

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

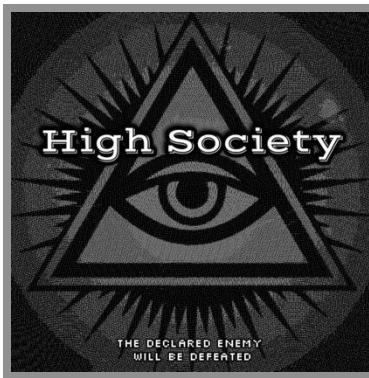


Don't Believe Anything I'm About to Say



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



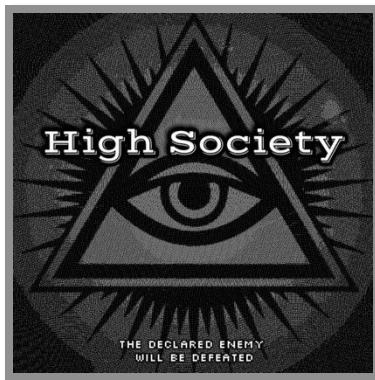
The Five Families
6,598 subscribers

t.me/FiveFamilies
Link

Official channel of the Five families.
Description

Notifications

[VIEW CHANNEL](#)



Channel Info



High Society
883 subscribers

t.me/highsociety
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-Narodnuyu-Kiberarmiyu-02-26>

Резерв: https://t.me/RCAT_reserve

Связь:
[@error_404_smoke](https://t.me/error_404_smoke)

Оснит бот [@dox_NKA_bot](https://t.me/dox_NKA_bot)

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

The Players Skiddies

Channel Info

Hunt3 Kill3rs | Охотники-убий...
2,850 subscribers

t.me/Hunt3kill3rs1
Link

Мы повсюду, как тень.
Администратор: @R351574N7
Обратный: @Hunt3kill3rsRev
<https://t.me/+Wr6WoTxjkl0zMW0>
Description

Notifications

[VIEW CHANNEL](#)



Channel Info

Pro-Palestine Hackers Moveme...
1,982 subscribers

t.me/freepalestine_PPHM
Link

Stay tuned for up-to-date cyber news with a pro-Palestine approach.

Contact for Cooperation and News:
[@pphm_news](https://www.instagram.com/pphm_news)

Instagram:
https://www.instagram.com/pphm_news
Twitter: https://twitter.com/PPHM_1
Description

Notifications

[VIEW CHANNEL](#)



Channel Info

LulzSec Muslims
5,909 subscribers

t.me/LulzsecMuslims_World
Link

Hackers for Gaza

Notifications

[VIEW CHANNEL](#)



Channel Info

SILENT CYBER FORCE
2,373 subscribers

t.me/team_scf_pk
Link

Don't Hate Us , Hate Your Security 🤝

Silent Cyber Force
(Pakistan Based Hacktivist Group)

Owner ~ AD MAGSI
Contact Support ~ [@AD_MAGS110](https://t.me/AD_MAGS110)

REMEMBER US IN YOUR PRAYERS 😍🙏❤️.

