(ISC)² Twin Cities Area Chapter
October 2013 Meeting

18 October 2013, 14.00 - 16.00

Distributed Denial of Service

Low Orbit Ion Cannon

Or just Denial of Service
or Resource Exhaustion

Originated on IRC

Used today as a form of
protest and for financial gain

Recent News

SPAMHAUS

"Anonymous", AntiSec, Lulzsec

Fraud and a part of larger bank heists "itsoknoproblembro" DDoS Tool against BofA, Chase, PNC, etc

ttp://www.scmagazine.com/fraudsters-target-wire-payment-switch-at-banks-to-steal-millions/article/307755/

http://www.infosecurity-magazine.com/view/30053/dissection-of-itsoknoproblembro-the-ddos-tool-that-shook-the-banking-world/

itsoknoproblembro

PHP Injection + JS = Browser Botnet

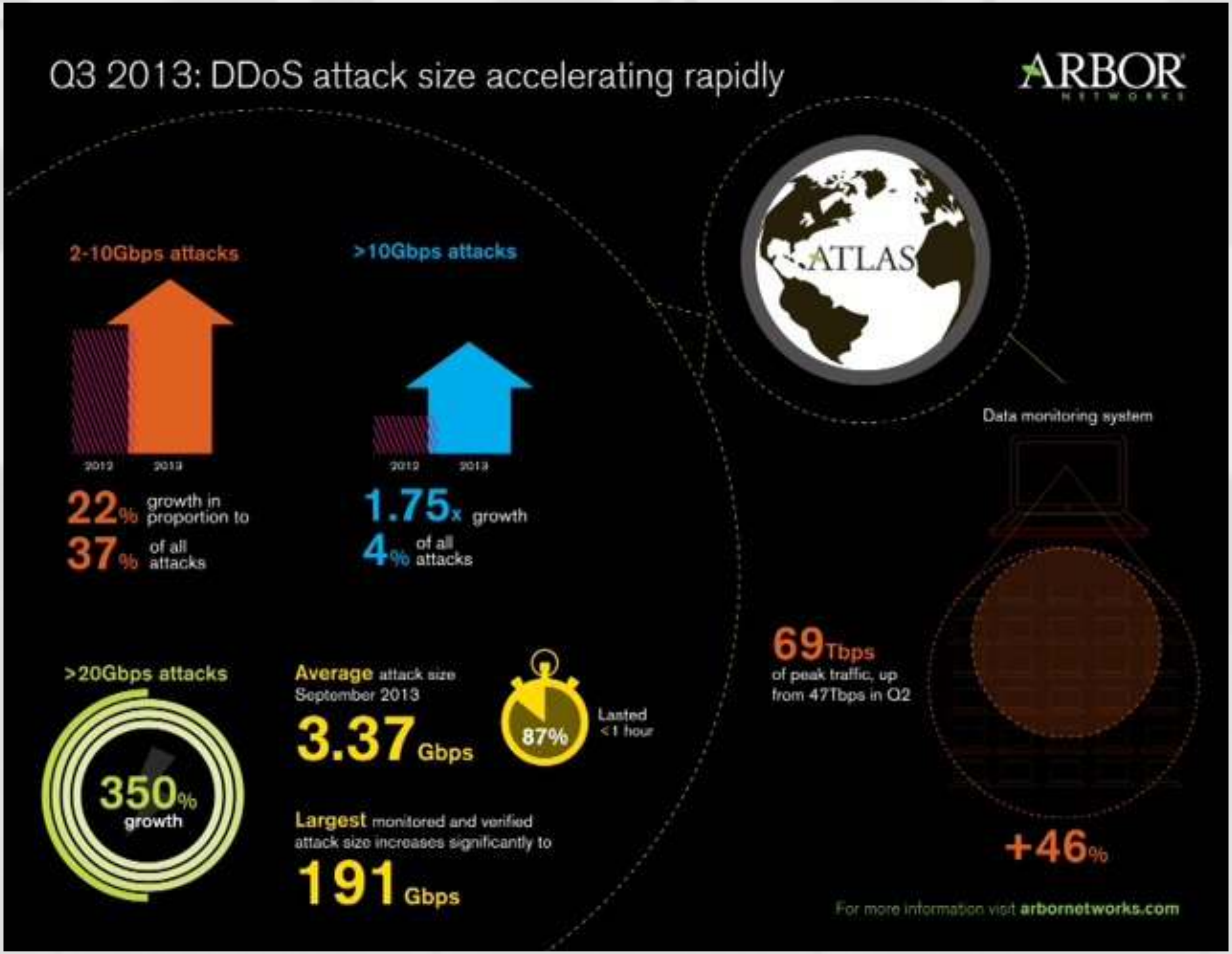
Skill Needed: High - Motivated Attacker

Further demonstrated by Jeremiah Grossman and Matt Johansen at BlackHat 2013

https://www.blackhat.com/us-13/briefings.html#Grossman

Hijack an advertising network, Akamai or any other similar service and you have a Million Browser Botnet

Latest DDoS Numbers



Q3 2013: DDoS attack size accelerating rapidly

ARBOR NETWORKS

2-10Gbps attacks

22% growth in proportion to 37% of all attacks

>10Gbps attacks

1.75x growth

4% of all attacks

>20Gbps attacks

350% growth

Average attack size September 2013

3.37 Gbps

87% Lasted < 1 hour

Largest monitored and verified attack size increases significantly to

191 Gbps

Data monitoring system

69Tbps of peak traffic, up from 47Tbps in Q2

+46%

For more information visit arbornetworks.com

http://www.arbornetworks.com/corporate/blog/5025-q3-findings-from-atlas

Risk Transference

Content Distribution Network (CDN)

