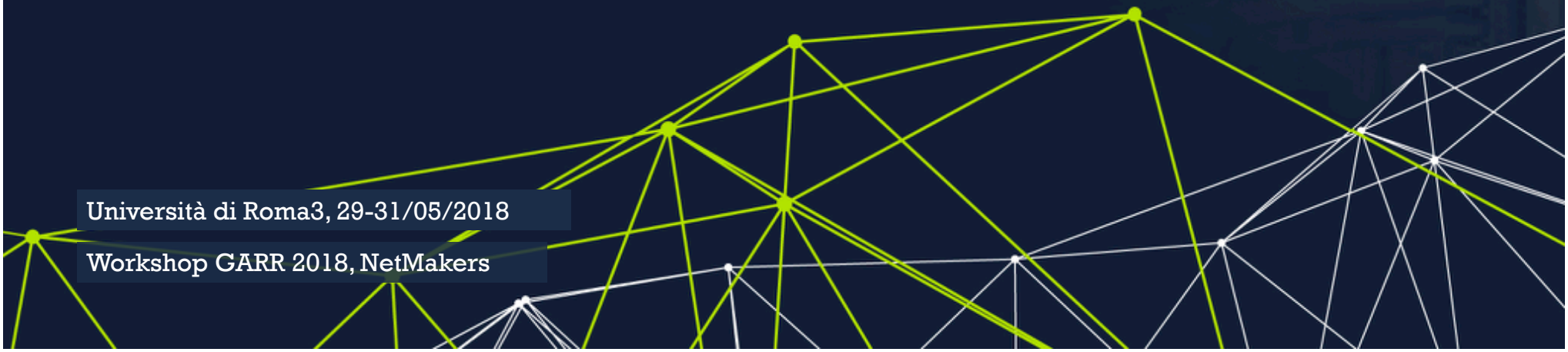
Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Mitigazione dei DDoS
Work in Progress

MASSIMO CARBONI



Università di Roma3, 29-31/05/2018

Workshop GARR 2018, NetMakers

Agenda

Motivazione e Caratterizzazione delle Minacce

- Punto di vista «esterno»
- Punto di vista «GARR»

