### **OSINT Recon part 2**

Employees, email addresses, other associated domains

Joe Sheer

CHIEF EXECUTIVE OFFICER

Email: joe@megacorpone.com

Twitter: [@Joe\_Sheer](https://twitter.com/joe_sheer/)

Tom Hudson

WEB DESIGNER

Email:thudson@megacorpone.com

Twitter: [@TomHudsonMCO](https://twitter.com/TomHudsonMCO)

Tanya Rivera

SENIOR DEVELOPER

Email: trivera@megacorpone.com

Twitter: [@TanyaRiveraMCO](https://twitter.com/TanyaRiveraMCO)

Matt Smith

MARKETING DIRECTOR

Email: msmith@megacorpone.com

Twitter: [@MattSmithMCO](https://twitter.com/MattSmithMCO)

Mike Carlow

Title: VP Of Legal

Email: [mcarlow@megacorpone.com](mailto:mcarlow@megacorpone.com)

Alan Grofield

Title: IT and Security Director

Email: [agrofield@megacorpone.com](mailto:agrofield@megacorpone.com)

Admin Name: Alan Grofield

Admin Organization: MegaCorpOne

Admin Street: 2 Old Mill St

Admin City: Rachel

Admin State/Province: Nevada

Admin Postal Code: 89001

Admin Country: US

Admin Phone: +1.9038836342

Search Google for site:megacorpone.com yields multiple pages. Simply looking at this provides information on multiple employees and their information.

Ports 22, 80, and 123 are open on 3.220.87.155 via shodan

Multiple cross-site scripting (XSS), denial of service (DDOS), ssh access, and Apache vulnerabilities can be used to attack these ports.

Subdomains found

[www.megacorpone.com](http://www.megacorpone.com), NS2.MEGACORPONE.COM, admin.megacorpone.com, beta.megacorpone.com, intranet.megacorpone.com, mail.megacorpone.com, mail2.megacorpone.com, ns1.megacorpone.com, ns2.megacorpone.com, ns3.megacorpone.com, router.megacorpone.com, siem.megacorpone.com, snmp.megacorpone.com, support.megacorpone.com, syslog.megacorpone.com, test.megacorpone.com, vpn.megacorpone.com, and www2.megacorpone.com.

With this information, Hackers can perform subdomain takeovers, enumeration, and discovery.

To mitigate the threat of certification transparency you can avoid having SSL/TLS support so that your internal hosts won’t get listed in the CT logs, use wildcard certifications you can have a single certificate that is valid for all your sub-domains, in turn not revealing the sub-domain names in CT logs, deploy your own Public Key Infrastructure(PKI) in your organization, opt-out of CT logs, but the overall best option is to secure your servers and application endpoints better.

