Study of a targeted attack on a Russian enterprise in the mechanical-engineering sector

Doctor Web

Back to the news list

Download PDF

March 11, 2024

Introduction

In October 2023, Doctor Web was contacted by a Russian mechanical-engineering enterprise that suspected malware was on one of its computers. Our specialists investigated this incident and determined that the affected company had encountered a targeted attack. During this attack, malicious actors had sent phishing emails with an attachment containing the malicious program responsible for the initial system infection and installing other malicious instruments in the system.

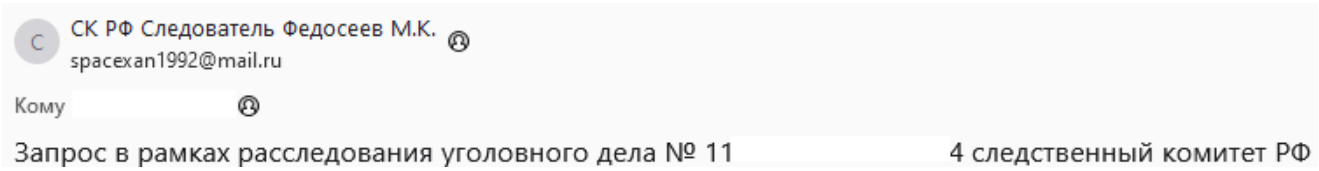
The goal of this attack was to collect sensitive information about the employees as well as to gather data about the company's infrastructure and its internal network. In addition, we detected that data had been uploaded from the infected computer; this included files stored on the computer and screenshots taken while the malware was in operation.

General information about the attack and the tools involved

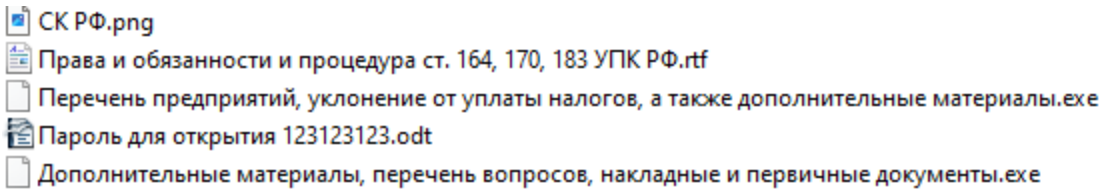
In early October 2023, malicious actors sent several phishing emails to the email address of the affected company. The subject of the messages was related to an "investigation" of certain criminal cases of tax evasion. These emails were supposedly sent on behalf of an investigator with the Investigative Committee of the Russian Federation and contained two attachments. The first one was a password-protected ZIP archive. It concealed a malicious program which, when executed, initiated the system infection process. The second attachment, a PDF document, was not malicious. It contained a phishing text stating that all the information about the "criminal case" was in the archive and encouraged the user to open the malicious program from it.

The very first such phishing message contained the ZIP archive Требование 19098 След ком РФ от 02.10.23 ПАРОЛЬ - 123123123.zip. For its part, the trojan app in it was concealed in the file Перечень юридических лиц и предприятий, уклонение от уплаты налогов, требования и дополнительные.exe.

One of the last messages sent is the one shown below:



The phishing PDF document Требование следователя, уклонение от уплаты налогов (запрос в рамках УД).pdf and the ZIP archive Требование 19221 СК РФ от 11.10.2023 ПАРОЛЬ - 123123123.zip were attached to it. The archive contained the following items:



Similar to in their earlier messages, the attackers indicated the password for extracting files from the archive, both in its name and in the name of the document Пароль для открытия 123123123.odt. This document itself, as well as the files Права и обязанности и процедура ст. 164, 170, 183 УПК РФ.pdf and the СК РФ.png, were not malicious.

This archive contained two copies of the trojan application: Перечень предприятий, уклонение от уплаты налогов, а также дополнительные материалы.exe and Дополнительные материалы, перечень вопросов, накладные и первичные документы.exe.

