	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 073	Fecha: 25-03-2023
		Página 12 de 23

Componente que reporta	COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ		
Nombre de la alerta	Nuevas URL maliciosas de empresas		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, entre otros		
Código de familia	G	Código de subfamilia	G03
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectaron varios sitios webs fraudulentos activos, donde suplantan páginas web de diversas empresas, con la finalidad de obtener las credenciales del usuario y robar información:

a. Facebook

PAÍS DE PROCEDENCIA	FECHA	IP	URL
Vietnam	2023-03-23	137.59.106.124	xxxx://tseruxsoerossuer18[.]click/
Vietnam	2023-03-23	137.59.106.124	xxxx://tseruxsoerossuer18[.]click
Vietnam	2023-03-23	103.18.7.159	xxxxs://tseruxsoerossuer15[.]click/
Vietnam	2023-03-23	103.18.7.159	xxxxs://tseruxsoerossuer15[.]click
Vietnam	2023-03-23	103.18.7.151	xxxxs://hilaface01[.]click/
Vietnam	2023-03-23	103.18.7.151	xxxxs://hilaface01[.]click
United States	2023-03-23	185.199.108.153	xxxx://memdad23[.]github[.]io/test/
United States	2023-03-23	185.199.109.153	xxxx://memdad23[.]github[.]io/test
United States	2023-03-23	185.199.110.153	xxxx://94edwin89[.]github[.]io/facebook-login-page
Desconocido	2023-03-23	2606:50c0:8000::153	xxxx://94edwin89[.]github[.]io/facebook-login-page/
United States	2023-03-23	185.199.109.153	xxxxs://abnerhuy[.]github[.]io/
United States	2023-03-23	185.199.111.153	xxxxs://abnerhuy[.]github[.]io
Vietnam	2023-03-23	103.18.7.151	xxxx://itaface12[.]click/
Vietnam	2023-03-23	103.18.7.151	xxxx://itaface12[.]click

b. Instagram

PAÍS DE PROCEDENCIA	FECHA	IP	URL
Republic of Lithuania	2023-03-23	89.117.9.169	xxxxs://www[.]ihnf[.]in/
Australia	2023-03-23	122.201.80.194	xxxxs://social[.]flynnassociates[.]com[.]au/
Australia	2023-03-23	122.201.80.194	xxxxs://social[.]flynnassociates[.]com[.]au
Turkey	2023-03-23	31.210.39.251	xxxxs://approvalsform[.]com[.]tr/login[.]html

c. Google

PAÍS DE PROCEDENCIA	FECHA	IP	URL
United States	2023-03-23	162.254.33.94	xxxxs://utente-infousr-online[.]162-254-33-94[.]cprapid[.]com/uscl/it/index[.]php
United States	2023-03-23	162.254.33.94	xxxxs://utente-infousr-online[.]162-254-33-94[.]cprapid[.]com/uscl
Canada	2023-03-23	162.0.236.181	xxxxs://client-lds-info[.]162-0-236-181[.]cprapid[.]com/lt-usr/home/index[.]php?sessione=b9b0ce2c168bb36ee323842ae80d8d34afd53529d4a2f0c4705d8f38cd63cf7a7dd33708
United States	2023-03-23	162.254.38.129	xxxxs://accedi-accountuser-infoweb[.]162-254-38-129[.]cprapid[.]com/ln/home/index[.]php?sessione=4f321beb88238928d513e112e0f9854bbbc2418cc7adb5b672457c0e96cb4f01839f8009
United States	2023-03-23	2606:4700:3031::ac43:8cea	xxxxs://m24-app[.]cc/
United States	2023-03-23	172.67.140.234	xxxxs://m24-app[.]cc
United States	2023-03-23	162.254.38.129	xxxxs://accedi-accountuser-infoweb[.]162-254-38-129[.]cprapid[.]com/ln/home/index[.]php?sessione=4547bdc30620d520036ae96acef07e661b4ed91c9d30164cdeb61a4caaff2d044a3fd599
United States	2023-03-23	162.254.38.129	xxxxs://accedi-accountuser-infoweb[.]162-254-38-129[.]cprapid[.]com/ln/checkclient[.]php?&sessionid=9d30164cdeb61a4caaff2d044a3fd599
United States	2023-03-23	162.254.38.129	xxxxs://accedi-accountuser-infoweb[.]162-254-38-129[.]cprapid[.]com/ln/
Republic of Lithuania	2023-03-23	2a02:4780:27:1066:0:37f8:1f19:2	xxxxs://is-a[.]info/ld-Hype
Canada	2023-03-23	162.0.236.181	xxxxs://client-lds-info[.]162-0-236-181[.]cprapid[.]com/lt-usr/home/index[.]php?sessione=4547bdc30620d520036ae96acef07e661b4ed91c9d30164cdeb61a4caaff2d044a3fd599
Canada	2023-03-23	162.0.236.181	xxxxs://client-lds-info[.]162-0-236-181[.]cprapid[.]com/lt-usr/checkclient[.]php?&sessionid=9d30164cdeb61a4caaff2d044a3fd599
Canada	2023-03-23	162.0.236.181	xxxxs://client-lds-info[.]162-0-236-181[.]cprapid[.]com/lt-usr/
United States	2023-03-23	208.109.26.112	xxxxs://arcentersinforint[.]com/eng/verification/

