FORESCOUT RESEARCH | VEDERE LABS

Better Safe Than Sorry

Proactively identifying at-risk, internet-exposed OT/ICS

April 22, 2024

Contents

Executive summary 3

1. Brief history and current risks of internet-exposed OT/ICS 4
2. The evolution of OT/ICS exposure between 2017 and 2024 6
3. Revisiting the Unitronics attacks: Israel and the US are not alone — nor is it only water 8
4. Does proactive notification of exposed asset owners help? 12
5. Further evidence from Project Memoria 16
6. Conclusions and recommended mitigations 17

Executive summary

Internet exposure of Operational Technology (OT) and Industrial Control Systems (ICS) continues to be a critical infrastructure security issue despite decades of raising awareness, new regulations and periodic CISA advisories [1,2,3]. Moreover, opportunistic attackers are increasingly abusing this exposure at scale — sometimes with a very lax targeting rationale driven by trends, such as current events, copycat behavior or the emergencies found in new, off-the-shelf capabilities or hacking guides.

A recent wave of attacks by the Iranian-affiliated Cyber Av3ngers hacktivist group targeted Israeli-made Unitronics Programmable Logic Controllers (PLCs) around the world. One of the attacks occurred at a water utility near Pittsburgh bringing the timeless issue of internet-exposed OT/ICS into the spotlight once more. Forescout Research – Vedere Labs has been tracking internet-exposed OT/ICS data for over seven years.

Our research takes a fresh look at the topic by examining the nuanced evolution of exposed OT/ICS data from 2017 to 2024. We identify countries and device types where exposure has been reduced but still poses risk. Then, we analyze details of three recent cases of device exposure beginning with the Unitronics attack wave. Additionally, we discuss our attempts to proactively identify and notify asset owners with exposed Schneider Electric Modicon and Wago 750 PLCs. And lastly, we delve into the exposure of devices using the Nucleus NET and NicheStack TCP/IP stacks — which was the subject of our research in Project Memoria.

Take note: The same ICS / SCADA detailing attacks against Unitronics PLCs also has attack examples for Schneider Electric Modicon PLCs. **These devices are likely to be mass targeted in the future, so action should be taken as soon as possible to protect them**.

Key findings of this research include:

1. **The US and Canada have significantly reduced exposed devices while EU countries and Russia have expanded.** With nearly 110,000 internet-facing OT/ICS devices worldwide in January 2024, the **US** has 27% of exposed devices followed by Italy, Spain, France and Canada with a combined total of 17%. Only the US and Canada significantly reduced the number of exposed devices during the period of study by 47% in the US and 45% in Canada. The other top 10 countries increased the number of exposed devices:
    - Spain: 82%
    - Italy: 58%
    - France: 26%
    - Germany: 13%
    - Russia: 10%

2. **Manufacturing and building automation protocols make up a major portion of exposed device types.** Modbus represents 29% of exposed services, followed by three building automation protocols – KNX, BACnet and Tridium Fox – with a combined total of 32%. The top 10 types of exposed services remained mostly constant since 2017, but Tridium Fox, Lantronix and MOXA Nport saw a significant decrease in the number of devices (70% for the first two and 53% for the last), while Modbus and Siemens S7 saw an increase: 48% for Modbus and 121% for S7. Some of these reductions correlate with proactive research and government notification.

3. **Many of these internet-exposed OT devices and protocols appear to be the result of system integrator practices,** such as delivering packaged units that act as black boxes to asset owners and inadvertently expose multiple systems to the internet as part of standard setups. In all likeliness, most asset owners are unaware these packaged units contain exposed OT devices. Once again, this situation highlights the need for an accurate and granular software and hardware bill of materials as part of a comprehensive risk management strategy.

4. **Reducing exposure rates can be achieved *proactively* through targeted notification efforts.** While a combination of CISA alerts and media attention in the wake of the Unitronics hacking attacks has resulted in a reduction of almost 48% in internet-exposed Unitronics PLCs in two months, this is a highly reactive approach. The decrease of Unitronics devices in Israel started in early 2022 coinciding with the earliest attacks reported on those devices. In the US, the decrease only started at the end of 2023 following recent attacks.

5. **Nearly half of previously reported ports are still open.** Considering the historical targeting of Modicon and Wago PLCs, we reassessed these exposed devices a year after we originally reported some of them to CISA. About half of the reported PLCs still had the same ports open with no changes or measures taken. About 30% were no longer internet exposed while the other 20% remained exposed but had closed the OT port in question. However, FTP and web interfaces were still open occasionally.

6. **There are now less than 1,000 exposed devices running Nucleus and around 5,500 running NicheStack** which is a significant reduction after our original research. These reductions happened even though there is no evidence of attacks targeting these vulnerabilities or these devices directly.

1. Brief history and current risks of internet-exposed OT/ICS

OT/ICS is at the core of critical infrastructure. It is found at water/wastewater management facilities and power generation, transmission and distribution plants. OT/ICS has been targeted for almost 25 years beginning with the seminal Maroochy water attack. In two and a half decades, attackers have evolved from predominantly being state-sponsored to now including cybercriminals and hacktivists.

After the Stuxnet attack in 2010 there was an explosion of research to identify and quantify internet-exposed OT/ICS. One of the earliest examples is Leverett's work in 2011 which identified over 7,500 exposed "HVAC systems, building management systems, meters, and other industrial control devices or SCADA servers" that could be used to "carry out remote attacks on selected devices or identify networks for further reconnaissance and exploitation." The author also shared almost 30 'dork' queries used to find these devices via the Shodan search engine. Since then, there have been many comparable articles attempting to map the attack surface of exposed ICS around the world (e.g., 2014, 2016, 2018, 2020, 2021, 2022, 2023).

Researchers *and* attackers have been sharing information and developing tools to compromise these systems. Although state-sponsored capabilities including custom malware and living off the land are now considered the status quo, hacktivist groups have also shown interest in critical infrastructure and internet-accessible OT for more than a decade. This interest took on much greater proportions after the Russian invasion of Ukraine in 2022. Today, basic OT attacks are commoditized due to the existence of public scanning and attack tools that do not require specialized knowledge.

Opportunistic attackers are increasingly devoting attention to internet-exposed OT/ICS devices. For instance, they are interacting with HMI and SCADA systems to change operational parameters, leveraging OT protocols to disable PLCs or write variables directly on their registers and even encrypting files on communication devices.

