



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

SlideShare Slammed with DDOS Attacks from China

TC <http://www.techcrunch.com/2008/04/23/slideshare-slammed-with-ddos-attacks->

Apple (132) Amazon eBay Yahoo! News (962)

TechCrunch

About Contact Company Index Advertise Archives Cool Jobs TC50 Crunchies Primaries LA Party

« Previous post Next post »

April 23 2008

SlideShare Slammed with DDOS Attacks from China

Mark Hendrickson 89 comments »

SlideShare, a Mountain View-based startup that lets you upload and embed PowerPoint presentations on the web, appears to have stirred the red dragon last week.

About ten days ago the company began receiving anonymous requests to delete slideshows that were deemed "illegal" by the requesters. The SlideShare staff checked out these slideshows and discovered them to be quite innocent. While some described ways to fight corruption in China, none of them violated the company's terms of service, and so SlideShare did nothing to fulfill the requests.

SlideShare soon began receiving a different type of request from the same people, who could now be identified by their email addresses. This time they were pretending to be users who had lost their passwords. Once again doing nothing, the company



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

Estonia recovers from massive DDoS attack

Denial-of-service onslaught may have Russian origins

Jeremy Kirk Today's Top Stories » or Other Security Stories »

Comments (2) Recommendations: 91 — Recommend this article

May 17, 2007 (IDG News Service) -- A spree of denial-of-service attacks against Web sites in Estonia appears to be subsiding, as the government calls for greater response mechanisms to cyber attacks within the [European Union](#).

The attacks, which started around April 27, have crippled Web sites for Estonia's prime minister, banks, and less-trafficked sites run by small schools, said Hillar Aarelaid, chief security officer for Estonia's Computer Emergency Response Team (CERT), on Thursday. But most of the affected Web sites have been able to restore service.

"Yes, it's serious problem, but we are up and running," Aarelaid said.

Source: Computerworld

National Cyber Alert System

Cyber Security Tip ST06-001

Understanding Hidden Threats: Rootkits and Botnets

Attackers are continually finding new ways to access computer systems. The use of hidden and botnets has increased, and you may be a victim without even realizing it.

What are rootkits and botnets?

Source: US-CERT

BREAKING: Upcoming Chinese hacker attack on CNN building steam

Published by [Helke](#) at 6:25 pm under [Nationalism](#), [Tibet](#), [US attacks](#)

Apr
17
2008

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>

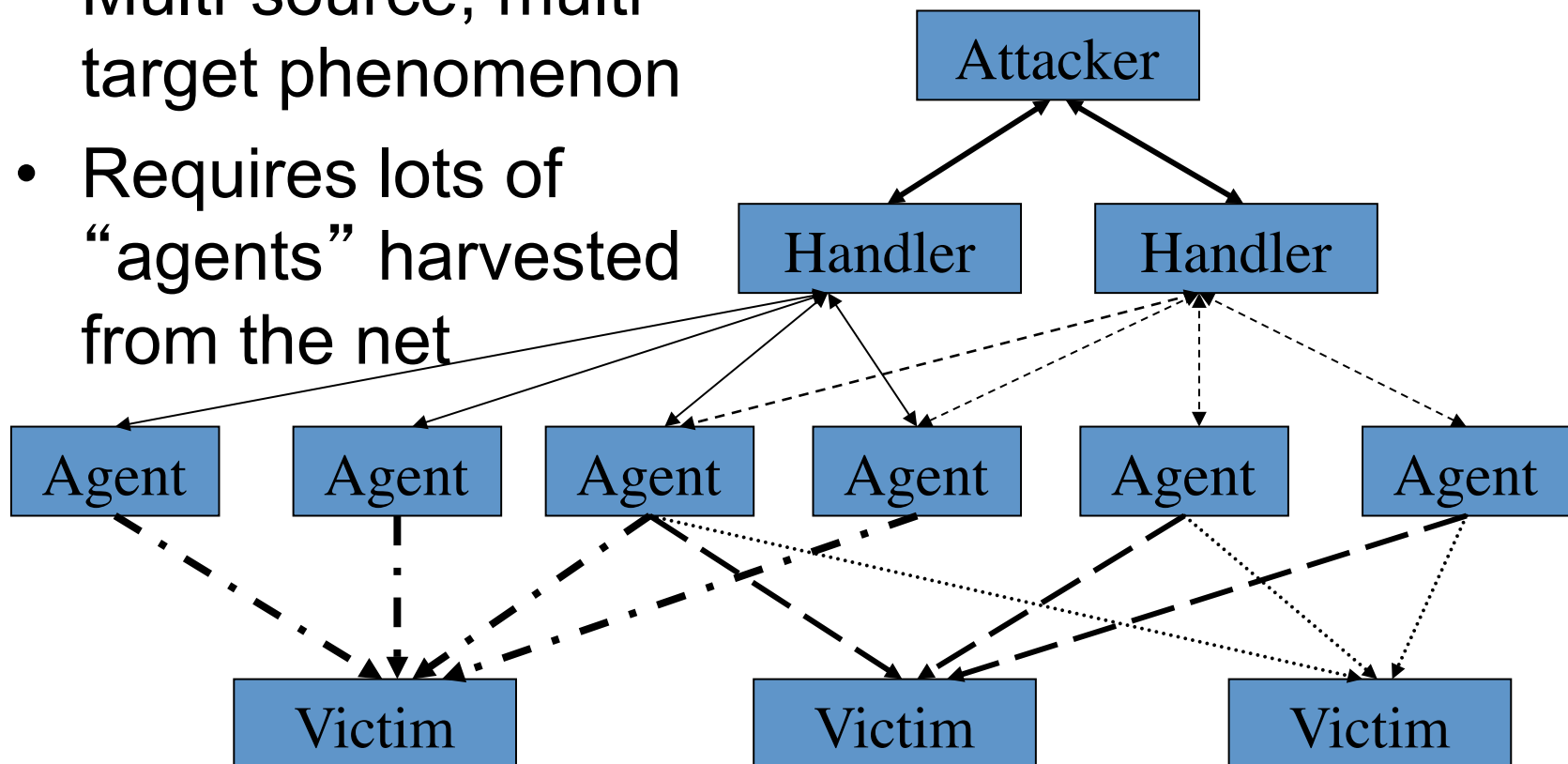
Why perform attacks?

