

Distributed Denial of Service (DDoS) Effects, Mitigations & Future

Tony Barber Nov 2013 TF-NOC

Wayne Routly, DANTE
GEANT APM, Vienna
8 October, 2013

- **Effects**
 - Real World Examples
- **Mitigations**
 - What Are We Doing Today
 - What Are We Doing Tomorrow
- **Future Plans**
- **Your Ideas – Lesson Learned**

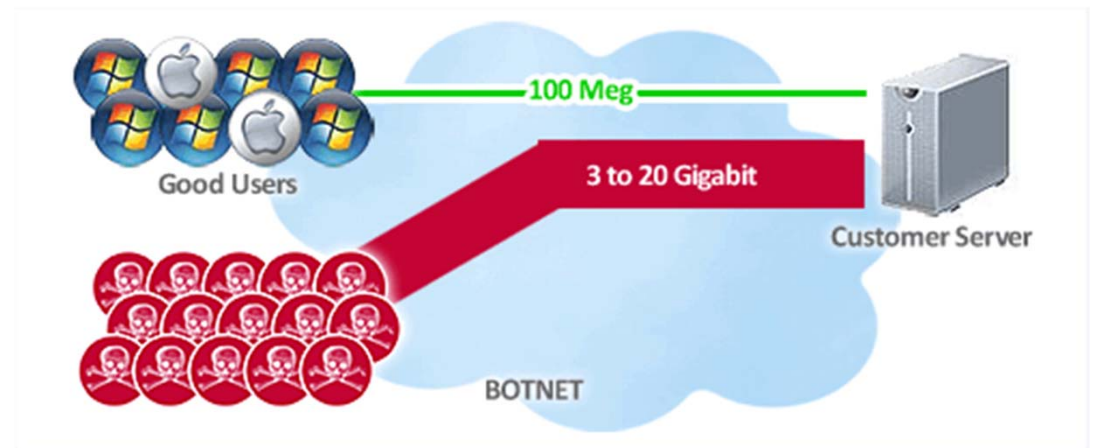


DDoS For DUMMIES



- **DDoS Attack**

- “Attackers” - Multiple Infected Machines
- Target **Single** Machine
- Inbound Traffic **Floods** Victim



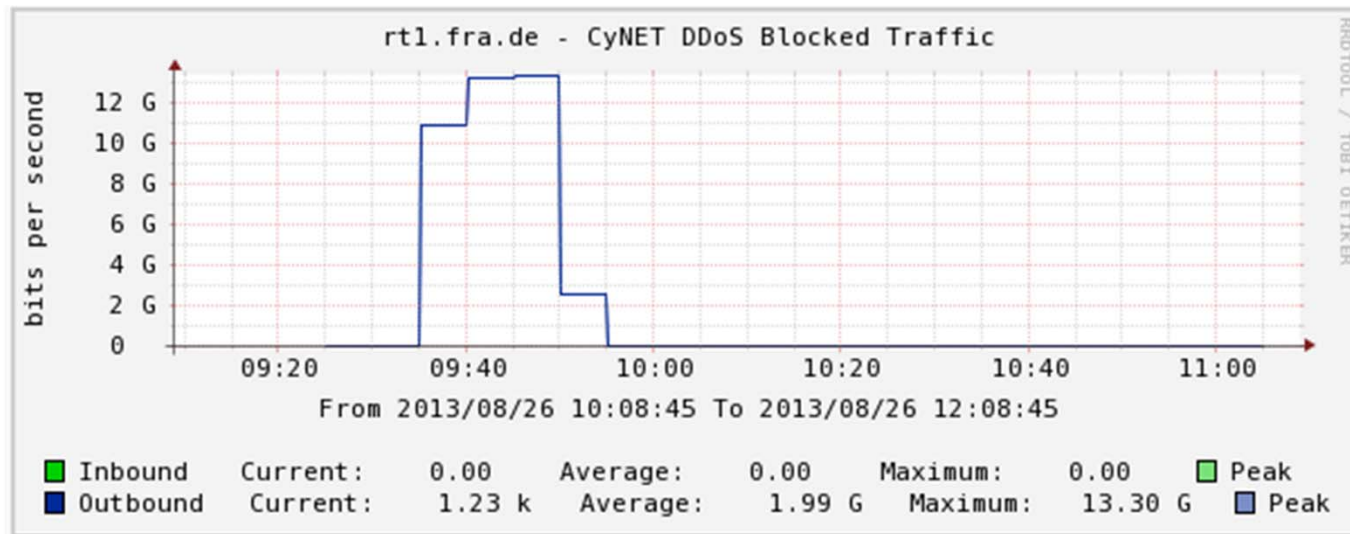
- **Problems**

- Potentially **Thousands Sources**
- “Difficult” to stop Attack
- Difficult to distinguish **legitimate traffic**