The GhostSec hacktivist group, for instance, recently claimed they defaced a Schneider Easergy T300 RTU (see Figure 1) and ran the Metasploit IEC-104 module against it (see Figure 2). A careful analysis of Figure 2 shows that the group sent a "double command" (C_DC_NA_1) for Information Object Address (IOA) 5 and command value 5 (DCO=5 -> DCS = Off, QU = Shortpulse, S/E = Execute), which is exactly the example available in the Metasploit readme file. The same group used on another attack the interrogation command C_IC_NA_1, which is the default Metasploit command type (100). This shows that while they are willing to go beyond defacing web interfaces to try and cause a physical impact, they most likely do not understand the technology, otherwise they could have iterated over IOAs, selected a target and then executed a command, as the more sophisticated Industroyer malware did.

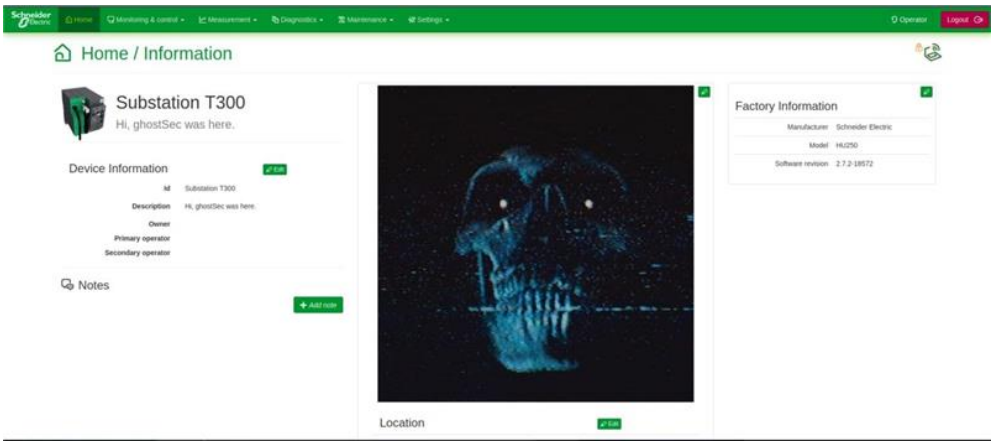

Figure 1 – Defaced Schneider Electric T300

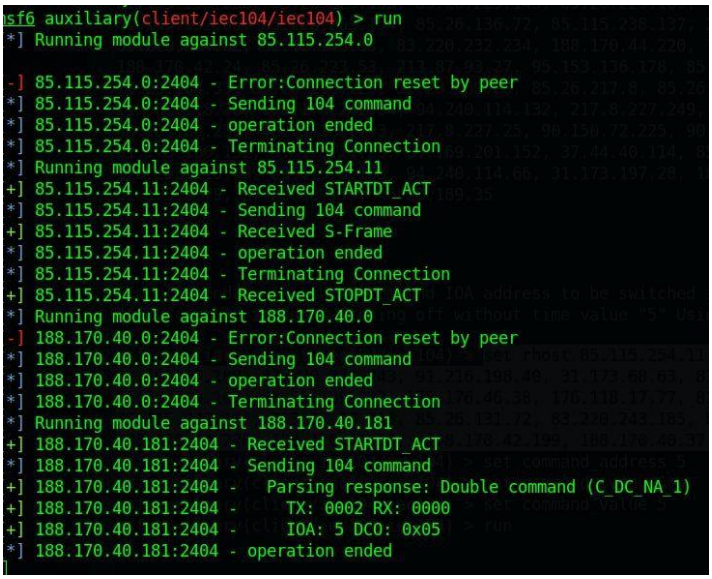

Figure 2 – Metasploit IEC-104 module ran by GhostSec against the T300

Our 2023 threat roundup also shows five main OT protocols are constantly being targeted by opportunistic attackers: Modbus (a third of attacks), Ethernet/IP, Step7 and DNP3 (with around 18% each) and IEC-104 with 10% of attacks. The remaining 2% are divided among many other protocols with a majority being BACnet. Most of the activity in these protocols is scanning and enumeration attempts. Yet, we also see messages with invalid, missing or truncated fields which could cause devices to crash upon parsing them.

The bottom line: Threat actors are eager to disrupt internet-facing devices. It is more important than ever to understand the state of OT/ICS exposure and help asset owners reduce the risk.

2. The evolution of OT/ICS exposure between 2017 and 2024

Using Shodan's pre-configured ICS tag search filter – which finds many but not all exposed OT/ICS devices – we can see close to 110,000 Internet-facing devices as of the end of January 2024 (Figure 3). In June 2017, there were 120,000 devices. This represents a drop of less than 10% in more than six and a half years with significant periods of increase, including between late 2018 and early 2020. Part of this periodic increase could be explained by exposed hosts only getting picked up by Shodan after new protocol modules are added by the tool. However, this is a small drop and is not an impressive result in risk reduction for the global ICS security community. The need for remote access during the COVID-19 pandemic years is another plausible reason for periods of increased exposure.