In all cases, **Trojan.Siggen21.39882** was the malicious program distributed by attackers. This malware, also known as WhiteSnake Stealer, is sold on the DarkNet and is used to steal account data from a variety of software and to hijack other data. Moreover, it can download and install other malicious apps on attacked computers. In the targeted attack in question, it was assigned the role of initiating the first infection stage. After receiving the corresponding commands, this trojan collected and transmitted to the attackers information about configuring Wi-Fi network profiles in the infected system as well as the passwords for accessing them. It then launched an SSH proxy server and installed the second stage in the system.

The second stage, and simultaneously the threat actors' main instrument, was the **JS.BackDoor.60** malicious backdoor program. It was the tool through which the main interaction between the attackers and the infected system took place. One of the backdoor's features is that it uses its own JavaScript framework. The trojan consists of the primary obfuscated body and additional modules that, owing to the specifics of the malware's architecture, are simultaneously a trojan component and the tasks that it executes via the JavaScript functions they share. The trojan receives new tasks from its C&C server, and *de facto* they turn it into a multi-component threat with expandable functionality, which allows it to be used as a powerful cyberespionage instrument.

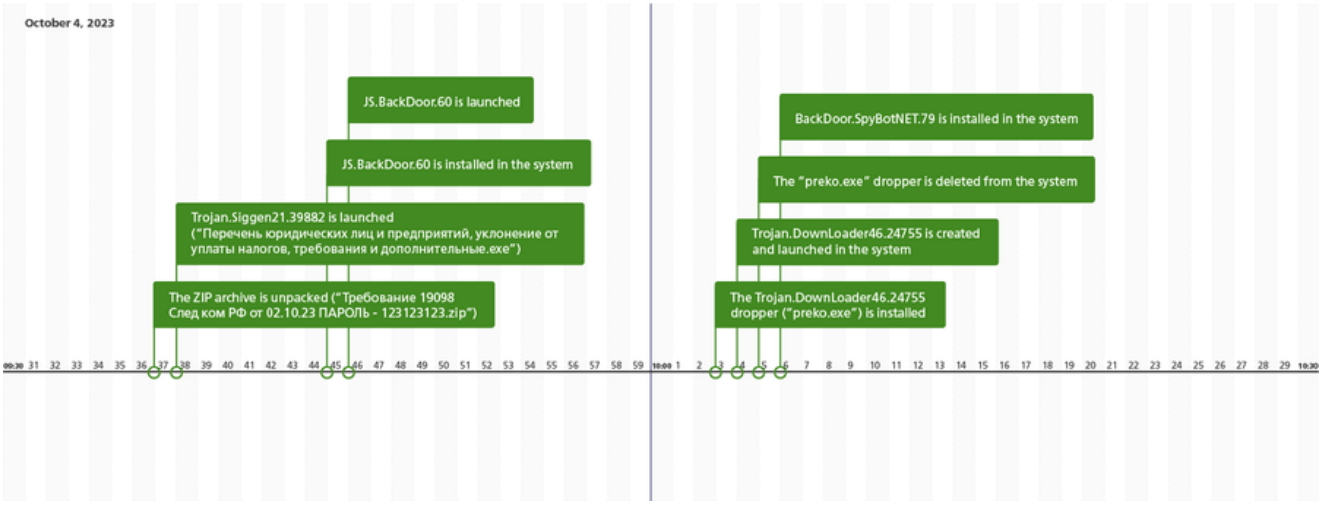
The mechanism that **JS.BackDoor.60** used to provide itself with the autorun ability is also of interest. Along with employing a traditional method—adding necessary changes to the Windows registry—the trojan modified the shortcut files (.lnk) in a specific way. For this, it verified the contents of a number of system directories, including the Desktop and taskbar directories. For all the shortcut files it found in them (excluding Explorer.lnk or Проводник.lnk), it assigned the program wscript.exe as a target app for launching. At the same time, it added special arguments for its execution, one of which was the Alternate Data Stream (or ADS), in which the backdoor body was written. As a result of the changes, the modified shortcuts launched the **JS.BackDoor.60** first, and only after that—the initial programs.

