Kaspersky ICS CERT

kaspersky

Attacks on industrial enterprises using RMS and TeamViewer: new data

Vyacheslav Kopeytsev

05.11.2020 Version 1.0

Contents

In summer 2019, Kaspersky ICS CERT identified a new wave of phishing emails containing various malicious attachments. The emails target companies and organizations from different sectors of the economy that are associated with industrial production in one way or another.

We reported these attacks in 2018 in an article entitled "Attacks on industrial enterprises using RMS and TeamViewer", but recent data shows that the attackers have modified their attack techniques and that the number of enterprises facing the threat of infection is growing.

Before publishing this report, we waited for the vendor of the RMS software to make changes to its services to ensure that the results of this research could not be used to exploit vulnerabilities.

This report in a nutshell

- From 2018 to at least the early fall of 2020, attackers sent phishing emails laced with malware.
- The attacks make use of social engineering techniques and legitimate documents, such as memos and documents detailing equipment settings or other industrial process information, which have apparently been stolen from the company under attack or its business partners.
- The attacks still use remote administration utilities. The graphical user interface of these utilities is hidden by the malware, enabling the attackers to control infected systems without their users' knowledge.
- In the new version of the malware, the attackers changed the notification channel used after infecting a new system: instead of malware command-and-control servers, they use the web interface of the RMS remote administration utility's cloud infrastructure.
- Stealing money from the organization under attack remains the main objective of the attackers.
- During an ongoing attack, the cybercriminals use spyware and the Mimikatz utility to steal authentication credentials that are subsequently used to infect other systems on the enterprise network.

The full article is available on Kaspersky Threat Intelligence.

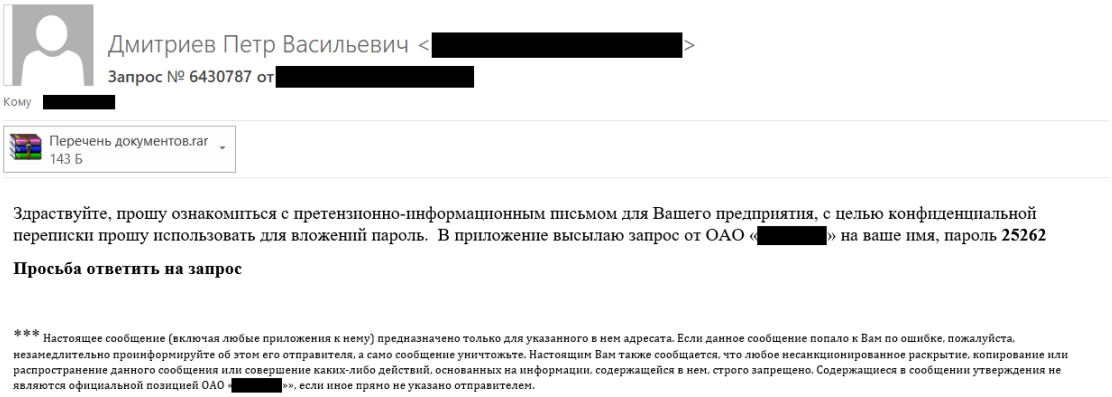
For more information please contact: ics-cert@kaspersky.com.

Technical Analysis

Since we described the technical details of this series of attacks in our previous report, Attacks on industrial enterprises using RMS and TeamViewer, in this document we only list the main stages of an attack and describe the changes to the attackers' tactics and toolset that have been implemented since the publication of the previous report.

Spreading

Phishing emails used in this attack are in most cases disguised as business correspondence between organizations. Specifically, the attackers send claim letters on behalf of a large industrial company.


Дмитриев Петр Васильевич <[redacted]>
Запрос № 6430787 от [redacted]
Кому [redacted]
Перечень документов.rar
143 Б

Здраствуйте, прошу ознакомиться с претензионно-информационным письмом для Вашего предприятия, с целью конфиденциальной переписки прошу использовать для вложений пароль. В приложение высылаю запрос от ОАО «[redacted]» на ваше имя, пароль **25262**