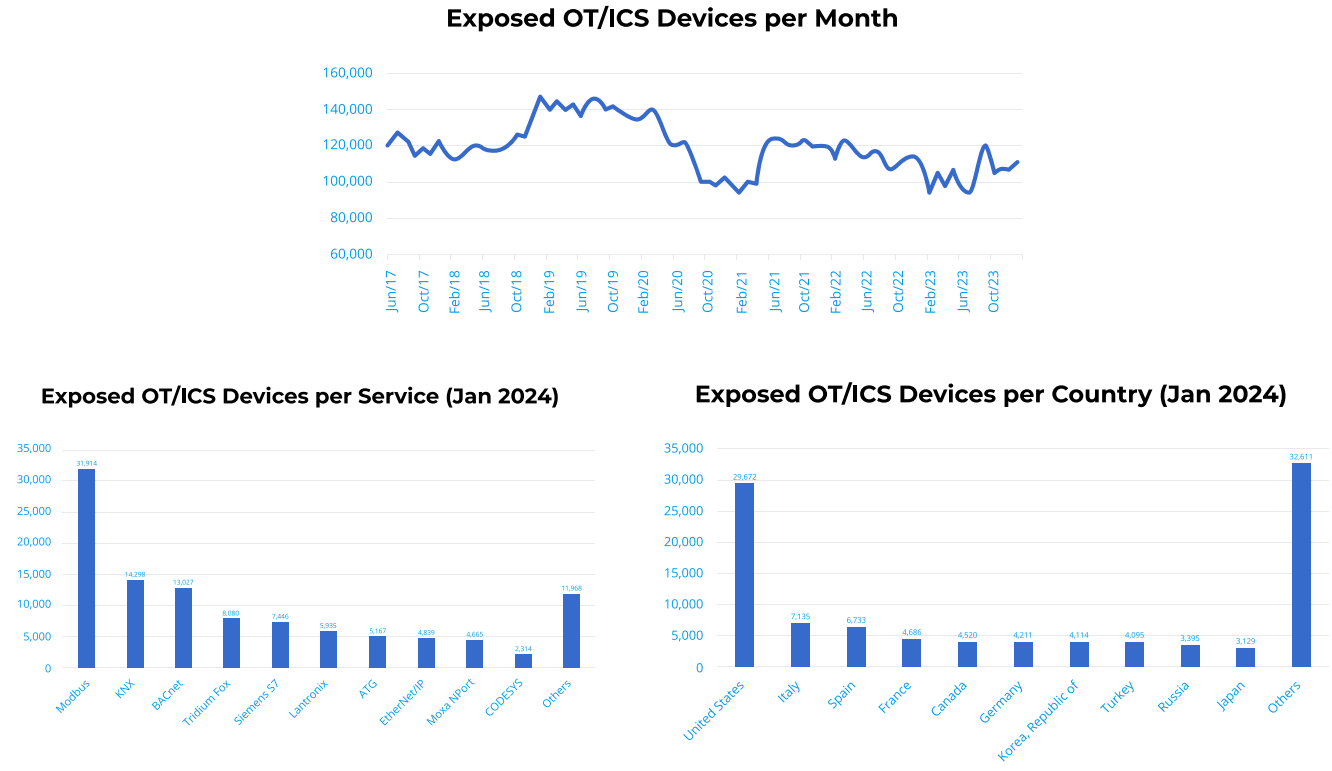

Figure 3 – Summary of exposed OT/ICS

Figure 3 also shows that Modbus, the most popular and most scanned industrial automation protocol, currently represents 29% of the exposed services. It is followed by three building automation protocols – KNX, BACnet and Tridium Fox – with a combined total of 32%. Roughly one third of the remaining total is split among several other protocols.

In terms of countries, unsurprisingly, the United States leads with 27% of exposed devices, followed by three European countries – Italy, Spain, France – and then Canada for a combined total of 17%. Looking more closely into the timeline for the top 10 countries (Figure 4) provides some interesting insights:

- **The US and Canada both had a significant decrease in the number of exposed devices during the period of study**: the US saw a decrease of 47%, from nearly 56,000 to 30,000. Similarly, Canada saw a drop of 45% from roughly 8,200 devices to 4,500.

- **All other countries that remained in the top 10 between June 2017 and January 2024 – Italy, Spain, France, Germany and Russia – saw an increase in the number of exposed devices**. The increase in Spain was of 82%, in Italy it was 58%, in France it was 26%, in Germany it was 13% and in Russia it was 10%.

Countries that appeared in the top 10 during portions of the period of study but not all of it include Sweden, Australia, the UK, the Netherlands, Taiwan, Austria, Poland, Korea, Turkey and Japan. In the overall period, Australia had a reduction of 51% and the UK 45%, however Japan saw a growth of 372%.

