ORDER VS. MAD SCIENCE
ANALYZING BLACK HAT SWARM INTELLIGENCE

Derek Manky
Global Security Strategist
Fortinet, Office of CISO
linkedin: /in/derekmanky
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

IM THE CREEPER, CATCH ME IF YOU CAN!
Evolving Attack Capabilities
Threat Landscape

CRIMEWARE PRODUCERS
- Exploits
- Packers
- Special Platform
- Mobile
- Junior Developers
- Senior Developers
- Source Code
- Copy & paste

COMPONUED CYBERCRIME
- Quality Assurance
- Crypters / Packers
- Scanners
- Hosting
- Infections / Drop Zones
- Management
- Botnet Rentals
- Installs / Spam / SEO / DDoS
- Money Mules
- Accounts Receivable
- Consulting
- CRIME SERVICES ENABLERS
- Quality Assurance
- Crypters / Packers
- Scanners
- Hosting
- Infections / Drop Zones
- Management
- Botnet Rentals
- Installs / Spam / SEO / DDoS
- Money Mules
- Accounts Receivable
- Consulting

Affiliates
- Affiliate Programs
- FakeAV / Ransomware / Botnets
- Sales, Licensing, Maintenance
- Partnerships

Victims
- Bank Accounts
- Credentials & Data
- Digital Real Estate
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

Starlings flock toward dusk in order to avoid predators... create a ‘murmuring’

Ants build resiliency through cooperative structures or mass defense / attack strategies
Other Biomechanical Examples of Swarm Behavior

<table>
<thead>
<tr>
<th>Old saying – a person is smart, a crowd is not</th>
<th>Tend to exhibit swarm behavior depending on situation</th>
<th>Aggregate and size of grouping determines behavior</th>
</tr>
</thead>
</table>

- **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)

1. PLANNING
   - Research target
   - Build or Acquire Tools
   - Test tools + detection

2. BREAK-IN
   - Deliver remote exploits and malware
   - Establish backdoors for commands

3. EXPAND
   - Move laterally to increase system access
   - Stronger Foothold

4. GATHER
   - Identify and collect sensitive data
   - Staging Server

5. EXFILTRATION
   - Data exfiltration through command and control services to external network

6. SURVIVE... Or PROFIT?

- Deliver remote exploits and malware
- Establish backdoors for commands
- Identify and collect sensitive data
- Staging Server
- Data exfiltration through command and control services to external network
- Move laterally to increase system access
- Stronger Foothold
• 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 perimeter security features gaining a foothold into internal networks.
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 systems

- **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
FORTIOS 6.0 HAS LAUNCHED!

MORE THAN 200 NEW FEATURES INCLUDING UNMATCHED NETWORK VISIBILITY, AUTOMATION, AND THREAT DETECTION

LEARN MORE

Featured Security Insights & Information
What you need to know to protect today and tomorrow.
Botnet Building Blocks

Typical Botnet Components

- Attacker (botmaster, herder)
- C&C Server
- Zombies
- Victim / target
- Communications channels

Initiate Attack

Attack Traffic

Attacker
Control Server
Botnet Attack Nodes
Victim
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

Once initially infected, it will randomly probe for other devices. If found a telnet port open, it will try to brute for logins. Once inside, a couple of commands are issued to further identify the environment:

```sh
$ enable
$ system
$ shell
$ sh
$ /bin/busybox ECCHI
```

Once identified the target architecture, binaries for that platform are downloaded from the hijacking host:

```sh
# echo -ne "\x7f\x45\x4c\x46\x01\x01\x00\x00\x00\x00\x01\x02\x00\x28\00\x01\00\x00\x00\x00\00\00\34\00\20\00\01\00\x00\00\00\00\00\00\00\00\00\00\00\01\00"
```

The purpose of this piece of code which is basically piped in hexadecimal through the network and dumped to a local file, is to download the stage 2.

The download of the stage 2 begins, which is the botnet communication part, using encrypted trackerless torrent uTP:

```sh
# unlink file
```

After all, Hajime deletes itself from the filesystem, having footprint in memory only.
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

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

Fig 4: List of supported run time commands
Hide and Seek

1) Seed the Swarm Autosploit
2) Target is identified by swarm
3) Target is swarmed, penetrated
4) File information leaked through swarm (IP, etc)

'\text{\textcolor{red}{e}}$'$s$'$ + IP:PORT

\begin{align*}
\text{\textcolor{red}{m}} & \text{\textcolor{blue}{\leftrightarrow}} \text{\textcolor{blue}{Y}} \text{\textcolor{blue}{<data>}} \\
\end{align*}
ORDER: HIVE NETWORKS (HIVENETS)

All Your Bots are Belong To Us

Building a Cohesive Security Fabric
## Hive – Group Survival Using the Individual

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

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

**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
“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
expert system
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

Feature Set Improvements
- Quality
- Stabilized Number
- Weighting Confidence

Continued Accuracy to a High Degree of Confidence
YESTERDAY'S PRIMARY STRATEGY:
STATIC BOUNDARY SECURITY

SWARM STRATEGY:
AGILE MACRO AND MICRO SEGMENTATION

- Visibility, Control, Consistency
- 5G
- 100G
- Campuses
- Core
- Private
- Public
- Access
- WAN
- Mobile
- Windows
- Mac
- IoT
SWARM STRATEGY:
AGILE MACRO AND MICRO SEGMENTATION
Accelerated Attack Chain Defense: Hive Defense in Kill Chain

- **Recon**
- **Delivery**
- **Exploit**
- **C & C**
- **Internal Recon**
- **Maintain**

**Protection Stages:**
- Protect
- Detect
- Disrupt
- Degrade
- Deceive
- Contain

**Key Components:**
- **NG Firewall AV, IPS, WF, Botnet Mail Security**
- **Advanced Threat Protection Framework** (Sandbox Technology working with FW, Endpoints, Mail, WAF)
- **Database Monitoring and Multi-Authentication**
- **Internal Segmentation Firewalls – Architecture**

**Risk Levels:**
- LOW
- HIGH
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