E il CERT.. cosa ha visto?

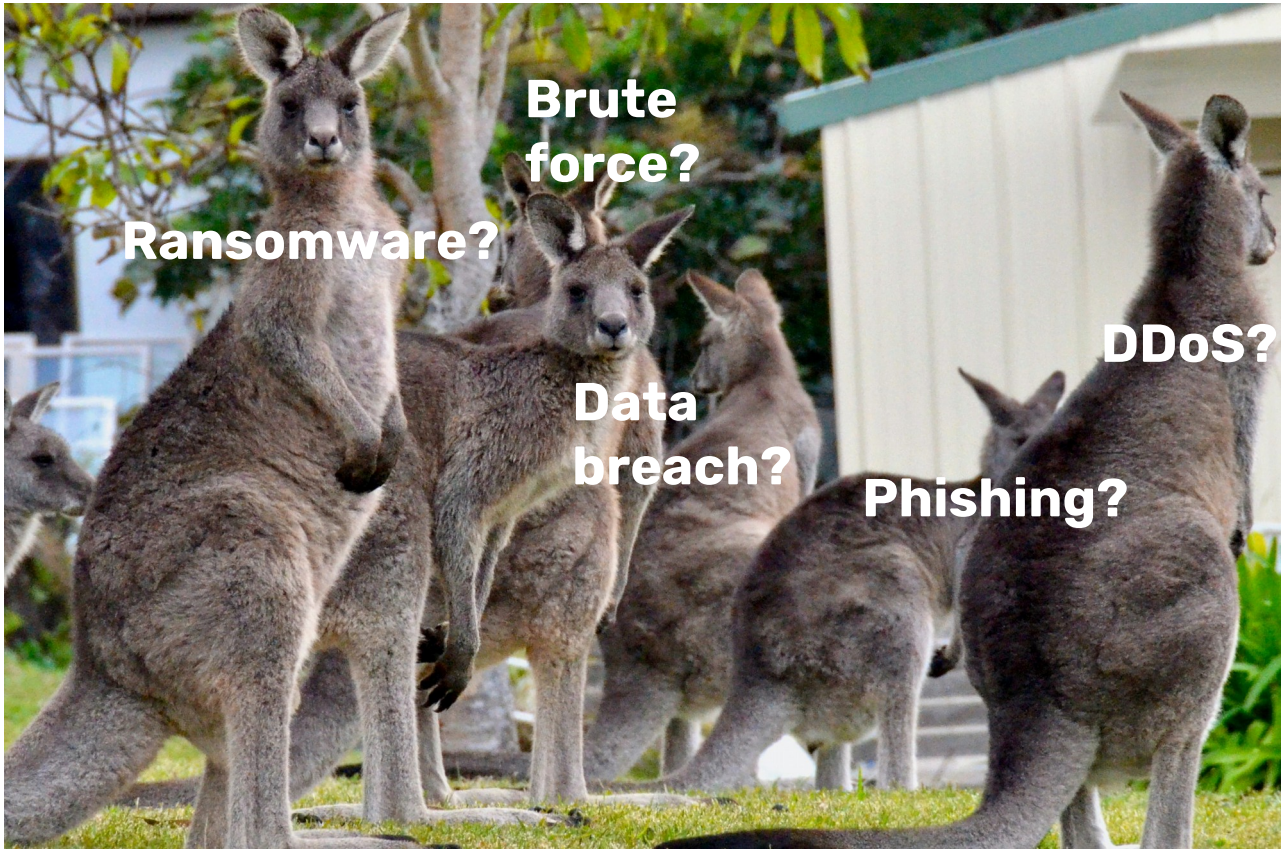
Leonardo Lanzi
GARR-CERT

WORKSHOP GARR 2020

NET MAKERS

Consortium GARR

E il CERT.. cosa ha visto?



GARR-CERT - Chi siamo

Leonardo Lanzi

Andrea Pinzani

Maria Sole Scollo

Simona Venuti

Agenda

Incidenti di sicurezza e alert automatici

Più o meno sicuri?

