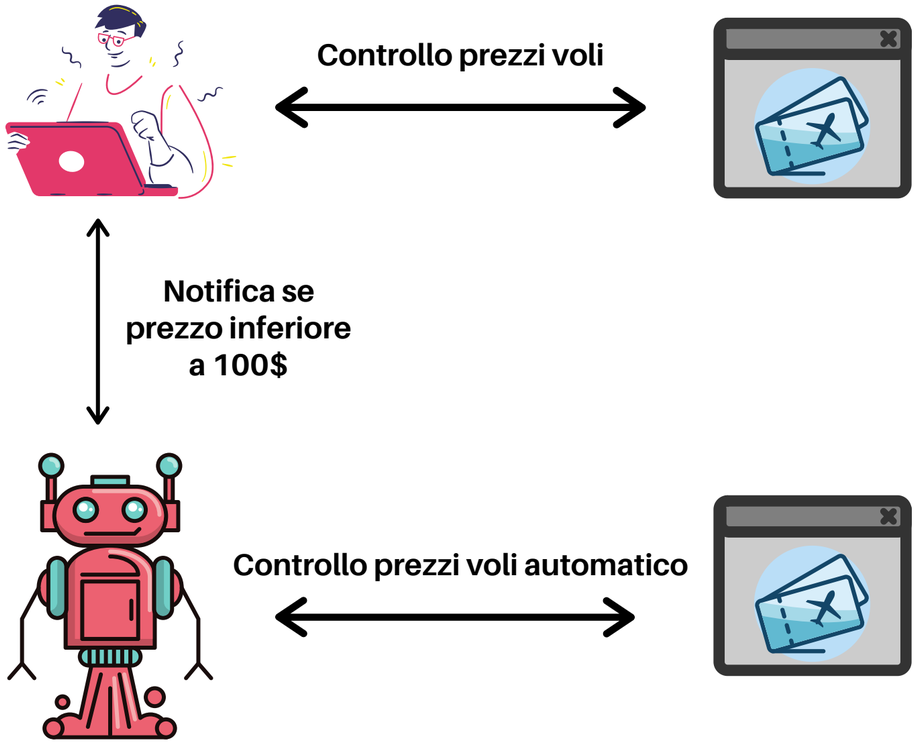
Antibot Systems

A cura di : T. Vendrame

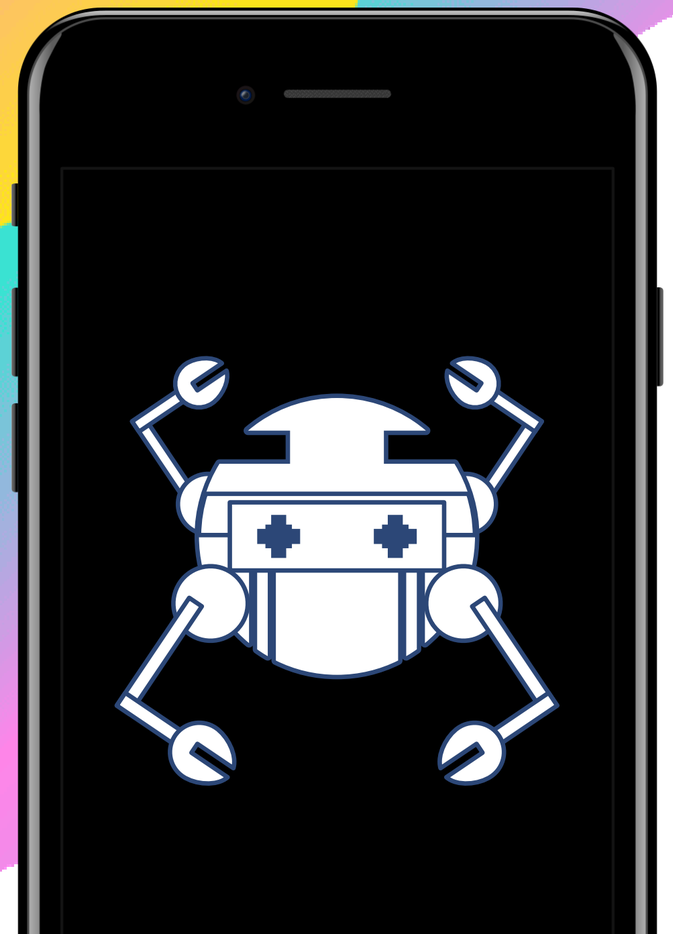
01

Cosa sono i bot?

