Tracking Industrial Advanced Threat Actors Who Aren't Really Advanced Just Skiddies Who Deface PLCs and Have Bad Manners

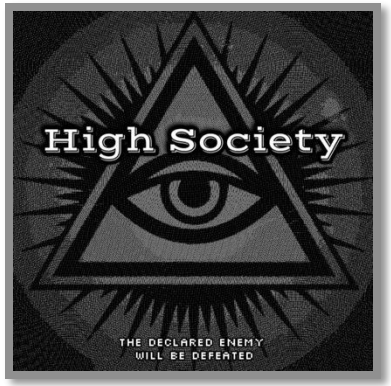
Methods and Results and Tears and Laughter and More Tears

Ron Fabela
CEO
Infinity squared group

Don't Believe Anything I'm About to Say

For even the very wise cannot see all ends

The ~~Players~~ Skiddies



The ~~Players~~ Skiddies

Channel Info

Cyber Av3ngers
8,215 subscribers

t.me/CyberAveng3rs
Link

twitter: https://twitter.com/CyberAveng3rs
Description

Notifications

VIEW CHANNEL

Channel Info

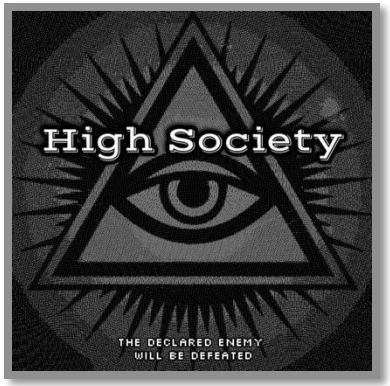
The Five Families
6,598 subscribers

t.me/FiveFamilies
Link

Official channel of the Five families.
Description

Notifications

VIEW CHANNEL



Channel Info

High Society
883 subscribers

t.me/highs0c1ety
Link

The declared enemy will be defeated.
Description

Notifications

VIEW CHANNEL

Channel Info

Народная CyberАрмия
64,309 subscribers

t.me/CyberArmyofRussia_Reborn
Link

Информация: 👇
https://telegra.ph/Dobro-pozhalovat-v-Narodnuyu-Kiberarmiyu-04-26

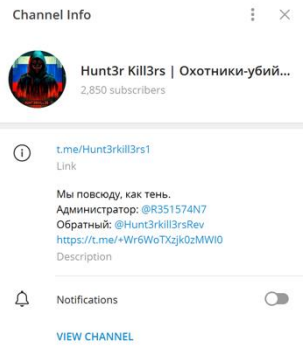
Резерв: https://t.me/RCAT_reserve

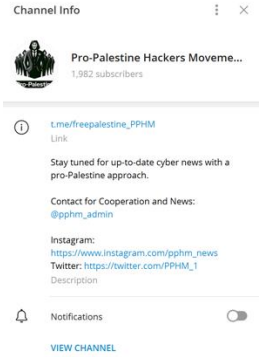
Связь:
@error_404_smoke

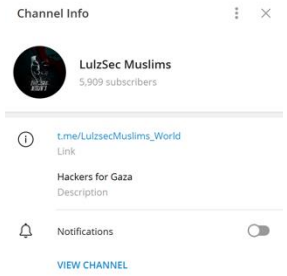
Осинт бот @dox_NKA_bot

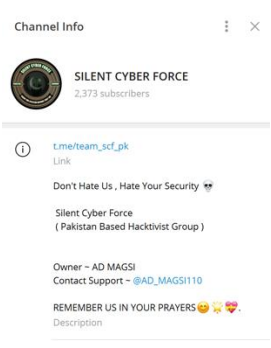
Поддержать: 👇
https://telegra.ph/Podderzhat-Narodnuyu-Kiberarmiyu-02-27
Description

