Industrial Enterprise and IoT Security Threats: Forecast for 2018

Kaspersky Lab ICS CERT

The Threat Landscape in 2017

The year 2017 was one of the most intensive in terms of incidents affecting the information security of industrial systems. Security experts discovered hundreds of new vulnerabilities, researched new threat vectors targeting ICS and industrial processes, collected and analyzed statistics on accidental infections of industrial systems and detected targeted attacks on industrial enterprises (specifically, Shamoon 2.0/StoneDrill). And, for the first time since Stuxnet, discovered and analyzed a malicious toolset targeting physical systems: CrashOverride/Industroyer. Some experts have categorized it as a "cyberweapon".

However, encryption ransomware attacks became the most significant threat to industrial systems in 2017. According to Kaspersky Lab ICS CERT, in the first half of the year, industrial information systems in 63 countries across the globe came under numerous attacks of encryption ransomware belonging to 33 different families. The WannaCry and ExPetr destructive ransomware attacks appear to have changed forever the attitude of industrial enterprises to the problem of protecting their key production systems.

What Can We Expect in 2018?

1. **A rise in general and accidental malware infections**

   With few exceptions, cybercriminals have not as yet discovered simple and reliable schemes for monetizing attacks on industrial information systems. Accidental infections and incidents in industrial networks caused by "ordinary" (general-purpose) malicious code designed for more traditional cybercriminal targets, such as corporate "office" networks and computers of individual users, will continue in 2018. At the same time, in the future we are likely to see such situations result in increasingly severe consequences for industrial environments. The problem of regularly updating software in industrial systems in line with corporate networks will remain unresolved, despite repeated warnings from the security community.

2. **Increased risk of targeted ransomware attacks**

   The WannaCry and ExPetr attacks have taught both security experts and cybercriminals that operational technology (OT) systems can be even more vulnerable to such attacks than IT systems and can also be accessed through the Internet. Moreover, damage caused by malware activity in the OT network can exceed that in the corresponding corporate network, and 'firefighting' in the case of OT is much more difficult. The worst part is probably that incidents in industrial companies have demonstrated how poorly organized and inefficient their staff can be when it comes to cyberattacks on their OT infrastructure. All of these factors make industrial systems an attractive target for ransomware attacks.

3. Increasing number of attacks on industrial enterprises by cyber fraudsters

In 2016 – 2017 we saw an unprecedented interest in industrial companies and organizations on the part of cyber fraudsters. We have described one such campaign that we investigated (“Business Email Compromise” attacks), which was carried out globally by Nigerian cybercriminals, in our reports.

Strange but true: the characteristic business processes of industrial enterprises and, consequently, the communications between the sellers and buyers of industrial goods and services, as well as the sales and supply of means of industrial production, turned out to be very vulnerable to the attack methods perfected by cyber fraudsters. Clearly, industrial companies have become an attractive target for criminals.

This distressing conclusion is also supported by our new discoveries: the “Nigerian” methods have been adopted by criminals from other countries. We are currently researching the activity of several such groups specializing in attacks on industrial organizations.

The problem is clearly not going to go away all by itself: we should expect a growing number of such attacks in the near future.

4. More incidents related to industrial cyberespionage

The growing threat of targeted ransomware attacks against industrial companies could trigger the development of another, related area of cybercrime: the theft of data from industrial information systems for subsequent use in the preparation and implementation of targeted (including ransomware) attacks.

5. The emergence of malware designed to exploit vulnerabilities in industrial automation system components

In 2017, the demand for zero day exploits targeting industrial control systems grew significantly on the black market. This means that criminals are actively developing targeted attacks on industrial enterprises. This is not surprising, given that in the past five years we have seen many forerunners of this development:

- A growing number of targeted attacks on industrial control systems, in which ordinary malware is used to gain remote access to industrial automation systems, after which malicious operations are conducted manually, using compromised legitimate control tools – HMI, the engineering environment, etc.;
- Inclusion of modules targeting ICS in malware platforms/frameworks (such as BlackEnegry);
- The emergence of specialized software designed to automate malicious impact on industrial systems (one example is CrashOverride);
- A growing interest of cybercriminals (even those with medium or low skill level) in industrial companies;
- The steady increase in industrial enterprise automation levels and, as a consequence, a growing number of industrial control systems that are in some way (not necessarily directly) available from the Internet.

At the same time, vulnerabilities in "shared" industrial system components developed by third-party vendors will probably be the first to be exploited in most cases.

In 2017, we have seen examples of vulnerabilities in third-party products (hasplms) that open up opportunities for attacking a variety of industrial automation systems. It is likely that threat actors will exploit primarily this type of vulnerability in their attacks.