Cloud Hosted Front End
(Linode, Digital Ocean, Rackspace)

CDN + Anti-DDoS (CloudFlare)

Mitigation

Risk Transference
(Somebody Elses problem)

Null Routing with BGP

Bigger Pipes

Application / Network Tweaks

Purpose

Revenge

Demonstration of Power (Botnet Rental)

Criminals (Extortion)

Espionage or Competition

Political (Protest)

Matthew J. Harmon & Phil Reno

Threat Sources

Competitor

Industrial Espionage

Organized Crime

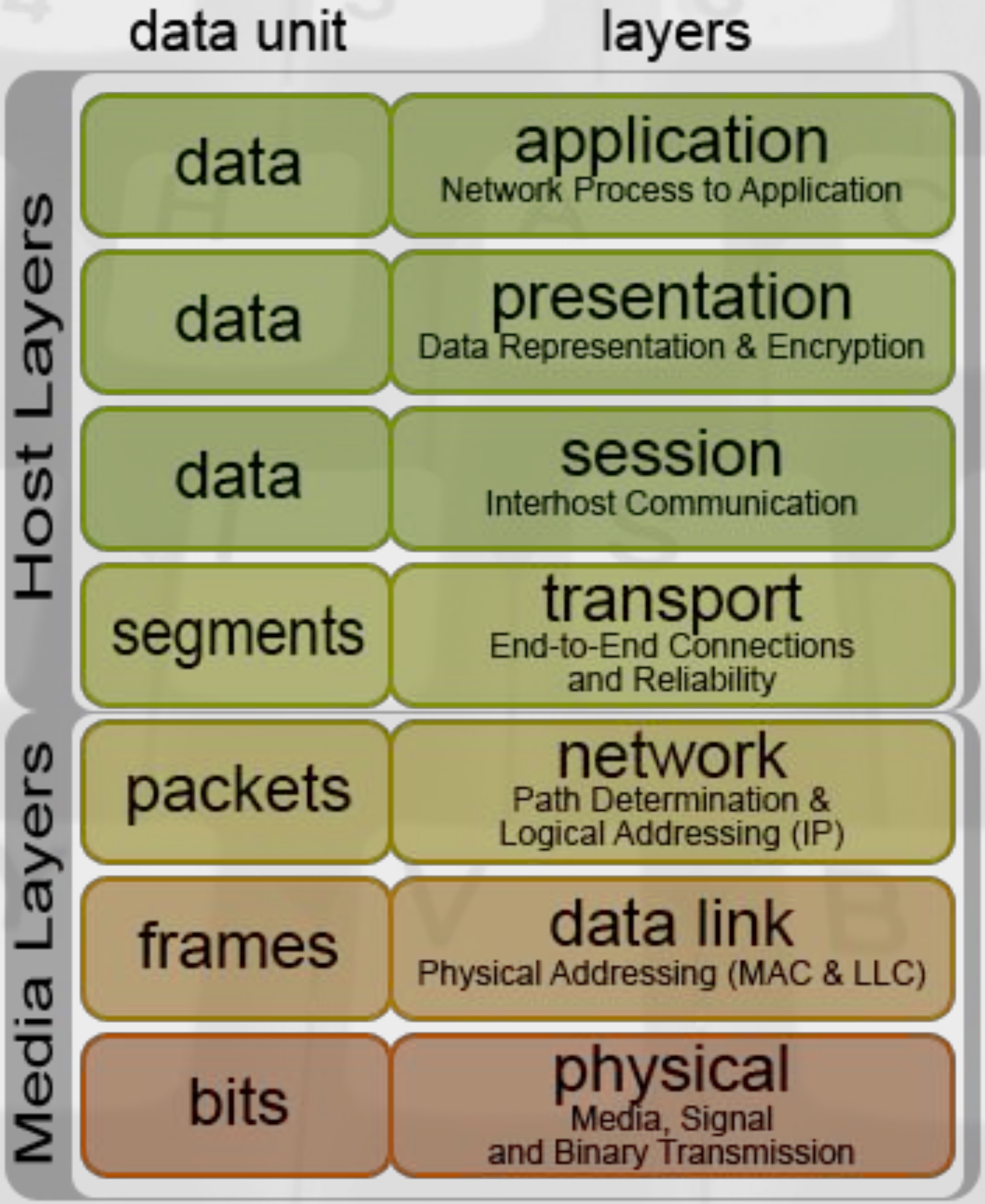
Radical or Civil Activist

Government Cyberwarrior

Insider or Employee (Reckless, Untrained)

Good Publicity

OSI Model



	data unit	layers
Host Layers	data	application Network Process to Application
	data	presentation Data Representation & Encryption
	data	session Interhost Communication
	segments	transport End-to-End Connections and Reliability
Media Layers	packets	network Path Determination & Logical Addressing (IP)
	frames	data link Physical Addressing (MAC & LLC)
	bits	physical Media, Signal and Binary Transmission