The ~~Players~~ Skiddies





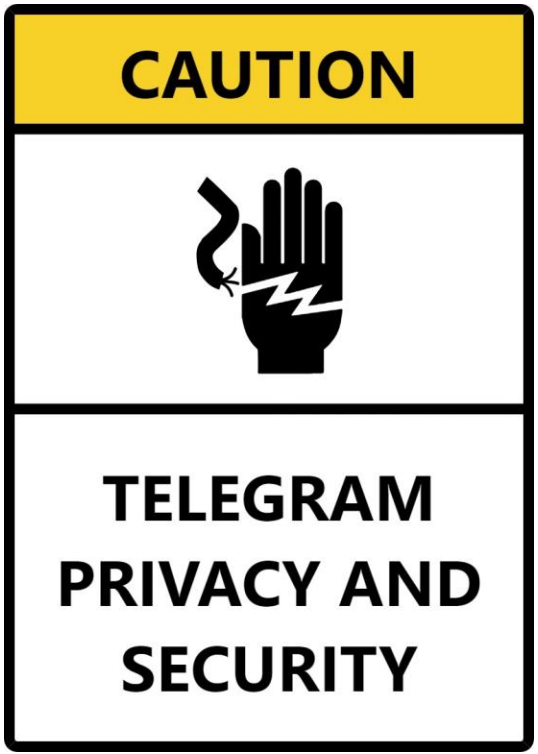


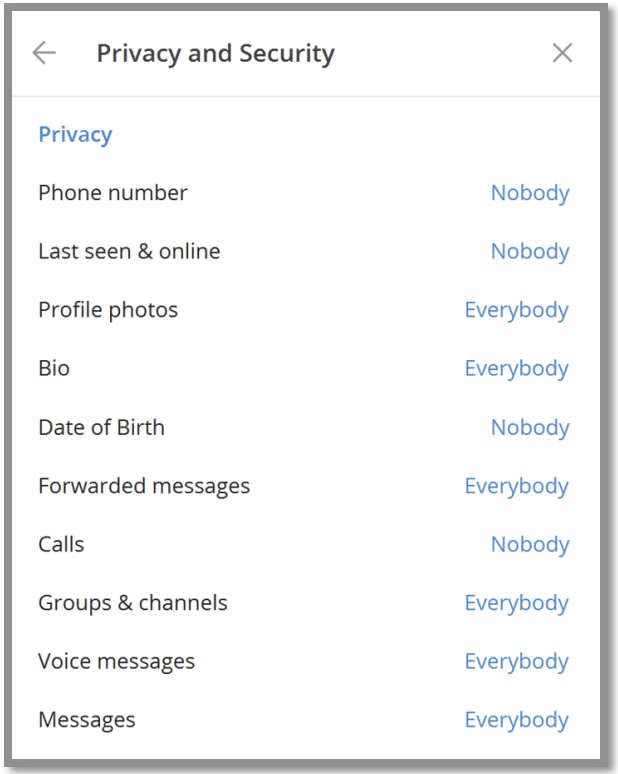


Communications

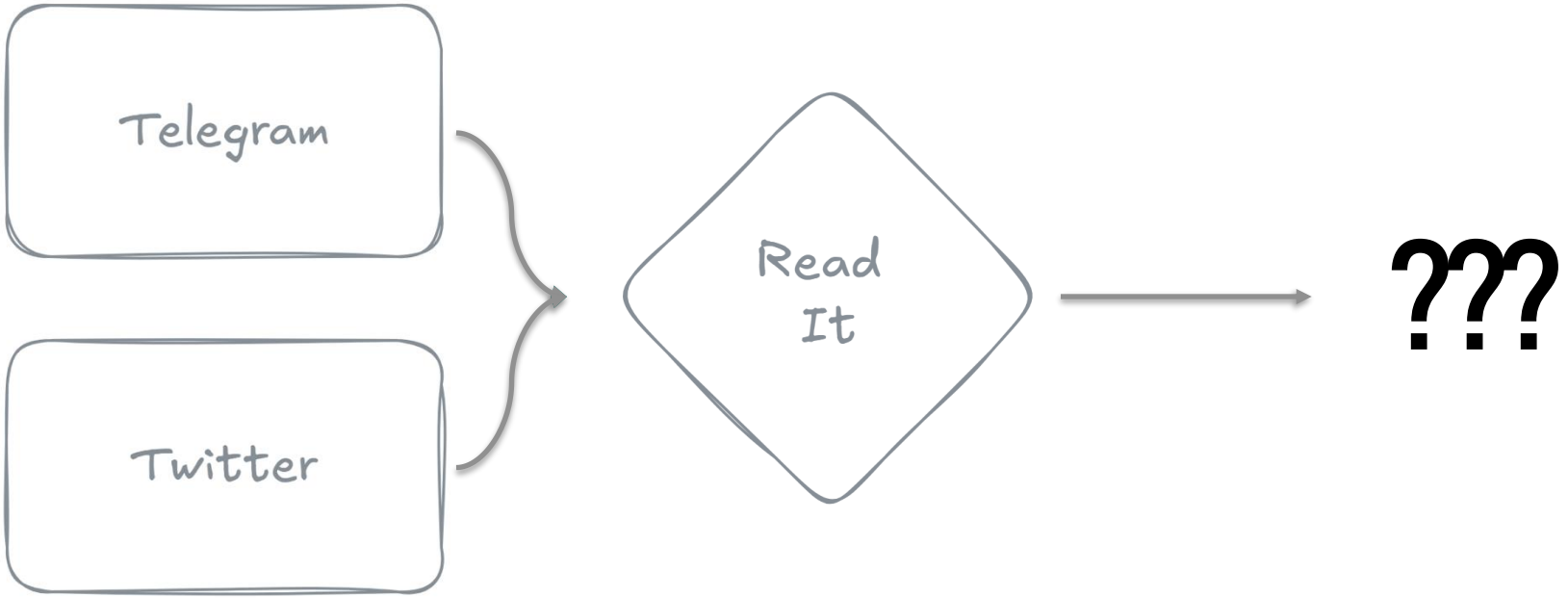
TELEGRAM

Communications





The Process



Use Case – Lulzsec Muslims

LulzSec Muslims

Hello everyone, today we collectively targeted the ICS / SCADA Systems to the following countries: France, Germany, and the Israeli occupation

