Domain Name System (DNS) e Security Extensions (DNSSEC): alcuni aspetti di Privacy e Sicurezza - Parte 1

Author : Andrea Pasquinucci

Date : 13 Maggio 2019

Il Domain Name System, d'ora in avanti DNS, è uno dei protocolli fondamentali alla base di Internet. Il suo scopo è risolvere un “nome” facilmente ricordabile e gestibile da una persona, in un “indirizzo IP” associato alla risorsa informatica da raggiungere. Oltre a permettere una facile e semplice gestione da parte delle persone, la separazione tra “nome” e “indirizzo IP” permette anche di risolvere un nome in più indirizzi - ad esempio a seconda della geolocalizzazione delle risorse - e di modificare gli indirizzi in maniera trasparente agli utenti.

Tutti noi utilizziamo la risoluzione dei nomi tramite il DNS ogni qualvolta accediamo a risorse in internet, ed anche in reti private aziendali. Noi tutti ci *fidiamo* che la risoluzione ci fornisca gli indirizzi corretti delle risorse a cui ci vogliamo connettere e non, ad esempio, di qualche sito di phishing.

Recentemente vari aspetti dell'integrità, disponibilità e riservatezza del DNS sono stati messi a dura prova (vedi Rif. 1). In questo articolo verrà fatta una sintetica introduzione al DNS per poi brevemente trattare di alcuni aspetti di sicurezza inclusa l'introduzione tuttora in corso del DNSSEC e alcuni approcci alternativi.

DNS, DoH e Privacy

Prima di una breve introduzione su come funziona la risoluzione DNS, vogliamo però accennare a un argomento non tecnico ma di sicuro interesse per la privacy dell'accesso a Internet di tutti noi. Tra i recenti protocolli proposti per migliorare sia la sicurezza che l'utilizzo del DNS, ve n'è uno chiamato “DNS queries over HTTPS” (DoH, RFC 8484) che semplicemente permette di trasportare il protocollo DNS all'interno di un canale cifrato HTTPS, come per qualunque altra navigazione sicura in Internet. È stata proposta un'applicazione di questo protocollo direttamente all'interno dei browser, quali Firefox, Chrome, IE ecc., tale che il browser richieda la risoluzione dei nomi a un servizio fornito ad esempio dal produttore del Browser stesso. Questo permetterebbe al fornitore del Browser di impedire accessi a siti compromessi o di phishing, ed in generale a materiale pericoloso, filtrando la risoluzione dei relativi nomi o

sostituendo l'indirizzo IP malevolo con uno benevolo, oltre che a potenzialmente migliorare l'efficienza e velocità delle risoluzioni sfruttando cache ottimizzate.

D'altra parte, il fornitore del Browser verrebbe a conoscenza della navigazione completa di ognuno di noi visto che per accedere a qualunque pagina web la prima operazione è quella di tradurre il nome del sito in un indirizzo IP. Come vederemo, oggi la risoluzione è un'attività distribuita e molteplici entità gestiscono informazioni diverse rendendo più difficile raccogliere la storia della navigazione di ognuno di noi se non nel Browser stesso o nelle cache DNS locali.

La discussione su questo argomento è in corso (si veda ad esempio Rif. 2) ma sicuramente devono essere valutati i possibili impatti sulla privacy della navigazione Web e le possibilità di censura centralizzata per l'adozione del protocollo DoH direttamente all'interno dei browser.

La risoluzione DNS

Il protocollo DNS è basato su tavole di traduzione tra i “nomi” dei servizi internet e i loro “indirizzi IP”, a cui sono associati numerosi parametri utili alla gestione del protocollo stesso[1]. Queste tavole sono gestite dai server DNS organizzati in una struttura gerarchica ad albero. All'origine (cima) dell'albero vi sono tredici “root server DNS” (vedi fig. 1) che forniscono tutti le stesse identiche informazioni e sono configurati in modo da garantire l'autenticità e l'integrità delle informazioni (ritorneremo più avanti su questo punto), e la disponibilità del servizio praticamente in ogni condizione e sotto qualsiasi attacco difendibile con le tecnologie odierne.