d. Netflix

PAÍS DE PROCEDENCIA	FECHA	IP	URL
United States	2023-03-23	2606:4700:3034::6815:cdd	xxxxs://fake-netflix[.]callmetak[.]com/login[.]html
United States	2023-03-23	185.199.109.153	xxxxs://shahinabbas[.]github[.]io/netflix1/
United States	2023-03-23	185.199.111.153	xxxxs://shahinabbas[.]github[.]io/netflix1
United States	2023-03-23	185.199.111.153	xxxxs://elmahdi-ratil[.]github[.]io/Netflix[.]github[.]io/
Desconocido	2023-03-23	2606:50c0:8002::153	xxxxs://elmahdi-ratil[.]github[.]io/Netflix[.]github[.]io

United States	2023-03-23	185.199.111.153	xxxxs://94edwin89[.]github[.]io/Netflix
United States	2023-03-23	185.199.109.153	xxxx://victrfiuza[.]github[.]io/Sign-In-Netflix
Desconocido	2023-03-23	2606:50c0:8002::153	xxxxs://94edwin89[.]github[.]io/Netflix/
Desconocido	2023-03-23	2606:50c0:8002::153	xxxxs://shahraim[.]github[.]io/netflix[.]github[.]io/

e. Outlook

PAÍS DE PROCEDENCIA	FECHA	IP	URL
United States	2023-03-23	2602:fea2:2::1	xxxxs://bafybeidpeijyj3nn5ahhoyfsclgxea2qzocipnpoldmzle6uronug47rse[.]ipfs[.]dweb[.]link/
United States	2023-03-23	18.234.20.234	xxxxs://leone75564[.]lt[.]emlnk[.]com/Prod/link-tracker?notrack=1&redirectUrl=aHR0cHMlM0ElMkYlMkZiYWZ5YmVpZGJkc3dmMzR4c2RlMnpmcW16NWwzZnpsejN6ejc3eW4yZGFqanpmY2J2YzI0bWd2aGoycS5pcGZzLmR3ZWIubGluayUyRmxhY28uaHRtbA==&sig=7Cuuh7zxgxQUvu6WVNW1C3yXLFjDNSZY8wSd442Y2mYc&iat=1679448241&a=%7C%7C478129977%7C%7C&account=leone75564[.]activehosted[.]com&email=ydLRfXnxfl5BcGpskCSCsqEyYtv3RwHaDBM12o1w7WUrbksb:ZMnCNXQK2LsbZrn3ugrHXDczYHHmlUH5&s=62b367a5eb9e6d8029635e5d4628f907&i=1A3A1A1
United States	2023-03-23	209.94.90.1	xxxxs://ipfs[.]io/ipfs/QmaZkma9WPNZ3PuqZ6TXeKXpSc17hddWkux7XXigiiY5Jz
United States	2023-03-23	2606:4700::6812:1634	xxxxs://bafybeiemg6idwecwn7cgfloxp26duakqkivpabl5ff76wfxu6dvuhmhqkm[.]ipfs[.]w3s[.]link
United States	2023-03-23	2602:fea2:2::1	xxxxs://bafybeidbdswf34xsde2zfqmz5l3fzlz3zz77yn2dajjzfcbvc24mgvhj2q[.]ipfs[.]dweb[.]link/laco[.]html
United States	2023-03-23	192.249.122.211	xxxxs://alsheikhavenue[.]com/qua/logon[.]php
United States	2023-03-23	192.249.122.211	xxxxs://alsheikhavenue[.]com/qua/?client-request-id=YmxhemVqLndhanN6Y3p1a0BibnBwYXJpYmFzLnBs
United States	2023-03-23	52.216.50.64	xxxxs://s3[.]amazonaws[.]com/appforest_uf/f1679460468077x706068467579039000/Outltookk[.]html#3mail@b[.]c
United States	2023-03-23	52.216.59.248	xxxxs://s3[.]amazonaws[.]com/appforest_uf/f1679409334458x145659541293319040/butt[.]html

f. WhatsApp Group Invite

PAÍS DE PROCEDENCIA	FECHA	IP	URL
United States	2023-03-23	172.66.44.165	xxxxs://whatsappservicesex[.]pages[.]dev/
United States	2023-03-23	2606:4700:310c::ac42:2ca5	xxxxs://whatsappservicesex[.]pages[.]dev

