MANDIANT

Schrödinger's Hack: Are Hacktivist Operations Placing Operational Technology at Risk?

Daniel Kapellmann Zafra

Technical Analysis Manager
Kapellmann@google.com
@Kapellmann
www.kapell.tech

Photo: Anonymous V for Vendetta Guy Fawkes Costume Halloween Mask by Marco Verch under Creative Commons 2.0

Photo by Daniele Franchi on Unsplash

Is there a hack in the box?

Icon from Flaticon.com

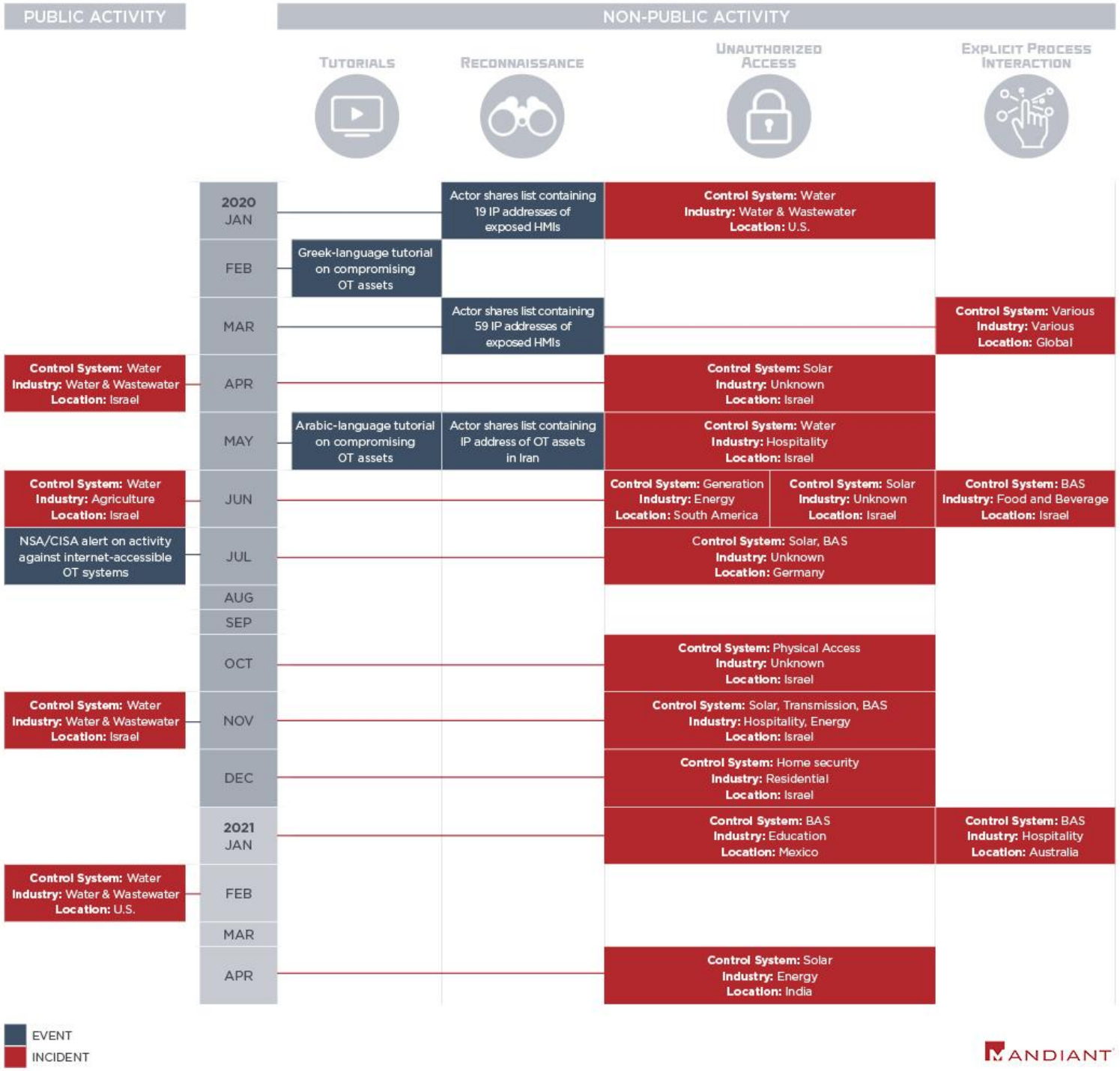
Photo by Brandable Box on Unsplash

MANDIANT®

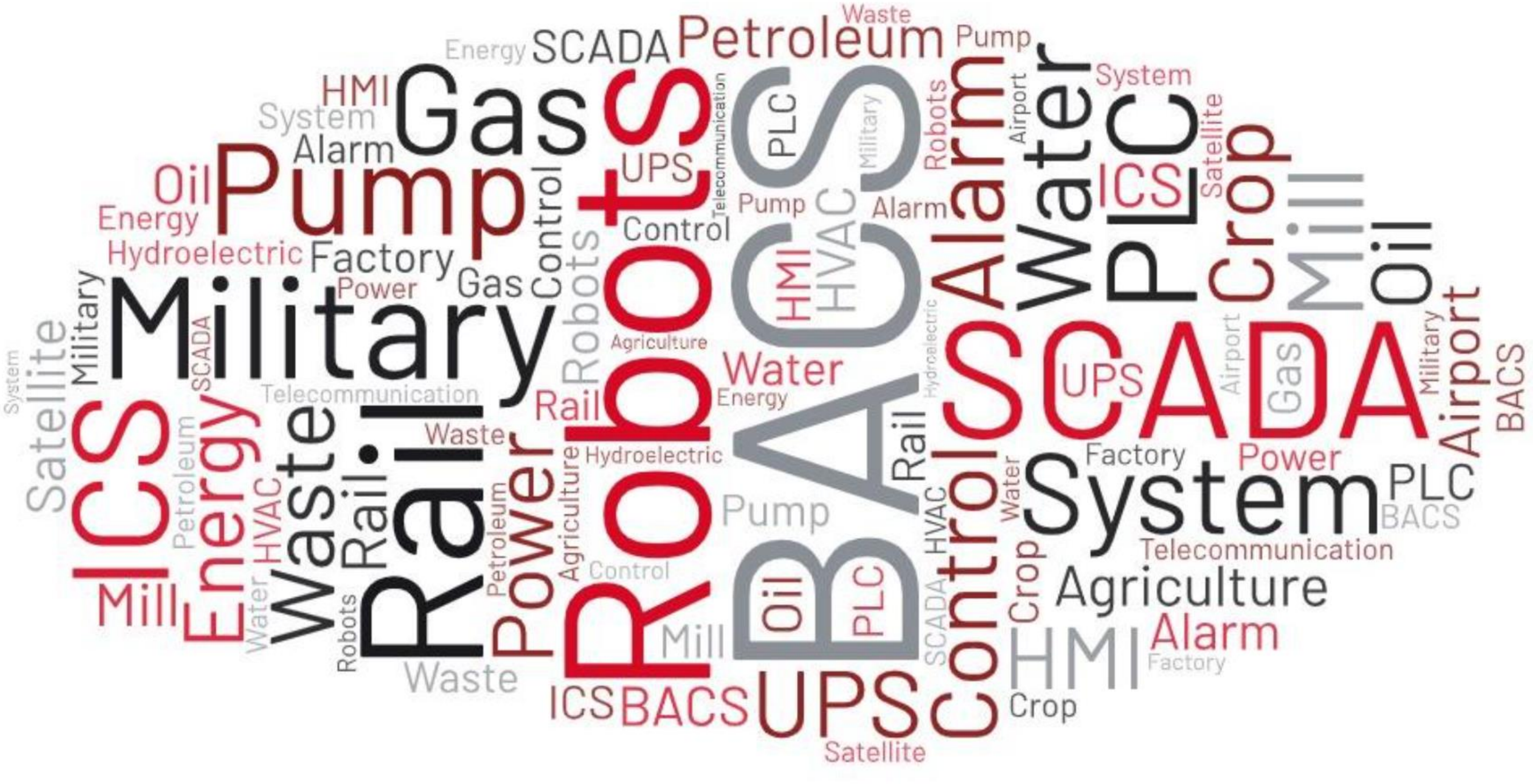