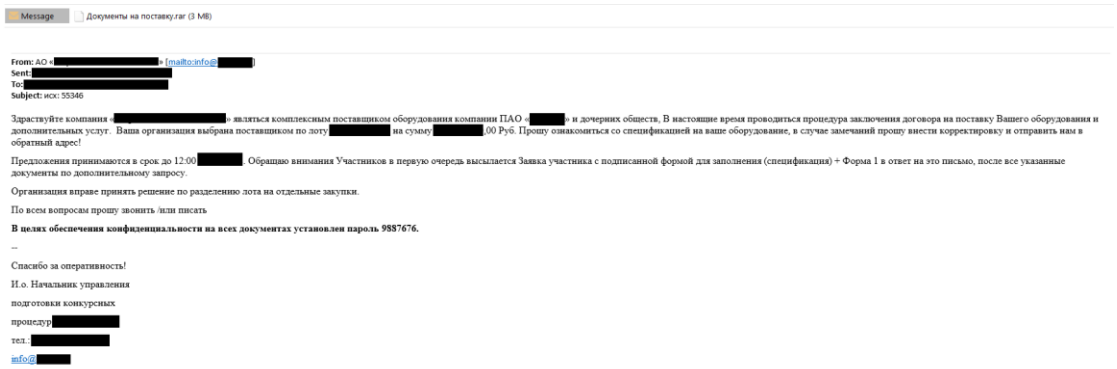
Просьба ответить на запрос

*** 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 ОАО «[redacted]», если иное прямо не указано отправителем.

Phishing email disguised as a claim letter

In the earlier attack series, the attackers used a sender email address with a domain name that was similar to the official website address of the organization on whose behalf their phishing emails were sent. Now they use public email services to send their phishing emails and they use a different technique to mislead message recipients and persuade them to open a malicious attachment: they pretend to be a real business partner or to represent a real subsidiary of the company under attack and ask the recipient to view the documents attached by the deadline specified in the email, explaining the request by the approaching end of a purchase tender, possible penalties or the need to review equipment configuration data as soon as possible.

It should also be emphasized that the phishing emails are individually crafted for each specific company that is attacked. This is demonstrated by the fact that the name of the company under attack is mentioned in the email text, as well as by the documents used by the attackers as attachments (descriptions of the documents are provided below). In some of the cases identified earlier, the attackers also addressed the recipient by his or her full name.



Message Документы на поставку.rar (3 MB)

From: АО «[redacted]» [mailto:info@[redacted]]
Sent: [redacted]
To: [redacted]
Subject: исх: 55346

Здраствуйте компания «[redacted]» являться комплексным поставщиком оборудования компании ПАО «[redacted]» и дочерних обществ, В настоящие время проводиться процедура заключения договора на поставку Вашего оборудования и дополнительных услуг. Ваша организация выбрана поставщиком по лоту [redacted] на сумму [redacted].00 Руб. Прошу ознакомиться со спецификацией на ваше оборудование, в случае замечаний прошу внести корректировку и отправить нам в обратный адрес!

Предложения принимаются в срок до 12:00 [redacted]. Обращаю внимания Участников в первую очередь высылается Заявка участника с подписанной формой для заполнения (спецификация) + Форма 1 в ответ на это письмо, после все указанные документы по дополнительному запросу.

Организация вправе принять решение по разделению лота на отдельные закупки.

По всем вопросам прошу звонить /или писать

В целях обеспечения конфиденциальности на всех документах установлен пароль 9887676.

--

Спасибо за оперативность!

И.о. Начальник управления

подготовки конкурсных

процедур[redacted]

тел.: [redacted]

info@[redacted]

Phishing email sent on behalf of a contractor

Attachments used in phishing emails are password-protected archives, with the password provided in the message body. The attackers explain this method of sending information by referring to confidentiality considerations in the message body, but in reality password protection prevents files stored in the archive from being scanned with antivirus tools.

Malware Features

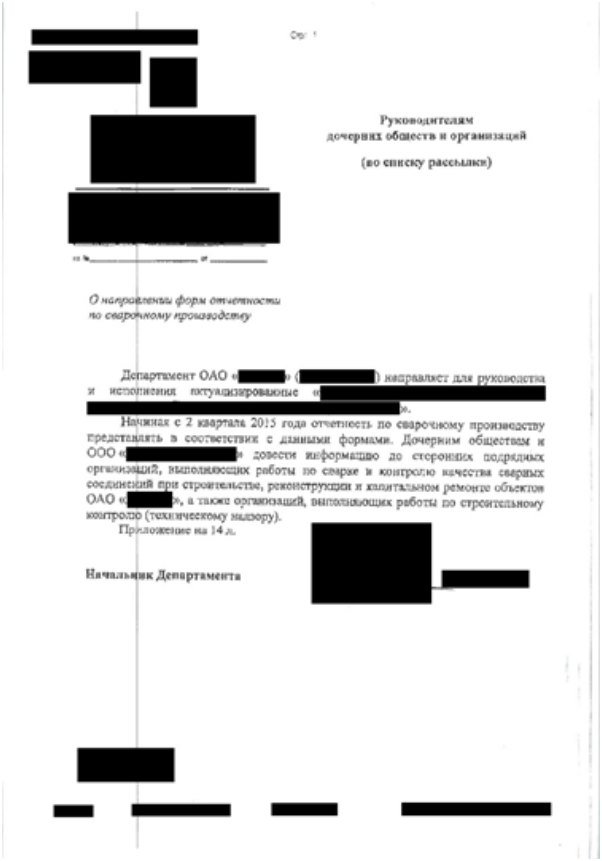
The archive attached to a phishing email contains several malicious obfuscated JS scripts that have an identical functionality but slightly different structure due to different code obfuscation techniques being used. The script names are usually disguised as document names.

