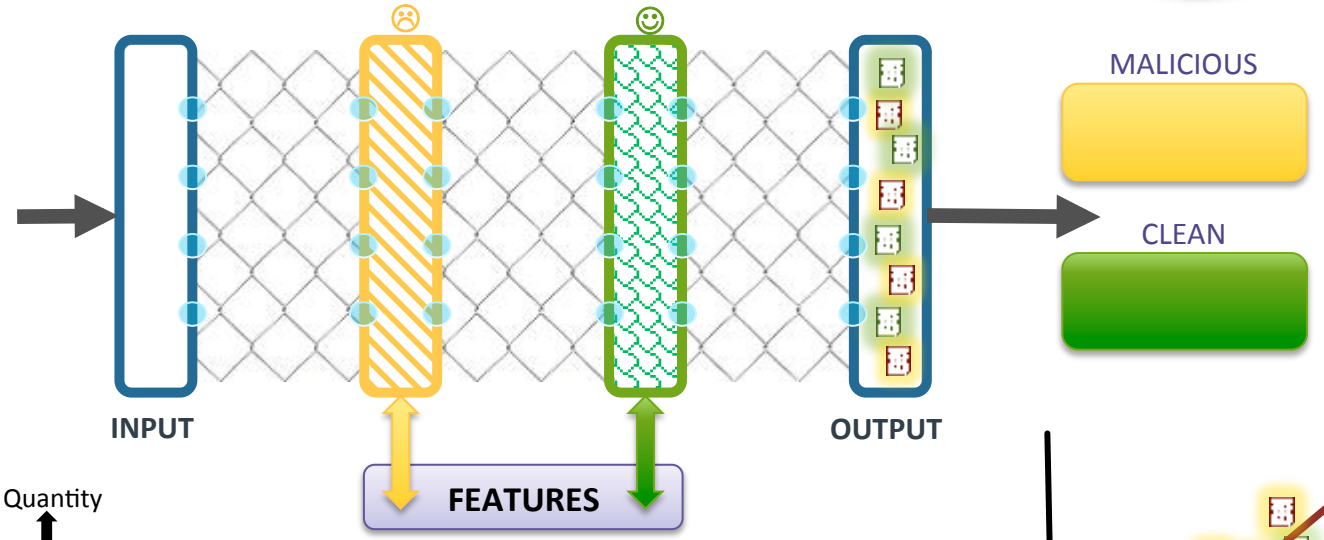
Advanced Solutions for Swarm

ex·pert sys·tem
noun
COMPUTING

a piece of software programmed using artificial intelligence techniques. Such systems use databases of expert knowledge to offer advice or make decisions in such areas as medical diagnosis and trading on the stock exchange.

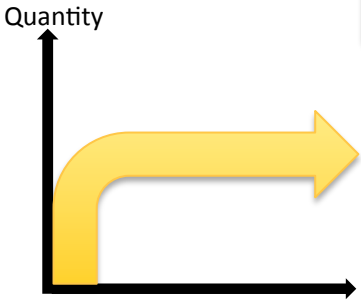
Advanced Solutions for Swarm: AI Anti-Malware