Image Source: https://commons.wikimedia.org/wiki/File:Osi-model.png

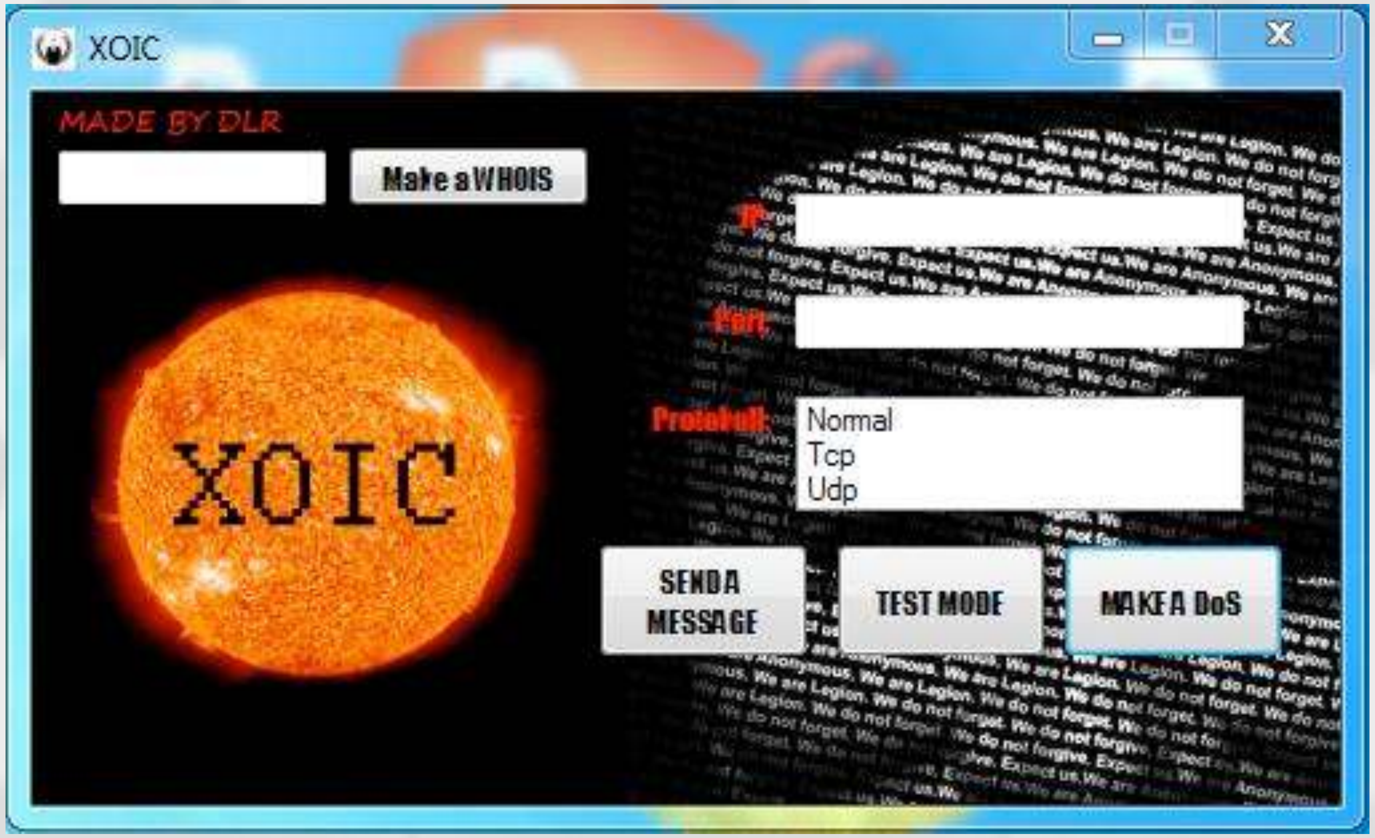
Like the Postal System

Application: Package / Letter Contents
(HTTP, DNS, SMTP)
Transport:
Certified Return Receipt (*TCP*) or Bulk (*UDP*)
Network: Source and Destination and *ICMP*
Data Link: Address Resolution Protocol (*ARP*)