If a user runs one of these scripts, two files are unpacked and opened: a malicious program detected as HEUR:Backdoor.Win32.Generic, and a legitimate PDF file. Some JS script variants found in phishing emails download these files from a remote server rather than extracting them from the script's body.

In earlier attacks, to ensure that the user didn't have questions regarding the absence of the documents mentioned in the message body and to distract the user while installing the malware, the attackers opened a damaged PDF document or image or launched a legitimate software installer.

Image opened by the malware in earlier attacks

In their later attacks, the threat actor began to use actual documents related to the attacked organization's area of work. A document can look like one created by a business partner or even the attacked organization itself. Specifically, documents used in attacks include scan copies of memos, letters to subsidiaries and contractors, as well as procurement documentation forms that were apparently stolen earlier.



Руководителям
дочерних обществ и организаций

(по списку рассылки)

О направлении форм отчетности по сварочному производству

Департамент ОАО «[redacted]» ([redacted]) направляет для руководства и использования актуализированные «[redacted]».

Начиная с 2 квартала 2015 года отчетность по сварочному производству представлять в соответствии с данными формами. Дочерним обществам и ООО «[redacted]» довести информацию до сторонних подрядных организаций, выполняющих работы по сварке и контролю качества сварных соединений при строительстве, реконструкции и капитальном ремонте объектов ОАО «[redacted]», а также организаций, выполняющих работы по строительному контролю (техническому надзору).

Приложение на 14 л.

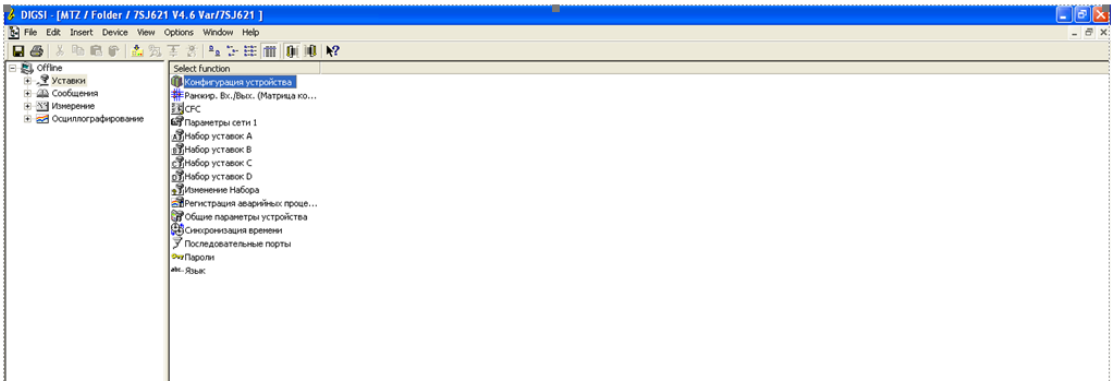
Начальник Департамента [redacted]

[redacted]

PDF document containing instructions for subsidiaries, used by the attackers

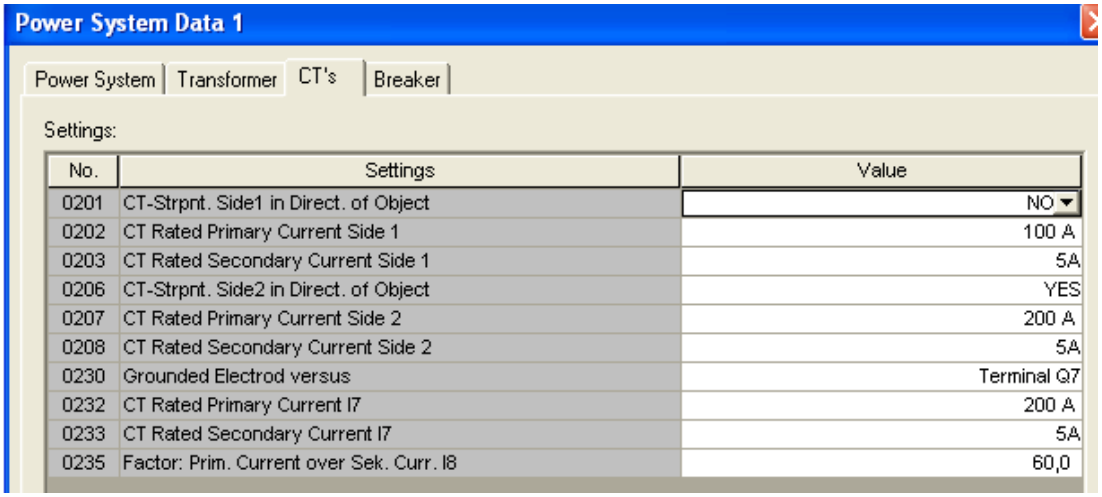
A fact of particular interest is that in some cases, the attackers used documents containing industrial equipment configuration data and other information related to the industrial process.