Hacktivists Increasingly Claim to Target OT

Timeline 2020

- Low sophistication attacks
- Attacks vs. unsecure OT assets
- Actors interacted with OT processes
- Some hacktivist tutorials



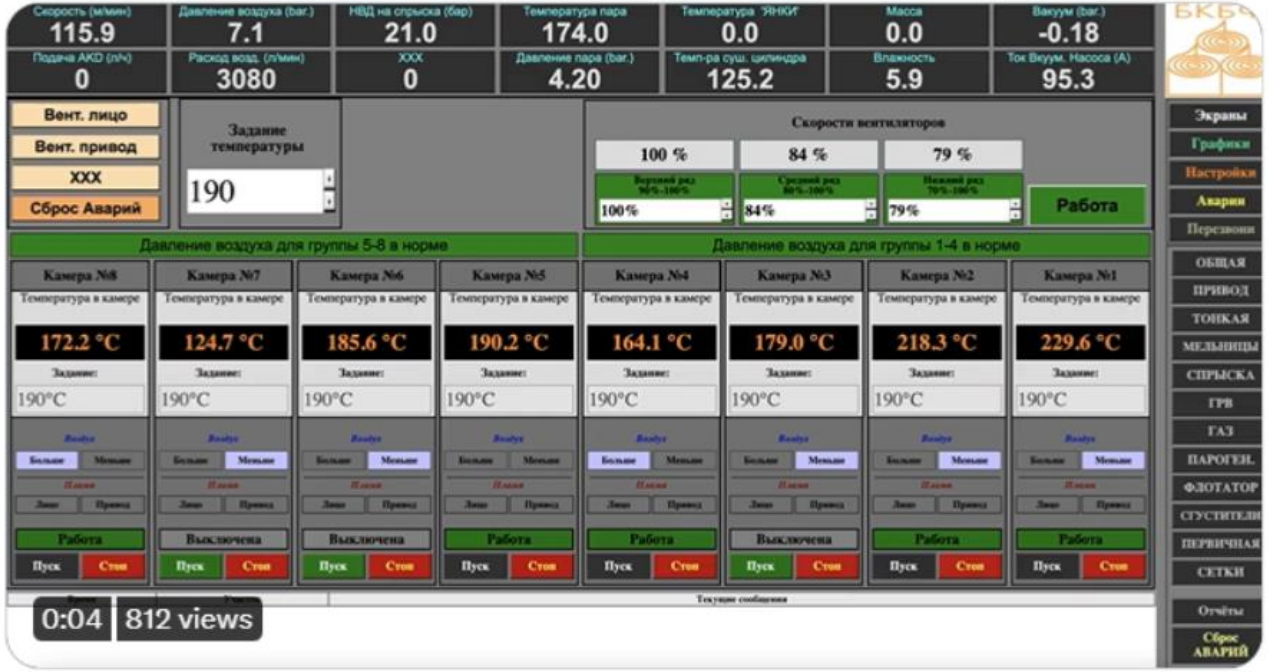
2022... The Return of Hacktivism



Note: Hacktivist Claims?

The attack was carefully planned and executed when the plant was first turn-on in the morning. 😉 The Orcs fought back, but they failed in the end as we destroyed the backup database and corrupted the primary. 30 hours later it is still gone. ✊🇺🇦 #StandWithUkraine #TeamOneFist