Description



Communications



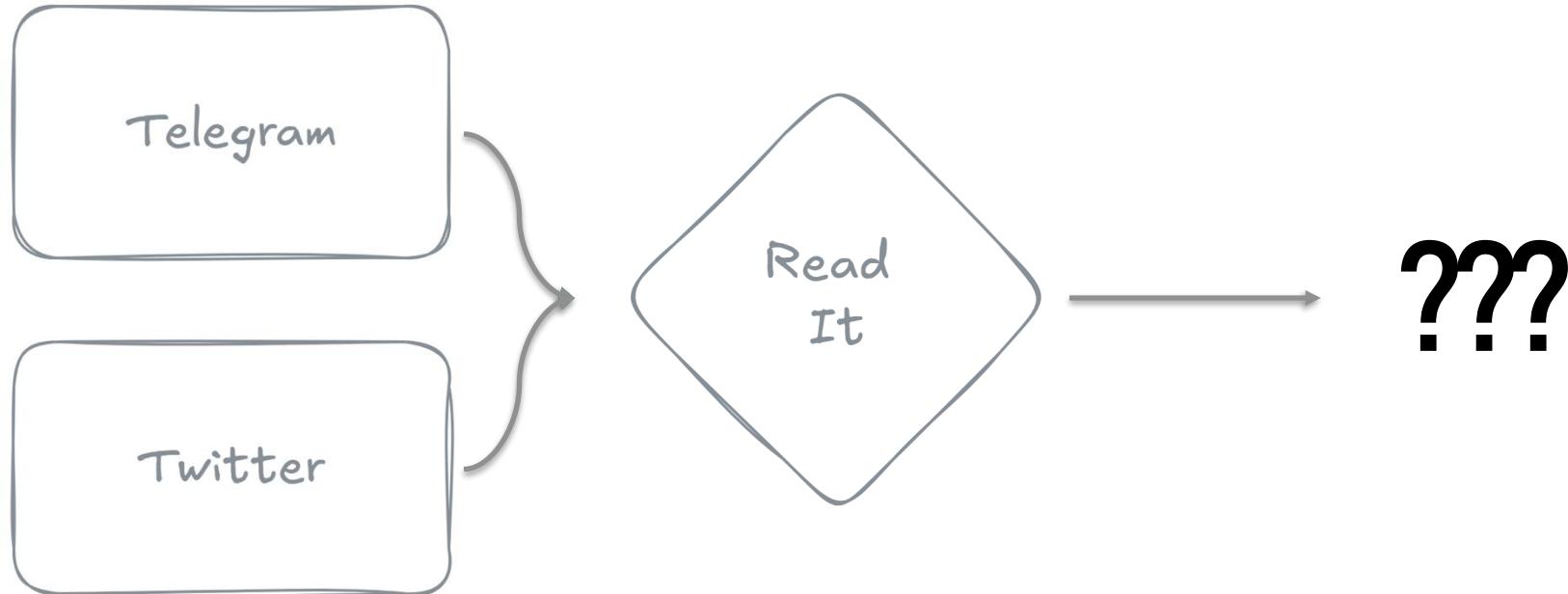
TELEGRAM

Communications



Privacy and Security	
Privacy	
Phone number	Nobody
Last seen & online	Nobody
Profile photos	Everybody
Bio	Everybody
Date of Birth	Nobody
Forwarded messages	Everybody
Calls	Nobody
Groups & channels	Everybody
Voice messages	Everybody
Messages	Everybody

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

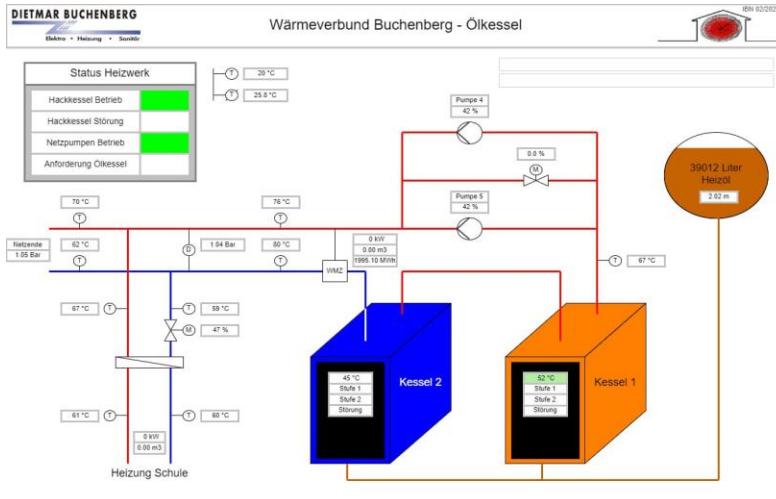
in response to their support and massacres against our people in Gaza.

