

# Criminal Clouds, Rogue Routers and Darknet DDoS Deals

# Agenda

- Security Team Challenges
- Criminal Cloud
- Actionable Network Intelligence Ecosystem
- How to mitigate IoT based DNS DDoS attacks
- Summary and Conclusions



# CYBER KILL CHAIN®

Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.

## A : ADVANCED

Targeted, Coordinated, Purposeful

## P : PERSISTENT

Month after Month, Year after Year

## T : THREAT

Person(s) with intent, opportunity, and capability

**WEAPONIZATION**  
Coupling exploit with backdoor into deliverable payload

**EXPLOITATION**  
Exploiting a vulnerability to execute code on victim's system

**COMMAND & CONTROL (C2)**  
Command channel for remote manipulation of victim

**RECONNAISSANCE**  
Harvesting email addresses, conference information, etc

**DELIVERY**  
Delivering weaponized bundle to the victim via email, web, USB, etc

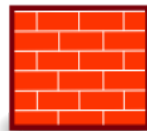
**INSTALLATION**  
Installing malware on the asset

**ACTIONS ON OBJECTIVES**  
With 'Hands on Keyboard' access, intruders accomplish their original goal

Vulnerability  
Management

Endpoint  
Protection  
(AV and/or  
Sandbox)

Intrusion  
Protection  
(IPS)

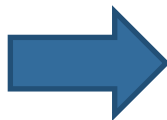


NG Firewall

Security Incident and  
Event Management  
System (SIEM)

*Many point solutions  
“high maintenance”,  
Silos, scarce  
security staff*

# Customer Security Challenges



**Security They Want**

**Security They Often Get**

Customer Security Challenges

Inability to Prioritize Events

Lack of Visibility

Lack of Vendor Integration

Manual Processes

Inability to Respond

# Well Organized Criminals



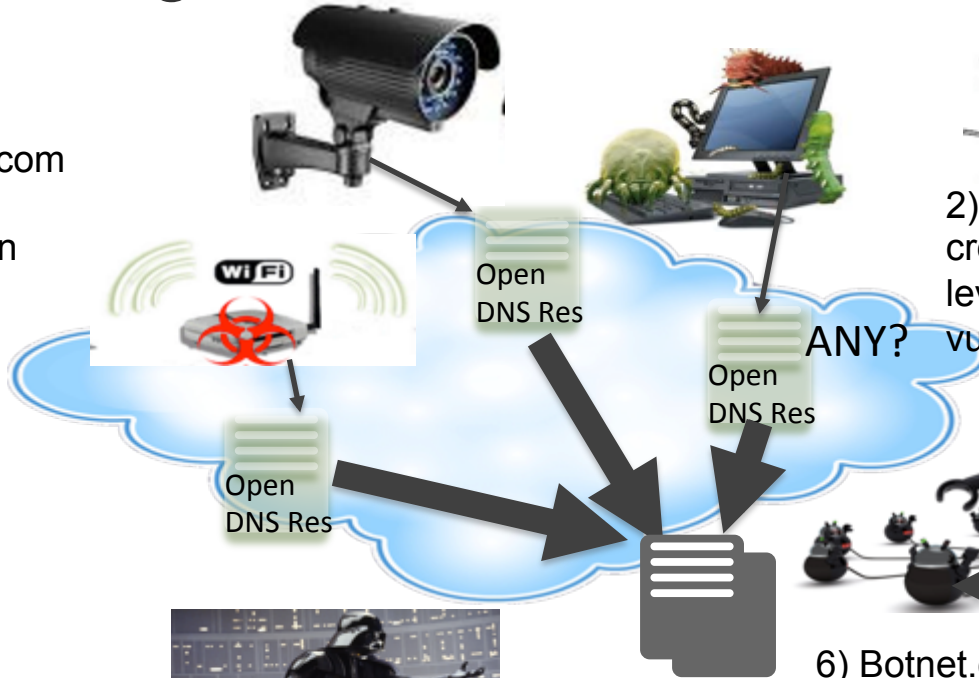
1) CentralAdministration.com sets up and maintains Cybergang Cloud, domain obfuscation