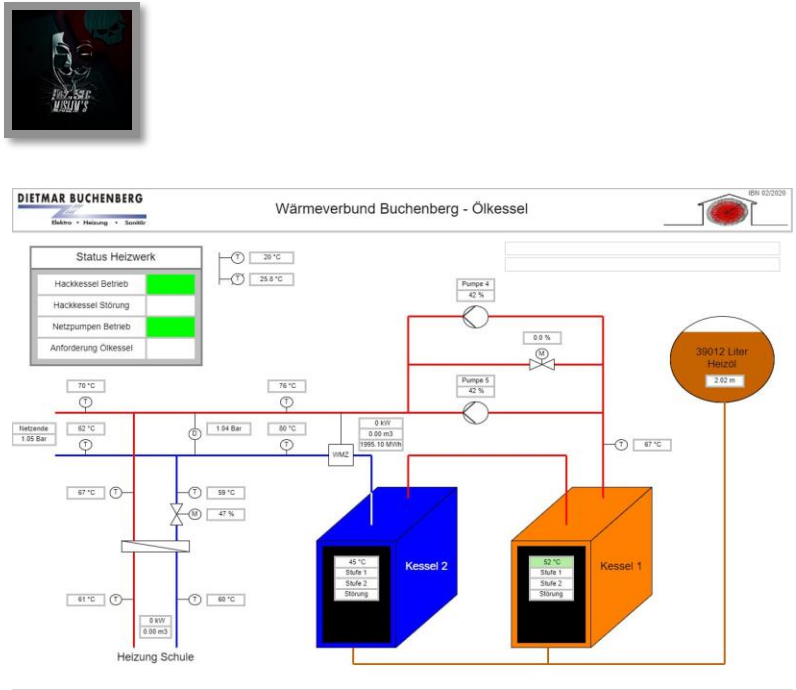
in response to their support and massacres against our people in Gaza.

#LulZsec_Muslims

🔥 9 👍 3 ❤️ 2 👾 1

1185 edited 10:35 PM

Use Case – Lulzsec Muslims



Use Case – Lulzsec Muslims

Use Case – Lulzsec Muslims

About

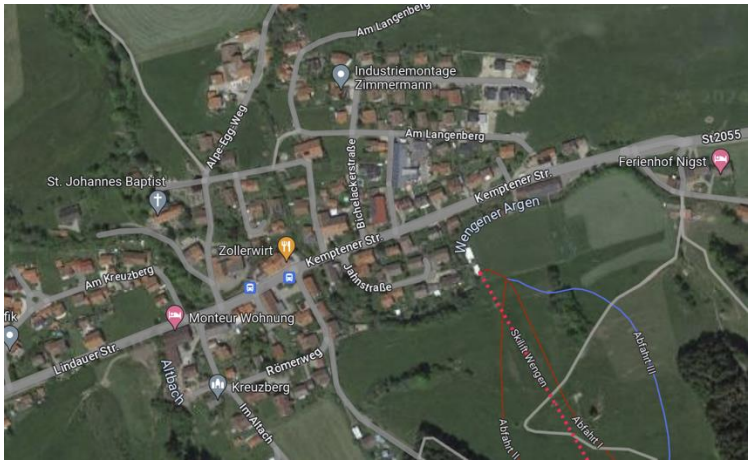
Weitnau is a municipality in the rural district Oberallgäu in Bavaria/Germany. Together with the neighboring municipality of Missen-Wilhams, Weitnau shares an administrative unit. Wikipedia

Elevation: 2,615′

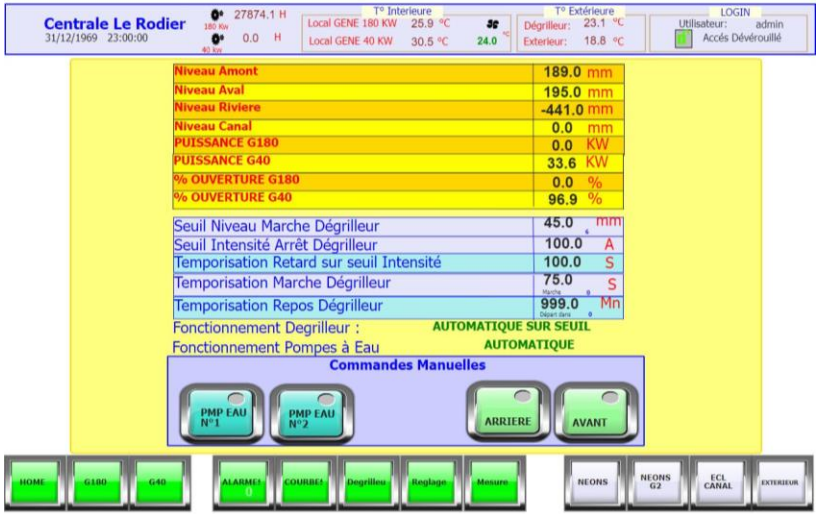
Postal code: 87480

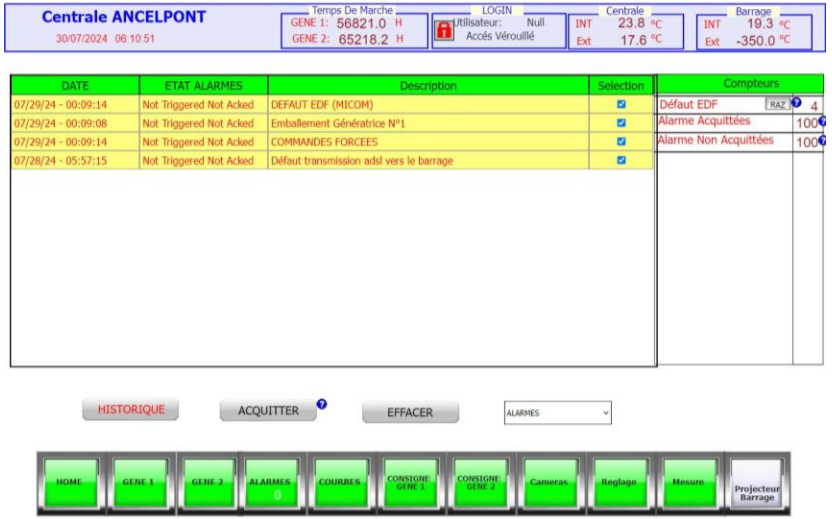
Population: 5,172 (Dec 31, 2008)