#LulZsec_Muslims

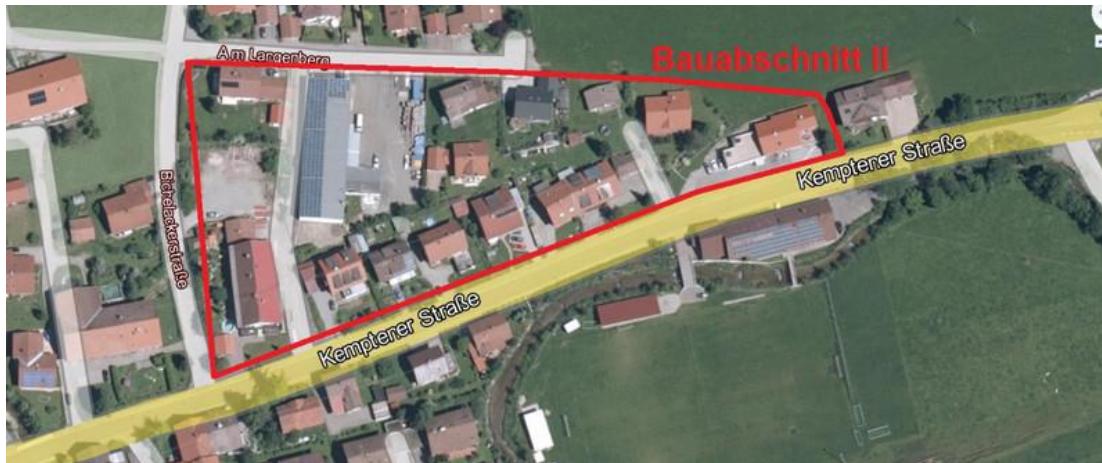
 9  3  2  1

1185 edited 10:35 PM

Use Case - Lulzsec Muslims



Use Case - Lulzsec Muslims



Use Case - Lulzsec Muslims



About

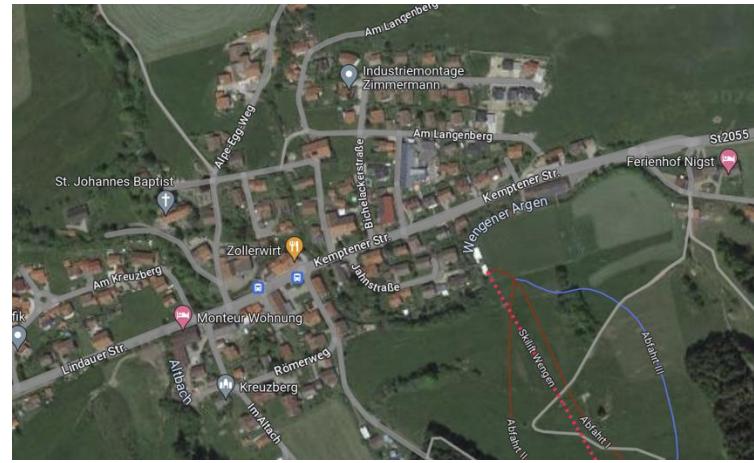
Weitnau is a municipality in the rural district Oberallgäu in Bavaria/Germany. Together with the neighboring municipality of Missen-Wilhams, Weitnau shares an administrative unit. [Wikipedia](#)

Elevation: 2,615'

Postal code: 87480

Population: 5,172 (Dec 31, 2008)

Area: 25.18 mi²



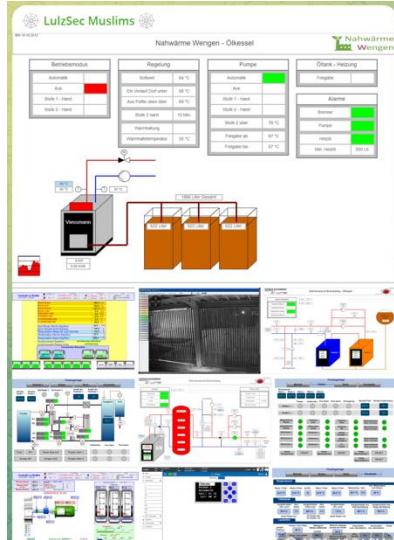
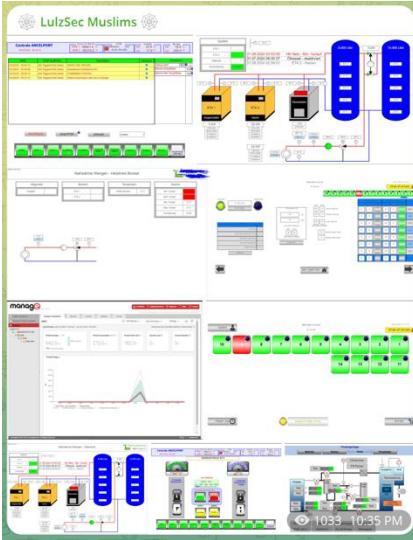
Use Case – Lulzsec Muslims



