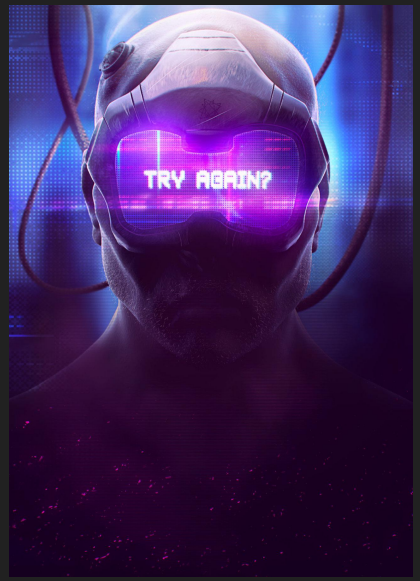
Stato Sicurezza Siti Startup Italiane



Luca Del Vecchio

Certificato eJPT, CPEH e Cysa+.

Cyber Security Consultant e Penetration Tester.

Da sempre appassionato di Hacking, Startup, Web3.0, Tecnologia, Spazio e Cyberpunk.

PERCHÉ

Da appassionato di sicurezza informatica e di startup tecnologiche ho voluto dare un punto di vista tecnico sullo stato della sicurezza dei siti delle Startup attualmente registrate (agosto 2022) al Registro delle Imprese Italiane (come Startup Innovative).

ARGOMENTI

Sono stati analizzati dati pubblici e dati estrapolati entrando in contatto diretto (chiamate http) con i siti analizzati. Non sono state utilizzate tecniche invasive o attive e i dati possono soffrire delle condizioni delle reti e temporanee irraggiungibilità degli host.

L'analisi ha riguardato i seguenti elementi:

- Status code di risposta degli host (200 OK, errori 400 e 500)
- Record DNS per determinare provider e paese ospitante
- Versione dei certificati di sicurezza SSL/TLS
- Http Security Headers configurati

ANALISI - Acquisizione e Normalizzazione Dati

Il primo step è stato quello di acquisire i dati dal registro delle imprese italiane, tramite form dedicato è possibile ottenere dati relativi alle Startup registrate in formato csv contenente 14747 record.

Dei dati ottenuti viene preso in considerazione il campo “Sito Internet”, parecchi record presentano inserimenti errati. La conseguente attività è stata la normalizzazione degli indirizzi URL, normalizzazione che ha visto l’analisi di 11580 record (i restanti non riportavano un Sito Internet).

ANALISI - Raggiungibilità Siti

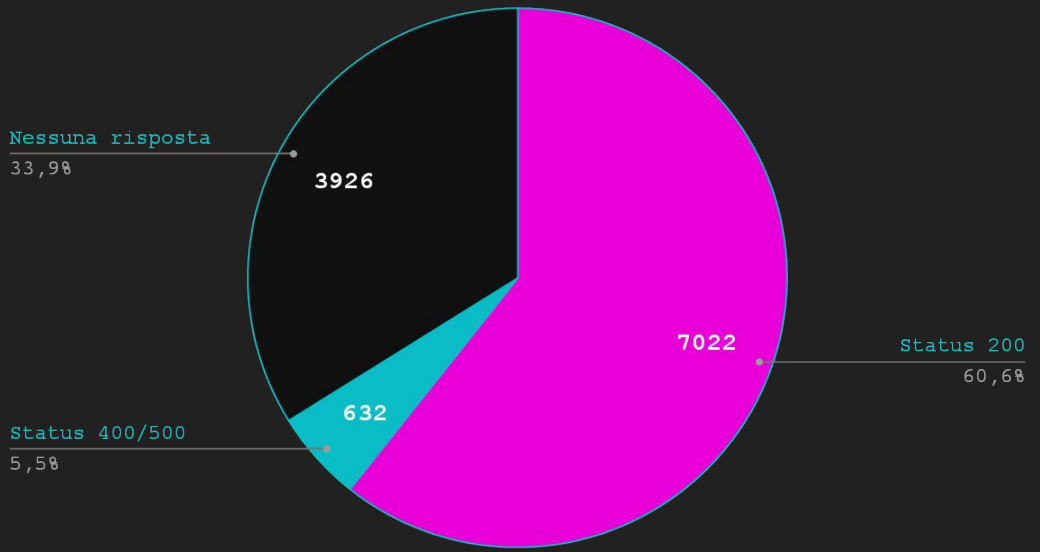
La prima analisi tecnica ha riguardato la reale presenza e raggiungibilità dei siti su internet, quindi sono state effettuate chiamate http, sono stati divisi nell'analisi i siti che rispondevano con lo status code 200 OK (quindi raggiungibili e fruibili) e quelli che hanno risposto con uno status code di errore di classe 400 o 500.

