Kaspersky ICS CERT

Why APTs are so successful

Stories from IR trenches

Vyacheslav Kopeytsev

30.05.2023 Version 1.0

‘Schrödinger's antivirus’ – it’s kind of there, but not really

At first glance, this is not one of those obvious issues since everybody’s saying, “We have cybersecurity solutions installed everywhere.” However, we know from practice that appearances are deceptive. Time and again, while trying to figure out what went wrong, we’ve found numerous issues with the settings and usage of security solutions.

Sometimes, **people responsible for information security do not access the control panel of their security solutions for months.** But hoping that an automated solution will protect your systems from all threats on its own, without your involvement, is naïve. Threat actors are resourceful and persistent – while something must be rotten in your state, too. When an incident occurs, attributing the failure solely to the security solution (by claiming that it overlooked the threat) is unproductive. In many cases, attackers are able to achieve their goals because some of the victim organization’s employees behave in an irresponsible, careless, and incompetent manner when it comes to following basic cybersecurity practices and rules. Thus, in 2022, improper settings of security solutions were among the reasons for successful attacks of an APT group on industrial organizations and government institutions.

As we analyze what caused an incident, we often see:

- numerous systems with security solution databases that haven’t been updated for a long time;
- systems on which the staff forgot to add a license key, although it had been purchased;
- systems on which a user can remove a license key (and those on which a user has actually removed one);
- systems on which a user has shut down the security solution or disabled its components that provide protection from modern threats;
- systems in which too much is excluded from scanning and protection.

If a security solution uses outdated databases and doesn’t have access to live cloud services that check the reputations of files and URLs, this can often result in malware spreading freely and uncontrollably. This is because, in APT attacks, the attackers devote significant resources to evading detection. For example, in an investigation that we conducted last year (in 2022), we determined that an APT group had been in an organization’s network for over three years – all because of a security solution that was outdated and, in addition, had some of its modules disabled.

Another thing worth keeping in mind is the **importance of using proper configurations of security solutions**. In most cases, during an attack, the attackers try to steal domain account credentials to connect to other systems and move laterally. In many cases, the attackers connect to the system via RDP and simply disable the security solution. Why are they able to do this? Because the employee responsible for setting up the security solution has forgotten to enable the feature that requires entering the administrator password when attempting to disable protection. Incidentally, enabling this option in the Kaspersky Security Center, for instance, takes just a couple of minutes.

In 2022, we noticed a new trend in APT tactics. When searching for ways to move laterally, the attackers no longer stop at hijacking the domain controller. Their next target is the administration servers of security solutions. The objectives can vary: getting access to detailed information on the infrastructure under attack, all gathered in one place; adding the malware to the exclusions list; disabling security solutions, sometimes even distributing malware using tools built into the security solution's administration system, including to systems that are not part of the hijacked domain. Sometimes the channel used to control security solutions is the only channel that connects different networks that have different security levels and it can be used to reach network segments that are, on paper, air-gapped (i.e., completely isolated from all networks).

To address this issue, Kaspersky ICS CERT and the Research and Development Department at Kaspersky did a joint project to develop the "Hardening Guide", a set of recommendations that helps to make major improvements to the protection of the Kaspersky Security Center. For example, the Hardening Guide provides instructions on enabling two-factor authentication in KSC to prevent security solutions from being hijacked even if the domain controller has been compromised. The Hardening Guide can be found on our technical support website.

Finally, **on some OT networks, protection is not installed on many endpoints at all.** There can be a number of reasons for this. Sometimes engineers believe that their ICS systems are completely isolated from other network segments. In other cases, engineers are simply afraid of installing anything new because of the principle "if it isn't broken, don't fix it". The choice of a security solution can be further complicated in situations where industrial equipment vendors require that only software certified by them be installed on ICS systems, threatening to cancel the warranty of systems that don't meet this requirement.

Even in cases where the OT network is in fact fully isolated from other networks and the outside world, attackers still have ways of gaining access to it. For example, by creating special versions of malware that are distributed via removable drives. In 2022 alone, we saw this tactic used in attacks on industrial organizations by at least two APT groups. Above, we mentioned one typical case, where industrial enterprise employees erroneously believe that the OT network is not connected to the office network (in reality, the two networks are connected via the channel used to control the security solution). Other similar issues related to the OT network's isolation are discussed below.

When designing an information security system, it should always be assumed that attackers will be able to gain access to ICS nodes. This is why we recommend using Kaspersky Industrial CyberSecurity – a native OT XDR platform, a product certified for compatibility and recommended by leading industrial equipment and automation system vendors.

OT network isolation issues – mythical air gap and flat network

A typical example of improper OT network isolation is **machines with several network interfaces**, such as engineering workstations, that are connected both to the IT network and the ICS network or computers connected to different networks at different times (mostly engineering laptops, but not only – we have seen infections spread to the OT network from a server that had been temporarily connected to the office network to perform maintenance after it was connected to the ICS again). On some occasions, we have seen situations where an engineer used the same computer for social networking and to make changes to a PLC project. By infecting such machines, attackers essentially gain access to equipment on the OT network. This is how, several years ago, the WannaCry malware penetrated the OT network on an oil refinery – an incident with dire consequences (disruptions in the product shipping system).

When granting access to the OT network to employees of the enterprise and its contractor organizations, the relevant information security measures are not always observed, either. Such access is often provided via remote administration utilities, for instance, TeamViewer or Anydesk. Many of the communication channels mentioned above, which were identified while investigating various incidents, were originally allowed on a temporary basis but remained operational permanently. Some of them were simply forgotten by enterprise personnel. It should be kept in mind, however, that attackers easily find such channels.