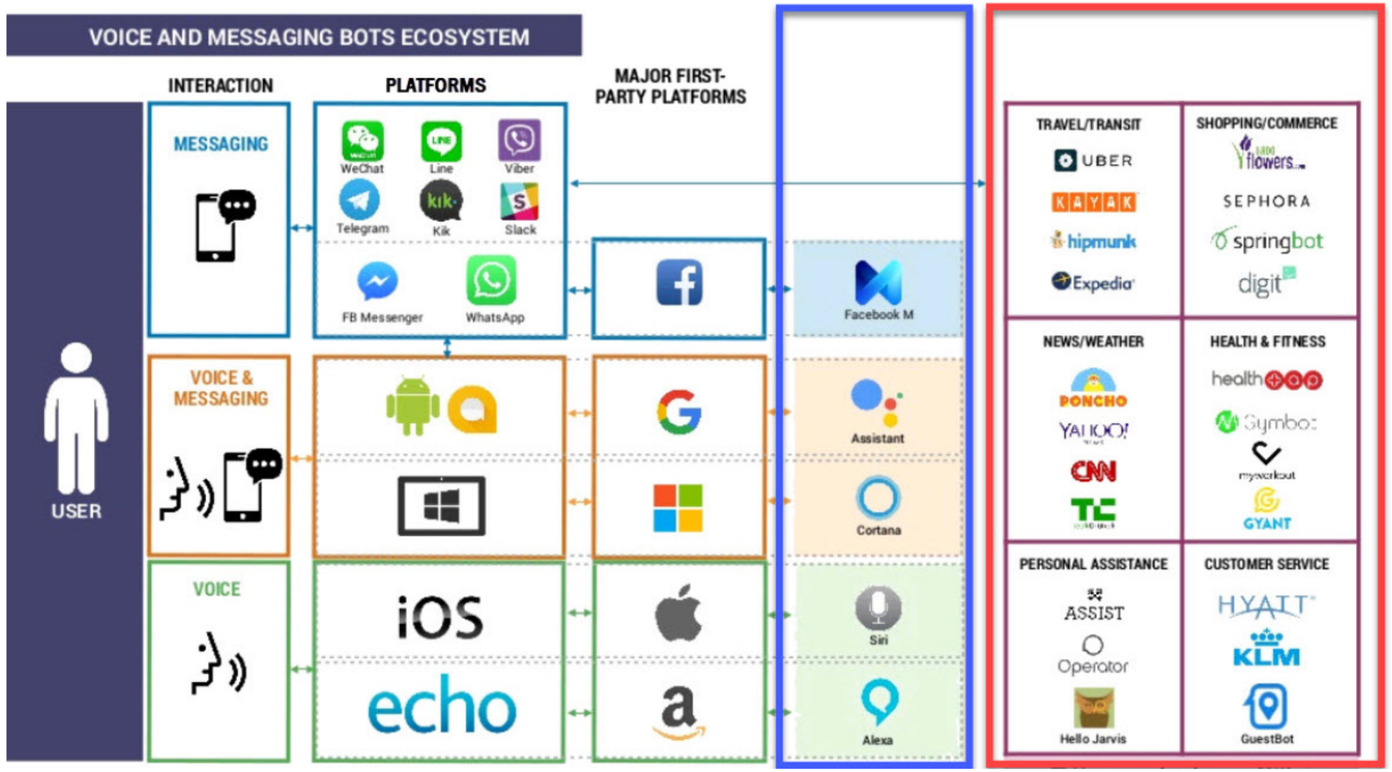
I bot sono programmi informatici che operano in modo indipendente e automatico, in generale questi programmi cercano di simulare alcune azioni che sono normalmente svolte dagli esseri umani.