Gli altri server DNS sono organizzati in maniera gerarchica ad albero sotto i 13 root server. Un semplice esempio è la maniera più rapida per descrivere il protocollo. Supponiamo di voler trovare l'indirizzo IP del sito **www.wikipedia.org**: il punto di partenza è un PC sul quale è installata una libreria di risoluzione DNS con la tabella degli indirizzi (fig. 2) dei 13 root server. La prima richiesta viene fatta a un root server, che risponde di non conoscere l'indirizzo IP del sito, ma rimanda al server DNS del dominio “org” (primo ramo dell'albero, Top Level Domain) fornendone gli indirizzi IP. La richiesta viene quindi fatta ad un server DNS del dominio “org” che a sua volta risponde di non conoscere l'indirizzo IP del sito, ma rimanda al server DNS del dominio “wikipedia.org” (secondo ramo dell'albero, 2nd Level Domain) fornendone gli indirizzi IP. La richiesta viene infine fatta ad un server DNS del dominio “wikipedia.org” che risponde dicendo di essere l'autorità per questo dominio e di conoscere l'indirizzo IP del sito, ovvero gli indirizzi ipv4 91.198.174.192 e ipv6 2620:0:862:ed1a::1. Il processo appena descritto è svolto da un servizio chiamato “iterative DNS resolver” (fig. 3).