Centrale Le Rodier	27874.1 H	1 ^{er} Intérieure	1 ^{er} Extérieure	LOGIN						
31/12/1969 23:00:00	180 Kw 0.0 40 V	Local GENE 180 KW 25.9 °C Local GENE 40 KW 30.5 °C	Dégrilleur: 23.1 °C Extérieur: 18.8 °C	Utilisateur: admin Accès Déverrouillé						
Niveau Amont	189.0 mm									
Niveau Aval	195.0 mm									
Niveau Rivière	-441.0 mm									
Niveau Canal	0.0 mm									
PUISSEANCE G180	0.0 KW									
PUISSEANCE G40	33.6 KW									
% OUVERTURE G180	0.0 %									
% OUVERTURE G40	96.9 %									
Seuil Niveau Marche Dégrilleur	45.0 mm									
Seuil Intensité Arrêt Dégrilleur	100.0 A									
Temporisation Retard sur seuil Intensité	100.0 S									
Temporisation Marche Dégrilleur	75.0 M									
Temporisation Repos Dégrilleur	999.0 Mn									
Fonctionnement Dégrilleur :	AUTOMATIQUE SUR SEUIL									
Fonctionnement pompes à eau :	AUTOMATIQUE									
Commandes Manuelles										
PMP EAU N°1	PMP EAU N°2	ARRIÈRE	AVANT							
HOME	G180	ALARME	COURBES	Degrilleur	Reglage	Mesure	NEONS	NEON G2	ECL CANAL	EXTÉRIEUR

Centrale ANCELPONT		Temps De Marche	LOGIN	Centrale	Barrage
30/07/2024 06:10:51		GENE 1: 56821.0 H GENE 2: 65218.2 H	Utilisateur: Null Accès Vérouillé	INT 23.8 °C Ext 17.6 °C	INT 19.3 °C Ext -350.0 °C
DATE	ETAT ALARMES	Description	Selection	Compteurs	
07/29/24 - 00:09:14	Not Triggered Not Acked	DEFAULT EDF (MICOM)	<input checked="" type="checkbox"/>	Defaut EDF	RAZ 4
07/29/24 - 00:09:08	Not Triggered Not Acked	Emballage Génératrice N°1	<input checked="" type="checkbox"/>	Alarme Acquittées	100
07/29/24 - 00:09:14	Not Triggered Not Acked	COMMANDES FORCES	<input checked="" type="checkbox"/>	Alarme Non Acquittées	100
07/28/24 - 05:57:15	Not Triggered Not Acked	Défaut transmission adsl vers le barrage	<input checked="" type="checkbox"/>		

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



JOINT CYBERSECURITY ADVISORY

Co-Authored by:



TLP:CLEAR Product ID: AA23-335A
December 1, 2023

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



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



 SHODAN Explore Downloads Pricing ↗  Account

TOTAL RESULTS **842**

TOP COUNTRIES



Spain	109
Australia	83
Italy	71
United States	50
France	47
More...	