Attività di Scouting

- Individuazione piattaforme per il PoC

Attività di PoC

- Schema generale e dell'ambiente di test
- Risultati

Conclusioni e prossimi passi

Attacchi DDoS

Volumetrici su Larga Scala

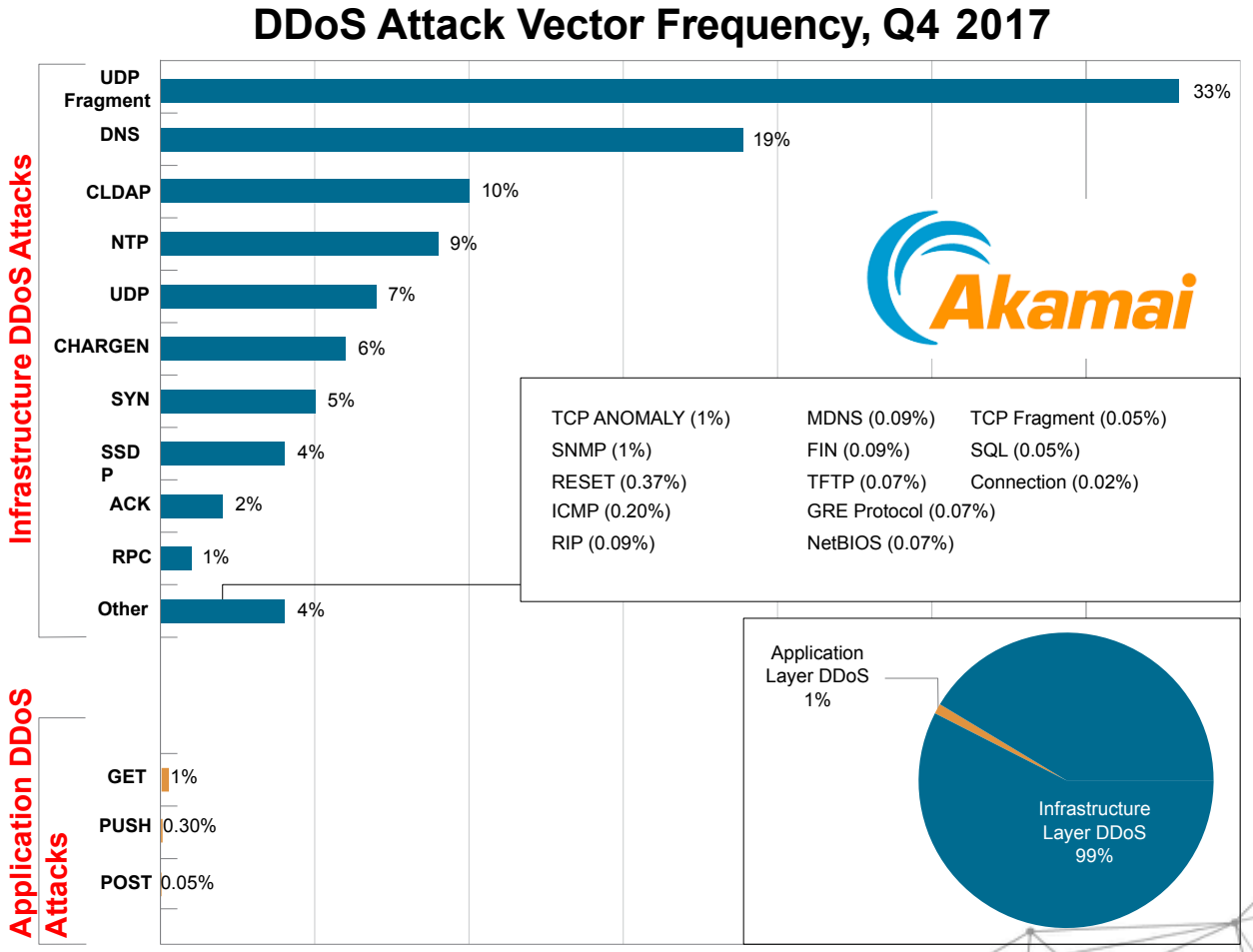
- Impatto su tutta l'utenza GARR (es. accesso Global Internet)

Volumetrici

- Impatto sull'utenza oggetto dell'attacco o su di un gruppo limitato di utenti connessi attraverso la medesima infrastruttura

