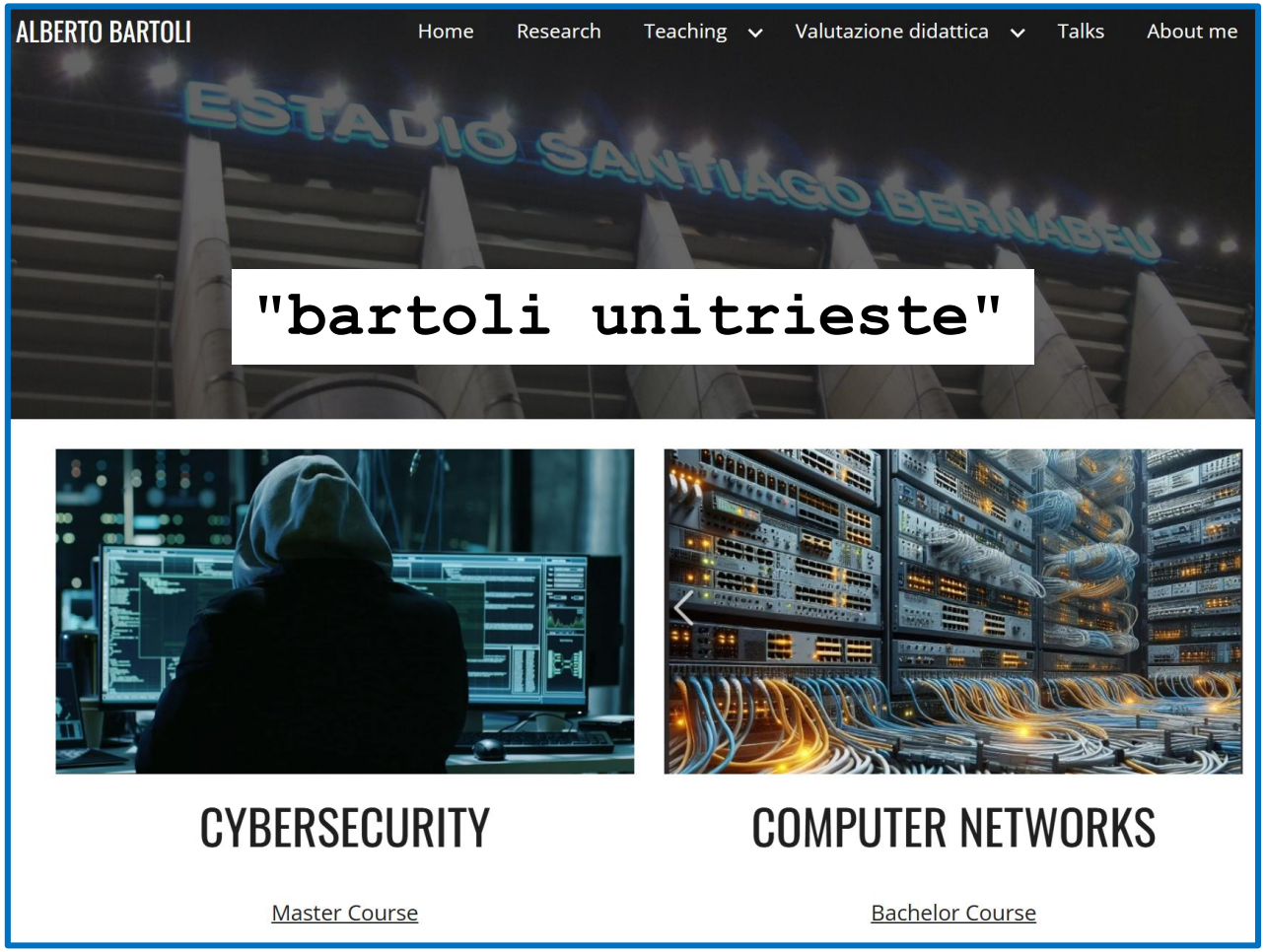
Cyber(in)security: il grave rischio invisibile per le nostre case, ospedali, industrie, pubbliche amministrazioni

Alberto Bartoli – https://bartoli.inginf.units.it

Who am I


ALBERTO BARTOLI
Home
Research
Teaching
Valutazione didattica
Talks
About me
ESTADIO SANTIAGO BERNABEU
"bartoli unitrieste"
CYBERSECURITY
Master Course
COMPUTER NETWORKS
Bachelor Course

What many people think

- Cybersecurity:
  - Only relevant for **software companies**
  - Only relevant for **IT specialists**

What you (hopefully) will think

- Cybersecurity:
  - ~~Only relevant for **software companies**~~
  - ~~Only relevant for **IT specialists**~~
  - Crucial in **every** type of **organization**
  - Relevant for **every** type of **specialist**

Why?

- Cybersecurity:
  - Crucial in **every** type of **organization**
  - Relevant for **every** type of **specialist**

- Software is **everywhere**
  - Cars, Ships, Aircrafts (engine, brakes, helm,...)
  - Healthcare (insulin pump, electrocardiograph,...)
  - ...
  - **Industrial Control Systems**
  - ...

Our roadmap

- Part 1
  - **Peculiarity** of computers and their **implications** (Examples shown in my recent talks)
- Part 2
  - Key **examples** of **state-sponsored** cybersecurity attacks
- Part 3
  - Where we are heading

Part 1

- **Peculiarity** of computers and their **implications**

- Examples that I have already shown in 1/2 recent talks

Miele Washer-Disinfector PG 8528

≈ Washing Machine:

- Disinfect medical and laboratory equipment
- Prevent contamination that can cause diseases such as cancer, asthma, skin irritation,...

A brave new world (?)

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / ICS Advisory / Miele Professional PG 85 Series

ICS ADVISORY

Miele Professional PG 85 Series

Last Revised: May 18, 2017 **Alert Code:** ICSA-17-138-01

The **America's Cyber Defense Agency**?

For a **washing machine**?

A brave new world (?)

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Topics Spotlight Resources & Tools News & Events Careers About

Home / News & Events / Cybersecurity Advisories / ICS Advisory / Miele Professional PG 85 Series

ICS ADVISORY

Miele Professional PG 85 Series

Last Revised: May 18, 2017 **Alert Code:** ICSA-17-138-01

A **web server** embedded in a **washing machine**?

AFFECTED PRODUCTS

Miele Professional reports that the following versions of the PG 85 product series, a large capacity cleaner and disinfector, and their embedded webservers are affected:

Only about "data"? Just an "IT issue"?

ICS ADVISORY

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Miele Professional PG 85 Series

IMPACT

Successful exploitation of this vulnerability could allow a remote attacker to read or modify sensitive data or files, execute unauthorized code or commands, and possibly cause a system crash.