TOP PORTS

[View Report](#) [Download Results](#) [Historical Trend](#) [Browse Images](#) [View on Map](#) [Advanced Search](#)

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

213.134.226.17
 fth-213-134-226-017solco
 n.nl
 DSL Solcon KPN

 Netherlands, Amsterdam


Unitronics PCOM:
 Model: V578-57-T20 / V298-19-T20
 Hardware Version: E
 OS Version: 3.8
 OS Build: 2
 UID Master: 1
 PLC Name: ZwbLooermarkBathmen
 PLC Unique ID: 14452997

2024-08-07T22.22.42.224741

77.131.6.13
 13.6.131.77.rev.sfr.net
 DSL

 France, Tourcoing


Unitronics PCOM:
 Model: V588-35-R34
 Hardware Version: B
 OS Version: 4.12
 OS Build: 38
 UID Master: 127
 PLC Name: Amour@8-Direct23
 PLC Unique ID: 11600390

2024-08-07T22.15.00.413982

Use Case - Cyber Av3ngers



213.134.226.17

ftth-213-134-226-017solco
n.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

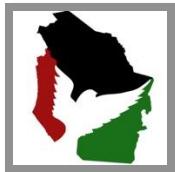
Use Case - Cyber Av3ngers



Zwembad Looermark

1.5K likes • 1.7K followers

Use Case - Cyber Av3ngers



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

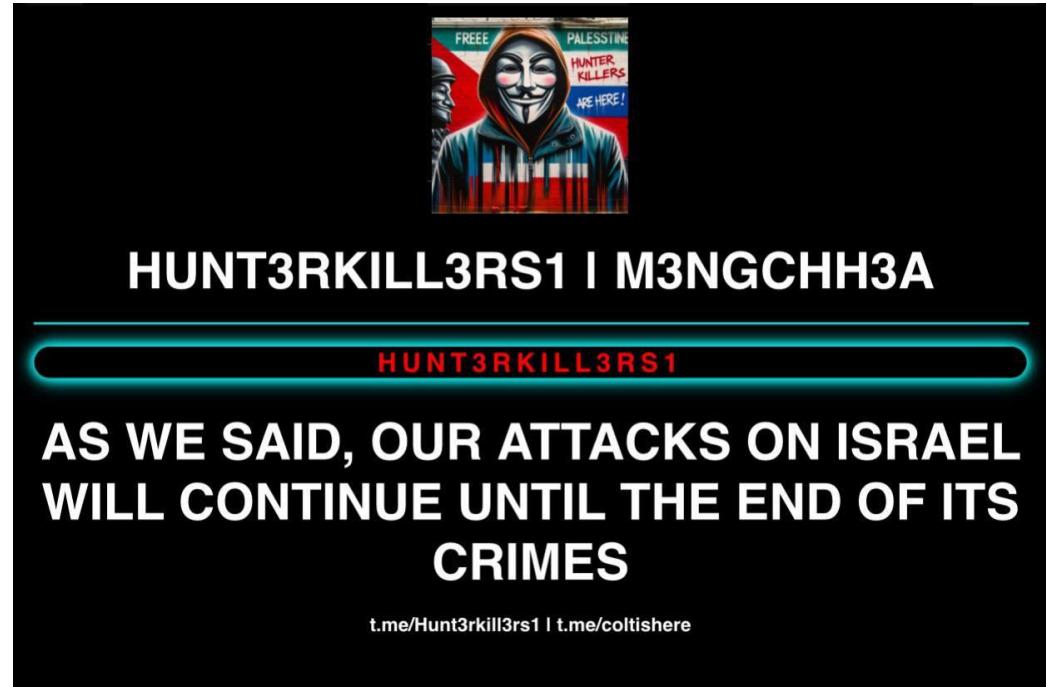


Use Case - Cyber Av3ngers

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



Use Case – Hunt3r Kill3rs



HUNT3RKILL3RS1 | M3NGCHH3A

HUNT3RKILL3RS1

AS WE SAID, OUR ATTACKS ON ISRAEL
WILL CONTINUE UNTIL THE END OF ITS
CRIMES

t.me/Hunt3rkill3rs1 | t.me/coltishere

Use Case - Hunt3r Kill3rs



Allen-Bradley 1766-L32AWAA B/13.00 Rockwell Automation

Home

- Expand
- Minimize
- Home
- Data Views
- User Provided Pages
- Diagnostics
- Administrative Settings

Device Name	1766-L32AWAA B/13.00
Device Description	MicroLogix 1400 Processor
Device Location	
Ethernet Address (MAC)	00-1D-9C-A4-D2-7D
IP Address	192.168.100.21
OS Revision	Series B FRN 13.0
HTML File Revision	2.3
Current Time	RTC is disabled
CPU Mode	Remote Run

Resources
Visit AB.com for additional information

Contacts

Copyright © 2008 Rockwell Automation, Inc. All Rights Reserved.

