Kaspersky ICS CERT

kaspersky

Threats to ICS and industrial enterprises in 2022

As they are foreseen from November 2021

Evgeny Goncharov

23.11.2021 Version 1.0

Continuing trends

In recent years, we have observed various trends in the changing threat landscape for industrial enterprises, most of which have been evolving for some time. We can say with high confidence that many of these trends will not only continue, but gain new traction in the coming year.

Further evolution of cyberthreats as a response to infosec tools and measures

Improved corporate cybersecurity and the introduction of ever more tools and protection measures are causing cyberthreats to evolve. Here are some of the evolution areas worth paying attention to:

- **Reduced number of targets per individual attack**

  Individual attacks as part of cybercriminal campaigns are already targeting ever fewer victims. For instance, we see a new trend emerging in the criminal ecosystem of spyware-based authentication data theft, with each individual attack being directed at a very small number of targets (from single digits to several dozen). The trend is snowballing so rapidly that in some regions of the world up to 20% of all ICS computers on which we block spyware are attacked using this tactic. Such attacks are likely to comprise an even larger portion of the threat landscape next year. And the tactic is likely to spread to other types of threats as well.

- **Reducing the life cycle of malware**

  To avoid detection, more and more cybercriminals are adopting the strategy of frequently upgrading malware in their chosen family. They use malware at its peak effectiveness to break through the defenses of security solutions, and then switch to a new build as soon as the current one becomes readily detectable. For some types of threats (for example, spyware again), the lifetime of each build is shortening, and in many cases does not exceed 3–4 weeks (often even less). The evolution of modern MaaS platforms makes it much easier for malware operators globally to use this strategy. Next year we are sure to encounter it even more frequently in various threat scenarios. Combined with the downward trend in the number of victims per individual attack, the widespread use of this strategy will lead to an even greater variety of malware, thus posing a major challenge for security solution developers.

- **Modern APTs: now more persistent than advanced**

  To some extent, a similar trend can be traced in the tactics of many APTs. The "P" quality (persistent) in the abbreviation APT has become less dependent on "A" (advanced). We have long seen how a persistent presence in the victim's infrastructure is maintained through the doggedness and diligence of the operators, and that expanding and regularly upgrading the toolkit is becoming an alternative to finding new technical solutions and developing costly complex frameworks designed to remain undetected for as long as possible. In all likelihood, this strategy will be traced increasingly often in APT campaigns.

- **Minimizing the use of malicious infrastructure**

  In the fight against protection tools, attackers naturally seek to reduce the detectable malicious footprint of their actions. This is particularly reflected in attempts to minimize the use of malicious infrastructure. For example, we observed how C&C servers in some APTs had a very short lifespan, operating for no more than a couple of hours during the attack phase for which they were intended.

  And sometimes attackers manage to refrain from using not only any malicious, but also suspicious and untrusted infrastructure. For example, a popular tactic in spyware attacks is now to send phishing e-mails from compromised corporate mail accounts of a partner organization of the intended victim. In this case, well-crafted messages are practically indistinguishable from legitimate ones and virtually undetectable with automated tools.

  In our investigations of APT-related incidents at industrial enterprises, we have come across traces of how attackers, in parallel to the main thrust of the attack, have simultaneously tried to gain access from the infrastructure of a compromised industrial facility to other organizations or resources of the parent company, government agencies and the like; most likely in the hope that such attempts will go unnoticed.

  There is no doubt that the coming year will see more frequent use of such tactics by attackers in various categories.

Actions of various attacker categories

The debate about which threats pose the most danger to industrial enterprises often revolves around comparisons between APTs and cybercrime. And plans to improve information security and introduce new protection tools and measures are predicated, in some way, on the chosen adversary model. At the same time,

bear in mind that perceptions of the interests, capabilities and modus operandi of some categories of attackers can become outdated, and therefore require constant refreshing. Let's look at the relevant trends that are likely to continue or intensify next year.

- **APT and cybercriminal techniques, tactics and even strategies are becoming increasingly alike and may require similar security measures**

  Indeed, many APT and cybercriminal operations are sometimes difficult to distinguish, even for experts. For example,

  - Technically flawed APTs and "sophisticated" cybercriminal attacks no longer surprise anyone. In particular, we have seen more than a few poorly crafted phishing e-mails full of clearly visible blunders in campaigns associated with well-known APTs. And many are the times that we have come across near-flawless e-mails in targeted cybercriminal campaigns.
  - Similarly, APTs masquerading as cybercrime, and attacks by cybercriminals pretending to be an APT, have lost their wow factor.
  - Without a doubt, we will see in the APT arsenal the continued use not only of commercial tools, but of MaaS infrastructure and delivery methods as a means of initial penetration.

