Nuovi DDoS, nuove contromisure

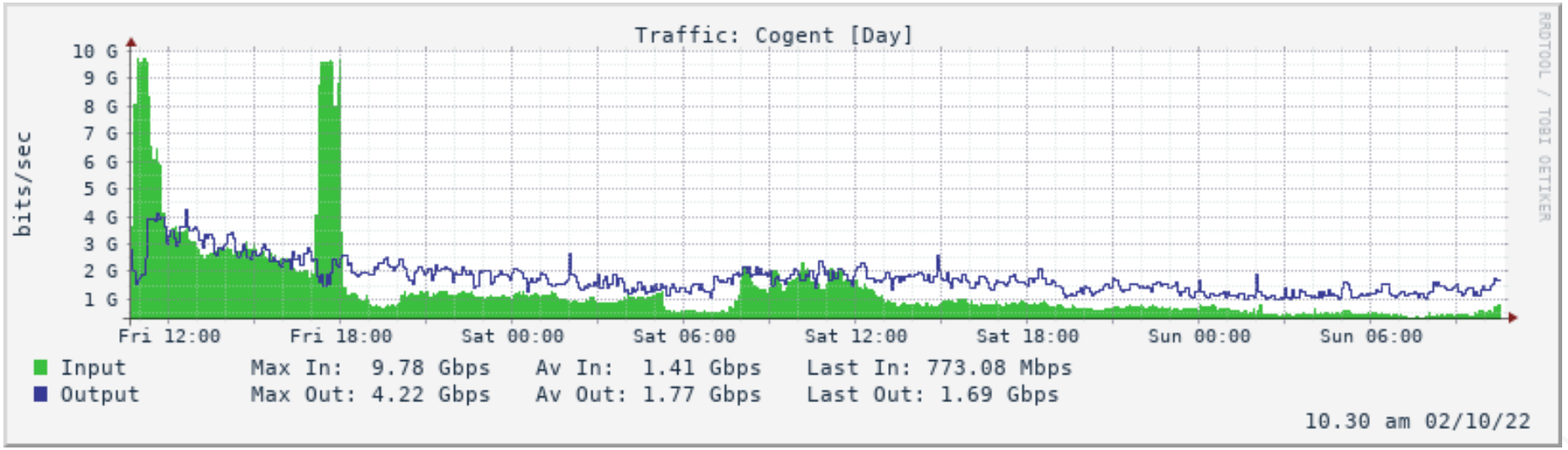
Leonardo Lanzi

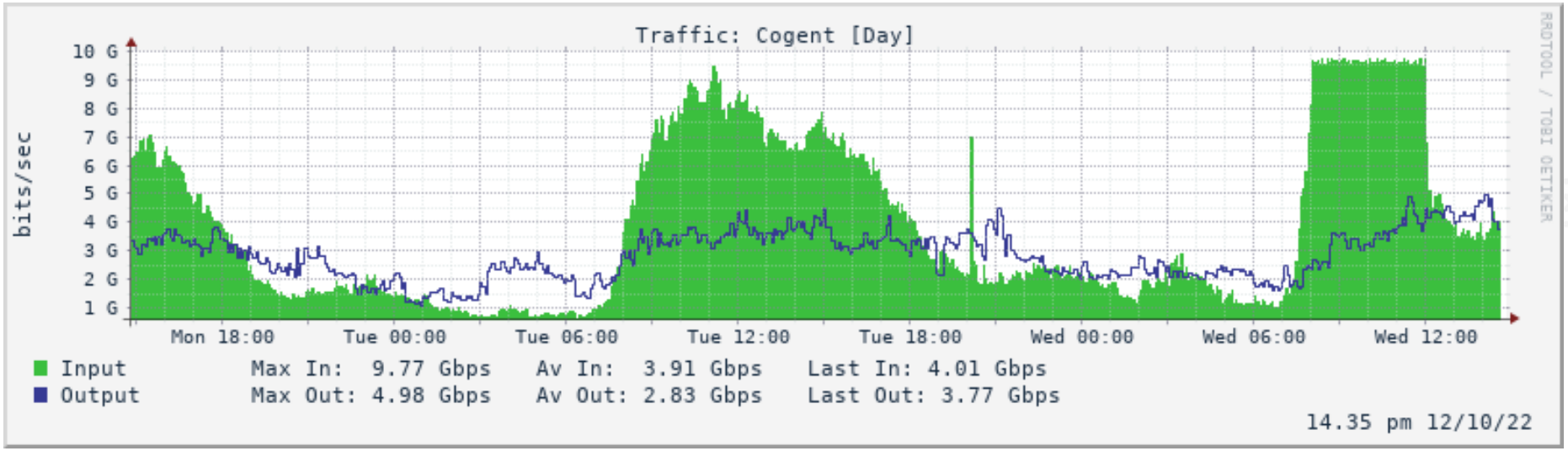
GARR-CERT

Agenda

- Definizioni
- *Use cases*
- Contromisure tecniche
- Ma … scala?
- Contromisure meno tecniche

Come appare (outfit di un DDoS)





DDoS: cosa ne pensano (i buoni)..

Viene definito DDoS il **traffico** di rete **cattivo**:

- proveniente da **più sorgenti**
- [per fortuna] quasi sempre destinato a un **singolo IP target**
- se supera una certa soglia:

  visibile, per es. 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.

.. e i cattivi

Distributed Denial Of Service (DDoS) – Clearnet

$100 – $410

2 sold in last 49 hours

TIME (DAY)

Choose an option

4 people are viewing this right now

Guaranteed Safe Checkout

Tor Secured | bitcoin | MONERO | reddit verified

DDoS Attack as a Service

$600.00