ATTENTION: Remotely exploitable/low skill level to exploit. Public exploits are available.

Only about "data"? Just an "IT issue"?

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities

IMPACT

Successful exploitation of these vulnerabilities may allow a nearby attacker to gain unauthorized access to a pacemaker and issue commands, change settings, or otherwise interfere with the intended function of the pacemaker.

A nice conference

17th
AUTOMOTIVE
WORLD 2025
(organized by RX Japan)
January 22 – 24, 2025
Tokyo Big Sight, Japan

Tesla

In-Vehicle Infotainment (IVI)

Electric Vehicle Chargers

A nice conference??? (I)

PWN2OWN AUTOMOTIVE

17th AUTOMOTIVE WORLD 2025
(organized by RX Japan)
January 22 – 24, 2025
Tokyo Big Sight, Japan

Pwn2Own Automotive Cybersecurity Challenge 2025

A **cybersecurity challenge** with **cars**???

A nice conference??? (II)

Pwn2Own Automotive 2025: Tesla EV Charger Exploits Take the Spotlight on Day Two

January 23, 2025

Day two of Pwn2Own Automotive 2025 was a "Tesla EV charger kind of day," with four Tesla Wall Connectors targeted. The day closed with an impressive haul of 23 unique zero-day vulnerabilities, surpassing the 16 uncovered on day one.

Pwn2Own Automotive 2025: Day One Uncovers 16 Unique Zero-Day Vulnerabilities

January 22, 2025

A total of 16 unique zero-day vulnerabilities were discovered on day one of Pwn2Own Automotive 2025, the world's largest zero-day vulnerability discovery contest focused on connected cars and software-defined vehicles.

Only about "data"? Just an "IT issue"?

Category	Impact
Electric Vehicle Chargers	Bypass authentication on the system.
In-Vehicle Infotainment (IVI)	Execute code in the context of the device.
In-Vehicle Infotainment (IVI)	Compromise the integrity of downloaded information.
Electric Vehicle Chargers	Compromise the integrity of downloaded information.
Electric Vehicle Chargers	Bypass authentication on the system.
Electric Vehicle Chargers	Disclose sensitive information.
Electric Vehicle Chargers	Disclose sensitive information.
Electric Vehicle Chargers	Execute code in the context of the device.
Electric Vehicle Chargers	Execute code in the context of the device.
Operating System	Disclose sensitive information.

« ‹ 1 2 4 5 ... 10 › »

Showing 1 to 10 of 96 entries

Solar Power for Electricity Generation

195 GW in 19 countries
(20% solar production worldwide)

Barcelona or Munich might use 1–2 GW.

Only about "data"? Just an "IT issue"?

60 Hurts per Second – How We Got Access to Enough Solar Power to Run the United States

Bitdefender

August 07, 2024

Vulnerabilities in the Solarman platform

Bitdefender-PReport-solarman-creat7907.pdf • 974 KB

1. **Full Account Takeover**: The Solarman platform's `/oauth2-s/oauth/token` API endpoint

Regulating the Power Grid

- Radio Ripple Control: A radio protocol to either **feed power** into or **ditch power** from **the grid**
- Used throughout Central Europe to … **regulate** the amount of power renewable electric generation facilities feed into the grid
- Approximately **60 GW** in Germany
  - Barcelona or Munich might use 1–2 GW.

Only about "data"?
Just an "IT issue"?

ars TECHNICA AI BIZ & IT CARS CULTURE GAMING HEALTH POLICY SCIENCE SECURITY SPACE TECH FORUM SUBSCRIBE

POWER FAILURE

Researchers say new attack could take down the European power grid

Power grid in Central Europe uses unencrypted radio signals to add and shed loads.

DAN GOODIN – JAN 23, 2025 1:00 PM | 63

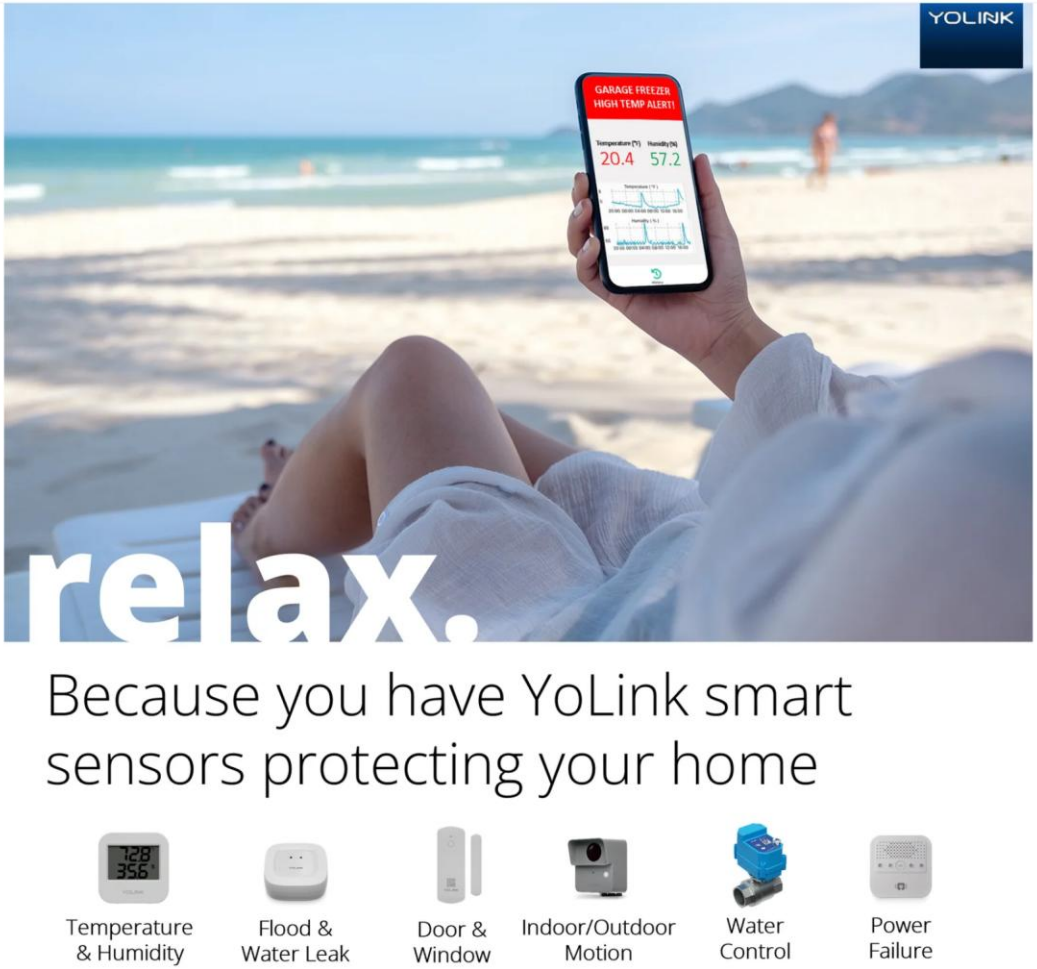
db-tronic Flipper Zero | Strumento multifunzionale

