Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

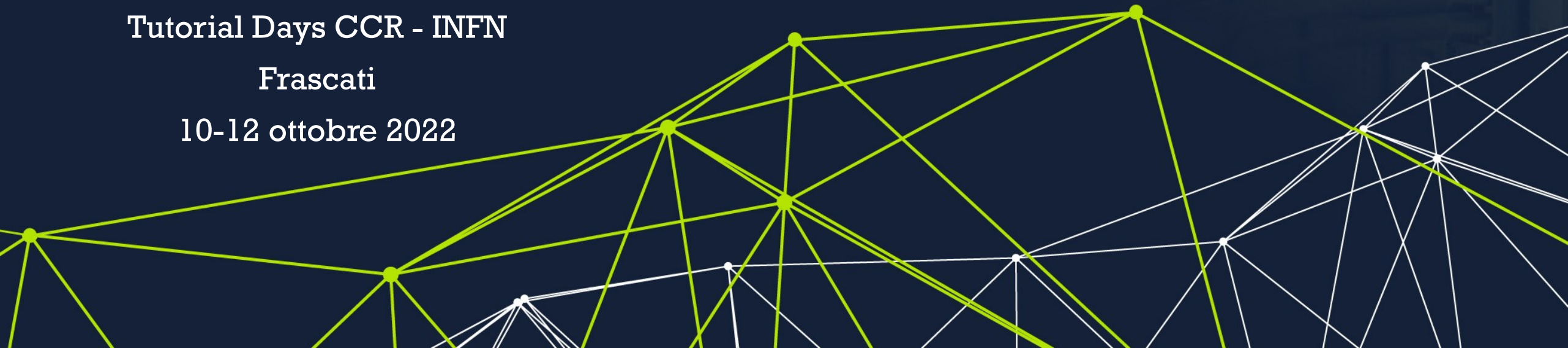
DDoS
per tutti i gusti

LEONARDO LANZI

Tutorial Days CCR - INFN

Frascati

10-12 ottobre 2022



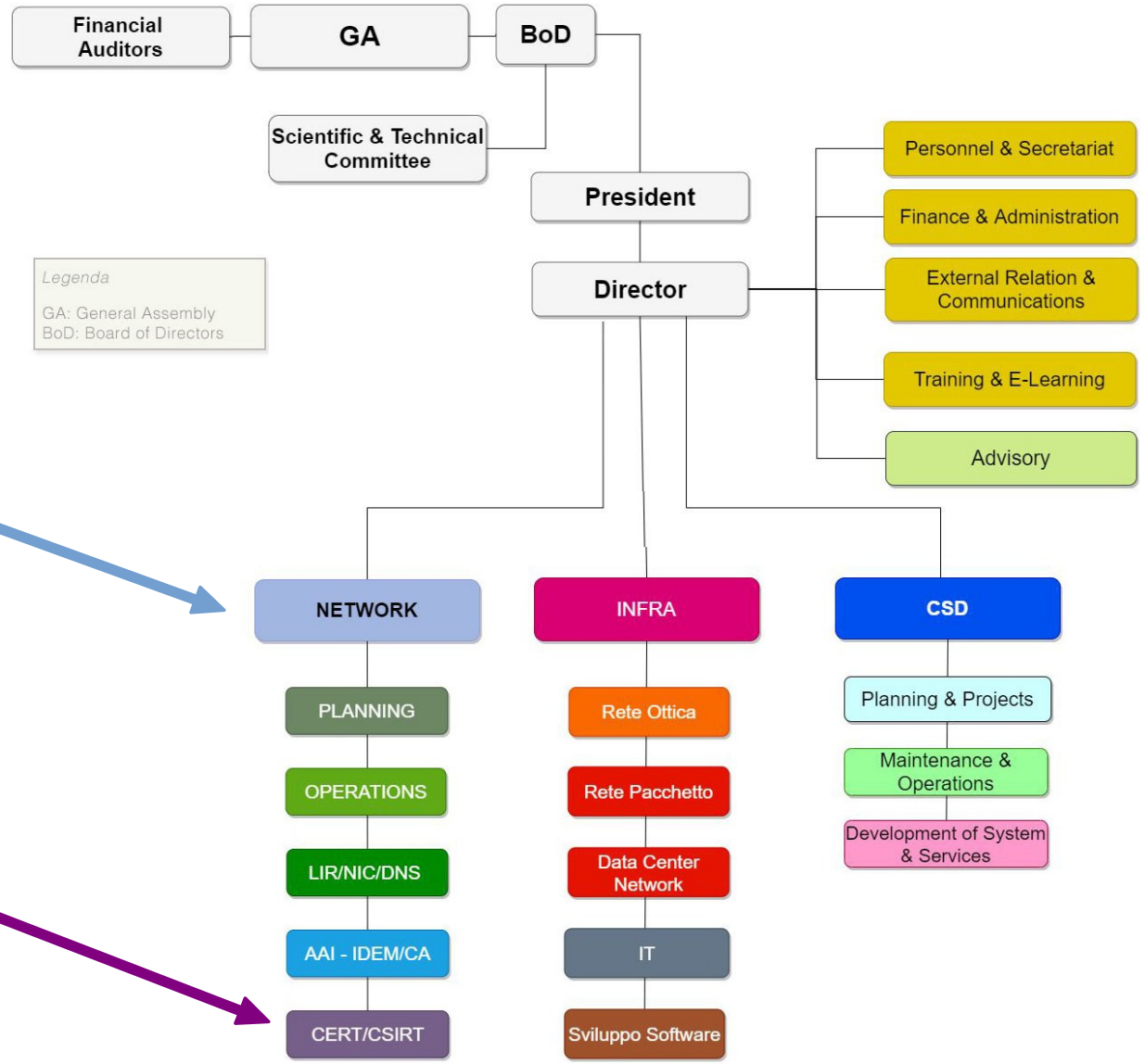
argomenti

- Introduzione / definizioni
- Casi reali / esempi con soluzione (quando c'è)
- Problemi di scala
- Progetti per il futuro
- Q&A

GARR-CERT

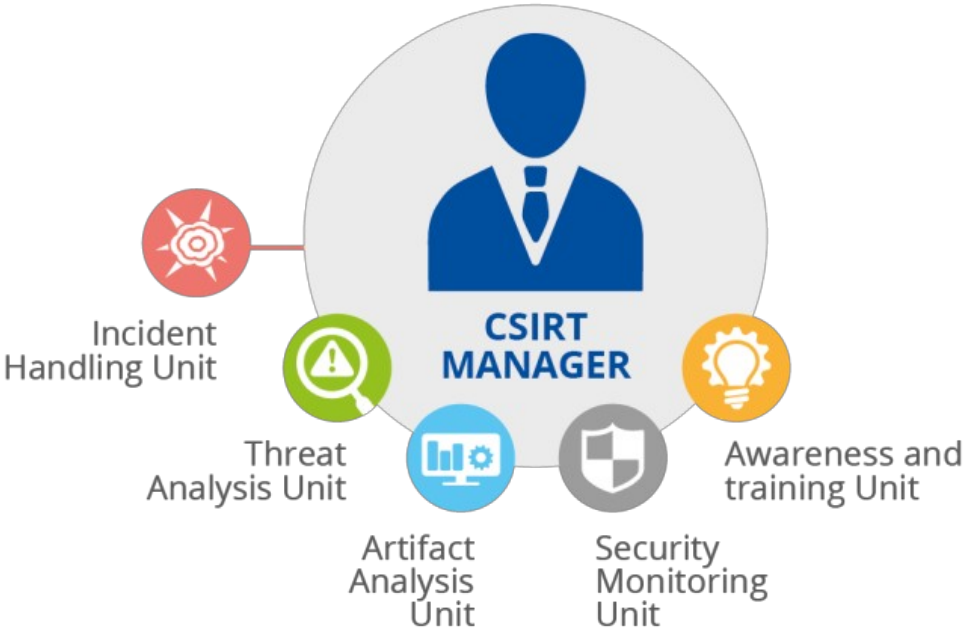
- Servizio operativo del Dipartimento Network della Rete GARR

user - oriented



GARR-CERT / *".. Sì, ma quanti siete?"*

Struttura di uno "small CSIRT"



Unità organizzative di un "bigger CSIRT"

[ENISA Report]

GARR-CERT

- Lunedì → Venerdì - 9:30 AM → 5:30 PM [compatibile con quello degli utenti]
- 4 unità di personale [in ordine di apparizione]


Andrea Pinzani


Maria Sole Scollo


Simona Venuti


Leonardo Lanzi

RFC 2350 - "*Expectations for Computer Security Incident Response*"

Mission Statement

- assistere gli utenti della Rete GARR nell'implementazione di misure proattive per ridurre il rischio di incidenti di sicurezza;

- assistere gli utenti della Rete GARR nella risposta agli incidenti di sicurezza quando questi accadono.