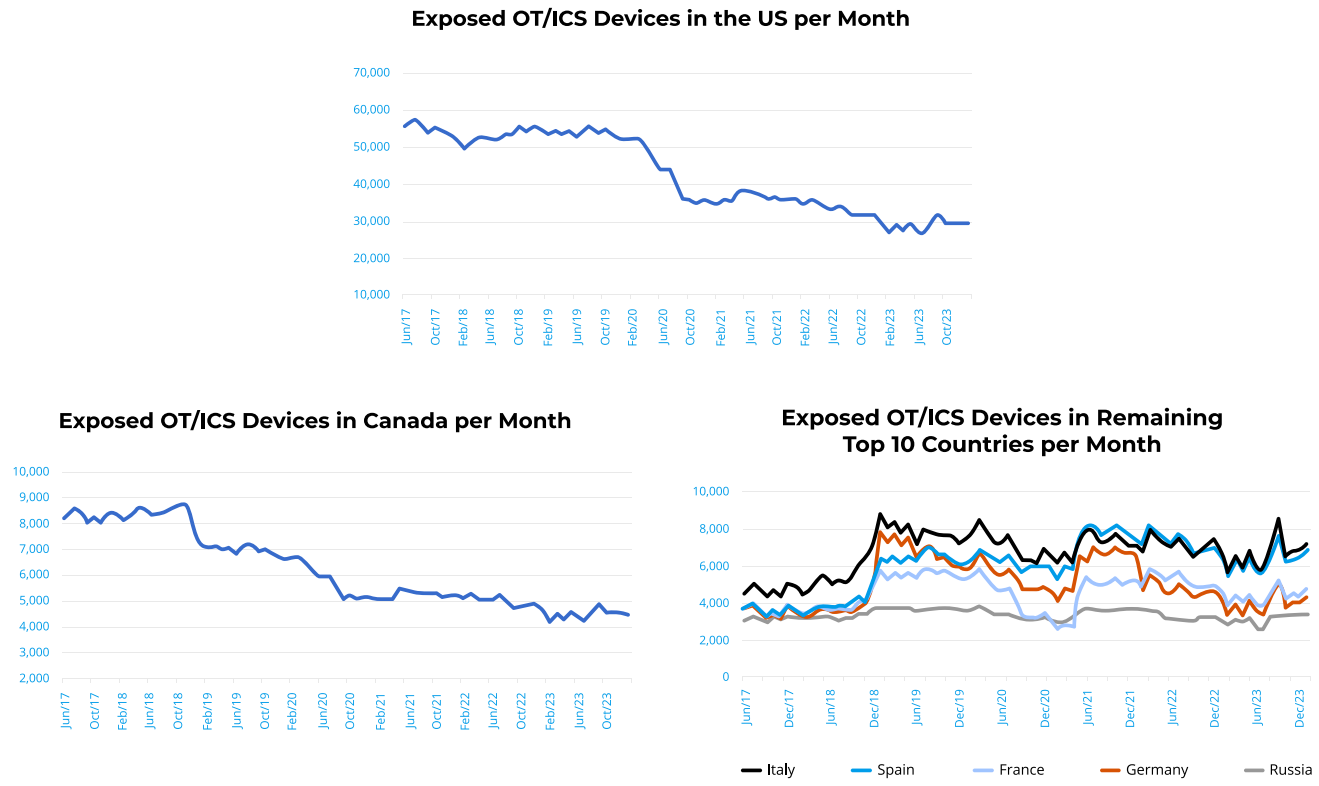

Figure 4 – Changes in exposed OT/ICS in the top 10 countries

The top 10 types of exposed service remained mostly constant since 2017, however Figure 5 highlights the most relevant changes in the number of devices exposing those services. There are two groups of services: Tridium Fox, Lantronix and MOXA Nport saw a significant decrease in the number of exposed devices, while Modbus and Siemens S7 saw an increase. The rest of the services in the top 10 (KNX, BACnet, ATG, EtherNet/IP and CODESYS) did not change significantly.

The number of exposed devices with enabled Fox and Lantronix protocols decreased by 70% each, MOXA was 53%. On the other hand, Modbus saw an increase of 48% and Siemens S7 more than doubled with a total growth of 121%. We are not certain why there was a dip in Modbus exposure between 2020 and 2021, but it is probably related more to Shodan's visibility on those devices than to the actual number of devices exposed.

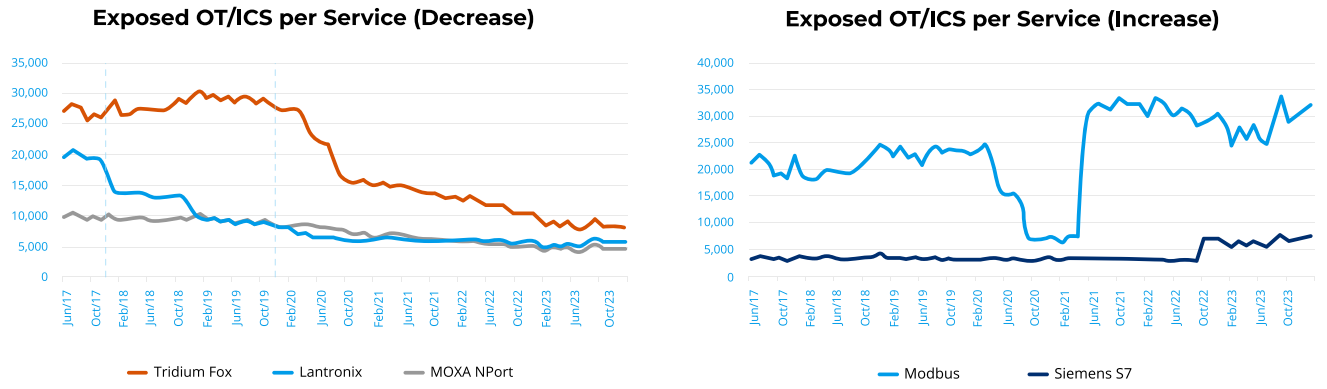

Figure 5 – Changes in the top exposed OT/ICS services

It is not always possible to know the exact reasons for increases and decreases in exposed devices, but some events can be correlated to the figures above. For instance, in December 2017 a researcher identified thousands of serial-to-Ethernet Lantronix devices leaking their passwords online which led to government alerts and a decrease in the number of exposed devices from early 2018. Another example is the FBI alert about exposed Tridium Fox systems in December 2019, which was reflected in a decrease in online devices from early 2020.

Although the data above is representative of exposed OT/ICS in general, it does not provide a full picture of devices, as we mentioned at the beginning of this Section. For instance, devices such as the cellular routers we researched on Sierra:21 are not included, and there are more than 100,000 of those alone. With that in mind, the next sections go into some details of systems that Shodan does not track as ICS but that we have been monitoring separately, with the goal of confirming the hypothesis that early research and proactive asset owner notifications can have a significant impact in the number of exposed devices.

3. Revisiting the Unitronics attacks: Israel and the US are not alone — nor is it only water

In the wake of the Israel-Hamas war (November 2023), a series of attacks on internet-exposed PLCs manufactured by the Israeli company Unitronics were carried out by a purported hacktivist group called Cyber Av3ngers. The hacktivists defaced the Human Machine Interfaces (HMIs) integrated on those PLCs with a message stating the equipment was targeted because it was manufactured in Israel – shown in Figure 6. Reportedly, none of the targeted PLCs were affected other than through defacement.

Figure 6 – Compromised Unitronics HMI in November 2023 [from https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/]

While Cyber Av3ngers have a history of false or inflated claims, multiple independent reports of defaced HMIs appeared on the internet and soon this attack wave gained media attention when it hit one of the booster stations of the municipal water authority of Aliquippa, PA in the US. On February 2, 2024, the US treasury department sanctioned six officials in the Iranian Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC) who are allegedly behind the Cyber Av3ngers persona.

CISA published an alert about the attacks in November 2023 and included the use of a default password in Unitronics PLCs – a newly-minted CVE-2023-6448 for a vulnerability that existed for a long time – was added to the Known Exploited Vulnerabilities (KEV) database in December. However, an earlier series of attacks using the same defacement imagery (but without referencing Cyber Av3ngers by name) had already targeted this same equipment in February 2022 and April 2023 affecting agricultural water controllers and parcel distribution centers in Israel.

As reported by Secureworks, the hacktivist group GhostSec also claimed to have targeted Unitronics PLCs in Israel in October 2023 (using a different defacement image). In March 2023, a Telegram channel associated with GhostSec posted an ICS / SCADA hacking guide explicitly showing how to identify Unitronics devices on Shodan and how to use the free Unitronics VisiLogic engineering software to connect to these devices using the PCOM protocol (port 20256/TCP) and then take control of their HMIs.

Multiple victims of Cyber Av3ngers and previous attacks had PCOM open to the internet and this is likely how the November attacks were carried out. Once simple-to-execute OT exploits or TTPs become public, they are eventually used by opportunistic attackers (see Section 2). These attacks were probably carried out manually. Had the attackers written a script to do it, they could have hit every public facing PCOM port.