★★★★★ (reviews)

Rent a Hornet Botnet of 67,000+ Bots For Attack

$850.00

★★★★★ (reviews)

TERMS:

1. If you'll leave us feedback with a video AKA **"Vouch"** you will get **10% ($85) cashback** in BTC for this service.

Novità?

HPP Grid: today

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

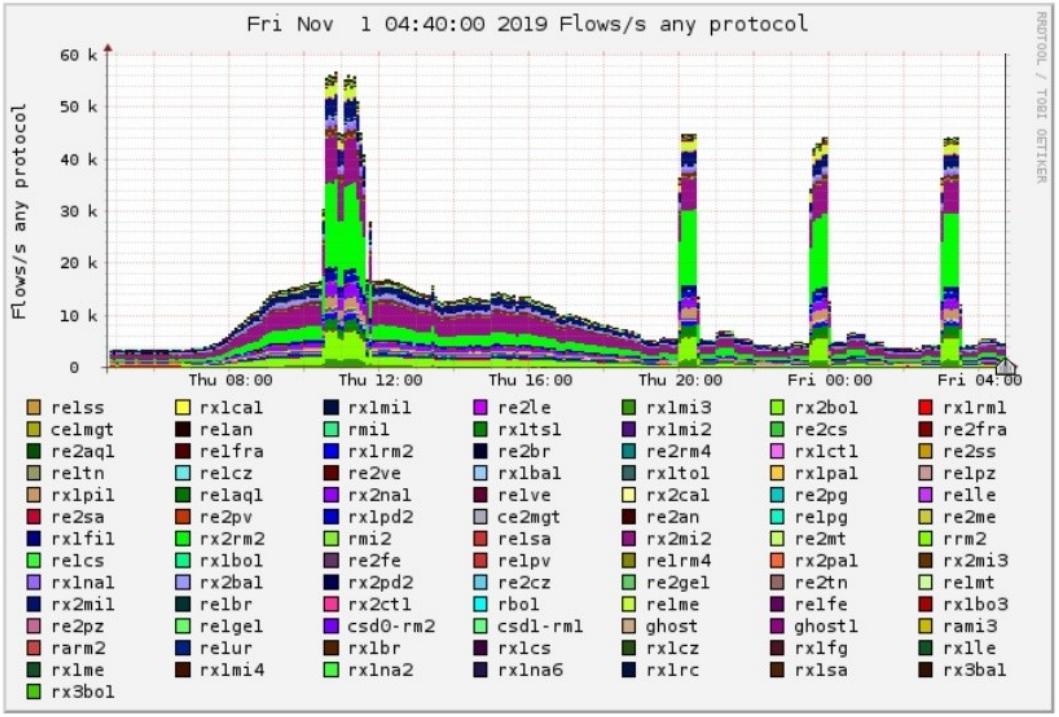
PROFILE	RANK	IMPACT LEVEL	TARGET	
Wanna Be Lamer	Amateur	NULL	End-User	
Script Kiddie		LOW	SME	Specific security flaws
Cracker	Hobbiest	MEDIUM / HIGH	Business company	
Ethical Hacker		MEDIUM	Vendor	Technology
Quiet, Paranoid Skilled Hacker		MEDIUM / HIGH	On necessity	
Cyber-Warrior	Professional	HIGH	"Symbol" business company	End-User
Industrial Spy		HIGH	Business company	Corporation
Government agent		HIGH	Government	Suspected Terrorist
			Strategic Company	Individual
Military Hacker		HIGH	Government	Strategic Company