Tutte le successive analisi sono state eseguite solamente sui siti che hanno risposto con uno status code 200 OK.

ANALISI - Status Code

11580 URL analizzate:

- Status Code 200 OK → 7022 (60,6%)
- Status Code 400/500 → 632 (5,5%)
- Nessuna risposta → 3926 (33,9%)



ANALISI - Domain Name Service

Tramite l'analisi dei DNS (Domain Name Service) è stato possibile estrapolare i dati dei provider che forniscono servizi di hosting (o CDN e/o reverse proxy) alle startup, è stato analizzato solo il risultato delle query per il record di tipo A (indirizzo IPv4).

Inoltre è possibile ottenere informazioni sulla località da cui i servizi vengono erogati, risulta che meno della metà delle startup italiane, 47.3% ha un sito hostato in italia, il 76.76% del totale ha un hosting in regione europea, il 18.53% in regioni extraeuropee e il restante non è stato possibile definirlo.

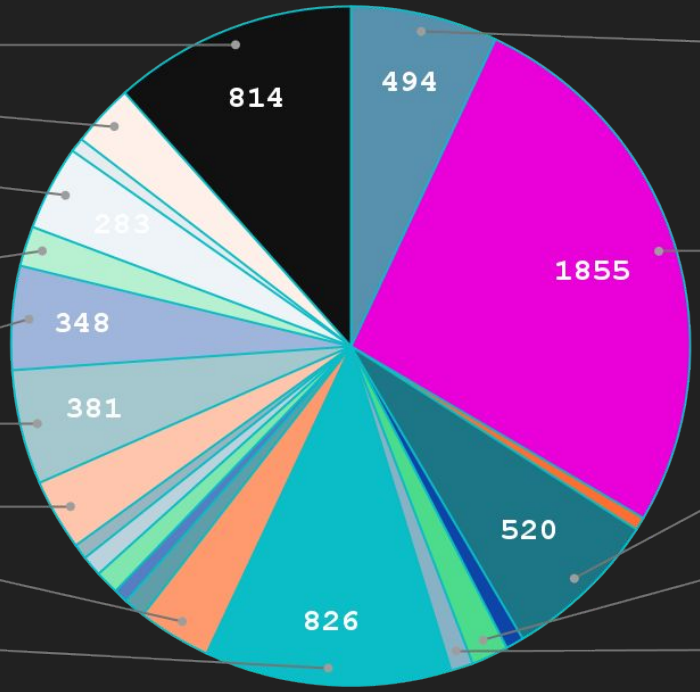
ANALISI - Distribuzione Provider

7022 DNS analizzati:

- Aruba S.p.a. → 1855 (26,42%)
- Google → 826 (11,76%)
- Cloudflare → 520 (7,41%)
- Amazon → 494 (7,04%)
- OVH SAS → 381 (5,43%)
- Register S.p.A. → 348 (4,96%)
- Server Plan S.r.l. → 283 (4,03%)
- Hetzner Online GmbH → 246 (3,50%)
- Netsons s.r.l. → 239 (3,40%)
- Wix.com Ltd. → 208 (2,96%)
- Seeweb s.r.l. → 135 (1,92%)
- Digitalocean → 127 (1,81%)
- Ionos SE → 80 (1,14%)
- Fastly → 74 (1,05%)
- Host Europe GmbH → 73 (1,04%)
- Keliweb S.R.L → 69 (0,98%)
- Contabo GmbH → 60 (0,85%)
- Microsoft → 52 (0,74%)
- Weebly → 48 (0,68%)
- Automattic → 45 (0,64%)
- Host SpA → 45 (0,64%)
- Altri → 814 (11,59%)