DDoS

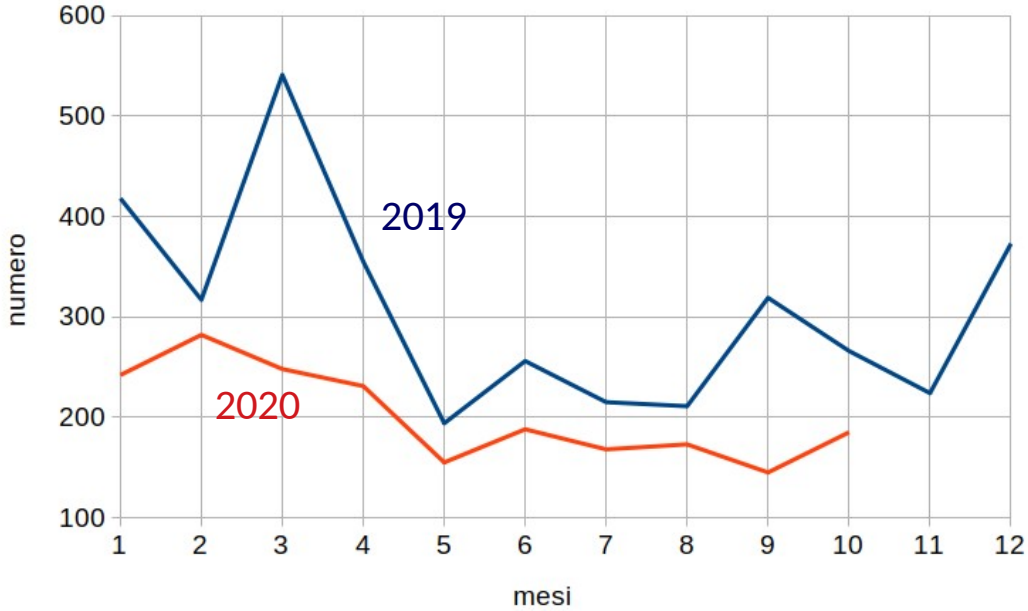
Attività GARR SCARR

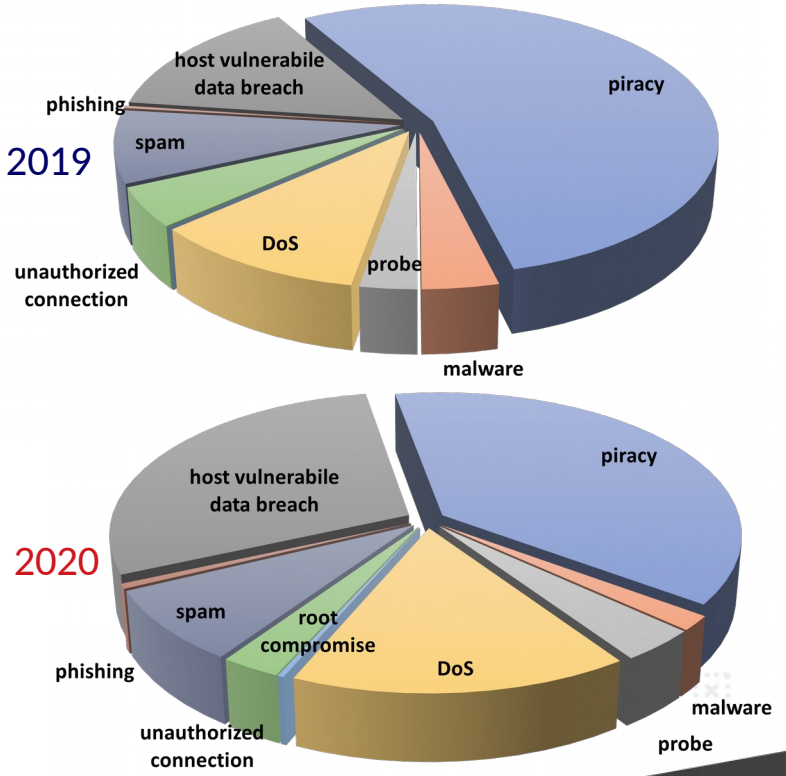
Risk analysis & monitor - PoC

2 domande

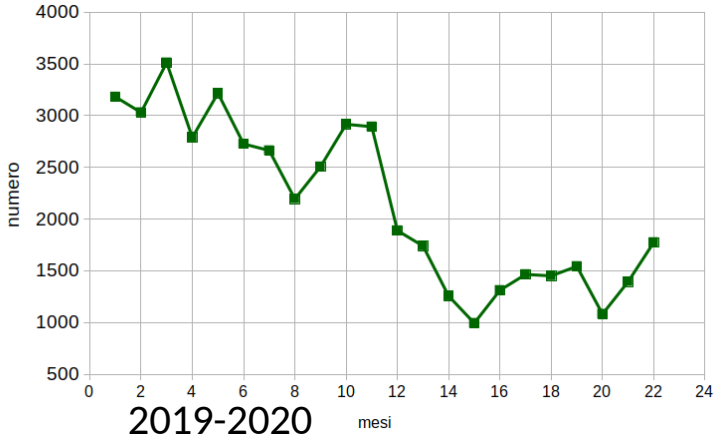
I soliti incidenti :(?

2019 - 2020


600
500
400
300
200
100
numero
1
2
3
4
5
6
7
8
9