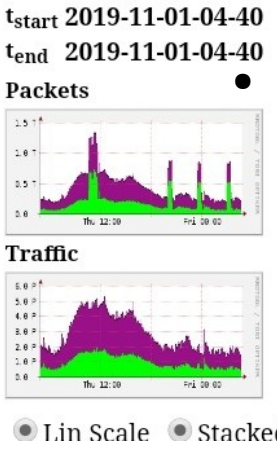
Hacker Profiling Project, 2005 – isecom.org – Raoul Chiesa, Stefania Ducci [UNICRI]

Profilo Hacker, 2006 – Raoul Chiesa, Silvio Ciappi.

Lottomatica [21/10/19]

- Segue una PoC di pochi giorni prima, e una mappatura sistematica dei servizi TCP aperti su rete GARR.
- SYN con IP sorgente spoofed dell'AS Lottomatica.
- 9 attacchi, con IP GARR partecipanti tra 25000 e 54000.





Risolto con:

- accordo tra AS
- istradamento su interfacce specifiche
- filtri su interfacce verso sorgenti "cattive".

Lottomatica [21/10/19]

Lesson learned

- Monitor su SYN distribuiti verso IP GARR (dai dati netflow dei RR)
- Aggiornamento della procedura di gestione degli incidenti (2020):
  - trattato esplicitamente il caso di nodi GARR target di attacchi
  - possibilità di filtraggi estesi del traffico in ingresso (sorgenti esterne ad AS137), tipicamente per /24
  - procedura di emergenza: CERT+NOC in casi particolari possono decidere per un filtraggio immediato.

E. The Brave (gennaio 2021)

- CERT apre ticket per due DDoS UDP con IP target GARR.
- Referente per la sicurezza risponde con un report [spettacolare] per alcuni IP, dal quale si capisce che non è il "solito DDoS":
  - aumento delle risorse per il FW non sufficienti
  - combinazioni di vettori di attacco inusuali, non tutte riconosciute da Corero (anche se singoli IP target)

E. The Brave (gennaio 2021)

target IP	start	duration (m)	description	flussi	details	impatto
.232	14:15 08/01/21	15				Rallentamento delle prestazioni
..193	14:15 08/01/21	15				Rallentamento delle prestazioni
.240	14:15 08/01/21	15				Rallentamento delle prestazioni
.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
.220	10:30 08/01/21	20	DDoS verso porte variabili	500K flussi con fw (senza attacco 20K)	source distribuita	Blocco della connettività
.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
.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
.68	21:50 07/01/21	15				Interruzione dei servizi di autenticazione