Marca: db-tronic

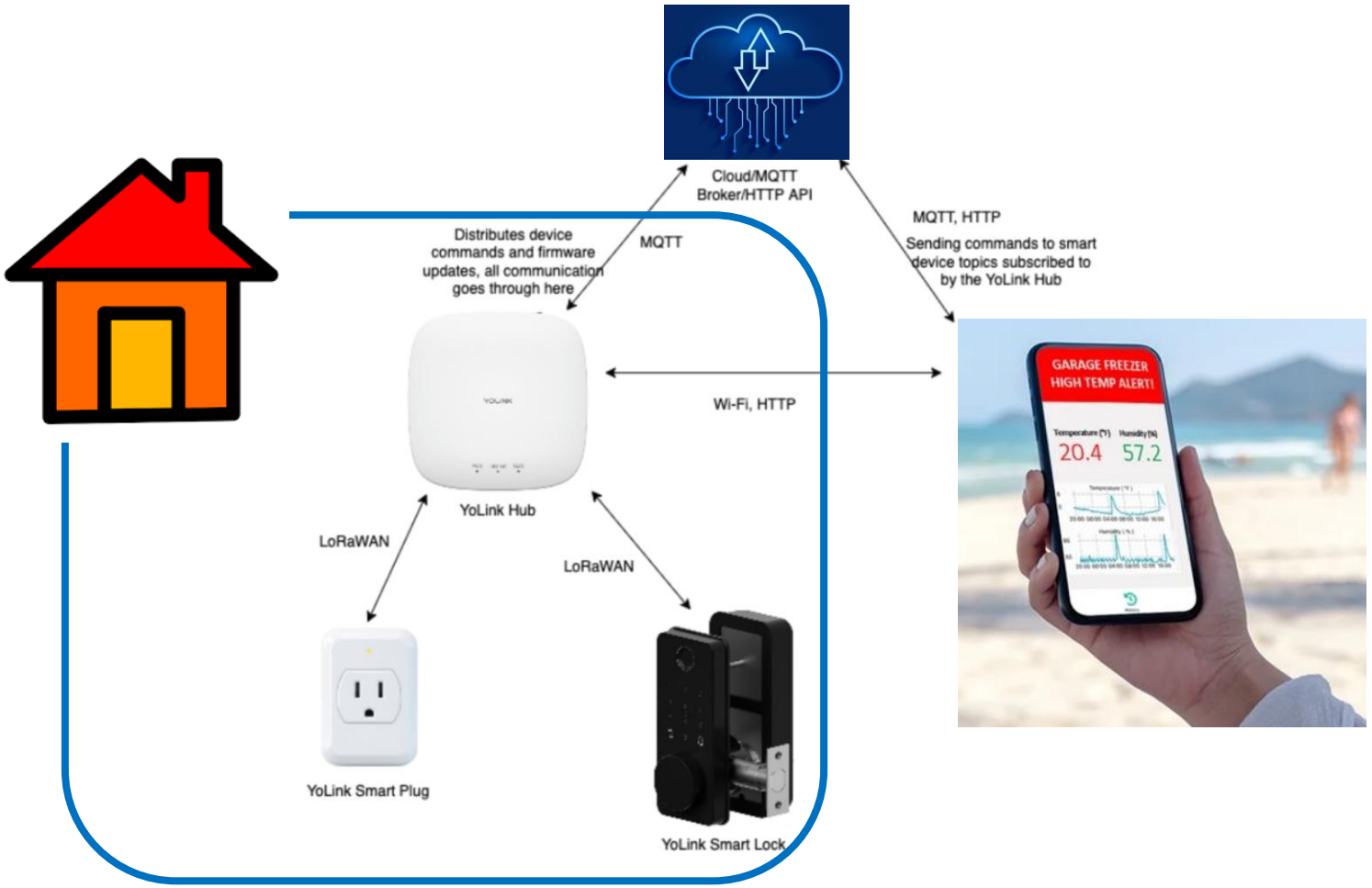
4,1 ★★★★☆ 40 voti | Cerca in questa pagina

209⁹⁰ €

Smart (?) Home (I)


YOLINK
GARAGE FREEZER
HIGH TEMP ALERT!
20.4
57.2
relax.
Because you have YoLink smart sensors protecting your home
Temperature & Humidity
Flood & Water Leak
Door & Window
Indoor/Outdoor Motion
Water Control
Power Failure