Area: 25.18 mi²

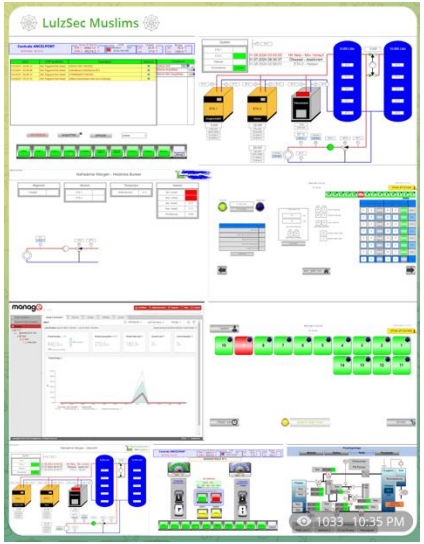


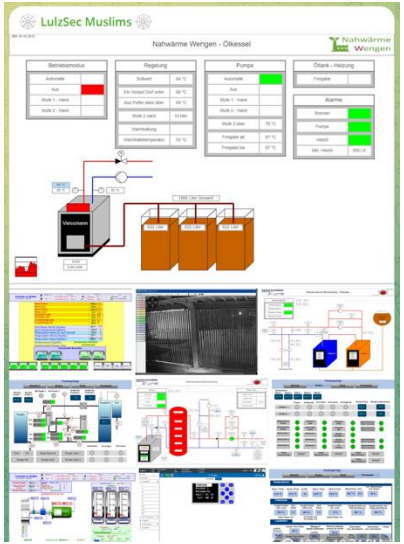
Use Case – Lulzsec Muslims

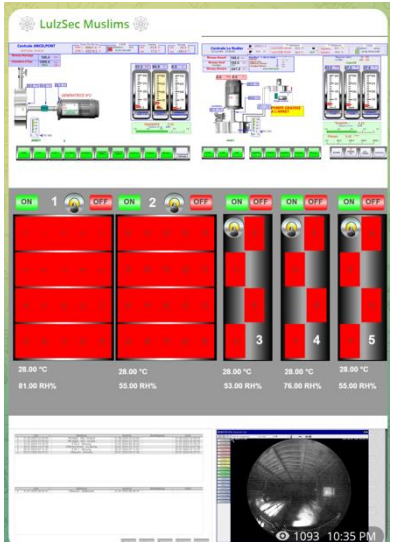




Use Case – Lulzsec Muslims







Use Case – Lulzsec Muslims

Summary:

Patriotic/Political

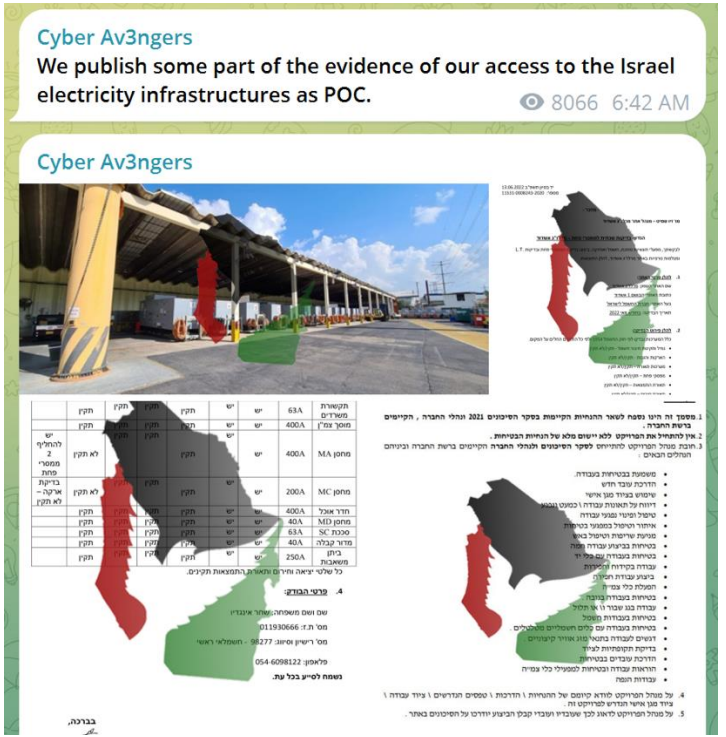
Opportunistic But Prolific

Targets Are "Industrial" Yet Low Impact

Use Case – Lulzsec Muslims

Question Everything:
Was it Targeted?
Was it Advanced?
Was it Critical Infrastructure