E. The Brave (gennaio 2021)

- Attacchi ripetuti per circa 10 giorni, vari IP, decine di vettori.
- Ampia e rapida diffusione ai media, con riferimenti non banali (immagini prese da GINS)
- Probabili **minacce** per prossimo evento pubblico di rilievo
- NOC, CERT, ed E., si preparano per varie possibilità:

  filtri manuali su Corero, flowspec su router GARR, fino a blocco di traffico verso subnet specifiche (target) sulle interfacce di peering commerciali internazionali (portatori della maggior parte del traffico di attacco)
- .. e nulla, poi l'attacco finale non c'è stato.

"You-Know-Who"

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

- 2021:
  - 266 eventi, 46 tipologie distinte
- 2022 (solo fino a marzo):
  - 282 eventi, 64 tipologie distinte

“You-Know-Who”

Mitigazione & lesson learned

- Corero [sempre acceso]
- Saturazione di vari link, più volte
- Filtraggio lato GARR di UDP verso alcune /24
- Scarse informazioni su eventuali problemi dell’infrastruttura
- …
- “Poi ne riparliamo”.

Boxes in the middle

Vari casi di DDoS reflection TCP, ad alta amplificazione, che sfruttano FW più o meno intelligenti:

- risposte verbose predefinite agli IP sorgenti di traffico per **qualunque protocollo/porte** non previsti, bellissime quelle in forma di pagine html (porta sorgente 443).
- Risposte censorie agli IP che vogliono aprire connessioni a siti non consoni all'attività lavorativa, tipicamente redirect a pagine di spiegazione del motivo per cui la navigazione non è consentita.

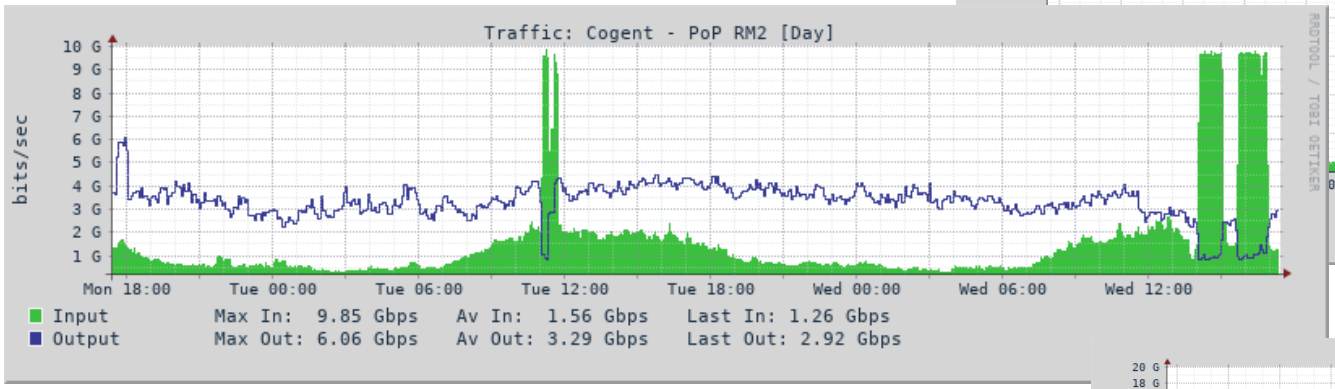
"*Sì, ma quanti siete?*"