In “Altri” vengono conteggiati 215 provider diversi

Distribuzione Provider



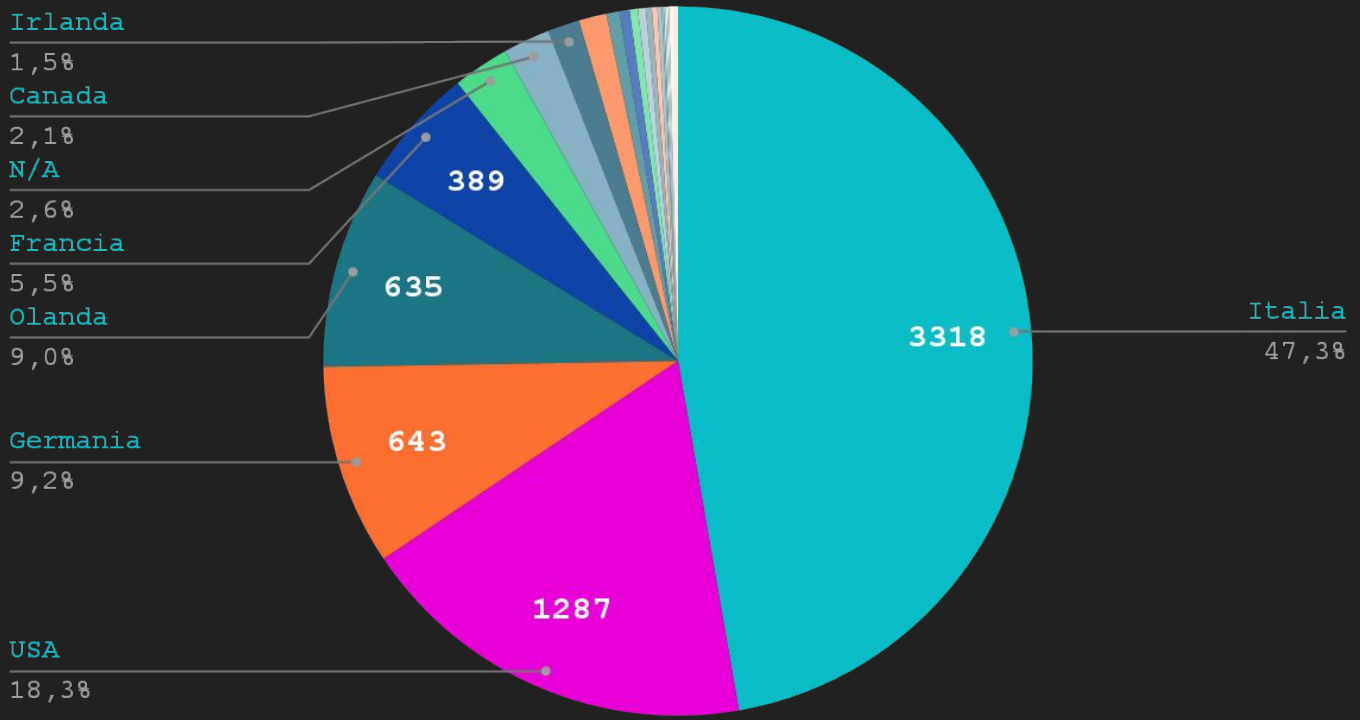
ANALISI - Distribuzione Paesi

7022 DNS analizzati:

- Italia → 3318 (47.3%)
- USA → 1287 (18.3%)
- Germania → 643 (9.2%)
- Olanda → 635 (9.0%)
- Francia → 389 (5.5%)
- N/A → 181 (2.6%)
- Canada → 150 (2.1%)
- Irlanda → 102 (1.5%)
- Regno Unito → 89 (1.3%)
- Finlandia → 42 (0.6%)
- Danimarca → 32 (0.5%)
- Spagna → 27 (0.4%)
- Svizzera → 25 (0.4%)
- Belgio → 19 (0.3%)
- Portogallo → 18 (0.3%)
- Repubblica Ceca → 14 (0.2%)
- Russia → 6 (0.1%)
- Spagna → 6 (0.1%)
- Australia → 5 (0.1%)
- Lituania → 5 (0.1%)
- Altri → 29 (0.4%)

In “Altri” vengono conteggiati 14 paesi

Distribuzione Geografica



ANALISI - Versioni Certificati SSL/TLS

L'analisi ha riguardato i certificati SSL/TLS, questi certificati vengono usati per creare una connessione cifrata e sicura (https) tra un client (browser) e un server.

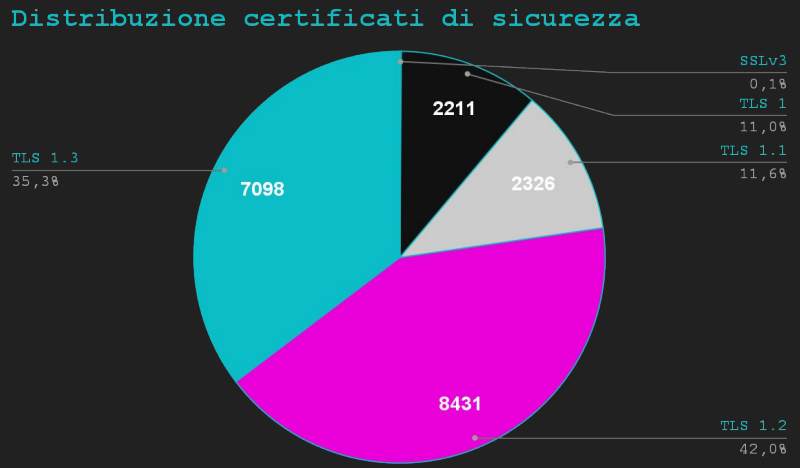
È stata testata anche la possibilità di effettuare connessioni senza certificato, quindi semplicemente in http, risulta possibile effettuare connessioni non sicure con 335 siti, cioè il 4.7% dei siti testati.

