Distributed Denial of Service Attack (DDoS)

Steven Wallace

Enterprise Architect

Indiana University

Let's start with a true DDoS story...

A prominent security software firm loses all Internet connectivity

May 4th down for 17 hours
May 13th down for 8 hours
May 14th down for hours
May 15th down for 6.5 hours
May 16th, 17th, 18th, and 19th - (intercepted by ISP)

I-Light & Indiana GigaPOP

Why was the firm targeted?

A 13 year old kid in Kenosha, Wisconsin, known as “Wicked”, was retaliating for the firm referring to hackers as “script kiddies”.

On May 15th, using social media, Wicked starts publicly taunting the firm.

> “...the reason me and my 2 other contributers do this is because in a previous post you call us "script kiddies", atleast so i was told, so, i teamed up with them and i knock the hell out of your cicso router, and....im building up more bots…”

What was the firm’s recourse?

The security firm provided Wicked’s IP address and evidence he was the culprit to Wicked’s ISP…..despite follow-ups...ISP does nothing.

The security firm contacts the FBI, and provides detailed information on Wicked and his Bots. The FBI (actually competent and responsive), responds with:

- Below a $5,000 loss it’s not a crime (them’s the law)
- An FBI prosecution costs on average more than 200K (Wicked is kid’s stuff)
- Oh, and Wicked is actual a kid (aka minor), so not much would happen

What's the firm's takeaway?

The firm's CEO writes in his detailed account of the attacks:

"I hope it is becoming clear to everyone reading this, that we can not have a stable Internet economy while 13 year-old children are free to deny arbitrary Internet services with impunity." – Steve Gibson, Gibson Research Corporation, **July 2nd 2001**

What changed in 15 years (i.e., why is this a new worry)?

- DDoS tools are more accessible
- Networks are generally more reliable, and relied upon, so disruptions are more impactful
- Online gamers are introduced to DDoS tools, as they are frequently the attacked or attacker

What is a DDoS attack?

“A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system...Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic.”- wikipedia

