Phishers Are Impersonating Maersk: What Other Container Shipping Companies Are Targeted?

Table of Contents

Executive Report

Phishing emails impersonating Maersk, one of the largest container shipping companies, targeted more than 18,000 people since the beginning of the year. The email address imitated the legitimate company's email address but led to a phishing page designed to look like Maersk's shipping portal login page. The campaign peaked in March, endangering the supply chain of millions of businesses worldwide.

WhoisXML API researchers combed through the Domain Name System (DNS) and other intelligence sources to see how Maersk and other shipping companies are being impersonated via look-alike domain names. Among our findings are:

- 1,100+ domains and subdomains added since 1 March 2022 containing the names of 10 of the largest shipping companies
- Only two of these properties could be publicly attributed to legitimate shipping companies
- 980+ cybersquatting resources resolved to 1,000+ unique IP addresses
- Dozens of domains hosted suspicious login pages that mimicked legitimate sites

Analysis of Shipping-Related Properties

Who Owns the Cyber Resources?

We discovered 600+ domains and 500+ subdomains added between 1 March and 15 June 2022. While this sample may not be as large as the 13,000+ e-commerce domains we uncovered, they are still a cause for concern. After all, it could only take a few malicious

domains to steal user credentials or convince key personnel to transfer funds to a supplier or CEO impersonator.

This study focused on 10 of the largest container shipping and logistics companies. They are listed in the table below, along with the search strings we used on Domains & Subdomains Discovery. The strings were chosen to remove as many false positives as possible.

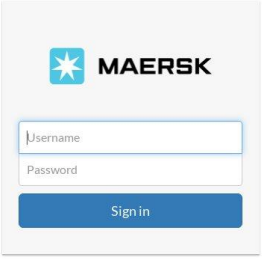
Company Name	Search Strings Used
Maersk	“maersk”
CMA-CGM	“cma + cgm”
COSCO	“cosco”
Hapag-Lloyd	“hapag + lloyd”
YangMing Marine Transport	“yangming”
Matson	“matson”
Unifeeder	“unifeeder”
Wanhai Lines	“wanhai”
Ocean Network Express (ONE)	“oneline” and “one-line,” excluding “phone,” “loneliness,” and “zone”
Arkas Container Transport	“arkasline” and “arkas”

Only two domains could be publicly attributed to the legitimate shipping companies. These domains shared the same registrant email address as the official domain of one of the organizations in this study.

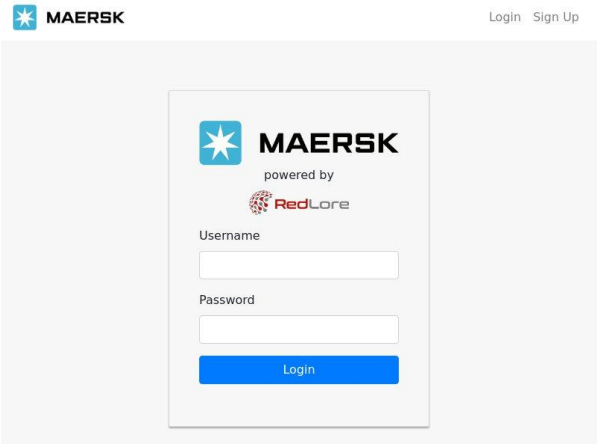
What Content Do the Resolving Properties Host?

Several domains were either parked or hosted 404 or index pages. Others hosted content that suggests businesses unrelated to container shipping or logistics. These may belong to legitimate organizations bearing similar names as the shipping companies.

However, we found more than 40 properties that hosted suspicious login pages. Below are some examples of Maersk and CMA-CGM look-alike login pages.