10
11
12
mesi
2019
2020

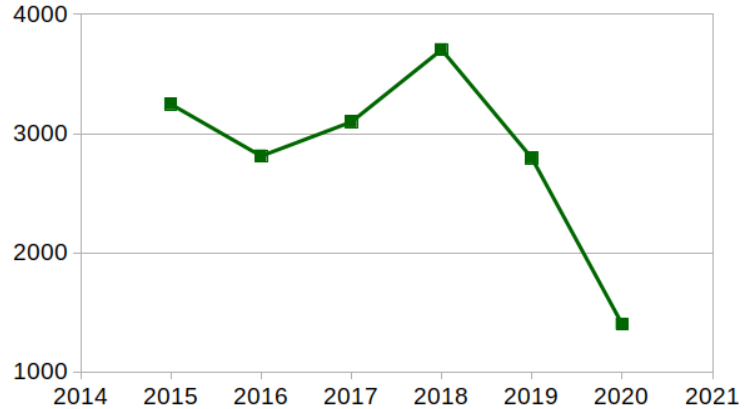

2019
host vulnerabile
data breach
phishing
spam
DoS
unauthorized
connection
probe
malware
piracy
2020
host vulnerabile
data breach
spam
root
compromise
phishing
DoS
unauthorized
connection
malware
probe
piracy