XOIC and LOIC

Low Orbit Ion Cannon’s

Skill Needed: Low - script kiddie with botnet amplification

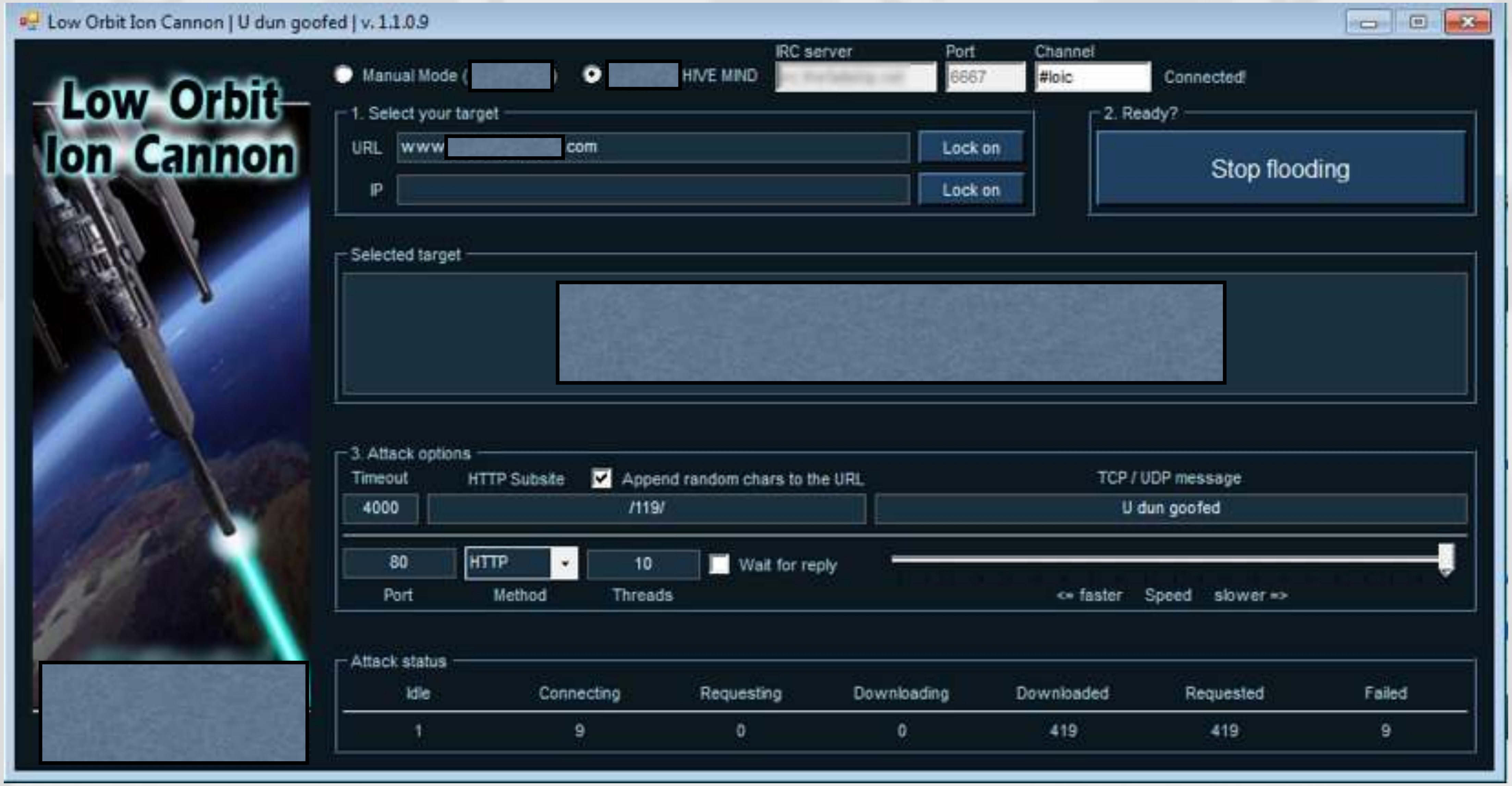


Matthew J. Harmon & Phil Reno

XOIC and LOIC

Low Orbit Ion Cannon’s

Skill Needed: Low - script kiddie with botnet amplification



Low Orbit Ion Cannon | U dun goofed | v. 1.1.0.9

○ Manual Mode ([redacted]) ● [redacted] HIVE MIND

IRC server: [redacted]

Port: 6667

Channel: #loic

Connected!

1. Select your target

URL: www [redacted] com

IP:

2. Ready?

Selected target: [redacted]

3. Attack options

Timeout: 4000

HTTP Subsite: /119/

☑ Append random chars to the URL

TCP / UDP message: U dun goofed

Port: 80

Method: HTTP

Threads: 10

□ Wait for reply

<= faster Speed slower =>

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
1	9	0	0	419	419	9

[redacted]

Good Publicity

Complexity: “Slashdot Effect”

Skill Needed:“Killer App” or Service

Impact

System Instability

System Overload

Pipes Full

Solution

Scale up and Content Distribution Network

Attacks (TCP + SSL)

Complexity: Easy

Skill Needed: Low - script kiddie
with botnet amplification

Impact

SSL Costs Attackers Resources
Router / Firewall NAT Table
Capacity of Upstream Network
Capacity of Physical Port

Matthew J. Harmon & Phil Reno

Attacks (HTTP)