Attualmente le versioni correnti considerate sicure sono TLS 1.2 e TLS 1.3, le precedenti versioni di TLS sono da intendersi deprecati (se presenti sono da considerare come vulnerabilità), i certificati SSL non sono più in uso da anni in quanto afflitti da diverse vulnerabilità, sono stati rimpiazzati dai certificati TLS.

ANALISI - Versioni Certificati SSL/TLS

Distribuzione versioni dei certificati di sicurezza web, un server potrebbe offrire più versioni per il certificato, quindi i dati non saranno coerenti con il totale dei siti analizzati. Certificati analizzati 20096:

- SSLv2 → 3 (<0.1%)
- SSLv3 → 27 (0.1%)
- TLS 1 → 2211 (11.0%)
- TLS 1.1 → 2326 (11.6%)
- TLS 1.2 → 8431 (42.0%)
- TLS 1.3 → 7098 (35.3%)



ANALISI - Security Headers

Analizzando le risposte HTTP è stato possibile estrapolare i dati relativi ai Security Headers.

Gli HTTP Security Headers sono direttive che vengono inviate tramite Headers di risposta dal server al client, queste direttive servono a limitare e gestire il comportamento del client nei confronti del server e delle risorse che gli vengono inviate.

Gli headers presi in analisi sono: X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security, Content-Security-Policy, X-XSS-Protection.

