Tracking A Renewable Energy Intelligence Gathering Campaign

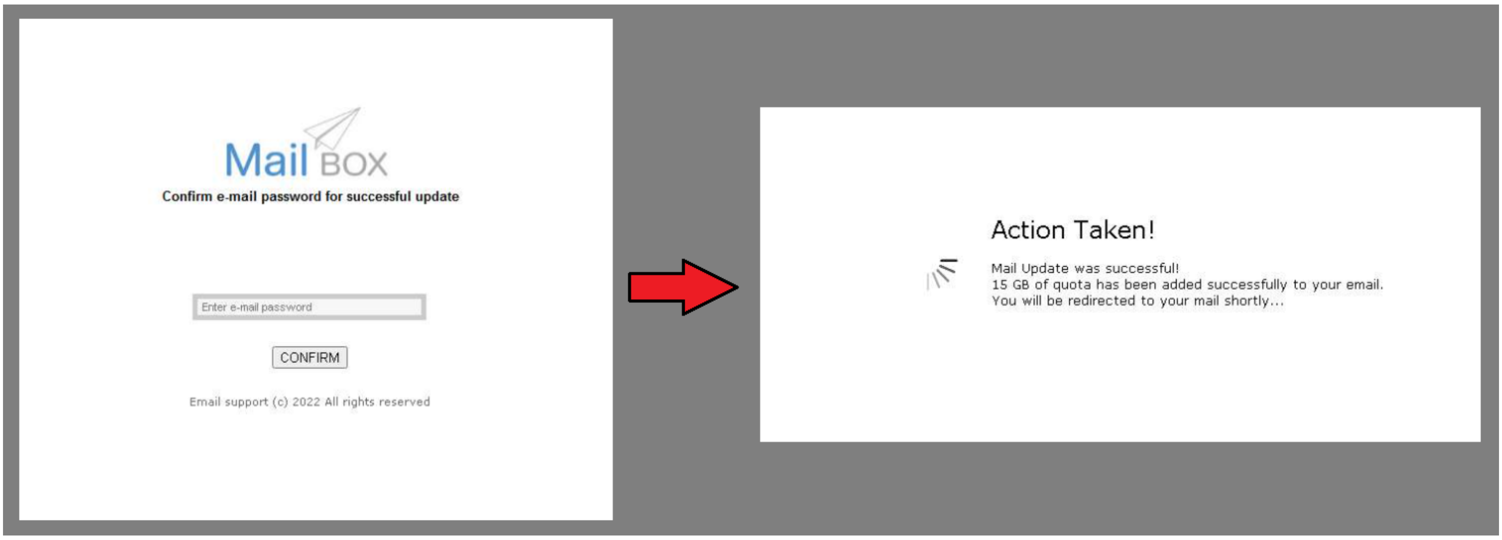
blog.bushidotoken.net/2022/01/tracking-renewable-energy-intelligence.html

For my first research blog of 2022, I analysed a suspected intelligence gathering campaign targeting renewable energy and industrial technology organisations, with a particular focus on Bulgaria. This long-running espionage campaign leveraged multiple credential harvesting pages to target the email accounts of employees at a number of organisations between 2019 and is ongoing in 2022. The attackers use the same 'Mail Box' phishing kit and host many of the pages on them infrastructure, supported by also compromising some legitimate websites.

This research was conducted using OSINT techniques such as query public sandbox submissions and passive DNS scan results. From this up to 40 individuals at target organisations from a variety of sectors were identified, but there was a focus on a few such as renewable energy, environmental protection organisations, and industrial technology. This research using OSINT alone is unable to acquire the full story, but hopefully can paint a picture of the motivation of the adversary behind this campaign.

Some of the targets include high-profile organisations such as operational technology (OT) and industrial control system (ICS) vendors like Schneider Electric and Honeywell, as well as Chinese telecommunications giant Huawei, semiconductor manufacturer HiSilicon, Telekom Romania, and US universities such as the University of Wisconsin, California State University, and Utah State University.

As mentioned above, one of the focuses of the campaign appeared to be renewable energy and environmental protection organisations. This includes the Kardzhali Hydroelectric Power Station (vec[.]nek[.]bg) and CEZ Electro (cez[.]bg), both located in Bulgaria, as well as the California Air Resources Board (arb[.]ca[.]gov), Morris County Municipal Utilities Authority (mcmua[.]com), the Taiwan Forestry Research Institute (tfri[.]gov[.]tw), the Carbon Disclosure Program (cdp[.]net), and Sorema, an Italian plastic recycling firm. There was also a small cluster of activty in 2019 linked to the same infrastructure targeting multiple banks in Bulgaria too.