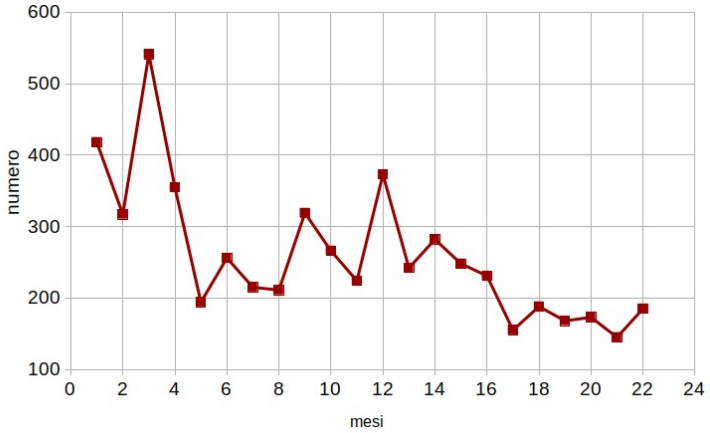
alert automatici & incidenti



2019-2020

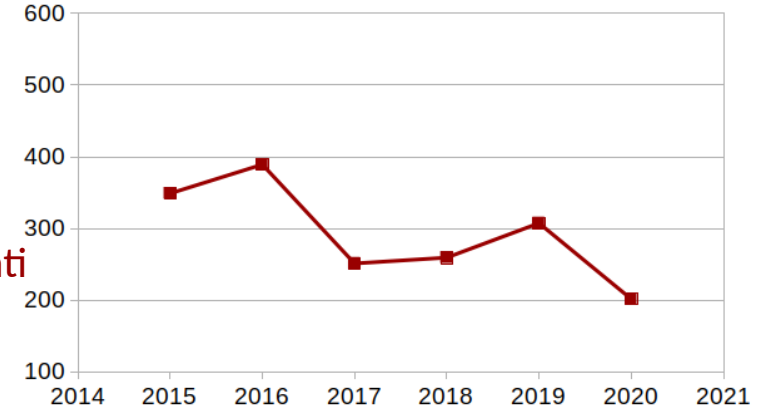
alert





incidenti

media mensile



Più o meno sicuri?

Incidenti totali: **3689** (2019) → **2017** (ottobre 2020)

\+ DoS

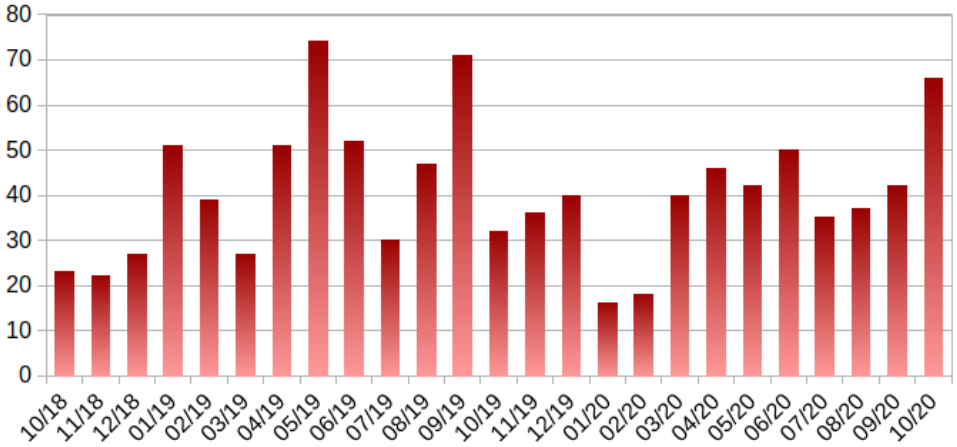
Aumento segnalazioni di host vulnerabili e data breach
(dal 6 maggio è operativo CSIRT-Italia).

Diminuzione del numero di IP GARR in quasi tutte le categorie ricevute da Shadowserver (fino a -70%), anche per tipologie non segnalate.