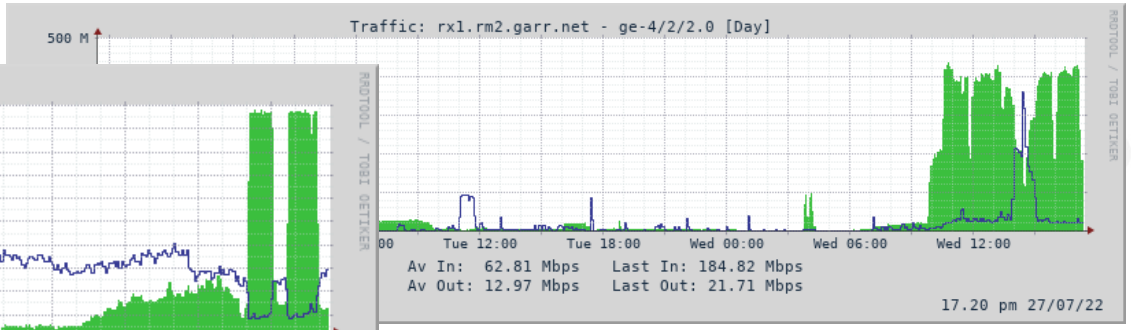
Ieri (27/10/22, fonte Shadowserver), **1231 IP**.

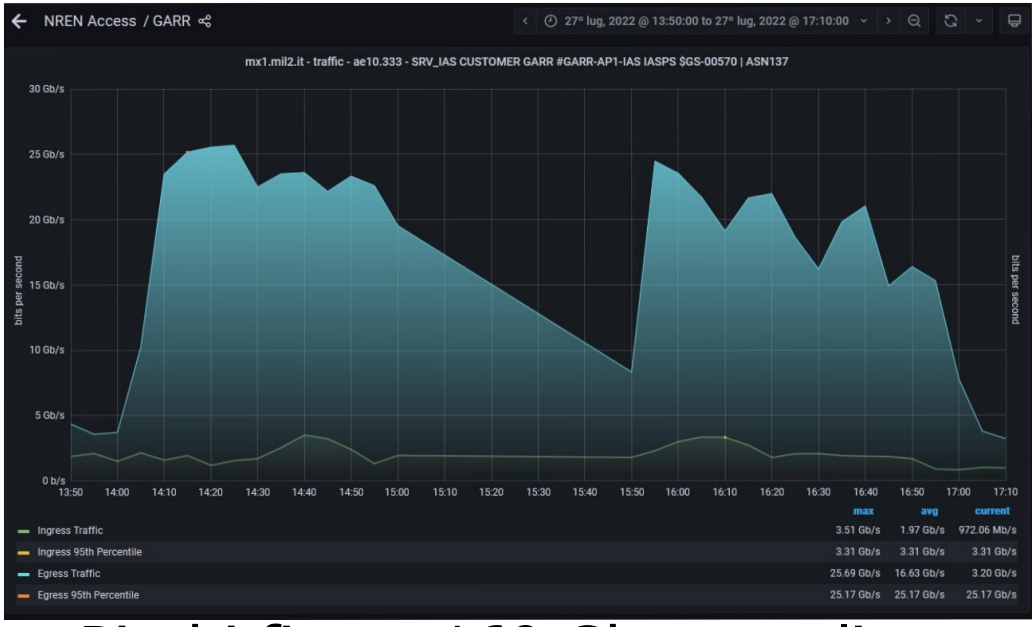
Killnet (11 maggio 2022)

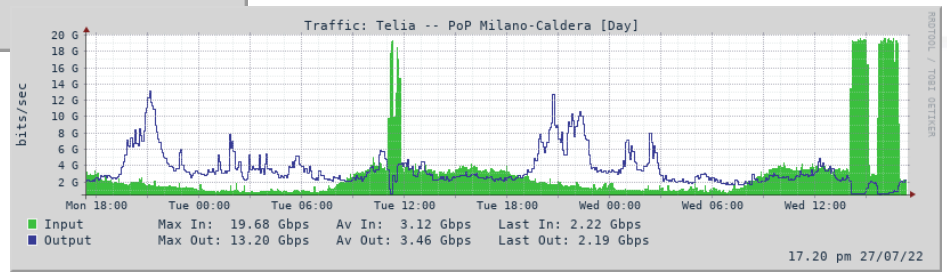
- 3 enti su rete GARR presenti tra i target indicati in un canale Telegram associato al gruppo Killnet [“pro Russia”, dopo inizio guerra in Ucraina].
- Attacchi http Get/Head/Post/Slow Flood e successivi upgrade, con sorgenti distribuite, eseguiti da volontari/simpatizzanti/..., tramite uno dei tanti tool scaricabili da github.
- Notizie di altri siti istituzionali colpiti esterni ad AS137, con anche qualche richiesta di aiuto.
- **Molto probabilmente**, 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 (o equivalenti).