Applicativi

- Impattano una singola applicazione

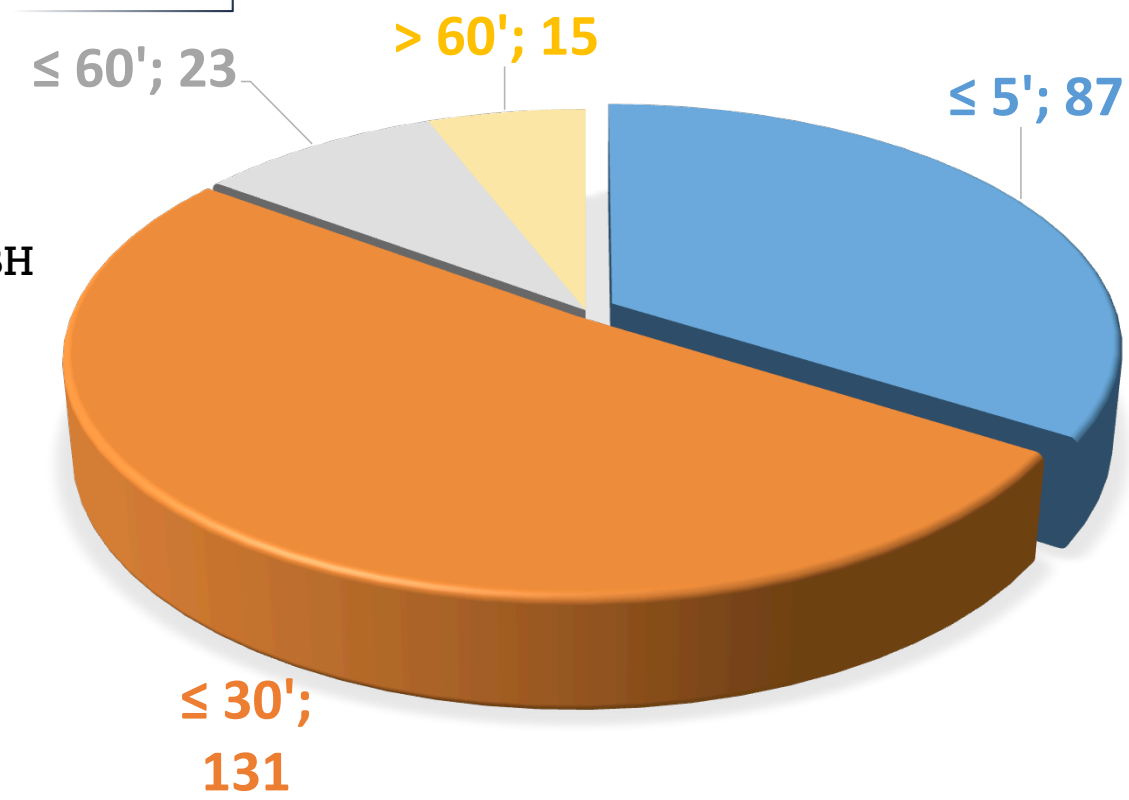


Durata degli attacchi DDoS

L'80% degli attacchi dura meno di 30'