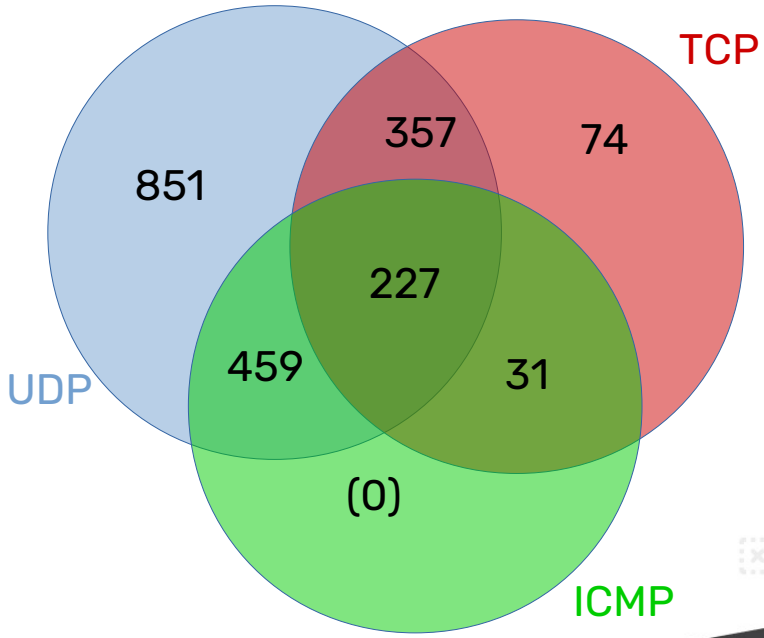
DDoS: monitor e mitigazione

DDoS monitor

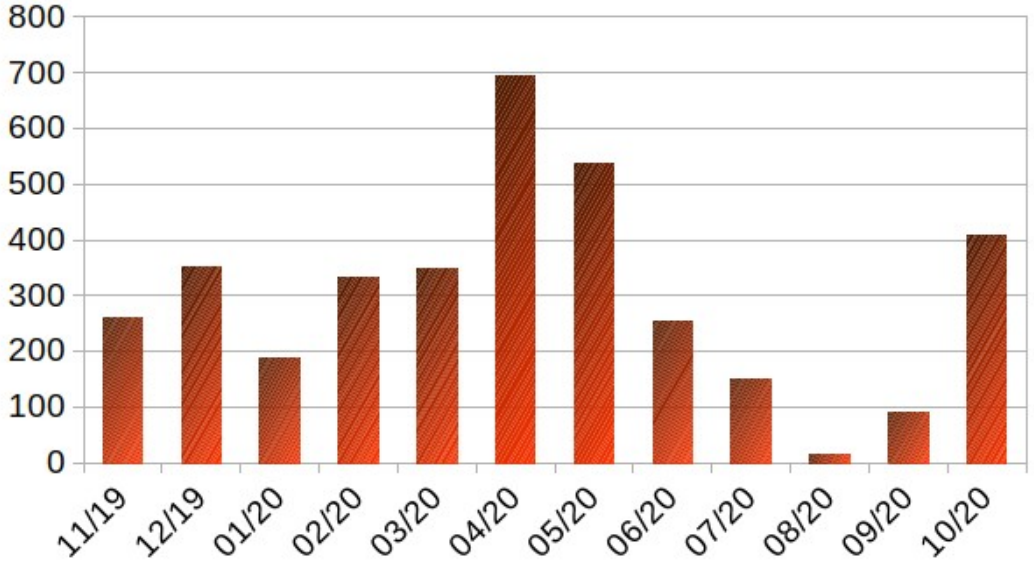
Eventi rilevati



	UDP	TCP	totali
Numero	1894	689	2583
Conteggio porte usate	14227	3656	17883

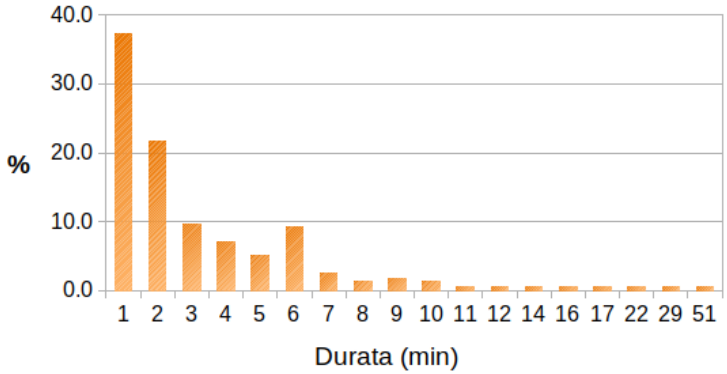


Mitigazione Corero's SmartWall



3904 filtri temporanei, di cui 10 su IPv6.

Durata media di un attacco
~ 3.5 minuti.



Attacchi TCP distribuiti

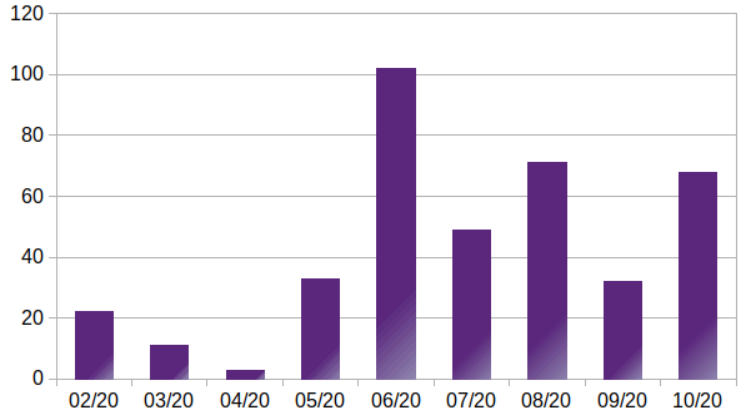
Corero funziona con target singoli.

