Strictly Confidential

# Beyond Sunset: Exposing the Occultations Lurking in Large-Scale Off-Grid Solar Systems

Bitdefender Cyber Threat Intelligence
Lab
DEF CON 32
2024

# Intro

- Green energy is at the forefront of transforming the global energy landscape
- 520 GW added just in 2023 with solar making up three quarters of it
- Both businesses and consumers install solar panels at an increasing rate
- Growing number of systems -> attractive targets
- Capacity increases but is their security keeping up?
- We investigated a manufacturer (X) and a management platform (Y) to find out

# Why X/Y?

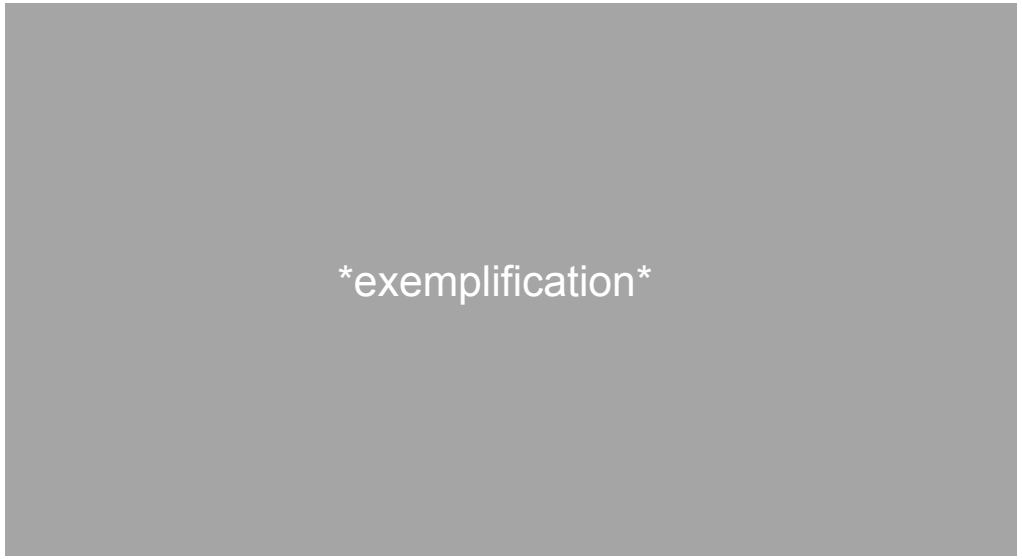
- Smart system – can be controlled over the internet
- Someone in the office noticed something strange after installation
- Inverter could be added on both (X) and (Y) apps
- Just the serial number required
- This warranted a closer look

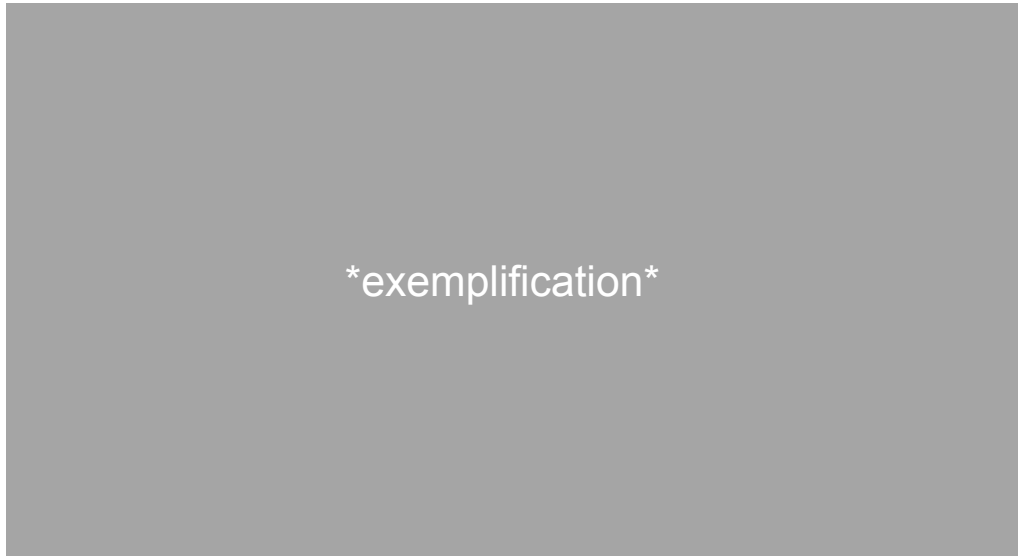
*Architecture diagram*

- Logger is a bridge between inverter/panels/battery and the online platform
- Responsible for settings, data collection, updates
- Users can control the system from the internet (platform) or from the local network by talking directly with the logger