Specifically, screenshots from the DIGSI application have been used. The application is designed to configure relay systems manufactured by Siemens.

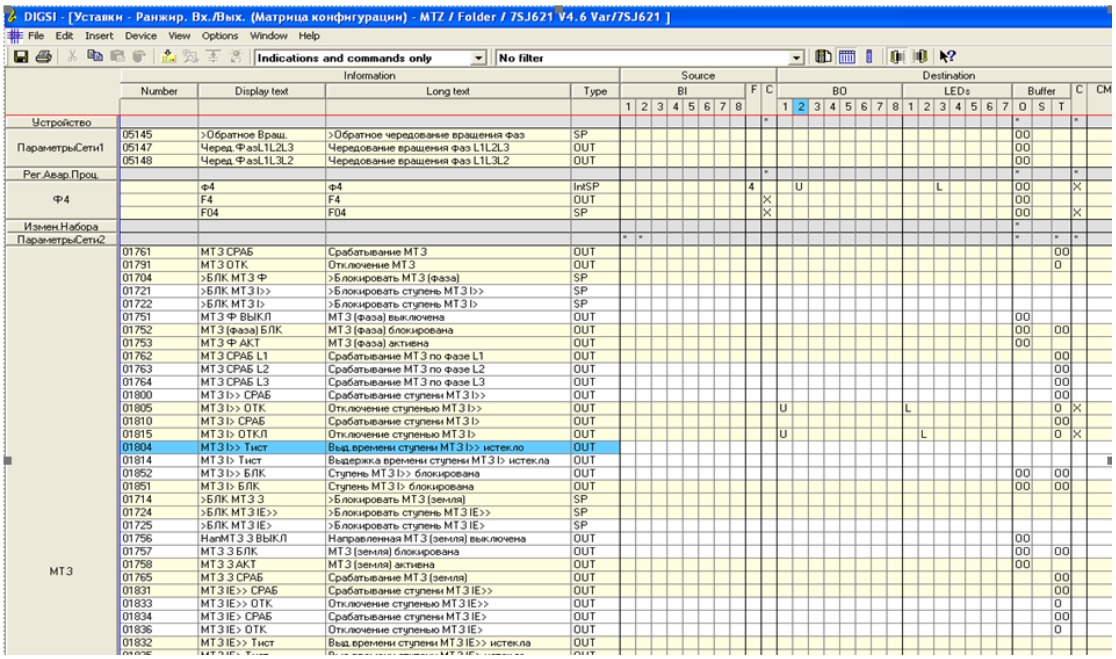


DIGSI software screenshot 1

DIGSI is used by electric power facilities, such as substations, to configure their relay protection systems.