Procedura di gestione degli incidenti

- Al verificarsi di un **problema di sicurezza** che veda coinvolto un soggetto appartenente alla rete GARR, **GARR-CERT valuta** l'apertura di un incidente di sicurezza e ne **decide** la priorità, le procedure di risoluzione e le modalità di comunicazione con i soggetti coinvolti.
- Distinzione dei casi in cui il soggetto GARR è vittima o origine, e di attacco esterno distribuito contro più utenti GARR.
- Convolgimento di APM/referente per la sicurezza [e/o soggetto esterno]
- Richiesta di risoluzione entro un **tempo commisurato alla gravità del problema**

1) Eventuali solleciti in assenza di risposta

2) Avviso di filtraggio

3) Richiesta di filtraggio al NOC, notifica a APM e APA.

Procedura di gestione degli incidenti

Chiusura incidente

- **Buona**

  APM interviene e comunica a CERT la risoluzione del problema.

  Eventuali verifiche, notifica alle parti coinvolte.

  Nel caso sia stato applicato un filtro, GARR-CERT ne richiede la rimozione a NOC (non sono previste altre opzioni). -> [CLOSED]

- **Non buona**

  Nessun intervento/comunicazione da APM, ma problema termina.

  Dopo X tempo -> chiusura d'ufficio [detta anche "per noia"].

Procedura di gestione degli incidenti

Emergenza

- Nel caso si verifichi un incidente, anche fuori dall'orario di attività di NOC e CERT, che impatti significativamente sulla connettività degli utenti, come per esempio un SYNFlood distribuito, i responsabili di NOC e CERT decidono le modalità di:

  a) applicazione di eventuali filtri a livello di router GARR anche entro tempi inferiori a quelli previsti nella Procedura di Gestione Incidenti,

  b) comunicazione agli utenti coinvolti e, sentito il Direttore del Dipartimento Network [e/o il Direttore GARR], se e come diffondere l'evento e i dettagli ad altri soggetti o pubblicamente.

- Anche altri casi che espongano gli utenti a gravi problemi di sicurezza, ad esempio nel caso di data breach in corso che riguardano dati particolari, possono essere trattati a scopo cautelativo come al precedente punto (a).

Trend

- > 2200 ticket di incidenti / anno

  in diminuzione come numero assoluto dal 2019, ma..

  - attacchi DoS aumentano di numero, complessità, durata [anche come eventi ripetuti su stesso target], e difficoltà di risoluzione
  - aumento percentuale di incidenti non direttamente collegati alla "rete":
    - "data breaches": dal 5% nel 2019 al 25% nel 2021
    - host vulnerabili (XSS, injection etc): ~ 20%

DDoS

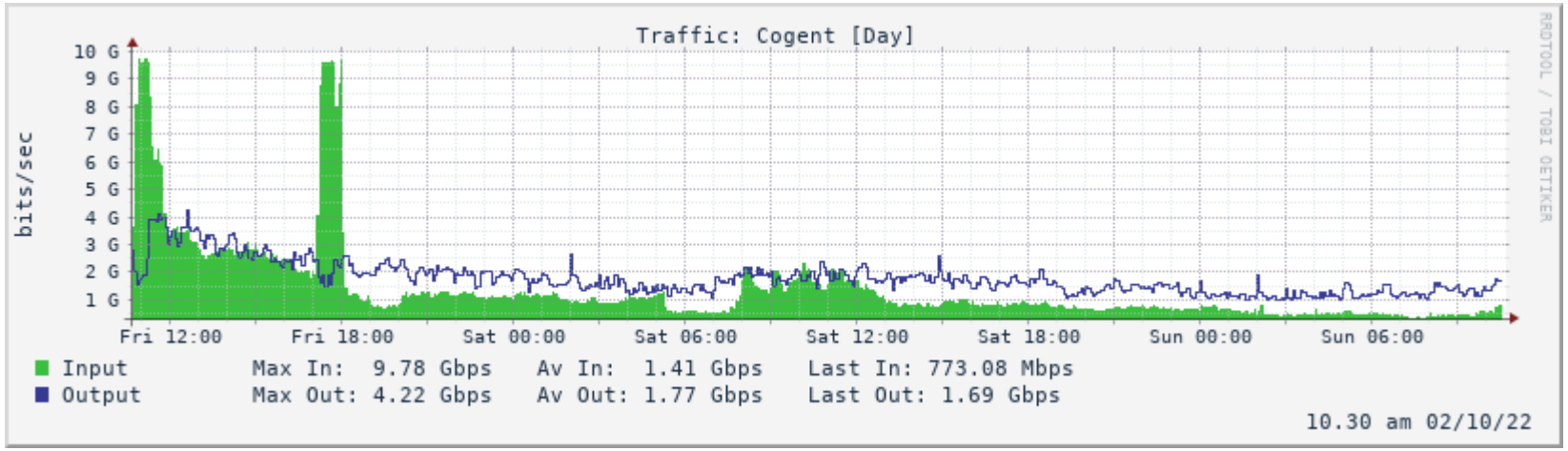
- Da evidenze sperimentali risulta che (almeno negli ultimi 4.5 anni) è stato definito DDoS il traffico di rete "cattivo":
  - proveniente da **più sorgenti**
  - quasi sempre destinato a un **singolo IP target**
  - Se supera una certa soglia: **visibile** sui monitor del NOC (GINS),

    più recentemente negli alert di Corero SmartWall

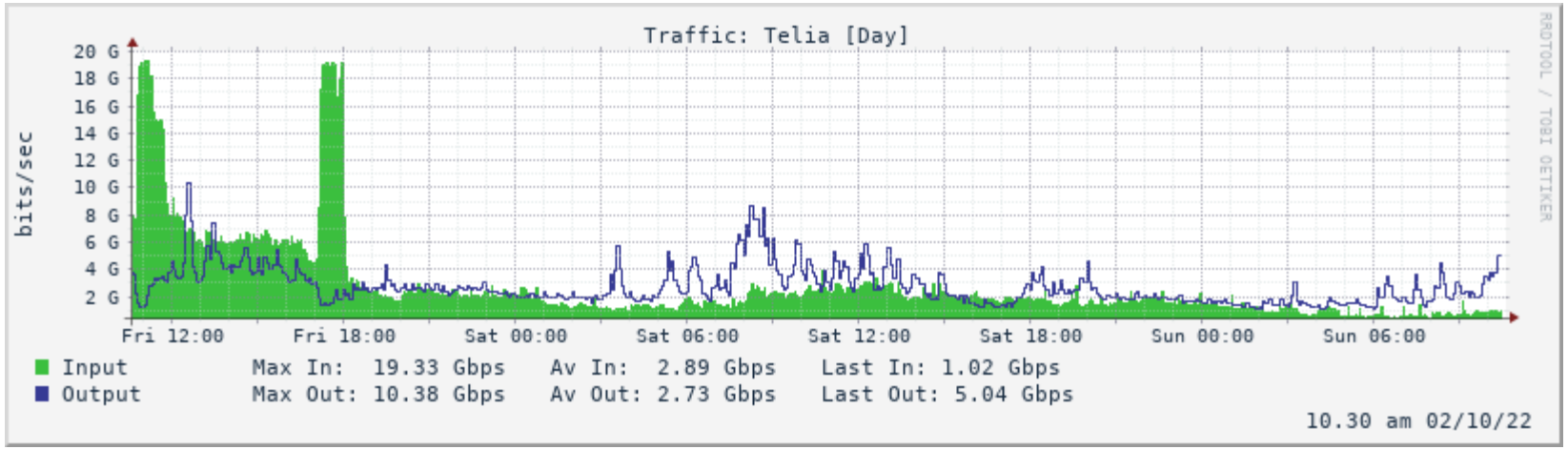
    → ***volumetrico***
  - **grave** se ha un **impatto sulla connettività** dell'utente (meno se su singoli servizi),
  - **molto grave**: anche quella dei vicini,
  - **molto molto grave**: saturazione dei peering.

DDoS – esempio recente [30/09/22]

Link 10 Gbps



Link 20 Gbps



Contromisure [fino a GARR-X]

- Automatiche
  - Corero SmartWall Threat Defense Director [Juniper], per gli amici sono *Corero*

- Manuali
  - filtri manuali su Corero
  - regole flowspec
  - black hole routing [equivalente a **`> /dev/null`**]
  - intervento manuale su routing/BGP

Corero SmartWall

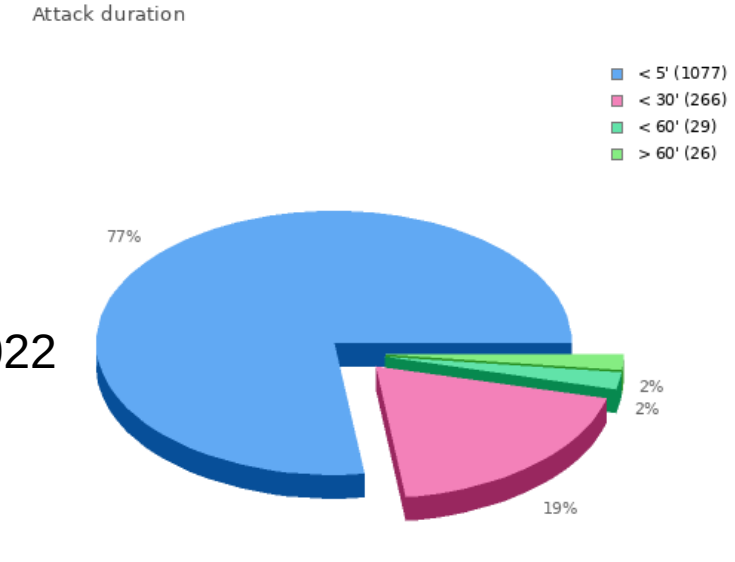
- ~ 50 controlli/sec su flussi campionati dei route reflector per eventuale superamento di una o più tra decine di soglie che controllano protocollo, porta, ttl, flag TCP, packet length.

