Threats posed by using RATs in ICS

Kirill Kruglov
Kaspersky Lab ICS CERT

Evgeny Goncharov
Kaspersky Lab ICS CERT

20.09.2018

Contents

While conducting audits, penetration tests and incident investigations, we have often come across legitimate remote administration tools (RAT) for PCs installed on operational technology (OT) networks of industrial enterprises. In a number of incidents that we have investigated, threat actors had used RATs to attack industrial organizations. In some cases, the attackers had stealthily installed RATs on victim organizations' computers, while in other cases, they had been able to use the RATs that were installed in the organization at the time of the attacks. These observations prompted us to analyze the scope of the threat, including the incidence of RATs on industrial networks and the reasons for using them.

Methodology

The statistical data presented in this paper was collected using the Kaspersky Security Network (KSN) from ICS computers protected by Kaspersky Lab products that Kaspersky Lab ICS CERT categorizes as part of the industrial infrastructure at organizations. This group includes Windows computers that perform one or several of the following functions:

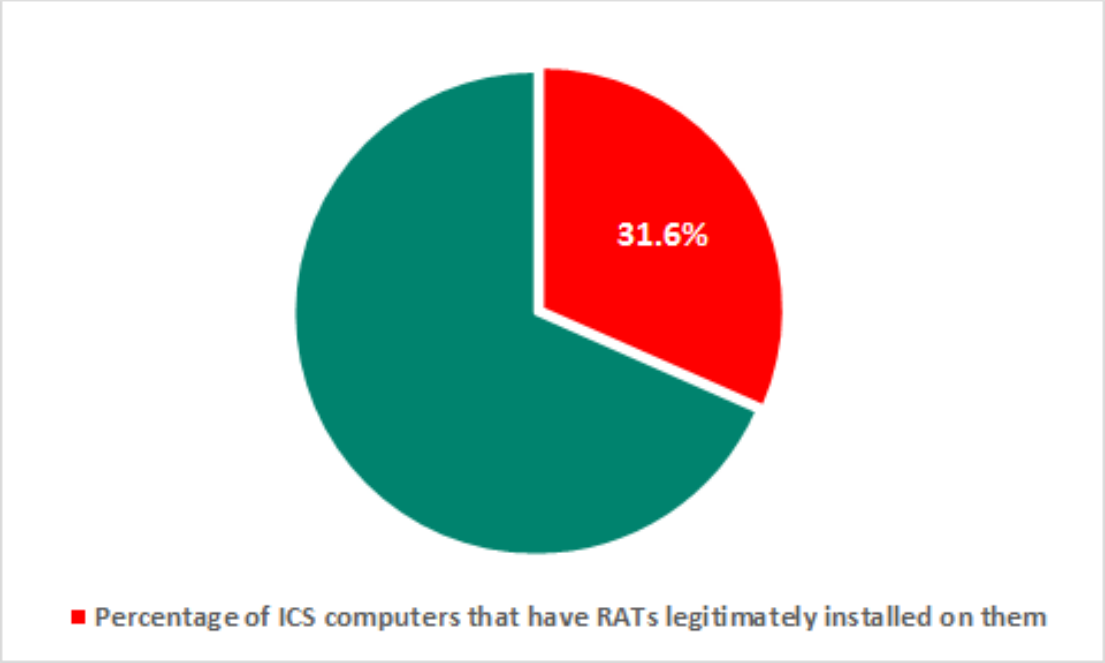
- supervisory control and data acquisition (SCADA) servers;
- data storage servers (Historian);
- data gateways (OPC);
- stationary workstations of engineers and operators;
- mobile workstations of engineers and operators;
- Human Machine Interface (HMI).

As part of our research, we considered and analyzed all popular RATs for Windows, with the exception of Remote Desktop, which is part of the Windows operating system. Our research into this RAT is ongoing and will be presented in the next paper of the series.