RAW SAMPLES

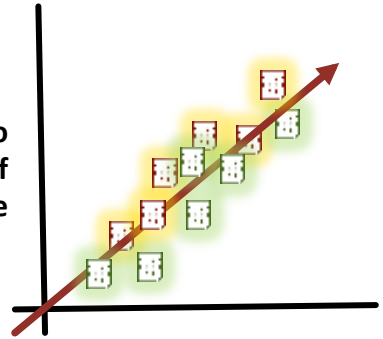


Feature Set Improvements

- Quality
- Stabilized Number
- Weighting Confidence

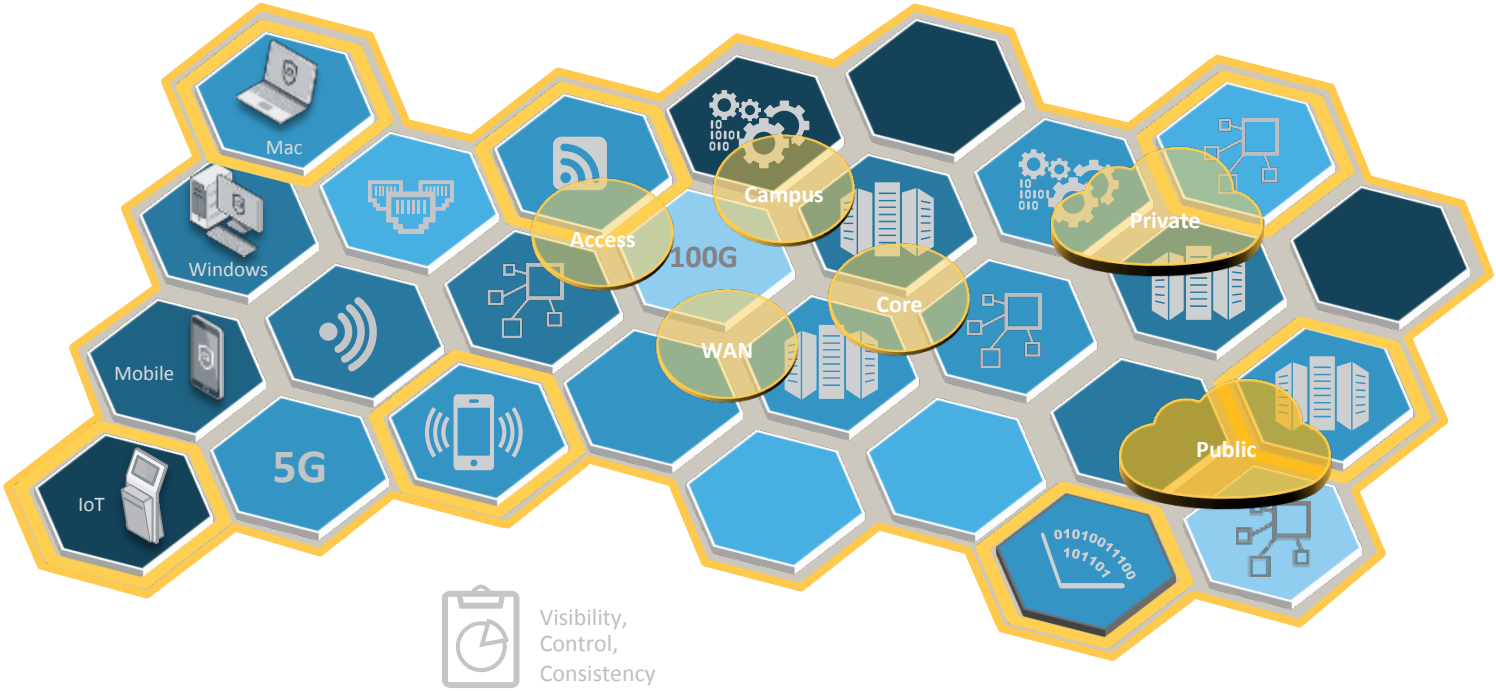


Continued Accuracy to a High Degree of Confidence