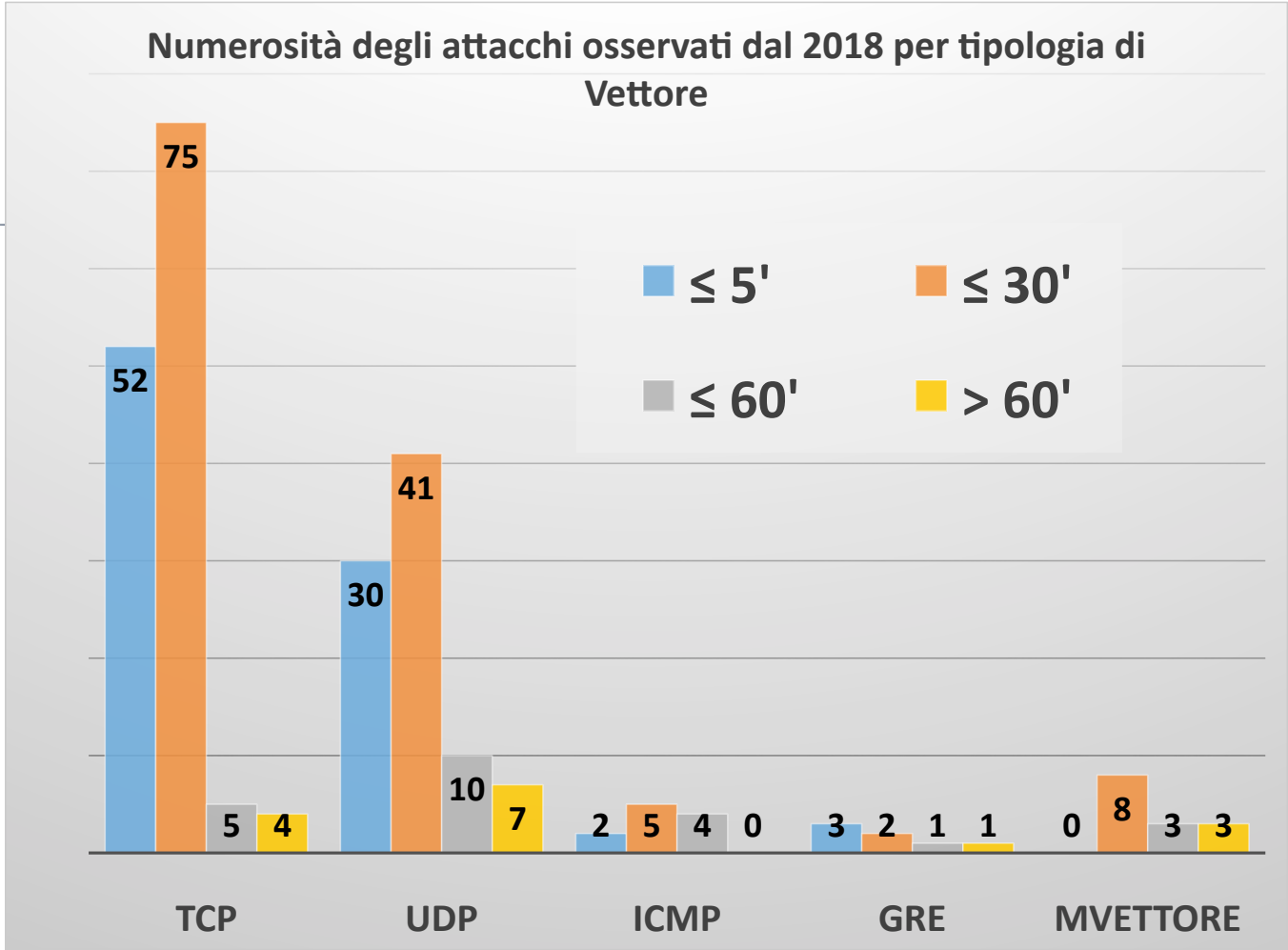
Processi standard lenti

Rimedi adottati talvolta estremi → RTBH



Vettori di Attacco

- Riduzione del numero di attacchi di tipo «Volumetrico UDP»
- Incremento degli attacchi TCP e UDP mirati alle applicazioni
- Vediamo ancora (per quanto?) un numero ridotto di attacchi multi-vettore



Analisi Tecnica Preliminare

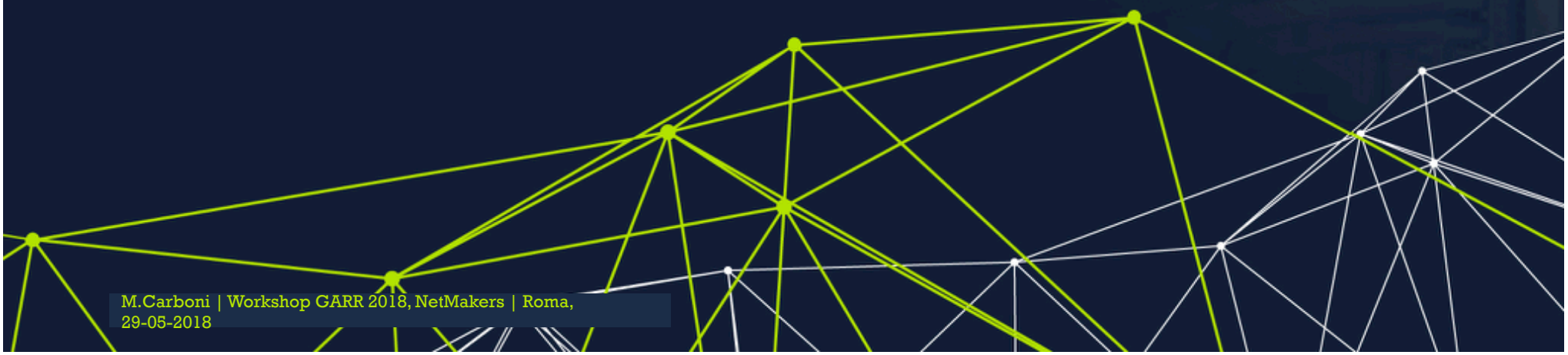
Abbiamo strumenti interni di monitoraggio Netflow

- Servono 20’ per avere informazioni abbastanza precise sugli attacchi
- Gli attacchi che individuiamo durano meno di questo tempo e dobbiamo decidere cosa è rilevante
- Per questo tipo di attacchi il nostro è uno strumento di reportistica

Attacchi percepiti come un malfunzionamento di rete

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Cosa Servirebbe



M.Carboni | Workshop GARR 2018, NetMakers | Roma, 29-05-2018

Necessità

Visibility
- Identificare i DDoS rispetto al traffico lecito
- Io conosco la rete i comportamenti Base e dunque so distinguere le Deviazioni e le Anomalie