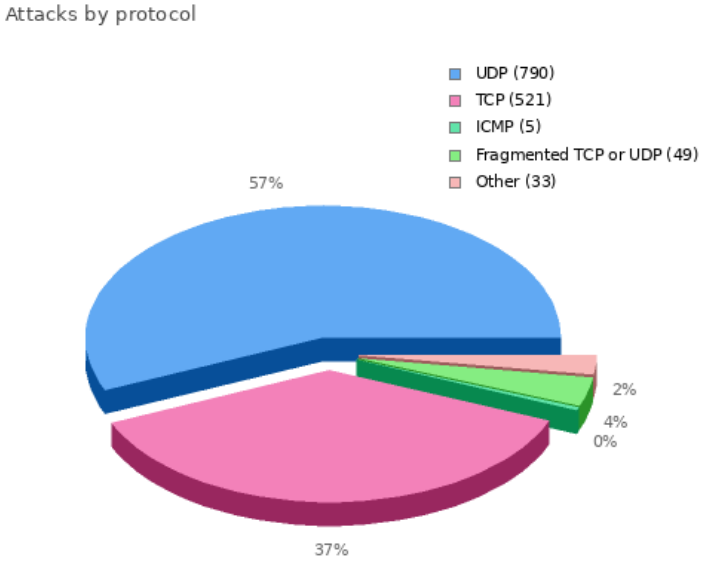
- In caso di anomalia, per singolo IP target vengono creati “filtri effimeri” (per questo funziona con apparati Juniper) corrispondenti all’anomalia rilevata.

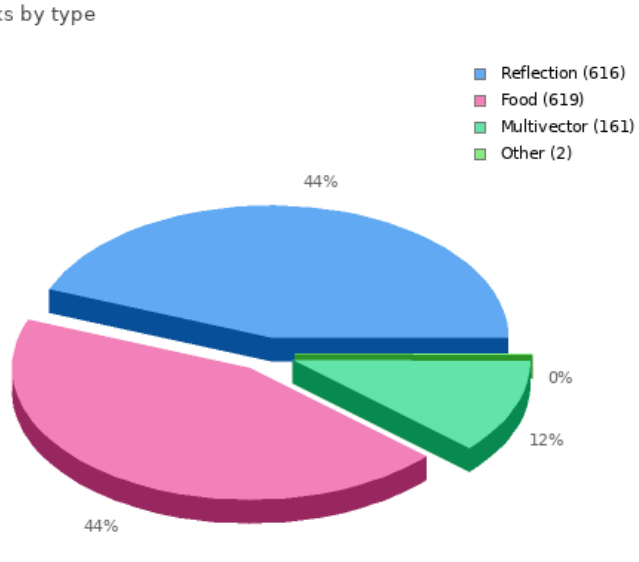
- Update ogni 5 minuti.

Corero SmartWall

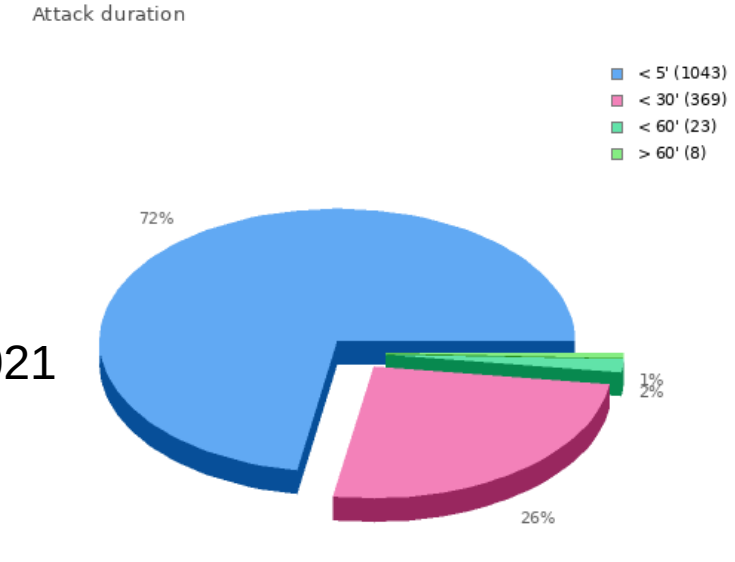
2022

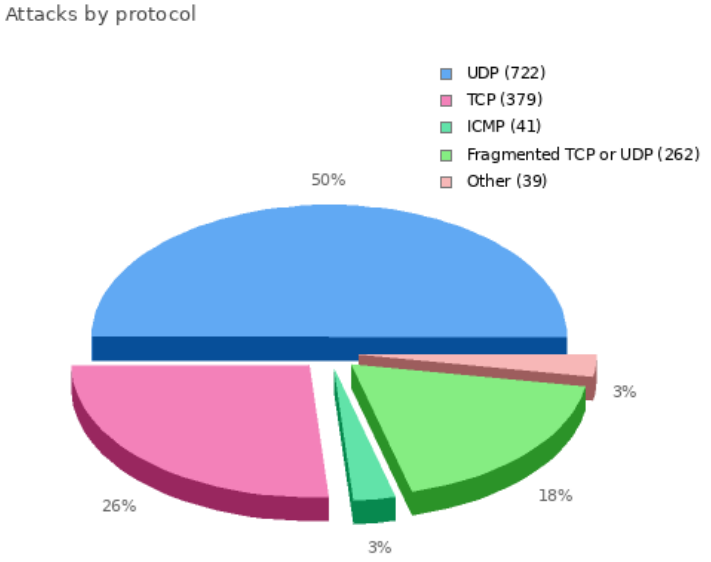


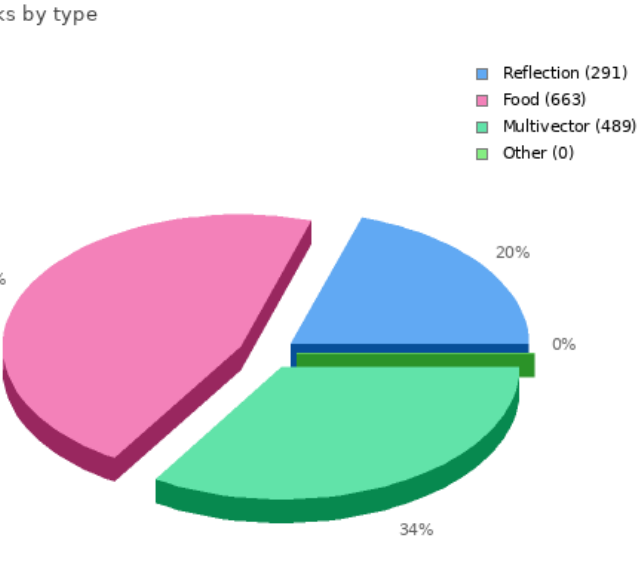




2021







Esempi DDoS

0) Eurobet
1) Lottomatica
2) *super-targeted DDoS* [con fasi preliminari di test]
3) *Colui che non deve essere nominato* [più volte]
4) Middlebox attacks, o *Il FW da 1'000'000 $* [più volte]
5) Killnet: *Molto rumore per nulla* [3 enti sotto attacco]
6) *Effetto Jenga* [un singolo IP, molto targeted, decine di vittime]
7) *Corero rocks, but...* [30/09/2022, più recente]

Eurobet – 16 ottobre 2019

10/16/19, 12:28 PM

Ciao,

c'è un attacco syn flood ddos in corso verso Eurobet, che sta creando diversi problemi a più utenti GARR (tra cui l'università del Mediterraneo RC).

In accordo con Leonardo, ho applicato un filtro flowspec su tutta la rete per il traffico con sorgente 185.90.116.0/22. Ticket NOC-CERT 728.

Ciao,

S

Reaction time ~ 15 minuti :)

[lieto] fine?

Lottomatica – 21 ottobre 2019

On 10/21/19 10:38 AM, [MM] wrote:

> ciao, c'è un nuovo attacco da 185.40.12.0/22, lottomatica

> sono di nuovo pacchetti spoofati, di nuovo syn flood

> INGV napoli ha il firewall a palla, probabilmente anche altri utenti

> valutiamo se filtrare, è comunque l'equivalente di far funzionare il DdoS[???????]