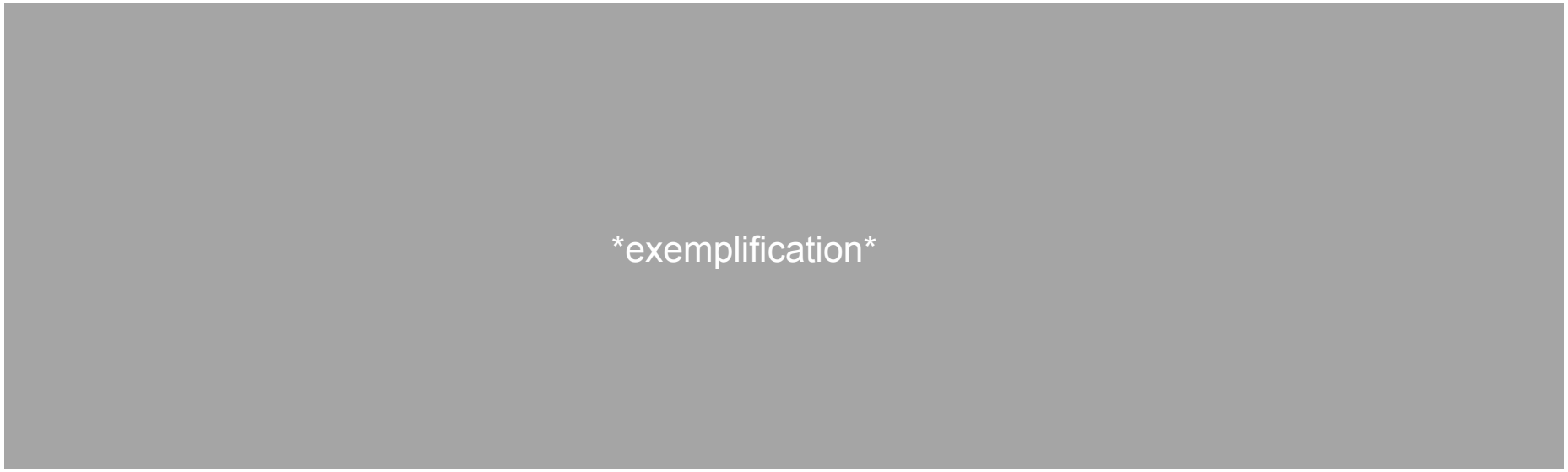
# Investigating the platform

- started by intercepting requests made by the (Y) Cloud app
- found a suspicious login request using hardcoded credentials



- The account is used to get info about the user’s devices.
- It obtains the model, version and **password** for a serial number.




- The account can get this info for ANY device if the serial number is known.

# Attack scenario

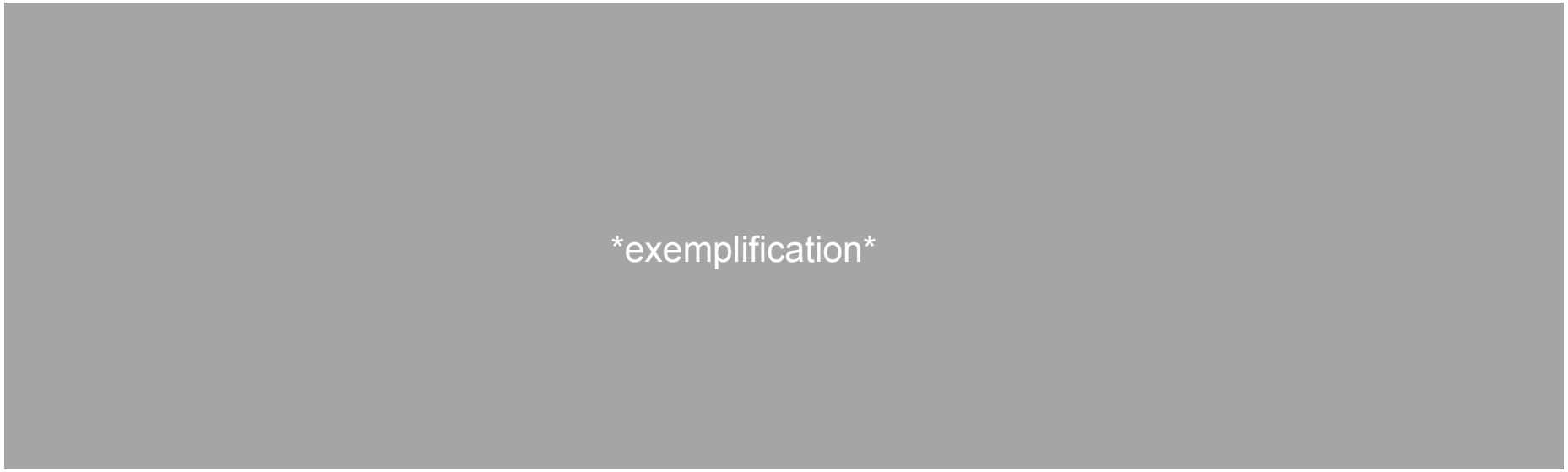
- Find an access point corresponding to a logger (convenient format)
- Get serial number and use the hardcoded account to get password
- ???
- Profit?