01 Bot
Tipologie



Generalist bots Specialist bots



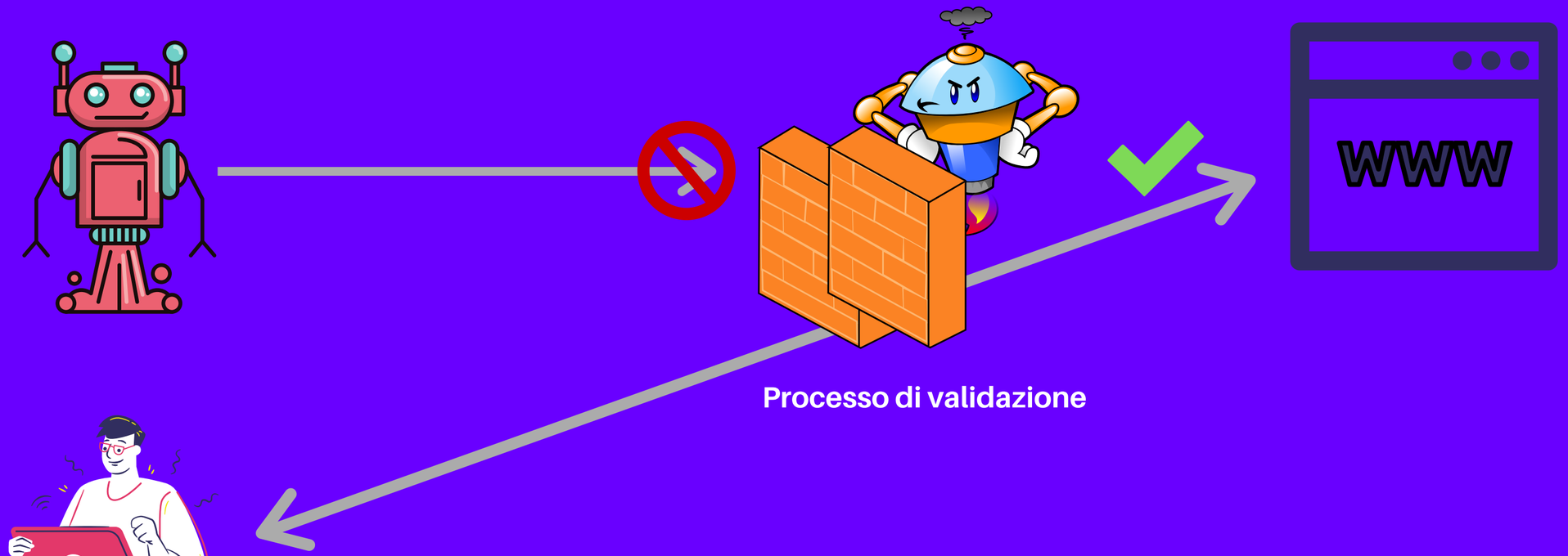
Fonte immagine: http://botnerds.com/types-of-bots/

01 Bot
Ambiti di utilizzo

- Utilizzo white hat
  - Chatbot per assistenza clienti.
- Utilizzo grey hat
  - Instagram bot per aumentare il numero di like/followers.
- Utilizzo black hat
  - Credential stuffing.