g. Microsoft Login

PAÍS DE PROCEDENCIA	FECHA	IP	URL
United States	2023-03-23	2602:fea2:2::1	xxxxs://bafybeidlzgkfoalzcst3xzvhtnzsiyas33p2iopjzgm6helzvbg6izr2cu[.]ipfs[.]dweb[.]link/office[.]html
United States	2023-03-23	2600:3c02::f03c:92ff:fe32:7a10	xxxxs://trust[.]us-southeast-1[.]linodeobjects[.]com/jun/pill[.]html
United States	2023-03-23	52.216.112.173	xxxxs://s3[.]amazonaws[.]com/appforest_uf/f1679410731851x295358009011027700/passwordreset[.]html
United States	2023-03-23	54.236.235.81	xxxxs://placememntt[.]publicvm[.]com/
United States	2023-03-23	54.236.235.81	xxxxs://placememntt[.]publicvm[.]com
United States	2023-03-23	52.72.89.99	xxxxs://mlcrosoft[.]live/render-template/?campaign_scenario_user_id=A4tukP8FlPU0qjsSRAPud5Yv/Ka4tk0WhkujbER3lvg=&status_id=JPLopEADwyrT0OaKcuj4tUSP8B7FZbX13bfknyC44SA=
United States	2023-03-23	69.49.245.48	xxxxs://lovepridejoy[.]com/Goodspeedsbils/SMGseee/
United States	2023-03-23	69.49.245.48	xxxxs://lovepridejoy[.]com/Goodspeedsbils/SMGseee
Germany	2023-03-23	144.91.73.214	xxxxs://invetec[.]eu/bboun/rydocs/
Germany	2023-03-23	144.91.73.214	xxxxs://invetec[.]eu/bboun/rydocs
United States	2023-03-23	69.49.245.48	xxxx://missy-hmb[.]biz/
United States	2023-03-23	69.49.245.48	xxxx://missy-hmb[.]biz
United States	2023-03-23	2602:fea2:2::1	xxxx://bafybeidlzgkfoalzcst3xzvhtnzsiyas33p2iopjzgm6helzvbg6izr2cu[.]ipfs[.]dweb[.]link/office[.]html
United States	2023-03-23	209.94.90.1	xxxxs://bafybeidlzgkfoalzcst3xzvhtnzsiyas33p2iopjzgm6helzvbg6izr2cu[.]ipfs[.]dweb[.]link/office[.]html#x@x[.]com
United States	2023-03-23	2602:fea2:2::1	xxxx://gateway[.]ipfs[.]io/ipfs/QmUwwTYL3U2ehstYvkKKeS953eD8B7T3Vz65LwBotVCmKE
United States	2023-03-23	54.231.162.40	xxxxs://s3[.]amazonaws[.]com/appforest_uf/f1679470176529x248678979991209020/Office365-876543212345678987654323456788764345678987654323456789876543456789-87654323456787632345678987654345678765432 4567876543-87654323456789876543234567898765 4[.]html
United States	2023-03-23	52.217.224.80	xxxxs://s3[.]amazonaws[.]com/appforest_uf/f1679402674440x414094557706522050/Offfice%20new%20index[.]html
United States	2023-03-23	209.94.90.1	xxxx://gateway[.]ipfs[.]io/ipfs/QmUwwTYL3U2ehstYvkKKeS953eD8B7T3Vz65LwBotVCmKE/
United States	2023-03-23	52.216.228.99	xxxxs://s3[.]amazonaws[.]com/appforest_uf/f1679400984398x754519447563045200/indexx[.]html
United States	2023-03-23	52.217.84.182	xxxxs://s3[.]amazonaws[.]com/appforest_uf/f1679400394437x992018621247154400/index%20%286%29[.]html#3mail@b[.]c
United States	2023-03-23	52.217.73.54	xxxxs://s3[.]amazonaws[.]com/appforest_uf/f1679400394437x992018621247154400/index%20%286%29[.]html
United States	2023-03-23	54.231.229.72	xxxxs://s3[.]amazonaws[.]com/appforest_uf/f1679323655774x555153142579554200/Offfice%20new%20index%20%281%29[.]html

United States	2023-03-23	69.49.230.119	xxxxs://mickeydrinkard[.]net/
United States	2023-03-23	2602:fea2:2::1	xxxxs://gateway[.]ipfs[.]io/ipfs/QmUwwTYL3U2ehstYvkKKeS953eD8B7T3Vz65LwBotVCmKE/
United States	2023-03-23	104.21.87.181	xxxxs://alicelane[.]co[.]za/cherish/testing[.]html#3mail@b[.]c

h. Office 365

PAÍS DE PROCEDENCIA	FECHA	IP	URL
Israel	2023-03-23	212.115.111.178	xxxxs://gadamrani[.]co[.]il/gpsengineeringsrlfiledoc
Israel	2023-03-23	212.115.111.178	xxxxs://gadamrani[.]co[.]il/gpsengineeringsrlfiledoc/
United States	2023-03-23	69.49.230.119	xxxxs://comfestmerch[.]com/ttddoc/
United States	2023-03-23	69.49.230.119	xxxxs://comfestmerch[.]com/ttddoc

2. Recomendaciones:

- Evitar ingresar datos personales a enlaces de dudosa procedencia
- Mantener los equipos protegidos, con el software actualizado

Fuentes de información	▪ Comandancia de Ciberdefensa de la Marina, Osint