10/21/19, 11:00 AM

Buon lunedi' a tutti,

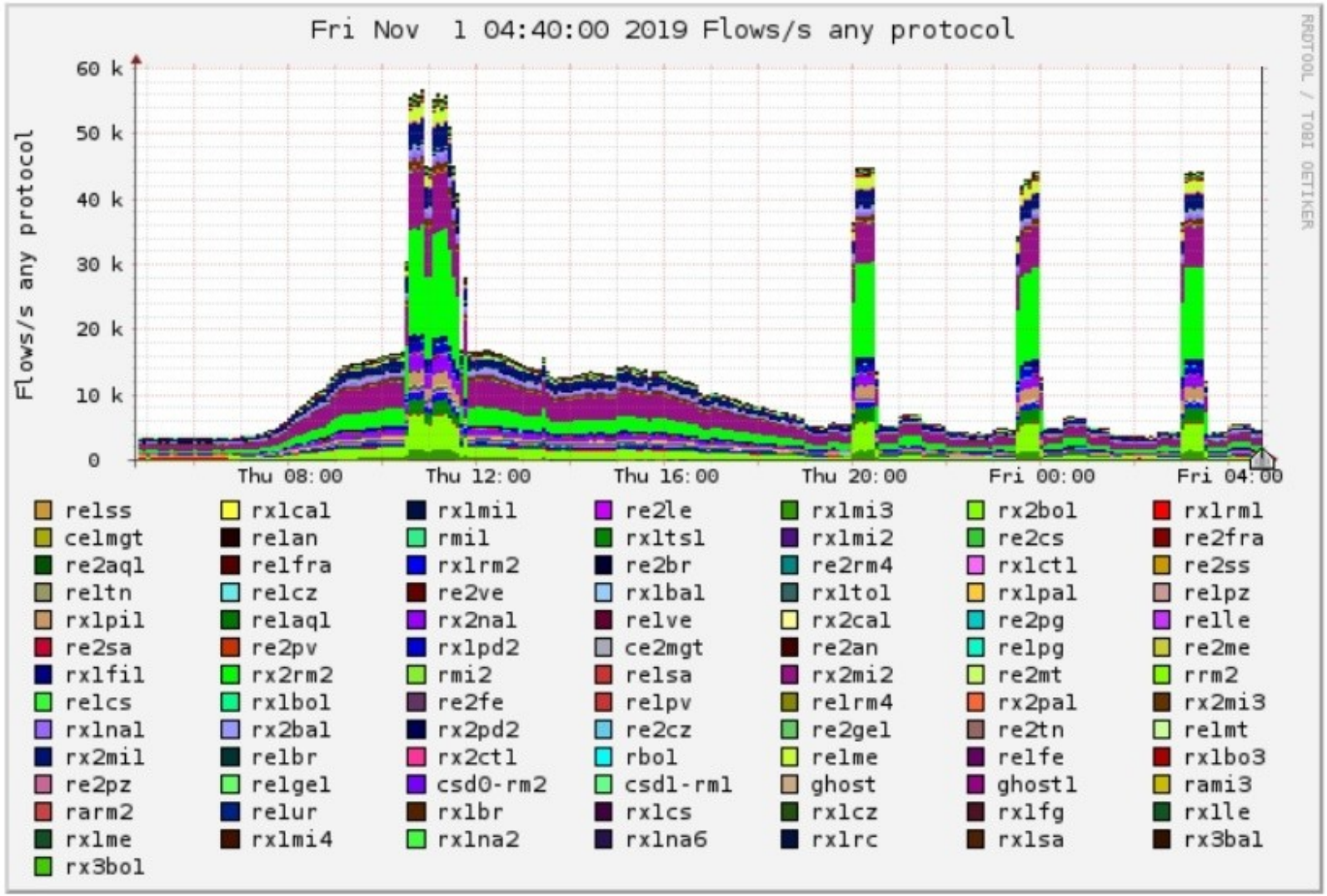
puo' valere la pena rifare un flowspec sulla rete indicata 185.40.12.0/22.

Vi allego l'elenco di IP trovati con nfdump sui peering dalle 9 alle 10:40, ordinati e uniqed con IP sorgenti nella rete 185.0.0.0/8, solo perche' non sembra sia solo 185.40.12.0/22 a fare casino.

Grazie, a presto

l

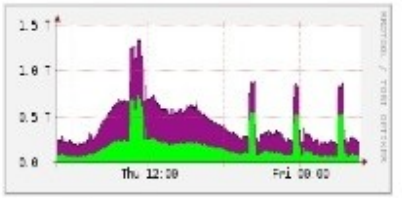
Lottomatica – netflow/nfsen – SYN spoofati



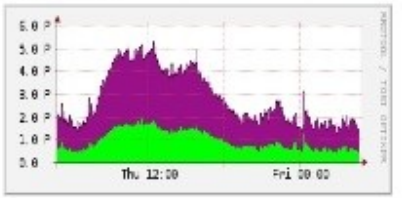
t_{start} 2019-11-01-04-40

t_{end} 2019-11-01-04-40

Packets



Traffic



Lin Scale Stacked Gr

Lottomatica – chiusura

2/11/2019 [AI]

filtraggio dei SYN da AS35574

[...]

vi mando un aggiornamento sulla situazione.

Da sabato pomeriggio dopo le 18:00, dopo gli ultimi due attacchi consistenti, [...], ho messo i filtri sulle interfacce dei due upstream (Telia e Cogent) che bloccano tutti i pacchetti SyS (non ACK) originati da indirizzi delle reti di Lottomatica. In pratica blocchiamo tutti i tentativi di instaurare connessioni TCP da ip Lottomatica che passano dagli upstream.

[…]

Nel frattempo Lottomatica ha applicato le modifiche al routing suggerite per cui adesso il traffico tra AS Lottomatica e AS GARR passa in entrambi i versi dai NAP dove abbiamo peering diretti.

Lottomatica / analisi

Ciao,

ho preso i dati da [].garr.it con nfdump per i 9 eventi visibili anche su gins.

1) 2019/10/31 10:20-11:50

2) 2019/10/31 20:00-20:30

3) 2019/10/31 23:30-00:00

4) 2019/11/01 03:00-03:30

5) 2019/11/01 06:00-06:30

6) 2019/11/01 08:30-08:40

7) 2019/11/01 09:10-09:25

8) 2019/11/02 16:25-16:40

9) 2019/11/02 18:50-19:10

Lottomatica / analisi

Gli IP GARR coinvolti - SYN-ACK verso Lottomatica - sono stati rispettivamente:

1) 54490 (20), 2) 27454 (46), 3) 27262 (41), 4) 28507 (50), 5) 30316 (19), 6) 26926 (30), 7) 26309 (30), 8) 27407 (75), 9) 25300 (280)

tra parentesi quelli che hanno risposto con meno di 30000 pacchetti;

praticamente tutti hanno partecipato.

[...]

Divisi in gruppi di /16, solo per avere un'idea di quanto sono distribuiti:

1) 73, 2) 67, 3) 70, 4) 68, 5) 70, 6) 67, 7) 67, 8) 69, 9) 67

Lottomatica / analisi

11/4/19, 6:26 PM

Qualche osservazione [...]

- Tranne UniPD, i top talker non sono stati bloccati per effetto dei troppi SYN spoofati, quindi hanno fatto "il massimo danno" a Lottomatica, mentre le sedi che non hanno retto i SYN, per il resto del mondo sono state le meno cattive [...]

- Il prodotto del (numero di servizi aperti che hanno risposto ai SYN) x (banda disponibile) penso ci collochi in alto nel rating di chi ci vuole sfruttare per veicolare attacchi di questo tipo.

- L'inaspettato cedimento di firewall anche nominalmente performanti puo' essere dovuto al fatto che gli algoritmi usati dai fw per decidere cosa fare sono nel caso medio buoni, anche O(log N), ma possono arrivare come worst-case a O(N^4) [tipo SYN molto probabilmente malformati], e nelle specifiche del venditore non credo sia pubblicizzata quest'ultima evenienza.

- Dopo questi attacchi, e durera' abbastanza, vari utenti staranno fissi a guardare i SYN in ingresso; temo diversi casi di falsi positivi (gia' sentiti).

- Visto come hanno spalmato gli attacchi, concordo con quanto ha gia' scritto Silvia sulla difficolta' nel valutare possibili soglie, quelli di questa volta avevano come fattore comune praticamente solo l'AS da attaccare.

Dopo Lottomatica (*lesson learned*)

- Monitor su SYN distribuiti (dai dati netflow dei RR)
- Modifiche alla procedura di gestione degli incidenti, tra queste..
- Introdotta possibilità di filtraggi estesi in ingresso, di solito a colpi di /24, per IP esterni ad AS137.

02 – "super-targeted" DDoS

8/1/2021 – da ticket CERT:

[...]