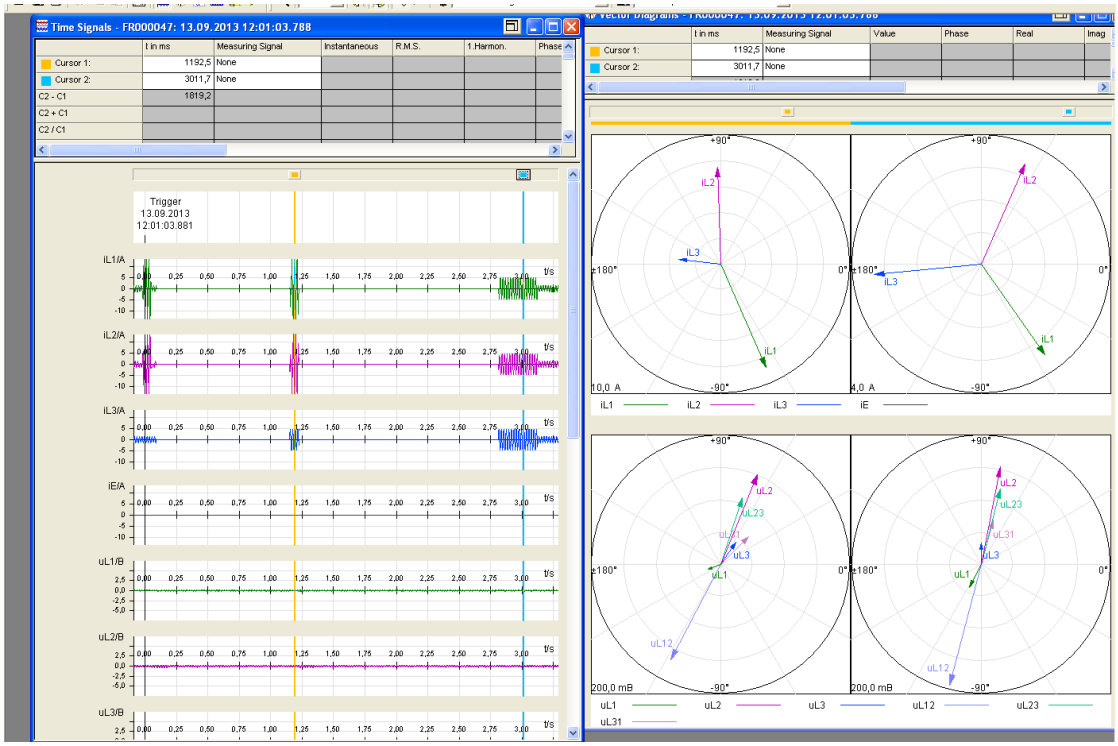


DIGSI software screenshot 2



Screenshot of a relay system's configuration matrix. List of setpoints

We also found screenshots with transformer oscillograms in documents used by the attackers:



Vector diagrams with oscillograms

It is worth noting that the last screenshot shows oscillograms for a system at the moment of an accident.

Phishing emails with such screenshots do not call for the settings shown in attached documents to be implemented. It is most likely that the attackers use documents with the above screenshots to distract the personnel while the malware is being installed. Since the data mentioned above can provide a relay protection expert with information on standard settings used at the facility, the fact that the attackers have such screenshots at their disposal is cause for concern.

The JS script then launches the malware, which installs a version of TeamViewer, a remote administration tool (RAT), modified by the attackers. As in earlier attacks, the attackers use a malicious DLL library to hide the graphical user interface in order to control the infected system without the user's knowledge.

If additional information needs to be collected, the attackers download an additional set of malware selected specifically for each victim. This can be spyware designed to collect credentials for a variety of programs and services, including email clients, browsers, SSH/FTP/Telnet clients, as well as recording keypresses and making screenshots. In some cases, the Mimikatz utility is used to collect account credentials for Windows accounts entered on the compromised system. The use of Mimikatz poses a particular danger, because it can provide the attackers with access to a large number of systems on the enterprise's network.

In most cases, the attackers disguise malware components as Windows components to hide traces of malicious activity on the system.

Infrastructure

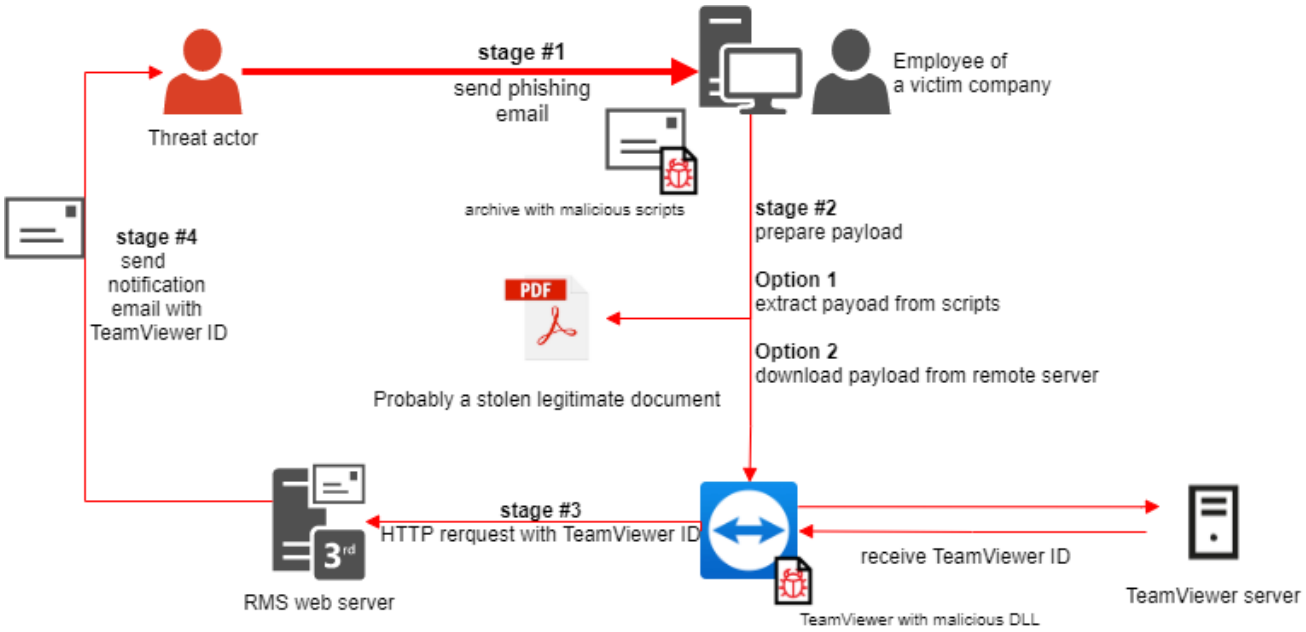
While analyzing the new series of attacks, we noticed two ways in which the infrastructure is organized differently from that used in earlier attacks.