Downsides:

- the attack requires physical proximity to the device
- the physical proximity must be maintained
- hacking only one device at a time

# Other platform features

- Users can invite other accounts to manage their system.
- The guest can be either another user or a business account.
- The search API returns data about all users and organizations.
- E-mails, phone numbers, addresses, user IDs



*exemplification*

*exemplification*

*exemplification*

- Privacy issue but not really exploitable by itself.
- Ballpark for number of users and businesses
- The user IDs and e-mails might be useful later

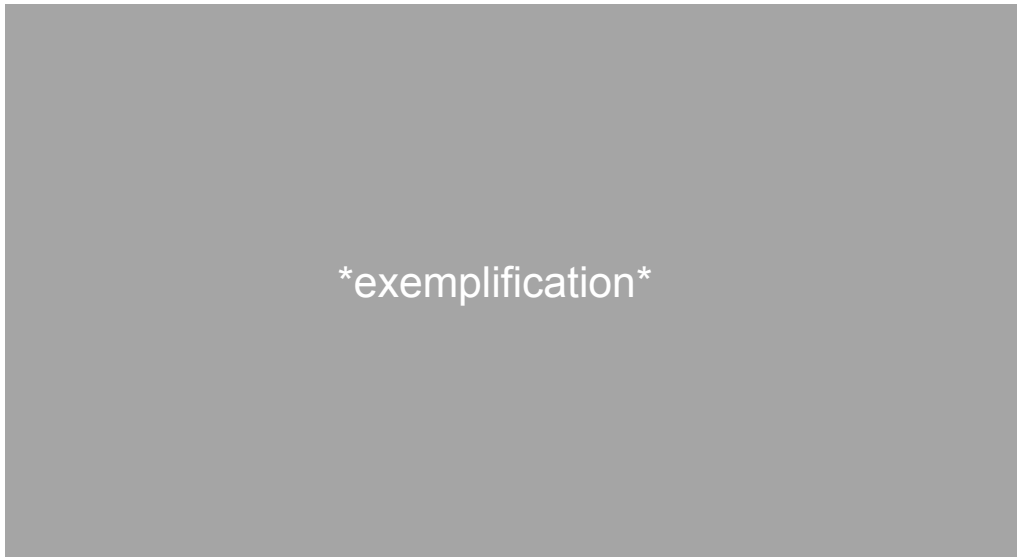
Strictly Confidential

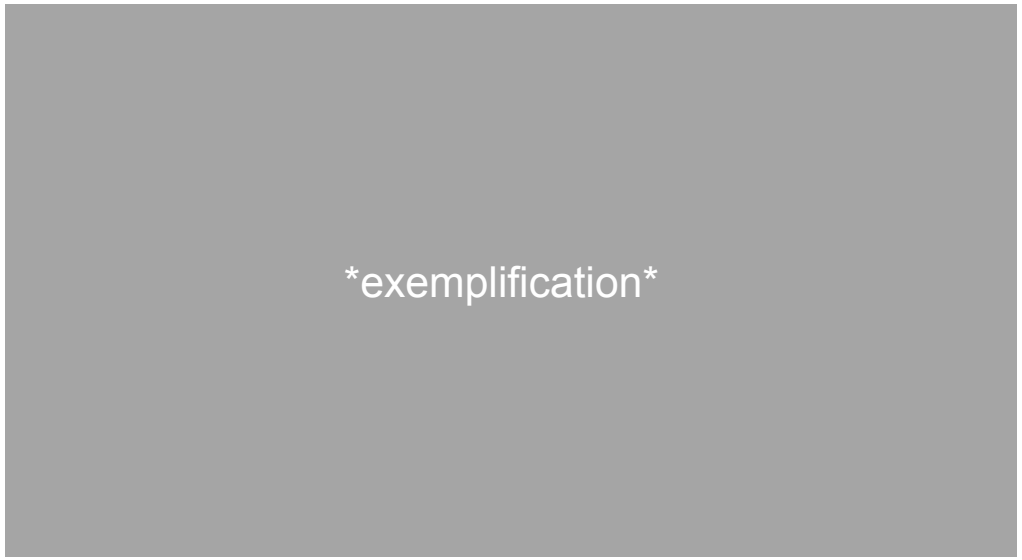
- Similar platform between (X) and (Y)
- (Y) recently built its own data center
- Users migrated but the code might still be the same
- Just how similar is the backend?

- Similar enough for a JWT token from (Y) to work on (X)
- Grants access to the account with the same user ID
- Incremental user IDs:
- ~ZZZZZZZZ on (X)
- ~ZZZZZZZZ on (Z)
- ZZZZZZZ accounts risking takeover



- JWT tokens are used for authorization but how are they obtained?
- Straight-forward for normal users