Detection
- Avere la possibilità di distinguere tra traffico legittimo e traffico «malevolo»
- NF (L3/L4) consente di avere informazioni sul numero di flussi, volume, porte, ecc. Può fornire molti falsi positivi → serve aggiungere dei criteri

Control
- Rilevante per GARR dobbiamo decidere cosa proteggiamo:
  - Accessi Utente, Applicazioni, Protocolli, Servizi
  - Agisco Internamente /Esternamente

Mitigation
- Butto tutto o mitigo, con procedure concordate (vedi RTBH)

Report
- Analisi dell'accaduto in termini di durata, tipo, volume, ecc. Informazioni riguardanti il modo con cui è stato identificato, chi ha innescato il processo ecc.

Necessità

Indagine di Mercato

Nel mercato ci sono una serie di soggetti che agiscono come gestori di tematiche DDOS, la questione è chi tra questi detiene le soluzioni hw e sw che possono indirizzare le nostre necessità

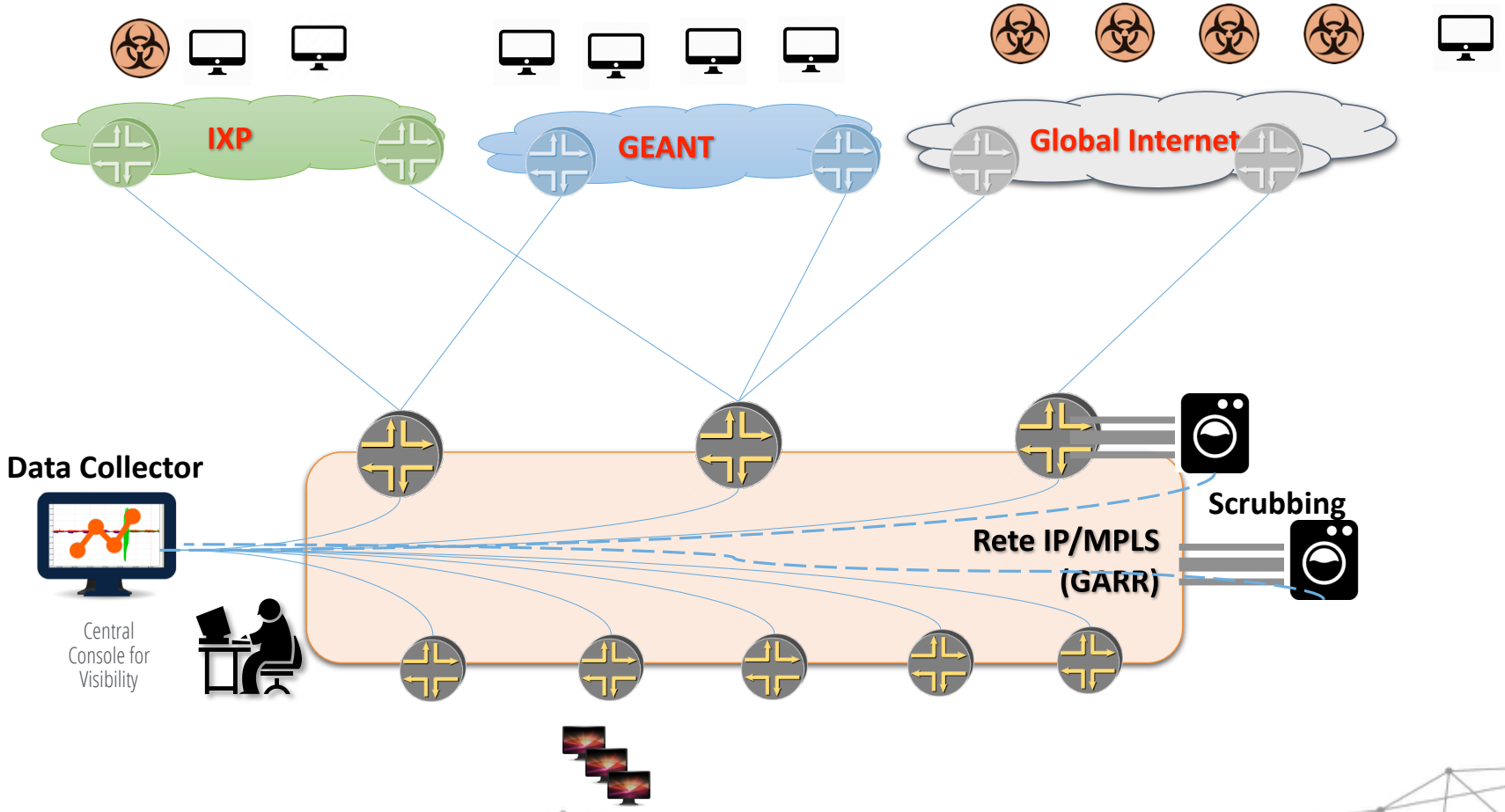
Arbor:

Strumento scalabile di analisi di traffico e **Visibility** evoluta verso la protezione di attacchi *DDoS*. **Detection** basata su ***Netflow*** *e DPI,* BGP e SNMP e arricchita da servizi di ***IP Intelligence***. **Mitigation** basata su BGP e appliance dedicata con funzioni stateless

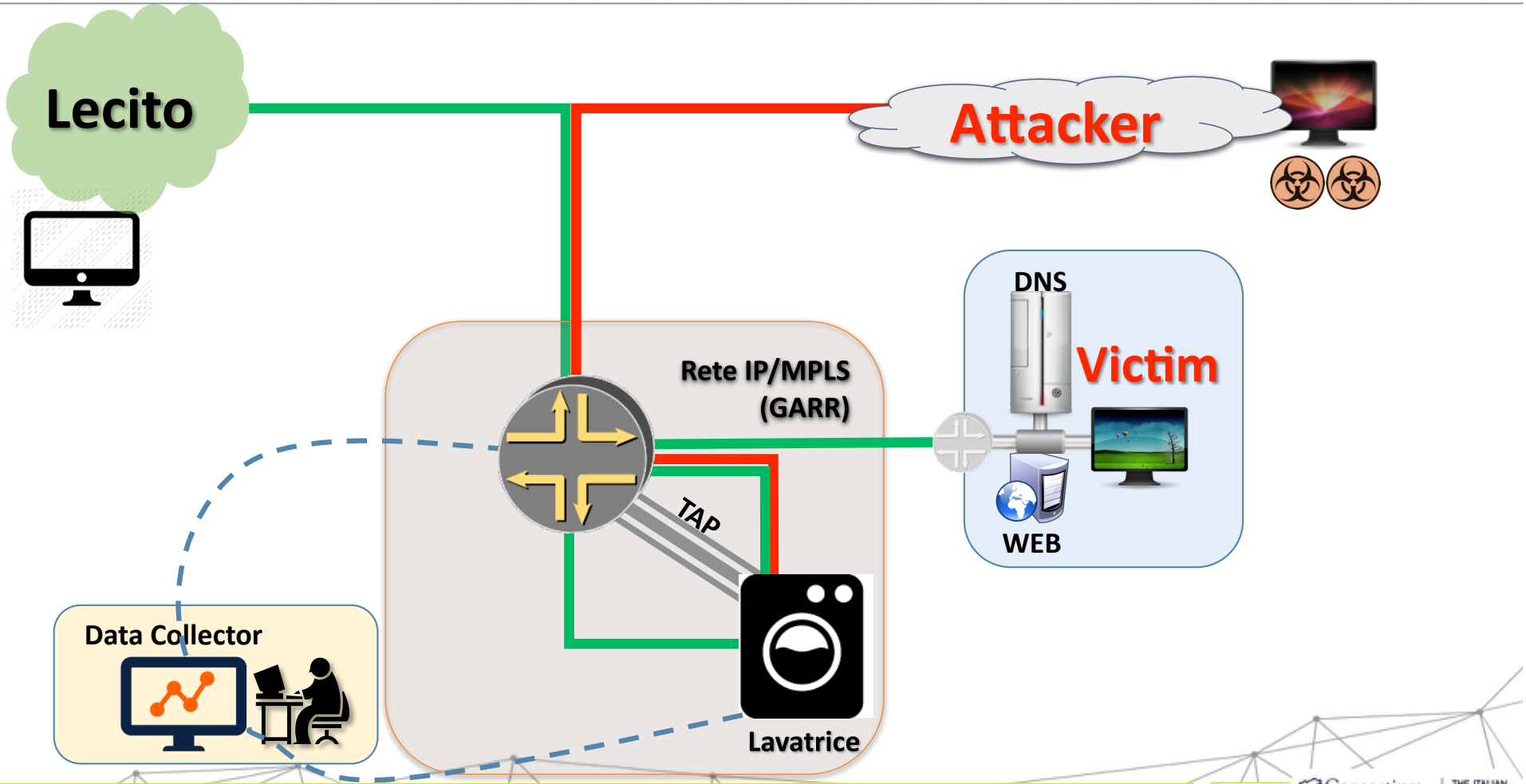
Radware:

Elementi chiave **Detection** e **Mitigation** (L3-L7), soluzione di tipo inLine (TAP-mode), usa algoritmi di ***Behavioral Analysis***. Soluzione aperta: **Detection** non solo ***Netflow***, offerta di API e integrazione con le più svariate terze parti, anche open source

Qual è l'Architettura di Mitigazione



Ambiente di PoC



Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Risultati delle POC

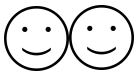
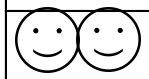
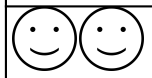
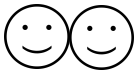
GARR: N.Ciurleo, S.d'Ambrosio, M.Marletta, E.Gucciardi, A.Inzerilli

Arbor: A.Tagliarino, M.DiDedda

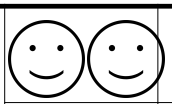
Radware: F.Palozza, M.Vinci, S.Cozzi

Ringrazio Arbor e Radware per il supporto nell'attivita' di PoC

Arbor: risultati

Visibility		**Vettori di Attacco:** Identificazione dettagliata, particolarmente efficace nella gestione di attacchi *multivettore*
Detection		**Global Detection:** Protezione di base di tutta la rete
		**Attacchi noti:** Algoritmo di riconoscimento attacchi noti efficace e con *pochi casi falsi positivi*. Rilevamento attacchi distribuiti (DDoS) e non distribuiti (Dos)
Control		**Web-GUI**: interfaccia di lavoro intuitiva, dispone di *viste utente*. Interfaccia di gestione della lavatrice (TMS) integrata con il sistema
		**Scalabilità:** ***Numero elevato*** di managed object supportati
		**Programmabile:** *Interfaccia di gestione* dei *managed object flessibile*, integrazione con DB GARR
Mitigation		**TMS:** ***Controllo del traffico*** in transito su lavatrice con evidenza sull'azione dei filtri
		**Diversion:** Supporto a varie tecniche: ***RTBH, BGP next hop, BGP flowspec drop to VRF***
		**Router-FlowSpec:** Supporto dei filtri flowspec per bloccare gli ***attacchi più semplici*** ma significativi direttamente sui router
Report		**Analisi:** fornisce la documentazione rispondente ai fatti. Fornisce informazioni complete, aggiunge informazioni di correlazione tra vettori di attacco multipli