Complexity: Moderate

Skill Needed: Low/Moderate

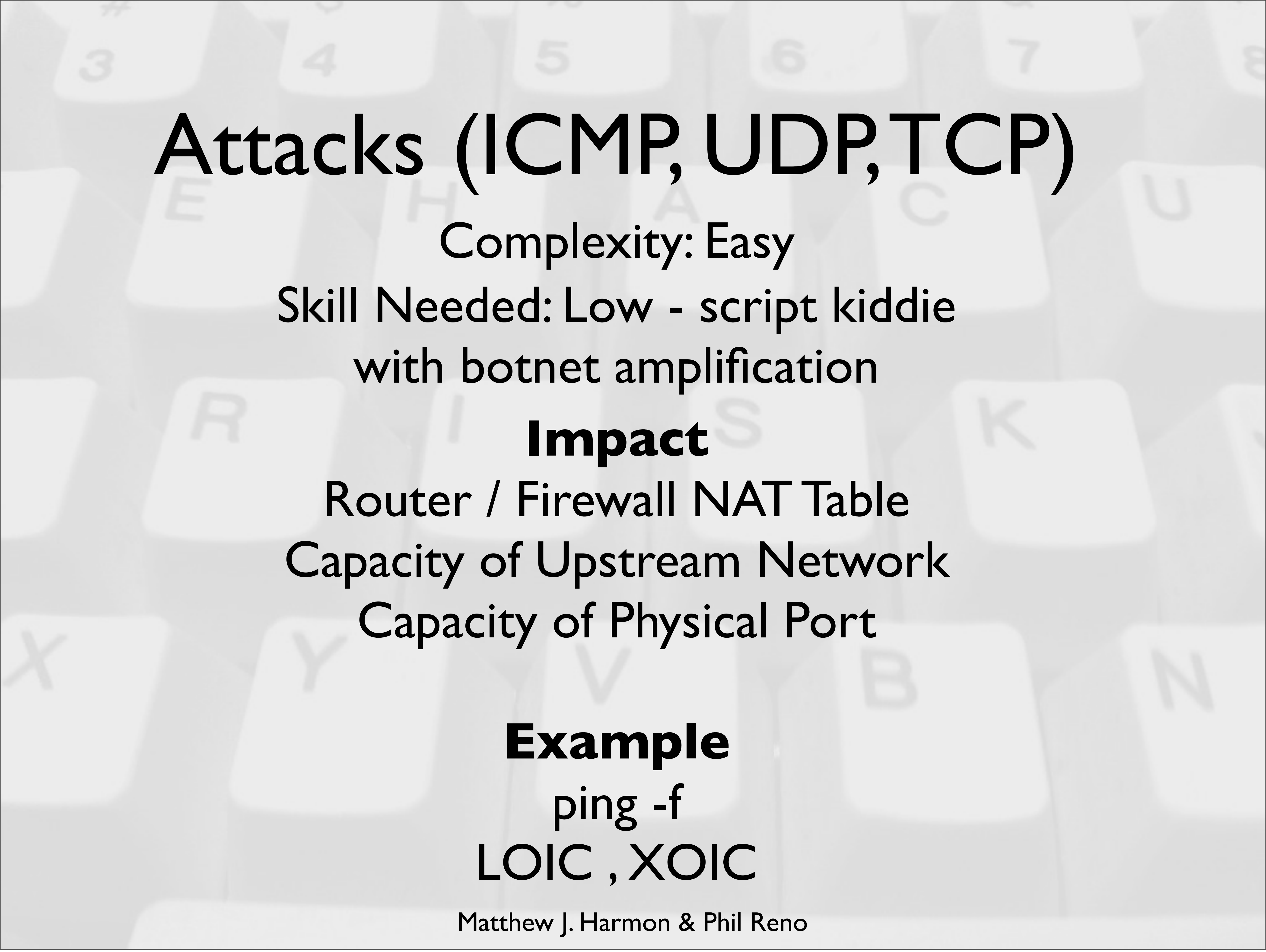
Motivated attacker with intelligence

Impact

Web Server
Kernel / Operating System

Chunked Header Attack (Apache, NGINX, IIS)
Slowloris Memory Exhaustion (All)

Matthew J. Harmon & Phil Reno



Attacks (ICMP, UDP, TCP)

Complexity: Easy

Skill Needed: Low - script kiddie with botnet amplification

Impact

Router / Firewall NAT Table

Capacity of Upstream Network

Capacity of Physical Port

Example

ping -f

LOIC , XOIC

DDoS Defense Architecture - Four Approaches

- **ISP** – including AT&T, Verizon, Century Link, Time-Warner (possibly others)
- **Cloud SOC, single IP or website via Proxy/DNS Redirect** – Services like Cloudflare, Neustar, Akamai KONA
- **Cloud SOC, able to do entire subnet** – Prolexic, Radware, Arbor, Imperva
- **In House / Homegrown** - <insert vendor name here>

DDoS Defense Architecture - ISP

ISP manages and maintains equipment, some ISP’s offer dedicated services and shared services

PROS

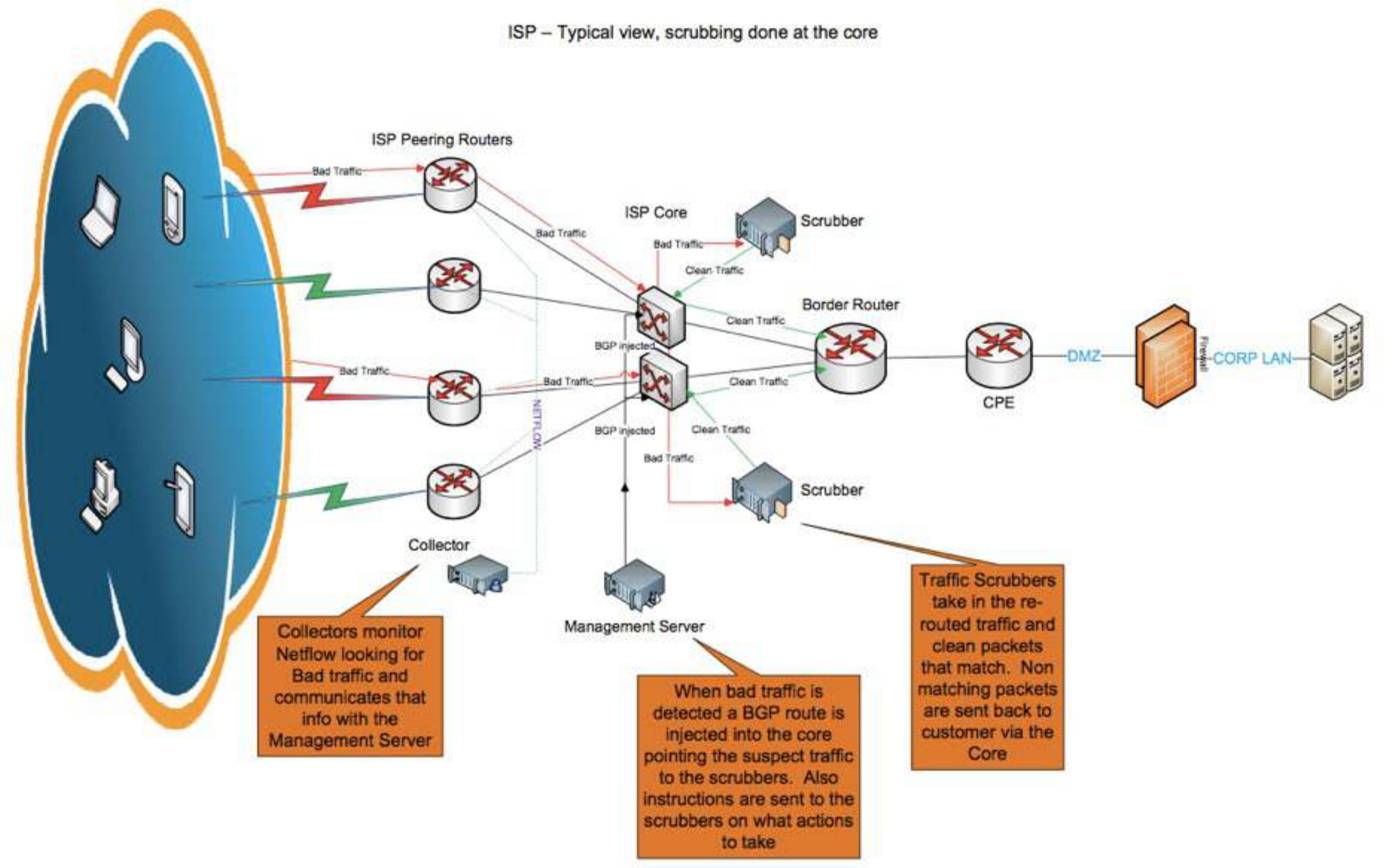
- Protects against volumetric and resource exhaustive attacks
- Scrubbing before your circuit
- Knowledgeable staff – lot’s of practice mitigating other customers getting attacked
- 24/7 monitoring with fast SLA’s
- Affordable (depending on ISP) – seen as a value add for existing circuit customers
- Extended view – like having a sniffer on the edge of the internet