The use of RATs in ICS

According to KSN data, in the first half of 2018, legitimate RATs (programs categorized as not-a-virus: RemoteAdmin) were installed and used on one ICS computer in three.

Percentage of ICS computers that have RATs legitimately installed on them



The statistics support our observations: RATs are indeed often used on OT networks of industrial enterprises. We believe this could be due to attempts to reduce costs associated with maintaining ICS and minimize the response time in the event of malfunction.

As we were able to find out, remote access to computers on the OT network is not restricted to administrators and engineers inside the enterprise network's perimeter. It can also be made available via the internet to users outside the enterprise network perimeter. Such users can include representatives of third-party enterprises – employees of system integrators or ICS

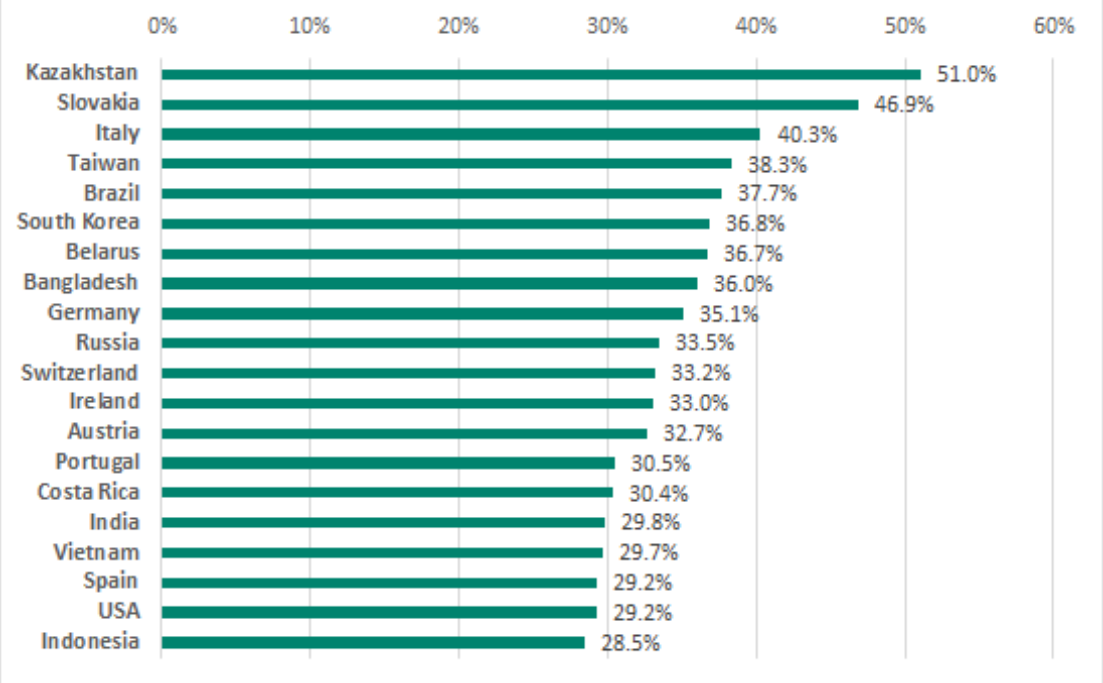
vendors, who use RATs for diagnostics, maintenance and to address any ICS malfunctions. As our industrial network security audits have shown, such access is often poorly supervised by the enterprise's responsible employees, while remote users connecting to the OT network often have excessive rights, such as local administrator privileges, which is obviously a serious issue in terms of ensuring the information security of industrial automation systems.

From interviews with engineers and operators of various industrial systems that we have audited, and based on an analysis of ICS user documentation, we have determined that RATs are most commonly used on industrial networks according to the following scenarios:

1. To control/monitor HMI from an operator workstation (including displaying information on a large screen);
2. To control/maintain HMI from an engineering workstation;
3. To control SCADA from an operator workstation;
4. To provide SCADA maintenance from an engineering workstation or a computer of a contractor/vendor (from an external network);
5. To connect multiple operators to one operator workstation (thin client-like architecture used to save money on licenses for the software used on operator workstations);
6. To connect to a computer on the office network from the OT network via HMI and perform various tasks on that computer (access email, access the internet, work with office documents, etc.).