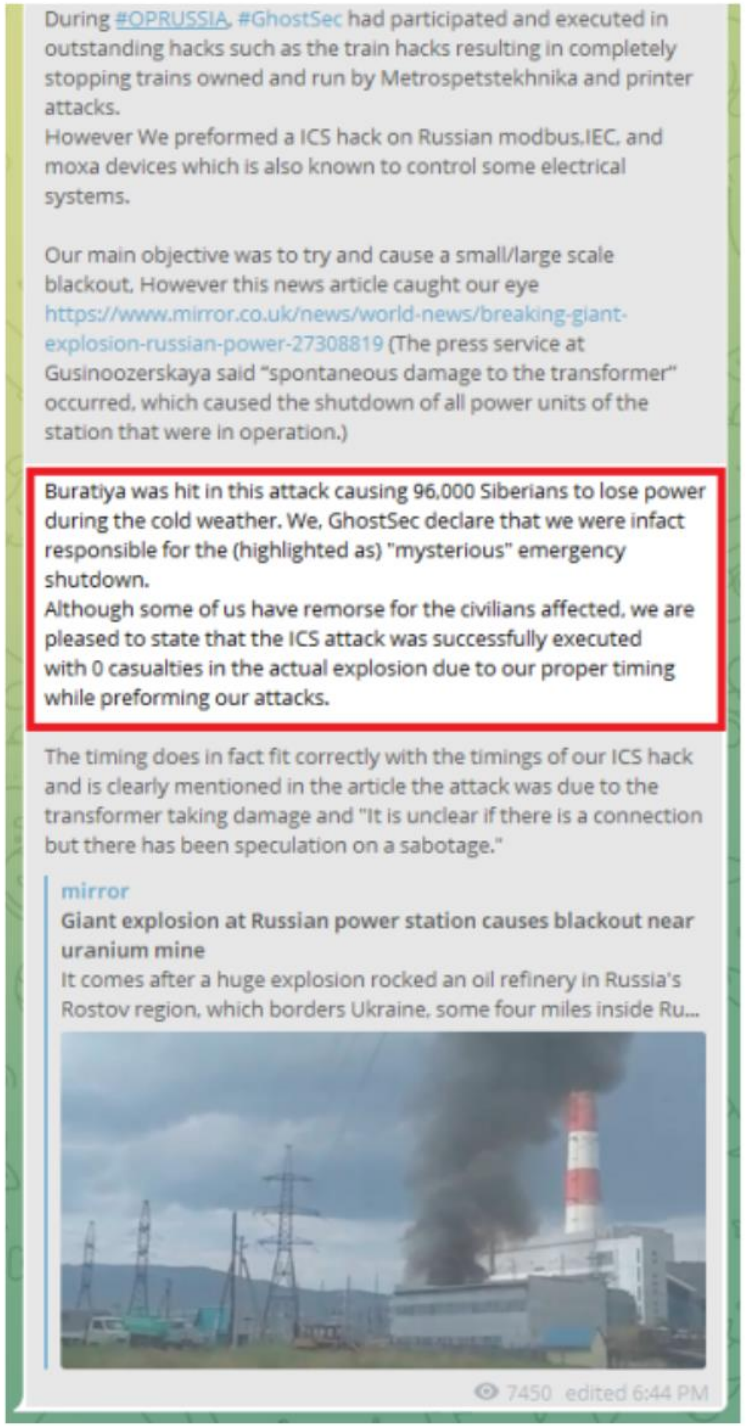
The last moments of life for the Paper Mill.. SCADA system still gone, operation complete. We will not tweet for some time, until a new group of attacks is complete. Please enjoy the final moments for the Orcs, #Ukraine ✊🇺🇦



Alert: This is most likely false/ inaccurate

"Buratiya was hit in this attack causing 96,000 Siberians to lose power during cold weather. We, Ghostsec declare that we were infact responsible for the (highlighted as) "mysterious" emergency shutdown.

Although some of us have remorse for the civilians affected, we are pleased to state that the ICS attack was successfully executed with 0 casualties in the actual explosion due to our proper timing while performing our attacks."



MANDIANT

Opening the Box: Are These Attacks Real?

Hacktivist Techniques in MITRE ATT&CK for ICS

Tactic	Technique
Initial Access	T0883: Internet Accessible Device
Initial Access	T0819: Exploit Public-Facing Application
Execution	T0807: Command-Line Interface
Execution	T0823: Graphical User Interface
Persistence	T0859: Valid Accounts
Evasion	T0872: Indicator Removal on Host
Lateral Movement	T0859: Valid Accounts
Collection	T0852: Screen Capture

Tactic	Technique
Collection	T0811: Data from Information Repositories
Command and Control	T0885: Commonly Used Port
Command and Control	T0869: Standard Application Layer Protocol
Inhibit Response Function	T0816: Device Restart/Shutdown
Inhibit Response Function	T0809: Data Destruction
Impair Process Control	T0855: Unauthorized Command Message
Impact	T0831: Manipulation of Control
Impact	T0882: Theft of Operational Information
Impact	T0826: Loss of Availability

Archived Content

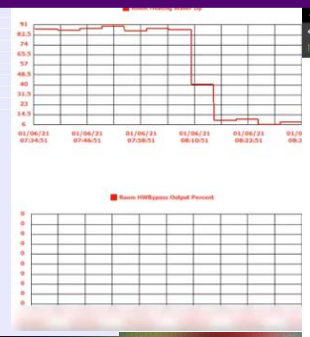
In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

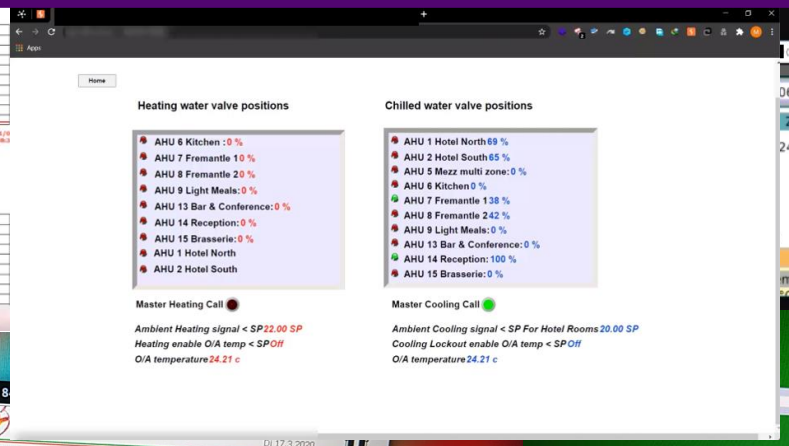
ALERT

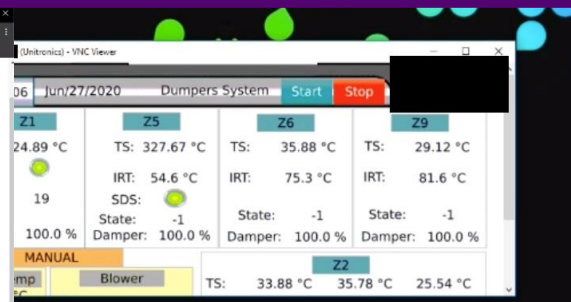
Mitigating Attacks Against Uninterruptable Power Supply Devices