While the impact of such low-effort defacement is limited, keep in mind that in at least one case there was a service disruption for two days — in Ireland. Beyond the effect on a small local community, this type of disruption can have a larger-scale psychological impact.

Interestingly, media focus has mostly been on the effects of these attacks on the US and Israeli water sector, but the latter waves have not been limited in geographical or sectoral scope. Indeed, this indiscriminate wave hit everything from water utilities in Ireland and Romania, oil pumps and a public aquarium in the US, a brewery in Pittsburgh, a factory in the Czech Republic, and various unspecified victims on the Unitronics support forum, to several agricultural entities in Western Europe that reported privately to Forescout.

During our analysis of these attacks in November, we noted there were over 1,800 internet-exposed Unitronics PLCs spread across the globe. As of early February 2024, this number had **fallen to 937**, as shown in Figure 7.

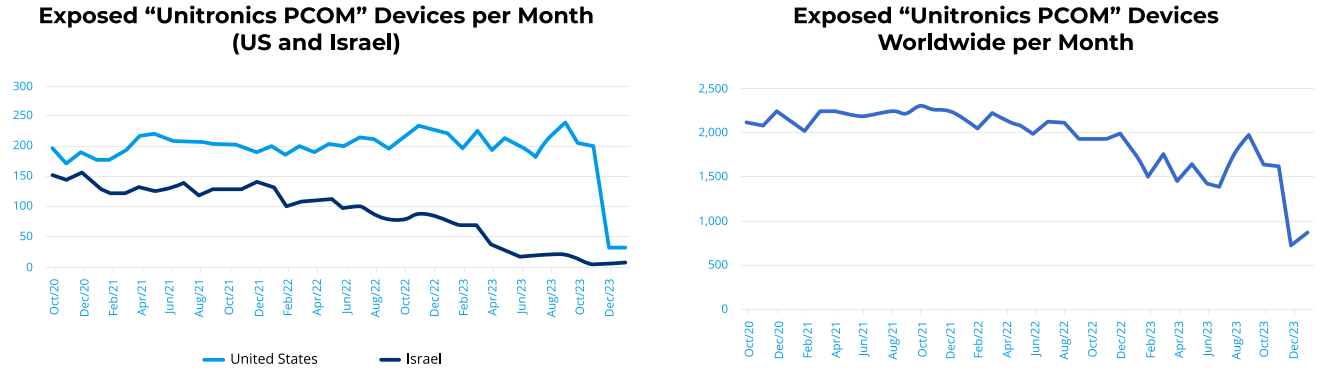

Figure 7 – Decrease in exposed Unitronics PLCs between late 2020 and early 2024

While this rapid reduction is a great development, two points should be highlighted:

- **Despite decreases, attacks in the US could have been avoided.** The worldwide decrease followed an earlier trend that was clearly accentuated after the Cyber Av3ngers attacks. The most interesting point is that if we zoom in the trend in the US and Israel, we can see that the decrease in Israel started in early 2022, which coincides with the earliest attacks reported on those devices. In the US, the decrease only started at the end of 2023. If US authorities had paid attention to the 2022 attacks in Israel, the attacks on the Aliquippa water authority, the brewery in Pittsburgh and other US asset owners could have been thwarted.

- **Too many PLCs remain exposed**. Drilling down, we identify the countries and sectors in which these PLCs are likely deployed to get a clearer picture of the remaining at-risk group.

First, Figure 8 shows the countries that still have significant numbers of exposed Unitronics devices. These countries have also been decreasing their exposed devices, albeit at a slower pace than Israel — which means that they still figured in the top 10.

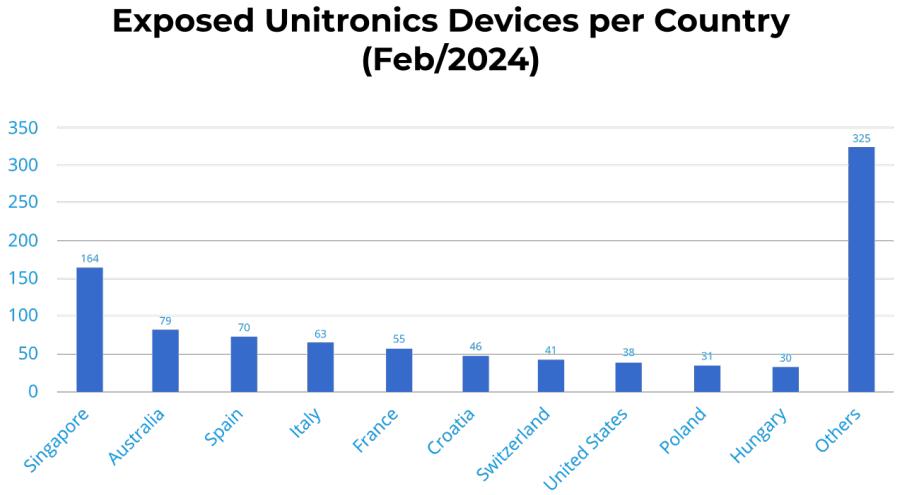

Figure 8 – Top 10 countries with remaining exposed Unitronics PLCs

Secondly, Figure 9 shows the "OS Version" distribution of exposed devices. The individual exposed versions are less important than the fact that there are 18 unique versions out there and none of them runs in more than 20% of devices. This type of version fragmentation is typical in OT where upgrades are uncommon. The older a version is, the less likely it is that the asset owner can easily upgrade an existing device.

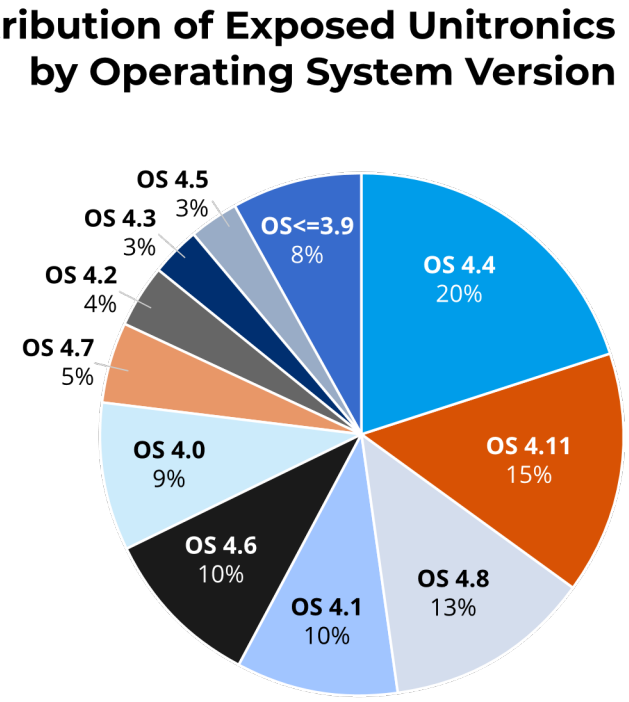

Figure 9 – Distribution of exposed Unitronics PLCs by OS version

Next based on a **combination of the PLC project name, hostname, ISP, geolocation data and information gathered from other exposed services** (such as SNMP, logos and descriptive information on embedded web servers) and further OSINT, we managed to identify several entities associated with the exposed PLCs.