6. **New types of malware and malicious tools**

We will probably see new malware being used to target industrial networks and assets, with features including stealth and the ability to remain inactive in the IT network to avoid detection, only activating in the much less secure OT infrastructure. Another possibility is the emergence of ransomware targeting field-level ICS devices and physical assets (pumps, switches, etc.).

7. **Criminals will take advantage of threat analyses published by security researchers**

In 2017, researchers did a good job finding and making public numerous new vectors of attacks on industrial assets and infrastructure and performing deep analysis of the malicious toolsets found. All of this is certainly good for the security of industrial facilities. However, in their attempts to demonstrate the need for protecting industrial automation systems, information security researchers may have gone a little too far by providing detailed information on the attack vectors found. Criminals could also make use of this information.

For example, hacktivists could take advantage of the CrashOverride/Industroyer toolset disclosure to run denial-of-service attacks on power systems; criminals may develop targeted ransomware and may even invent new monetizing schemes for blackouts. The PLC worm concept could inspire criminals to create real-world malicious worms that spread from one PLC to another; while others could try to implement malware using one of the standard languages for programming PLCs. It is even possible that some threat actors will develop PLC malware operating at a low level based on an approach demonstrated by information security researchers. The latter two approaches could pose a serious problem for developers of existing security solutions.

8. **New underground market segments focused on attacks on industrial systems**

The focus of threat actors on industrial control systems will inevitably result in the emergence of new segments of the cybecriminal market focused on the theft of ICS configuration data and access credentials. Offerings of botnets with "industrial" nodes may also appear on the market.

Design and implementation of advanced cyberattacks targeting physical objects and systems requires an expert knowledge of ICS and the relevant industries. Demand for such specialized knowledge is expected to drive growth in such areas as "malware as a service", "attack vector design as a service", "attack campaign as a service" and other services related to attacks on industrial enterprises.

Using the "Business Email Compromise" type fraud attacks as an example, we can see that criminals have already begun to specialize by industry – metallurgy, petrochemistry, etc. To carry out even such relatively simple attacks on industrial organizations, the criminals need some industry-specific knowledge – at the very least to "speak the same language" as their potential victims.

9. Changes in national regulations

In 2018, many new regulatory initiatives having to do with industrial automation systems will come into effect in Russia and in other countries. On top of everything else, this will force companies that own critical infrastructure objects and industrial assets to put more effort into their cybersecurity assessment. As a result, we will probably see new vulnerabilities identified in industrial systems. We may also learn of incidents at industrial enterprises and previously unknown attacks.

However, some regulatory decisions, which restrict the access of foreign companies and experts to industrial enterprises and critical infrastructure objects, will have a negative impact on information security – at least in the short run (i.e., in the next several years), while these countries lack the necessary number of sufficiently highly qualified experts or proven technologies. During that time, criminals will have a substantial advantage. Even in the long run, such decisions are not likely to be beneficial. Kaspersky Lab's many years of experience show that combating global crime locally is ineffective, to say the least.

10. Growing availability of, and investment in industrial cyber insurance

Cyber-risk insurance is becoming an integral part of risk management for industrial enterprises. Until recently, risks associated with cybersecurity incidents were excluded from insurance contracts – in effect, insurance companies equated them with terrorist attacks. But the situation is changing, with new initiatives introduced both by cybersecurity companies and by the main players in the insurance business. In 2018, this will increase the number of industrial automation system audits/security assessments, as well as the number of recorded and investigated cybersecurity incidents.

11. Using cyberattacks to commit traditional crimes against industrial enterprises

As mentioned above, schemes for monetizing attacks on industrial control systems are complicated and not very accessible for cybercriminals who are outsiders to the enterprise or the industry. Obviously, it is next to impossible to make money on a stolen tank car of petroleum products while sitting at the computer, without using the methods of "ordinary" (not "cyber") criminals. However, this does not mean that "ordinary" criminals do not use "cyber" methods to commit their crimes. In our experience, a significant proportion of such crimes against industrial facilities are committed with active involvement of industry insiders, who know perfectly well how an unaccounted-for tank car of fuel can be disposed of. The increasing level of industrial automation makes using methods characteristic of cyberattacks to commit such crimes not only possible but unavoidable. Without doubt, such attacks will steadily grow in number in the coming years.

Internet of Things

When it comes to IT security, both organizations and individual users relegate IoT devices to the periphery of their attention. These devices always seem to be "secondary" and "non-essential" – though "useful" and "convenient", still "not essential" and therefore "less important". Today, the number of existing IoT devices is already very large and these are mostly narrow-purpose devices that cannot be protected using traditional methods, with timely patching, installing and configuring antivirus solutions, keeping antivirus databases up-to-date, etc.