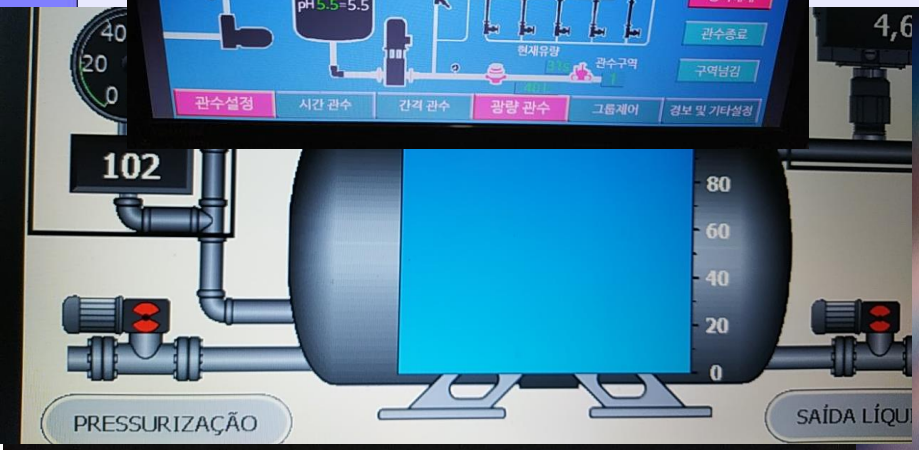
Last Revised: April 29, 2022

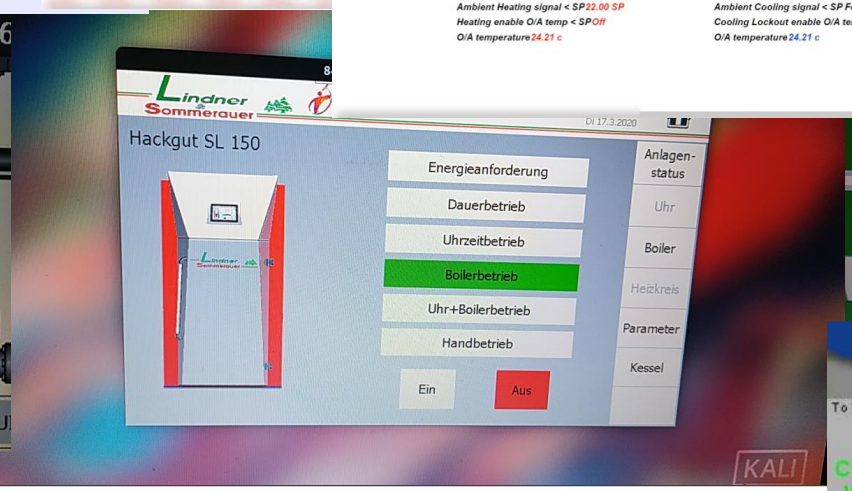
Graphical User Interfaces

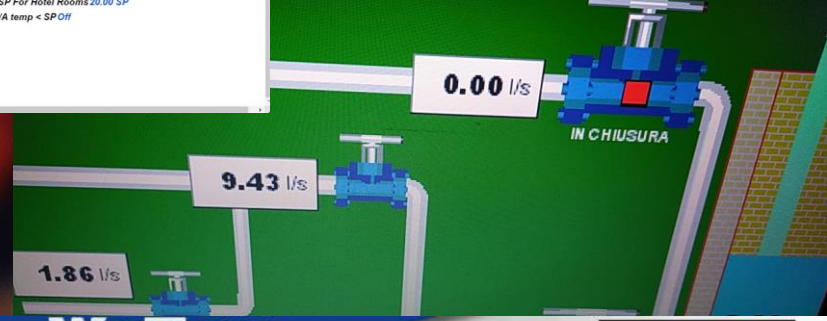


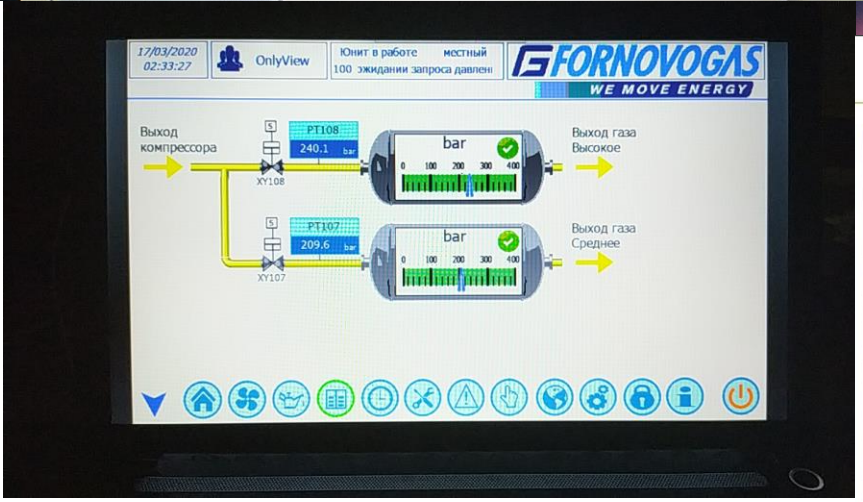