Mail BOX

Confirm e-mail password for successful update

Enter e-mail password

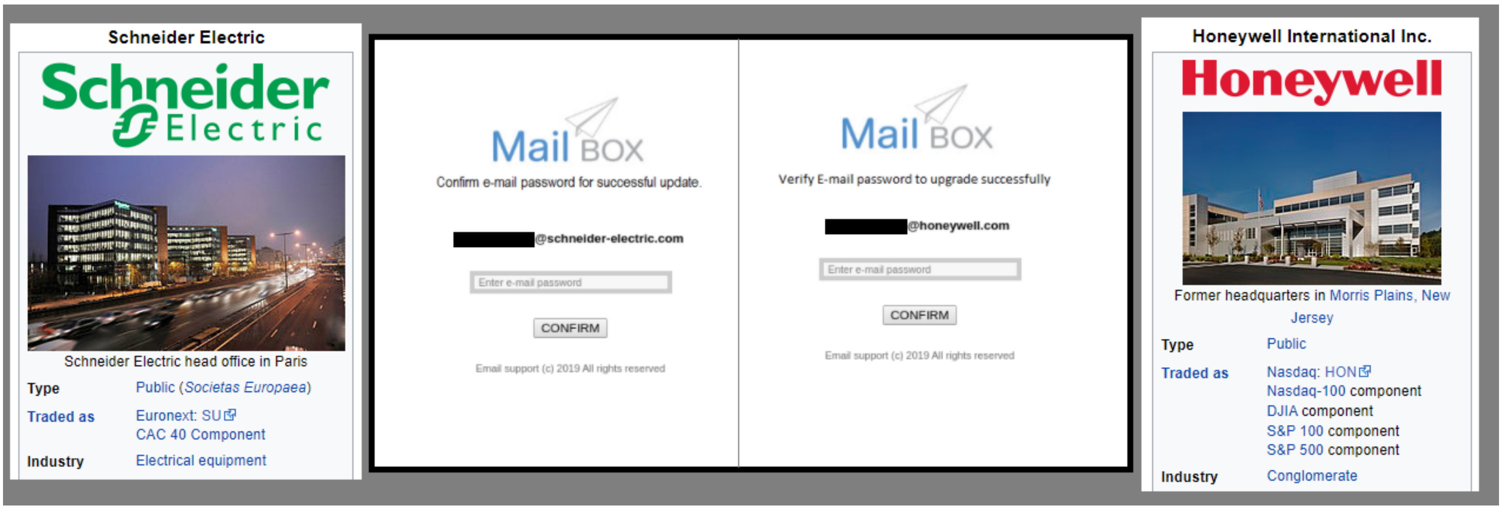
CONFIRM

Email support (c) 2022 All rights reserved

Action Taken!

Mail Update was successful!
15 GB of quota has been added successfully to your email.
You will be redirected to your mail shortly...

Fig. 1 - 'Mail Box' phishing kit



Schneider Electric

Schneider Electric head office in Paris

Type	Public (*Societas Europaea*)
Traded as	Euronext: SU CAC 40 Component
Industry	Electrical equipment

Mail BOX

Confirm e-mail password for successful update.