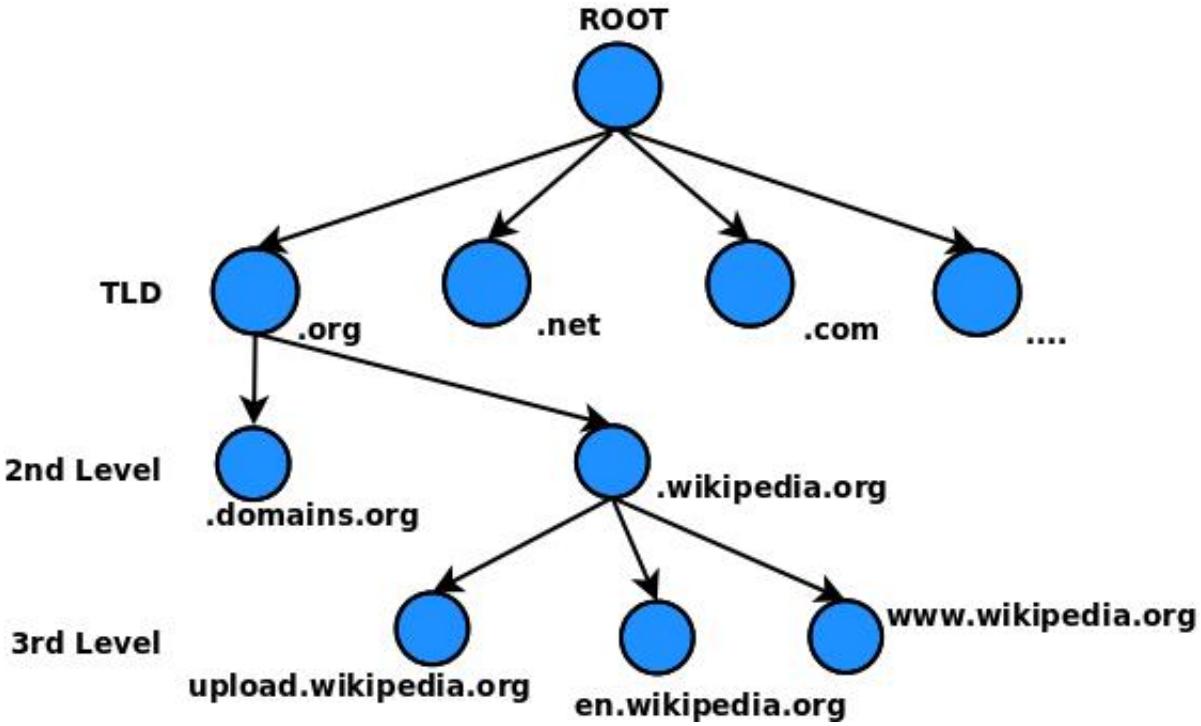

Fig. 1 Gerarchia ad albero dei server e nomi DNS

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:     January 07, 2019
;       related version of root zone:     2019010702
;
; FORMERLY NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     199.9.14.201
B.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:200::b
;
; FORMERLY C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
C.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2::c
;
[...]
```

Fig. 2 Indirizzi ipv4 e ipv6 dei primi tre root server DNS

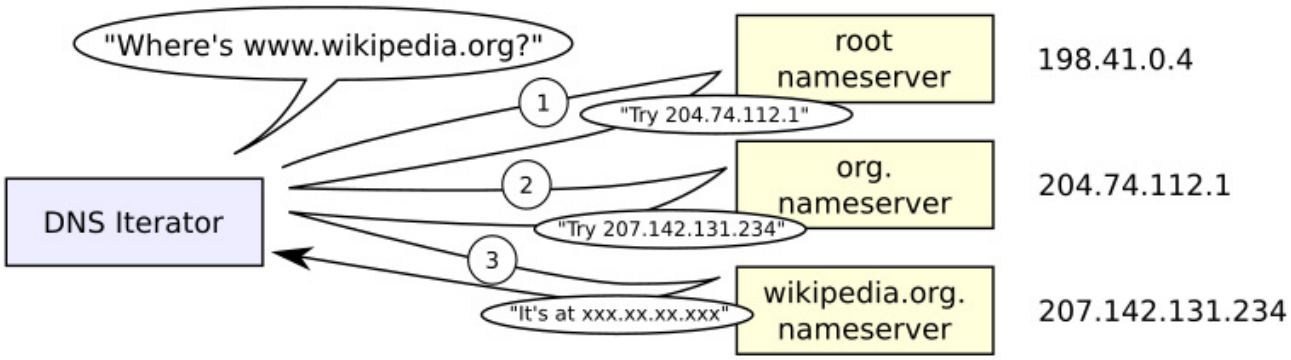

Fig. 3 Processo di risoluzione iterativa da nomi agli indirizzi IP [wikipedia]

La Cache DNS

Il processo di risoluzione DNS tramite resolver iterativi non è efficiente, in quanto richiede per ogni risoluzione di un nome di ripartire dai server root. In pratica si utilizza un **processo inverso** basato sull'uso di cache e che naviga l'albero di risoluzione al contrario, dall'estremo verso l'origine. Quindi, parallelamente ai server DNS d'autorità vi è un albero di server DNS interconnesso a quello principale. Questi sono chiamati tipicamente “server DNS ricorsivi”. Il processo di risoluzione dei nomi in indirizzi IP utilizzato in ogni istante dai nostri dispositivi informatici è, ad alto livello, il seguente (vedi Fig. 4).

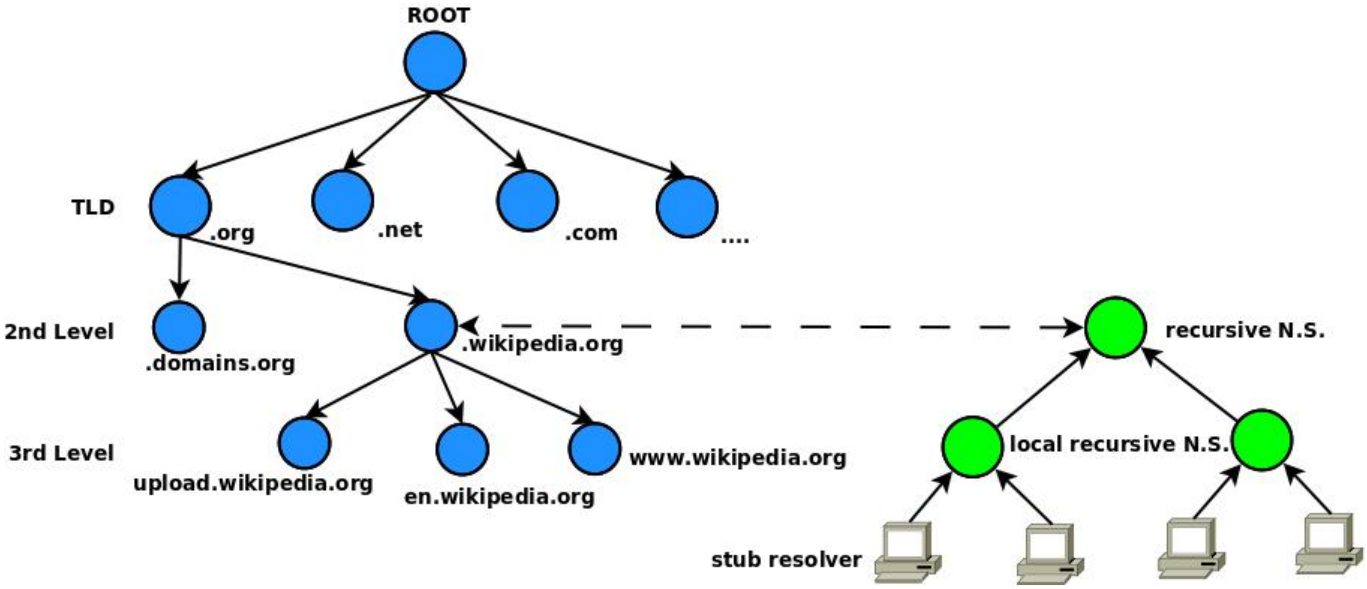

Fig. 4 Risoluzione ricorsiva di www.wikipedia.org: il client (stub resolver) ed il server DNS locale non hanno in cache dati del dominio wikipedia.org, mentre il server DNS ricorsivo ha in cache gli indirizzi IP dei server DNS del dominio wikipedia.org.

Innanzitutto, quando a un client arriva la risoluzione di un nome nei suoi indirizzi IP, tra i parametri ricevuti vi è anche il “Time To Live” (TTL), ovvero il tempo, da alcuni secondi a qualche giorno, di validità della risoluzione. Ogni sistema operativo ha un servizio di risoluzione DNS utilizzato da tutte le applicazioni in esecuzione sul sistema, che memorizza la risoluzione del nome in una cache locale per il tempo indicato dal TTL.

Nel caso in cui la risoluzione non sia nella cache locale, il servizio DNS sul client non chiede ai root server DNS ma a un “nameserver” locale, ad esempio aziendale o del proprio ISP, il cui indirizzo IP è tipicamente fornito al momento di configurazione dell'interfaccia di rete IP, ad esempio tramite il protocollo DHCP. In questa modalità, il servizio di risoluzione DNS del client è

chiamato “Stub resolver”.

Il nameserver locale è tipicamente un server DNS ricorsivo, sempre con cache, a cui si rivolgono molti client, ad esempio tutti i dispositivi di un'azienda o tutti i clienti di un ISP. Nel caso il nameserver locale non abbia in cache la risoluzione di un nome, può rivolgersi a sua volta a un altro server DNS ricorsivo, ad esempio del Carrier che fornisce la connettività internet nazionale e internazionale. In questo modo si forma una **catena ad albero di servizi di risoluzione DNS** con server la cui cache è sempre più grande, visto che forniscono un numero maggiore di clienti. Nel caso l'ultimo server DNS ricorsivo di questa catena non abbia la risoluzione in cache, procede con il processo iterativo descritto precedentemente partendo dai root server o dai server DNS d'autorità di cui già conosce gli indirizzi IP.