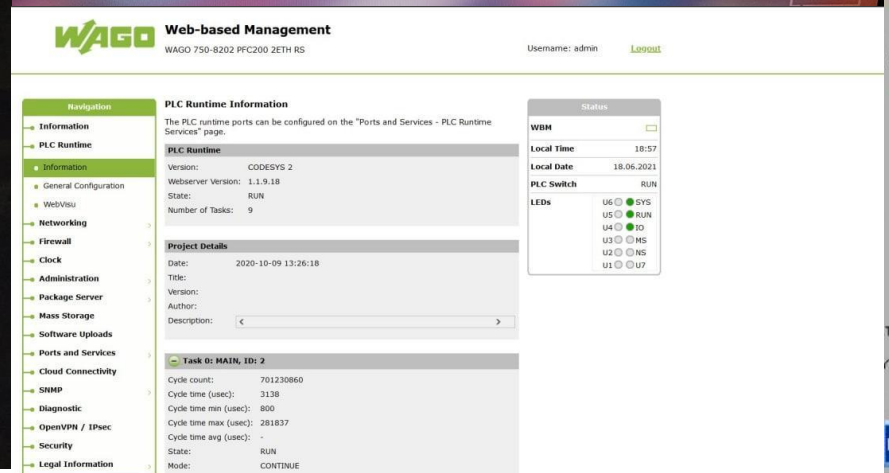


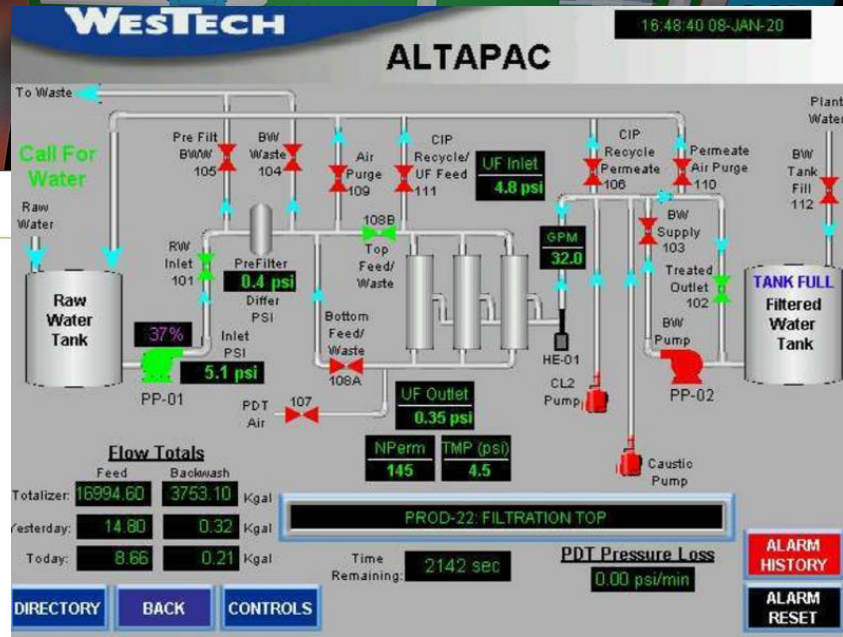




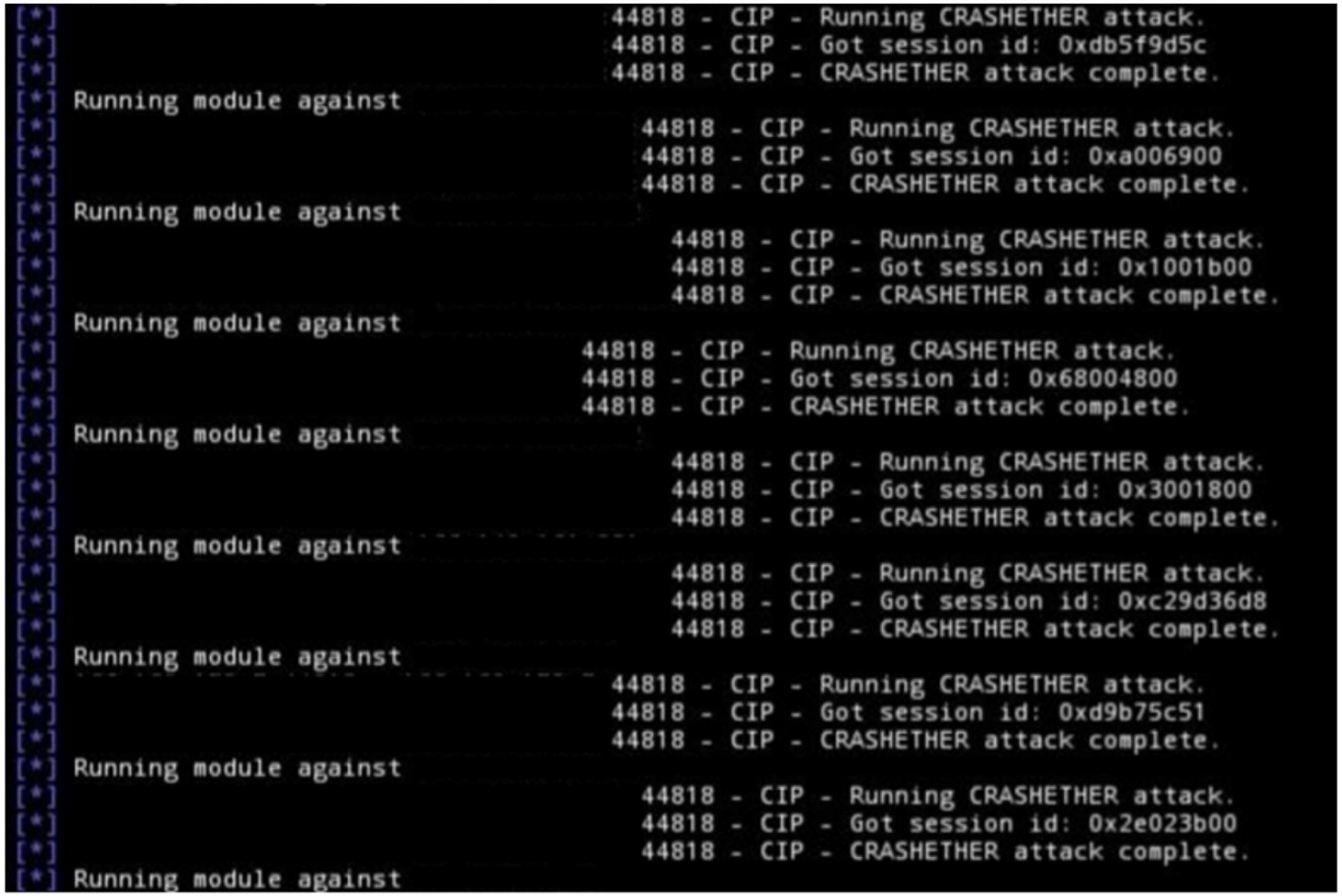








Exploit Public-Facing Applications



- Metasploit
  - IEC-104
  - EtherNet-IP CIP
- Killbus
  - Modbus

What’s the Impact?!