CONS

- Scrubbing at the edge – Bad traffic from inside the ISP may get through, more scrubbers=more cost
- Scrubbing at the Core – Easier to size correctly at the edge, combination of peering routers throughput may exceed Core Scrubbing capability

Matthew J. Harmon & Phil Reno

DDoS Security Overview - Scrubbing at the Core



ISP – Typical view, scrubbing done at the core

Collectors monitor Netflow looking for Bad traffic and communicates that info with the Management Server

When bad traffic is detected a BGP route is injected into the core pointing the suspect traffic to the scrubbers. Also instructions are sent to the scrubbers on what actions to take

Traffic Scrubbers take in the re-routed traffic and clean packets that match. Non matching packets are sent back to customer via the Core

DDoS Defense Architecture - Cloud SOC Proxy/DNS

A Cloud provider that relies on you changing your DNS records to point traffic at them, typically these services are used to protect a single URL.

PROS

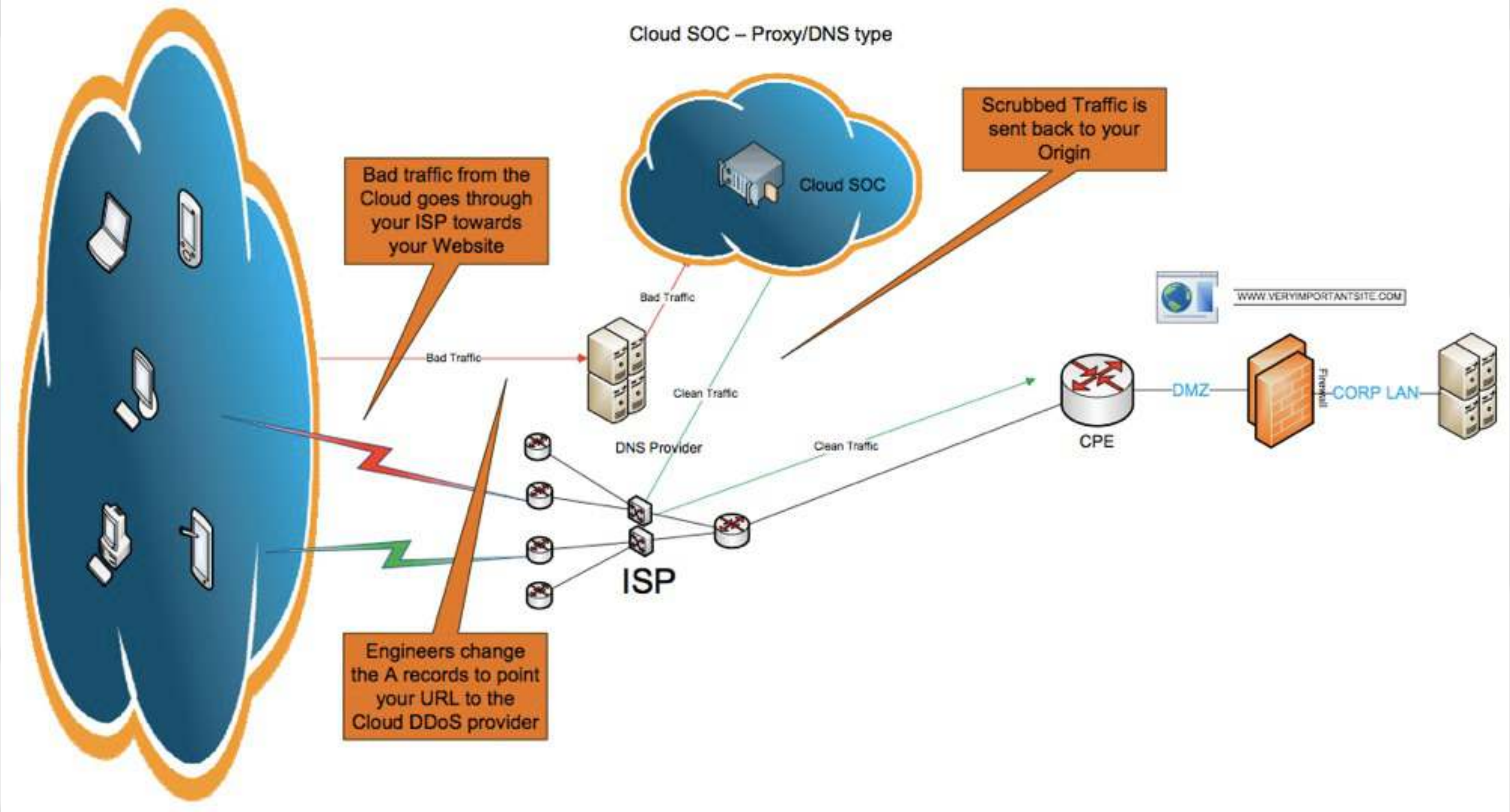
- Affordable – typically low monthly cost to retain service with increases that occur during an event
- Great for websites running in the cloud with little supporting infrastructure
- Knowledgeable staff – lot’s of practice when the other customers get attacked

