Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

20 anni di GARR-CERT

LEONARDO LANZI

Roma, 8 – 10 ottobre 2019

Workshop GARR – NET MAKERS

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

GARR-CERT is 20 years young

LEONARDO LANZI

Roma, 8 – 10 ottobre 2019

Workshop GARR – NET MAKERS

Init

2° WORKSHOP GARR - LA SICUREZZA IN RETE

EVENT

Title:	2° Workshop GARR - La Sicurezza in Rete
When:	Mon, 17. January 2000 - Tue, 18. January 2000
Where:	Università degli Studi di Napoli Federico II - Napoli, NA
Category:	Workshop
Community:	Scientific Research, Biomedic Research, Cultural Heritage, University, School, Music & Art

DESCRIPTION

2° WORKSHOPO GARR: LA SICUREZZA IN RETE
NAPOLI, 17 E 18 GENNAIO 2000

L'aumento dell'utilizzo delle risorse di rete si accompagna inevitabilmente all'acuirsi dei problemi legati al loro uso non autorizzato vedi ad esempio il proliferare dei mail pubblicitari non sollecitati, i cosiddetti spam mail, e le intrusioni, anche con gravi conseguenze, nei sistemi meno protetti.

Per questo motivo, nell'ambito di GARR-B, come in tutte le altre realtà di questo genere, è stato istituito GARR-CERT, un servizio per la gestione delle problematiche legate alla sicurezza software.

Una delle finalità di GARR-CERT, se non forse la principale, è la sensibilizzazione degli utenti a questo tipo di problematiche.

....

Enzo Valente - Direttore del Progetto GARR-B

Roberto Cecchini - Responsabile di GARR-CERT

GARR - CERT

Dal II incontro di GARR-B, gennaio 2000:

- Istituito nel Marzo 1999, pienamente operativo da Giugno 1999;
- 8 unità: 2 a tempo pieno e 6 a tempo parziale.
- Gli utenti sono tutte le istituzioni afferenti alla rete GARR.
- I compiti
  - rispondere alle segnalazioni di incidenti, avvertire ed assistere gli utenti coinvolti e seguire gli sviluppi;
    - **politica di riservatezza**
  - diffondere informazioni sulle vulnerabilità più comuni e sugli strumenti di sicurezza da adottare;
  - controllare periodicamente "lo stato di salute" dell'utenza per le vulnerabilità più gravi o più comuni;
  - gestire corsi di aggiornamento tecnico;
  - provare strumenti esistenti, e svilupparne di nuovi per esigenze specifiche.

Incidente

- Gestito con procedura approvata dal CTS GARR il 23/1/2007
  - tempi di intervento richiesti:
    - open mail relay :)) : 3 giorni
    - source di cattive azioni (portscan ecc): 1 giorno
    - nodi usati per DoS: 5 ore
    - incidenti con conseguenze anche penali: 4 ore

  Q: Altrimenti ?
- Si apre con mail da cert@garr.it, PGP-signed, a: APM

  Subject: GARR-CERT-20J.. <argomento><IP>

  Salve,

  sono un operatore del GARR - CERT *[..], abbiamo ricevuto una segnalazione, in copia [...], secondo la quale [...]*

  Si chiude quanto tutto è felicemente risolto, o per noia.

Segnalazione automatica

- Mail da cert@garr.it

  Subject: **GARR-CERT-A ...**

  con descrizione di un possibile problema:

  Caro Collega,
  riceve questo messaggio perche' risulta APM
  https://www.garr.it/it/comunita/la-comunita-garr/gli-apm
  della rete sotto indicata: se cosi' non fosse la preghiamo
  di scrivere all'indirizzo segreteria@garr.it per far aggiornare
  le informazioni di contatto.
  Ci e' stato segnalato che….
  Timestamp
  IP
  ...

~ 30 tipi di segnalazioni

quasi in ordine	alfabetico
Android Debug Bridge esposto in rete	Inserimento in blacklist
Infezione generica da malware	Compromissione sito web - botnet
DNS sfruttabile per DRDoS	LDAP sfruttabile per DRDoS
IPMI aperto accessible dall'esterno	MDNS sfruttabile per DRDoS
vulnerabilita' IKEv1 Cisco IOS	MongoDB accessibile senza autenticazione
memcached sfruttabile per DRDoS	NTP (monitor e version) sfruttabili per DRDoS
MS-SQL Server Resolution Service sfruttabile per DRDoS	CISCO Smart Install accessibile
portmap utilizzabile come amplificatore per DrDoS	SNMP sfruttabile per DRDoS
SMB accessibile	XDMCP sfruttabile per DRDoS
SSDP sfruttabile per DRDoS	IoT, si accendono?