- **APT and cybercriminal lists of targets and potential victims can often include the same organizations**

  Of the many industrial companies out there, APTs are likely to focus on:

  - The military-industrial complex and aerospace industry — most likely for military and technological espionage purposes
  - Energy, transport and utilities — in an attempt to gain a foothold in the critical infrastructure of a "potential adversary" just in case, and to use it to develop other attacks (see examples above)
  - Knowledge-based industries — primarily for industrial espionage purposes

  Cybercriminals will continue to attack everyone they can reach, and in the vast majority of cases will monetize attacks using the same tried-and-tested methods:

  - Direct theft of funds by substituting bank details — through BEC tactics or access to the organization's financial systems
  - Extortion and ransomwaring of those able and willing to pay up
  - Reselling of stolen information to fellow cybercriminals, competitors of the victim and other interested parties

- **The direct financial harm caused by cybercrime is larger, but the damage from APTs is harder to predict and may be greater in the long term**

  Judging by the events of the past year, in terms of direct financial harm, the actions of cybercriminals might seem far more significant to industrial organizations than APTs. In 2021, for instance, we have seen many industries brought to a standstill and tens of millions of dollars paid out to ransomwarers. Meanwhile, there has been only one known case of significant financial damage from an APT over the entire year — and that happened when the attackers decided to masquerade as extortionists.

  That said, APT attacks can have a delayed negative effect that is very difficult to assess in advance (for example, years later a rival company might create a new product based on stolen data).

- **Don't forget about cyberhooligans and hacktivists**

  In 2021, cyberhooligans and hacktivists made global headlines on at least three occasions, demonstrating that vital industrial infrastructure is often poorly protected and ripe for the picking. The question of whether everything possible has been done to prevent such cases next year, we invite readers to ponder for themselves.

- **Extortion**

  As for perhaps the main trend of the outgoing year, despite the rhetoric of politicians and the frenzied actions of governments, the flywheel of extortion is spinning and cannot easily be stopped. The attacks are set to continue, including on industrial enterprises. Cybercriminals will protect themselves better and hedge the risks. The additional outlays will naturally be covered by victims, in the form of higher ransoms.

Current attack vectors

The following cybercriminal tactics and techniques will no doubt be used actively in the coming year.

- **Phishing** is the top initial penetration tool for targeted (and not-so-targeted) attacks. As shown by the past year:

  - Even bad phishing, we are sorry to say, works pretty well. Train your employees to read all incoming mail with a critical eye. Spelling and grammar mistakes, poor phrasing, incorrect names of companies and

officials, strange topics and unusual requests are all signs of poorly executed phishing. Any employee, even without IT security expertise, can recognize them
  - High-quality spear phishing, regrettably, is almost guaranteed to work. In every company, there is bound to be someone who blindly opens an attachment, follows a link, clicks a button or even makes contact with the attackers and unwittingly helps them to launch a malicious payload in the system
  - Cybercriminals of various stripes have mastered the art of spear phishing without using malicious infrastructure and of phishing using only trusted infrastructure (as covered above). Moreover, the latter is the most dangerous and hard-to-detect method. Unfortunately, it will doubtless claim many victims in the year to come.

- **Known vulnerabilities in internet-facing hardware** are also sure to remain a popular penetration vector. Update firewalls and SSL VPN gateways in good time.
- **Zero-day vulnerabilities in OS components and popular IT products** will remain a relatively rare tool in advanced APTs, while **unknown security holes in less common (and therefore probably less-well tested) products** will be actively exploited by cybercriminals.
- **Compromise of domain name registrars and certification authorities, attacks on suppliers**

  Regarding these "advanced" tactics, last year we again saw compromise attacks on domain name registrars (access to the victim's web control panel at the bare minimum) and certification authorities, as well as new attack scenarios aimed at suppliers. Such threats have the potential to go undetected for a long time, allowing attackers to carry out sustained operations. Those of them who can afford such vectors will certainly not abandon them.

  So, when planning protection means and measures for the coming year, keep an eye on the security not only of your own infrastructure, but of third-party services you use. When choosing suppliers of products for your IT/OT systems, stamp your own cybersecurity requirements on both the products and the suppliers themselves. And when collaborating with business partners, be aware of the threats that their security weaknesses could pose to you.

Building on the success of 2021

Cybercriminals have definitely made significant strides in 2021: the list of high-profile ransomware attacks on industrial enterprises this year is probably longer than for all previous years combined. APT campaigns targeting industrial organizations have also been keeping researchers very busy.

Note that many of the achievements of cybercriminals this year will be used as a stepping stone into the next.

- **Stolen data and compromised IT systems**

  According to our telemetry and analysis of information found on the dark web, cybercriminals in 2021 compromised at least thousands of industrial organizations worldwide. We think that their total number vastly exceeds the number of organizations hit by ransomware or targeted by APTs. Some of those compromised might get lucky and simply fall off the cybercriminal radar. But not all. And for some companies, the consequences of a security compromise in 2021 will catch up with them only in 2022.

- **Threats to OT**

  Disturbingly, we also found signs of compromise in many organizations on computers directly related to ICS. So the damage in some cases may not be limited to encryption of IT systems and data theft in the office network.

- **P stands for perseverance**

  As noted above, the letter P in the abbreviation APT should be understood not only as persistent (as in continuous), but also in the sense of persevering (as in relentless). So organizations that have already been attacked should be on their guard: it is very likely (with some APTs, even "certain") that they will be targeted again, possibly more than once.

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