CONS

- Monitoring – they are not actively monitoring your traffic because they can’t see it until you redirect you’re A records
- Your Origin IP is still open to attack, so this really only works when the attack is heading towards your URL
- Not scalable for entire subnets, Not protecting your circuit

Matthew J. Harmon & Phil Reno

DDoS Security Overview - Cloud SOC - Proxy/DNS



Cloud SOC – Proxy/DNS type

Bad traffic from the Cloud goes through your ISP towards your Website

Scrubbed Traffic is sent back to your Origin

Engineers change the A records to point your URL to the Cloud DDoS provider

Matthew J. Harmon & Phil Reno

DDoS Defense Architecture - Full Service

Similar to ISP, This Service provider puts a collection device in front of your firewall and uses BGP injection to route your traffic to their cloud during an event

DISCLAIMER Author has not directly interfaced with this type of vendor

PROS

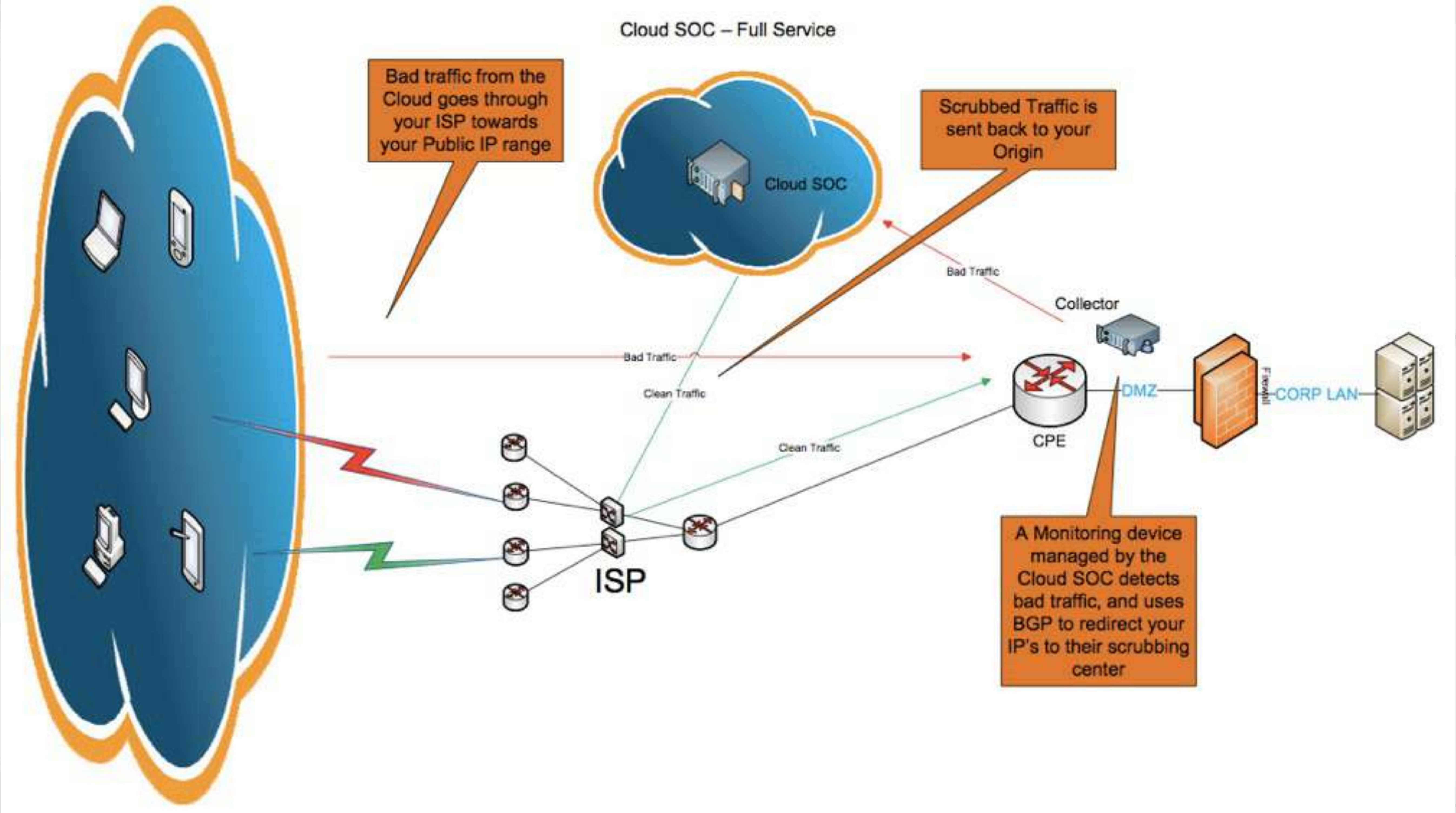
- Protects against volumetric and resource exhaustive attacks
- Scrubbing before your circuit
- Knowledgeable Staff
- 24/7 monitoring with fast SLA's

CONS

- More Hops – Scrubbers are not located inline with your ISP, so it is assumed that more hops are between you and the scrubbers
- Not all are created equal – Some say they are a full SOC in the Cloud but really only offer one to one IP scrubbing (Proxy/DNS types). Make sure you are asking a lot of questions and bring in more than one vendor to compare.