ANALISI - Security Headers

Sono state analizzate le risposte dei 7022 siti presi in esame per l'analisi. Per tali siti sono configurati i seguenti headers di sicurezza:

- X-Frame-Options → 692 (9.85%)
  L'intestazione X-Frame-Options indica al browser che il sito non può essere incorporato in un altro tramite iframe, embed o object.
- X-Content-Type-Options → 1610 (22.92%)
  Questa intestazione indica al browser di utilizzare fedelmente il Type Mime presente nell'header Content-Type e non gli è permesso di cambiarlo arbitrariamente.

ANALISI - Security Headers

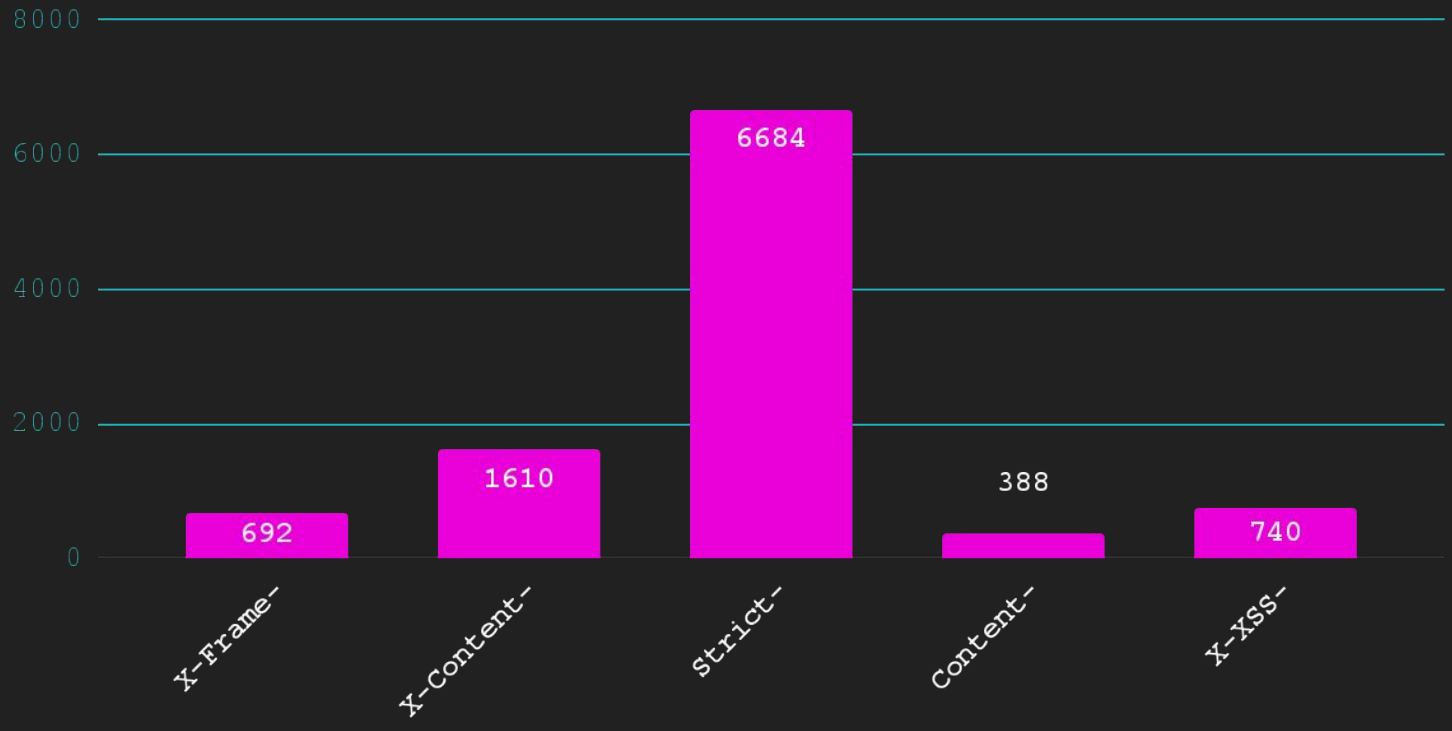
- Strict-Transport-Security → 6684 (95.18%)