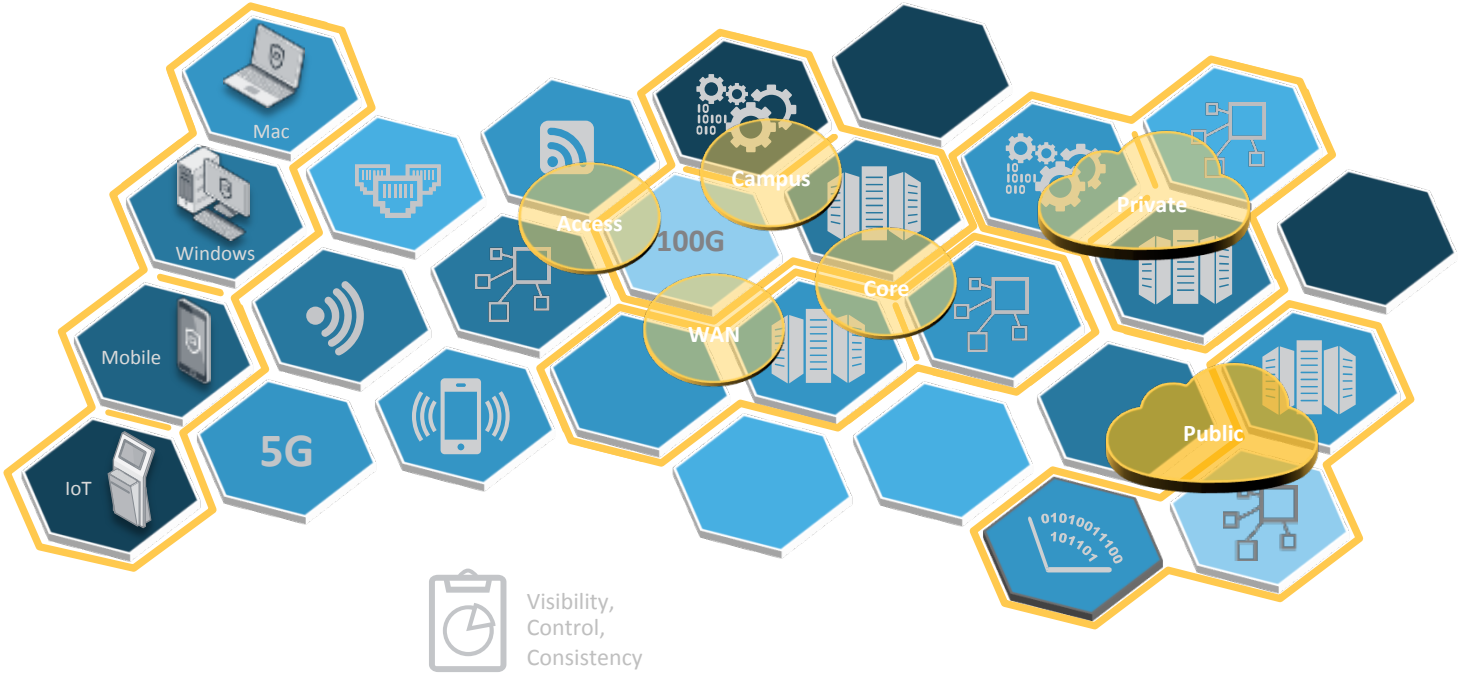


SYSTEM DYNAMIC PRIMARY STRATEGY:
AGILE MACRO AND MICRO SEGMENTATION

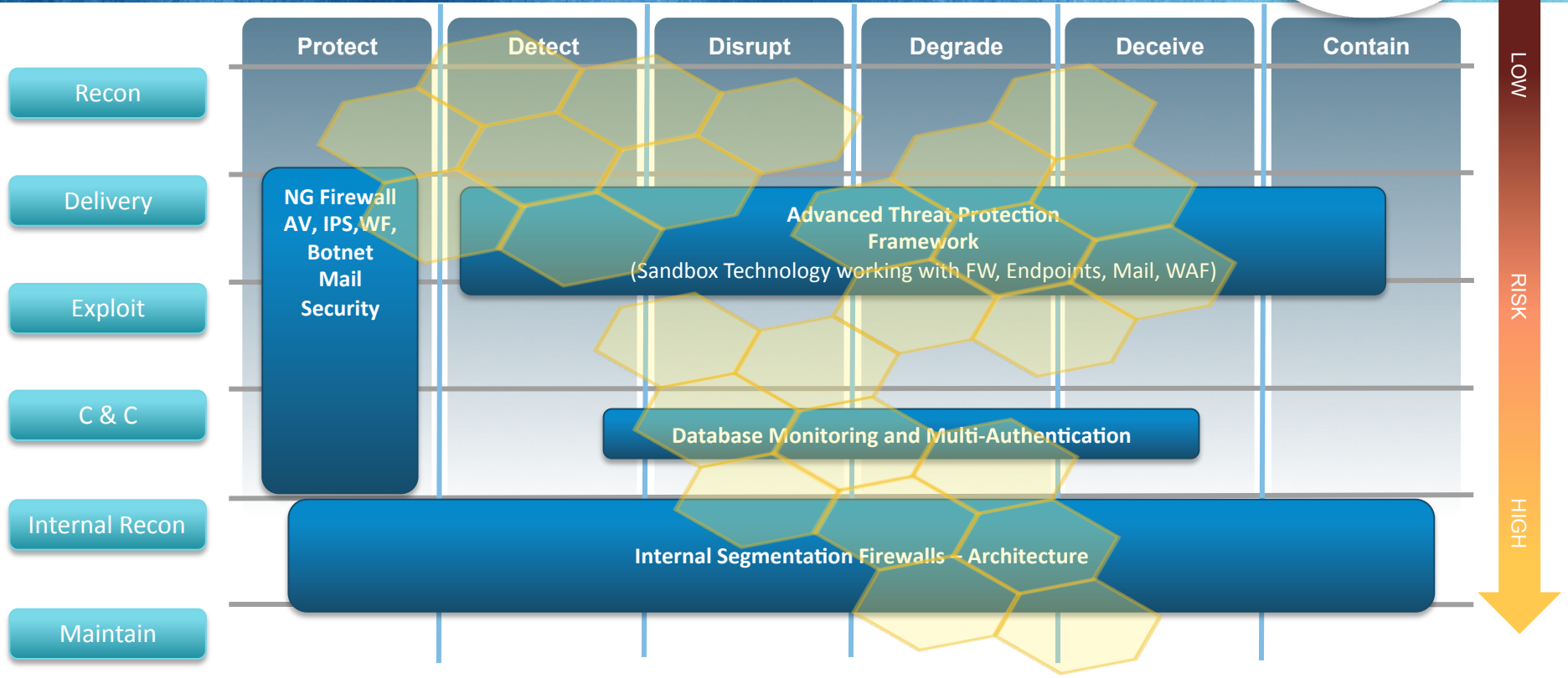
SYSTEM DYNAMIC PRIMARY STRATEGY:
AGILE MACRO AND MICRO SEGMENTATION
STATIC BOUNDARY SECURITY