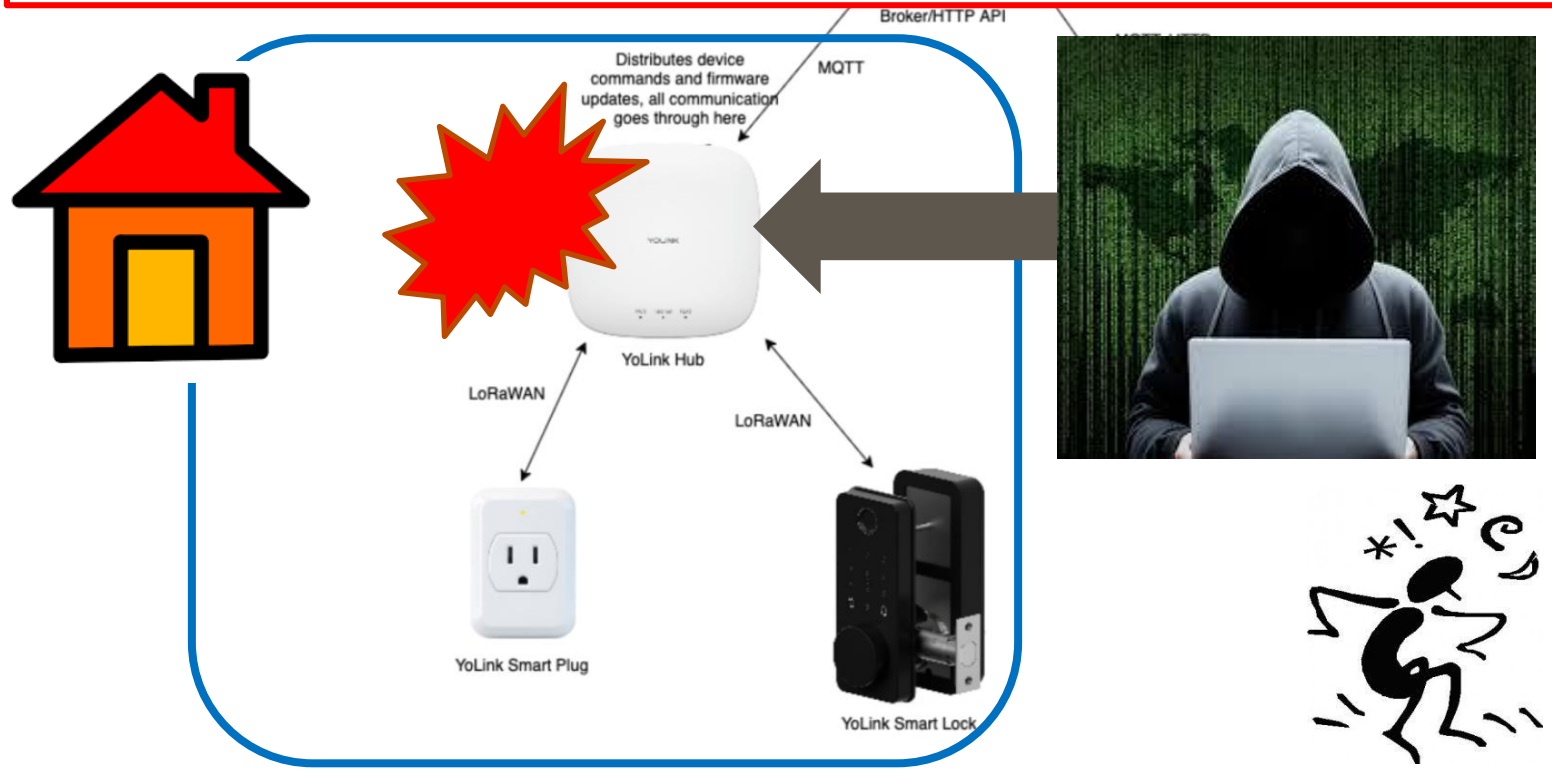
Smart (?) Home (II)



Opsss...

Key Findings:

Authorization bypass → *attackers can remotely control other users' devices.*



What many people think

- Cybersecurity:
  - Only relevant for **software companies**
  - Only relevant for **IT specialists**

Keep in mind #1

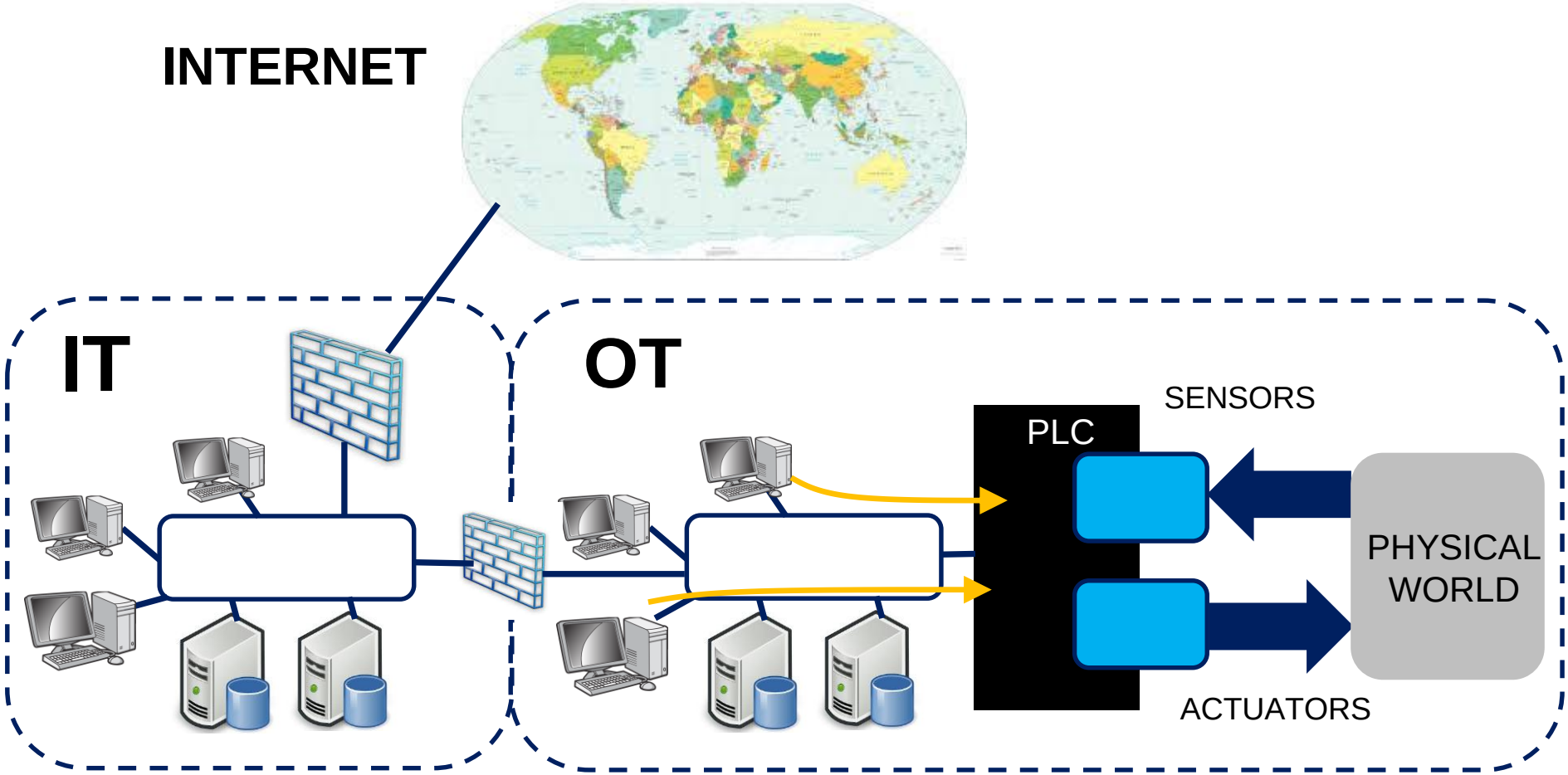
- Computers no longer operate just on **"files"**
- They also operate on the **"physical world"**
  - **Read** information (**sensors**)
    - Temperature, Pressure, Concentration,...
  - **Write** information (**actuators**)
    - Motors, Valves, ...

- Can you name a technology where computers are not essential?