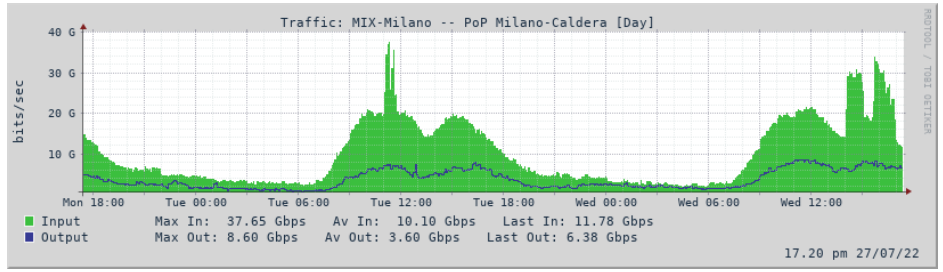
DDoS per un IP, caos per gli altri











- Picchi fino a 160 Gbps totali
- Corero ferma fino a 90%, ma.. dopo gli uplink

Contromisure (tecniche) di GARR

- Automatiche

  Corero [SmartWall Threat Defense Director]

- Un po’ meno automatiche

  filtri manuali su Corero

  regole flowspec

  black hole routing per IP/CIDR [equivalente a > dev/null]

  intervento su routing di singole interfacce

Riepilogo (tecnico) per tutti

- Corero funziona molto bene, su quello per cui è programmato.

- Ogni porta aperta è sfruttabile per una qualche forma di reflection..