Use Case - Cyber Av3ngers



Use Case - Cyber Av3ngers

Use Case – Cyber Av3ngers

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities

Congress of the United States
Washington, DC 20515

November 28, 2023

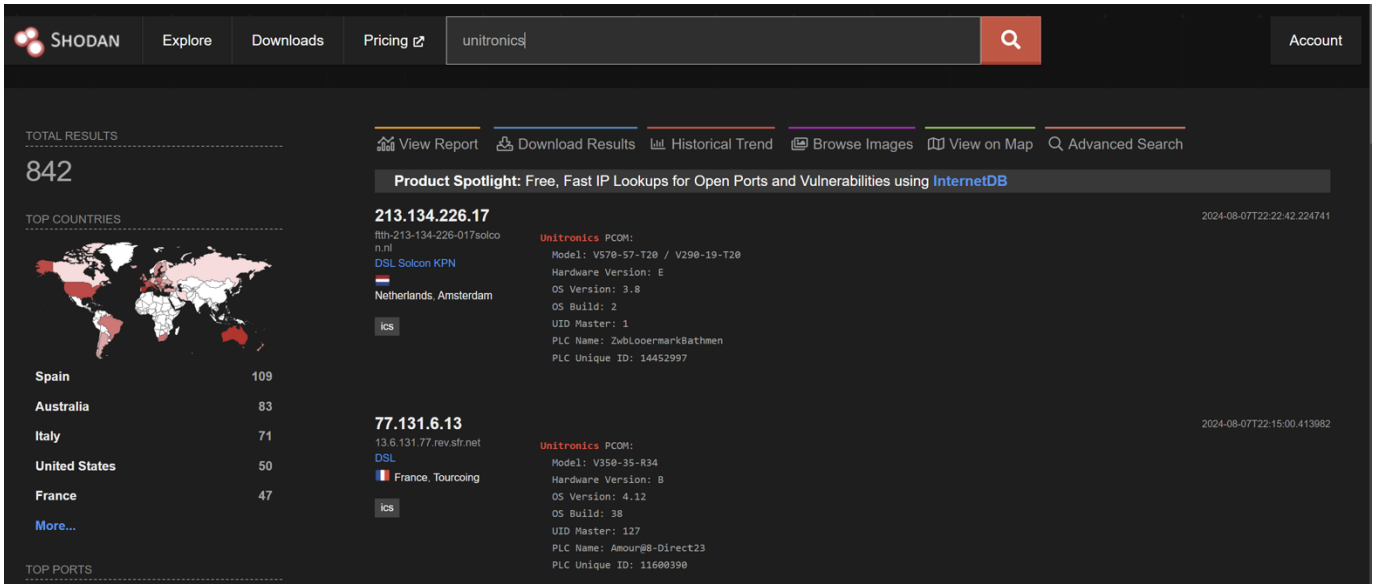
The Honorable Merrick Garland
Attorney General of the United States
United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Attorney General Garland,

On November 24, 2023, an Iranian-backed cyber group, the "Cyber Av3ngers," attacked the Municipal Water Authority of Aliquippa by hacking Israeli-made equipment in the water system. The authority serves the City of Aliquippa and Raccoon, Potter, and portions of Hopewell

Use Case - Cyber Av3ngers

Use Case - Cyber Av3ngers



Use Case - Cyber Av3ngers

213.134.226.17

ftth-213-134-226-017solcon.nl

DSL Solcon KPN

Netherlands, Amsterdam

ics

Unitronics PCOM:

```
Model: V570-57-T20 / V290-19-T20
Hardware Version: E
OS Version: 3.8
OS Build: 2
UID Master: 1
PLC Name: ZwbLooermarkBathmen
PLC Unique ID: 14452997
```

Use Case - Cyber Av3ngers

ZWEMBAD DE LOOERMARK

Zwembad Looermark

1.5K likes • 1.7K followers

Use Case - Cyber Av3ngers

UNITRONICS

Home | Products | Software | Technical Support | Case Studies | Distributors Zone | Where to Buy | About | Contact Us

All-in-One software enables you to:

- Develop your PLC, HMI, VFD and Servo applications in one programming environment
- Configure Hardware & Communications
- Establish modem and data communications
- Test and debug your programs
- Software Utilities Suite: remote access and data management tools

Control your application remotely from everywhere and anytime!

- Click here to download the App from Google play
- Click here to download the App the from App store

Unitronics Added Value:

- All Unitronics software & utilities—plus updates—provided at no charge.

Download the latest version

Use Case – Cyber Av3ngers

Summary:

Patriotic/Political

Opportunistic But Prolific

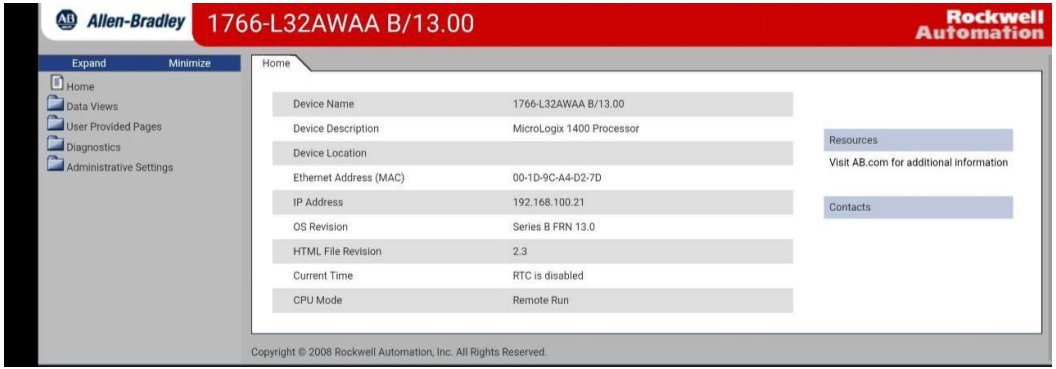
Targets Are “Industrial” Yet Low Impact

Use Case – Cyber Av3ngers

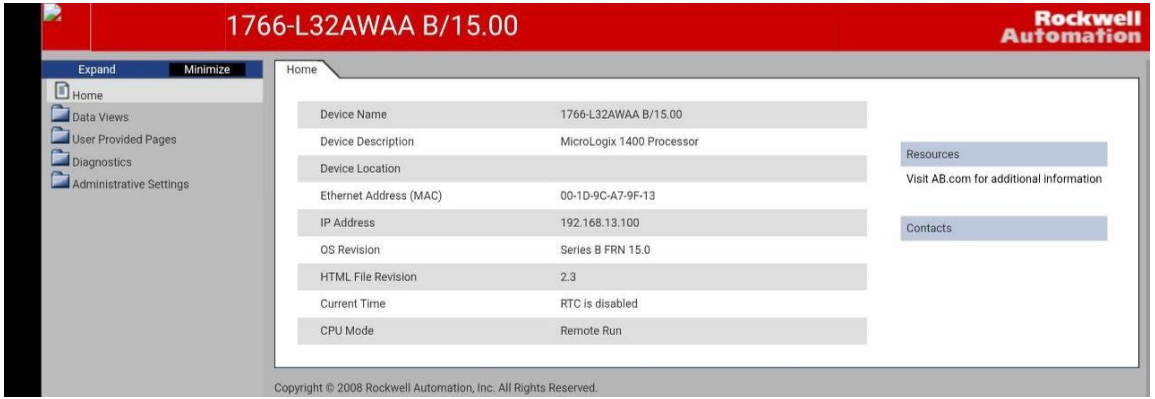
Question Everything:
Was it Targeted?
Was it Advanced?
Was it Critical Infrastructure