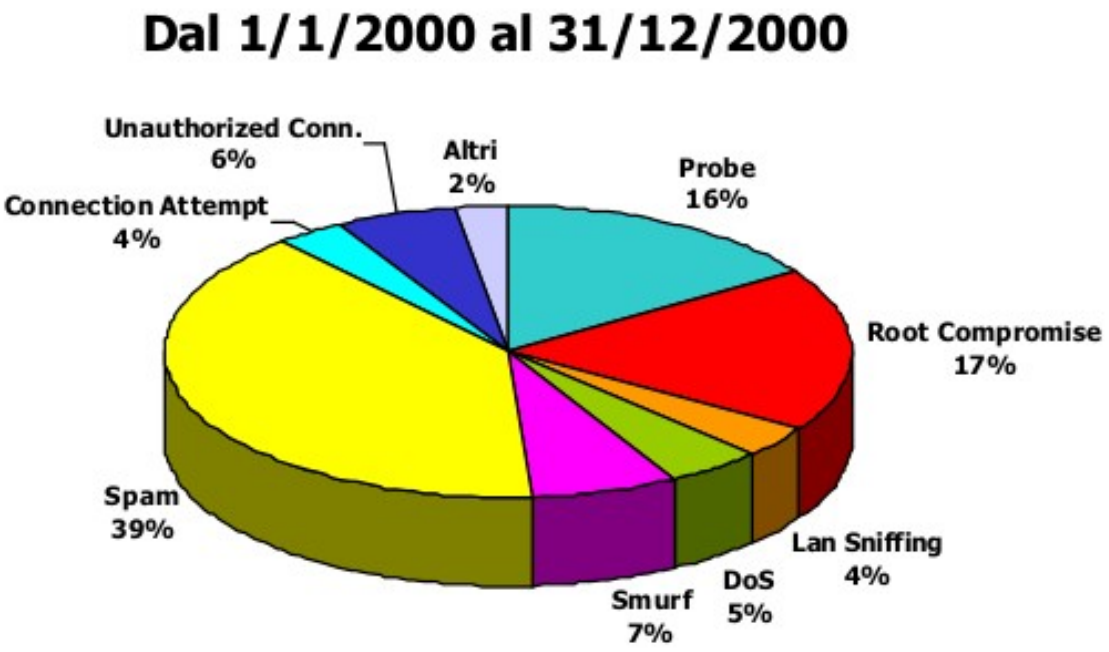
Fonte primaria
shadowserver

~20 in elenco.

Alcune non attivate perché:

- *a noi serve così*
- sono troppe

I primi incidenti



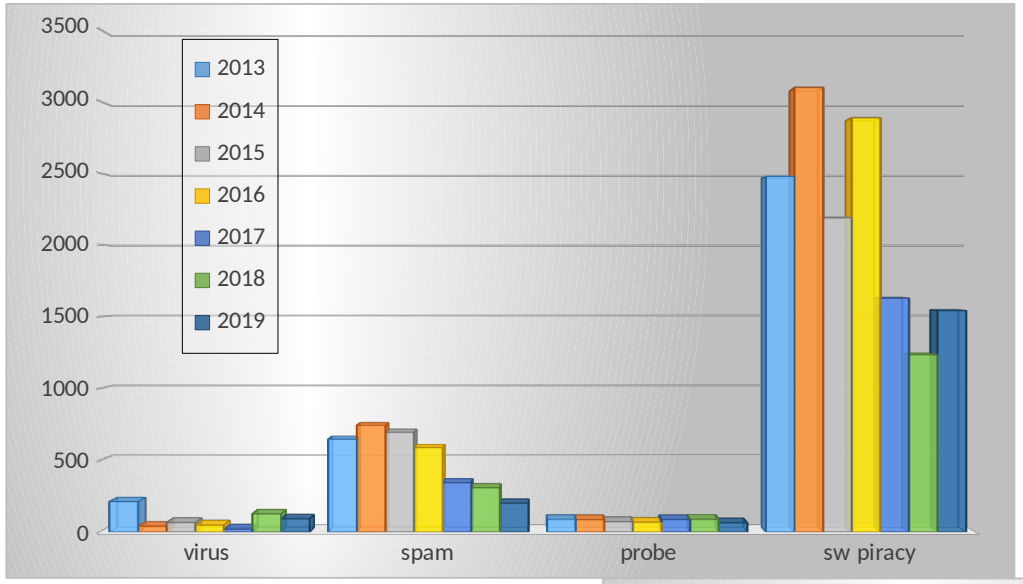
Totale: 1381

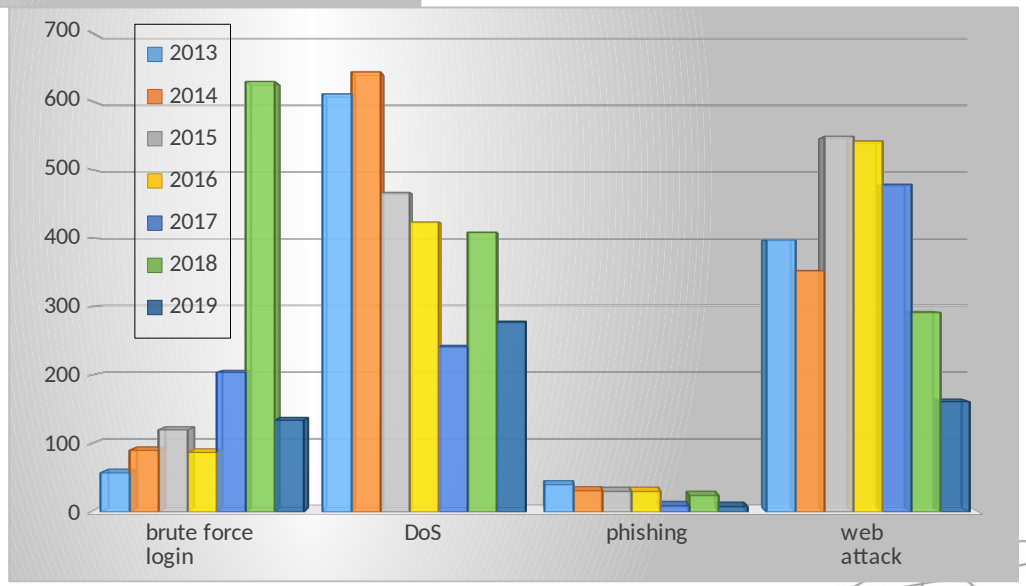
messaggi di e-mail: 10300

III Incontro di GARR-B

Firenze, 24-25 Gennaio 2001

Strada facendo





Adesso - 1/3

- Gestione, analisi, statistiche degli incidenti
- Valutazione e escalation di alert e azioni
- Monitoraggio della rete: per ricerca, a richiesta|supporto
- Alert di sicurezza via mail | sito GARR-CERT

- Segnalazioni automatiche preventive
- Scansioni di vulnerabilità … no, niente anticipazioni!! :P

- Tutorial, corsi, “Capture The Flag”

Adesso - 2/3

Attività congiunta con NOC:

- Allarmi automatici DDoS, SYNflood
- Monitoraggo di traffico row
- Gestione incidenti per DDoS / filtraggi

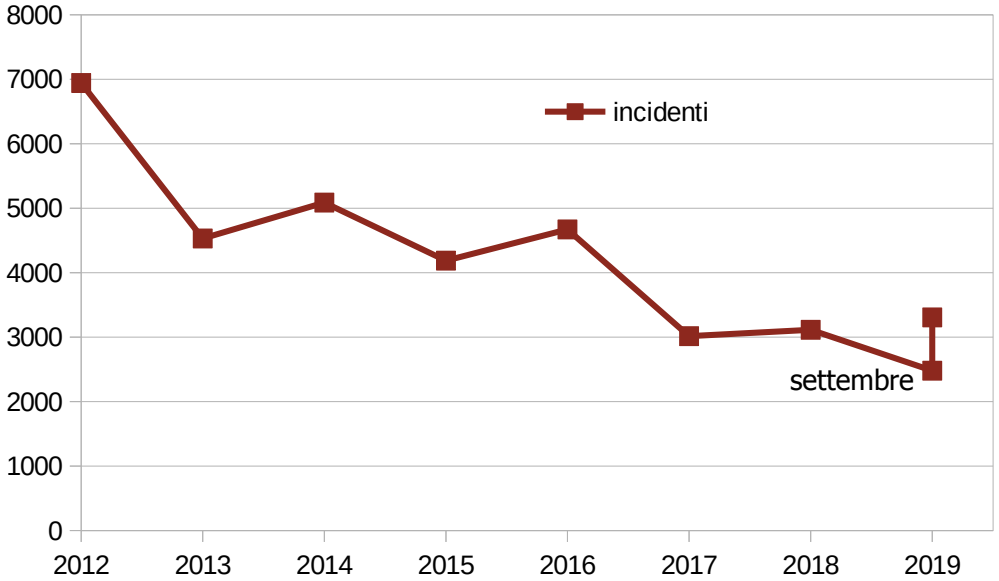
Workgroup Sicurezza – wg-sec (con utenti GARR):