Vendors rush to release more and more new products and, in their attempts to attract as many customers as possible and to keep ahead of the competition, they only care about their products' functionality.

Having cut their teeth on traditional IT systems, cybercriminals are taking advantage of the existing situation with the security of IoT devices. The number of attacks on IoT devices is undoubtedly set to grow.

1. **New botnets made up of IoT devices will be created for DDoS attacks on traditional IT systems**

The most obvious application of infected IoT devices is to conduct large-scale DDoS attacks on Internet services and telecoms.

The world first realized the scope of this threat in 2016, when the actors behind the Mirai botnet demonstrated that seemingly harmless devices can pose a very serious threat. More than half a million "smart" IP cameras were used to conduct a series of large-scale DDoS attacks.

This year, we also saw the emergence of several large zombie networks consisting of IoT gadgets.

Without doubt, botnets made up of IoT devices are of interest both to the expert community and to the general public. The numerous studies, research papers, conference reports and mass media publications catch the attention of threat actors. For example, according to an article published in April 2017, more than 1,000 IP camera models by 354 different vendors had a dangerous vulnerability in the built-in web server. It didn't take threat actors long to respond: a new IoT botnet made up of vulnerable cameras was detected as early as May. Researchers dubbed the botnet Persirai.

A very short time ago, in October 2017, one more large network made up of infected IP cameras was detected. The new botnet was dubbed Reaper. It has been reported that the malware exploits multiple vulnerabilities to infect cameras by different vendors. According to experts, there may be up to two million vulnerable devices. If Reaper succeeds in reaching at least some of these devices, cybercriminals may turn the botnet into a major cyberweapon.

It is highly probable that we will see a considerable increase in the number of IoT zombie networks in 2018. It can also be expected that threat actors will no longer focus on IP cameras and will look to other types of "smart" devices, as well.

2. **Compromised IoT devices used as an entry point to penetrate the IT and OT network perimeter**

   The lamentable state of IoT information security has opened up one more opportunity for cybercriminals: IoT devices can be used to penetrate a “well-protected” network belonging to an organization or a person. In the process of performing information security research or penetration tests we often detect this type of vulnerability and tell our customers about the associated risks. There is evidence that video surveillance systems, as well as other IoT systems, have already been used in targeted attacks on industrial and infrastructure facilities.

   It is highly probable that this vector will be used by threat actors in the future to carry out targeted attacks and, possibly, even for mass random infections of both IT and OT systems.

3. **IOT ransomware**

   The evolution of attacks on IoT today is in many ways similar to that of early attacks on IT, with “childish” vulnerabilities and relatively unsophisticated attack vectors. Clearly, a very disagreeable phenomenon can be expected to emerge in the near future – ransomware targeting IoT systems, such as smart building components, elements of smart city or public transit infrastructure, etc. Judging by the experience of “classical” IT systems, ransomware attacks can be very lucrative for cybercriminals. Sadly, we have already seen the first examples of such attacks.

4. **Attacks via shared technologies**

   A variety of IoT solutions are often built using numerous shared technologies: the ARM CPU architecture and Linux family operating systems, various IoT broker applications (such as MQTT), OPC UA for IIoT solutions, etc. Vulnerabilities in such shared components pose a huge threat – they can be used to organize large-scale cyberattacks and are sure to be exploited by threat actors in the near future.

5. **Penetration of Internet of Things technologies into the sphere of traditional crime**

   It is well known that systems like Shodan or Censys that help to find services, including IoT components, which are available through the Internet, can be intentionally used to find vulnerable devices that can be reached through the Internet. For example, owners of the Insecam service did this to make images from unprotected surveillance cameras across the globe available to the general public. Since the service’s goal is to raise awareness, its owners do not publish information that can be used to determine a camera’s location, but they have suggested that this is possible.

   Data from IP cameras, smart home and smart city devices can be used by threat actors to plan and coordinate traditional (non-cyber) crimes (a Kaspersky Lab expert wrote about this as far back as two years ago).

   It is likely that the next step to be made by cybercriminals after creating botnets for DDoS attacks will be to develop “platforms” that will be used to collect information and control IoT devices as an auxiliary tool for “traditional” criminals.

Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) is a global project of Kaspersky Lab aimed at coordinating the work of industrial automation system vendors, owners and operators of industrial facilities and IT security researchers in addressing issues associated with protecting industrial enterprises and critical infrastructure facilities.

Kaspersky Lab ICS CERT

Ics-cert@kaspersky.com