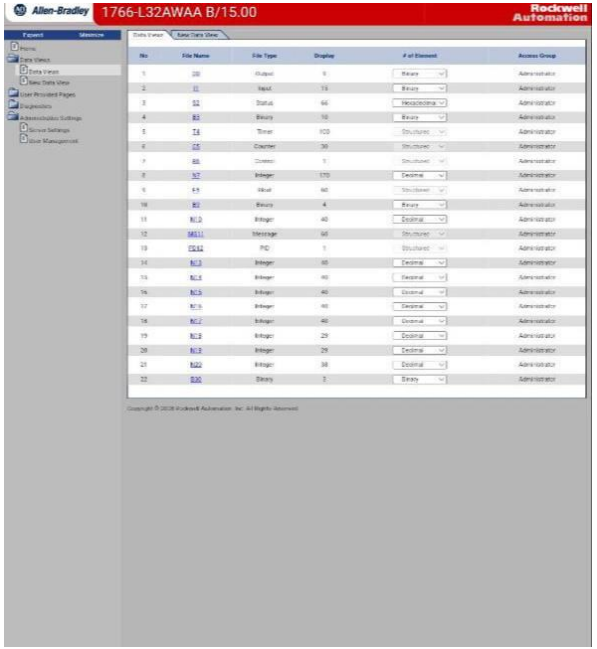
Use Case – Hunt3r Kill3rs

Use Case – Hunt3r Kill3rs

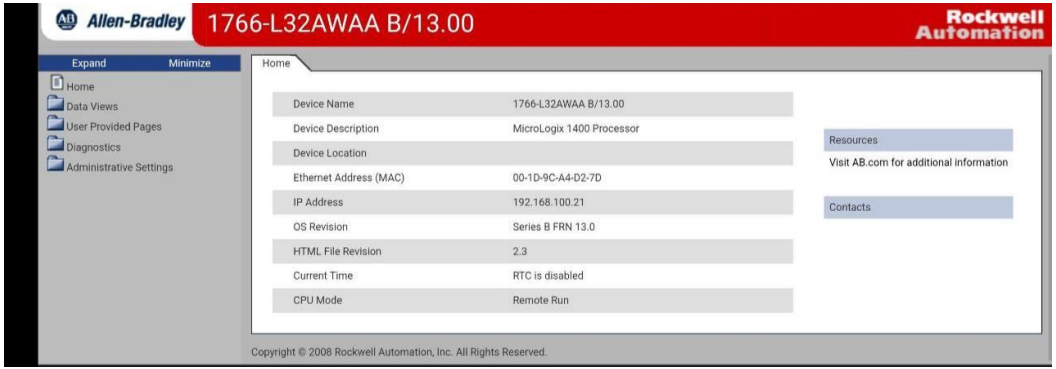


Use Case – Hunt3r Kill3rs

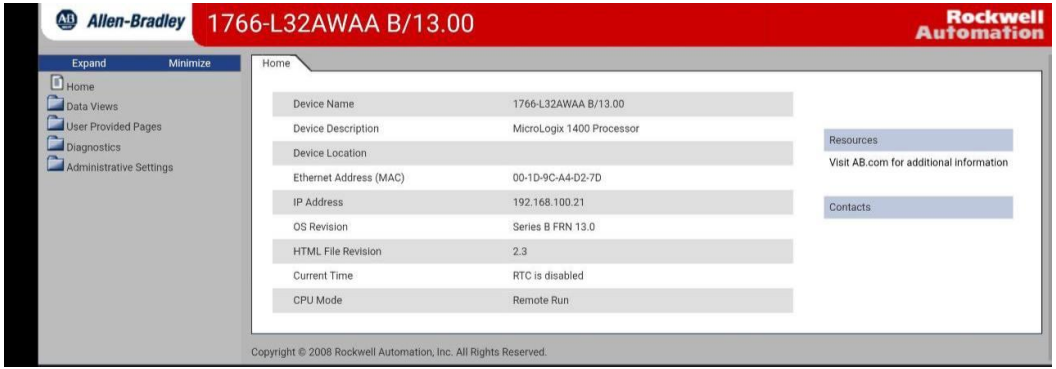




Use Case – Hunt3r Kill3rs



Use Case – Hunt3r Kill3rs



Use Case – Hunt3r Kill3rs

Schneider Electric

PowerLogic® EGX100

Home | Logout

Monitoring | Control | Diagnostics | Maintenance | Setup

- Ethernet & TCP/IP
- Serial Port
- Device List
- **User Accounts**
- Web Page Access
- Modbus TCP/IP Filtering
- SNMP Parameters

User Accounts

Groups

Administrators	Engineering	Operations	Maintenance

Users

Name	Password	Group	Language
Administrator	**********	Administrators	English
Hunt3rkill3rs	**********	Administrators	English
Hunt3rkill3rs2	**********	Engineering	English
		Maintenance	English
Guest	*****		

Schneider Electric

WADE

Visualisation

Accueil

Visualisation | Commande | Diagnostic | Maintenance | Paramétrage

Classes

- Internal Information

Etats équipement

Libellé	Etat
Internal Information	
VLV_STOP	Inactive
RESET TOTAL FLOW	Inactive
Error in communication with slaves	Inactive
Event Pile 2 80 percent	Inactive
CT-2 FLOW RATE	1984.000 m3/hr
CT-2 PRESSURE	0.302 kg/cm2
CT-2 LEVEL	4.991 mtr
CT-2 TURBIDITY	-24.970 ntu
CT-2 CHLORINE	-1.249 mg/l
CT-2 VLV_POSITION	77.020 Percent

Use Case – Hunt3r Kill3rs

Hunt3r Kill3rs Group Claims to Breach German Schneider Electric Systems

June 17, 2024

"Schneider Electric's German systems were allegedly compromised, according to the infamous cybercriminal collective Hunt3r Kill3rs. The company's networks were claimed to be compromised by the Hunt3r Kill3rs group, possibly compromising sensitive data and vital infrastructure."

Use Case – Hunt3r Kill3rs

Summary:

Patriotic/Political

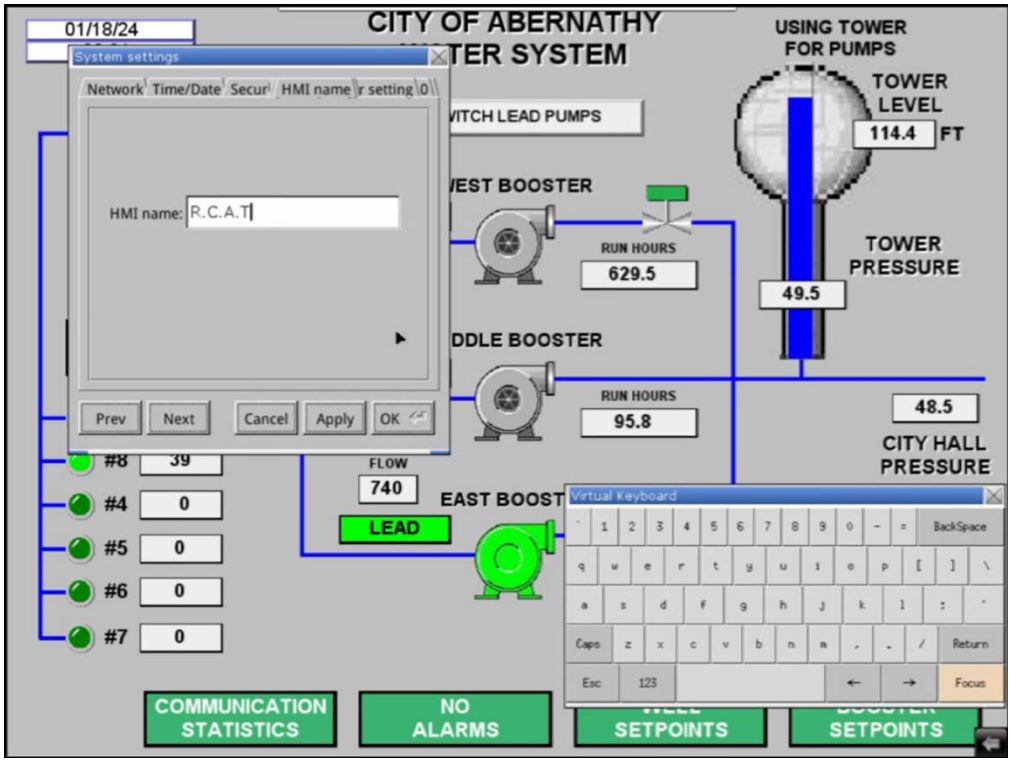
Opportunistic

Targets Are “Industrial” Yet Low Impact

Use Case – Hunt3r Kill3rs

Question Everything:
Was it Targeted?
Was it Advanced?
Was it Critical Infrastructure

Use Case – RCAT/CARR



Use Case – RCAT/CARR

FORT MEADE, Md. – Pro-Russia hacktivists are conducting malicious cyber activity against operational technology (OT) devices and critical infrastructure organizations are encouraged to implement mitigations

While none of the cyberattacks impacted drinking water for communities, the incidents mark a notable escalation in Russia's targeting of critical infrastructure in the United States.