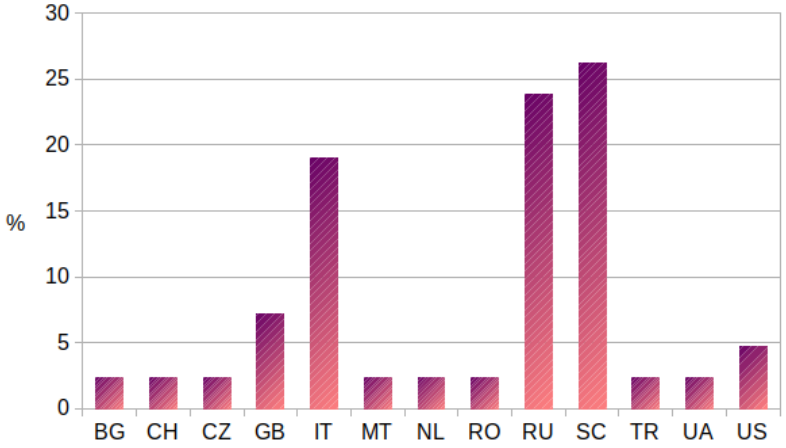
Da febbraio, allarme per network sorgenti di > 80M SYN / 5 min.

Rilevati 391 attacchi verso ~tutta la rete GARR.

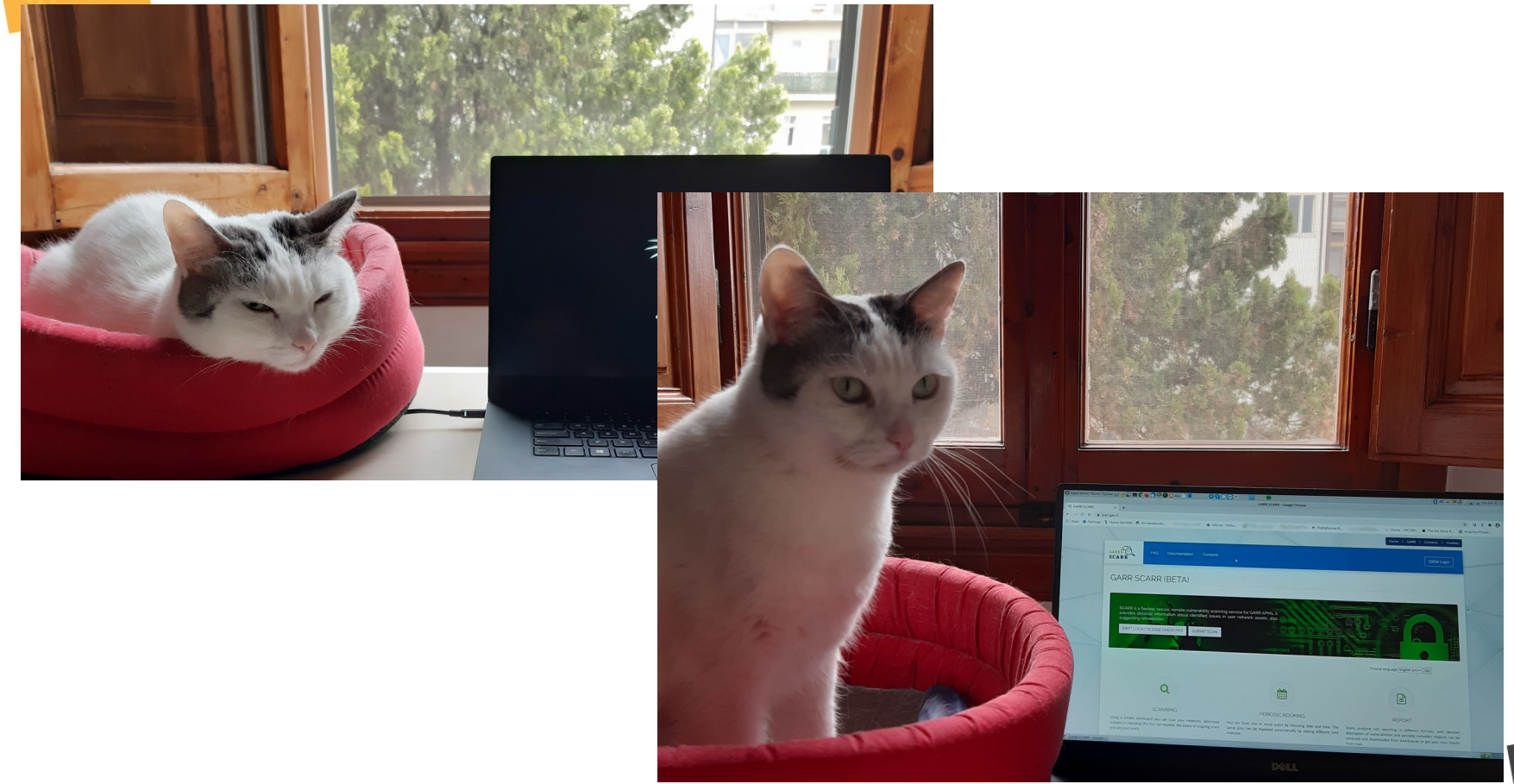
41 reti (qualche /16, varie /24), 14 ASN, 13 paesi.