Matthew J. Harmon & Phil Reno

DDoS Security Overview - Cloud SOC - Full Service



Cloud SOC – Full Service

Bad traffic from the Cloud goes through your ISP towards your Public IP range

Scrubbed Traffic is sent back to your Origin

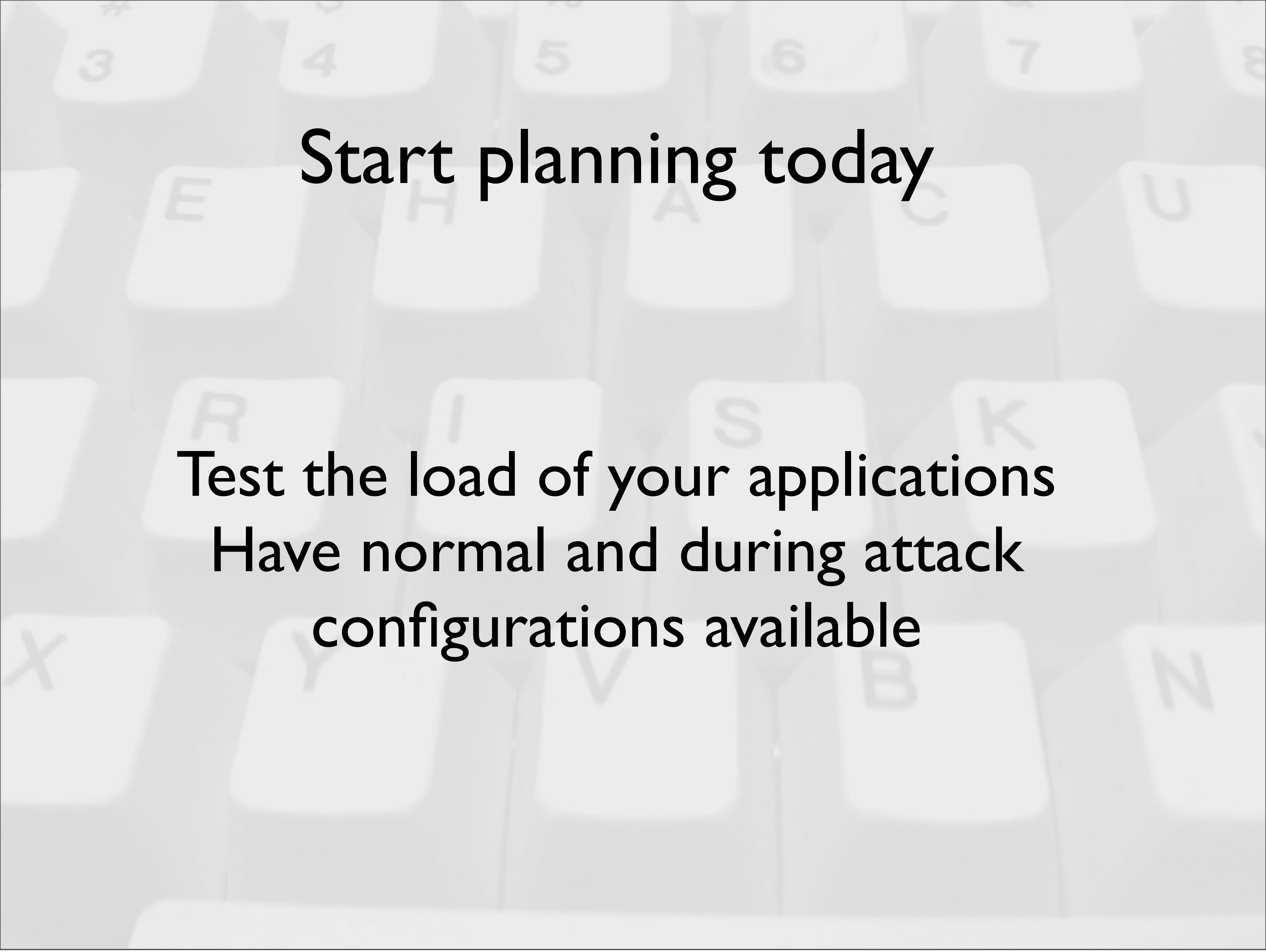
A Monitoring device managed by the Cloud SOC detects bad traffic, and uses BGP to redirect your IP's to their scrubbing center

Matthew J. Harmon & Phil Reno

Some questions to ask your DDoS provider

- Definitely drill into their cost structure!
- Know what their capabilities are for mitigation – do they do more than just signatures, can they mitigate HTTP, FTP, DNS, or VOIP based attacks
- Understand the exact process they use from DDoS event start to finish?
- Will they start scrubbing just because you are concerned?
- Did they build there own solution or are they using a known vendor partner?
- What kind of training does there staff get, do they perform fire drills?
- How many customers do they have?
- How frequently are they running mitigations?
- What are the SLA's?
- How long will they leave your traffic in a scrubber?
- What are you doing for DDoS protection against yourself? (Data Centers)

Matthew J. Harmon & Phil Reno



Start planning today

Test the load of your applications
Have normal and during attack configurations available

Be Ready to Scale

Chef - http://www.opscode.com/chef/

Puppet - http://puppetlabs.com

Scale and Verify

ANSIBLEWORKS
Radically simple IT orchestration

Ansible - http://ansibleworks.com

SALTSTACK

Salt Stack - http://saltstack.com/index.html

Fabric - http://docs.fabfile.org/en/1.8/

(ISC)^2 Twin Cities Area Chapter

isc2tc.org

@isc2tc on Twitter

(ISC)2 Twin Cities Area Chapter on LinkedIn