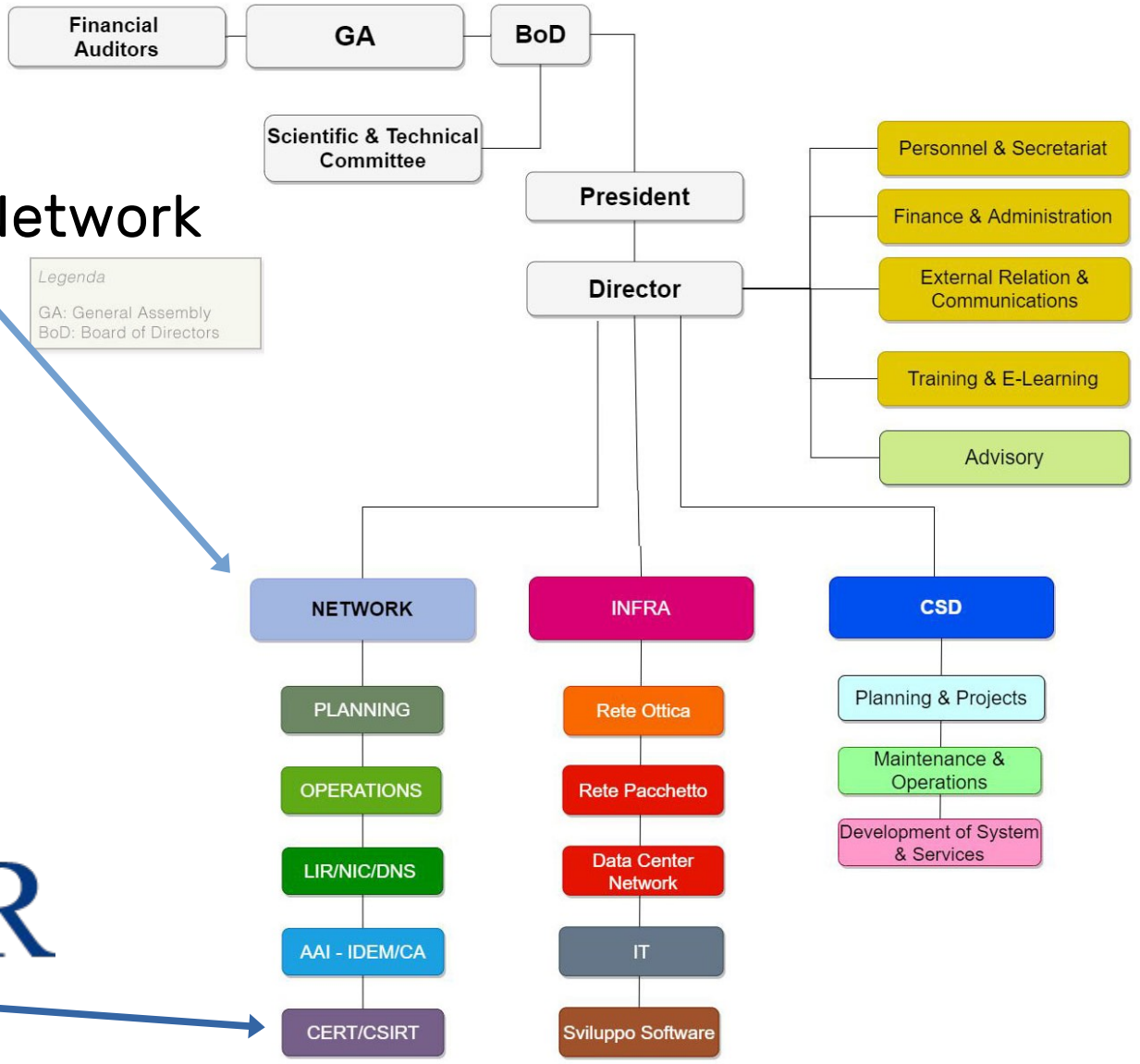
  .. ma anche ogni porta chiusa male.

  Versione alternativa: più il firewall è grosso, più fa rumore quando cade.

- Ogni IP del path Internet → … → servizio aperto (compreso), va difeso (spesso basta poco, come non annunciarlo se non serve) come se gli altri fossero fuori controllo.

GARR-CERT

- Servizio operativo del Dipartimento Network della rete GARR **user-oriented**



CERT GARR

RFC 2350 (CERT Ansible Playbook)

"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 gestione 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 gestione 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.