02

Anti-bot



Processo di validazione

02 Anti-bot

Qual è il loro ruolo e cosa cercano di tutelare

- Verificano la presenza umana
- Tutelano risorse di vario genere:
  - Credenziali
  - Oggetti fisici acquistabili online
  - Interi siti web (DDoS)

02 Anti-bot
Ambiti di utilizzo

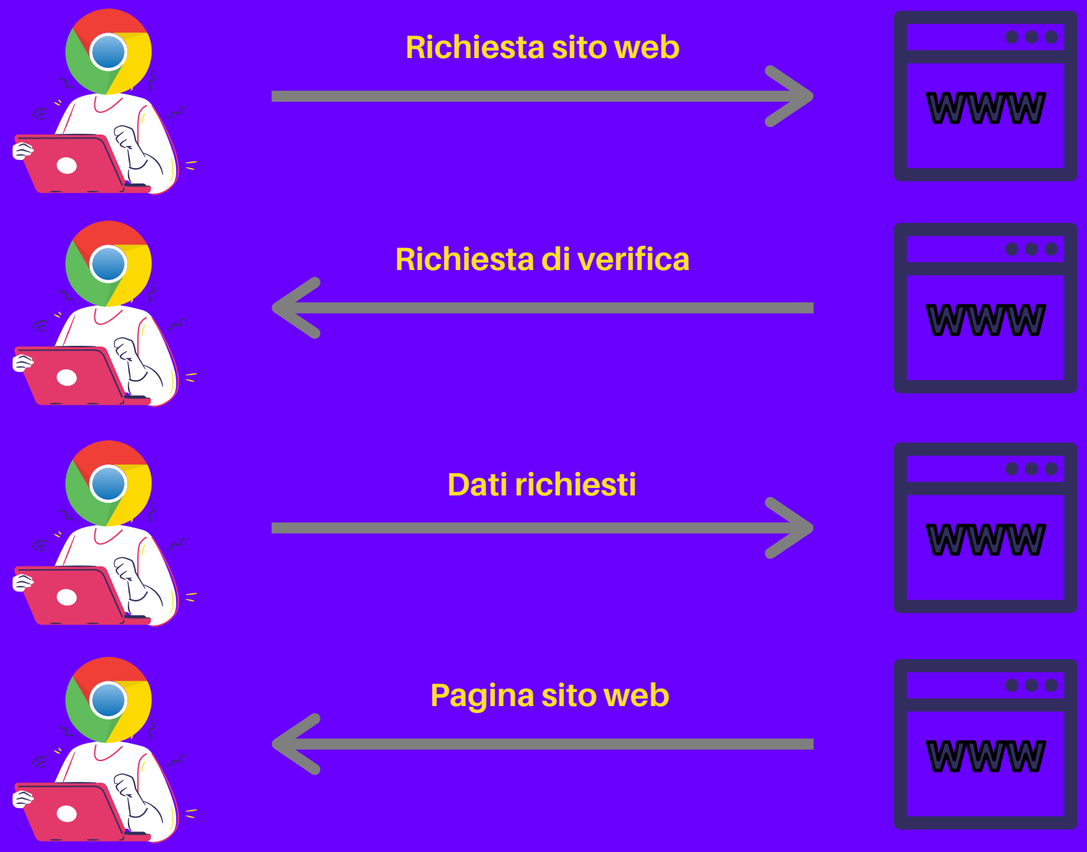
- Social network login.
- Utilizzo del motore di ricerca.
- Prevenzione di crash/down dei sistemi informatici.
- Prevenzione Scraping