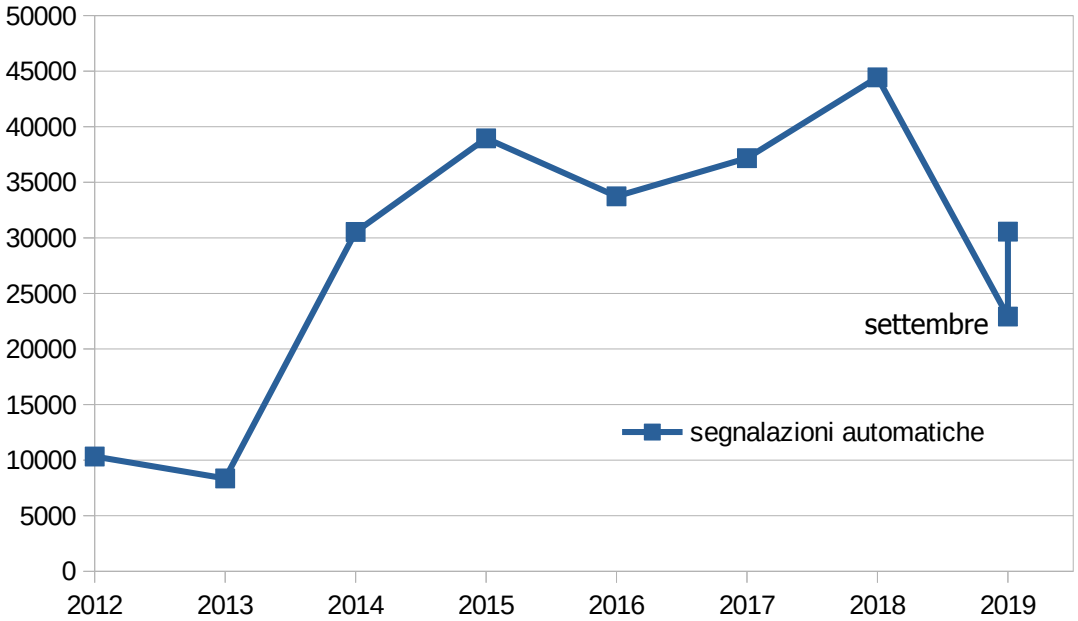
- Riunioni, VC, presentazioni
- Implementazioni per test di prodotti
- Condivisione documenti, materiali, idee

Adesso - 3/3

~ 1/3 delle segnalazioni automatiche diventano incidenti

Q: Qualche idea brillante?



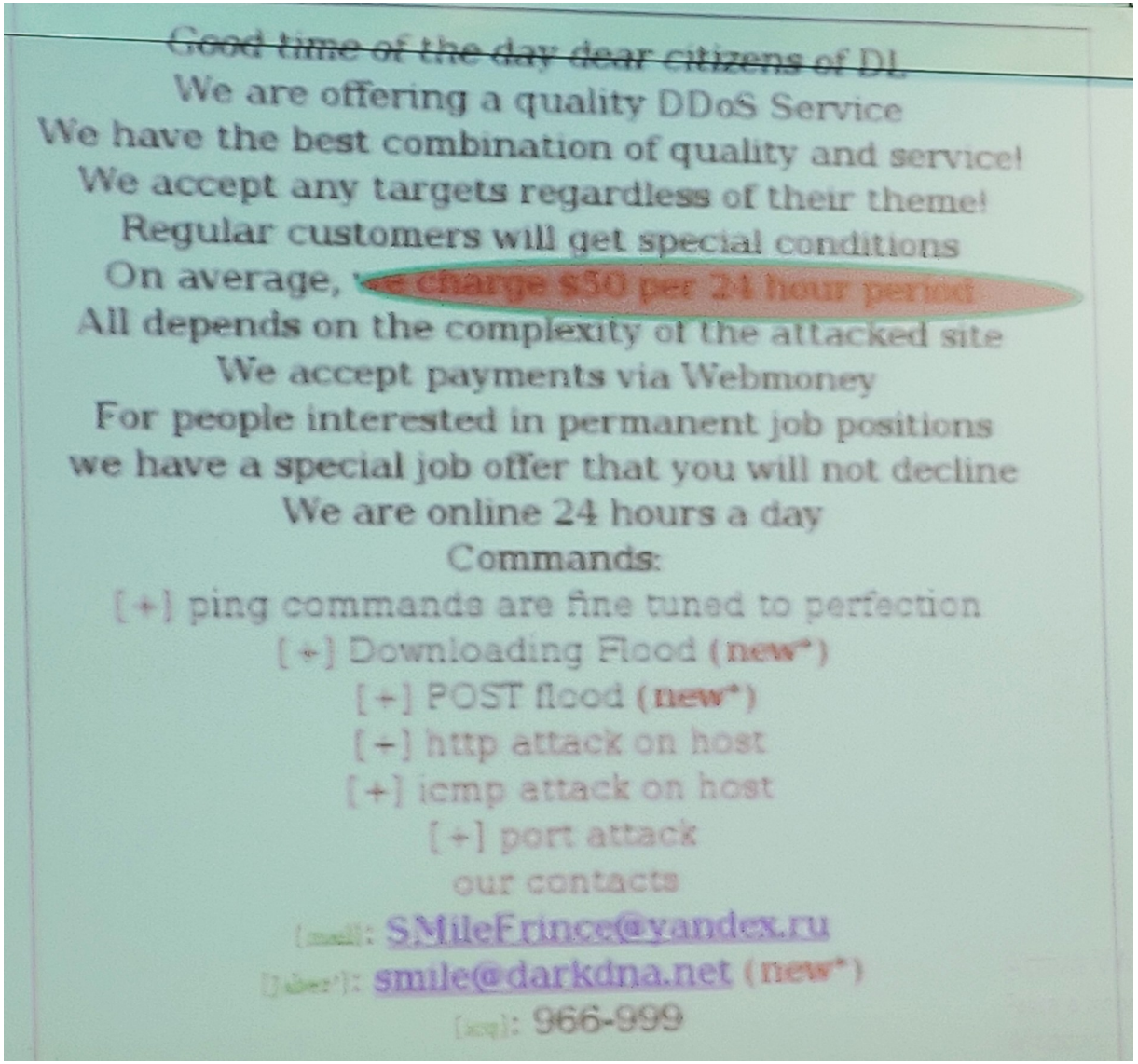


Quindi.. tutto ok.

