ICS threat predictions for 2021

Evgeny Goncharov

We present our vision of what challenges industrial cybersecurity will soon be (or already is) facing, and what to expect from cybercriminals in 2021.

Random infections

1. Infections will tend to be less random or have non-random follow-ups, as cybercriminals have spent the past several years profiling randomly infected computers that are connected to industrial networks or have periodic access to them. Access to such computers will be — and is perhaps already being — resold to more sophisticated groups with specific schemes for monetizing attacks on industrial facilities already in place.
2. For several years now, various groups have specialized in attacks against industrial enterprises with the express aim to steal money — through BEC schemes or advanced hacks to gain access to victims' financial and accounting systems. Through years of criminal operations, they have come to understand the business processes of industrial enterprises and gained access to a large amount of technical information about network assets and operational technologies. We expect to see new and unconventional scenarios of attacks on OT/ICS and field devices, coupled with ingenious monetization schemes. Cybercriminals have had more than enough time and opportunities to develop them.
3. End of support for Windows 7 and Windows Server 2008, which are popular in ICS around the world, and, especially, the leak of the source code of Windows XP, which is still very common on industrial networks, pose a significant threat to the security of industrial enterprises. There is a high chance that a WannaCry-like scenario will be repeated in the very near future. And industrial enterprises may be among the hardest hit.

Ransomware attacks

1. Ransomware is becoming more technically advanced and sophisticated. Cybercriminals will continue to employ hacker and APT techniques, painstakingly exploring and probing the network of the target organization to locate the most valuable/vulnerable systems, hijack administrator accounts, and launch simultaneous blitz attacks using standard admin tools.
2. Cybercriminals have developed a fondness for industrial companies, because they tend to pay ransom. This means that the attacks will continue.
3. There will be hybrid attacks involving document theft with the threat to publish the documents or sell them on the darknet in case of refusal to pay up.
4. The ideas implemented in Snake for ransomware attacks targeting OT/ICS will gain traction.
5. It is highly likely that we will see attacks disguised as ransomware but pursuing completely different goals — a repeat of the ExPetr technique.

Cyberespionage

1. Cybercriminals will figure out (some already have) that inside the OT perimeter secrets are not guarded as well as in office networks and that OT networks may be even easier to break into, since they have their own perimeter and attack surface.
2. The flat network topology and other access control issues in OT networks can make them an attractive entry point into the intimate recesses of the corporate network and a springboard into other related organizations and facilities.
3. The desire of many countries for technological independence, alongside with global geopolitical and macroeconomic upheaval, means that attack targets will include not only traditional opponents, but also tactical and strategic partners — threats can come from any direction. We have already seen examples of such attacks.

APT

1. The number of APT groups will continue to grow — we will see more and more new actors, including ones that attack various industrial sectors.
2. The activity of these groups will correlate with local conflicts, including those in the hot phase, with cyberattacks on industrial enterprises and other facilities used as a warfare tool, alongside drones and media-driven misinformation.
3. In addition to data theft and other piecemeal operations, some group is likely to get down to more serious business in 2021, perhaps in the vein of Stuxnet, Black Energy, Industroyer and Triton.

COVID consequences

1. Against the backdrop of economic decline, lockdowns, slower growth and ruin for small businesses, the ranks of cybercriminals are sure to swell as skilled people seek alternative employment, and groups associated with national governments will strengthen as well.
2. The online presence of municipal services and utilities and the increased digitization of government and public services will make them more vulnerable to attacks of cybercriminals and create more opportunities for cross-agency attacks and assaults on central and local government functions and the systems that support and implement them. For example, a threat actor could use a governmental or municipal web service as an entry point, compromise the victim's internal infrastructure and use the communication channels and supply chain connecting various governmental, municipal and even private organizations to reach their final target (such as shutting down transportation systems).
3. Restrictions on on-site work, which prevented new equipment from being installed and configured, have slowed down the efforts of many industrial enterprises to beef up their perimeter security. Together with the increasing number and variety of remote sessions, this may even reduce the level of perimeter protection of industrial networks. This being the case, the safety of industrial facilities will largely depend on the performance of endpoint solutions and the security awareness of employees. At the same time, cyberattacks aimed at industrial companies are maturing. As a result, despite the currently observed drop in attacks on OT/ICS computers, the number of serious incidents is not going to decrease.

4. The reduction in on-site personnel who are able to promptly transfer systems and installations to manual control in the event of a successful cyberattack on the industrial network could facilitate the wider spread of malware and lead to more severe consequences.

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