Use Case – RCAT/CARR

Summary:

Patriotic/Political

Opportunistic

Targets Are "Industrial" Yet Low Impact

Use Case – RCAT/CARR

Question Everything:
Was it Targeted?
Was it Advanced?
Was it Critical Infrastructure

Conclusion

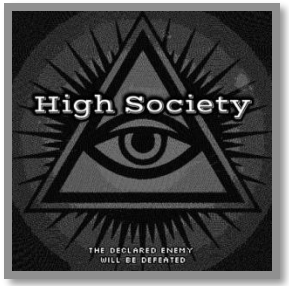
"It's the small things, everyday deeds of ordinary folk that keeps the darkness at bay"

"The wise speak only of what they know"

Telegrams

~~https://t.me/CyberAveng3rs~~ PWN'D LOL
https://twitter.com/CyberAveng3rs

https://t.me/FiveFamilies



https://t.me/highs0c1ety

https://t.me/CyberArmyofRussia_Reborn

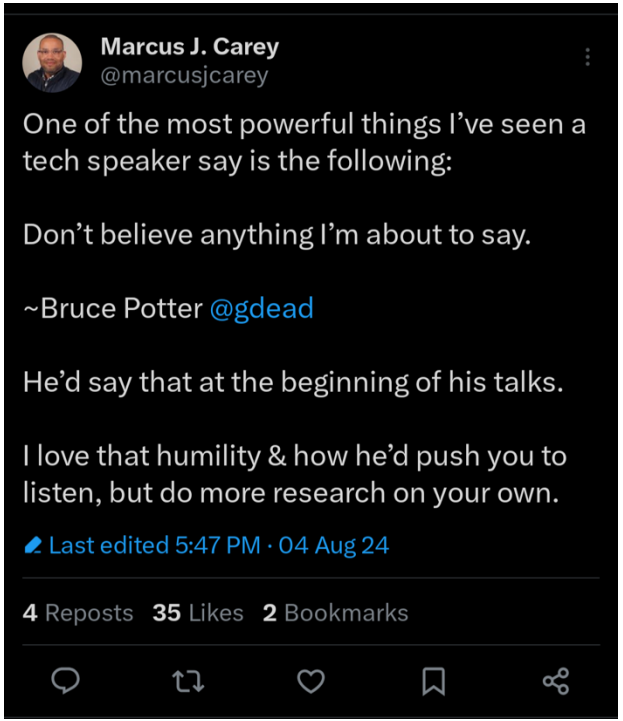
https://t.me/Hunt3rkill3rs1

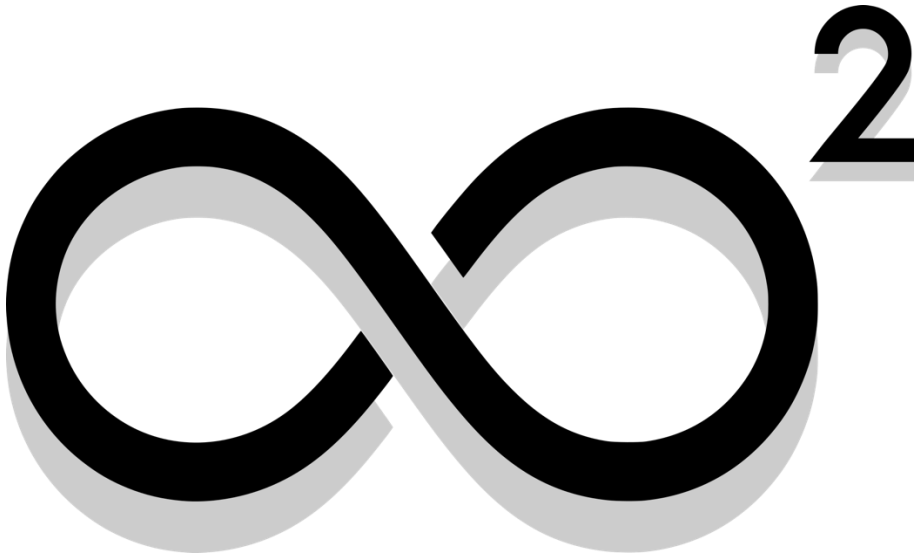
https://t.me/freepalestine_PPHM

https://t.me/LulzsecMuslims_World

https://t.me/team_scf_pk

GOATS


Marcus J. Carey
@marcusjcarey
One of the most powerful things I've seen a tech speaker say is the following:
Don't believe anything I'm about to say.
~Bruce Potter @gdead
He'd say that at the beginning of his talks.
I love that humility & how he'd push you to listen, but do more research on your own.
Last edited 5:47 PM · 04 Aug 24
4 Reposts 35 Likes 2 Bookmarks



@ron_fab
ron@infntysqrd.com