Dall'analisi dei flussi di rete sembra che il nodo x.y.55.220 (app.v.w.z) sia stato vittima di due attacchi DDoS di tipo UDP flood:

start	end	bytes	bps	flows	connections
08/01/21 11:30	08/01/21 11:40	54,38 GB	278,42 Mbps	126345	126345
08/01/21 10:10	08/01/21 11:15	193,53 GB	369,71 Mbps	571650	570619

02 – "super-targeted" DDoS

Risposta [Responsabile sicurezza]

"vi mando un breve resoconto".. [le virgolette sono mie]

Preludio dell'attacco:

start => 21:50 circa

stop => 22:05 circa

[dettagli su servizi impattati / effetti collaterali / dati misurati]

Prima parte dell'attacco:

start => 10:00 circa

stop => 10:30 circa

[dettagli su servizi impattati / effetti collaterali / dati misurati]

Ecc ecc. ecc. ecc.

Quarta parte dell'attacco..

Ho saputo che entrato in funzione il vostro sistema anti-DDOS: funziona anche come anti-SynFlood?

Potete mica dirmi da quando a quando è intervenuto?

02 – I log - monitor "storico" [via netflow]

Analisi attacco DoS contro dell'8 gennaio 2021

DDOS attack monitor (https://gins.garr.it/Monitor/ddos.php)

target	start	end	int	bytes	bps	flows	connections
.55.240	21:25 08/01/21	21:25 08/01/21	1	5,4 GB	140 Mbps	90195	89707
.95.68	14:20 08/01/21	14:20 08/01/21	1	5,8 GB	157 Mbps	97463	97454
.181.193	14:20 08/01/21	14:20 08/01/21	1	5,1 GB	124 Mbps	86406	86237
.55.220	11:30 08/01/21	11:40 08/01/21	3	54,4 GB	278 Mbps	126345	126345
.55.220	10:10 08/01/21	11:15 08/01/21	13	193,5 GB	370 Mbps	571650	570619

02 – I log - report della vittima

target IP	start	duration (m)	description	flussi	details	impatto
.181.232	14:15 08/01/21	15				Rallentamento delle prestazioni
.181.193	14:15 08/01/21	15				Rallentamento delle prestazioni
.55.240	14:15 08/01/21	15				Rallentamento delle prestazioni
.55.220	11:35 08/01/21	5	DDoS verso porte variabili	500K flussi con fw (senza attacco 20K)	source distribuita	Blocco connettività, riavvio di un nodo del cluster fw
.55.220	10:30 08/01/21	20	DDoS verso porte variabili	500K flussi con fw (senza attacco 20K)	source distribuita	Blocco della connettività
.55.220	10:00 08/01/21	30	SYN Flood to https (443/tcp)	250K flussi con fw (senza attacco 20K)	source ≈ Cina (30% del traffico da 4 IP: 221.122.91.71, 221.122.91.74, 221.122.91.75, 58.220.95.80)	Nessun problema sulla connettività di frontiera
.95.68	10:00 08/01/21	30	DDoS (circa 200 connessioni per IP)	200K flussi con fw (senza attacco 2K)		Nessun problema sulla connettività di frontiera
.95.68	21:50 07/01/21	15				Interruzione dei servizi di autenticazione

02 – I log - Corero

DDOS CORERO Syslog (https://gins.garr.it/Monitor/ddosCorero.php)

target IP	start	duration (m)	max bps	max pps	volume bytes	description	details
.55.240	21:27 08/01/21	6	2,30 Gbps	4,9 Mpps	63 GB	SYN Flood to https (443/tcp)	Ongoing attack Max Values: 5832 pps / 2 Mbps
.55.220	21:17 08/01/21	6	2,80 Gbps	6 Mpps	78 GB	SYN Flood to https (443/tcp)	Ongoing attack Max Values: 1 pps / 0 Mbps
.55.220	21:11 08/01/21	2	15 Mbps	43 Kpps	157 MB	SYN/ACK Reflection from ftp (21/tcp) to https (443/tcp)	Ongoing attack Max Values: 19443 pps / 6 Mbps
.55.220	18:08 08/01/21	2	297 Mbps	632 Kpps	3,6 GB	SYN Spoofed Flood to https (443/tcp)	Ongoing attack Max Values: 393596 pps / 185 Mbps
.95.68	14:23 08/01/21	1	418 Mbps	884 Kpps	3,2 GB	SYN Spoofed Flood to https (443/tcp)	New attack Max Values: 883918 pps / 418 Mbps
.181.193	14:20 08/01/21	1	1,70 Gbps	3,7 Mpps	13 GB	SYN Spoofed Flood to https (443/tcp)	New attack Max Values: 3695541 pps / 1740 Mbps
.55.220	11:29 08/01/21	14	15 Mbps	45 Kpps	112 MB	ICMP Flood	Ongoing attack Max Values: 0 pps / 0 Mbps
.55.220	10:27 08/01/21	52	15 Mbps	40 Kpps	120 MB	ICMP Flood	Ongoing attack Max Values: 0 pps / 0 Mbps
.55.220	10:18 08/01/21	3	2,25 Gbps	4,7 Mpps	34 GB	SYN Flood to https (443/tcp)	Ongoing attack Max Values: 1165570 pps / 559 Mbps
.55.220	10:10 08/01/21	1	2 Gbps	4,3 Mpps	15 GB	SYN Spoofed Flood to https (443/tcp)	New attack Max Values: 4261059 pps / 2009 Mbps
.95.68	22:54 07/01/21	3	39 Mbps	105 Kpps	561 MB	SYN Flood to https (443/tcp)	Ongoing attack Max Values: 17087 pps / 5 Mbps

02 – "super-targeted" DDoS

- Attacchi a ripetizione fino al 19/01, contro vari IP dell'ente, con decine di vettori diversi.
- Ampia diffusione ai media molto rapida, con riferimenti tecnici non banali: link a pagine specifiche di GINS del traffico sui link dell'ente.
- Contatti tra responsabile sicurezza e settore dell'autorità di PS: minacce per evento pubblico importante previsto qualche giorno dopo.
- Contattato Corero per eventuali filtri ad-hoc in base all'analisi effettuata [niente da fare].
- NOC e CERT si preparano a una mattinata probabilmente pesante:

  varie possibilità di escalation, da filtri manuali su Corero, flowspec su router GARR, blackholing, fino a blocco di traffico verso subnet specifiche (dell'ente) sulle interfacce dei peering commerciali internazionali, da dove proveniva la maggior parte del traffico di attacco.
- .. e nulla. Poi l'attacco finale non c'è stato.

03 - DDoS contro *colui che non deve essere nominato*

Evidenze: vari mesi di DDoS, a fasi alterne, sia volumetrici che applicativi.

Dati dai log **aggregati** di Corero

- **2021**
  - 266 eventi, 46 tipologie distinte
- Fino a **metà marzo 2022**
  - 282 eventi, 64 tipologie distinte

    poi “soluzione esterna”.

    Silenzio fino al 27 luglio, quando arriva DDoS n. 6.

03 - DDoS contro ..

Mitigazione & *lesson learned*

- Corero [sempre acceso]
- Saturazione di vari link, più volte
- filtraggio lato GARR di UDP verso alcune /24
- reverse / social engineering durante le call: perché certi servizi sono pensati/configurati in un certo modo?

- "Poi ne riparliamo"… ancora niente.

04 – Il FW da l'000'000 $

01/05/22, 12:09

Salve,

sono un operatore del GARR-CERT [...]

Negli ultimi giorni abbiamo rilevato alcuni eventi classificabili come traffico syn flood destinato a molti indirizzi della vostra rete.

La porta target di tale traffico e' la 179/tcp (BGP).

Analizzando questi eventi risulta del traffico di risposta apparentemente da parte di tutti gli indirizzi contattati, con un volume dati elevato.

04 – Il FW da l'000'000 $

[...]
Provando a collegarsi con un browser ad uno qualsiasi dei nodi coinvolti, appare il seguente messaggio:

SONICWALL
Network Security Appliance
This site has been blocked by the network administrator.
Security Rule: ...
Client IP : ...

04 – Il FW da l'000'000 $

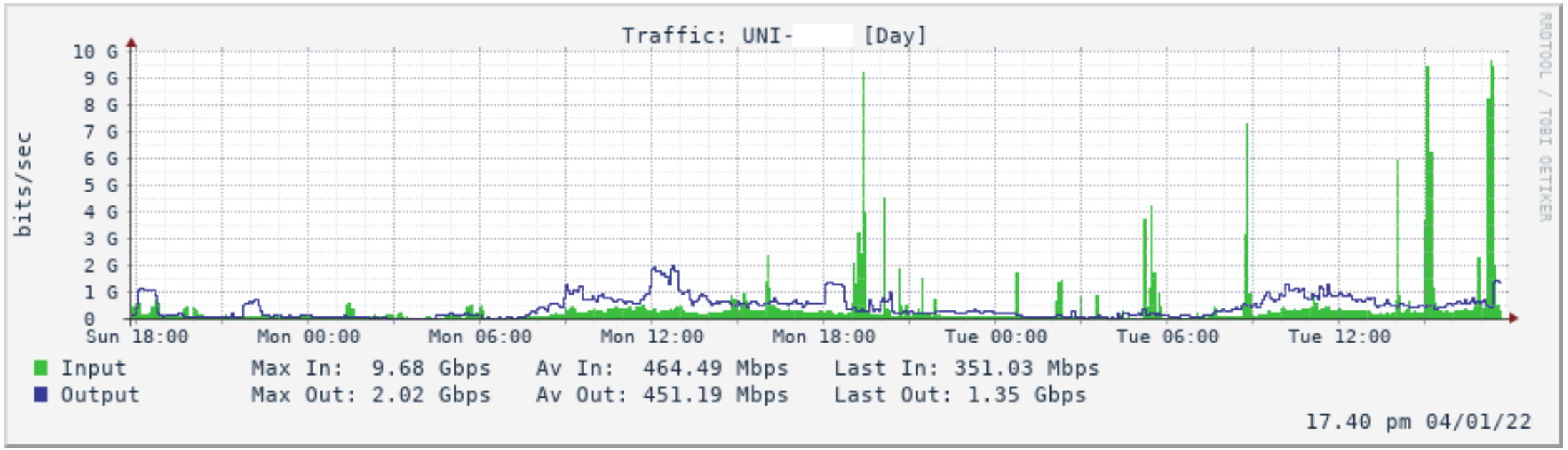
[...]