Some of the scenarios listed above indicate that the use of RATs on the OT network can be explained by operational requirements, which means that giving up the use of RATs would unavoidably entail modifications to work processes. At the same time, it is important to realize that an attack on a poorly protected RAT could easily cause disruptions to the industrial process and any decisions on using RATs on the OT network should be made with this in mind. Tight controls on the use of RATs on the OT network would help to reduce the attack surface and the risk of infection for systems administered remotely.

TOP 20 countries by percentage of ICS computers on which RATs were used at least once during the first half of 2018 (to all ICS computers in each country)

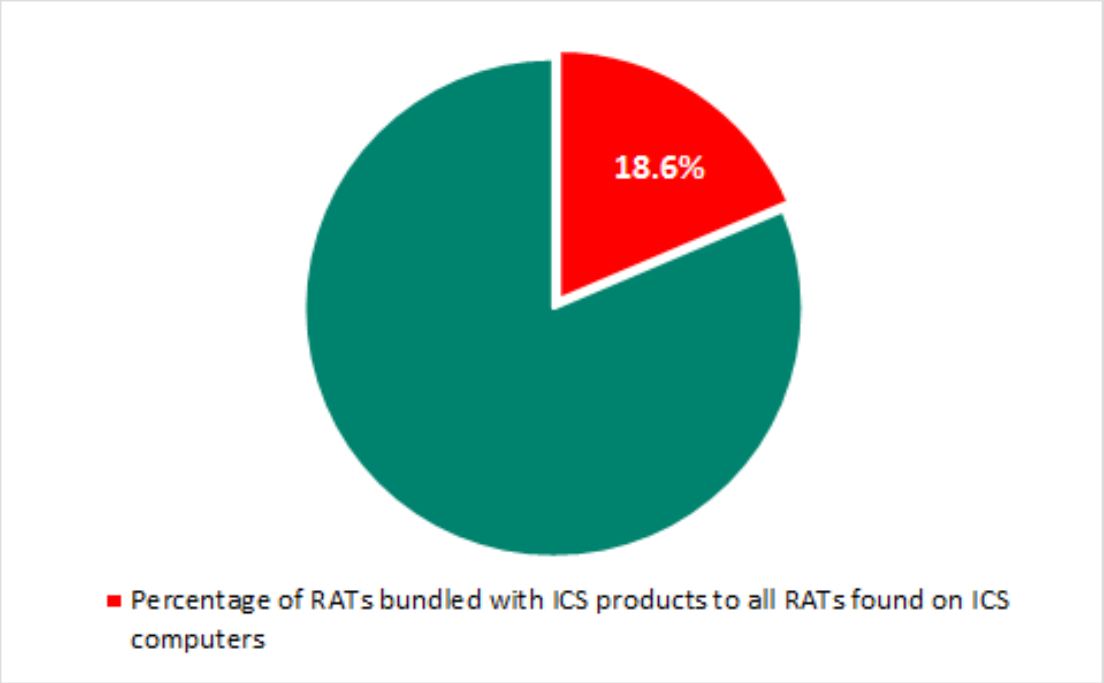


Scenarios of RAT installation on ICS computers

According to our research, there are three most common scenarios of RAT installation on ICS computers:

1. Installation of ICS software distribution packages that include RATs (using separate distribution packages or ICS software installers). RATs included in ICS software distribution packages make up 18.6% of all RATs we have identified on ICS computers protected by Kaspersky Lab products.