Effects – CYNET DDoS



- Destination IP: The University of Cyprus (www.ucy.ac.cy)
- Port Ranges: 0, 2070 and 3475
- Multiple Source IP's and source AS's.
- Multiple Actions Taken
- Attack peak: **Over 13Gbps over 1Gbps link**



Effects – CYNET DDoS [2]



Destination AS 3268 Traffic

Date first seen	Dst IP Addr	Flows (%)	Packets (%)	Bytes (%)
2013-09-02 04:58	194.42.1.1	124919(97.2)	440.6 M(99.2)	517.4 G(99.5)
2013-09-02 04:59	82.116.202.17	129(0.1)	143000(0.0)	154.3 M(0.0)
2013-09-02 05:00	194.42.22.9	128(0.1)	244000(0.1)	12.3 M(0.0)
2013-09-02 04:59	194.42.1.50	114(0.1)	57000(0.0)	10.5 M(0.0)
2013-09-02 04:59	82.116.192.118	90(0.1)	239500(0.1)	311.4 M(0.1)
2013-09-02 04:59	194.42.1.55	81(0.1)	40500(0.0)	8.7 M(0.0)

Destination ports for 194.42.1.1

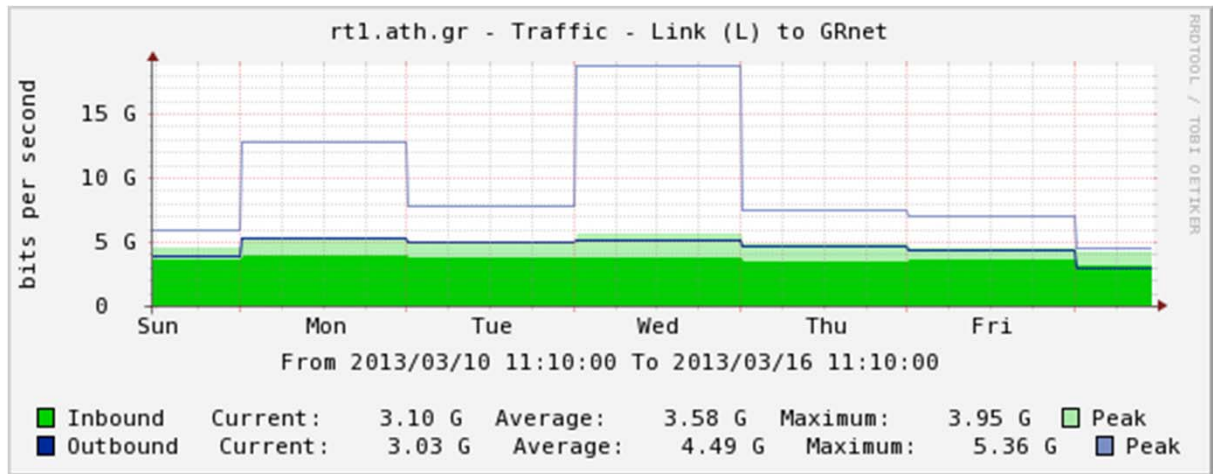
Date first seen	Dst Port	Flows (%)	Packets (%)	Bytes (%)
2013-09-02 04:58	2070	47268(37.8)	144.2 M(32.7)	182.4 G(35.3)
2013-09-02 04:58	0	46315(37.1)	260.0 M(59.0)	295.4 G(57.1)
2013-09-02 04:58	3475	29714(23.8)	31.3 M(7.1)	39.2 G(7.6)
2013-09-02 04:58	771	1348(1.1)	4.3 M(1.0)	243.6 M(0.0)
2013-09-02 04:58	769	145(0.1)	516000(0.1)	29.0 M(0.0)
2013-09-02 04:58	2816	55(0.0)	199500(0.0)	16.7 M(0.0)
2013-09-02 04:58	1024	30(0.0)	114500(0.0)	6.4 M(0.0)

Effects – GRNET DDoS



DNS Amplification Attack

- **Destination IP:** GRNET
- **Port Ranges:** 53 (DNS)
- **Multiple Source IP's and source AS's.**
- **Multiple Actions Taken**
- **Attack peak: 20G over 20G link**



Date first seen	Dst IP Addr	Flows (%)	Packets (%)	Bytes (%)
2013-03-13 09:34	194.177.211.102	35531(7.8)	36.1 M(11.3)	53.5 G(11.9)
2013-03-13 09:34	194.177.211.100	34632(7.6)	35.6 M(11.1)	52.6 G(11.7)
2013-03-13 09:33	194.177.211.101	34469(7.6)	35.3 M(11.1)	52.2 G(11.6)
2013-03-13 09:33	194.63.239.233	49621(11.0)	31.8 M(10.0)	44.3 G(9.9)
2013-03-13 09:33	194.63.239.234	48220(10.6)	27.1 M(8.5)	36.7 G(8.2)
2013-03-13 09:33	194.63.239.237	39278(8.7)	26.1 M(8.2)	36.5 G(8.1)