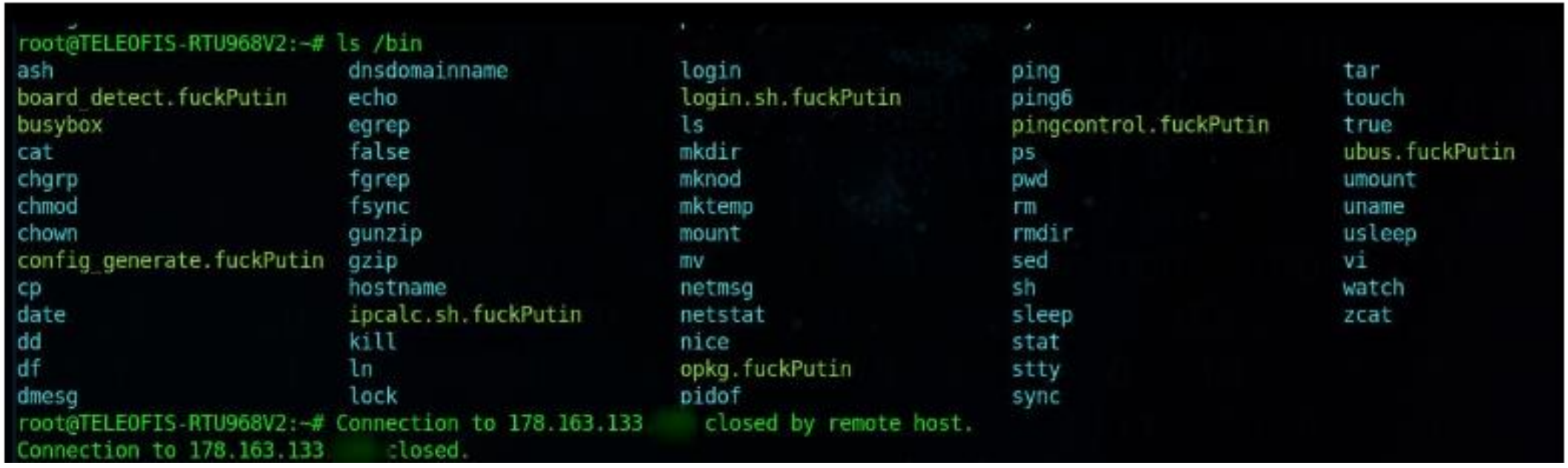
MANDIANT

Debunking Some OT Hacking Claims

Case 1: GhostSec Claimed to Deploy Ransomware on Belarusian RTU

Photo by Mahdi Bafande on Unsplash

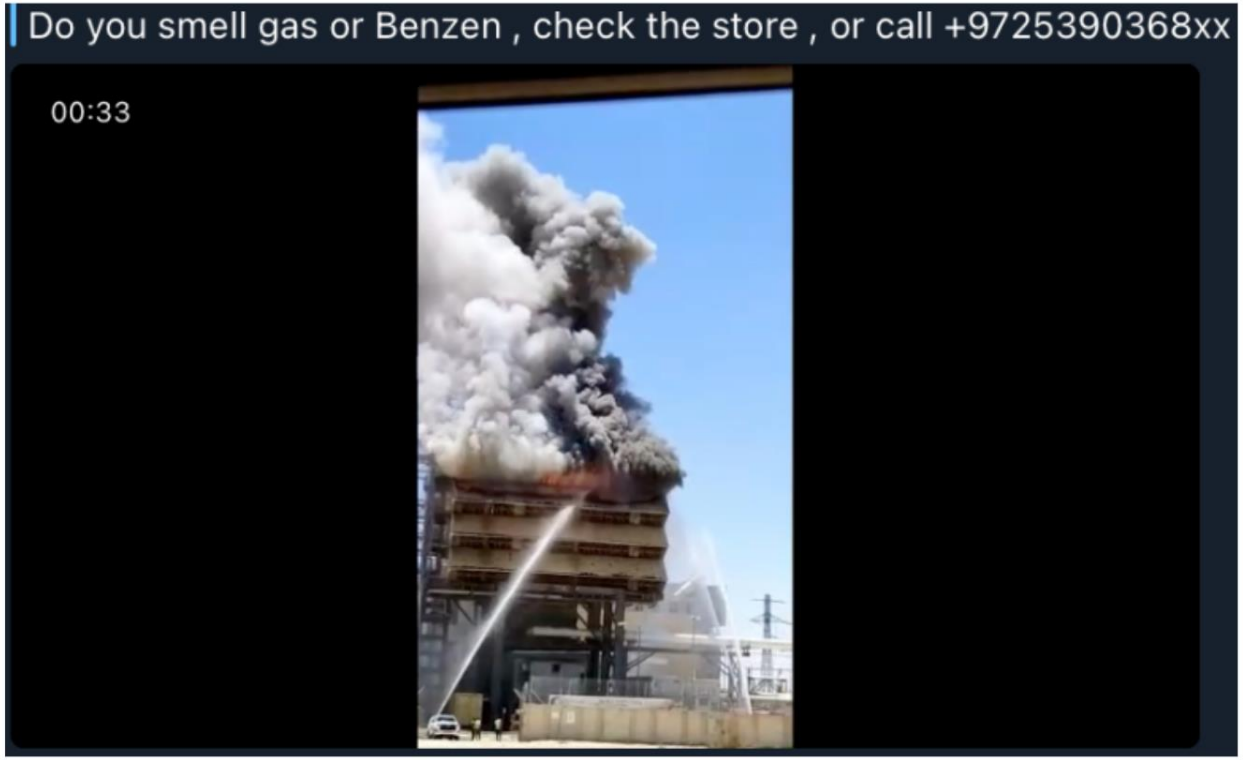

root@178.163.133 password:
BusyBox v1.23.2 (2021-03-29 10:37:34 MSK) built-in shell (ash)
Build for RTU968V2 v.2.6.9S
OpenWrt Chaos Calmer
root@TELEOFIS-RTU968V2:~# ls /bin ; uname -a
ash config_generate echo hostname ls netstat ps stat umount
board_detect cp egrep ipcalc.sh mkdir nice pwd stty uname
busybox date false kill mknod opkg rm sync usleep
cat dd fgrep ln mktemp pidof rmdir tar vi
chgrp df fsync lock mount ping sed touch watch
chmod dmesg gunzip login mv ping6 sh true zcat
chown dnsdomainname gzip login.sh netmsg pingcontrol sleep ubus
Linux TELEOFIS-RTU968V2 3.18.29 #1 Mon Mar 29 10:43:13 MSK 2021 armv5tejl GNU/Linux
root@TELEOFIS-RTU968V2:~#
root@TELEOFIS-RTU968V2:~#
root@TELEOFIS-RTU968V2:~#
root@TELEOFIS-RTU968V2:~#


root@TELEOFIS-RTU968V2:~# ls /bin
ash dnsdomainname login ping tar
board_detect.fuckPutin echo login.sh.fuckPutin ping6 touch
busybox egrep ls pingcontrol.fuckPutin true
cat false mkdir ps ubus.fuckPutin
chgrp fgrep mknod pwd umount
chmod fsync mktemp rm uname
chown gunzip mount rmdir usleep
config_generate.fuckPutin gzip mv sed vi
cp hostname netmsg sh watch
date ipcalc.sh.fuckPutin netstat sleep zcat
dd kill nice stat
df ln opkg.fuckPutin stty
dmesg lock pidof sync
root@TELEOFIS-RTU968V2:~# Connection to 178.163.133 closed by remote host.
Connection to 178.163.133 closed.

CASE 2: Claim Responsibility for Destruction of Assets

Taking advantage of real-world events...

- Altahrea Team claims responsibility over Orot Yosef power plant fire.
- GhostSec claims responsibility for hydro-power plant in Russia.
- Team OneFist claims to disable cellular router supporting OT in Russia.