While many of the exposed PLCs are active in the water and agricultural sectors, we noticed a sizeable number of PLCs are deployed for building management purposes, including at a major distribution center, a healthcare contractor, a research lab gas management system and multiple residential apartment complexes managed by the same property management company — and **identified by their street address in the PLC project name**.

Another interesting use case is the deployment of Unitronics PLCs in **so-called packaged units or modular skid systems**. These self-contained systems are typically integrated by a third party into a customer's control system in a turnkey fashion with the internals of the unit being a black box to the asset owner. We found examples of Unitronics PLCs being **part of oil field pump controllers** (which had not previously been reported, though the manufacturer noticed their exposed products had been hit), brewery solutions, biofuel boilers and industrial heating boilers, and substation battery tripping units.

It is highly likely that most of the responsible asset owners are **unaware** that these systems contain Unitronics devices exposed to the internet, once again **highlighting the need for an accurate and granular software and hardware bill of materials** as part of a comprehensive risk management strategy.

Finally, many PLCs were exposed in similar ‘clusters’: e.g. various water controllers belonging to several *different* municipal utilities in a Nordic country with very similar configurations. This points to the likely **role of system integrators** servicing multiple asset owners **in the misconfigured exposure to the internet**.

Examining data from Forescout Device Cloud, which contains information about devices that are not necessarily exposed to the Internet but deployed at customer networks, we see more than 600 Unitronics PLCs, distributed as follows: 58% in manufacturing, 16% in financial services, 9% in technology and the remaining 17% spread across other industries. These devices are mostly located in Israel (63%), UK (16%) and US (6%), with other countries making up only 15% of the global presence.

4. Does proactive notification of exposed asset owners help?

As part of our Deep Lateral Movement research published in February 2023, we enumerated internet-exposed instances of two PLC lines covered in that research: the Schneider Modicon exposing UMAS and the Wago 750 series exposing web and/or FTP interfaces. At the time of that research, we applied the same OSINT-based identification approach as discussed at the end of Section 4 to identify dozens of affected asset owners and contacted CISA to alert them.

In retrospect, several of these cases stand out because they match our Unitronics observations above. The first being a cluster of Modicon PLCs from **five small French hydro power stations** (with capacities of 1-3.3MW) owned by at least three different companies but which turned out to have been built by the same engineering firm which used the same system integration subcontractor – identifiable from project names – on multiple projects. Pivoting off that information, we also identified an exposed PLC of a **large hydro power station** in the same country with a capacity of **420MW**.

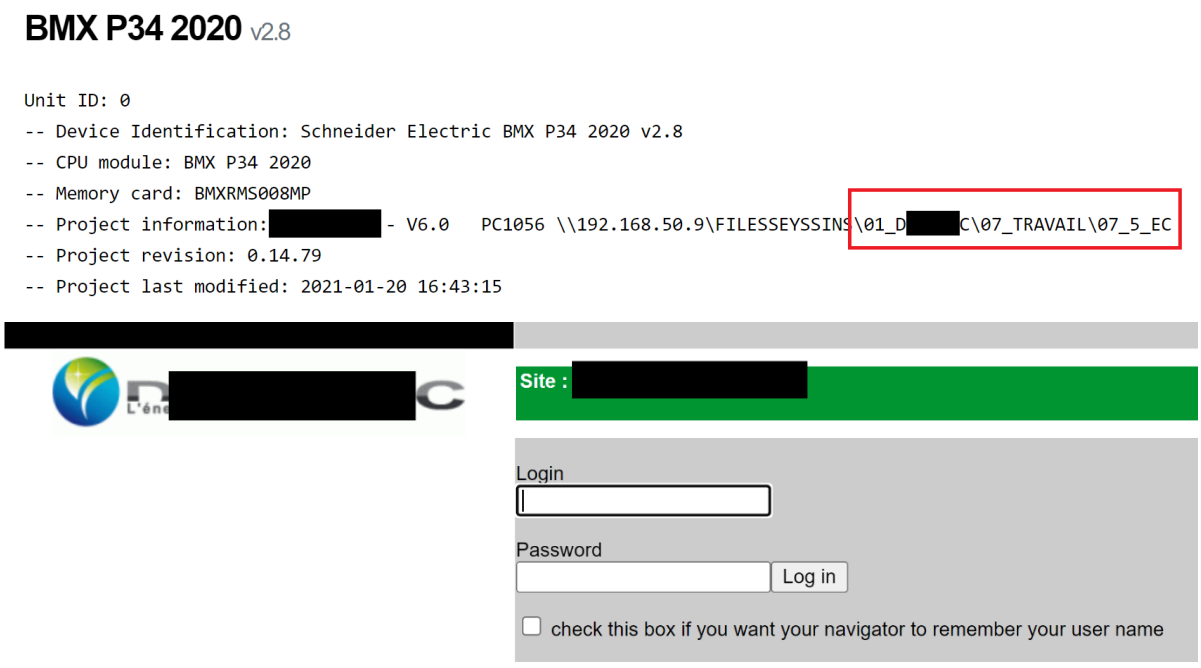

Figure 10 – Exposed Schneider Modicon PLC at French hydro power station with distinct project file path and web server info containing system integrator and location names