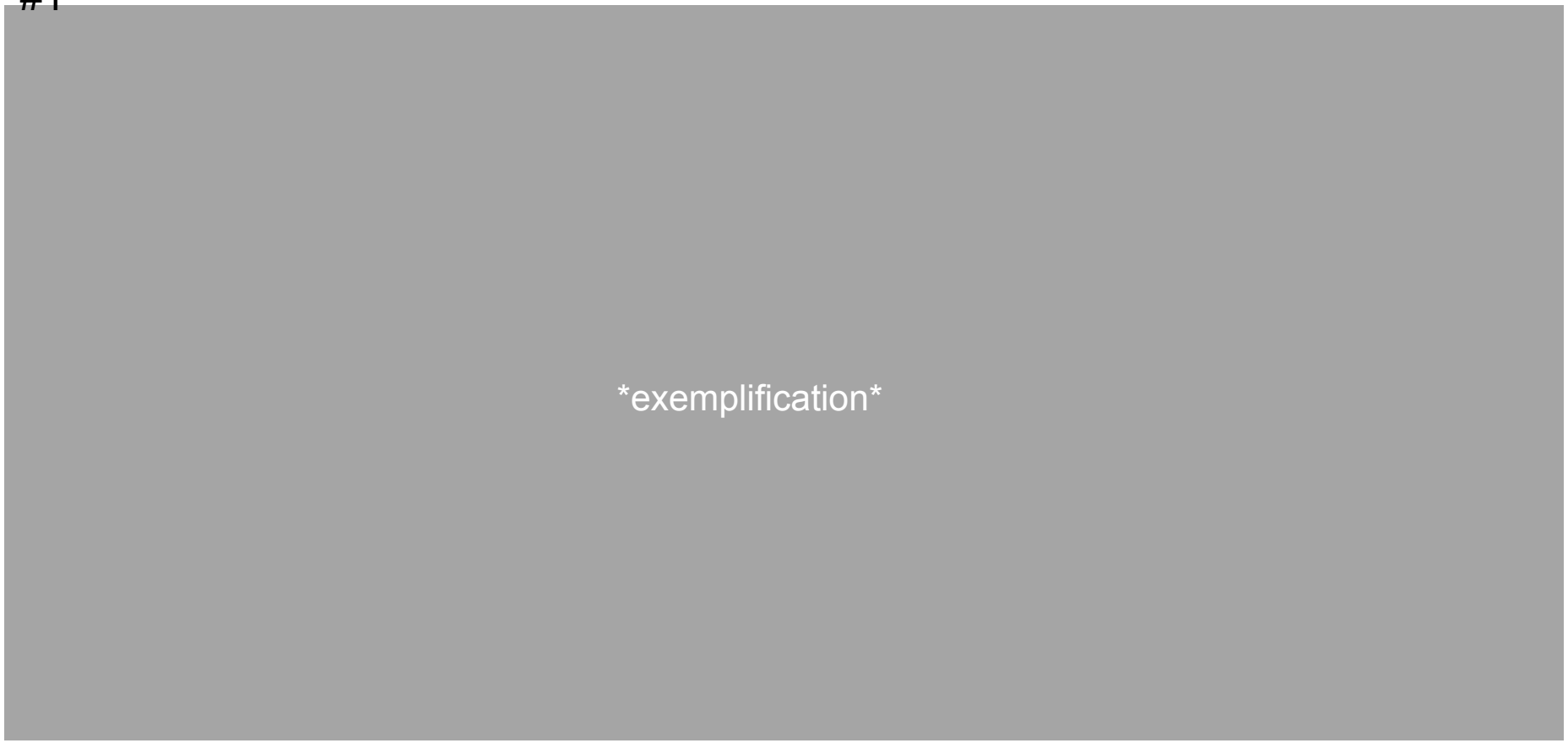


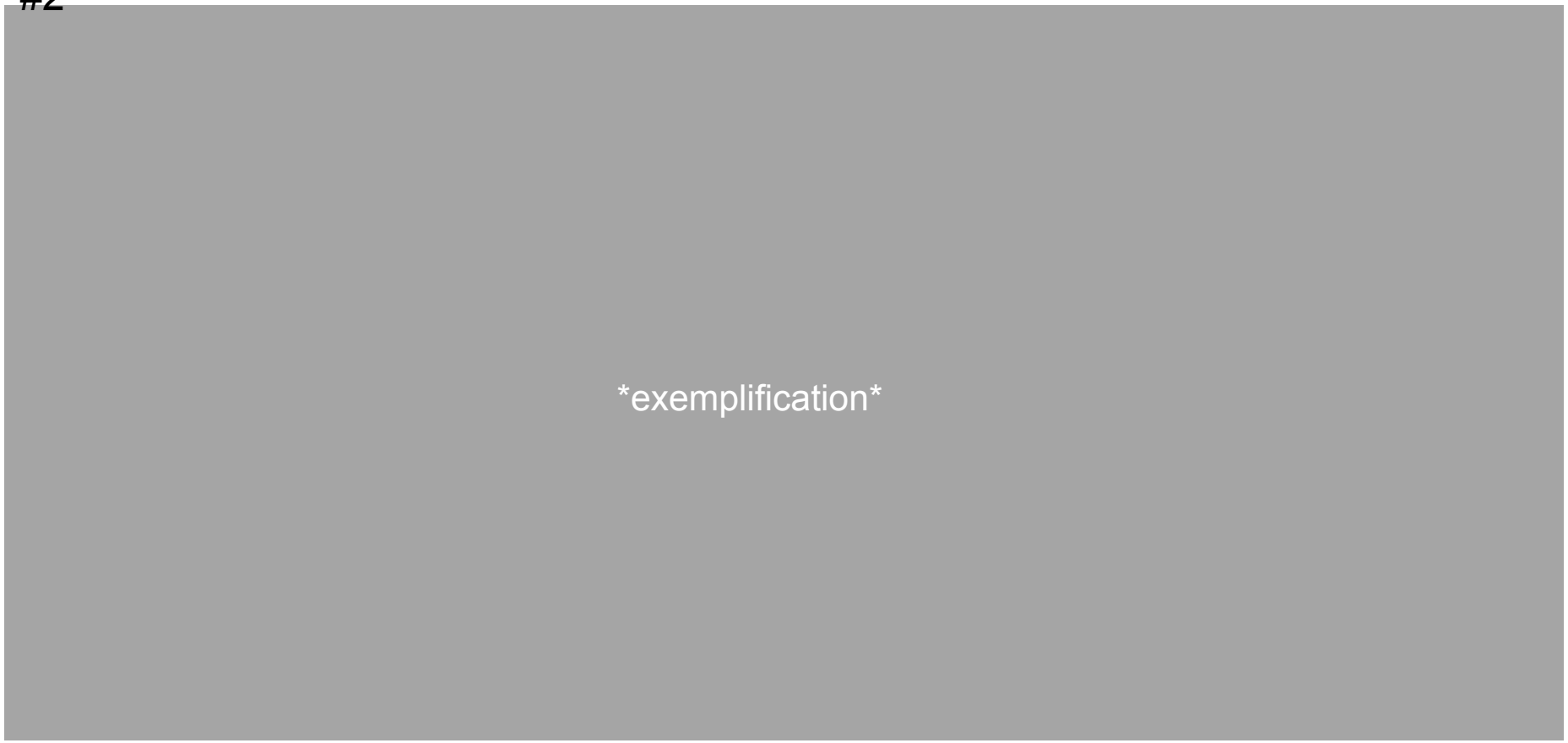
- There is a twist for a business account.
- Multiple organizations can be managed from the same account.
- Each organization requires a token with different parameters.
- After login the business account selects the organization and the token is created.