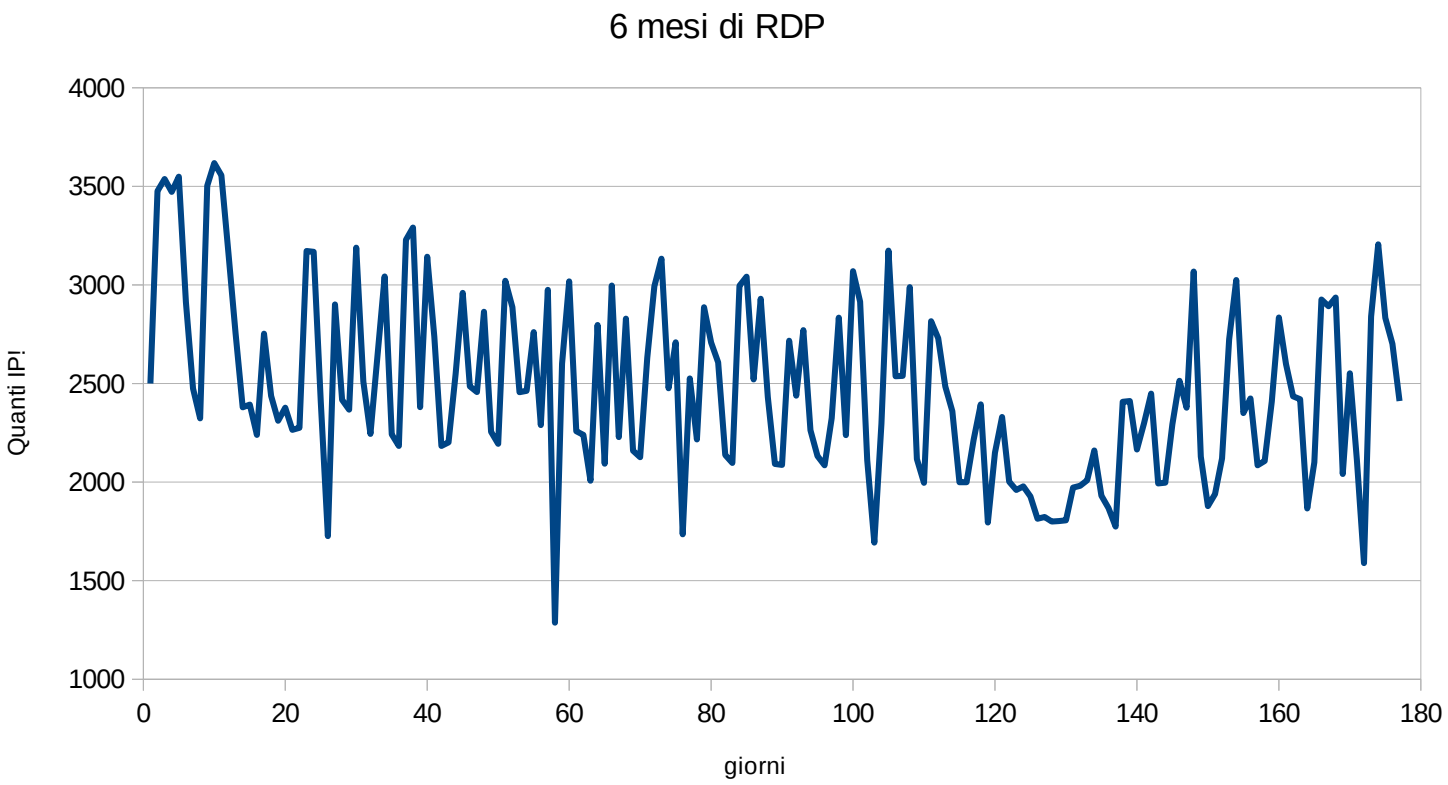
Ultimo anno

- Attacchi DDoS targeted verso alcune istituzioni: sono stati usati tutti i vettori possibili: reflection classici, SYNflood, low&slow http.
- Attacchi verso scuole in coincidenza di eventi importanti (esami, prove INVALSI)
- DDoS su ARP - Apple Remote Desktop - nessun allarme, centinaia di IP coinvolti, > 70 incidenti in un giorno
- DDoS classici su IP ordinati lessicograficamente, correlati entro qualche giorno di allarmi; es: classe B. + 13.130, 13.131, 13.132, 14.131, 24.35, 25.163...
- Vari casi di spear phishing preoccupanti
- Malware made in Italy via PEC
- Burst di mining o cryptojacking
- "Troppa" collaborazione, in aumento

