

Favalli Group

Informazioni passive

Si riescono a reperire informazioni generali dal sito aziendale con le diverse attività aziendali:

- Acquariva
- Il Rivale al lago
- Kuoki
- Honerè
- BBay
- SplendidoBay
- SplendidoYou
- Il Rivale in città

Work in progress per l'anno 2024:

- WineB
- Smeraldo

Azienda che gestisce l'email: GV-net situata a Mantova, referente dell'azienda Luca Lazzeroni.

Servizi gestione ristorazione : Azienda trend service srl situata a castiglione delle stiviere; sistemi operativi utilizzati sono : Tavolinux, Tap menù, Spirario.(<https://trendservizi.com/>)

Dopo attente ricerche le differenti società fanno capo a Global Gest srl, sede Padenghe sul Garda, uffici fisici Desenzano del Garda. Non sono disponibili dati online pubblici riguardo l'azienda come fatturato ecc...

Poriretario:

Ivan Favalli, Paolo Favalli

Info Ivan Favalli:Aziende partnership:Global Gest, planetel(compagnia telefonica, Astir srl(opera nell'e-Health, servizi consulenza IT)titolare Giulio Gilli. Interessante ricerche più approfondite su queste aziende.

Le aziende appena trovare fanno capo a myclubgourmet.it, sito mancante, decaduto il dominio.(<http://myclubgourmet.it/>)

Azienda Splendido Bay e Il Rivale al lago sono proprietà effettiva di un'altra azienda: Mael spa. Fanno parte del patrimonio immobiliare di Mael spa, si occupa principalmente di chiusure fallimentari, sede Brescia e Milano(nessun dato aziendale pubblico gratuito).<https://www.maelspa.it/>

Notizie pubbliche: Scandalo capodanno 2020 causa covid.

Il gruppo Favalli group esposto pubblicamente (social e media classici), per avere infranto le norme restrittive causa covid.

Esposizione di articoli di giornale locale e nazionale; esposizione televisiva (rete Rai, Lucarelli); canali social: Facebook, Instagram e tweeter.

IP legati al sito ufficiale: 62.149.128.45 ⇒ domain gestito da trendservice
utilizzo di VPN località totalmente diversa da quella delle strutture.

Vulnerabilità:

⚠ Vulnerabilities	
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.	
CVE-2019-8331	4.3 In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.
CVE-2018-20677	4.3 In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.
CVE-2018-20676	4.3 In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.
CVE-2018-14042	4.3 In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.
CVE-2018-14040	4.3 In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.
CVE-2016-10735	4.3 In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.

Porte aperte:

21, 80, 443, 8443, 8880