Only a few months ago, we investigated an incident where a contractor organization's employee attempted sabotage, taking advantage of remote access to the ICS network legitimately granted to him several years before.

This story demonstrates once again that **the human factor should never be ruled out**: employees can be unhappy with the way their work is assessed or with their income, or they can be politically or ideologically motivated.

If **the OT network's isolation relies exclusively on the configuration of networking equipment,** experienced hackers can always reconfigure that equipment to suit their own purposes, such as converting it to proxy servers for malware control traffic and/or servers used to store malware and deliver it to (formerly) "isolated" networks – we have seen this kind of abuse on multiple occasions, too.

When designing industrial networks, engineers are commonly guided by principles of simplicity (minimizing the effort required to configure systems) and low cost, without keeping information security risks in mind. The result is usually a **"flat network" that is not segmented into VLANs and has no demilitarized zones or firewalls inside the network.** Once attackers penetrate one node, they can usually easily move laterally to gain control of the entire OT network and sometimes even reach the networks of related enterprises, the parent organization or even systems of government organizations.

Kaspersky Industrial CyberSecurity for Nodes supports rules that prevent certain programs from running on ICS systems, helping block any unauthorized use of remote administration utilities. At the same time, a map of the network built using Kaspersky Industrial CyberSecurity for Networks will help identify issues related to the lack of proper network segmentation.

Outdated operating systems, application software, and device firmware

Curiously, even those internet-facing **systems of industrial enterprises which are not that hard to update may remain vulnerable for a long time**, exposing OT to attacks and introducing serious risks, as showcased by real-world attack scenarios.

In some cases, installing updates is next to impossible – for example, when an operating system update on the server requires updating specialized software (such as the SCADA server) which, in turn, requires upgrading the equipment. As a result, there is an **amazing variety of antiques** that you can find on ICS networks – such as CNC machines running Windows XP SP1, or servers running Windows NT 4.0, or even MS-DOS used to control the industrial process!

But apart from these extreme scenarios, it should be kept in mind that industrial control systems work in such a way that even basic things like **installing an operating system security update** on workstations and servers **require careful testing**. In many cases, this work can only be performed at specially allocated times, during scheduled maintenance downtime. This means that operating system and application software updates are, as a rule, installed very rarely and attackers have large windows of opportunity to abuse known vulnerabilities and carry out their attacks. In such cases, given the high cost of the upgrade project, information security issues are not treated as essential.

If an enterprise has found itself in this situation, ICS engineers and information security experts should work together to develop a set of mitigation measures that will help prevent vulnerabilities from being exploited without requiring the system to be updated. Such measures can involve, for example, modifying the settings of software used on such systems or disabling a vulnerable service or component if it is not used, or isolating the vulnerable system, such as implementing additional segmentation or setting up a dedicated firewall rule.

Unfortunately, it is not always easy for an engineer or security professional to determine whether a particular OT system is vulnerable, how great the security risk really is, whether it is worth trying to patch the vulnerability, and what mitigation options are available if patching is not possible.

All popular publicly accessible vulnerability databases, including national ones, provide, at best, only information taken from advisories released by vulnerable products' vendors. The problem is that ICS manufacturers' advisories often contain incomplete or, even worse, incorrect data.

As a result, widely used vulnerability data sources contain a variety of inconsistencies and errors, including: incorrect severity scores that can greatly affect the perception of risk; lists of affected products that don't include some products that are affected by a given vulnerability or include products that aren't. This means that it is easy to make wrong conclusions about existing security issues in a given OT system and, consequently, come up with poorly informed decisions.

Another common situation is when the vulnerability description and assessment are correct, but suggested mitigation measures, namely updating to a newer version, do nothing to fix the issue: the update doesn't address the problem because the vulnerability is a major design flaw that requires a full revision and redesign of the vulnerable software or firmware, which the vendor failed to implement in the process of 'closing' the vulnerability.

One of the latest examples of such issues that we have dealt with is UMAS, Schneider Electric's proprietary protocol used to configure, monitor, collect data and control Schneider Electric's most widely used industrial controllers. In 2022, Kaspersky ICS CERT researchers published a detailed report about the issues and significant shortcomings discovered in the protocol that critically affected the security of automation systems based on Schneider Electric solutions.

And to make the problem even worse, most ICS systems have third-party technologies and common components built into them that also contain vulnerabilities. Examples include operating systems, license managers, web servers, communication protocols, engineering frameworks, and execution environments (for example, technologies widely used in ICS such as Codesys and IsaGRAPH, which have been researched in detail by Kaspersky ICS CERT experts), to name a few. Such vulnerabilities too often remain under the radar of OT manufacturers, who don't treat them as their responsibility, as well as vendors of vulnerable third-party components, who often don't know who uses their technology or don't consider themselves responsible for informing all their end users of the risks involved. This lack of responsibility and of accessible information is a huge cybersecurity risk, essentially a time bomb.

To get a more realistic understanding of risks associated with vulnerabilities in OT solutions and to make informed decisions on mitigating them, we recommend that you get access to Kaspersky ICS Vulnerability Intelligence in the form of human-readable reports or a machine-readable data feed, depending on your technical capabilities and needs.

Kaspersky Industrial Cybersecurity uses Kaspersky ICS Vulnerability Intelligence for automatic vulnerability identification and assessment. The solution identifies outdated and vulnerable software, detects and blocks attempts to exploit vulnerabilities, including those in ICS and other systems.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global project of Kaspersky 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