First, the attackers use resources disguised as websites of existing Russian-speaking companies to store files downloaded by malicious JS scripts at the system infection stage.

The second and more important difference is that the attackers no longer use a malware command-and-control server in their communication with infected systems.

The main reason for having a malware command-and-control server in this type of attack was the need to get the infected machine's ID in the TeamViewer system. The attackers already had any other information they needed (the password required to connect was provided in a special configuration file). In the new series of attacks, the attackers sent the infected machine's TeamViewer ID using the legitimate infrastructure of the RMS remote administration system.

This was possible because the RMS remote administration infrastructure has a dedicated web service designed to notify the administrator that an RMS distribution package has been installed on a remote system. To send the notification, the RMS server generates an email message that contains the machine's ID in the RMS system in the message body. For the message to be generated, it is sufficient for the RMS client to send an HTTP POST request to the dedicated web page, providing the following data: product name, ID of the language pack used in the system, user name, computer name, email address to which the notification should be delivered, and the machine's ID in the RMS system assigned after installing the program.



Attack kill chain

The underlying mechanism of the web service contained a vulnerability: it did not use any kind of authorization procedure. The malicious DLL responsible for hiding the TeamViewer graphic interface included code for sending the request described above to the RMS server. However, it sent the machine's ID in the TeamViewer system instead of its ID in the RMS system.

The ID length in the TeamViewer system is different from the ID length in the RMS system; however, since there is no verification of the contents of fields sent to the server in the HTTP POST request, a notification message with information on a newly infected machine was successfully delivered to the attacker's address.

Kaspersky ICS CERT has notified RMS developers that their infrastructure is being used for criminal purposes, providing them with all the technical details needed to close the vulnerability. To date, the vulnerability has not been closed by the developers, but a workaround, filtration based on an address whitelist, has been implemented.

In other words, the functionality still works, but notification emails are only sent to email addresses included in a special list of customers 'verified' by RMS developers.

For technical details about this vulnerability please contact: ics-cert@kaspersky.com

Victims

As mentioned above, the vast majority of attacked systems are industrial enterprises in Russia representing various sectors of the economy. We identified attacks on companies from the following industries:

- Manufacturing
- Oil and gas
- Metal industry
- Engineering
- Energy
- Construction
- Mining
- Logistics

Consequently, this is not a case of an attack narrowly targeting one specific industry; however, since most legitimate documents used in the attacks are from the energy sector, it can be assumed that the attackers have a particular interest in the sector.

Attribution

We are convinced that a Russian-speaking group is behind these attacks.

The main arguments in favor of this theory were offered in our previous report, "Attacks on industrial enterprises using RMS and TeamViewer".

Note also that the code used to send requests to the RMS server, which was identified in the process of analyzing the new version of the malicious DLL, contains a language ID for the Russian localization of the operating system.

According to available information, the main objective of the criminals is to steal money from victim organizations' accounts. This means that the attackers must have a good understanding of the financial workflow, which differs in some of its aspects from country to country, and support the appropriate infrastructure for cash withdrawal.

The group does not use any sophisticated tactics or technologies, but it carefully prepares each attack and expertly uses social engineering techniques, as well as technologies that are already known from attacks staged by other criminal groups.

We believe that the group includes people responsible for the technical aspect of infecting victims' systems, as well as people responsible for financial operations, i.e., for stealing money from the group's victims.

Conclusions

The threat actor continues to attack industrial enterprises successfully using relatively simple techniques, but its methods are evolving. To persuade users of the legitimacy of phishing emails, criminals have begun to use documents that were apparently stolen during earlier attacks. It is worth noting that some of the documents used for this purpose contain information on industrial equipment settings and industrial process parameters. This is one more reason to believe that these attacks specifically target industrial enterprises.