  Spesso scritta in forma abbreviata HSTS, indica al browser che ogni futura connessione deve essere eseguita in HTTPS, nel caso la connessione sia in HTTP questa verrà automaticamente convertita in HTTPS.
- Content-Security-Policy → 388 (5.52%)

  Limita il browser a caricare risorse solamente dalle origini e dagli endpoint indicati dall'header.
- X-XSS-Protection → 740 (10.53%)

  Indica al browser di attivare o disattivare il filtro XSS (filtro utilizzato per limitare gli attacchi di tipo Cross Site Scripting)

Headers di Sicuezza



CONCLUSIONI

I dati mostrano che solo il 78,5% delle startup registrate ha inserito un Sito Internet, inoltre solamente il 60% dei siti è, durante l'analisi, raggiungibile portando così il totale a 7022 Startup ad avere una visibilità e un'esposizione tramite sito web, raggiungendo solo il 47.7% di quelle registrate.

Un altro dato che risulta evidente è quello della posizione geografica, che attesta meno del 50% dei siti in italia.

Dal punto di vista dei provider abbiamo il predominio di Aruba e di Google, scelti sicuramente per praticità di configurazioni e per prezzi concorrenziali.

CONCLUSIONI

Andando sul tecnico, per i certificati si può notare come la maggioranza dei provider e degli hosting supporti TLS 1.2 e TLS 1.3, anche se ancora il 22% dei certificati analizzati utilizza TLS 1 e TLS 1.1 (ormai deprecati e da disattivare), questo permette di negoziare un certificato insicuro anche nei casi in cui sono presenti quelli più recenti. Sono stati individuati 30 certificati che vengono serviti tramite SSL e che andrebbero aggiornati con urgenza.

CONCLUSIONI

Un altro dato rilevante è la forte presenza del Security Header HSTS, sicuramente gestito spesso dai provider in fase di installazione dei certificati TLS.

Gli altri header di sicurezza come X-Content-Type-Options e X-XSS-Protection andrebbero sempre aggiunti alla configurazione hosting.

Per quanto riguarda l'X-Frame-Options e il Content-Security-Policy potrebbero non essere configurati per seguire in maniera aderente quelle che sono le logiche di business e gli elementi necessari per il corretto funzionamento del sito, ma nel caso in cui si hanno delle risorse definite e non sia necessario che il sito o una sua parte di esso debbano essere inclusi in altro, il consiglio è quello di configurarli.

CONCLUSIONI

L'analisi ha interessato un porzione delle realtà presenti e tecnicamente solamente quei siti che rispondevano alle chiamate, ma si evince una scarsa attenzione ai temi relativi la sicurezza web, questo comporta un atteggiamento poco propenso alla sicurezza e alla consapevolezza dei rischi che ogni azienda (piccola o grande) deve affrontare avendo un'esposizione su internet.

Il sito web è spesso il primo vettore che un attaccante utilizza per testare e confrontarsi con i livelli di sicurezza di una Startup che intende attaccare, quindi (incluso alla formazione del personale) deve essere uno degli elementi a cui prestare più attenzione in termini di Sicurezza Informatica.

RIFERIMENTI e RINGRAZIAMENTI

- Registro Imprese Italiane - acquisizione dati
- Drishti - test status code (https://github.com/devanshbatham/Drishti)
- Webchk - test https e http (https://github.com/amgedr/webchk)
- InfoByIp.com (Domain and IP bulk lookup tool) analisi DNS
- Testssl.sh analisi SSL/TLS e Headers di Sicurezza
- Terminale linux per normalizzazioni e grep sui risultati
- MDN Web Docs documentazione varia