1763-L16DWD B/12.00

Home

- Home
- Data Views
- Data Views New Data View**
- Diagnostics
- Diagnostic Overview Net
- Administrative Settings
- User Management

Device Name	1763-L16DWD B/12.00
Device Description	MicroLogix 1100 Processor
Device Location	
Ethernet Address (MAC)	00-1D-9C-A0-69-8D
IP Address	166.239.207.55
O/S Revision	Series B FRN 12.0
HTML File Revision	1.10
Current Time	Jul 4 2024, 15:47: 8
CPU Mode	Remote Run

Resources
Visit AB.com for additional information

Contacts

Copyright © 2005 Rockwell Automation, Inc. All Rights Reserved.

Use Case - Hunt3r Kill3rs



1766-L32AWAA B/15.00

Rockwell Automation

Home

- Expand**
- Minimize**
- Home**
- Data Views**
- User Provided Pages**
- Diagnostics**
- Administrative Settings**

Device Name	1766-L32AWAA B/15.00
Device Description	MicroLogix 1400 Processor
Device Location	
Ethernet Address (MAC)	00-1D-9C-A7-9F-13
IP Address	192.168.13.100
OS Revision	Series B FRN 15.0
HTML File Revision	2.3
Current Time	RTC is disabled
CPU Mode	Remote Run

Resources

Visit AB.com for additional information

Contacts

Copyright © 2008 Rockwell Automation, Inc. All Rights Reserved.

Allen-Bradley 1766-L32AWAA B/15.00						Rockwell Automation
Event		Data View				Action Data View
No.	File Name	File Type	Display	# of Element	Access Group	
1	00	Object	0	0	Administrator	
2	01	Object	1	Binary	Administrator	
3	02	Status	66	Headline	Administrator	
4	03	Binary	10	Binary	Administrator	
5	04	Timer	100	Structure	Administrator	
6	05	Counter	30	Structure	Administrator	
7	06	Counter	1	Structure	Administrator	
8	07	Integer	170	Structure	Administrator	
9	08	Object	60	Structure	Administrator	
10	09	Binary	4	Binary	Administrator	
11	010	Integer	40	Structure	Administrator	
12	MELI	Message	60	Structure	Administrator	
13	011	PCD	1	Structure	Administrator	
14	012	Integer	40	Structure	Administrator	
15	013	Integer	40	Structure	Administrator	
16	014	Integer	40	Structure	Administrator	
17	015	Integer	40	Structure	Administrator	
18	016	Integer	40	Structure	Administrator	
19	017	Integer	20	Structure	Administrator	
20	018	Integer	20	Structure	Administrator	
21	019	Integer	30	Structure	Administrator	
22	020	Binary	1	Binary	Administrator	

Copyright © 2008 Rockwell Automation, Inc. All Rights Reserved.

Use Case - Hunt3r Kill3rs



Allen-Bradley 1766-L32AWAA B/13.00 Rockwell Automation

Home

- [Expand](#)
- [Minimize](#)
- [Home](#)
- [Data Views](#)
- [User Provided Pages](#)
- [Diagnostics](#)
- [Administrative Settings](#)

Device Name	1766-L32AWAA B/13.00
Device Description	MicroLogix 1400 Processor
Device Location	
Ethernet Address (MAC)	00-1D-9C-A4-D2-7D
IP Address	192.168.100.21
OS Revision	Series B FRN 13.0
HTML File Revision	2.3
Current Time	RTC is disabled
CPU Mode	Remote Run

Resources
Visit AB.com for additional information

Contacts

Copyright © 2008 Rockwell Automation, Inc. All Rights Reserved.

