DDoS: a 20-year journey from compromised workstations to IoT attacks

Dr. Sven Dietrich

Associate Professor
Mathematics and Computer Science Department
CUNY John Jay College of Criminal Justice

spock@jjay.cuny.edu
http://jjcweb.jjay.cuny.edu/sdietrich

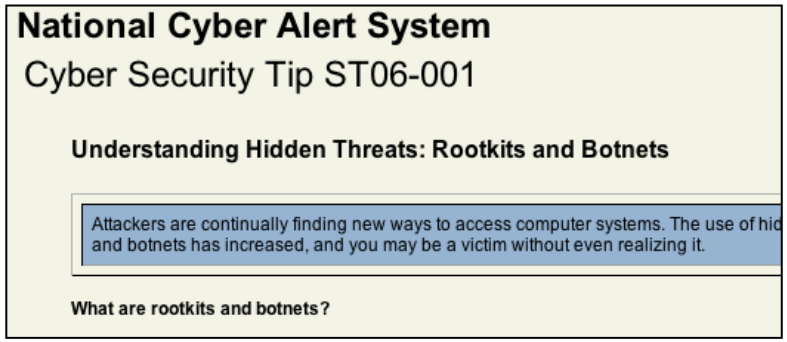
Denial of Service: Terminology

- Overwhelming the victim to the point of unresponsiveness to the legitimate user
- By carefully constructing a sequence of packets with certain characteristics, an intruder can cause vulnerable systems to crash, hang, or behave in unpredictable ways

Motivation

U.S., South Korea Targeted in Swarm Of Internet Attacks
Hacking Focused on Government Sites
PCs Used in Korean DDoS Attacks May Self Destruct
Source: Washington Post, July 2009

Source: Computerworld



Source: US-CERT

Source: Dark Visitor

DDoS from IoT botnets (2016-now)

Why DoS?

Why DoS?

- "An Introduction to Denial of Service," Hans Husman, 1996
  - Sub-cultural status
  - To gain access
  - Revenge
  - Political reasons
  - Economic reasons
  - Nastiness