02 Anti-bot
Tipologie

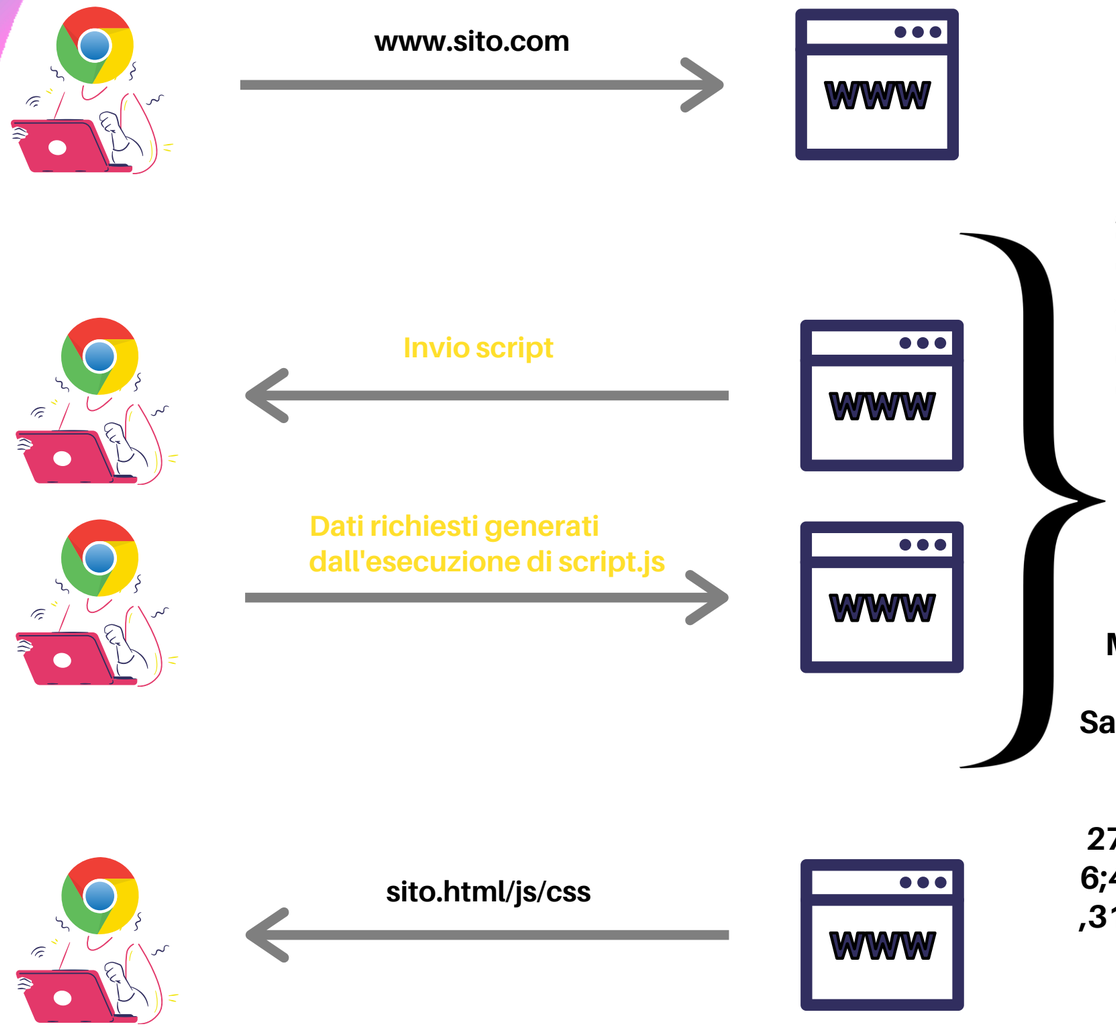
- Sensor data based
- Captcha
- DDoS protections

1 caso di studio.

Bilateral script based antibot systems.