Riteniamo si tratti di una specie di attacco DoS reflection, dove il traffico syn flood ha mittente falsificato e funziona da innesco ad un traffico di risposta amplificato, probabilmente prodotto dal firewall.

In allegato un log e dei grafici.

Anche in questo momento si rileva un traffico rilevante in uscita dalla vostra rete relativo alla porta 179/tcp.

04 – Il FW da 1’000’000 $



04 – Il FW da 1’000’000 $

riassumendo:

- **5 gennaio** 2022, apertura incidente.
- Nessuna risposta da APM.
- **10 gennaio**, saturazione verso upstream provider, NOC filtra 179 TCP (BGP) [anche perche’, a che serve?]. Poi filtro rimosso.
- **7 febbraio**, stesso DDoS BGP, “ci siamo ovviamente accorti del flusso BGP, che altrettanto ovviamente non entra nella nostra rete”.
- **10 febbraio**, stesso DDoS con link utente saturo.
- **16 febbraio**, “[NOC] un filtro su Corero per **bloccare** tutte le connessioni dall'esterno che hanno come destinazione **la /16 porta 179 TCP** di xxx.”

04 – variante, quando c'è content inspection

Web filtering and censorship middleboxes

Domanda: che succede quando un firewall può ispezionare contenuto non cifrato, ed è configurato per ridirigere i naviganti a una paginona che spiega perché la consultazione di certi siti non è consona al luogo di lavoro, e quindi ecc. ecc. ecc.?

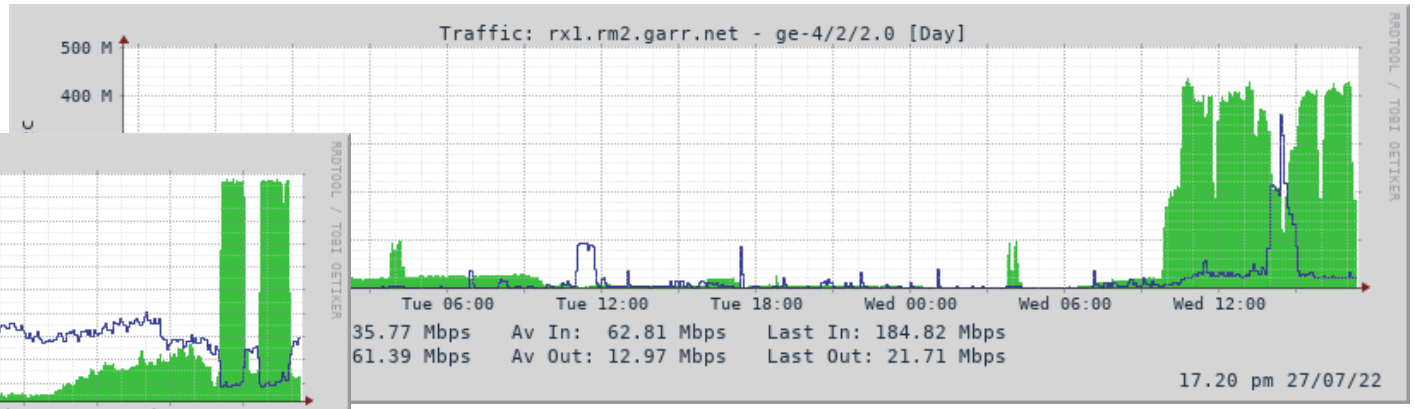
In pratica, escono fino a qualche centinaio di KB in risposta a una GET appositamente modificata, che contiene semplicemente una stringa con un dominio "non idoneo".