*exemplification*

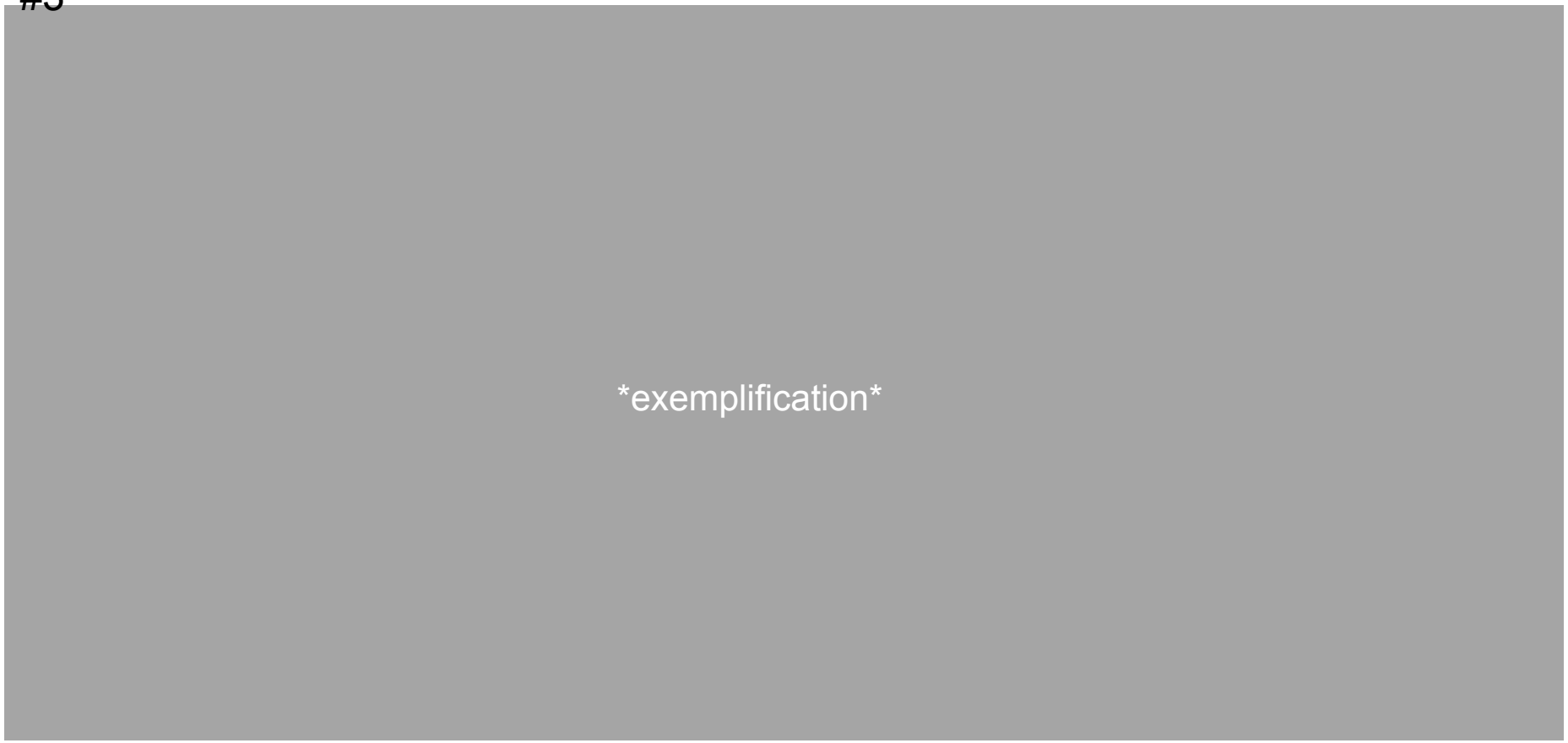
Login steps.
#1



# Login steps.
# #2



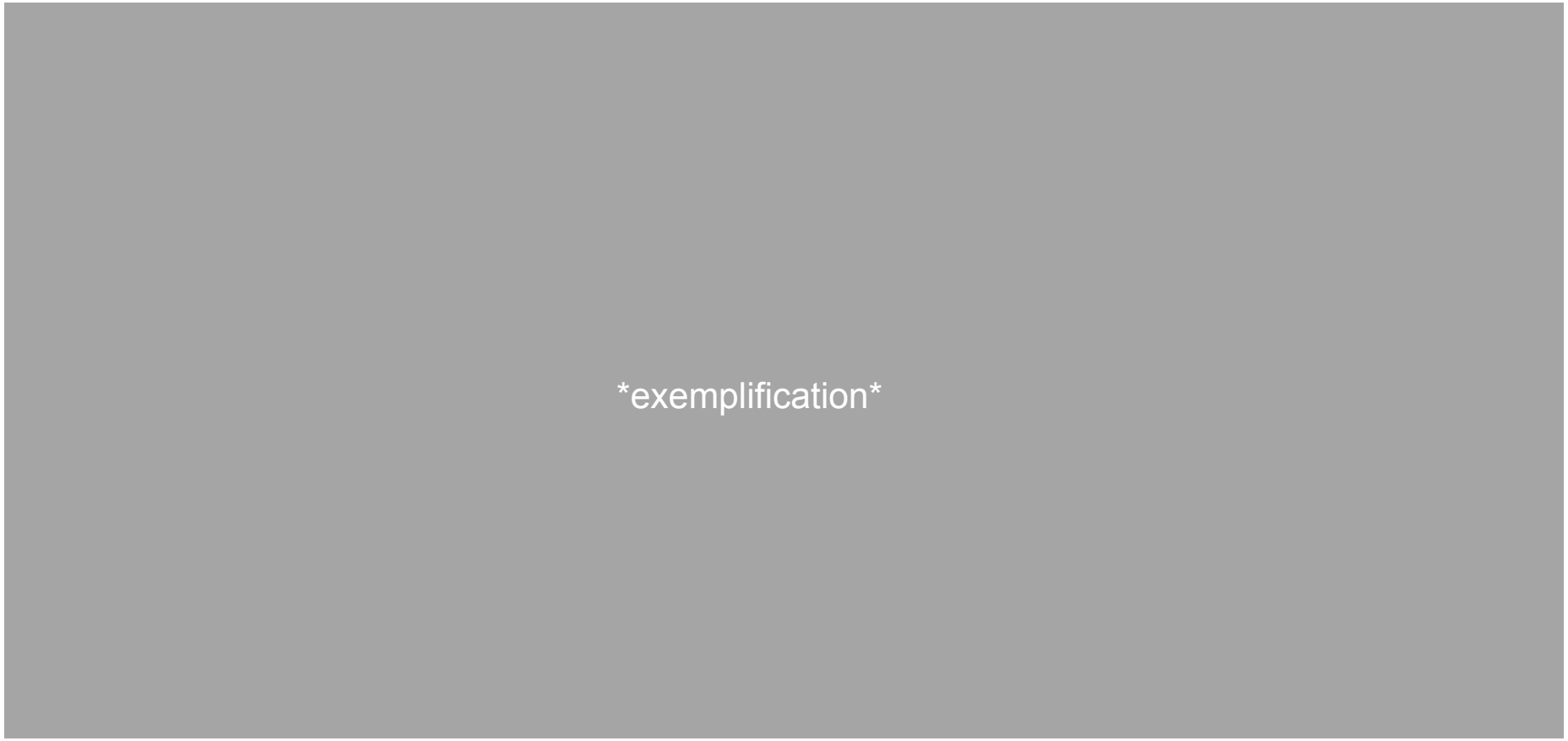
# Login steps.
# #3



# The issue

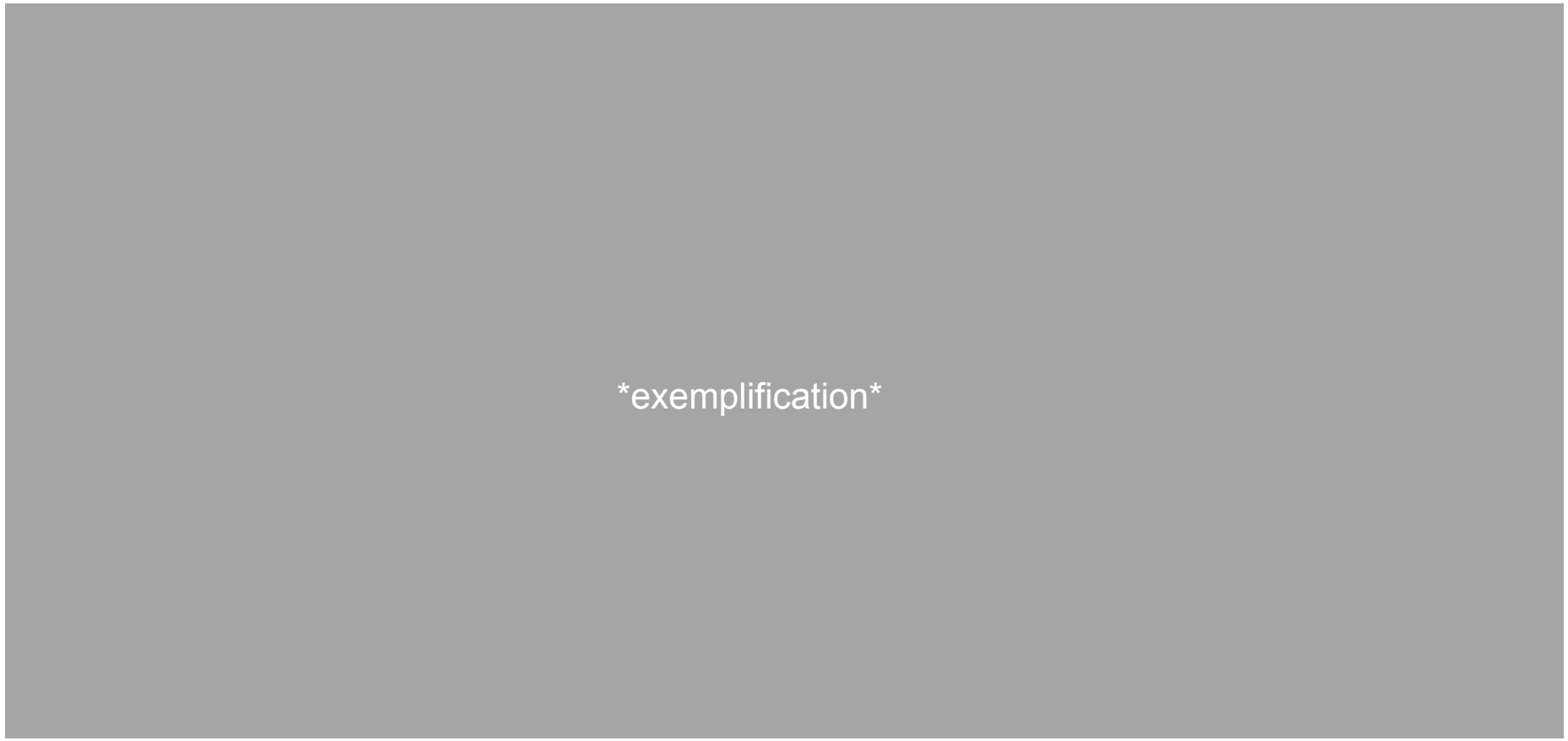
- In the third step the endpoint uses the data from the sent token to create a new token.
- We tried changing the user_ID and e-mail in the sent token (*additional details)
- It worked!
- No signature checks, no errors, didn’t even need “alg:none” (Not today https://www.howmanydayssinceajwtalgnonevuln.com/)
- The endpoint could have been used even without the authorization header

*exemplification*




- Remember the id-email combo mentioned earlier?
- This time all (Z mil) accounts were risking takeover

# Impact



# Impact

- Z million users and Z thousand business that might control multiple systems
- Rough location of the users can be obtained through the info disclosure
- Voltage oscillations with a sufficient number of inverters could damage the grid

Disclaimer! We didn’t do anything stupid; this is purely speculation

# Timeline

# Questions

Strictly Confidential

# Bitdefender Cyber Threat Intelligence Lab
# DEF CON 32
# 2024