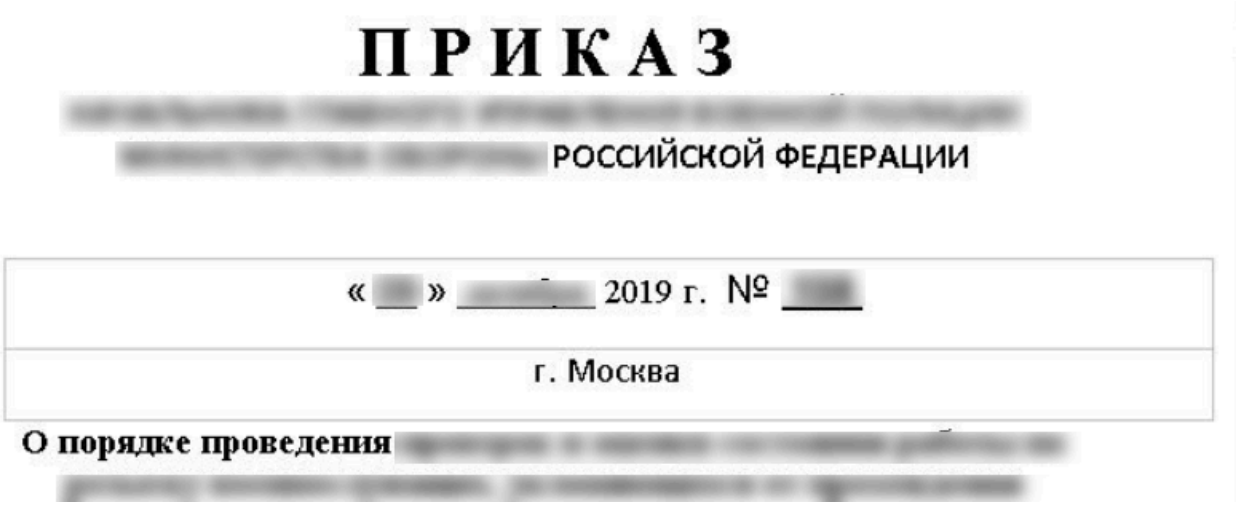
Core Werewolf targets the defense industry and critical infrastructure

Published: 2026-03-12 · Archived: 2026-04-05 12:52:34 UTC

The file used in the first attack that we uncovered was uploaded to VirusTotal on August 6, 2021. Curiously enough, the malicious files were always disguised as Microsoft Word or PDF documents, even though these were executables in self-extracting archives. For example, `Прил._7_критерии_оценки_...ГУВП.docx.exe` (Appendix 7. Assessment criteria). Hence, the content of the documents did not raise any concern with the user. However, opening the file triggered the background installation of UltraVNC. This enabled the attackers to gain complete control over compromised devices.

The file discovered first contained an order of a defense organization (fig. 1).