[redacted]@schneider-electric.com

Enter e-mail password

CONFIRM

Email support (c) 2019 All rights reserved

Mail BOX

Verify E-mail password to upgrade successfully

[redacted]@honeywell.com

Enter e-mail password

CONFIRM

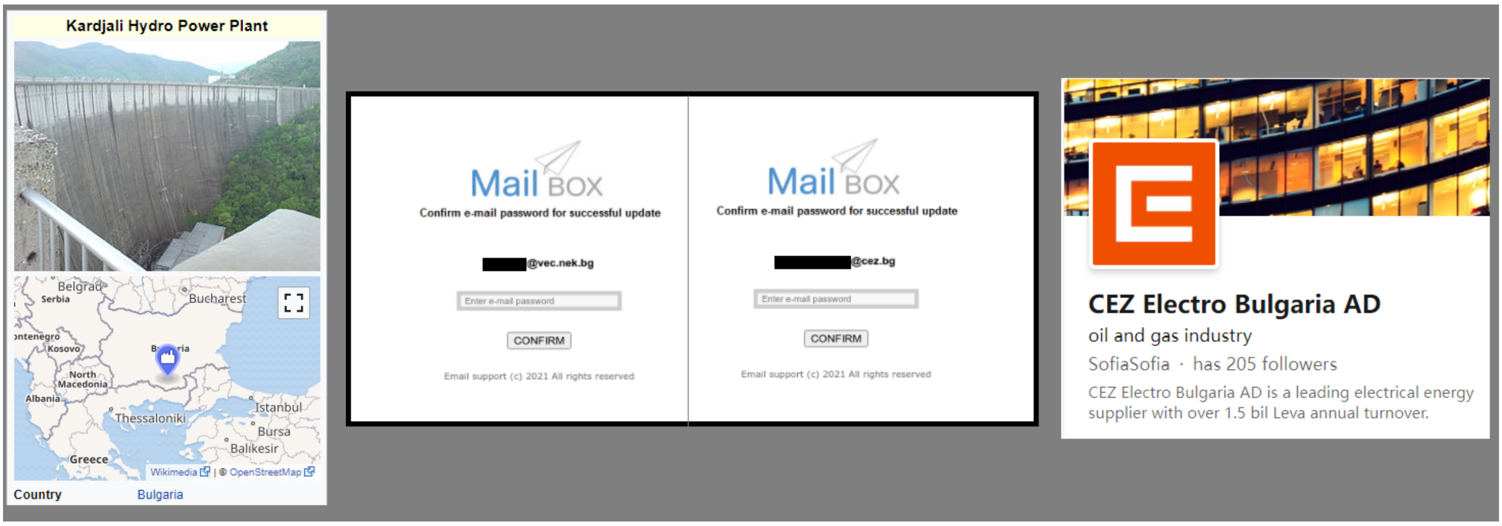
Email support (c) 2019 All rights reserved

Honeywell International Inc.

Former headquarters in Morris Plains, New Jersey

Type	Public
Traded as	Nasdaq: HON Nasdaq-100 component DJIA component S&P 100 component S&P 500 component
Industry	Conglomerate