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

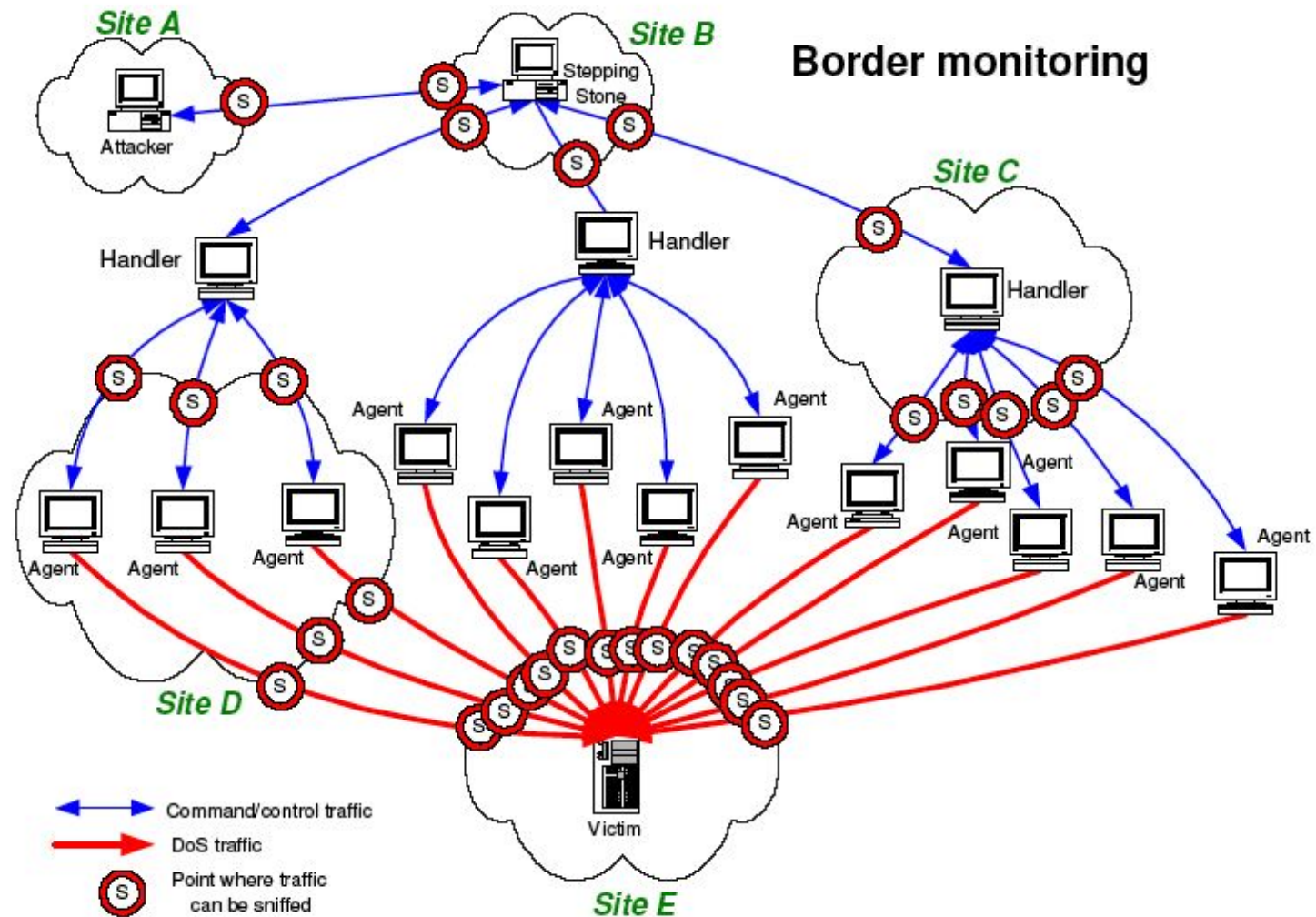
“Plus ça change, plus c'est la même chose”
(Jean-Baptiste Alphonse Karr, Les Guêpes, 1848)