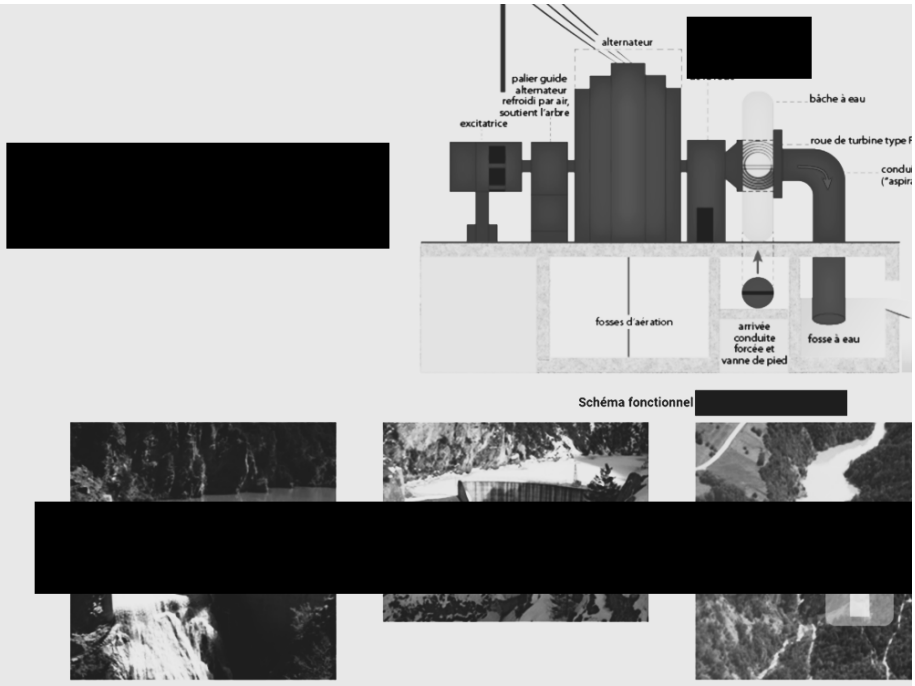

Figure 11 – Website with hydro power station details, identified through OSINT (figure in black and white with redacted details to avoid identification)

The second case concerned a cluster of Modicon PLCs from **seven small Eastern European solar farms** (with capacities of 2-15MW, representing 2.8% of all solar capacity in the country in 2023) built and sold by the engineering subsidiary of a prominent Asian Global 500 company. In addition to UMAS with identifiable project names, these solar parks exposed a variety of services including webcams showing the (geolocated) solar parks. **Most of these PLCs resided sequentially on the same public /24 subnet**.

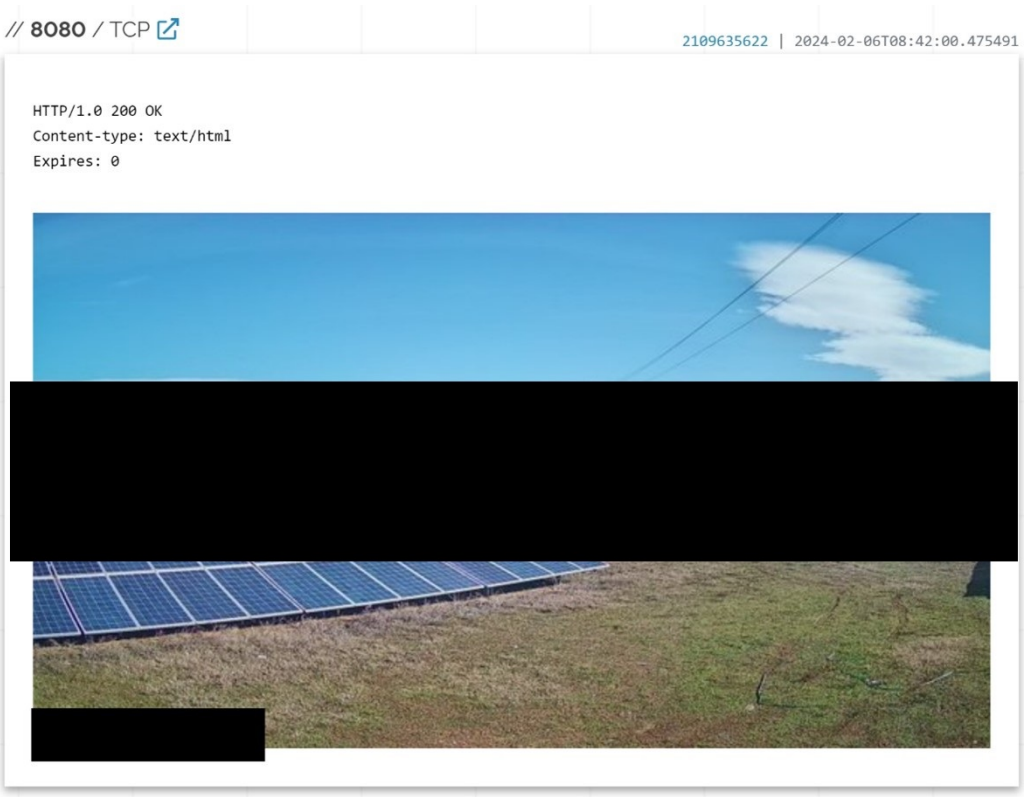

Figure 12 – Exposed webcam associated with a Schneider Modicon PLC at European Solar power station with site geolocation information (figure with redacted details to avoid identification)

Finally, we identified a single country with a large number of internet exposed Wago 750 devices used as RTUs. All of these hosts co-exposed sensitive OT protocols, such as IEC 60870-5-104 or CODESYS and the web interface of a particular cellular router brand. In almost all cases, the router name on this web interface contained a geographic location together with the abbreviation “GES”, which stands for *Güneş Enerjisi Santrali* (Solar Power Plant - SPP) in Turkish.

This led us to **several clusters which in total comprised almost 100 small solar array controllers in Turkey** (each with a capacity of 0.2-5MW), most of which seemed to be commercial rooftop installations, in addition to a **few small solar parks** (with a capacity of 10MW+). Interestingly, while it appeared at least five different EPC contractors were associated with these solar parks, they all shared the same telco and very similar choices in RTU, cellular router, OT protocols and naming schemes.

Figure 13 – Several exposed Turkish solar park controllers, sharing similar exposed services

Figure 14 – Solar park project site identified through the cellular router name

We found several other clusters of identifiable exposed PLCs ranging from **sewer pumping stations** and **chemical industry oven controllers in the US** to **mining crushing plants** and **agricultural silos in Europe**. This shows that with a bit of effort one can identify the asset owners and functionality associated with internet-exposed PLCs — something that could aid preventative efforts in reporting to the right party as well as **distinguishing between worrisome and less relevant exposed systems** (such as model trains and swimming pools).