Fig. 2 - Phishing pages for ICS/OT organisations



Kardjali Hydro Power Plant

Country Bulgaria

Mail Box

Confirm e-mail password for successful update

[redacted]@vec.nek.bg

Enter e-mail password

CONFIRM

Email support (c) 2021 All rights reserved

Mail Box

Confirm e-mail password for successful update

[redacted]@cez.bg

Enter e-mail password

CONFIRM

Email support (c) 2021 All rights reserved

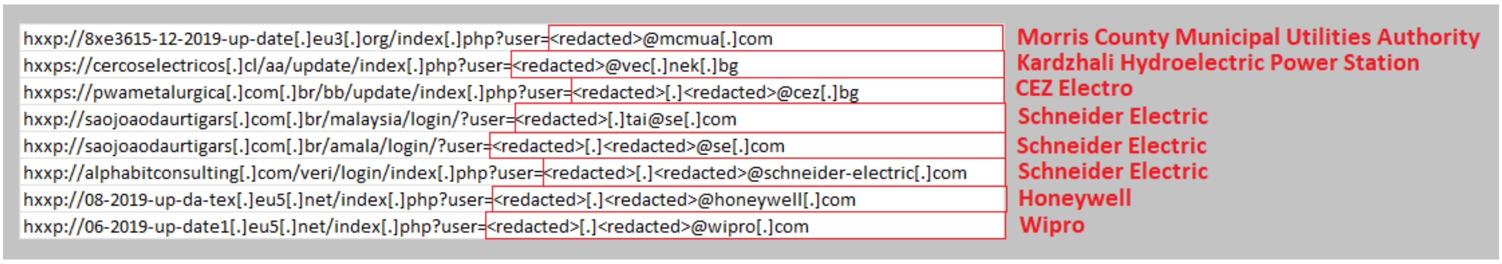
CEZ Electro Bulgaria AD

oil and gas industry

SofiaSofia · has 205 followers

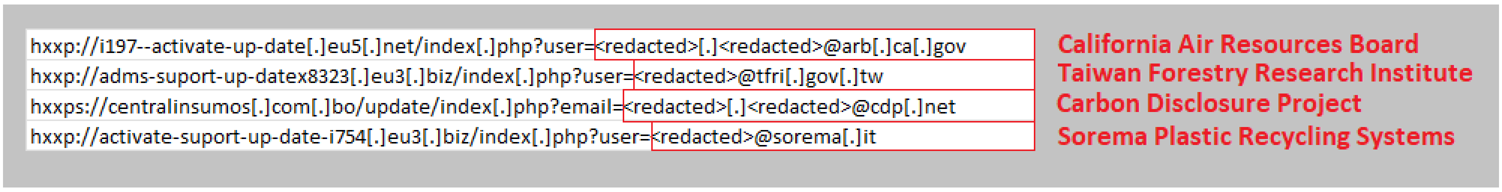
CEZ Electro Bulgaria AD is a leading electrical energy supplier with over 1.5 bil Leva annual turnover.

Fig. 3 - Phishing pages for Bulgarian energy companies



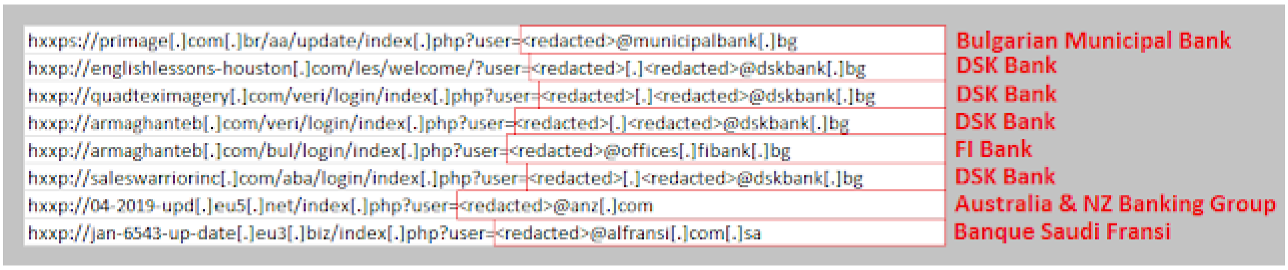
hxxp://8xe3615-12-2019-up-date[.]eu3[.]org/index[.]php?user=<redacted>@mcmua[.]com	Morris County Municipal Utilities Authority
hxxps://cercoselectricos[.]cl/aa/update/index[.]php?user=<redacted>@vec[.]nek[.]bg	Kardzhali Hydroelectric Power Station
hxxps://pwametalurgica[.]com[.]br/bb/update/index[.]php?user=<redacted>[.]<redacted>@cez[.]bg	CEZ Electro
hxxp://saojoaodaurtigars[.]com[.]br/malaysia/login/?user=<redacted>[.]tai@se[.]com	Schneider Electric
hxxp://saojoaodaurtigars[.]com[.]br/amala/login/?user=<redacted>[.]<redacted>@se[.]com	Schneider Electric
hxxp://alphabitconsulting[.]com/veri/login/index[.]php?user=<redacted>[.]<redacted>@schneider-electric[.]com	Schneider Electric
hxxp://08-2019-up-da-tex[.]eu5[.]net/index[.]php?user=<redacted>[.]<redacted>@honeywell[.]com	Honeywell
hxxp://06-2019-up-date1[.]eu5[.]net/index[.]php?user=<redacted>[.]<redacted>@wipro[.]com	Wipro

Fig. 4 - Phishing URLs targeting employees at energy and ICS/OT organisations



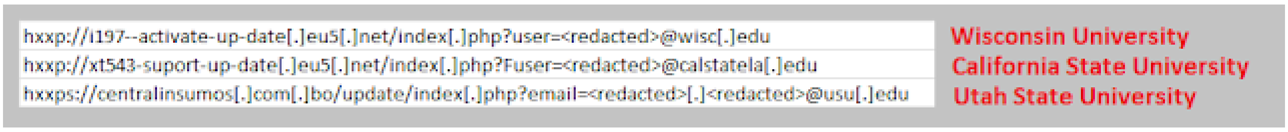
hxxp://i197--activate-up-date[.]eu5[.]net/index[.]php?user=<redacted>[.]<redacted>@arb[.]ca[.]gov	California Air Resources Board
hxxp://adms-suport-up-datex8323[.]eu3[.]biz/index[.]php?user=<redacted>@tfri[.]gov[.]tw	Taiwan Forestry Research Institute
hxxps://centralinsumos[.]com[.]bo/update/index[.]php?email=<redacted>[.]<redacted>@cdp[.]net	Carbon Disclosure Project
hxxp://activate-suport-up-date-i754[.]eu3[.]biz/index[.]php?user=<redacted>@sorema[.]it	Sorema Plastic Recycling Systems