Dati scambiati da Bilateral script based system



script.js

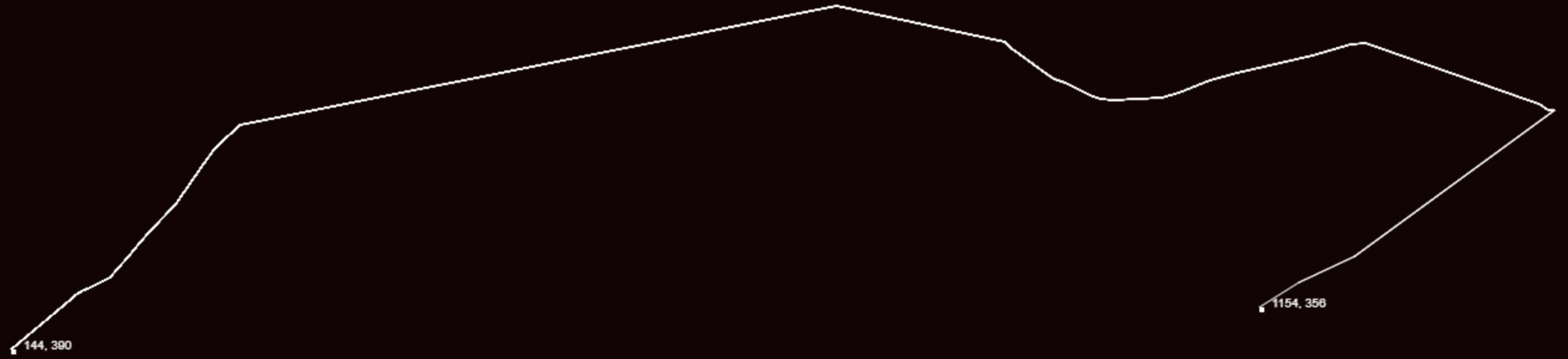
,"\x68\x79\x70\x6f\x74","\x63\x6c\x69\x63\x6b","\x74\x6f\x75\x63\x68\x73\x74\x61\x72\x74",
"\x24\x63\x68\x72\x6f\x6d\x65\x5f\x61\x73\x79\x6e\x63\x53\x63\x72\x69\x70\x74\x49\x6e\x66\x6f",
"\x63\x6c\x65\x61\x72\x43\x61\x63\x68\x65","\x73\x6c\x69\x63\x65","\x61\x63\x63\x65\x6c\x65\x72\
x61\x74\x69\x6f\x6e\x49\x6e\x63\x6c\x75\x64\x69\x6e\x67\x47\x72\x61\x76\x69\x74\x79",
"\x6e\x61\x76\x69\x67\x61\x74\x6f\x72","\x61\x6c\x6c","\x2c\x22\x61\x75\x74\x68\x22\x20\x3a\x20\x22",
"\x67\x65\x74\x5f\x73\x74\x6f\x70\x5f\x73\x69\x67\x6e\x61\x6c\x73","\x74\x6f","\x4d\x65\x6e\x6c\x6f",
"\x70\x61\x63\x74","\x6b\x65\x79\x64\x6f\x77\x6e","\x69\x73\x49\x67\x6e","\x73\x65\x61\x72\x63\x68"

Esempio parziale di risposta

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36,1653,1143,1715,1143,1652,496,1653,0,165,-1,-1,-1,-1,-1,-1,-1,-1,Google Inc. (NVIDIA),ANGLE (NVIDIA, NVIDIA GeForce MX150 Direct3D11 vs_5_0 ps_5_0, D3D11-27.21.14.6589)"0,1,2784,144,390;1,1,2785,193,349;2,1,2786,194,348;3,1,2794,196,346;4,1,2821,203,342;5,1,2821,206,341;6,1,2847,224,332;7,1,2851,230,325;8,1,2857,239,315;9,1,2865,248,304;10,1,2872,256,295;11,1,2893,277,273;12,1,2910,300,240;13,1,2

In particolare tra i dati scambiati questa stringa numerica identifica il movimento del mouse

"0,1,2784,144,390;1,1,2785,193,349;2,1,2786,194,348;3,1,2794,196,346;4,1,2821,203,342;5,1,2821,206,341;6,1,2847,224,332;7,1,2851,230,325;8,1,2857,239,315;9,1,2865,248,304;10,1,2872,256,295;11,1,2893,277,273;12,1,2910,300,240;13,1,2918,308,229;14,1,2923,317,220;15,1,2931,324,214;16,1,2938,329,209;17,1,3927,812,113;18,1,3933,948,142;19,1,3937,953,147;20,1,3941,960,152;21,1,3991,982,168;22,1,3997,988,172;23,1,4001,997,175;24,1,4005,1005,179;25,1,4012,1017,185;26,1,4019,1025,188;27,1,4026,1036,189;28,1,4042,1075,187;29,1,4047,1089,183;30,1,4058,1114,173;31,1,4062,1136,167;32,1,4068,1171,159;33,1,4085,1197,153;34,1,4102,1228,144;35,1,4106,1240,143;36,1,4283,1380,192;37,1,4288,1382,193;38,1,4292,1386,196;39,1,4300,1388,197;40,1,4305,1389,197;41,1,4312,1391,197;42,1,4319,1392,197;43,1,4328,1393,197;44,1,4664,1231,315;45,1,4671,1186,336;46,1,4676,1154,356;"