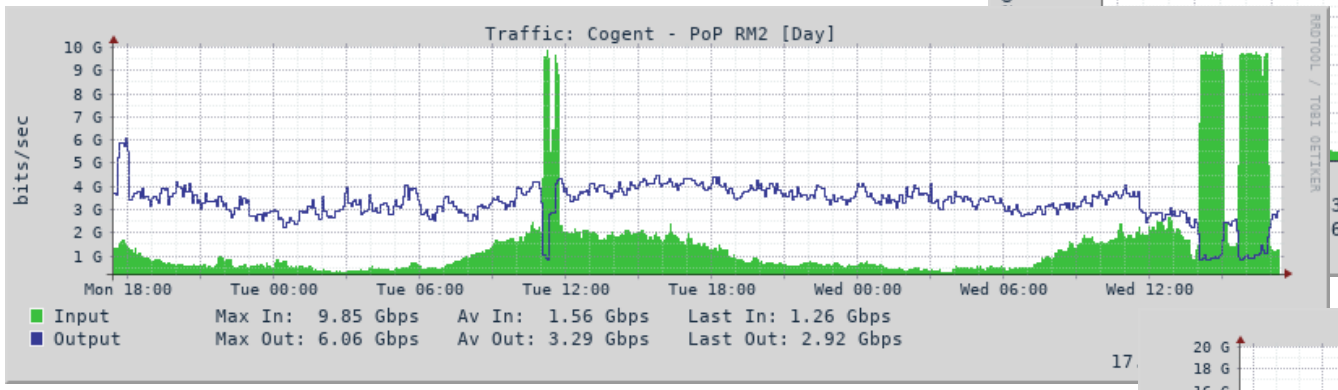
05 - Killnet

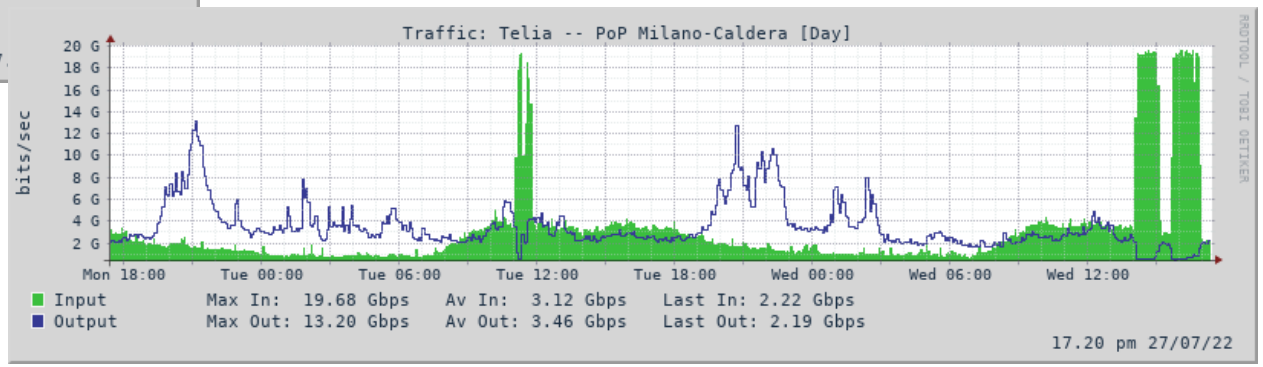
11 maggio 2022

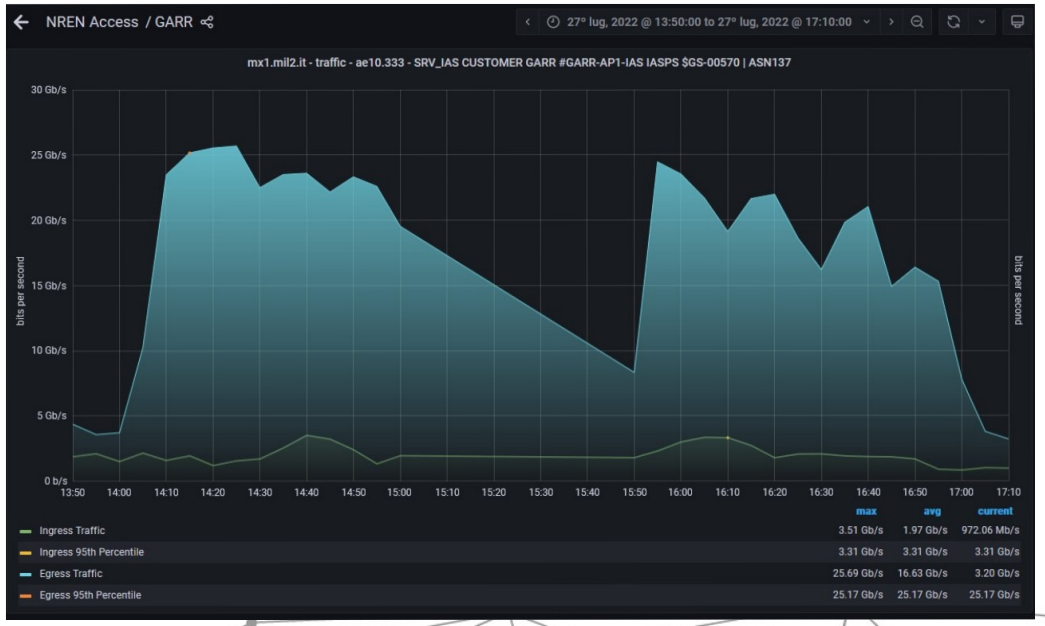
- 3 enti su rete GARR presenti tra i target indicati in un canale Telegram associato al gruppo Killnet [pro Russia, dopo inizio guerra in Ucraina].
- Attacchi http Get/Head/Post/Slow Flood e successivi upgrade, con sorgenti distribuite, eseguiti da volontari/simpatizzanti/idioti*, tramite uno dei tanti tool scaricabili da github.
- Notizie di altri siti istituzionali colpiti esterni ad AS137, con anche qualche richiesta di aiuto.
- Nessuno dei server target aveva configurazioni del server web per rate-limit o simili, né uso attivo dei log per update di ipset, .. , nemmeno un povero fail2ban.

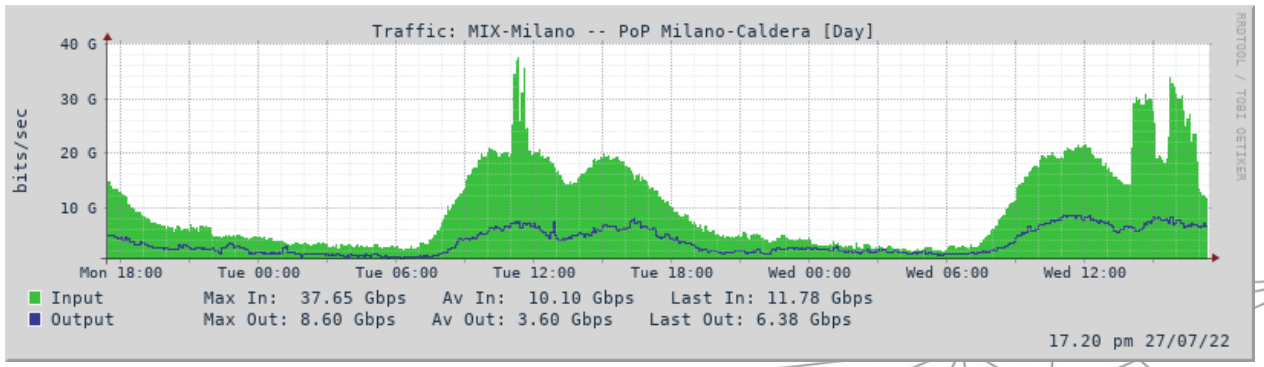
06 – 1 singolo IP molto targeted, upstream internazionali down





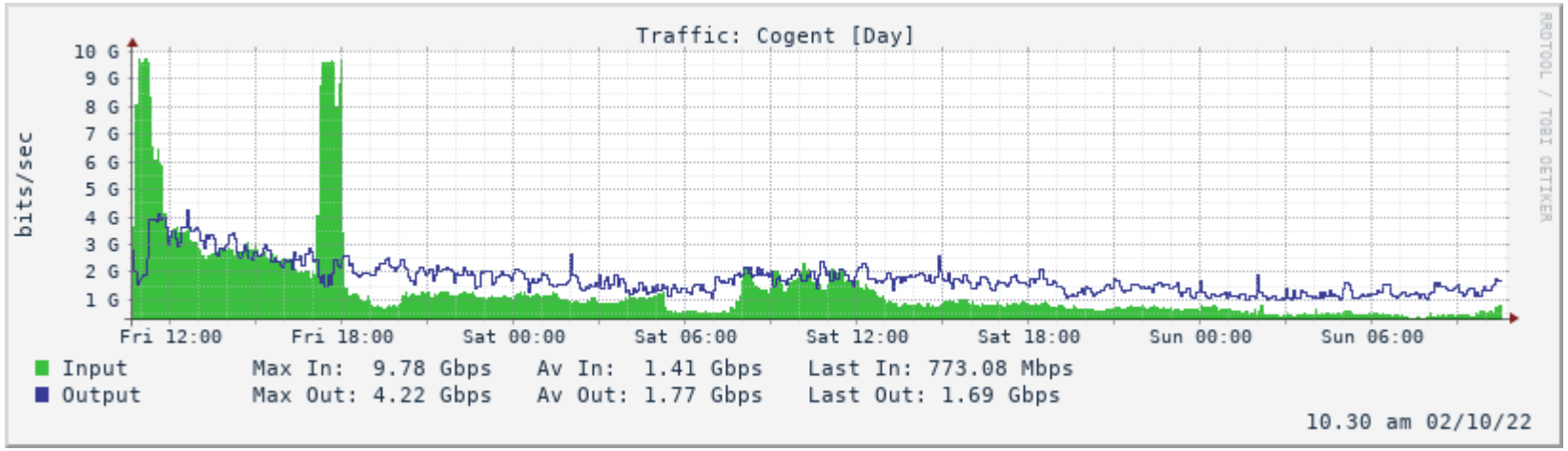




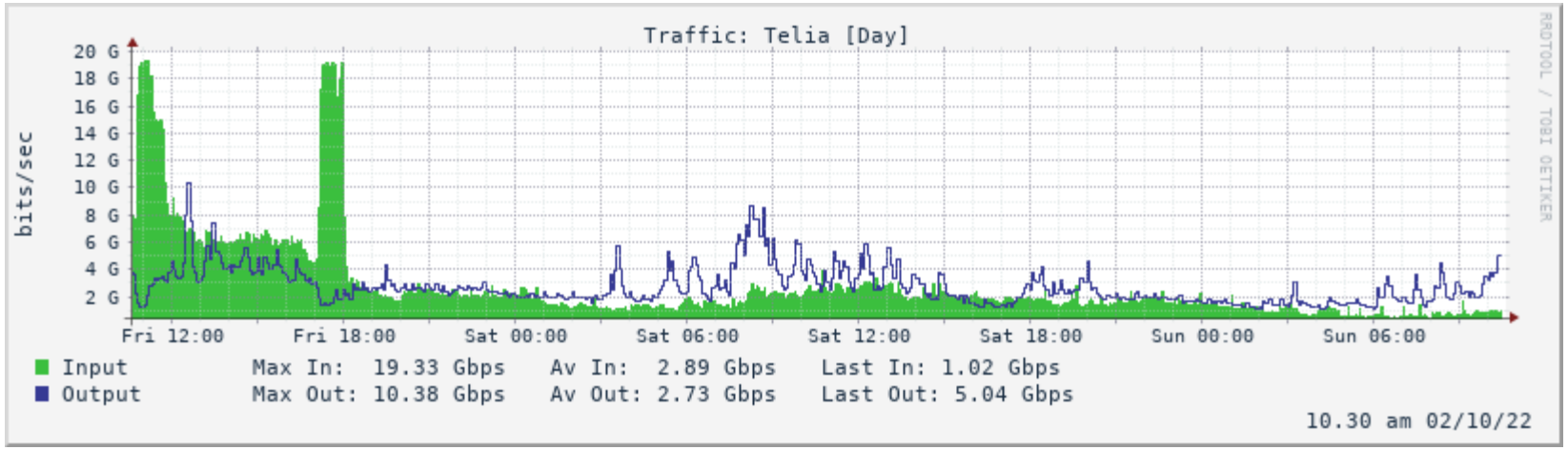


07 – 1 singolo target protetto molto bene da Corero, i *soliti noti* saturi

Link 10 Gbps



Link 20 Gbps



Non solo DDoS - Problemi di scala

Abbiamo [aggiornati a oggi 11/10/2022] 2305 record di email di APM, divisi per:

- 1655 record di associazione rete (v4 e v6),
- 650 record di associazione IP di una connessione punto-punto,
- e non mettiamo nel conto 3767 IP punto-punto gestiti da GARR.

Un DoS "banale" contro un singolo IP può generare, sempre più spesso, disservizi estesi indiretti.