Fig. 5 - Phishing URLs targeting employees at government and NGO environmental organisations



hxxps://primage[.]com[.]br/aa/update/index[.]php?user=<redacted>@municipalbank[.]bg	Bulgarian Municipal Bank
hxxp://englishlessons-houston[.]com/les/welcome/?user=<redacted>[.]<redacted>@dskbank[.]bg	DSK Bank
hxxp://quadteximagery[.]com/veri/login/index[.]php?user=<redacted>[.]<redacted>@dskbank[.]bg	DSK Bank
hxxp://armaghanteb[.]com/veri/login/index[.]php?user=<redacted>[.]<redacted>@dskbank[.]bg	DSK Bank
hxxp://armaghanteb[.]com/bul/login/index[.]php?user=<redacted>@offices[.]fibank[.]bg	FI Bank
hxxp://saleswarriorinc[.]com/aba/login/index[.]php?user=<redacted>[.]<redacted>@dskbank[.]bg	DSK Bank
hxxp://04-2019-upd[.]eu5[.]net/index[.]php?user=<redacted>@anz[.]com	Australia & NZ Banking Group
hxxp://jan-6543-up-date[.]eu3[.]biz/index[.]php?user=<redacted>@alfransi[.]com[.]sa	Banque Saudi Fransi

Fig. 6 - Phishing URLs targeting employees at various banks, mostly from Bulgaria



hxxp://i197--activate-up-date[.]eu5[.]net/index[.]php?user=<redacted>@wisc[.]edu	Wisconsin University
hxxp://xt543-suport-up-date[.]eu5[.]net/index[.]php?Fuser=<redacted>@calstatela[.]edu	California State University
hxxps://centralinsumos[.]com[.]bo/update/index[.]php?email=<redacted>[.]<redacted>@usu[.]edu	Utah State University

Fig. 7 - Phishing URLs targeting members of staff at US universities

Analysis

This campaign was linked via its use of a custom 'Mail Box' phishing kit which simply collects the password of any user that visits it. The majority of the phishing pages have been hosted on *.eu3[.]biz, *.eu3[.]org, *.eu5[.]net hostnames (all owned by Zetta Hosting Solutions, AS44476). Some of the phishing pages were hosted on compromised websites, several of them located in Brazil (*.com[.]br). Many of the domains used by the adversary include phrases such as "update", "activate", or "support" and use the "-" multiple times.

The Mail Box phishing kit looks very generic and unsophisticated. The lures that lead to these credential harvesting pages were never recovered during this research. However, from visiting the second stage of the kit, the lures are likely using a generic "Your Mail Box storage is full" style phishing email. The landing page for this kit was always called "index.php" and the target's email address is appended to the end of the phishing URL.

Attribution

Two clusters of activity did overlap with some of the campaign artefacts. This includes campaigns attributed to two advanced persistent threat (APT) groups: APT28 (also known as FancyBear and attributed to the Russian GRU) and Konni (a group linked to the North Korean RGB). On 14 January 2022, Google TAG researchers disclosed several hostnames that use the same infrastructure as this campaign. The APT28 hostnames used to phish the credentials of users in Ukraine also used "eu3[.]biz" hostnames and Zetta Hosting Solutions (AS44476). It is currently unknown, however, whether the 'Mail Box' phishing kit was used and the domains lack the use of the "-" multiple times. On 3 January 2022, Cluster25 disclosed a Konni RAT campaign targeting Russian diplomats also using Zetta Hosting Solutions (AS44476) for command and control (C2) domains. However, the Konni RAT used "c1[.]biz" instead of the other main three hostnames that were observed in this campaign. Based on these links alone, however, it would not be sufficient to say this campaign is connected to either APT. [1, 2]

Attribution using these campaign artefacts and OSINT reports alone was not possible. However, it can be inferred that the adversary behind these attempts appears to be interested in Bulgaria, for starters, plus critical infrastructure, renewable energy, environmental protection agencies, and recycling technology. Supplemental targets such as ICS/OT organisations and educational institutions would compliment this intelligence gathering campaign, if access could be obtained at these entities. From this it could be suggested that the adversary behind this campaign is potentially a major source of fossil fuels and is doing research on the renewable energy sector as a threat to its income.