Radware: risultati del PoC

Visibility		**SmartAP**: in questa modalità è in grado di identificare un attacco in tempi estremamente rapidi, con limitate informazioni riportate al gestore (/utente) ➔ Magic Box
		**Behavioral DoS**: è efficace nell'identificare e distinguere dettagliatamente il traffico malevolo, consentendo di bloccare il solo traffico d'attacco
Detection		**Global Detection:** il sistema non prevede questa funzione
		**Attacchi noti:** funzione attiva solo nel caso di traffico Mirror (inLine), Gestisce signature applicative di traffico malevolo (port scan, ecc)
Control		**Web-GUI**: interfaccia di lavoro da migliorare (java), coerente con l'approccio (Magic Box, manca la visione integrata della lavatrice con il resto del sistema
		**Scalabilità:** ***limitato numero*** di *protected object* supportati → *Richiede un diverso modello di implementazione, mediante soluzioni esterne*
		**Programmabile:** ***Interfaccia di gestione*** dei *protected object* ***flessibile***, integrazione con DB GARR. Integrazione con strumenti di 3th (sonde, firewall, LLB, ecc.)
Mitigation		**DP:** ***Controllo del traffico*** su lavatrice con scarza evidenza sull'azione dei filtri, "***insegue***" dinamicamente (20sec) anche in caso di variazione dei vettori di attacco
		**Diversion:** Supporto a varie tecniche: ***BGP next hop, BGP flowspec drop to VRF***
		**Router-FlowSpec:** non disponibile
Report		**Analisi:** fornisce una limitata documentazione in relazione agli eventi. In ragione della velocita' di «reazione» (<1 minuto) non mette in relazione eventi nel tempo.

GARR: N.Ciurleo, S.d'Ambrosio, M.Marletta, E.Gucciardi, A.Inzerilli

Arbor: A.Tagliarino, M.DiDedda

Radware: F.Palozza, M.Vinci, S.Cozzi

Riassunto dei risultati		Arbor	Radware
Visibility	Vettori di Attacco	🙂	🙂🙂
Detection	Global Detection	🙂	😐
	Attacchi noti	🙂	😐
Control	Web-GUI	🙂🙂	😐
	Scalabilità	🙂🙂	😐
	Programmabile	😕	🙂🙂
Mitigation	Washing Machine	😐	🙂
	Diversion	🙂🙂	🙂
	Router-FlowSpec	🙂	☹
Report	Analisi/ Documentazione	🙂🙂	😐

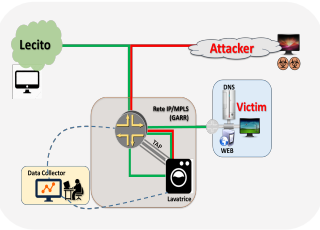
Cosa abbiamo Imparato

Traffico GARR non predicibile → BURST + Commodity Internet

Bacchette magiche non ne abbiamo trovate

Che nessuno è perfetto, nemmeno GARR:

- Dobbiamo rivedere alcuni aspetti del **disegno di rete IP/MPLS**
- Gestione separata del traffico **Clean** da quello **Dirty**

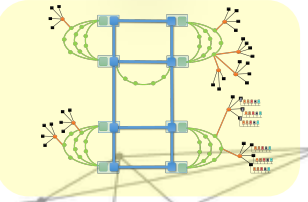


Che un sistema di mitigazione dei DDoS non è una «pozione magica», se non correttamente inserito nei processi operativi interni è potenzialmente in grado di portare via molte risorse:

- Tecniche, Economiche, Umane

Abbiamo bisogno di rivedere il disegno di rete IP/MPLS

- Dobbiamo implementare funzioni non previste inizialmente



Conclusioni

A fronte della revisione di rete GARR, potremo adottare un sistema in grado di affiancare l'azione del GARR-NOC e del GARR-CERT riguardo alla **Mitigazione** degli attacchi DDoS

- La tecnica del RTBH (SdA) rappresenta una soluzione tecnica sufficiente?

È necessario riconsiderare la questione del **Controllo** come processo chiave nella implementazione di una qualsiasi soluzione

- GARR deve agire solo quando è messa a rischio la funzionalità di rete globale (**Attacchi Volumetrici**)
- APM deve essere in grado di vedere (**Visibilità**) cosa sta accadendo e decidere di agire direttamente oppure in modo mediato da GARR, anche quando non c'è presidio?
- Gli strumenti che adotteremo devono essere in grado di rispondere in modo chiaro a queste domande

Faremo una attività di indagine interna alla comunità GARR al fine di capire quale sia la necessità

- Passare da gruppo di lavoro sui DDOS a servizio di mitigazione

Scopo dell'attività è incrementare la disponibilità dei servizi di Rete

Ringrazio Arbor e Radware per il supporto e la pazienza dimostrata in questi mesi

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Grazie