1763-L16DWD B/12.00

Home

- [Home](#)
- [Data Views](#)
- [Data Views New Data View](#)
- [Diagnostics](#)
- [Diagnostic Overview Net](#)
- [Administrative Settings](#)
- [User Management](#)

Device Name	1763-L16DWD B/12.00
Device Description	MicroLogix 1100 Processor
Device Location	
Ethernet Address (MAC)	00-1D-9C-A0-69-8D
IP Address	166.239.207.55
O/S Revision	Series B FRN 12.0
HTML File Revision	1.10
Current Time	Jul 4 2024, 15:47: 8
CPU Mode	Remote Run

Resources
Visit AB.com for additional information

Contacts

Copyright © 2005 Rockwell Automation, Inc. All Rights Reserved.

Use Case - Hunt3r Kill3rs



Allen-Bradley 1766-L32AWAA B/13.00 Rockwell Automation

Home

- Expand
- Minimize
- Home
- Data Views
- User Provided Pages
- Diagnostics
- Administrative Settings

Device Name	1766-L32AWAA B/13.00
Device Description	MicroLogix 1400 Processor
Device Location	
Ethernet Address (MAC)	00-1D-9C-A4-D2-7D
IP Address	192.168.100.21
OS Revision	Series B FRN 13.0
HTML File Revision	2.3
Current Time	RTC is disabled
CPU Mode	Remote Run

Resources
Visit AB.com for additional information

Contacts

Copyright © 2008 Rockwell Automation, Inc. All Rights Reserved.

1763-L16DWD B/12.00

Home

- Home
- Data Views
- Data Views New Data View**
- Diagnostics
- Diagnostic Overview Net
- Administrative Settings
- User Management

Device Name	1763-L16DWD B/12.00
Device Description	MicroLogix 1100 Processor
Device Location	
Ethernet Address (MAC)	00-1D-9C-A0-69-8D
IP Address	166.239.207.55
O/S Revision	Series B FRN 12.0
HTML File Revision	1.10
Current Time	Jul 4 2024, 15:47: 8
CPU Mode	Remote Run

Resources
Visit AB.com for additional information

Contacts

Copyright © 2005 Rockwell Automation, Inc. All Rights Reserved.

Use Case - Hunt3r Kill3rs





Schneider Electric

[Home](#)

[Monitoring](#)

[Control](#)

[Diagnostics](#)

[Maintenance](#)

[Setup](#)

[Logout](#)

User Accounts

Groups			
Administrators	Engineering	Operations	Maintenance
Administrator	Administrators	English
Hunt3rKill3rs	Administrators	English
Hunt3rKill3rs2	Engineering	English
		Maintenance	English

Users

Name	Password	Group	Language
Administrator	Administrators	English
Hunt3rKill3rs	Administrators	English
Hunt3rKill3rs2	Engineering	English
		Maintenance	English

PowerLogic® EGX100

WADE

Visualisation			
Commande	Diagnostic	Maintenance	Paramétrage
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