Keep in mind #2

- **Every** sw **may** have **vulnerabilities**
  - **Mistakes** in design / implementation / deployment that might allow "**unintended** and **undesired**" behavior
- **Some** vulnerabilities allow **arbitrary** usage (!) by a **remote** attacker (!!)
- Read it again. Then read it again
- **Only** technology in human history with this feature

ICS: Industrial Control Systems

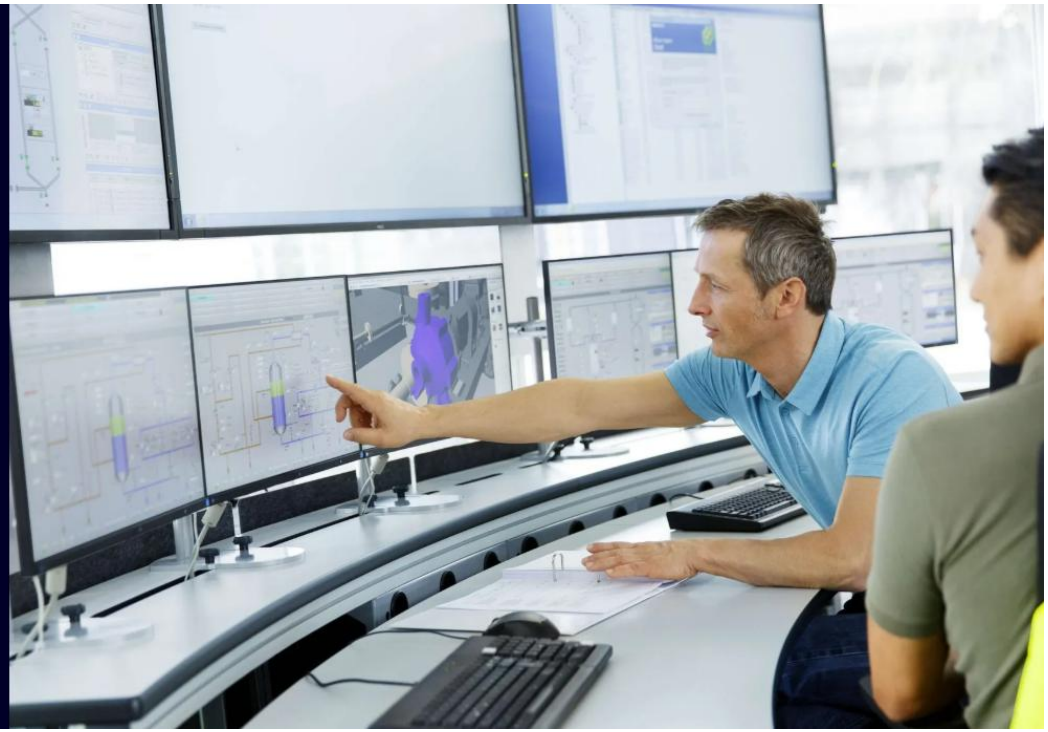


Siemens Telecontrol Server (I)

Telecontrol solutions for the control center

With our high-performance telecontrol systems, you can efficiently monitor and control plants from the control center. In this way, you're making an important contribution to meeting the constantly growing requirements for plant availability and cost-efficiency in industry.

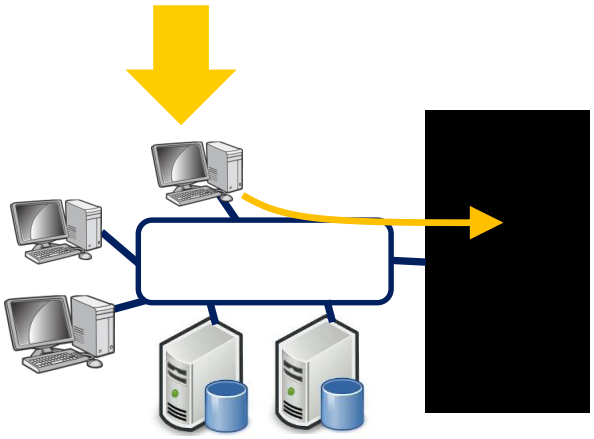
TIA Selection Tool



Siemens Telecontrol Server (II)

- Interface between the operator and the **PLCs**
  - Process **visualization** and operator **control**
  - **Alarm** display
  - Machine **parameter** management

- Used in many industries:
  - Food and beverage,
  - Water and wastewater,
  - Oil, gas, chemical
  - Critical manufacturing



November 14, 2024

ICS ADVISORY

Siemens TeleControl Server

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Release Date: November 14, 2024 **Alert Code:** ICSA-24-319-10

1. EXECUTIVE SUMMARY

- **CVSS v4 10.0**
- **ATTENTION**: Exploitable remotely/low attack complexity

Successful exploitation of this vulnerability could allow an unauthenticated attacker t
execute arbitrary code on the device.

Siemens today: they have a CERT (!)

Siemens ProductCERT and Siemens CERT

Siemens ProductCERT is a team of security experts managing security issues (receipt, investigation, coordination, reporting) for Siemens products, solutions and services. ProductCERT builds global relationships to enhance product security.

ID	CVSS Score	Document Title
SSA-212953	10	Multiple Vulnerabilities in COMOS
SSA-089022	10	Multiple Vulnerabilities in Third-Party Components in SINEC OS before V3.3
SSA-014678	10	Authorization Bypass Vulnerability in Industrial Edge Device Kit
SSA-001536	10	Authorization Bypass Vulnerability in Siemens Industrial Edge Devices
SSA-430425	9.9	Multiple Vulnerabilities in SINEC Security Monitor before V4.9.0

66 entries

Jan-Apr 2026

Siemens is NOT the problem

Insecure by Design in the Backbone of Critical Infrastructure

Jos Wetzels
Forescout
United States
jos.wetzels@forescout.com

Daniel dos Santos
Forescout
United States
daniel.dossantos@forescout.com

Mohammad Ghafari
TU Clausthal
Germany
mohammad.ghafari@tu-clausthal.de

CPS-IoT Week '23

- We inspected 45 actively deployed Operational Technology (OT) product families from 10 major vendors and found that **every system suffers from at least one trivial vulnerability**.

- We reported a total of 53 weaknesses…They enable attackers to:
  - take a device offline,
  - manipulate its operational parameters,
  - and execute arbitrary code without any constraint.

Certified Secure (?)

- We noted that 74% of the products had achieved one or more of the following certifications…products that were IEC 62443 certified, suffered from issues which **should have been caught by these standards**.