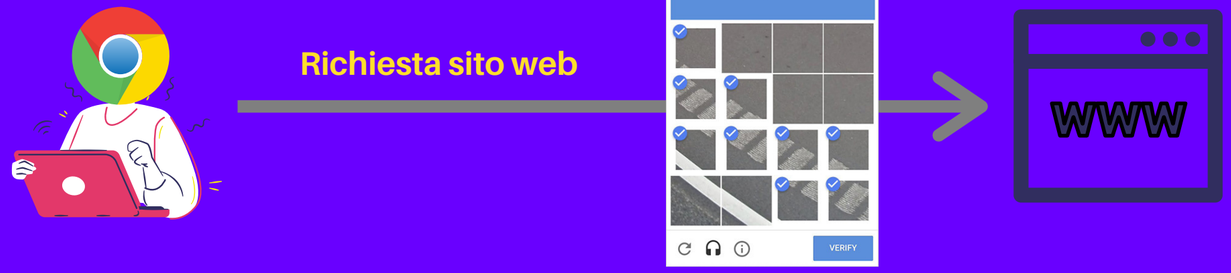


2 caso di studio

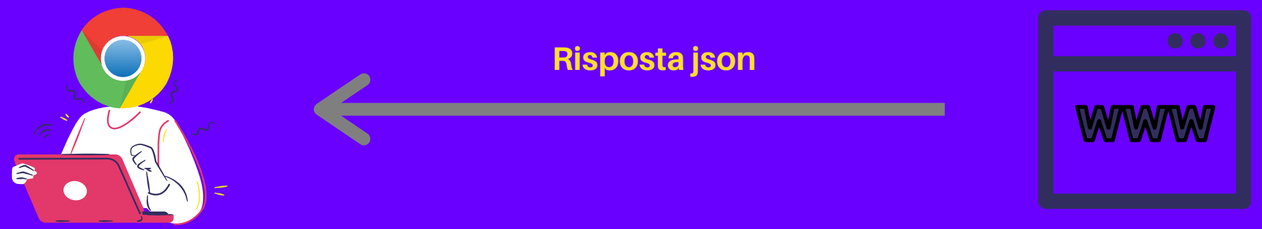
Captcha

03

Analisi dei dati scambiati aptcha




```
{
  "success": true|false,      // whether this request was a valid reCAPTCHA token for your site
  "score": number             // the score for this request (0.0 - 1.0)
  "action": string            // the action name for this request (important to verify)
  "challenge_ts": timestamp,  // timestamp of the challenge load (ISO format yyyy-MM-dd'T'HH:mm:ssZZ)
  "hostname": string,         // the hostname of the site where the reCAPTCHA was solved
  "error-codes": [...]        // optional
}
```



Possibile impatto di uso improprio di un sistema automatico (bot)

Spotify confirms new credential stuffing attack; reset your password immediately

Spotify confirms new credential stuffing attack; reset your password immediately - Incidents - Information Security Newspaper | Hacking News

Information Security Newspaper / Octavio Mares / Feb 5

Considerazioni finali

01

I dati aggregati richiesti dai sistemi antibot possono in generale dare vita a una forma di profiling, anche spaziale del soggetto/macchina che utilizza il servizio.
Per questo motivo il principio di privacy by design deve essere sempre garantito.

02

Si vengono a creare delle white/black list nelle quali gli hash delle macchine (fingerprint) risiedono e comportano un trattamento diverso durante la navigazione.

Grazie per la partecipazione