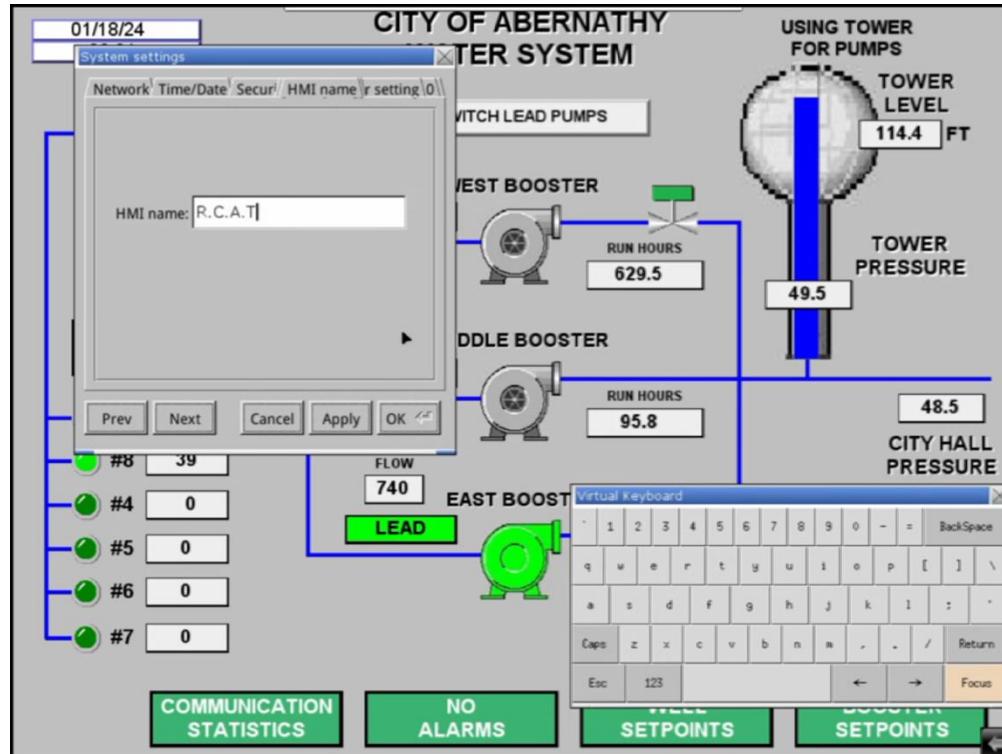


Use Case – Hunt3r Kill3rs

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



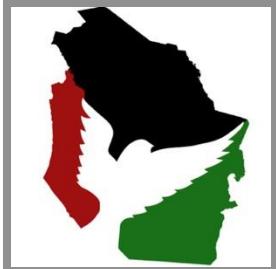
Conclusion



"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

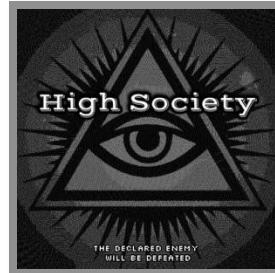


PWN'D LOL

<https://t.me/CyberAveng3rs>
<https://twitter.com/CyberAveng3rs>



<https://t.me/FiveFamilies>



<https://t.me/highsociety>



https://t.me/CyberArmyofRussia_Reborn



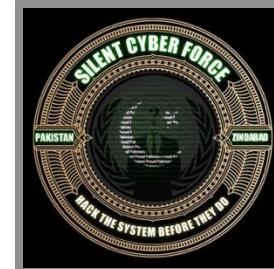
<https://t.me/Hunt3rkill3rs>



https://t.me/freepalestine_PPHM



https://t.me/LulzsedMuslims_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](#)

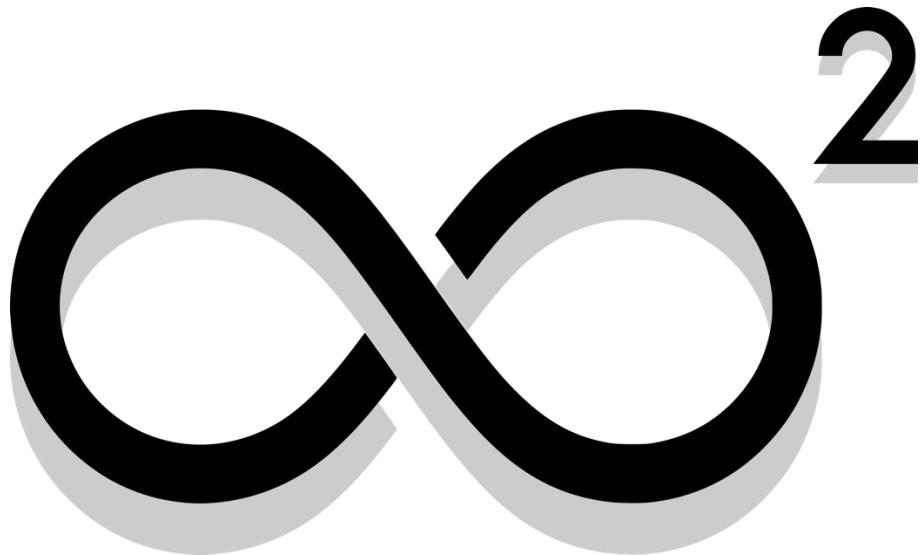
He'd say that at the beginning of his talks.

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@infntysqr.com