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?

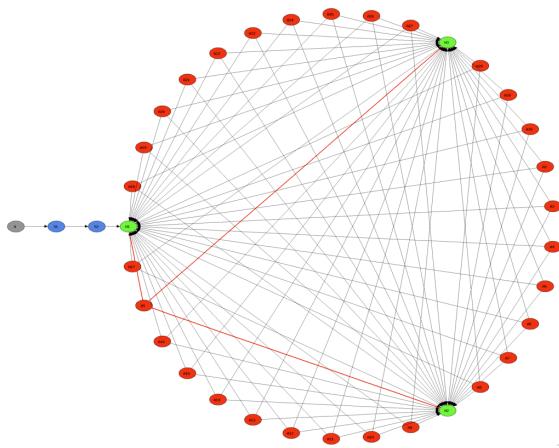
DDoS

Botnets and Worms

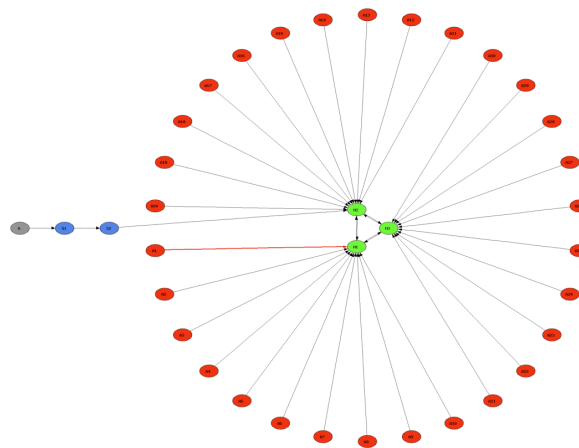
- DDoS attacks (1999-2000)
 - Universities & E-commerce sites
- Code Red (2001)
 - DDoS on whitehouse.gov
- W32/Leaves (2001)
 - Click fraud
- AgoBot/Phatbot (2004)
 - Gambling: DDoS, Blackmail
- Nugache (2006)
 - DDoS, Extortion
- Conficker (2007)
 - Propagation, Payload distribution
- Stuxnet, Mirai,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

Topologies

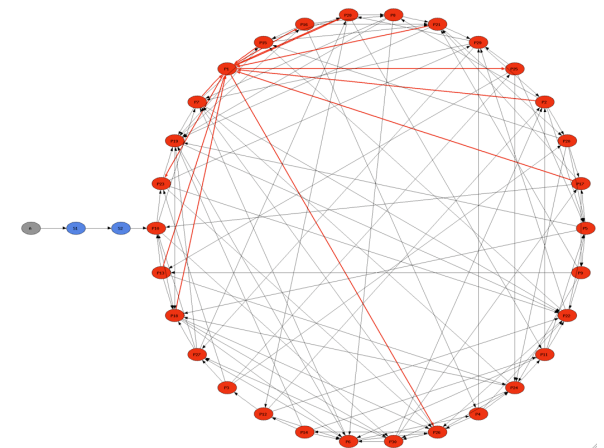
- Star topology
- Peer-to-peer (P2P)
- Multi-tiered, structured P2P



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)



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...