The main technical change in the attacks is that the attackers have discarded the most vulnerable stage in data collection and transmission – that is, malware command-and-control servers, which can be disconnected by the hosting provider or blocked by information security systems. Instead, new system infection notifications are delivered via the legitimate web interface of the RMS remote administration utility's cloud infrastructure. Resources disguised as legitimate websites of existing organizations are used to store malware samples.

The attackers have full control of an infected system from the moment it becomes infected. Stealing money from the organization's accounts remains their main objective. When the attackers connect to a victim's computer, they look for financial and accounting software (1C accounting software, bank-client, etc.). In addition, they find and analyze procurement-related accounting documents and peruse the email correspondence of the enterprise's employees. After that, the attackers look for various ways in which they can commit financial fraud. We believe that the criminals are able to substitute the bank details used to pay invoices.

Clearly, the attackers' remote access to infected systems also poses other threats, such as the organization's sensitive data being leaked, systems being put out of operation, etc. As the latest events have shown, the attackers use documents that were probably stolen from organizations to carry out subsequent attacks, including attacks on victim companies' partners.

If you have encountered an attack of this kind, you can report it to us through a form on our website.

Recommendations

- Train employees at enterprises in using email securely and, specifically, in identifying phishing messages
- Restrict the ability of programs to gain SeDebugPrivilege privileges (wherever possible)
- Install antivirus software with support for centrally managing the security policy on all systems; keep the antivirus databases and program modules of security solutions up to date
- Use accounts with domain administrator privileges only when necessary. After using such accounts, restart the system on which the authentication was performed
- Implement a password policy with password strength and regular password change requirements
- If it is suspected that some systems are infected: remove all third-party remote administration utilities, scan these systems with antivirus software and force a change of passwords for all accounts that have been used to log on to compromised systems
- Monitor network connections for any traces of remote administration utilities installed without proper authorization. Make a special emphasis on the use of RMS and TeamViewer utilities
- Use network activity filtration systems to block connections to servers and IP addresses listed in Appendix I – Indicators of Compromise
- Never use obsolete versions of the TeamViewer utility (versions 6.0 and earlier). To discover any instances of obsolete versions of TeamViewer being used, the YARA rule provided in Appendix I – Indicators of Compromise can be used
- It should be noted that, since the attack uses legitimate remote administration software, that software can remain on the victim's computer and continue operating even when the malicious downloader has been removed. If remote administration software has been identified at the stage of scanning corporate systems, it should be determined in each case whether it was installed legitimately

For more information please contact: ics-cert@kaspersky.com

Appendix I – Indicators of Compromise

File Hashes (malicious documents, malware, emails etc.)

- 386a1594a0add346b8fbbebcf1547e77
- 203e341cf850d7a05e44fafc628aeaf1
- 3b79aacdc33593e8c8f560e4ab1c02c6
- ea1440202beb02cbb49b5bef1ec013c0
- 1091941264757dc7e3da0a086f69e4bb
- 72f206e3a281248a3d5ca0b2c5208f5f
- da4dff233ffbac362fee3ae08c4efa53
- d768a65335e6ca715ab5ceb487f6862f
- 9219e22809a1dff78aac5fff7c80933c
- 86e14db0bcf5654a01c1b000d75b0324

File Names

- Акт.js
- Запрос 17782-09-1.js
- Перечень документов.js
- спецификация на оборудование xls.js
- tv.dll
- tv.ini

Some malware modules installed on the system have randomly generated names that follow a specific format. The following regular expression can be used to search for such files:

```
%TEMP%\\[a-z]{2,3}[0-9]{2}.exe
```

These files are saved in the temporary file directory (%TEMP%); the first part of the file name consists of two or three Roman characters; the second is a two-digit number followed by the extension .exe

Domains and IPs

- timkasprot.temp.swtest[.]ru (RemoteAdmin.Win32.RemoteManipulator.vpj)
- 77.222.56[.]169 (RemoteAdmin.Win32.RemoteManipulator.vpj)
- z-wavehome[.]ru (RemoteAdmin.Win32.RemoteManipulator.vpj)
- dncars[.]ru (RemoteAdmin.Win32.RemoteManipulator.vpj)