Si noti che per bilanciare il carico di lavoro e garantire la disponibilità del servizio, i resolver ricorsivi e iterativi utilizzati sono sempre molteplici e condivisi. Ad eccezione dei resolver locali, nessun resolver sa esattamente chi richieda la risoluzione di un nome sia perché può essere fornita via cache locale o distribuita, sia perché può essere un altro resolver a chiederla. Anche se non perfetto, questo processo garantisce un certo livello di privacy, ed in alcuni casi anche anonimato, per l'accesso alle risorse in Internet tramite la risoluzione dei nomi in indirizzi.

Estensioni del protocollo DNS ed altri dati

Il protocollo DNS originale prevedeva lo scambio di dati via UDP con messaggi di dimensione massima di 512 byte. Ben presto però si è compreso che il DNS può essere anche utilizzato come libreria centrale di altre informazioni relative ai sistemi in rete, oltre alla necessità di estensioni del protocollo stesso principalmente per motivi di sicurezza, come sarà discusso in seguito. Il protocollo DNS è stato pertanto esteso (EDNS) in maniera retro-compatibile, sia permettendo pacchetti UDP sino a 4096 byte, sia introducendo la possibilità di scambiare dati via TCP.

È già stato indicato come un record DNS contiene il nome da tradurre, gli indirizzi IP che gli corrispondono, i nomi ed indirizzi IP dei server DNS d'autorità per il dominio (o zona), ed altri parametri quali il TTL. È anche possibile indicare quali siano nome e indirizzo del server di posta elettronica che gestisce la posta per il dominio indicato (record MX), oppure creare blacklist di indirizzi IP (ad esempio: se l'indirizzo IP 1.2.3.4 è in una blacklist gestita dal servizio “example blacklist”, la query DNS 4.3.2.1.blacklist.example ritorna 127.0.0.1, altrimenti ritorna 127.0.0.2, ove blacklist.example è un server DNS appositamente configurato). I record DNS possono anche essere utilizzati per distribuire informazioni di sicurezza associate a nomi e indirizzi IP quali i Certificati Crittografici (CERT records, RFC 4398), le fingerprint SSH (SSHFP, RFC 4255), le chiavi pubbliche IPSec (IPSECKEY, RFC 4025), le Trust Anchor TLS (TLSA, RFC 6698) eccetera.

Minacce e debolezze del protocollo DNS

Il protocollo DNS fu inizialmente proposto nel novembre del 1983 (RFC 882 e 883) e non prevedeva particolari misure di sicurezza se non una iniziale attenzione alla scalabilità e

disponibilità del servizio. È indubbio che il **disegno gerarchico e decentrato** evolutosi negli anni abbia raggiunto gli obiettivi di garantire un servizio *scalabile* alle dimensioni di Internet di oggi, e *disponibile* in quanto ogni accesso a risorse in Internet richiede una preventiva risoluzione DNS. Più che la scalabilità, quello che preoccupa oggi i fornitori di servizi DNS sono gli attacchi di Distributed Denial of Service (DDoS) che possono bloccare temporaneamente l'erogazione del servizio e quindi l'accesso ad un gruppo anche esteso di risorse in Internet (si veda ad esempio Rif. 3).

Sino alle più recenti evoluzioni, il protocollo DNS ha però fornito ben poche funzionalità a garanzia di:

- autenticità dei dati;
- integrità dei dati;
- confidenzialità dei dati;
- privacy, ad esempio rispetto al tracciamento della navigazione in Internet.

Le minacce all'autenticità e integrità dei dati sono quelle ritenute più critiche e si spera che le misure che saranno descritte nella seconda parte di questo articolo siano in grado di mitigarle efficacemente.

Le **principali minacce** vanno usualmente sotto i nomi di “DNS spoofing” e “cache poisoning”. Questi attacchi si basano sul fatto che le relazioni nell'albero dei server DNS dipendono da un rapporto di fiducia (*trust*) tra i server stessi. Infatti il protocollo DNS non prevede un processo di autenticazione delle sorgenti se non il fatto di ottenere in maniera gerarchica gli indirizzi IP dei server DNS a partire dai server DNS root. Ma le comunicazioni tra server non sono né autenticate, né protette rispetto alla confidenzialità e integrità dei dati trasmessi. In mancanza di un processo forte di autenticazione tra i server DNS è possibile, ad esempio, sia introdurre dei server DNS maligni e dirottare le richieste verso questi (DNS spoofing), sia intercettare le richieste di risoluzione di un server DNS ricorsivo verso un server d'autorità od un altro server ricorsivo, e rispondere con dati modificati in modo da “avvelenarne” la cache DNS (cache poisoning). Questi attacchi sono possibili grazie al fatto che le richieste e le risposte standard delle query DNS sono singoli pacchetti UDP, che non richiedono la creazione di una sessione di comunicazione e che sono spesso facilmente modificabili in transito.[1]

Come garantire l'autenticità e l'integrità dei dati a partire dai server DNS root sino agli stub resolver sui nostri PC (vedi Fig. 4) anche in presenza di attacchi malevoli sulle reti pubbliche?

Prima di affrontare questo punto, è conveniente considerare gli **aspetti di confidenzialità e privacy** relativi al servizio DNS. Prima di tutto, tutti i dati gestiti dal DNS sono pubblici, per cui non vi è alcuna esigenza di proteggere la confidenzialità dei dati stessi. La confidenzialità invece è una proprietà molto utile per poter garantire la privacy degli utenti ed è solo in questo contesto che viene di solito considerata nell'ambito del DNS.

Si consideri infatti il caso di un utente che naviga in Internet con il proprio dispositivo (smartphone, tablet, PC ecc.). Per fare questo, il dispositivo si collega al nameserver locale del fornitore di accesso a Internet. Si supponga inoltre che qualcuno possa osservare il traffico del

dispositivo verso il nameserver locale. Visto che tutti i pacchetti DNS scambiati non sono di solito cifrati, questo attaccante è in grado di avere la lista di tutte le risoluzioni di nomi richieste dal client, quindi di tutti i siti e servizi visitati dal client con la data esatta della prima visita.[2] Se invece la connessione tra il client e il nameserver locale fosse cifrata, l'attaccante non potrebbe ricavare alcuna informazione sulla navigazione dell'utente dalle sue richieste di risoluzione DNS.