Mitigations – TODAY



- NSHaRP Process
 - NRENS Subscribed
 - **Anomaly Detection**
 - Notification of Events
 - *Email, Evidence*
 - *Trouble Ticket*
- Remediation – DANCERT / GEANT NOC
 - **Filter (Block)**
 - **Rate Limit**



Mitigations – TOMORROW



- Firewall on Demand

FoD is a security provisioning service**inject firewall-like rules at the upstream level** and mitigate attacks there...using **BGP FlowSpec**

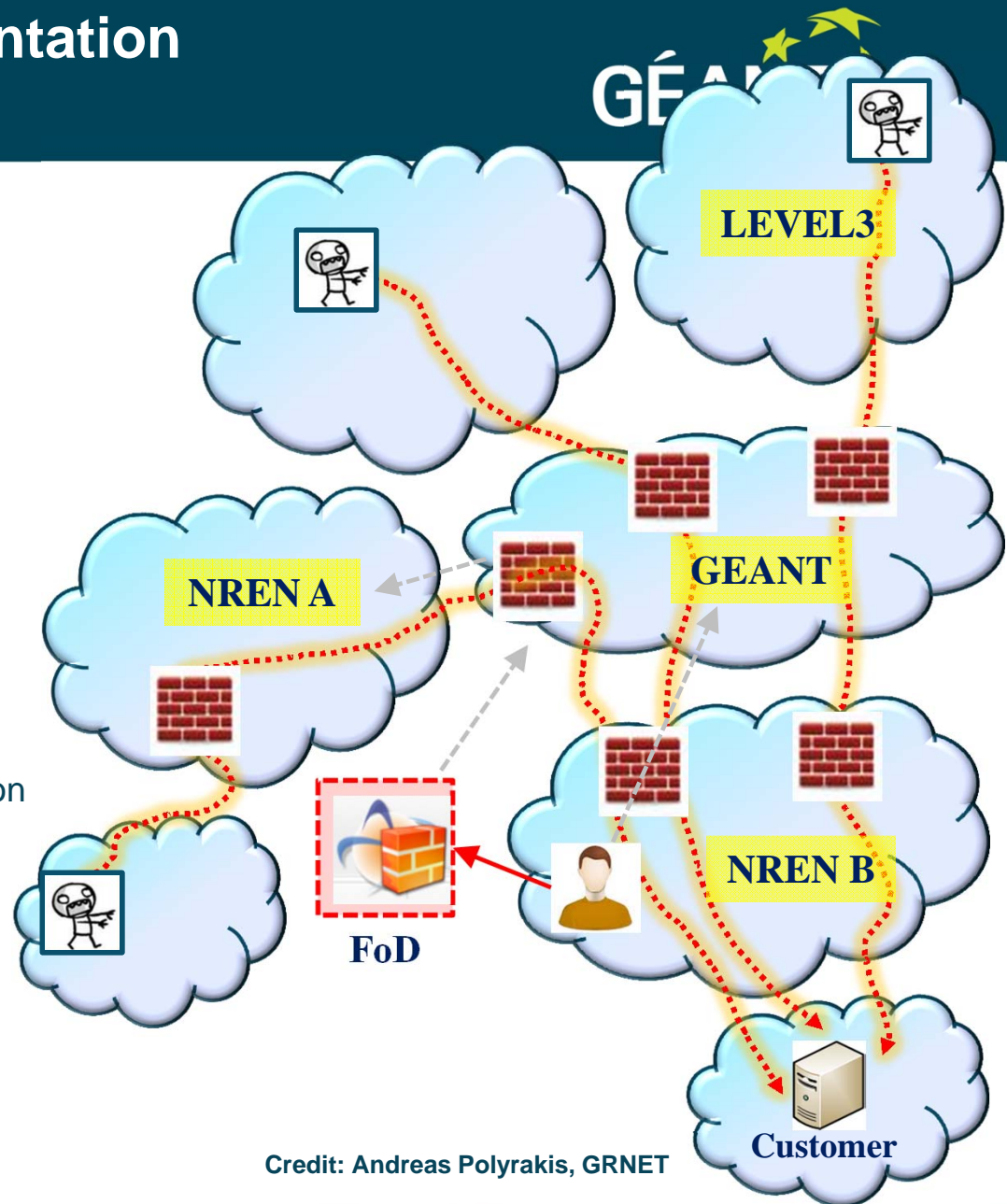
- Incorporate into NSHaRP Service
 - Enhanced Customer Capabilities
 - **Complete Incident Lifecycle**