Screenshot of maersk[.]smartconsultant[.]co

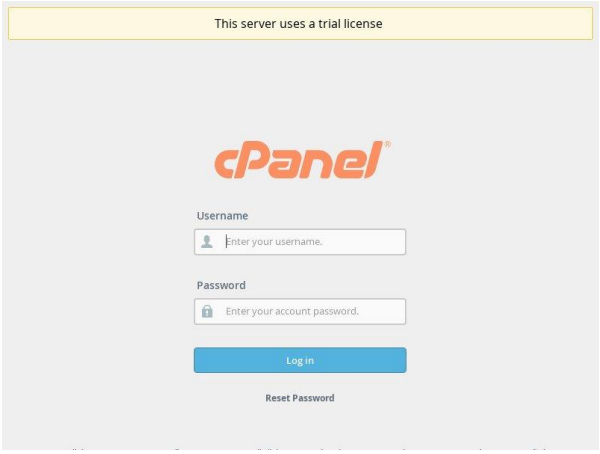


Screenshot of dev[.]maersk[.]monitor[.]redlore[.]com

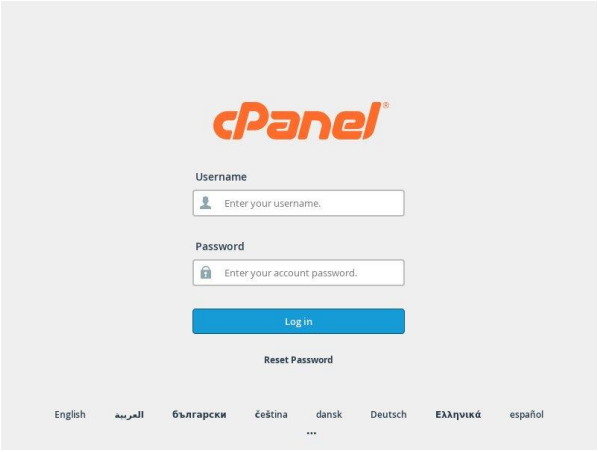
Screenshot of cma-cgm[.]tevatelcloud[.]com

Screenshot of cmacgm[.]ativated[.]com[.]br

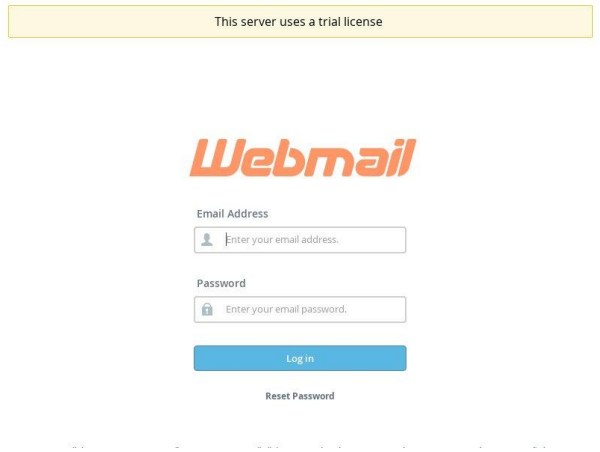
Other login pages were hosted on Zendesk, while some pointed to Webmail and cPanel login pages hosted on Duck DNS and Sleck Express. A few examples are shown below.



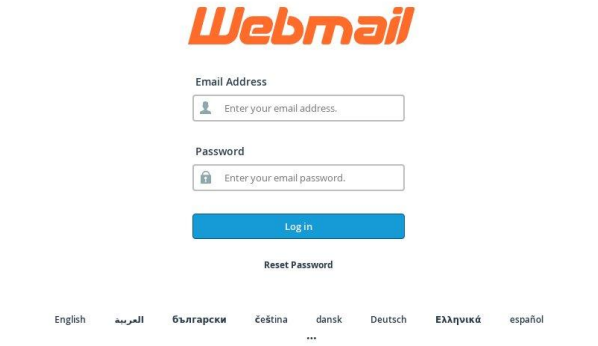
Screenshot of cpanel[.]accessoneline222[.]duckdns[.]org



Screenshot of cpanel[.]hapaglloydshipping[.]sleckexpress[.]com



Screenshot of webmail[.]accessoneline222[.]duckdns[.]org



Screenshot of webmail[.]hapaglloydshipping[.]sleckexpress[.]com

Screenshot of arkashelp[.]zendesk[.]com	*Screenshot of maersk2110[.]zendesk[.]com*

While legitimate companies could have created these subdomains and hosted content, it is also possible for threat actors to be behind them.

Have Any of the Resources Been Used Maliciously?

As of 15 June 2022, seven cybersquatting properties have been reported as malicious by various malware engines. Five were newly registered domains (NRDs), while two were subdomains.

One of the malicious subdomains—accessoneline33[.]duckdns[.]org—is similar to more than a dozen Duck DNS subdomains bearing the strings “access,” “online,” and a series of numbers. Some of these subdomains hosted Webmail and cPanel login pages, including those provided as examples above.

—

Businesses heavily rely on their supply chains for day-to-day activities. A cyber attack on a shipping company carrying products or accessories and parts could cripple their operations, similar to the supply chain attack Toyota suffered early this year.

Monitoring cybersquatting domains and subdomains that could serve as vehicles for such attacks can help protect businesses.

If you wish to perform a similar investigation or research, please don’t hesitate to contact us. We’re always on the lookout for potential research collaborations.

