Cyber espionage campaign targets renewable energy companies

bleepingcomputer.com/news/security/cyber-espionage-campaign-targets-renewable-energy-companies

Bill Toulas

- January 17, 2022

A large-scale cyber-espionage campaign targeting primarily renewable energy and industrial technology organizations have been discovered to be active since at least 2019, targeting over fifteen entities worldwide.

The campaign was discovered by security researcher William Thomas, a Curated Intelligence trust group member, who employed OSINT (open-source intelligence) techniques like DNS scans and public sandbox submissions.

Thomas' analysis revealed that the attacker uses a custom 'Mail Box' toolkit, an unsophisticated phishing package deployed on the actors' infrastructure, as well as legitimate websites compromised to host phishing pages.

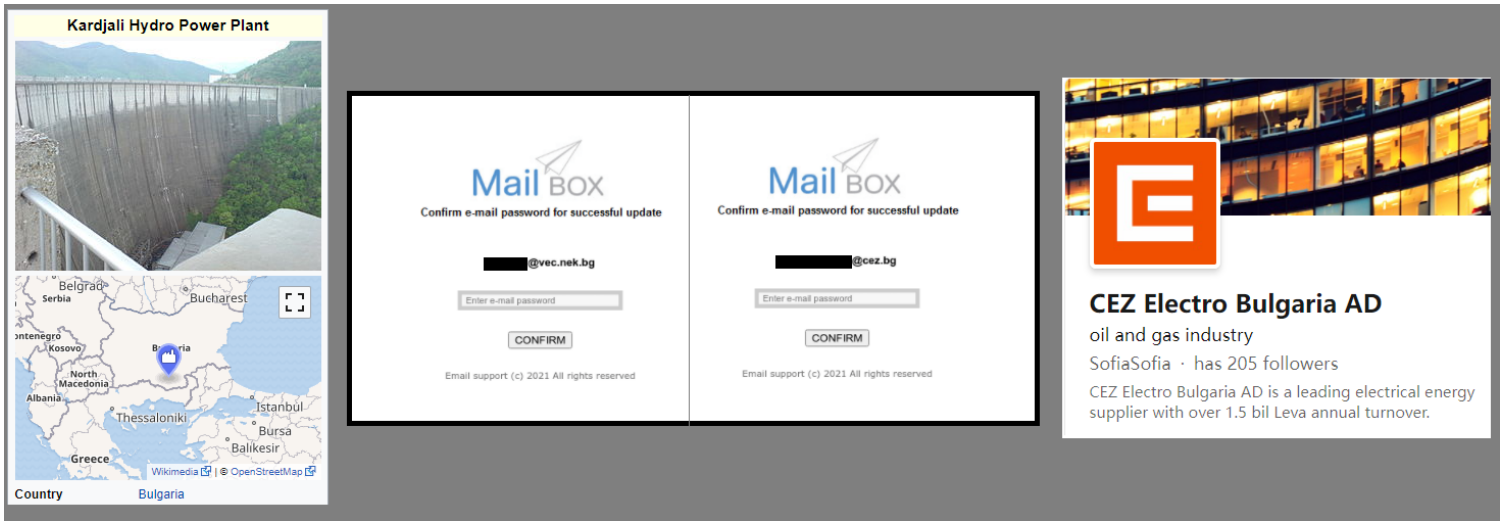
Most of the phishing pages were hosted on "*.eu3[.]biz", "*.eu3[.]org", and "*.eu5[.]net" domains, while the majority of the compromised sites are located in Brazil ("*.com[.]br").

Targeting the renewable energy sector

The phishing campaign's goal is to steal the login credentials of those working for renewable energy firms, environmental protection organizations, and industrial technology in general.

Examples of organizations targeted by the phishing attacks include:

- Schneider Electric
- Honeywell
- Huawei
- HiSilicon
- Telekom Romania
- University of Wisconsin
- California State University
- Utah State University
- Kardzhali Hydroelectric Power Station (Bulgaria)
- CEZ Electro (Bulgaria)
- California Air Resources Board
- Morris County Municipal Utilities Authority
- Taiwan Forestry Research Institute
- Carbon Disclosure Program
- Sorema (Italian recycling firm)



Phishing sites set up for stealing employee credentials
Source: blog.bushidotoken.net

The researcher couldn't retrieve any samples of the phishing emails used in the campaign, but Thomas believes the emails used a "Your Mail Box storage is full" lure based on the landing pages.

Unknown actor

Thomas couldn't attribute this campaign to any specific actors, but evidence points to two clusters of activity, one from APT28 (aka FancyBear) and one from Konni (North Korea actors).

Google Threat Analysis Group researchers have recently found phishing activity attributed to APT28, which uses several "eu3[.]biz" domains.

> Since mid-Dec, @Google TAG has detected ongoing APT28 cred phishing campaigns targeting Ukraine. Some IOCs:
>
> consumerpanel.eu3[.]biz
> consumerpanel.eu3[.]org
> consumerspanelsrv.eu3[.]org
> protectpanel.eu3[.]biz
> updateservicecenter.blogspot[.]com
>
> — billy leonard (@billyleonard) January 14, 2022

An overlap point for both groups is that the hostnames used for phishing credentials are owned by Zetta Hosting Solutions, a name that has appeared in many analyst reports recently.

"Konni" used Zetta Hosting Solution domains in the Diplomat-targeting campaign uncovered by Cluster25, and also in a T406 (Korean hackers) campaign analyzed by Proofpoint.

Thomas explained to BleepingComputer that many APT hacking groups use Zetta in malicious campaigns.

> "Zetta is used a lot by APTs and malware, and I'd be very surprised if they didn't know. They're not a huge company. Threat actors also like these types of free hostname services where they can setup infrastructure quickly, freely, and anonymously." - Thomas.

However, the researcher underlined that he doesn't have proof or concrete evidence that Zetta Hosting is knowingly helping malicious campaigns.

Focus on Bulgaria and potential motive

Apart from the two entities mentioned in the victimology section above, the researcher has noticed a small cluster of activity from 2019 linked to the same infrastructure targeting multiple Bulgarian banks.

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

Phishing URLs targeting Bulgarian banks
Source: blog.bushidotoken.net

The researcher believes that the adversary is financially supported by entities interested in fossil fuels, particularly someone selling energy to Bulgaria who sees renewables as a threat.

The previous targeting of banks could be an attempt to gather intelligence on the funding and construction of new renewable energy facilities.

APT28 is a Russian group linked to the state, and Bulgaria is known to import significant amounts of Russian natural gas, so the link between this campaign and the particular actors has a logical basis, even if it's not proven at this point.