- This suggests that **apart from what the standards may not cover**, even the things they do cover are **not** always properly covered in practice

Keep in mind #3

- Computers "read / write on the physical world"

  +

- Every sw may have vulnerabilities

- The functioning of **every industrial plant** might be deeply altered from a remote location

One of the many possibilities

- The functioning of **every industrial plant** might be **deeply altered from a remote location**

- Sensors display A (while the **actual** reading is B)
- Actuators execute A (while **instructed** to do B)
- Read it again. Then read it again.

Not a theoretical possibility! (April 2026)

Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure

April 7, 2026

- Iran-affiliated actors are conducting exploitation activity targeting … PLCs manufactured by Rockwell Automation/Allen-Bradley.

- This activity has led to PLC disruptions across several U.S. critical infrastructure sectors through …manipulation of data on human machine interface (HMI) and supervisory control and data acquisition (SCADA) displays, resulting in operational disruption

Remark

- We have briefly mentioned:
  - Things that **might** occur
  - Only **one** real attack

Part 2

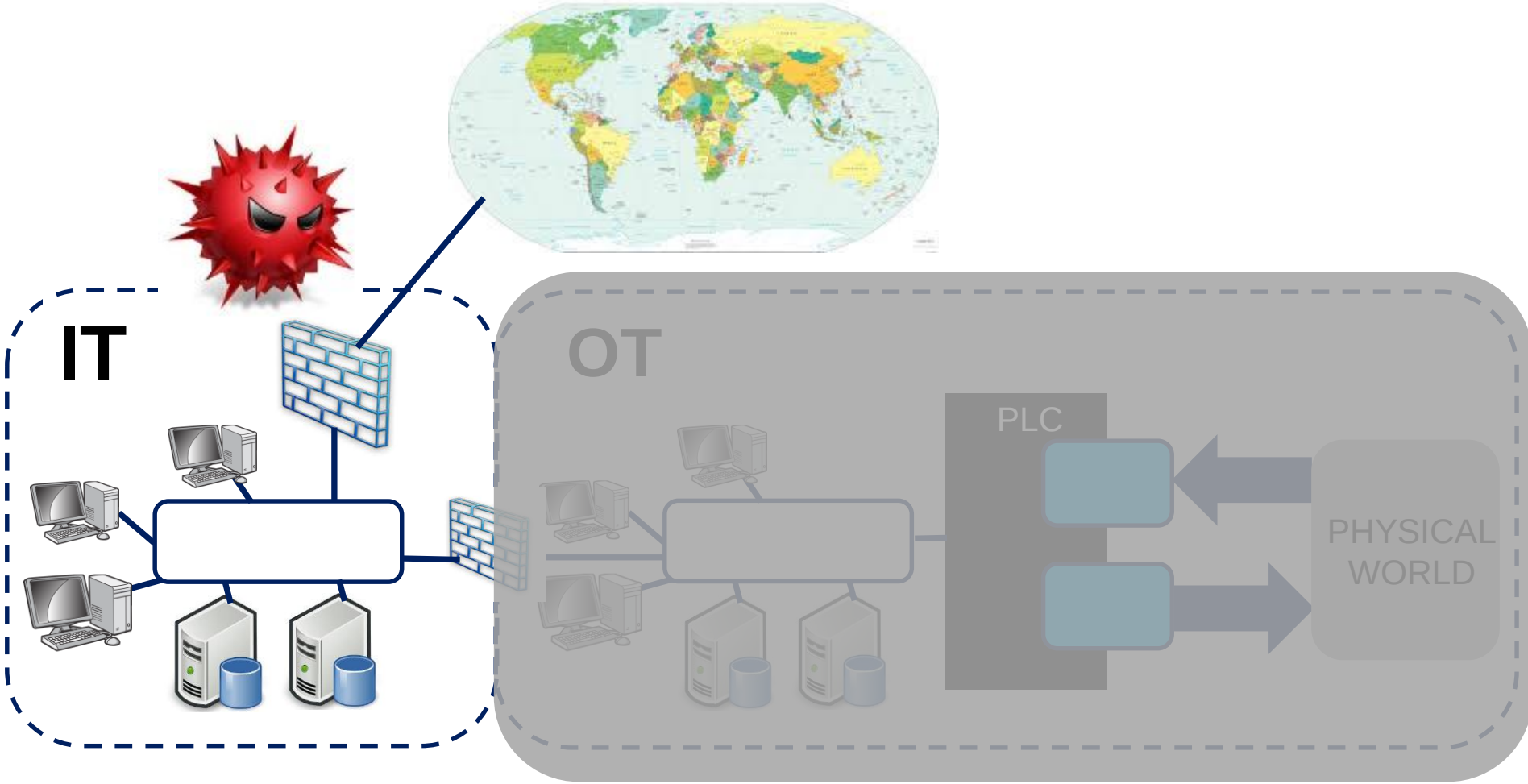
- Key **examples** of **state-sponsored** cybersecurity **attacks**

Our path

- Examples of major attacks in **non-IT domains**

1. By **criminal organizations**
2. What makes **state-sponsored** attacks different

Very well known problem



MANY examples

MOTHERBOARD | By Lorenzo Franceschi-Bicchierai | Mar 19 2019, 5:33pm
TECH BY VICE

Ransomware Forces Aluminum Manufacturing Giant to Shut Down Network Worldwide 160 plants, 40 countries, 35K people

Colonial Pipeline Cyber Incident

Office of Cybersecurity, Energy Security, and Emergency Response

- 45% **FUELS** on the East Coast (**including aircrafts**)
- distribution completely suspended for 1 week

ONE recent incident (September 2025)

> Jaguar Land Rover shutdown extended to next week
>
> BBC

- A cyber attack which has **halted production** at Jaguar Land Rover (JLR) factories **across the world** could be costing the firm "**around £5m a day**" in lost profits
- The company usually builds 1,000 cars a day…**more than two full weeks of global output** will have been lost.

Horrible! No more beer! (October 2025)

Asahi restarts beer production after cyber-attack

BBC

- Asahi is the **biggest brewer** in Japan.
- The production systems at the factories themselves had not been affected by the cyber-attack, but it had been **forced to halt production** because **it could not process orders and shipments**.

Maritime Ports: Nagoya (July 2023)

Japan's Busiest Port Restarts Operations After Ransomware Attack

SECURITY MANAGEMENT
A PUBLICATION OF ASIS INTERNATIONAL

6 July 2023

- Japan's Port of Nagoya handles the **largest amount of cargo** for the nation, roughly 177.79 million tons *(≈Trieste x 3)*

- It is **gradually resuming** operations after a **ransomware attack**…that resulted in a **halt of operations** on the morning of 4 July.

Hhmmm…

- We see **IT attacks** everywhere every day
- Why don't we see **ICS attacks**?