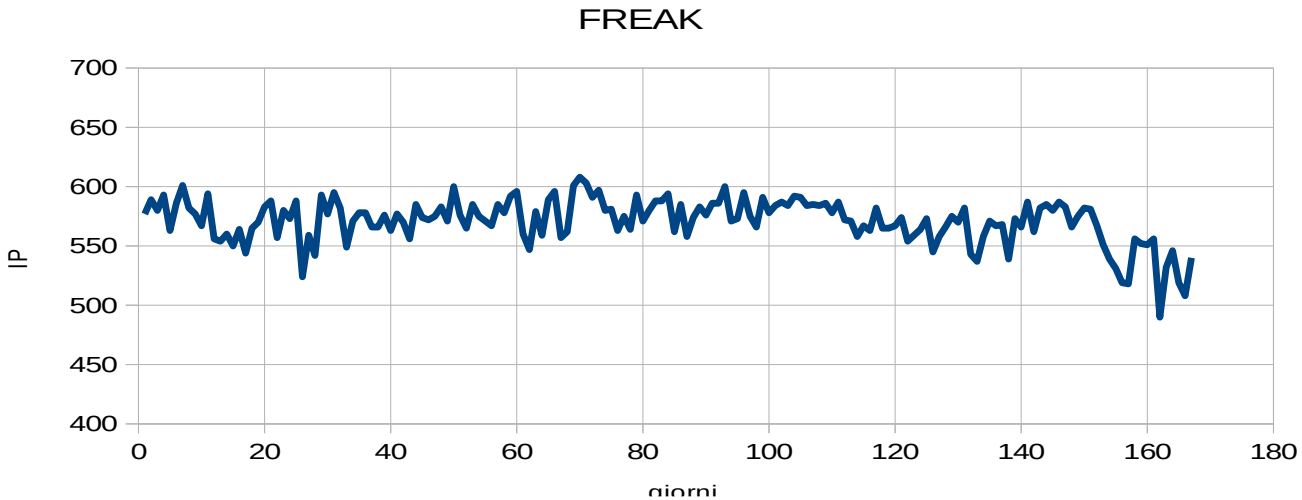
Dal corso del 7/10/2019 – DF & CTI

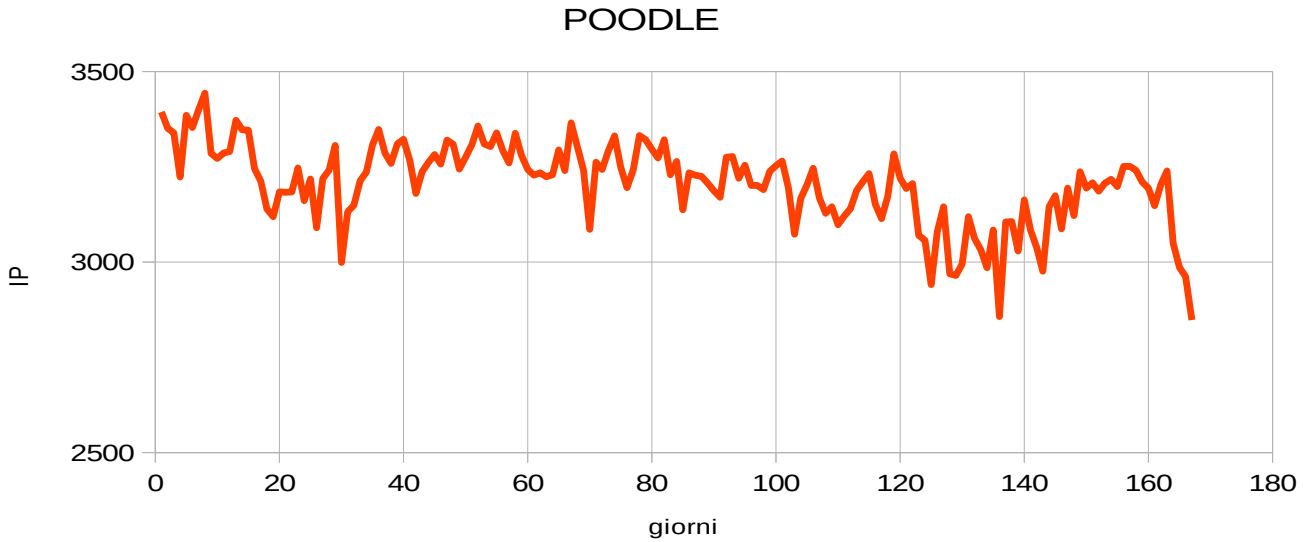


Remote Desktop [MS] – da aprile 2019



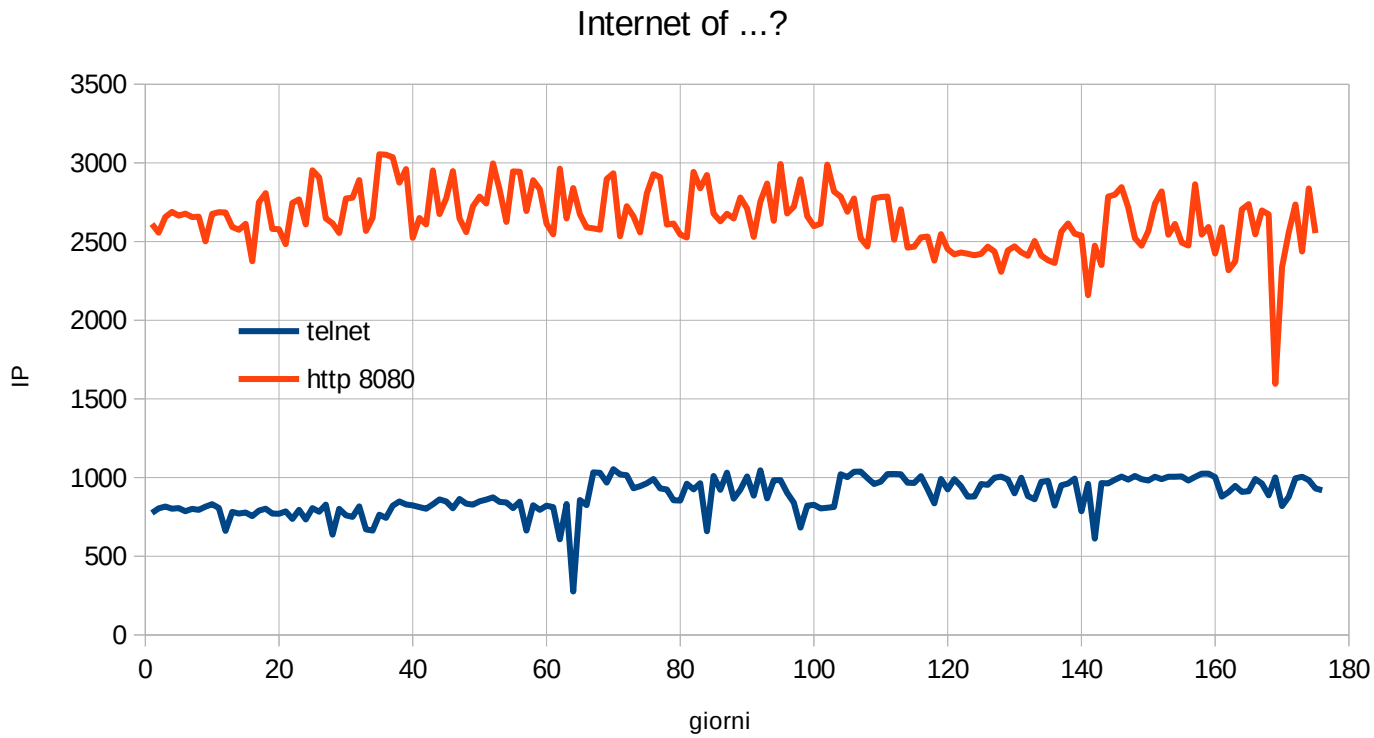
SSL FREAK & POODLE – da aprile 2019



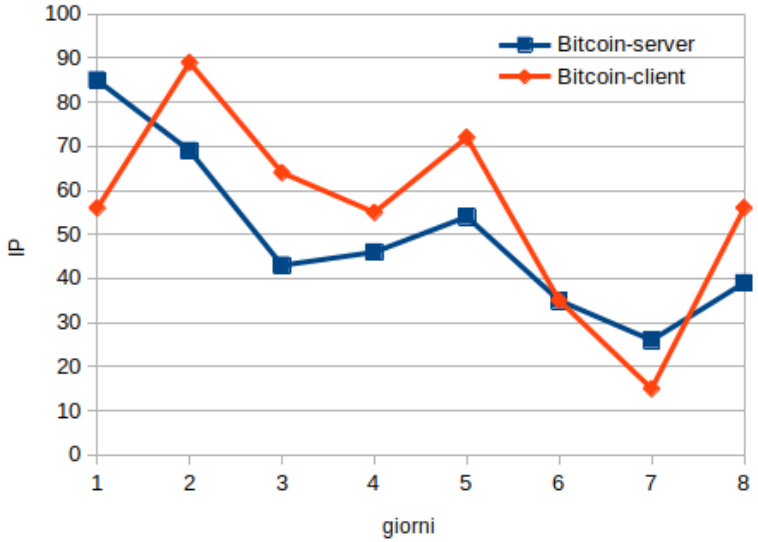


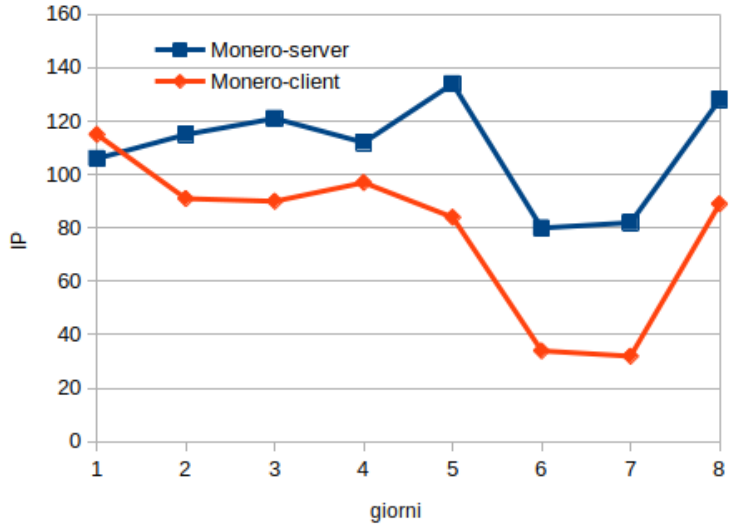
Internet of * [20 years young]