Percentage of RATs bundled with ICS products to all RATs found on ICS computers



2. Deliberate installation of RATs by personnel or suppliers – network administrators, engineers, operators, or integrator companies. We do not undertake to judge whether these installations are legitimate. Based on our experience of industrial network audits and incident investigation, we can state that many such installations do not comply with the organization's information security policy and some are installed without the knowledge of respective enterprises' responsible employees.
3. Stealthy installation of RATs by malware. An example of this is a recent attack that we have investigated (see below).

RAT-related threats to ICS

Threats associated with the use of RATs on industrial networks are not always obvious, nor are the reasons for which RATs are used.

Most of the RATs we have identified on industrial systems have the following characteristics that significantly reduce the security level of the host system:

- Elevated privileges – the server part of a RAT is often executed as a service with system privileges, i.e., NT SYSTEM;
- No support for restricting local access to the system / client activity;

- Single-factor authentication;
- No logging of client activity;
- Vulnerabilities (our report on zero-day vulnerabilities identified in popular RAT systems that are used, among other applications, in products by many ICS vendors, will be published by the end of the year);
- The use of relay servers (for reverse connections) that enable RATs to bypass NAT and firewall restrictions on the network perimeter.

The most critical RAT-related problem is the use of elevated privileges and the absence of any means to limit these privileges (or to restrict a remote user's local access). In practice, this means that if attackers (or malware) gain access to a remote user's computer, steal authentication data (login/password), hijack an active remote administration session or successfully attack a vulnerability in the RAT's server part, they will gain unrestricted control of the ICS system. By using relay servers for reverse connections, attackers can also connect to these RATs from anywhere in the world.

There are also other issues that affect RATs built into ICS software distribution packages:

- RAT components and distribution packages are rarely updated (even if new versions of ICS distribution packages are released). This makes them more likely to contain vulnerabilities;
- In the vast majority of cases, the default password is used – it is either hardcoded into the RAT by the ICS software vendor or specified in the documentation as "recommended".

RATs are legitimate software tools that are often used on industrial networks, which means it can be extremely difficult to distinguish attacks involving RATs from legitimate activity. In addition, since the information security service and other employees responsible for ICS security are often unaware that a RAT is installed, the configuration of RATs is in most cases not analyzed when auditing the security of an industrial network. This makes it particularly important to control by whom, when and for what purposes RATs are used on the industrial network and to ensure that it is completely impossible to use RATs without the knowledge of employees responsible for the OT network's information security.

Attacks of threat actors involving RATs

Everything written above applies to potential threats associated with the use of RATs.

Based on our analysis of KSN statistics, we were able to identify a number of attacks and malware infection attempts involving RATs installed on ICS computers. In most cases, attacks were based on the following scenarios (in the descending order of attack incidence):

1. A brute force network attack from the local network or the internet designed to crack logins/passwords;
2. An attacker or malware using a RAT to download and execute malware using stolen or cracked authentication credentials;
3. A remote user (probably a legitimate user deceived by attackers) using a RAT to download a Trojan to an ICS computer and then executing it; the Trojan can be disguised as an office document, non-industrial software (a game, multimedia software, etc.), a crack/keygen for office, application or industrial software, etc.;
4. A network attack from the local network or the internet on the server part of the RAT using exploits.

Brute force type network attacks (designed to crack logins/passwords) are the most common: their implementation does not require any special knowledge or skills and the software used in such attacks is publicly available.

It cannot be determined based on available data who connects to a RAT's server part installed on an ICS computer – a legitimate user, an attacker or malware – or why. Consequently, we can only guess whether this activity represents a targeted attack, sabotage attempts or a client's error.

Network attacks from the internet were most probably conducted by threat actors using malware, penetration testing tools or botnets.

Network attacks from the local network could indicate the presence of attackers (possibly including an insider) on the network. Another possibility is that there is a compromised computer on the local network that is either infected with malware or is used by the attacker as a point of presence (if the authentication credentials were compromised earlier).