Throughout the whole attack, malicious actors were actively sending various commands to the backdoor. With its help, they stole the contents of dozens of directories from the infected computer, which contained both personal and corporate data. Moreover, we found evidence that the trojan had created screenshots.

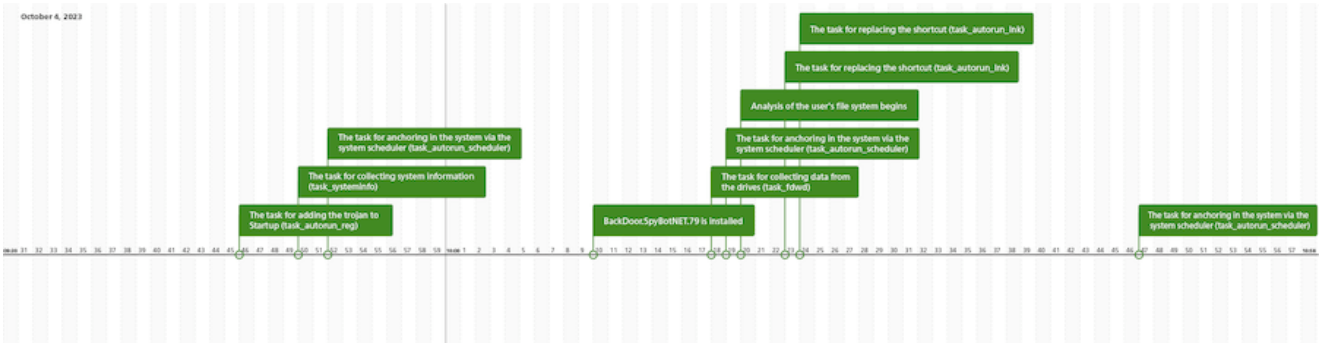
The additional spying instrument in this attack was the BackDoor.SpyBotNET.79 malicious program, which was used for audio surveillance and for recording conversations through the microphone attached to the infected computer. This trojan recorded audio only when it detected a certain sound intensity—in particular, one characteristic of a voice.

At the same time, the attackers also tried to infect the system with the Trojan.DownLoader46.24755 downloader trojan, but failed due to an error that occurred.

The chronology of the attack is shown in the next illustration:



The chronology of the tasks received by **JS.BackDoor.60**:



The analysis conducted by our specialists did not clearly indicate the involvement of any of the previously known APT groups in this attack.

For detailed technical descriptions of the malicious programs detected, please refer to the PDF version of the study or visit the Doctor Web virus library.

More details on **Trojan.Siggen21.39882**

More details on **JS.BackDoor.60**

More details on **BackDoor.SpyBotNET.79**

More details on **Trojan.DownLoader46.24755**

Conclusion

The use of malicious instruments, which are available as a commercial service (MaaS — Malware as a Service), such as **Trojan.Siggen21.39882**, allows even relatively inexperienced malicious actors to carry out quite sensitive attacks against both businesses and government agencies. For its part, social engineering still poses a serious threat. This is a relatively simple but effective way to bypass a built-in protection layer, and it can be used

by both experienced and novice cybercriminals. In this regard, it is especially important to ensure that the entire infrastructure of an enterprise is protected, including its workstations and email gateways. Moreover, it is recommended to conduct periodic training sessions for employees on the topic of information security and to familiarize them with current digital threats. All these measures will help reduce the likelihood of cyber incidents and minimize the damage from attacks.

Indicators of compromise

What is the benefit of having an account?

Tell us what you think

To ask Doctor Web's site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

Other comments