Source: https://packetstormsecurity.com/files/14846/denial.txt.html

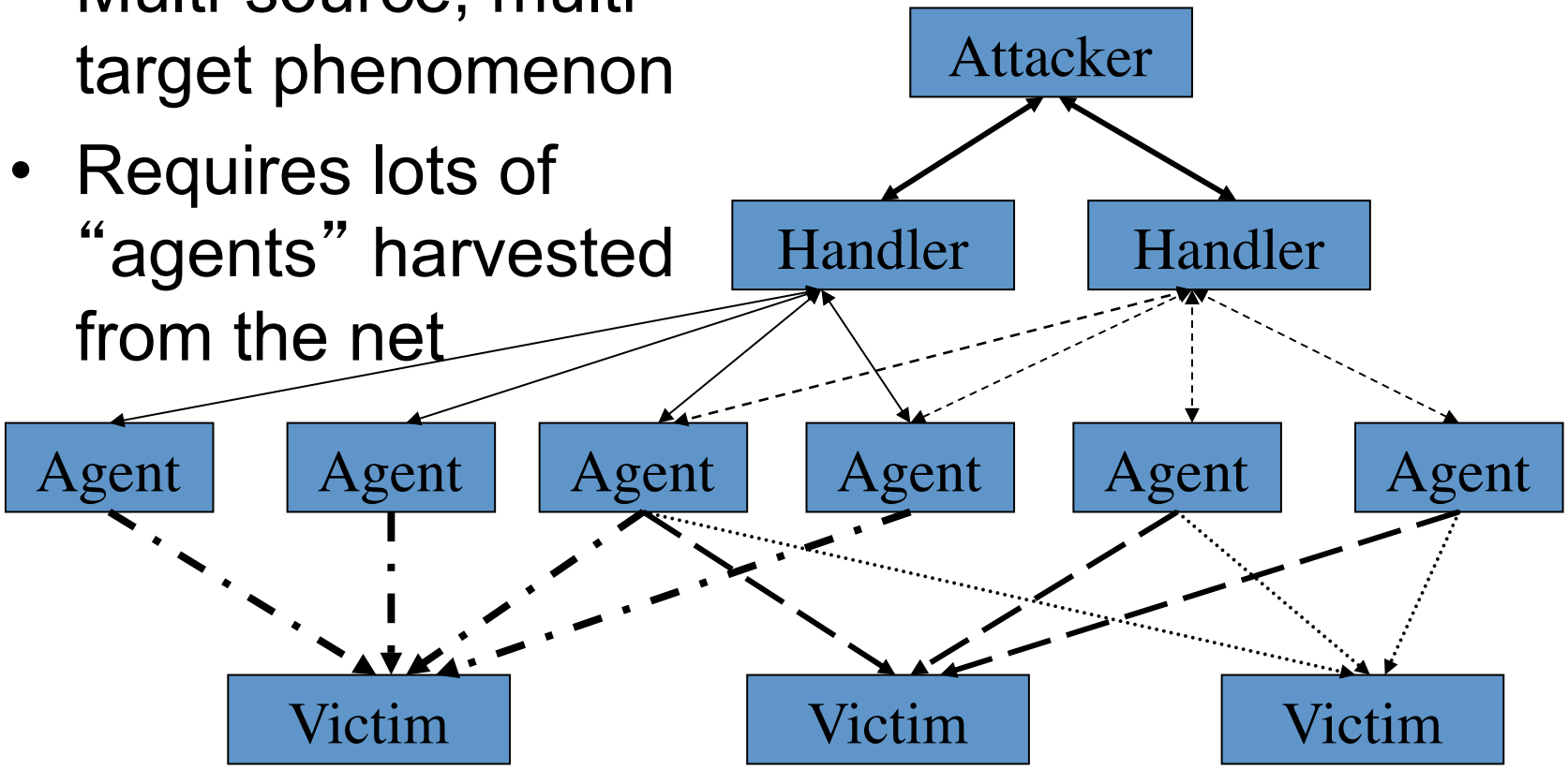
Why perform attacks?

- 2019 version
  - Hacker street cred
  - Hacktivism
  - Commercial advantage
  - Blackmail
  - Nation-state activity