Yara Rules

```
rule TeamViewer_ver6_and_lower {
meta:
    description = "Rule to detect TeamViewer ver 6.0 and lower"
    hash = "4f926252e22afa85e5da7f83158db20f"
    hash = "8191265c6423773d0e60c88f6ecc0e38"
    version = "1.1"
```

```
condition:
                uint16(0) == 0x5A4D and
                pe.version_info["CompanyName"] contains "TeamViewer" and
                (pe.version_info["ProductVersion"] contains "6.0" or
                pe.version_info["ProductVersion"] contains "5.1" or
                pe.version_info["ProductVersion"] contains "5.0" or
                pe.version_info["ProductVersion"] contains "4.1" or
                pe.version_info["ProductVersion"] contains "4.0" or
                pe.version_info["ProductVersion"] contains "3.6" or
                pe.version_info["ProductVersion"] contains "3.5" or
                pe.version_info["ProductVersion"] contains "3.4" or
                pe.version_info["ProductVersion"] contains "3.3" or
                pe.version_info["ProductVersion"] contains "3.2" or
                pe.version_info["ProductVersion"] contains "3.1" or
                pe.version_info["ProductVersion"] contains "3.0")
}
```

The attackers use outdated versions of the TeamViewer client that contain a vulnerability enabling them to hide the utility's graphic interface. This YARA rule can be used to determine whether there are outdated versions of the TeamViewer software installed on the system. Checking whether any such software found was installed legitimately is a first-priority task.

If instances of outdated versions of the TeamViewer client being used legitimately are identified, it is recommended that the software in question be updated to the latest version.

Registry keys

- Key:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\rundll32
Value:
rundll32.exe shell32.dll,ShellExec_RunDLL
"%AppData%\Roaming\TeamViewer\5\TeamViewer.exe"
- Key:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\CCFTray
Value:
rundll32.exe shell32.dll,ShellExec_RunDLL "%temp%\TeamViewer.exe"

Threat actors' email addresses

- timkas@protonmail.com
- smoollsrv@gmail.com
- nataly@z-wavehome.ru
- info@dncars.ru

Appendix II – MITRE ATT&CK Mapping

Tactic	Technique/Subtechnique	Description
Initial Access	T1566.001	**Phishing: Spearphishing Attachment** The attackers use phishing emails with archives containing malicious scripts
Execution	T1204.002	**User Execution: Malicious File** Malicious software is executed when the user opens the file
	T1059.007	**Command and Scripting Interpreter: JavaScript/Jscript** Used to execute malicious PE and open bait PDF files
Persistence	T1547.001	**Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder** The malware creates a registry value to run automatically after system restart
Defense Evasion	T1027.002	**Obfuscated Files or Information: Software Packing** To make analysis more difficult, files of the malware are packed and its code is obfuscated
	T1564.001	**Hide Artifacts: Hidden Files and Directories** The attributes “hidden” and “system” are assigned to malware files
	T1574.001	**Hijack Execution Flow: DLL Search Order Hijacking** To hide the GUI of the TeamViewer remote administration utility, a malicious program is loaded into the process instead of a system library
	T1036.005	**Masquerading: Match Legitimate Name or Location** In most cases, attackers disguise malware components as Windows operating system components to hide the traces of malicious activity in the system

Credential Access	T1003.001	**OS Credential Dumping: LSASS Memory** The attackers use the Mimikatz utility in cases where they need authentication credentials to infect other systems in an organization
	T1056.001	**Input Capture: Keylogging** In some cases, malware (class: Spyware) designed to collect logins and passwords for various different programs and services, record keypresses and capture screenshots is downloaded to an infected system
Discovery	T1057	**Process Discovery** The malware collects information on antivirus software running on the system
	T1018	**Remote System Discovery** The attackers explore the organization's other systems to which they can gain access over the network
	T1518	**Software Discovery** The attackers take notes on which software associated with financial operations is installed on an infected system
Lateral Movement	T1021.001	**Remote Services: Remote Desktop Protocol** RDP connections with account credentials obtained earlier using the Mimikatz utility are used for lateral movement
Collection	T1005	**Data from Local System** The attackers analyze documents found on infected systems; these documents can be used in subsequent attacks
	T1114.001	**Email Collection: Local Email Collection** The attackers analyze the business correspondence of the organization under attack in order to use it for subsequent attacks on the victim's business partners
	T1056.001, T1113	**Input Capture: Keylogging and Screen Capture** In some cases, malware (class: Spyware) designed to collect logins and passwords for various different programs and services, record keypresses and capture screenshots is downloaded to an infected system

Command And Control	T1071.001	**Application Layer Protocol: Web Protocols** To send the TeamViewer ID, an HTTP POST request is sent to the RMS server
	T1071.003	**Application Layer Protocol: Mail Protocols** The RMS server sends an email to an address controlled by the attackers. The email contains the infected machine's TeamViewer ID
	T1219	**Remote Access Software** The attackers use the TeamViewer remote administration utility to connect to the infected system
Exfiltration	T1020	**Automated Exfiltration** The attackers use malware to receive information collected on the infected system
Impact	T1565.001	**Data Manipulation: Stored Data Manipulation** Substitution of bank details in payment forms

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

Kaspersky ICS CERT ics-cert@kaspersky.com