Kaspersky ICS CERT

kaspersky

ICS and OT threat predictions for 2024

Evgeny Goncharov

31.01.2024 Version 1.0

We do not expect rapid changes in the industrial cyberthreat landscape in 2024. Most of the below-described trends have been observed before, many for some years. However, some of them have reached a critical mass of creeping changes, which could lead to a qualitative shift in the threat landscape as early as next year.

Ransomware

1. **Ransomware will remain the No. 1 scourge of industrial enterprises in 2024.**

   In 2023, ransomware attacks consolidated their hold on the top of the ranking of information security threats to industrial enterprises. As seen from the official statements of organizations affected by cyber incidents in H1 2023, at least one in six ransomware attacks caused a halt in the production or delivery of products. In some cases, the damage from the attack was estimated in the hundreds of millions of dollars. At present, there appears to be no reason to believe the threat will decrease in the near future.

2. **Ransomware attacks on large organizations**, suppliers of unique products (equipment, materials), or big logistics and transport companies **can have severe economic and social consequences**.

   Today, according to targeted companies, no less than 18% of ransomware attacks on industrial companies lead to disruptions in production and/or product delivery. Moreover, cybercriminals are clearly aiming "upmarket" in their choice of victims, preferring to target large organizations able to pay substantial ransom.

   This is creating a situation where attackers, by design or accident, could again cross the line beyond which the attack consequences become infrastructural, as in the case of Colonial Pipeline. As a further example, a recent attack on DP World, the Dubai-based international container terminal and supply chain operator, brought work at the ports in Melbourne, Sydney, Brisbane and Fremantle to a standstill, blocking approximately 30,000 containers from being delivered.

3. The **ransomware market** is heading for a peak, which may be followed by a decline or stagnation. Potential victims are unlikely to become immune to attacks any time soon. However, they can learn to mitigate the impact more effectively (for example, through better securing the most confidential data, and with proper backup and incident response plans).

   If this results in victims paying out less money less frequently, cybercriminals will have to find **new types of targets and new schemes for monetizing attacks**. Potential avenues of development:

   a. **Attacks on logistics and transport companies may become targeted** not at the IT infrastructure supporting operations, but the **vehicles themselves** (cars, ships).

      At first glance, the large variety of vehicles in parks and fleets would seem to hinder the implementation of such an attack, greatly adding to the attackers' development costs. However, rather than one specific owner or operator, the attack could target multiple vehicles of a certain type that have identical or similar internal control systems.

      Another factor facilitating the attack is that fleet owners and operators additionally equip vehicles with their own custom telemetry-gathering systems, which often have remote control capabilities by default (for example, to remotely re-flash the firmware or to change the data set to be collected). Vehicle manufacturers and service providers sometimes do likewise. As a result, this vector becomes feasible.

      In the event of such an attack, the victim will be unable to restore operations by itself without incurring costs that render the business no longer viable. It is far easier to restore the operation of encrypted IT systems (for example, from backups) than it is to resolve even a technically simple issue affecting vehicles scattered across a wide area (for example, removing malware that prevents a truck engine from starting or cuts the power inside a ship). Companies may find themselves unable to bring operations back to normal on their own in a timely manner and without inacceptable financial losses.

   b. **The same vector applies equally to owners and operators of various specialized equipment** operating at remote hard-to-reach sites, such as in **mining or agriculture**.

   c. The problem of cyber-securing multiple hard-to-reach sites is also relevant for oil and gas companies, public utilities, and, in general, any organization with a highly distributed OT infrastructure. An **attack on a distant out-of-the-way site** that **excludes the possibility of remote recovery** (for example, because the regular remote access channel is blocked by malware) **guarantees a ransom payout**.

d. **Unconventional methods of monetizing attacks (for example, through stock market speculation) on economically significant enterprises** — major transport and logistics organizations, large mining companies, manufacturers and suppliers of materials (such as metals, alloys, or composites), agricultural and food products, suppliers of unique/in-demand products, shortfalls of which are hard to cover quickly (such as microchips or fertilizers).

   Disruptions in the supply of products from such enterprises can significantly impact their market price. Besides the direct consequences, there may be chain reactions and indirect side effects. Recall how the Shamoon attack on Saudi Aramco had a bombshell effect on the price of hard drives globally, following the company's unexpected decision to replace the hard drives of all its computers affected by the attack with new ones.

Hacktivists

4. **Politically motivated hacktivism** along geopolitical fault lines will grow sharper teeth and have **more destructive consequences**.