There have been (and are) many

History of Industrial Control System Cyber Incidents

TECHNICAL REPORT · 31 December 2018

- For **many years** malicious cyber actors have been targeting the ICS that manage our critical infrastructures.
- **Most of these events are not reported to the public**, and the threats and incidents to ICS are not as well-known as enterprise cyber threats and incidents.

Cybersecurity 101: Why?

- **Motivations**
  1. Money
  2. Espionage (Information gathering)
  3. Disruption and Sabotage

- **Money** is by far the **most common** motivation

Cybersecurity 101: Who?

- **Motivations**
  1. Money
     - **Criminal** organizations
  2. Espionage (Information gathering)
  3. Disruption and Sabotage
     - **State-sponsored** groups

- Many more criminal organizations than state-sponsored groups

What State Attackers do

- Espionage (Information gathering)
  - **A lot**
  - Mostly unreported to the public

- Disruption and Sabotage
  - **Rare** for strategic reasons (at least so far)
  - You do **not** want to:
    - Make your adversaries **aware** of how **weak** their defenses are
    - **Reveal your capabilities**

A few examples

- Espionage (Information gathering)
- Disruption and Sabotage

- They occur **more and more often**

Espionage (I)

Review of the Summer 2023 Microsoft Exchange Online Intrusion

CYBER SAFETY REVIEW BOARD

EXECUTIVE SUMMARY

In May and June 2023, a threat actor compromised the Microsoft Exchange Online mailboxes of 22 organizations and over 500 individuals around the world. The actor—known as Storm-0558 and assessed to be affiliated with the People's Republic of China in pursuit of espionage objectives—accessed the accounts using authentication tokens that were signed by a key Microsoft had created in 2016. This intrusion compromised senior United States government representatives working on national security matters, including the email accounts of Commerce Secretary Gina Raimondo, United States Ambassador to the People's Republic of China R. Nicholas Burns, and Congressman Don Bacon.

Espionage (II-a)

Gli Stati Uniti non riescono a togliere gli hacker cinesi dai loro telefoni

il POST

24 novembre 2024

Il gruppo "Salt Typhoon" è da mesi nei server delle principali aziende di telecomunicazioni americane

- Oltre ad avere «ascoltato in tempo reale» le conversazioni di importanti figure politiche e istituzionali (Trump, Vance, collaboratori di Kamala Harris), Salt Typhoon è riuscito a ottenere un elenco quasi completo dei numeri di telefono di persone sottoposte a intercettazioni perché sospettate di spionaggio.
- Informazioni importanti, perché consentono all'intelligence cinese di avere un quadro piuttosto attendibile delle spie già identificate dall'intelligence statunitense.

Espionage (II-b)

Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

September 03, 2025

- ...telecommunications, government, transportation, lodging, and military **infrastructure** networks.... These actors often modify routers to maintain **persistent**, long-term access to networks.

- Italian External Intelligence and Security Agency (AISE) - Agenzia Informazioni e Sicurezza Esterna
- Italian Internal Intelligence and Security Agency (AISI) - Agenzia Informazioni e Sicurezza Interna

Espionage (III)

US Treasury says it was hacked by China in 'major incident'

BBC

31 December 2024

FBI says China's Salt Typhoon hacked at least 200 US companies

TechCrunch

August 27, 2025

FBI declares suspected Chinese hack of US surveillance system a 'major cyber incident'

The designation suggests the hackers successfully compromised swathes of sensitive data stored directly on FBI systems.

POLITICO

04/01/2026

Espionage (IV)

Russian GRU Targeting Western Logistics Entities and Technology Companies

PP-26-1297 | April 2026 Ver. 1.1

Executive Summary

This joint cybersecurity advisory (CSA) highlights a Russian state-sponsored cyber campaign targeting Western logistics entities and technology companies.

This cyber espionage-oriented campaign targeting logistics entities and technology companies

- Defense Industry
- Transportation and Transportation Hubs (ports, airports, etc.)
- Maritime
- Air Traffic Management
- IT Services

Are we really doing what we should?

campaign targeting Western logistics entities and technology companies. This includes those involved in the coordination, transport, and delivery of foreign assistance to Ukraine.

Executives and network defenders at logistics entities and technology companies should recognize the elevated threat of unit 26165 targeting, increase monitoring and threat hunting for known TTPs and indicators of compromise (IOCs), and posture network defenses with a presumption of targeting.

- Better not ask...

Italy is not missing just the Football World Cup…

Intelligence gathering: HOME routers

APT28 exploit routers to enable DNS hijacking operations

National Cyber Security Centre

Russian cyber actor APT28 exploit vulnerable routers to hijack DNS, enabling adversary-in-the-middle attacks and theft of passwords and authentication tokens.

PUBLISHED
7 April 2026

- The DNS hijacking operations are believed to be **opportunistic**…
- …with the actor targeting a **wide pool of victims** and then likely filtering down for users of potential intelligence value at each stage of the exploitation chain.

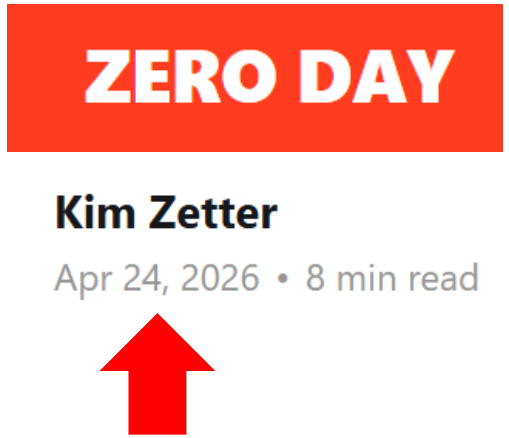
Sabotage

- Espionage (Information gathering)
- Disruption and Sabotage

- They occur **more and more often**

Sabotage prior to military attack

Mystery Around Venezuelan Cyberattack Deepens, with New Discovery of "Highly Destructive" Wiper



- "We believe that this wiper is:
  - **extremely targeted**,
  - has **no financial motivation**,
  - and aims to **erase all** of a device's files and data,"

- A couple of weeks before the USA attack to Venezuela

Sabotage during a military attack (I)

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

The hack on Ukraine's power grid was a first-of-its-kind attack that sets an ominous precedent for the security of power grids everywhere.

WIRED

KIM ZETTER

MAR 3, 2016

Sabotage during a military attack (II)

Iran claims US exploited networking equipment backdoors during strikes — says devices from Cisco and others failed despite blackout in attack that 'indicates deep sabotage'

News By Luke James published April 22, 2026

Cisco, Juniper, Fortinet, and MikroTik devices allegedly rebooted or disconnected during the conflict.

