Client: MegaCorpOne

Google Searching

- Inspection of megacorpone.com source code revealed the following web hosting/server:

```
        });
    })(jQuery);
  </script>
  <data id="esmail" src="20203034302020303630202030363720203036362020303430202030363120
/body>

/html>
```

Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 443

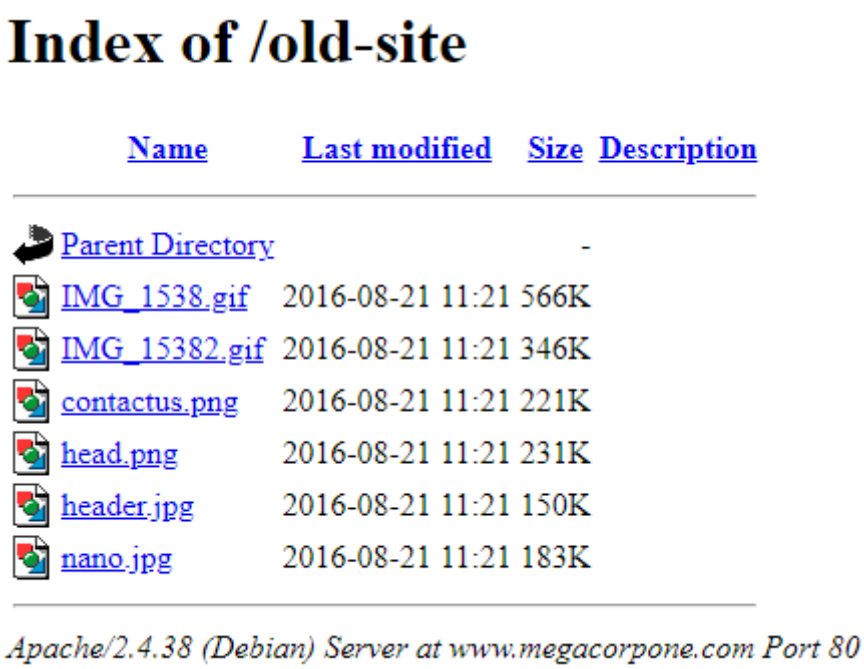
- Google search found a list of assets http://www.megacorpone.com/assets/

Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
css/	2016-08-21 11:21	-	
fonts/	2016-08-21 11:21	-	
img/	2017-10-03 09:08	-	
js/	2016-08-21 11:21	-	

Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 80

- Google search also revealed a link entitled "Index of /old-site" http://www.megacorpone.com/old-site/



Front-End Website

megacorpone.com

- Contact Us page revealed email contact info

Contact Our Departments

Department: Human Resources

Email: hr@megacorpone.com

Department: Sales

Email: sales@megacorpone.com

Department: Shipping

Email: shipping@megacorpone.com

Physical Address, Phone, Sales contact

Our Address

MegaCorp One
2 Old Mill St
Rachel, NV 89001
United States.

Email: sales@megacorpone.com
Tel: (903) 883 - MEGA
Web: http://www.megacorpone.com

nslookup

```
The Groehlers@DESKTOP-BELCLER MINGW64 ~
$ nslookup www.megacorpone.com
Server:  rns01.charter.com
Address:  2607:f428:ffff:ffff::1

Non-authoritative answer:
Name:    www.megacorpone.com
Address:  149.56.244.87
```

Shodan

https://www.shodan.io/host/149.56.244.87

General Information

Hostnames	www.megacorpone.com
Domains	MEGACORPONE.COM
Country	Canada
City	Montréal
Organization	OVH Hosting, Inc.
ISP	OVH SAS
ASN	AS16276

Open Ports

22 80 443

Web Technologies

BOOTSTRAP GOOGLE HOSTED LIBRARIES JQUERY PRETTYPHOTO

// 22 / TCP

-1487338745 | 2023-06-21T05:11:05.743507

OpenSSH 7.9p1 Debian 10+deb10u2

```
SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCqwgSBR7aTX60TSlNJwbsj15167JlhvTxf6CeilyU7WS3j
sRW6R5bephaO/iyVgGa6pCoVDxFHKBRWcajSGiLBpWC4AGHlhd8s9CdnGirqb5BnuxlcvuRydo1o
nyIt/jZDDi2c1OUrE77wDqQWJqQPjvsqVwCn2LSqCfHV/bo+PFYampdhVzsj7aYIq5r/U7yJhqZJ
u2uhQc73ZnmNAHol+0ivPP8+jv8Jv7gKfyUQfcb+qBWNxWZhc600YBEJ15VBKR7frx6APqazIlo2
zr+d1dgcILE5TUQoqzlewNuZZj3RRmY1aUT1N+Zu09QWCpSTh+6HBDk/m15RYSvB/8Zj
Fingerprint: cd:bd:1d:f0:c2:fb:c3:d8:48:ef:7f:5f:ba:34:1f:06
```

// 80 / TCP

-683791476 | 2023-06-24T21:16:28.593560

Apache httpd 2.4.38

```
HTTP/1.1 200 OK
Date: Sat, 24 Jun 2023 21:16:28 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html
```

// 443 / TCP

-683791476 | 2023-06-28T14:24:33.642849

Apache httpd 2.4.38

```
HTTP/1.1 200 OK
Date: Wed, 28 Jun 2023 14:24:33 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html
```

Recon-ng

MegaCorpOne

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	18
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[-] Hosts

host	ip_address	region	country	latitude	longitude	notes	module
admin.megacorpone.com	51.222.169.208						hackertarget
beta.megacorpone.com	51.222.169.209						hackertarget
fs1.megacorpone.com	51.222.169.210						hackertarget
intranet.megacorpone.com	51.222.169.211						hackertarget
mail.megacorpone.com	51.222.169.212						hackertarget
mail2.megacorpone.com	51.222.169.213						hackertarget
ns1.megacorpone.com	51.79.37.18						hackertarget
ns2.megacorpone.com	51.222.39.63						hackertarget
ns3.megacorpone.com	66.70.207.180						hackertarget
router.megacorpone.com	51.222.169.214						hackertarget
siem.megacorpone.com	51.222.169.215						hackertarget
snmp.megacorpone.com	51.222.169.216						hackertarget
support.megacorpone.com	51.222.169.218						hackertarget
syslog.megacorpone.com	51.222.169.217						hackertarget
test.megacorpone.com	51.222.169.219						hackertarget
vpn.megacorpone.com	51.222.169.220						hackertarget
www.megacorpone.com	149.56.244.87						hackertarget
www2.megacorpone.com	149.56.244.87						hackertarget

Created by: Pentester
Fri, Jul 07 2023 18:33:04