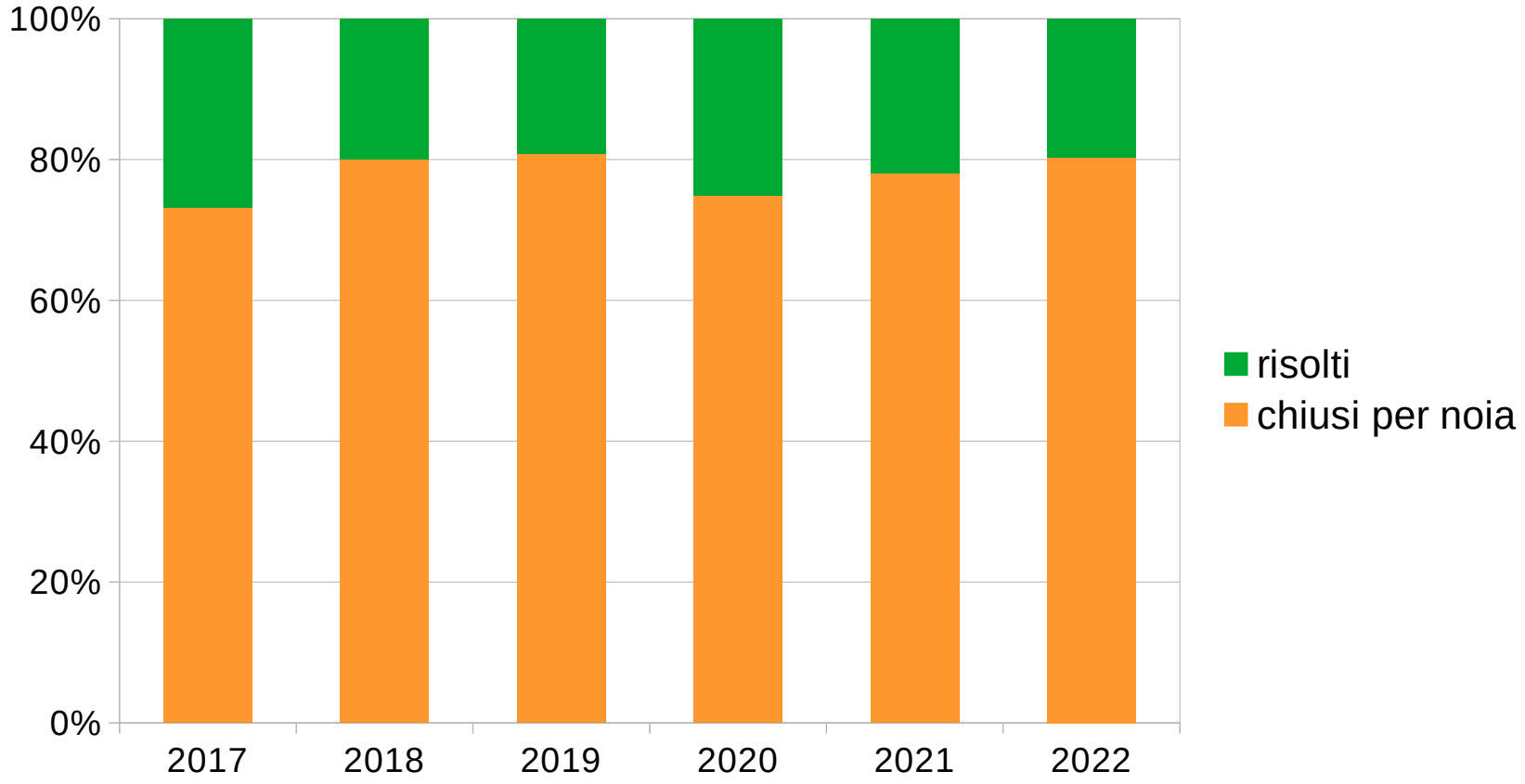
  Dopo X tempo -> chiusura d'ufficio, detta anche "**per noia**".

Ma.. scala?

- Abbiamo [aggiornati al 27/10/2022] 2305 record di email di APM, divisi per:
- 1658 record di associazione a una rete (v4 e v6),
- 647 record di associazione IP di una connessione punto-punto (non mettendo nel conto gli IP 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?**

In queste condizioni.. no.

Andamento % della chiusura dei ticket **totali** di GARR-CERT



Contromisure (meno tecniche)

Da implementare velocemente

- Maggiore coordinamento e collaborazione con GARR degli enti collegati alla rete **su tutti gli aspetti relativi alla sicurezza**.

- Forme di mitigazione condivisa con le "reti confinanti", da adottare in tempo, finché abbiamo attacchi che coinvolgono solo pochi IP alla volta.

.. e basta?

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://youtu.be/PLJJY5UFtqY
- https://www.nginx.com/blog/mitigating-ddos-attacks-with-nginx-and-nginx-plus/
- https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/
- isecom.org

WORKSHOP GARR 2022

NET MAKERS

Q&A alla fine della sessione?

Grazie!

Leonardo Lanzi

GARR-CERT