Spunti per una difesa “globale”.

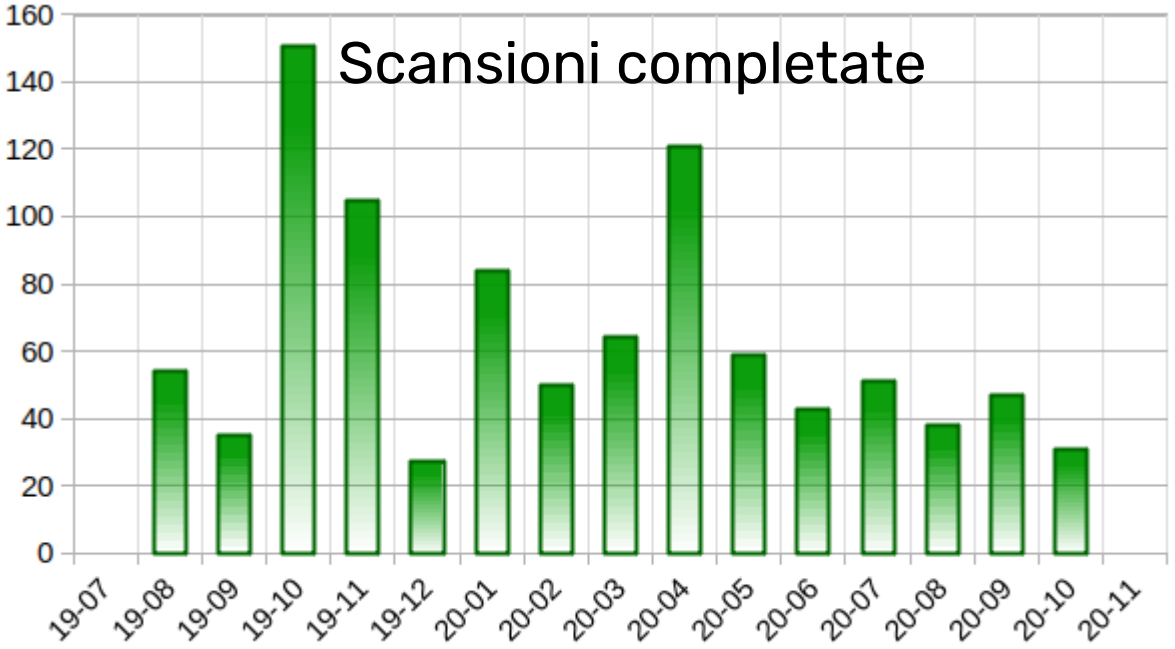




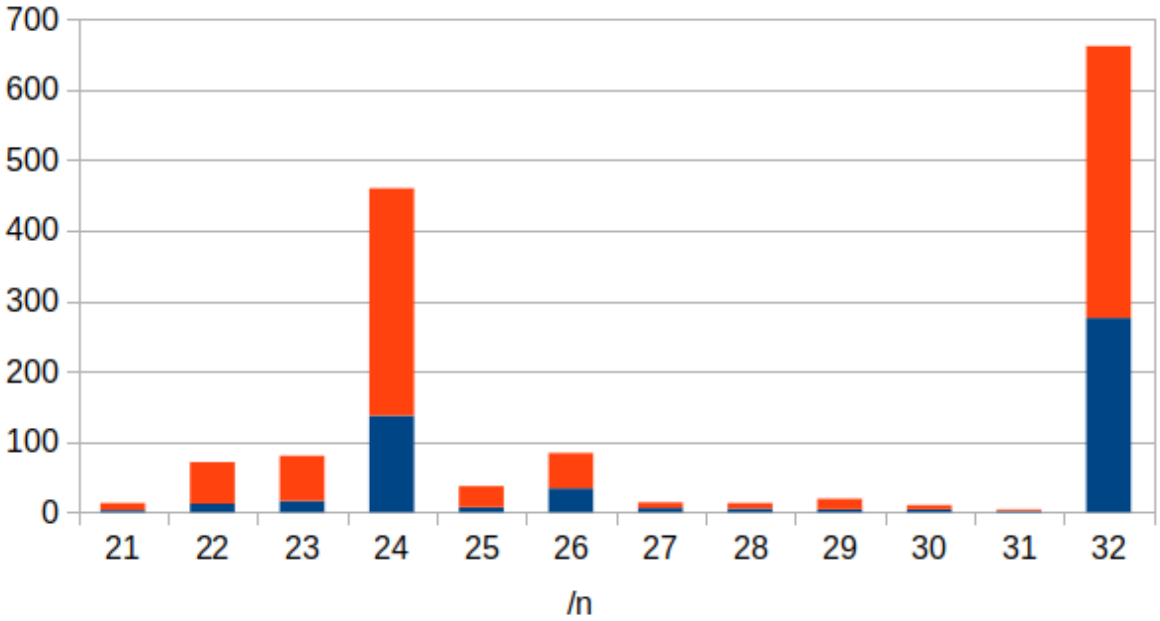
Scansioni in *Full Remote Mode*



Un anno di SCARR



Un anno di SCARR



/ n	21	22	23	24	25	26	27	28	29	30	31	32
unique	3	12	16	137	7	34	6	5	4	4	2	276
all	10	59	64	323	30	50	8	8	15	6	2	386

Oltre 65’000 IP unici esaminati.

Quasi 200’000 IP contando le scansioni ripetute.

90% scansioni completate.

Risk analysis

Sicurezza dell'informazione

Sicurezza di reti e sistemi:

- Firewall, SIEM, analizzatori di traffico..
- Scansioni di vulnerabilità
- Difesa dai DDoS

E i dati?

CTI per la rete GARR

Collaborazione con Resecurity, Inc.

PoC di una piattaforma di Cyber Threat Intelligence, *Risk.*

- Stima dei rischi per domini, reti, host esposti, servizi in cloud.
- Monitor di oltre 20 vettori di rischio, tra questi: data breach, malware, botnet.. da fonti open e closed, referenziate.

> 10 beta tester (30 domini) già reclutati.

API in arrivo.

2 domande

Accendiamo qualche altro alert automatico?

Volete aggiungervi ai volontari della PoC di Risk?

menti.com/ipkxccuh87

Grazie !

Leonardo Lanzi
GARR-CERT

WORKSHOP GARR 2020

NET MAKERS

Consortium GARR