3) wrapper.com malware obfuscation



4) distributors.com spread packaged malware via spam, drive-bys: **end user interaction**



2) MaliciousCoder.com creates, new malware leveraging common vulnerabilities



5) CnC.com: maintains infections on machines: **end user interaction**



6) Botnet.com coordination of infected computers, obfuscate communication: **end user interaction**



# Agenda

- Criminal Cloud
- Security Team Challenges
- **Actionable Network Intelligence Ecosystem**
- How to mitigate IoT based DNS DDoS attacks
- Summary and Conclusions



# How to make (Network, Threat) Intelligence Actionable:

- Realtime
- Intelligence that focusses on what is to do rather than overwhelm Security Operations with countless alerts:
  - What
  - Where
  - Who
  - Why
- Reduces Operational Effort
- Reduces Risk



# DNS and Threat Intelligence: Existing Security become more effective

## DNS Security

Unique Threat Data to improve malware and data exfiltration visibility & prevention



QUALYS

**RAPID7**



ArcSight  
An HP Company



LogRhythm  
The Security Intelligence Company

## DNS DHCP IP Address Management

Critical data for correlation, prioritization or events and reduced incident response times



CISCO



ForeScout

## Ecosystem & Data Exchange

Scalable infrastructure and API's to enable data to flow between separate security systems



Bit9 + CARBON BLACK  
ARM YOUR ENDPOINTS.



## Enforcement & Mitigation

Pervasive DDI coupled with Threat Intelligence enables mitigation, enforcement across infrastructure



# Agenda

- Criminal Cloud
- Security Team Challenges
- Actionable Network Intelligence Ecosystem
- How to mitigate IoT based DNS DDoS attacks
- Summary and Conclusions



# Mirai based DNS attacks: What Can We Do?

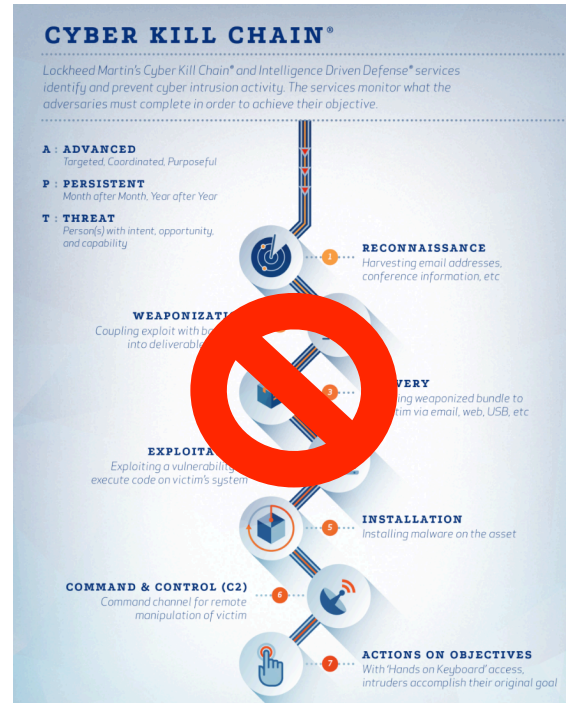
Use a mixed set of authoritative name servers

- On-premises name servers
- Hosted name servers
- If your DNS hosting provider or one of its customers is attacked, recursive name servers on the Internet will notice that they're not responding and will favor your on-premises name servers



# Disrupt Cyber Kill Chain, improve Control, Visibility

- Supplement current security systems with new technologies that are relevant throughout chain and provide visibility:
  - DNS to understand what is REALLY going on
  - Threat Intelligence to find malicious identifiers
    - Entropy
    - Machine Learning



# Agenda

- Criminal Cloud
- Security Team Challenges
- Actionable Network Intelligence Ecosystem
- Summary and Conclusions



# Summary and Recommendations

- Bridge SOC / NOC gap: leverage Infoblox DDI for Security teams (if not done already)
- Leverage Security Ecosystem to improve efficiency
  - Ask each Security Vendor about their ecosystem
  - Ask about integrating new systems
- Domain Names centric Threat Intelligence across entire cyber killchain
- Get PCAP or POC Network Activity Analysis
- View a Dossier Demo

# Thank You!