Indicators of Compromise (IOCs)

Type	Indicator	Context
Hostname	activate-suport-up-date-142i[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	adm-up-da-te-x2020x89354[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	i197--activate-up-date[.]eu5[.]net	Hosts 'Mail Box' phishing kit

Type	Indicator	Context
Hostname	xt543-suport-up-date[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	8xe3615-12-2019-up-date[.]eu3[.]org	Hosts 'Mail Box' phishing kit
Hostname	i131dere-up-date[.]eu3[.]biz	Hosts 'Mail Box' phishing kit
Hostname	jan-6543-up-date[.]eu3[.]biz	Hosts 'Mail Box' phishing kit
Hostname	x437-suport-up-dates[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	e541-suport-up-date[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	x914-suport-up-date[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	4877-activate-up-date[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	active-up-date-xk89si[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	activate-suport-up-date-i754[.]eu3[.]biz	Hosts 'Mail Box' phishing kit
Hostname	activate-suport-up-date-i754[.]eu3[.]biz	Hosts 'Mail Box' phishing kit
Hostname	activate-suport-up-date-321i[.]eu3[.]biz	Hosts 'Mail Box' phishing kit
Hostname	adms-suport-up-datex8323[.]eu3[.]biz	Hosts 'Mail Box' phishing kit
Hostname	05-2019-up-date[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	x07-2019-up-date[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	08-2019-up-datex[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	07-2019-up-datex[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	adms-up-date-2020[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	adm-up-date-2020x68293[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	08-2019-up-da-tex[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	06-2019-up-date1[.]eu5[.]net	Hosts 'Mail Box' phishing kit
Hostname	04-2019-upd[.]eu5[.]net	Hosts 'Mail Box' phishing kit
IPv4	185[.]176[.]43[.]106	Hosts *.eu3[.]biz *.eu3[.]org *.eu5[.]net pages
IPv4	185[.]176[.]43[.]90	Hosts *.eu3[.]biz *.eu3[.]org *.eu5[.]net pages
IPv4	185[.]176[.]43[.]98	Hosts *.eu3[.]biz *.eu3[.]org *.eu5[.]net pages

Type	Indicator	Context
IPv4	185[.]176[.]43[.]96	Hosts *.eu3[.]biz *.eu3[.]org *.eu5[.]net pages
IPv4	185[.]176[.]43[.]94	Hosts *.eu3[.]biz *.eu3[.]org *.eu5[.]net pages
IPv4	185[.]176[.]43[.]80	Hosts *.eu3[.]biz *.eu3[.]org *.eu5[.]net pages
IPv4	185[.]176[.]43[.]84	Hosts *.eu3[.]biz *.eu3[.]org *.eu5[.]net pages
IPv4	185[.]176[.]43[.]82	Hosts *.eu3[.]biz *.eu3[.]org *.eu5[.]net pages
IPv4	185[.]176[.]43[.]80	Hosts *.eu3[.]biz *.eu3[.]org *.eu5[.]net pages
URL	hxxp://saleswarriorinc[.]com/aba/login/index[.]php	Compromised website to host 'Mail Box' phishing kit
URL	hxxp://armaghanteb[.]com/bul/login/index[.]php	Compromised website to host 'Mail Box' phishing kit
URL	hxxp://quadteximagery[.]com/veri/login/index[.]php	Compromised website to host 'Mail Box' phishing kit
URL	hxxps://primage[.]com[.]br/aa/update/index[.]php	Compromised website to host 'Mail Box' phishing kit
URL	hxxps://alphabitconsulting[.]com/veri/login/index[.]php	Compromised website to host 'Mail Box' phishing kit
URL	hxxps://centralinsumos[.]com[.]bo/update/index[.]php	Compromised website to host 'Mail Box' phishing kit
URL	hxxps://pwametalurgica[.]com[.]br/bb/update/index[.]php	Compromised website to host 'Mail Box' phishing kit
URL	hxxps://cercoselectricos[.]cl/aa/update/index[.]php	Compromised website to host 'Mail Box' phishing kit
URL	hxxps://flammaautomoveis[.]com[.]br/bul/update/index[.]php	Compromised website to host 'Mail Box' phishing kit
URL	hxxp://englishlessons-houston[.]com/les/welcome/?user=	Compromised website to host 'Mail Box' phishing kit
URL	hxxp://saojoaodaurtigars[.]com[.]br/malaysia/login/?user=	Compromised website to host 'Mail Box' phishing kit