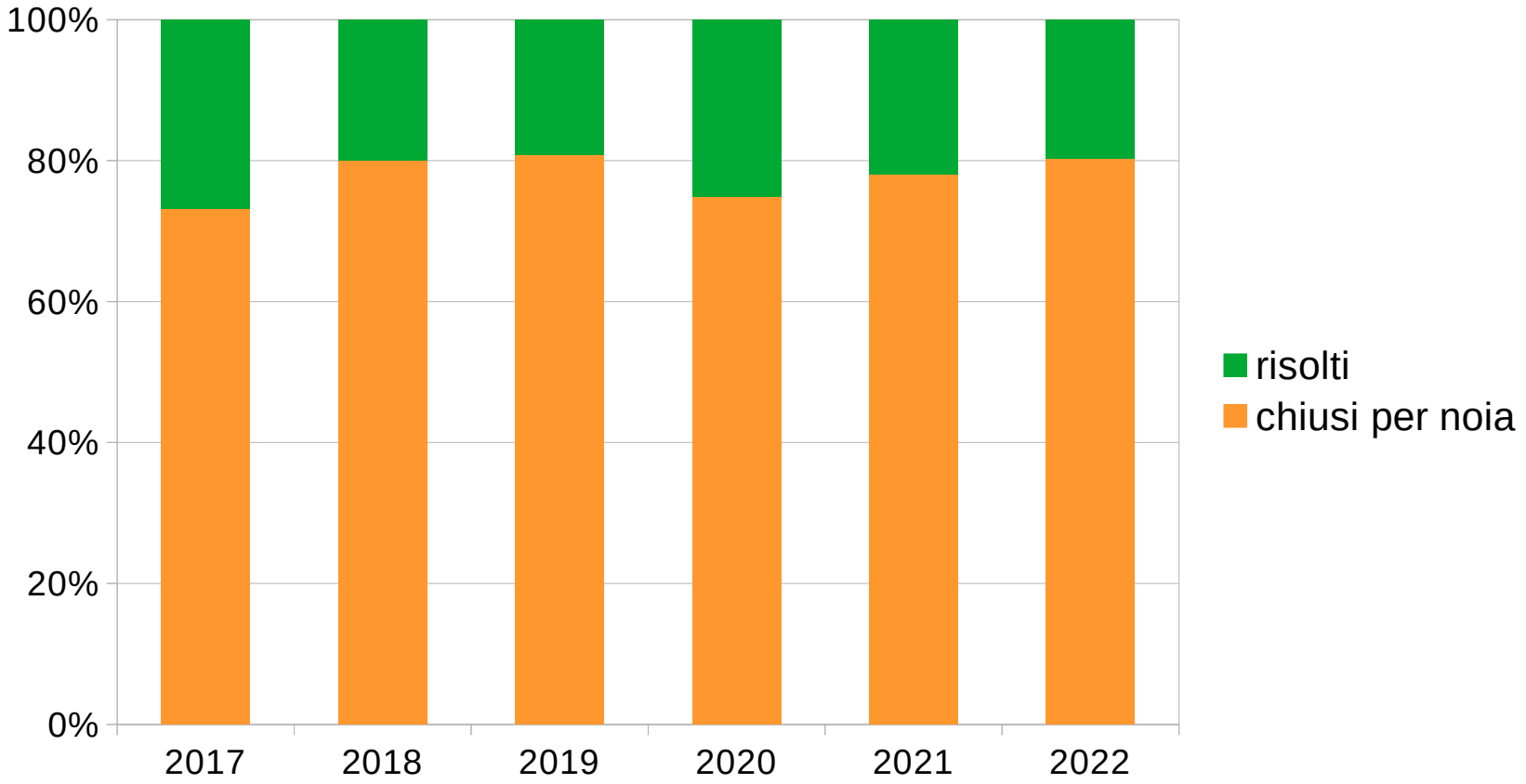
Che succede se invece di un IP ne attaccano qualche decina, distribuiti sulla tutta la rete GARR?

Non possiamo permetterci:

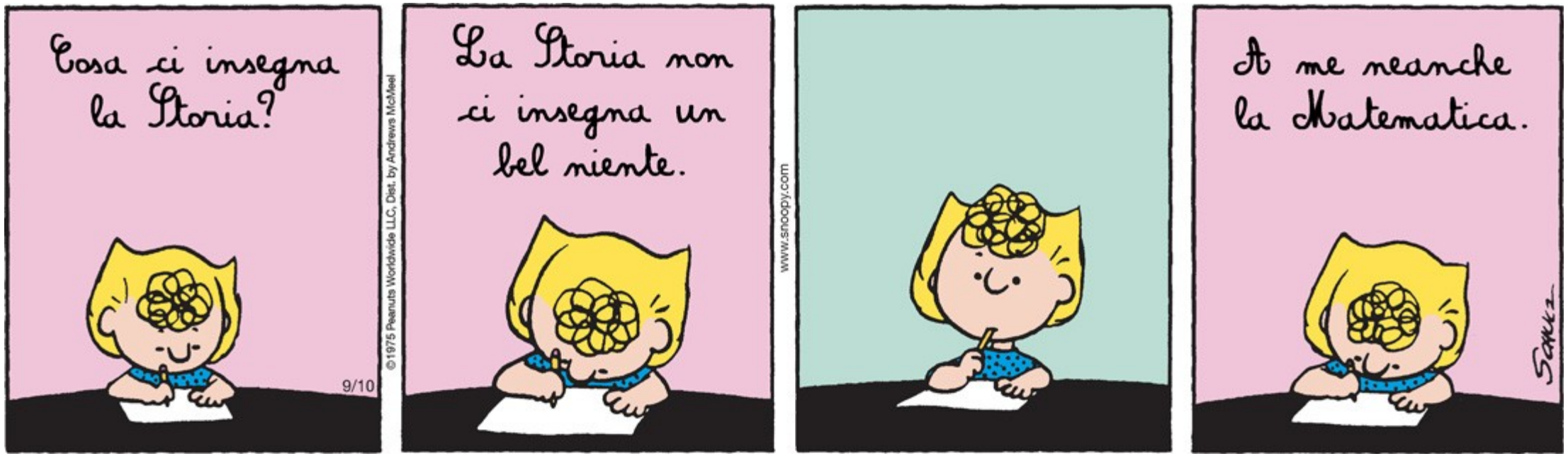
- di perdere informazioni per strada
- troppa improvvisazione quando non serve

Un dato triste

- Andamento % della chiusura dei ticket di GARR-CERT



Questa concedetemela



Progetti “politici”

1) Linee guida sulla conduzione di procedure dedicate alla riduzione del rischio di incidenti di sicurezza ~ come fare [cosa chiedere a] un vulnerability assessment, un penetration test, …
2) Individuazione di una nuova figura [ruolo | servizio] appositamente preposta all'interazione con GARR per tutte le tematiche che, nell'ente, impattano la sicurezza [se volete, *Cybersecurity*].
3) Formazione di una rete di persone del punto (2), un ”CERT federato”, con tutti i vantaggi di un sistema distribuito connesso e fidato, dedicato alla soluzione degli stessi problemi.

Progetto “tecno-politico”

- Il Remotely Triggered Black Hole (RTBH, RFC 5635) consente di fermare al bordo dell’AS, tramite BGP, con un update del next-hop verso un black hole, il traffico dannoso diretto verso un IP o una rete.
- In pratica, ogni AS può ricevere un trigger dall’AS dell’IP sotto attacco, e contribuire ad allontanare dall’AS vittima il traffico dannoso. Effettuando una difesa reciproca, si potrebbe evitare anche la saturazione degli uplink.

Riepilogo - 1/2

- Corero funziona molto bene, su quello per cui è programmato.
- Ogni porta aperta è come minimo sfruttabile per una qualche forma di reflection.
- Ogni IP del path Internet → … → servizio aperto (compreso), va difeso come se gli altri fossero fuori controllo.
- A che serve loggare 50’000 IP che stanno attaccando contemporaneamente, o rispondere loro con una pagina html (+css/immagini) per dire “brutto cattivo così non si fa” ?
- Più il firewall è grosso, più fa rumore quando cade.

Riepilogo - 2/2

- Con INFN in 3 anni circa 180 ticket:
  - ~ 10 per problemi di rete in corso (scansioni/brute-force da nodi compromessi).
  - Segnalazioni esterne di breach di credenziali (spesso mail istituzionale usata per registrazione su siti esterni), e spesso già risolte.

    Nei casi non risolti, associate a spam e affini.
  - Vulnerabilità di servizi.
- Non c'era tempo per parlare di altre cose (OSINT ecc.) ma, come esercizio per cominciare, ci può stare il DNS

  (es. shodan.io/domain/infn.it)

Riferimenti

- https://www.cert.garr.it
- https://www.rfc-editor.org/info/rfc2350
- "Attacks are a technical problem, defense is a political problem" - *Why we are not building a defendable Internet* - Thomas Dullien, BH ASIA 2017
- https://www.nginx.com/blog/mitigating-ddos-attacks-with-nginx-and-nginx-plus/
- https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/
- https://github.com/team-cymru/network-security-templates/tree/master/UTRS-Peering-Guide

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Domande?

LEONARDO LANZI

Tutorial Days CCR - INFN

Frascati

10-12 ottobre 2022