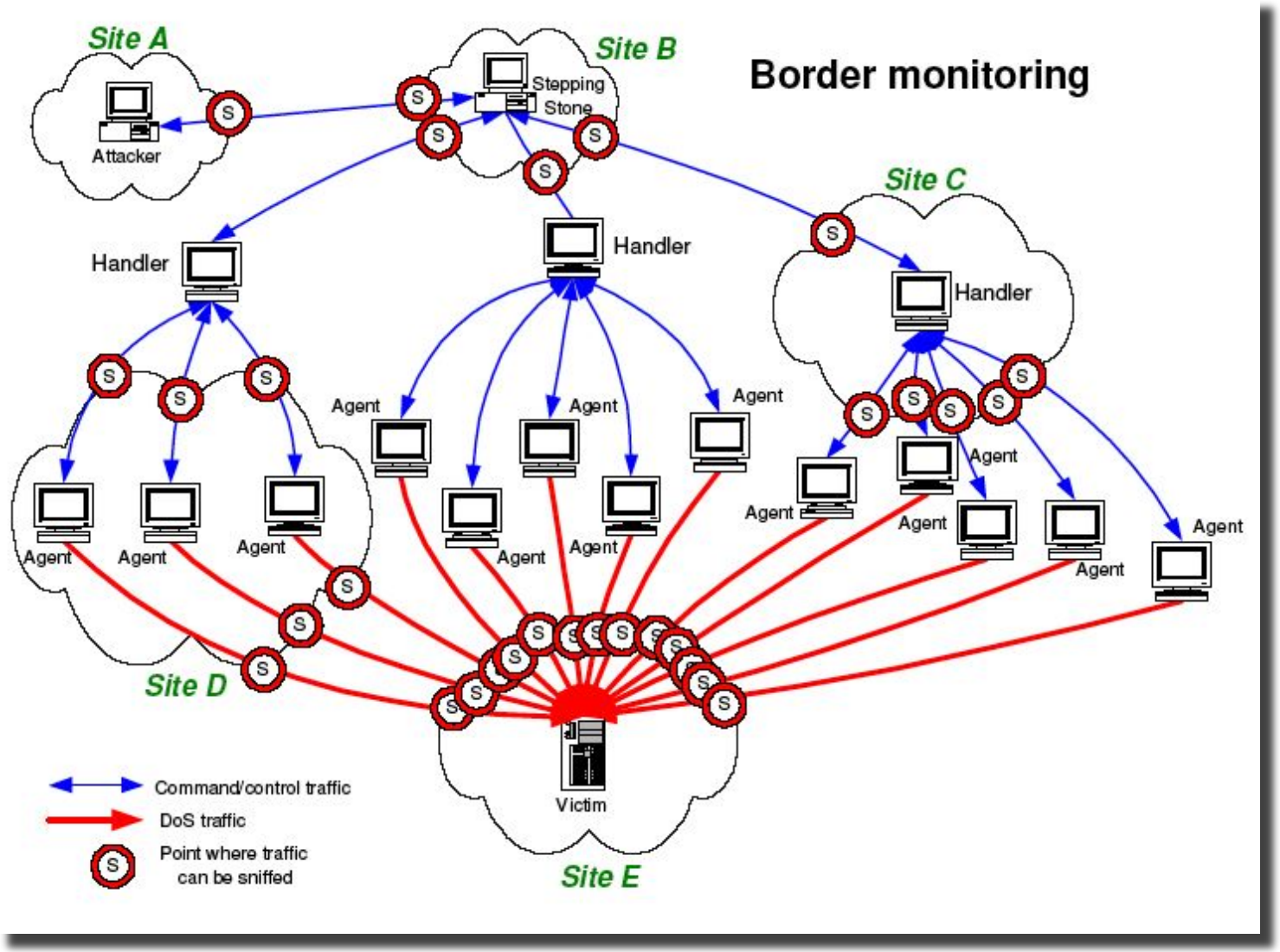
“Plus ça change, plus c'est la même chose”
(Jean-Baptiste Alphonse Karr, Les Guêpes, 1848)

Distributed Denial of Service (DDoS)

- Multi-source, multi-target phenomenon
- Requires lots of "agents" harvested from the net



Attack setup



Types of attack

- Obvious attack traffic
  - Registered as malicious
- Attack traffic disguising itself as “normal traffic”
  - Looks like normal users’ web traffic on a busy day
  - Mimics flash crowds

Attack sources

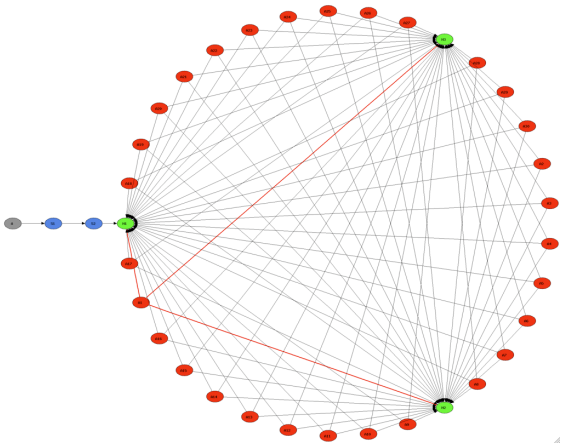
- Simply put:
  - Vulnerable, (mostly) always connected systems
  - Unpatched, poorly designed/maintained systems
- Roughly:
  - 1990s: mostly university and government computers
  - 2000s: broadband-connected (desktop) computers, commercial sites
  - 2010s: mobile, IoT devices
  - 2020s: quo vadis?