Appendix: Sample Cybersquatting Domains and Subdomains Targeting Shipping Companies

Sample Cybersquatting Domains

- aloneline[.]xyz
- ararkasline[.]com
- arkasline[.]ru
- arkaslinear[.]com
- arkaslinemetaverse[.]com
- arkaslinenft[.]com
- arkaslinevr[.]com
- australiahapaglloyd[.]com
- boneline[.]kr
- cgm-cman[.]com
- cmacgm[.]aero
- cmacgm-aircargo[.]aero

- cma-cgm-cmrsarl[.]com
- cma-cgmg[.]com
- cma-cgmi[.]com
- cmacgm-log[.]xn--fiqz9s
- cmacgm-logistics[.]xn--fiqs8s
- cma-cgm-logistics[.]xn--fiqz9s
- cma-cgmshippingservices[.]com
- containershapaglloyd[.]com
- coscoairexpress[.]com
- coscom[.]us
- coscon[.]ga
- coscos[.]us
- cosco-shipping[.]ws
- cosco-surveys[.]com
- coscout[.]in
- droneline[.]es
- droneline[.]gr
- ffsandusr0maersklineas[.]ws
- glenorchocosco[.]ml
- hapag-lloyd[.]kr
- hapag-lloyd[.]ws
- hapaglloyddelivery[.]com
- hapaglloydlogistic[.]com
- hapaglloydlogistics[.]co[.]uk
- hapag-lloyd-rla[.]com
- hapaglloyd-schiffe[.]de
- jktidyangming[.]com
- lsyangming[.]com
- maersk[.]cyou
- maersk[.]ink
- maersk[.]xn--fiqs8s
- maerskaircargo[.]ru
- maerskbusinesssummit[.]com
- maersklineshipment[.]online
- maersk-logist[.]com
- maersktraining[.]xn--fiqs8s
- maersktz[.]com
- matson[.]tk
- matsonfreight[.]com
- matsonm[.]com
- matsonn[.]ph
- matsontracking[.]com
- matsontracks[.]com
- matsontracks[.]org
- metaversearkasline[.]com
- nammotorcarriermaersk[.]com
- nftarkasline[.]com
- ocosco[.]jp
- one-line[.]consulting
- one-line[.]design
- one-line[.]ink
- oneline17[.]cn
- onelineco[.]com
- one-line-crm[.]ch
- one-line-direct[.]gq
- oneliner[.]run
- oneliner[.]tk
- oneliners[.]in
- oneliners[.]us
- onelinesb[.]com
- one-line-studio[.]com
- plusone-line[.]com
- posidoniamaerskbroker[.]com
- sandcoscoatrac[.]ml
- shawnamatson[.]com
- sunyangming[.]cc
- tala-samantha-cma-cgm[.]com
- theone-line[.]com
- unifeeder[.]cc
- unifeeder[.]cf
- unifeeder[.]us
- unifeeder[.]xyz
- unifeederlogistics[.]com
- unifeedermaritimetransportser[.]com
- unifeeders[.]com
- vrarkasline[.]com
- wanhai[.]com[.]au
- wanhai[.]icu
- wanhaicloud[.]com
- wanhai-com[.]cf

- wanhaiglobal[.]com
- wanhaitech[.]com
- wanhaius[.]online
- yangmingbeats[.]com
- yangminghd[.]ws
- yangmingltd[.]cn
- yangmingwenti[.]xyz
- yangmingxin[.]xyz