   We all remember the headline-grabbing hacktivist attacks on railways and gas stations in Iran in 2021 that the pro-Israeli hacktivist group claimed responsibility for. And we saw many more cases last year: the irrigation systems hit in Israel, the attacks on the Israeli made Unitronics Vision all-in-one (PLC with integrated HMI) solutions that found their victims in US and Ireland and one more attack on Iranian gas stations in 2023. Leaving aside the PR effect, the actual scale of the negative consequences was quite modest in all these cases.

   That said, more recent hacktivist attacks have demonstrated the ability to get to OT systems. In some of the similar cases that Kaspersky ICS CERT investigated this year it was only a slight lack of the attackers' preparation and perseverance that saved the victims from physical damage. Escalating tensions may well raise politically motivated hacktivist attacks to a whole new threat level.

5. In addition to **protest movements within countries** against a backdrop of rising social tension (caused by religious and ethnic strife and growing economic instability in many regions of the planet), we will **see growing cosmopolitical protest hacktivism,** such as that driven by—or, conversely, aimed against—the introduction of a new socio-cultural and macro-economic agenda. An example, associated with environmental protection and green technology, is so-called "eco-hacktivism", such as the attack on a mining company in Guatemala by the Guacamaya Roja hacktivist group).

6. The overall rise of hacktivism across the globe will inspire more individuals and groups to start their own fight for "whatever", even **"just for fun"**, similarly to the attack on the Idaho National Laboratory by the hacktivist group SiegedSec this year.

From grey zone towards the shadows

7. Widespread **use of "offensive cybersecurity"** for gathering cyberthreat intelligence will have **both positive and negative consequences**.

   On the one hand, we will see some improvement in corporate security, as offensive cyberthreat intelligence will give the user signs of potential compromise not with the telemetry of security solutions, incident research, indirect sources, and the dark web, as traditional cyberthreat intelligence does, but also directly from attacker-controlled infrastructure. This will enable victims to restore system security more quickly and efficiently.

   On the other hand, by becoming the new norm (albeit not officially legalized, but applied with the tacit consent of governments), the development of offensive cyberintelligence will also produce negative consequences for the border between the gray zone and the shadows might be too thin and the temptation to cross it might be too hard to resist. Following the states, some commercial enterprises may try and benefit from the help of commercial offensive intelligence solution and service providers, including for not the cybersecurity purposes. And some Industrial enterprises might also be in the game. This might be especially true for the high-completive ecosystems, such as in construction, mining and energy, as well as in many other industrial sectors.

   These "profit-driven" cyberactivities will be even more pinpointed than we are used to seeing in APT campaigns. Campaigns will be armed primarily with commercial and open-source tools, which will allow them to mask their activity against the generally high backdrop of cybercriminal attacks. As a result, the operations will be detected and investigated even less frequently than the APT campaigns.

Threats related to logistics and transport

8. The ongoing and rapid **automation and digitization of logistics and transport will lead to**:

    a. **Greater intertwining of cyber- and traditional crime**, particularly in long-established criminal fields such as:

    - Theft of cars, applicable to all modern cars, but especially relevant for the Asian brands and expected for the new car brands due to aggressive fast-to the market strategy that normally prioritizes cyber security maturity as one of the first things to sacrifice.
    - Maritime piracy and logistical disruptions powered by cyber-means—as a logical continuation of known attack tactics and technologies, such as the latest tapping of AISs (Automated Tracking Systems) in the Red Sea and the Indian Ocean or the attack on the Iranian Shahid Rajaee port terminal back in 2020.
    - Theft of goods using cyber means.
    - Smuggling powered by cyber-means—as the development of tactics used in the notorious "Ocean's Thirteen" case in the port of Antwerp.
    - Other logistics and transport fraud for example, receipt of money in relation to insurance claims/cancellation penalties, and many other schemes, some hard to predict, such as messing with DRM as a means of unfair competition that we recently saw in Poland.

    b. **Increased likelihood of physical consequences of non-targeted attacks**. Already there are known cases of vehicles of various types being infected with malware. If we peer into the near future, due to the adoption of "traditional" operating systems such as Android and Linux in transport, the widespread integration of standard IT components and communication protocols, and the increasing number of use cases involving connections to cloud services, such infections look set to multiply. Chances are that some may lead to failures of critical monitoring and control systems with hard-to-predict consequences. Above all, the risk concerns river, sea, truck, and emergency transport — information security in such vehicles is often inferior to that in passenger cars.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com