In light of the Unitronics attack wave, the historical targeting of Modicon and Wago PLCs and the reported interest in Wago PLCs, we decided to reassess the exposed devices a year after we originally reported them to CISA.

Unfortunately, we noticed that **about half** of the reported PLCs **still had the same ports open** with no changes or measures taken. **About 30% were no longer internet exposed**, while the other **20% remained exposed but had closed the OT port in question (though sometimes leaving FTP and web interfaces open)**.

Although we saw a reduction in exposed devices due to proactive asset owner notifications, that has not happened with the same speed as for Unitronics – possibly because there have been no mass exploit campaigns against Schneider Electric or WAGO equipment yet. However, there are early examples of opportunistic attackers targeting these devices. The same ICS / SCADA hacking guide that detailed attacks against Unitronics also has examples of attacks against Schneider Electric Modicon PLCs. These devices are likely to be mass targeted in the future. Action should be taken as soon as possible to protect them.

5. Further evidence from Project Memoria

In August 2022, we looked at Shodan to see the effect our research had had on exposed devices running those software programs — 18 months after we disclosed the NAME:WRECK vulnerabilities affecting the Nucleus NET TCP/IP stack and one year after we disclosed INFRA:HALT affecting NicheStack. In a blog post published in December 2022, we reported a sharp decrease of exposed devices running Nucleus NET, but an increase of almost 50% in devices running NicheStack.

Figure 15 extends our previous analysis to January 2024. What we see now is much more encouraging. Both Nucleus FTP and Nucleus RTOS continued to decrease significantly and now have less than 1,000 exposed devices. NicheStack started decreasing at the end of 2022, following the period of growth we had noticed earlier. There are now around 5,500 exposed devices which is less than when we published our research in August 2021 and less than August 2022 when we first did the comparison. This reduction happened even though there is no evidence of attacks targeting these vulnerabilities or these devices directly.

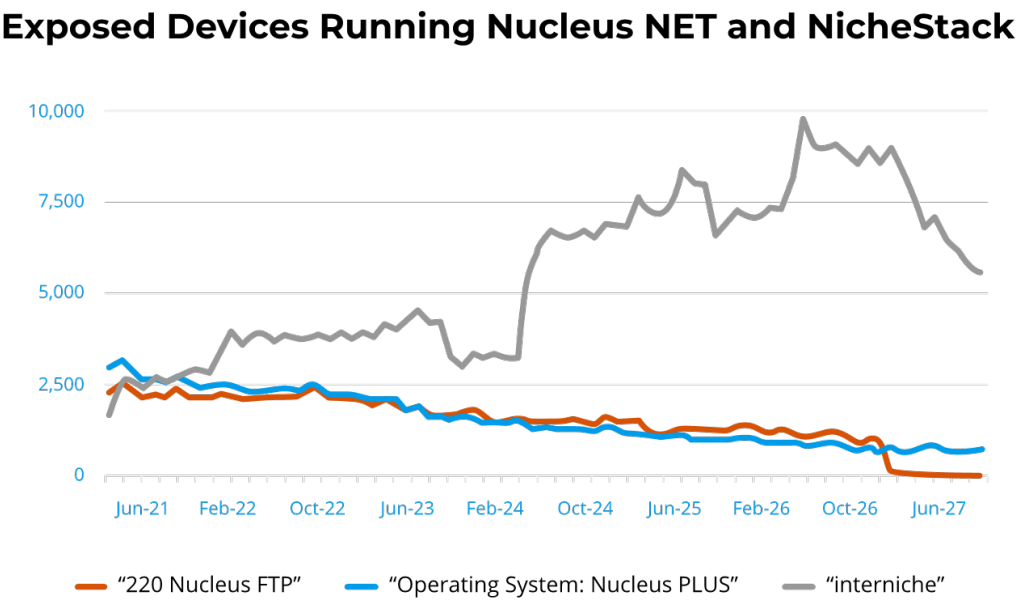

Figure 15 – Exposed devices running Nucleus NET and NicheStack

6. Conclusions and recommended mitigations

In this report, we show how internet exposure of OT/ICS continues to be a timely issue and how opportunistic attackers are increasingly abusing this exposure at scale. Many internet-exposed OT devices are the result of system integrator practices where asset owners are likely unaware of exposed devices. To reduce risk, organizations should proactively leverage targeted notifications.

Due to the increased scope of attacks on exposed OT/ICS, we recommend asset owners:

- **Harden connected devices**
  - Start by identifying every device connected to the network and enumerating known vulnerabilities, used credentials and open ports. Change default or easily guessable credentials and use strong unique passwords for each device.
  - Disable unused services and patch vulnerabilities to prevent exploitation.
  - Make sure you have an accurate picture of your internet exposed assets and do not assume you will never be a target.
  - Make sure your asset inventory is granular enough to cover third-party 'black box' systems (e.g. through HBOMs or automatic asset inventory construction) and ensure cyber-security best practices form an integral part of all Site Acceptance Tests (SATs).

- **Segment**
  - Do not expose unmanaged devices directly to the internet, with very few exceptions such as routers and firewalls.
  - Follow CISA's guidance on providing remote access for industrial control systems. Segment the network to isolate IT, IoT and OT devices, limiting network connections to only specifically allowed management and engineering workstations or among unmanaged devices that need to communicate.
  - Ensure administrative interfaces, such as web UIs and engineering ports on connected devices are behind IP-based access control lists or are only accessible from a separate, VPN-protected management VLAN.

- **Monitor**
  - Use an IoT/OT-aware, DPI-capable monitoring solution to alert on malicious indicators and behaviors.
  - Watch internal systems and communications for known hostile actions, such as vulnerability exploitation, password guessing and unauthorized use of OT protocols.

Finally, monitor the activity of hacktivist groups on Telegram, Twitter and other sources where attacks are planned and coordinated. Monitoring what kind of hacking material gets shared in these communities gives early warning as to what exposed systems are more likely to be targeted than others. There is a wealth of different protocols and devices exposed but opportunistic attackers seem to prefer whatever happens to have a Metasploit module or a guide available, walking them through the engineering software step-by-step.