Part 3

- Where we are heading

The coming AI Apocalypse (?) (I)

- **Before** the AI hysteria:
  - **Hundreds** of **new** vulns **every week**
  - **>350K** known vulns
  - Organizations can patch **≈15%** of them
  - The world has not fallen apart
- Abundance of vulnerabilities <> Cybersec Apocalypse

The coming AI Apocalypse (?) (II)

```
while(TRUE)
  doNotBelieveTheHype();
```

Unexpected, Deeply Worrying #1

1. **Hidden Persistence**
   - **Pre-position** just in case
   - Use as needed

Hidden Persistence (I-a)

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

Release Date: February 07, 2024 **Alert Code:** AA24-038A

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assess that People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.

Hidden Persistence (I-b)

- CISA / NSA / FBI have confirmed that Volt Typhoon has compromised the IT environments of **multiple critical infrastructure organizations** — primarily in **Communications**, **Energy**, **Transportation Systems**, and **Water** and **Wastewater** Systems Sectors.

- Choice of **targets** and pattern of **behavior** is **not consistent** with **traditional cyber espionage**

- We assess with high confidence that Volt Typhoon actors are **pre-positioning themselves on IT networks to enable lateral movement to OT assets for disruptive or destructive cyberattacks** …in the event of a major crisis or conflict with the United States.

Hidden Persistence (II-a)

BPFdoor in Telecom Networks: Sleeper Cells in the Backbone

RAPID7

Mar 26, 2026

- Our investigation uncovered a **long-term** and **ongoing** operation attributed to a China-nexus threat actor.

- …long-term positioning by embedding **stealthy** access mechanisms deep inside **telecom** and **critical environments**…**dormant** footholds positioned **well in advance** of operational use.

Hidden Persistence (II-b)

- BPFdoor, a stealth Linux backdoor engineered to operate within the operating system kernel.

- BPFdoor does **not** expose **listening ports** or maintain visible **command-and-control traffic**.
- Instead, it …inspects network traffic directly inside the kernel, **activating only when it receives a specifically- crafted trigger packet**.

- The result is a **hidden trapdoor** embedded **within the operating system itself**.

Unexpected, Deeply Worrying #2

1. **Hidden Persistence**
   - **Pre-position** just in case
   - Use as needed

2. **Disruption**
   - Suddenly **stop** a **paid** service given to **other countries**
   - For mere **political** reasons

Civil servants doing their job

Credit cards cancelled, Google accounts closed: ICC judges on life under Trump sanctions

The Guardian

18 Feb 2026

Trump's sanctions on ICC halt tribunal's work, staffers claim

According to ICC staff members, sanctions imposed by the Trump administration have made it near impossible for the tribunal to conduct basic tasks, let alone seek justice for victims of war crimes.

euronews.

15/05/2025

- The court's top prosecutor had his **bank accounts closed …** and **Microsoft even canceled his ICC email address**.
- Canadian judge…**immediately lost access to her credit cards**, and Amazon's Alexa stopped responding to her.

Already occurring?

1. **Hidden Persistence**
   - **Pre-position** just in case
   - Use as needed

2. ~~Disruption~~ **Espionage**
   - Abuse Stop a **paid** service given to **other countries** (e.g., **read private** data)
   - For mere **political** reasons

What do the Danes think?

US discussing options to acquire Greenland including using military, White House says

BBC

7 January 2026

Sad but unavoidable (I)

- In the summer of 2025, **Denmark**'s government put forward a major policy change in its digital infrastructure: **moving away from using Microsoft Office 365**, and in part, open-source its operations with LibreOffice

- The **French** government referenced some of these concerns when it announced last week that 2.5 million civil servants **would stop using video conference tools from U.S. providers** — including Zoom, Microsoft Teams, Webex and GoTo Meeting — by 2027 and switch to Visio, a homegrown service.

Sad but unavoidable (II)

- **Schleswig-Holstein** fully completed the **migration of its state administration email system** — comprising more than 44,000 mailboxes and 110 million emails and calendar entries — to Open-Xchange and Thunderbird.

- **Austria's Armed Forces** have confirmed a major shift in military IT: 16,000 systems have been migrated from Microsoft Office to LibreOffice on Linux desktops. Finalized in 2025, the rollout is one of Europe's largest open-source deployments, carried out on a military scale.

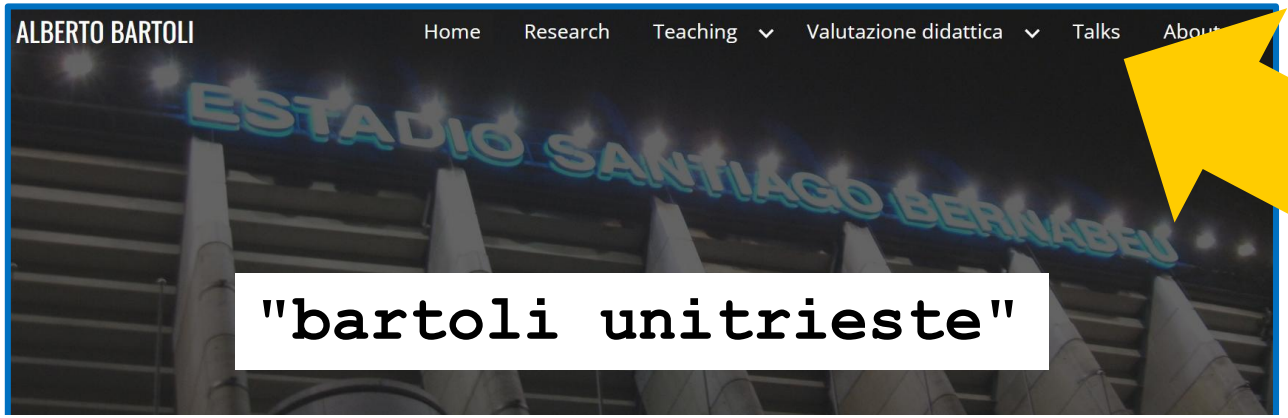
Keep in mind #4

- **Espionage** and **Sabotage**

- A new **fact of life**
  - **Stealth**
  - Potentially **pervasive**
  - From **unexpected** actors ("friends")

- **Many** implications
- Are we sufficiently **aware**?

Thanks for your attention



Anthropic Mythos - from the inside

 An excerpt from a blog post by one of the maintainers of curl. A person with a lot of "real world experience" on one of the most widely used software tools in the planet.

May 11, 2026

Cose che racconto nei corsi (e che poi si verificano) - April 2026

 Questa volta in italiano.Ogni tanto vedo notizie strettamente collegate ad argomenti di cui ho parlato a lezione pochissimi giorni prima (esempio).

April 30, 2026

A subtle hallucination by "the AI"

April 16, 2026