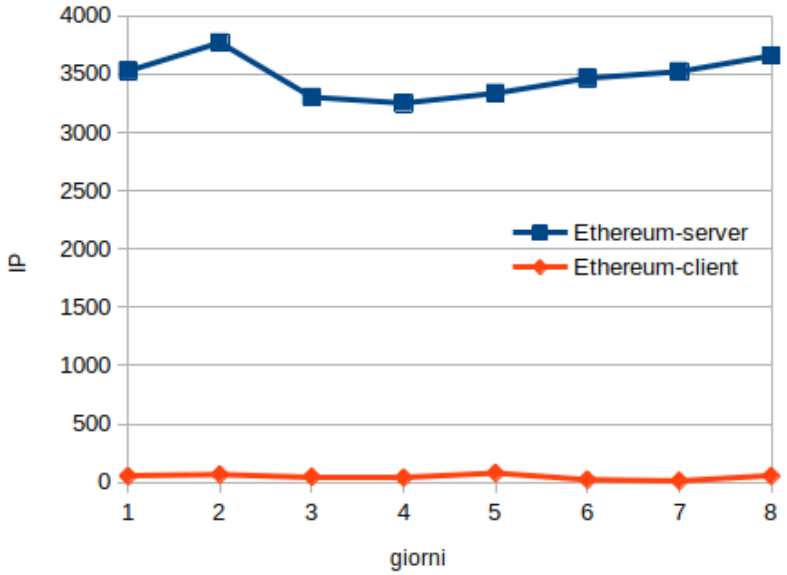
IP cam, NAS, lettori badge|apriporta, router|switch, pannelli solari, gruppi di continuità, luci di emergenza, prese AI, stampanti AI, proiettori AI...

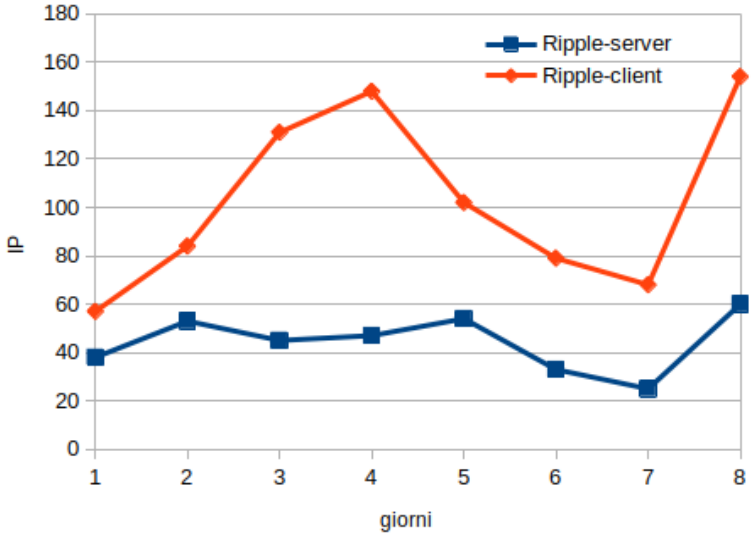


In un giorno qualunque.. mining o cryptojacking?









Progetti per il futuro?

- Reagire agli incidenti gravi (DDoS e cose brutte), basta?
- Aumentare il livello di sicurezza, o almeno ridurre il livello di rumore.
- Scalare con le minacce:
  - Coinvolgimento attivo degli utenti
  - Sfruttare le caratteristiche uniche che abbiamo come rete di istruzione e ricerca

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Grazie a tutti!

LEONARDO LANZI

Roma, 8 – 10 ottobre 2019

Workshop GARR – NET MAKERS