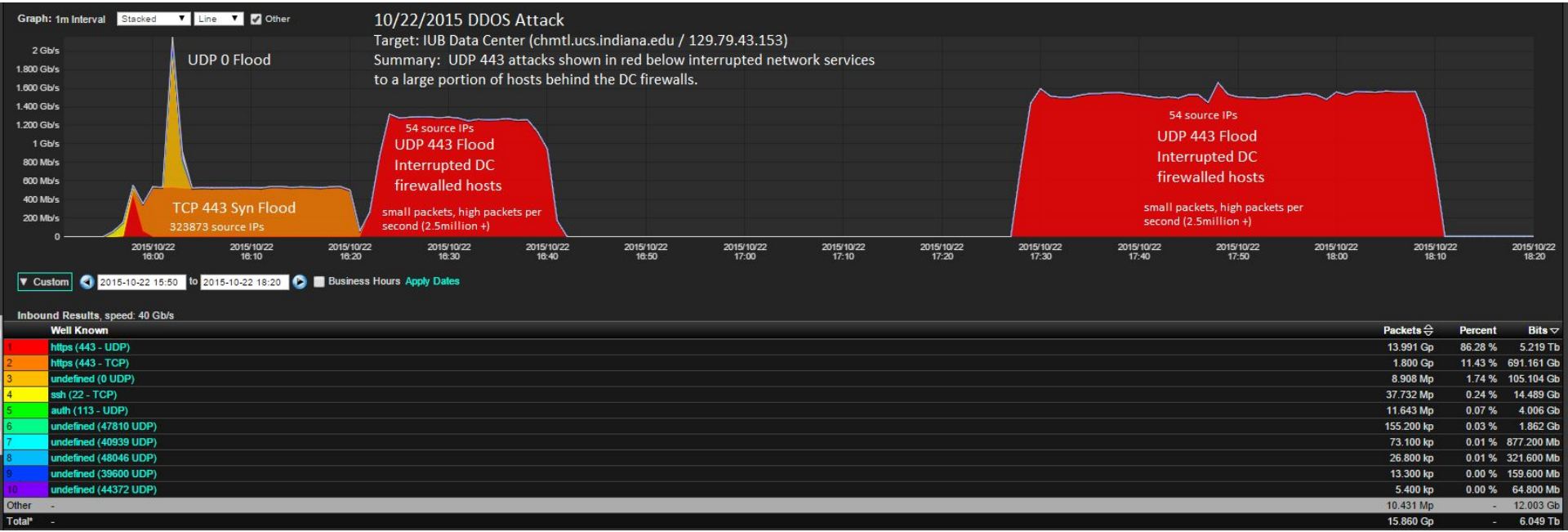
I-Light & Indiana GigaPOP

How frequently are DDoS attacks? Often!

Date	Time	Targets	Bandwidth	Number of Sources
4/19/2016	5:09PM - 5:11PM	1	3G	9k
4/23/2016	7:52AM - 7:55PM	1	3G	800
4/25/2016	1:45AM - 1:47AM	1	1G	10K
4/25/2016	2:23AM - 2:38AM	1	6G	2.3k
5/2/2016	9:43PM - 9:45PM	1	6G	11k
5/3/2016	12:00AM - 12:02AM	1	4G	13k

I-Light & Indiana GigaPOP

A Disruptive DDoS



Inbound Results, speed: 40 Gb/s

	Well Known	Packets	Percent	Bits
1	https (443 - UDP)	13.991 Gp	86.28 %	5.219 Tb
2	https (443 - TCP)	1.800 Gp	11.43 %	691.161 Gb
3	undefined (0 UDP)	8.908 Mp	1.74 %	105.104 Gb
4	ssh (22 - TCP)	37.732 Mp	0.24 %	14.489 Gb
5	auth (113 - UDP)	11.643 Mp	0.07 %	4.006 Gb
6	undefined (47810 UDP)	155.200 kp	0.03 %	1.862 Gb
7	undefined (40939 UDP)	73.100 kp	0.01 %	877.200 Mb
8	undefined (48046 UDP)	26.800 kp	0.01 %	321.600 Mb
9	undefined (39600 UDP)	13.300 kp	0.00 %	159.600 Mb
10	undefined (44372 UDP)	5.400 kp	0.00 %	64.800 Mb
Other	-	10.431 Mp	-	12.003 Gb
Total*	-	15.860 Gp	-	6.049 Tb

At 16:20 the attacked morphed to a sustained UDP 433 flood on the target.

- This disrupted routing protocols to IUB DC firewalled networks & services
- IT Notice went out for this disruption

· The first attack stopped then showed up again just before 17:30.

- This disrupted routing protocols to IUB DC firewalled networks & services

I-Light & Indiana GigaPOP

What's the worst case scenario?

- Sit down first - then google "Rutgers DDoS"
- All Internet down for many, many hours
- Zero ability to mitigate attack for days
- Attack repeats again and again over the course of weeks and months
- The entire campus is taunted via social media

Defending Against a DDoS Attack

- First step is knowing you're being attacked, and, specifically, what host is being attacked
- The Indiana GigaPoP and I-Light are working towards developing the capability to detect attacks against members

Defending Against a DDoS Attack

- Some attacks can be simply absorbed (i.e., they aren't intense enough to cause a problem)
- Attacks typically last only a few minutes, and target gamers

Defending Against a DDoS Attack

- If the attack can't be absorbed, then it needs to be blocked or scrubbed
- The Indiana GigaPoP and I-Light are developing means for members to drop DDoS traffic upstream
- The GigaPoP is also working with Internet2 to develop a scrubbing service

I-Light & Indiana GigaPOP

Defending Against a DDoS Attack

Scrubbing vs. Blocking

- Blocking means what it says, *all* traffic to the attacked host is dropped before it gets to the campus
- Scrubbing re-routes all traffic to the attacked host to a scrubbing center, where computers remove the attack traffic and return the normal traffic

I-Light & Indiana GigaPOP

Oct 21st…..a bad day for the Internet

Dyn is taken down via a massive DDoS attack