L'attaccante potrebbe allora osservare il traffico tra il nameserver locale e gli altri server DNS da questo contattati. In questo caso però la quantità di informazioni che riuscirebbe a estrarre sarebbe molto limitata, soprattutto in caso di server DNS che gestiscono molti utenti, perché non è facile mettere in diretta relazione le richieste del nameserver locale con quelle dei suoi client, e soprattutto molte richieste dei client trovano risposta direttamente nella cache del nameserver locale senza necessità di una ulteriore richiesta ad altro server DNS.

Si noti infine che, per la privacy degli utenti, è anche importante come sia lo stub resolver sul client stesso sia il nameserver locale traccino le richieste di risoluzione. Infatti un file di log che contiene tutti i dati di richieste di risoluzione DNS di un client permette di ricostruire la navigazione - almeno il primo accesso - del client stesso. Recentemente, alcuni servizi pubblici di risoluzione DNS hanno cominciato a dare informazioni sulla loro politiche di gestione dei log dei server DNS: quali dati vengono tracciati, quando vengono cancellati, chi vi può accedere e per quali scopi (anche a seguito della normativa GDPR). Prima di scegliere un servizio DNS pubblico è quindi meglio informarsi su come questo tratti i dati di log dei propri server DNS.

Chi ha **particolari esigenze di privacy** può quindi valutare se procedere come segue:

- scegliere un servizio di risoluzione DNS (ovvero “nameserver locale”) molto grande;
- verificare le politiche di gestione dei log dei server DNS del fornitore;
- connettersi al server DNS con canale cifrato;
- assicurarsi che il proprio stub resolver non tracci le richieste di risoluzione DNS.

Al termine della seconda parte di questo articolo daremo alcune indicazioni pratiche di come sia possibile implementare questo approccio.

Nella seconda parte di questo articolo verrà considerato il protocollo DNSSEC e come questo affronti buona parte delle debolezze del protocollo DNS.

Note

[1] In questo articolo non viene discussa la risoluzione DNS inversa, ovvero da indirizzo IP a nome.

[2] Questo richiede ovviamente di poter accedere alla rete di comunicazione ove transitano i pacchetti UDP delle risoluzioni DNS.

[3] Le visite successive alla prima in tempi ravvicinati, e comunque entro il TTL, non sono visibili in quanto in dati sono in cache sul dispositivo utente e quindi non vengono richiesti nuovamente al nameserver locale.

Riferimenti bibliografici

Rif. 1: Si veda ad esempio l'avviso CERT “Alert (AA19-024A): DNS Infrastructure Hijacking Campaign” https://www.us-cert.gov/ncas/alerts/AA19-024A , e Ars Technica “The wave of domain hijackings besetting the Internet is worse than we thought”, https://arstechnica.com/information-technology/2019/04/state-sponsored-domain-hijacking-op-targets-40-organizations-in-13-countries/.

Rif. 2: L'approccio di Mozilla Firefox e una delle tante discussioni sull'implementazione di DoH direttamente nei browser è disponibile a questo indirizzo: https://mailarchive.ietf.org/arch/browse/doh/?gbt=1&index=HPTOUtziIYe_PFuawExeetkSjVg.

Rif. 3: famoso è l'attacco DDOS a Dyn il 21 ottobre 2016, si veda ad esempio https://en.wikipedia.org/wiki/2016_Dyn_cyberattack.

Articolo a cura di **Andrea Pasquinucci**