Attacks on industrial enterprises using RMS and TeamViewer

In the first half of 2018, Kaspersky Lab ICS CERT identified a new wave of phishing emails disguised as legitimate commercial offers. Although the attacks targeted primarily industrial companies within the territory of Russia, the same tactics and tools can be used in attacks on industrial companies in any country of the world.

The malware used in these attacks installs legitimate remote administration software on the system — TeamViewer or Remote Manipulator System/Remote Utilities (RMS). In both cases, a system DLL is replaced with a malicious library to inject malicious code into a legitimate program's process. This provides the attackers with remote control of the infected systems. Various techniques are used to mask the infection and the activity of the software installed on the system.

If necessary, the attackers download an additional malware pack to the system, which is specifically tailored to the attack on each individual victim. This set of malware may contain spyware, additional remote administration tools that extend the threat actor's control of infected systems, malware to exploit vulnerabilities in the operating system and application software, as well as the Mimikatz utility, which makes it possible to obtain account data for Windows accounts.

According to available data, the attackers' main goal is to steal money from victim organizations' accounts, but possible attack scenarios are not limited to the theft of funds. In the process of attacking their targets, the attackers steal sensitive data belonging to target organizations, their partners and customers, carry out surreptitious surveillance of the victim companies' employees, and record audio and video using devices connected to infected machines. Clearly, on top of the financial losses, these attacks result in leaks of victim organizations' sensitive data.

Multiple attacks on an auto manufacturer

A characteristic example of attacks based on the second scenario was provided by attacks on the industrial network of a motor vehicle manufacturing and service company, in particular, on computers designed to diagnose the engines and onboard systems of trucks and heavy-duty vehicles. Multiple attempts to conduct such attacks were blocked by Kaspersky Lab products.

A RAT was installed and intermittently used on at least one of the computers in the company's industrial network. Starting in late 2017, numerous attempts to launch various malicious programs using the RAT were blocked on the computer. Infection attempts were made regularly over a period of several months – 2-3 times a week, at different times of the day. Based in part on other indirect indicators, we believe that RAT authentication data was compromised and used by attackers (or malware) to attack the enterprise's computers over the internet.

After gaining access to the potential victim's infrastructure via the RAT, the attackers kept trying to choose a malicious packer that would enable them to evade antivirus protection.

The blocked programs included modifications of the malware detected by Kaspersky Lab products as Net-Worm.Win32.Agent.pm. When launched this worm immediately begins to proliferate on the local network using exploits for the MS17-010 vulnerabilities – the same ones that were published by ShadowBrokers in the spring of 2017 and were used in attacks by the infamous WannaCry and ExPetr cryptors.

The Nymaim Trojan family was also blocked. Representatives of this family are often used to download modifications of botnet agents from the Necus family, which in turn have often been used to infect computers with ransomware from the Locky family.

Conclusion

Remote administration tools are widely used on industrial networks for ICS monitoring, control and maintenance. The ability to manipulate the ICS remotely significantly reduces maintenance costs, but at the same time, uncontrolled remote access, the inability to provide 100% verification of the remote client's legitimacy, and the vulnerabilities in RAT code and configuration significantly increase the attack surface. At the same time, RATs, along with other legitimate tools, are increasingly used by attackers to mask malicious activity and make attribution more difficult.

To reduce the risk of cyberattacks involving RATs, we recommend the following high-priority measures:

- Audit the use of application and system remote administration tools on the industrial network, such as VNC, RDP, TeamViewer, and RMS / Remote Utilities. Remove all remote administration tools that are not required by the industrial process.
- Conduct an audit and disable remote administration tools which came with ICS software (refer to the relevant software documentation for detailed instructions), provided that they are not required by the industrial process.
- Closely monitor and log events for each remote control session required by the industrial process; remote access should be disabled by default and enabled only upon request and only for limited periods of time.

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

Kaspersky Lab ICS CERT **Ics-cert@kaspersky.com**