Sample Cybersquatting Subdomains

- api[.]demo[.]matson[.]analytics[.]hazcheckdetect[.]com
- autodiscover[.]hapaglloydshipping[.]sleckexpress[.]com
- clay-matson[.]jewsonproperties[.]com
- cmacgm[.]ativated[.]com[.]br
- cmacgm[.]investflow[.]io
- cma-cgm[.]mubarekmuhasebe[.]com
- cmacgm[.]pdx[.]pashagroup[.]com
- cma-cgm[.]tevatelcloud[.]com
- cmacgmbe[.]securecontainerrelease[.]com
- cmacgmtest[.]syncfish[.]app
- cmascgms[.]blogspot[.]com
- cosco[.]bigdeo[.]com
- cosco[.]cloudcontrolapp[.]com
- cosco[.]goto56[.]cn
- cosco[.]sandcats[.]io
- cpanel[.]hapaglloydshipping[.]sleckexpress[.]com
- cpcalendars[.]hapaglloydshipping[.]sleckexpress[.]com
- cpcontacts[.]hapaglloydshipping[.]sleckexpress[.]com
- demo[.]matson[.]hazcheckdetect[.]com
- ecoscopa[.]ifremer[.]fr
- ecoscore[.]hollevoet[.]dev
- func-unifeeder-map-test[.]azurewebsites[.]net
- gregmatson[.]mailrocs[.]com
- hapag-lloyd[.]com-en[.]info
- hapag-lloyd[.]com-en-au[.]info
- hapaglloyd[.]p6-hamburg-production[.]dcsa[.]org
- hapaglloydshipping[.]sleckexpress[.]com
- iwanhaidar[.]workers[.]dev
- maersk[.]byteswap[.]org
- maersk[.]morpg[.]hu
- maersk[.]movildata[.]com
- maersk[.]outliner[.]me
- maersk[.]seidat[.]net
- maersk[.]splunkcloud[.]com
- maersk-apmtis-appser-aps-inlandnet-prod[.]azurewebsites[.]net
- maersk-apmtis-appser-aps-module aps-prod[.]azurewebsites[.]net
- maersk-apmtis-appser-csl-modulecsl-prod[.]azurewebsites[.]net
- maersk-apmtis-appser-csl-modulecsl-qa[.]azurewebsites[.]net
- maersk-apmtis-appser-sd1-inlandnet-prod[.]azurewebsites[.]net
- maersk-apmtis-appser-sd1-module sdc-qa[.]azurewebsites[.]net
- maersk-apmtis-appser-sd1-module sdy-uat[.]azurewebsites[.]net
- maersk-apmtis-appser-sls-mltmain-prod[.]azurewebsites[.]net
- maersk-apmtis-appser-sls-mltslo-prod[.]azurewebsites[.]net
- maersk-apmtis-appser-sls-mltslt-prod[.]azurewebsites[.]net

- matson[.]amadn[.]com
- matson[.]jessicabrowncollections[.]com
- matson[.]milwaukeeprec[.]com
- matson[.]my[.]onevoice[.]site
- matson[.]web[.]app
- matson5740[.]repl[.]co
- matson-dn[.]financial-net[.]com
- matsonlima[.]repl[.]co
- oneline[.]aquila[.]it
- oneline[.]bvn[.]jp
- oneline[.]factsandcomparisons[.]com
- one-line[.]info[.]at
- oneline[.]metalic-art[.]eu
- oneline[.]opencraft[.]hosting
- oneline[.]smc-automobiles[.]com
- one-line[.]vercel[.]app
- one-linebarrels[.]blogspot[.]com
- one-liner[.]blogalimentoseguro[.]com
- one-liner[.]christopherkellen[.]com
- one-liner[.]ddns[.]net
- one-liner[.]oulzo[.]com
- one-liner[.]virtualbenidorm[.]com
- one-liner-orchestra[.]herokuapp[.]com
- one-liners[.]belau[.]pw
- oneliners[.]bulkje[.]nl
- ricoscom[.]kpages[.]online
- ridhwanhaikal[.]repl[.]co
- rorymatson[.]repl[.]run
- scosco[.]github[.]io
- simcosco[.]luyq[.]ru
- smatsonks[.]repl[.]co
- stone-lined[.]barsy[.]online
- taiwanhair[.]com[.]bigwit[.]com[.]tw
- tsekanimatson[.]intomodeling8[.]com
- unifeederftp[.]azurewebsites[.]net
- wanhai[.]adhdtc[.]org[.]tw
- wanhai[.]fncc[.]cc
- wanhaishijiedefangfa[.]cloudcon
- wanhaizzi[.]repl[.]co
- webdisk[.]hapaglloydshipping[.]sleckexpress[.]com
- webmail[.]hapaglloydshipping[.]sleckexpress[.]com
- www[.]cmacgm[.]ativated[.]com[.]br
- www[.]cma-cgm[.]mubarekmuhasebe[.]com
- www[.]hapaglloydshipping[.]sleckexpress[.]com
- www[.]matson[.]jessicabrowncollections[.]com
- www[.]taiwanhair[.]com[.]bigwit[.]com[.]tw
- www[.]wanhai[.]adhdtc[.]org[.]tw
- yangming[.]adpjmu[.]com
- yangming[.]alesnet[.]com
- yangming[.]edu[.]ws
- yangming[.]qingchikj[.]com
- yangming[.]rlbcgg[.]com
- yangming1[.]direct[.]quickconnect[.]to
- yangming998[.]direct[.]quickconnect[.]to
- yangminglogistics[.]winnerstraders[.]online
- yangmingproperty[.]blogspot[.]com

Malicious Properties Flagged during the Malware Check Dated 15 June 2022

- accessoneline33[.]duckdns[.]org
- groundboneline[.]xyz

- lns-maersk[.]xyz
- logisticoscorreos-peru[.]com
- maersk[.]workers[.]dev
- oneline24[.]top
- onelinelink[.]space