SWARM STRATEGY:
AGILE MACRO AND MICRO SEGMENTATION

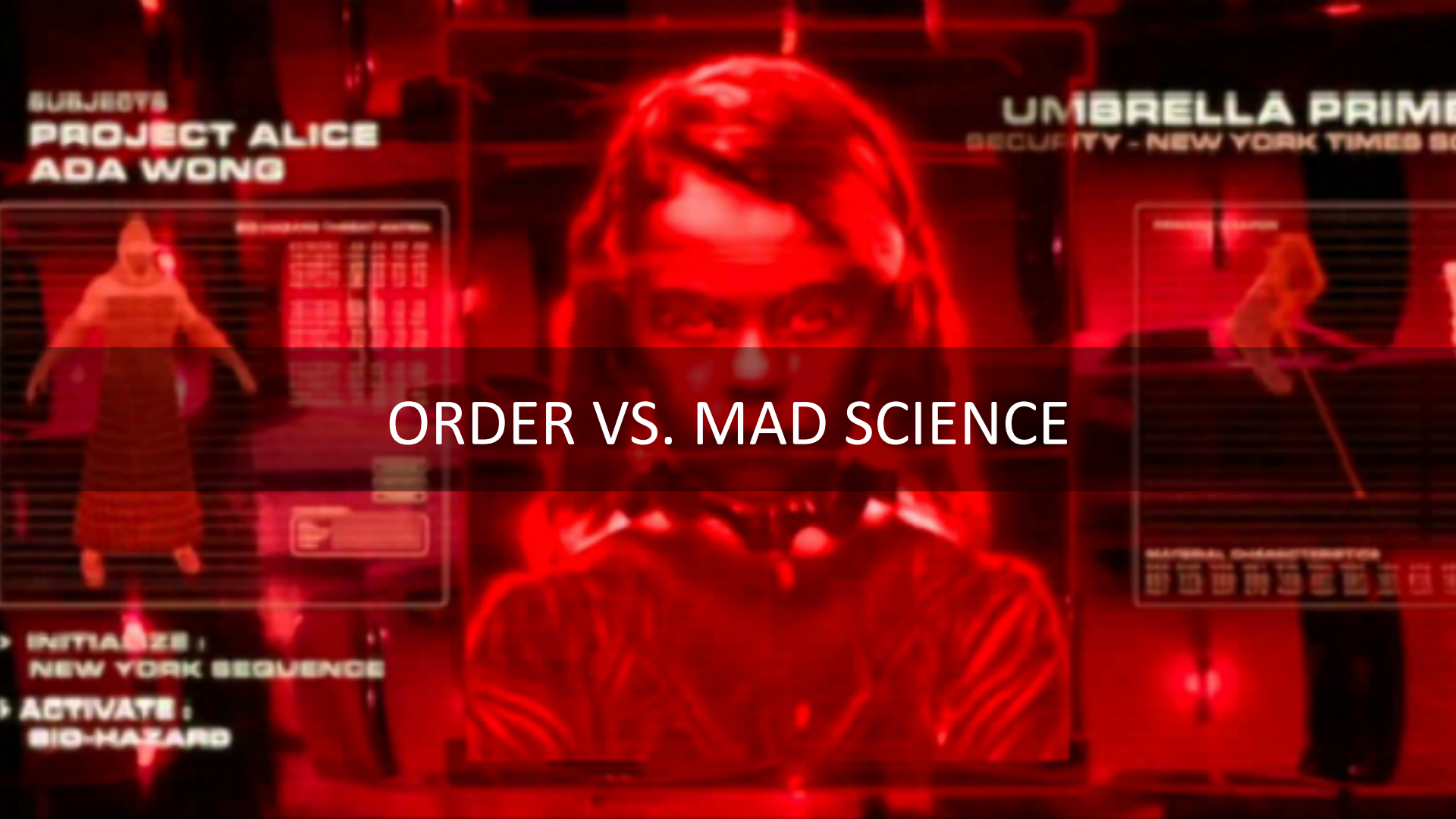


Accelerated Attack Chain Defense: Hive Defense in Kill Chain



Following Through

- **Next week you should:**
  - Think about your hive – where is it located (distributed, centralized, etc)
- **In the first three months following this presentation you should:**
  - Identify critical assets, resources within your hive
- **Within six months you should:**
  - Create an orchestrated security model that is your hive defense
    - Integration of security devices vs. kill chain
  - Consider AI solutions vs. zero day code
  - Shared, actionable intelligence between security solutions
  - Think about how to repurpose human admins (SOC/NOC) with such solutions



ORDER VS. MAD SCIENCE