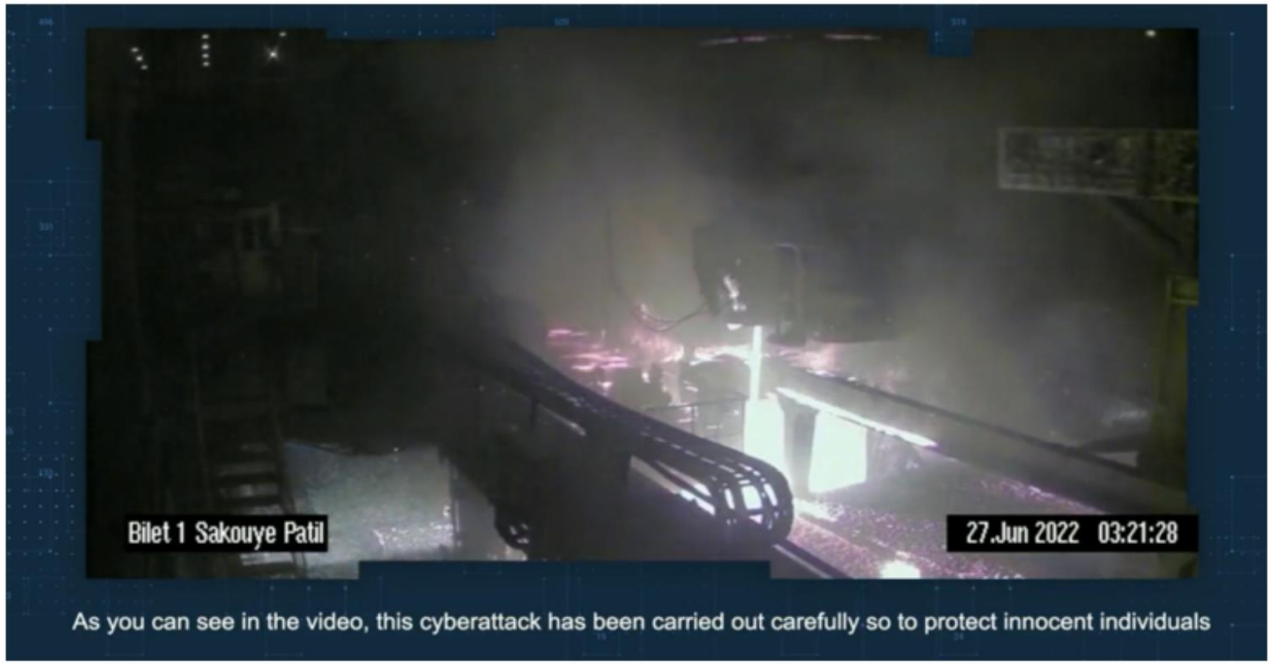


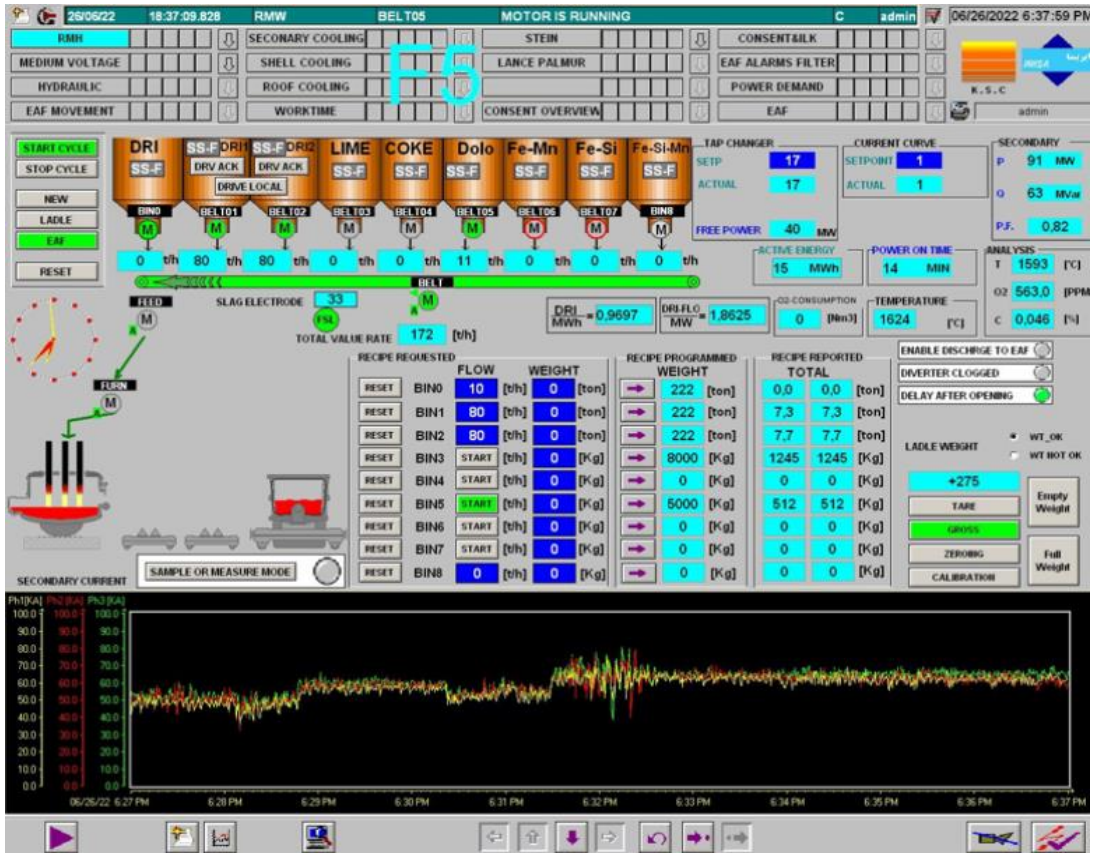
CASE 3: Claim Responsibility for Destruction of Assets

#cyberattack against Iran's steel industry

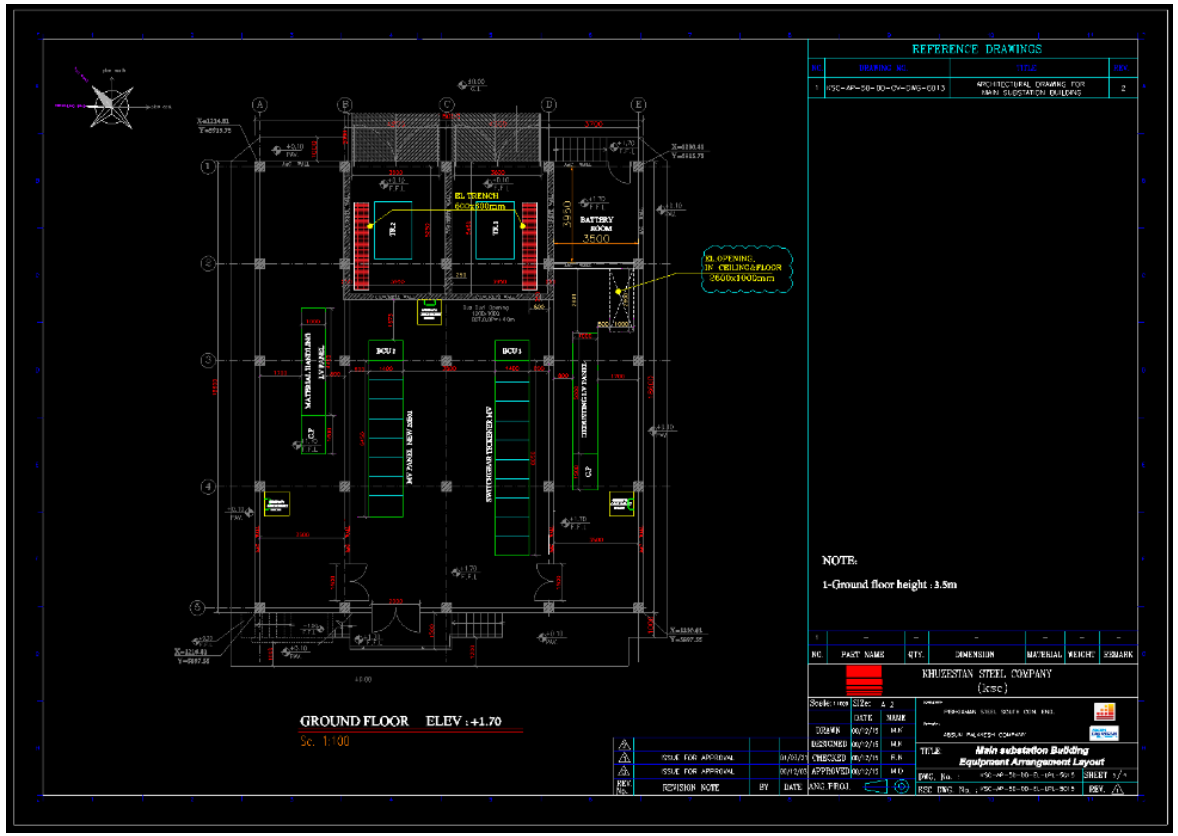
7:12 AM · Jun 27, 2022

CASE 3: Claim Responsibility for Destruction of Assets





CASE 3: Claim Responsibility for Destruction of Assets



MANDIANT

So...is there a ~~Cat~~/Hack in the Box?

Do Hacktivists Pose a Risk to Operational Technology?

Yes and no...

- Hacktivists interact with OT assets
- Higher frequency means higher risk
- Calls media attention and invites for copycats
- Helps nation-states to deny actions
- Actors share knowledge which will remain after conflict

Yes

No

- Hacktivists use very simple techniques
- Higher frequency des not mean higher impact
- OT attacks require more resources to generate impact
- Hacktivists can call media attention without OT
- Nation-state actors have hacked OT with little to no repercussions

And yet… hacktivists continue to normalize hacking OT

MANDIANT

Thanks!

Daniel Kapellmann Zafra

@Kapellmann

www.kapell.tech