DDoS
Botnets and Worms

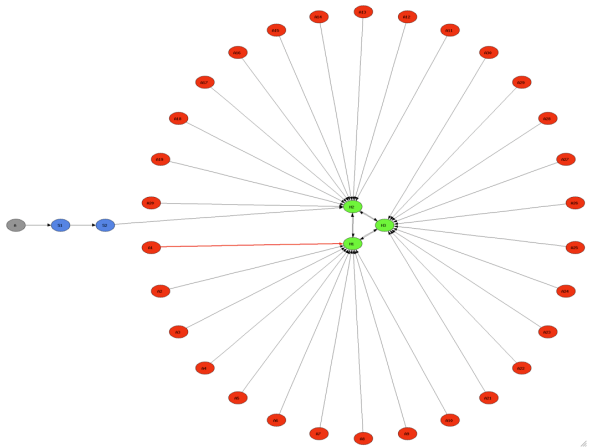
- DDoS attacks (1999-2000)
  - Universities & E-commerce sites
- Code Red (2001)
  - DDoS on whitehouse.gov
- W32/Leaves (2001)
  - Click fraud
- AgoBot/Phatbot (2004)
  - Gambling: DDoS, Blackmail
- Nugache (2006)
  - DDoS, Extortion
- Conficker (2007)
  - Propagation, Payload distribution
- Stuxnet, Mirai, Reaper, Gafgyt/Bashlite,Satori, APTs (recent)
  - Gov’ts, infrastructure, espionage, sabotage

Topologies

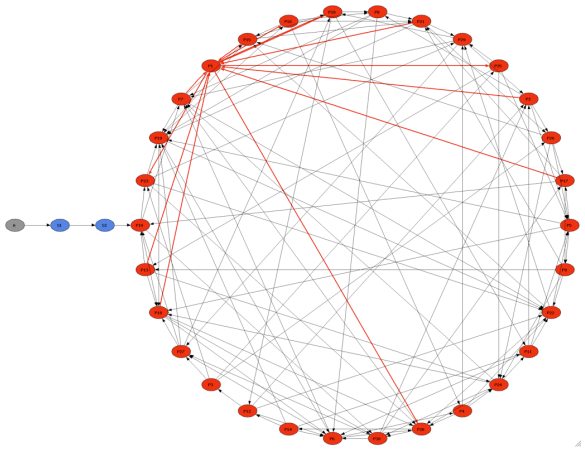
- Star topology
- Peer-to-peer (P2P)
- Multi-tiered, structured P2P



DDoS agent



IRC botnet



P2P

Why IoT?

- Protection has been improved on desktop & mobile devices
  - At the center of attention, awareness
- IoT devices
  - Limited resources (RAM, speed)
  - Neglected
  - Setup and go
  - Simple compromise
    - Zero days
    - Bad defaults (and available online)
  - Injection of malware

IoT DDoS attacks

- Mirai botnet & friends
  - Recruits IoT devices (broadband routers, online cameras) into a large botnet
  - Uses credential defaults to infect IoT devices and perform attacks (device-specific binaries)
- Attack targets
  - Web, BK ~620 Gbps, OVH ~1.3 Tbps (Sep 2016)
  - Infrastructure, DynDNS (500k hosts) (Oct 2016)
    - Affected Spotify, Twitter, etc.
  - Other targets, 359 Gbps (2018)
- New attack sources
  - Embedded devices (April 2019)

https://arstechnica.com/information-technology/2019/04/new-variants-of-mirai-botnet-detected-targeting-more-iot-devices/

Detection & Mitigation

- Some questions to ponder:
  - Detection of which type?
    - The attack itself? Which type?
    - The C&C?
    - The reconnaissance?
  - Mitigation of which type?
    - Volumetric attacks? Disruptive low-packet attacks?
    - Prevention of routing impact?
    - Traceback to source?
    - Dissipation?
    - Proactive measures (network, host)?

Nextgen design

- Separation of control and data planes
  - Software Defined Networks (SDN)
  - Future Internet Architectures
- May create new (D)DoS opportunities/ problems
  - SDN is built on “software,” which inherently has flaws

Q&A

- Sven Dietrich
  - http://jjcweb.jjay.cuny.edu/sdietrich

- Are we done? Maybe not...