- Time Frame
 - Phase 1 – **End 2013**
 - *GEANT Athens Router*
 - Phase 2 – **Early 2014**
 - *All GEANT Routers*
 - *API*



Future – FoD Implementation

- **NSHaRP Customer** or GN NOC logs into web tool and describes **flows and actions**
- Flow destination is **validated** against the customer's **IP space**
- Dedicated router is configured to **advertise the route via BGP flowspec**
- iBGP propagates the tuples to all GEANT routers.
- **Dynamic firewall filters** are implemented on all routers
- Attack is **mitigated** (dropped, rated-limited) upon entrance
- **End of attack: Removal via the tool, or auto-expire**



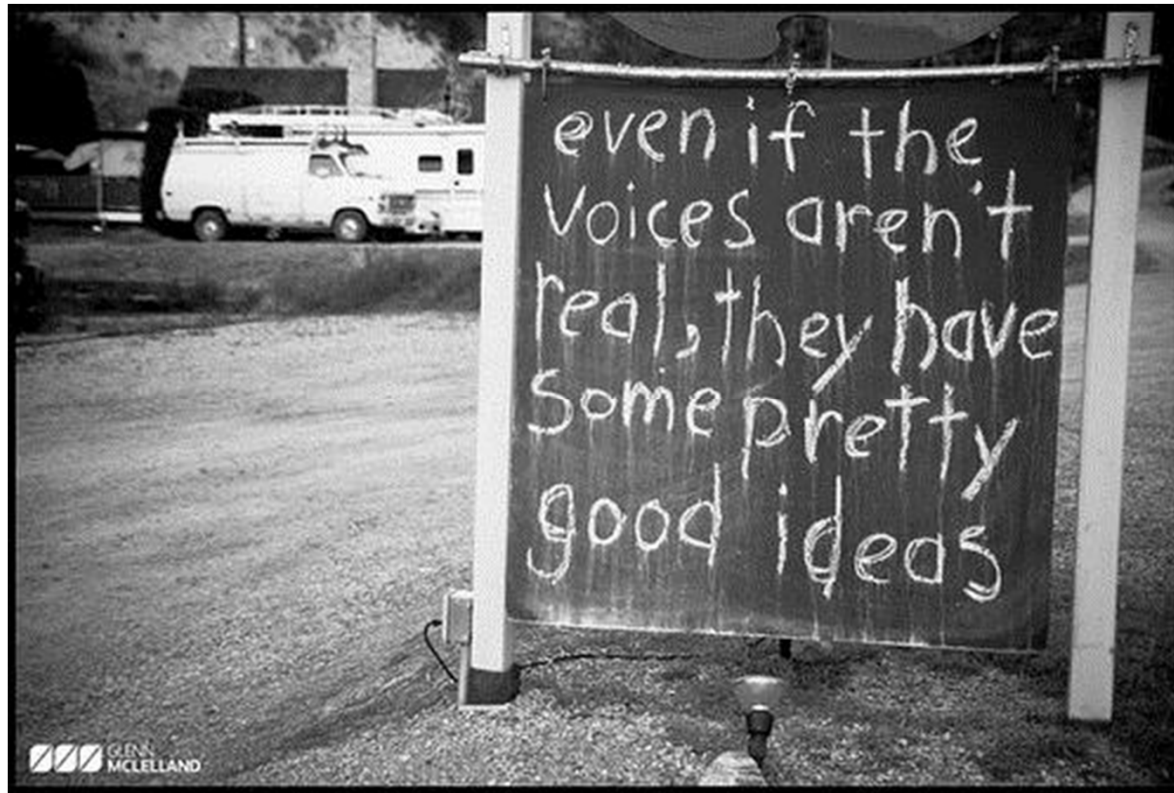
Credit: Andreas Polyraakis, GRNET

..... **better tools** to mitigate **transitory** attacks and anomalies

- “**Better**” in terms of
 - **Granularity:** Per-flow level
 - *Source/Dest IP/Ports, protocol type, DSCP, TCP flag.....*
 - **Action:**
 - *Drop, rate-limit, redirect*
 - **Speed:** More responsive
 - *(Seconds / Minutes vs. Hours / Days)*
 - **Efficiency:**
 - *Closer to the source, Multi Domain*
 - **Automation:**
 - *Integration with other systems (IDS/IPS)*
 - **Manageability**

Credit: Andreas Polyraakis, GRNET

Your Ideas, Your Thoughts



Experience is the best teacher . . .

Thank you!



Connect | Communicate | Collaborate

www.geant.net

www.twitter.com/GEANTnews | www.facebook.com/GEANTnetwork | www.youtube.com/GEANTtv