ПРИКАЗ

[redacted] РОССИЙСКОЙ ФЕДЕРАЦИИ

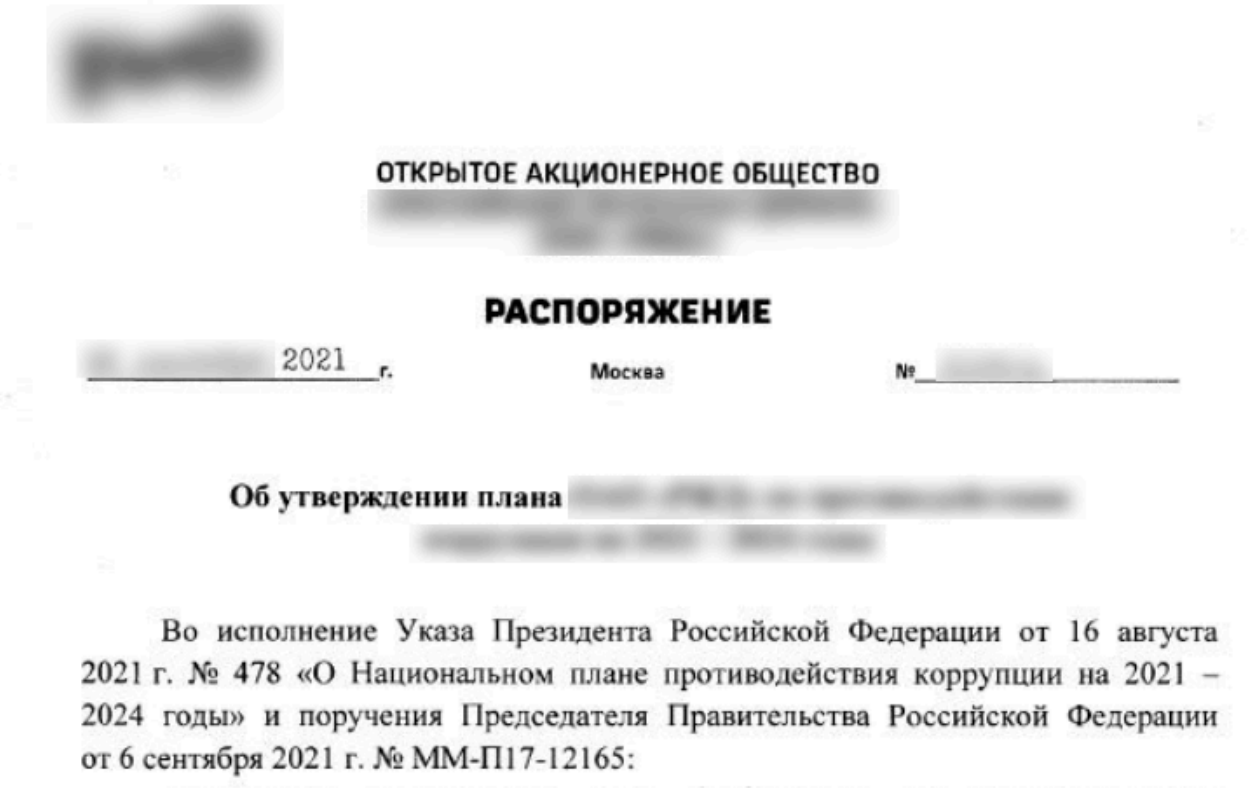
«[redacted]» [redacted] 2019 г. № [redacted]

г. Москва

О порядке проведения [redacted]

Fig. 1. Excerpt of the document used by the attackers

The file detected next was posted on December 16, 2021. The phishing document included an internal order by one of the largest joint-stock companies in Russia (fig. 2).



ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

РАСПОРЯЖЕНИЕ

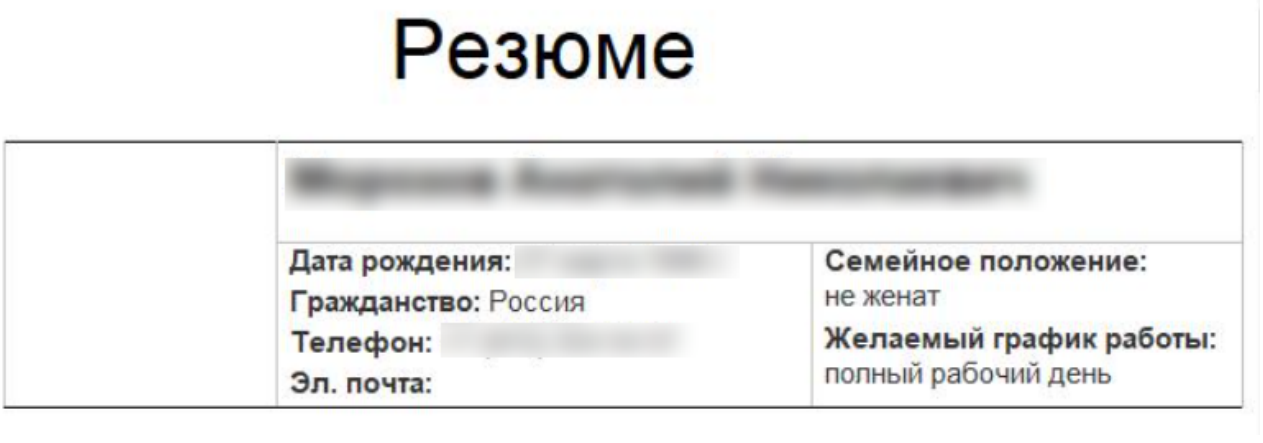
2021 г. Москва №

Об утверждении плана

Во исполнение Указа Президента Российской Федерации от 16 августа 2021 г. № 478 «О Национальном плане противодействия коррупции на 2021 – 2024 годы» и поручения Председателя Правительства Российской Федерации от 6 сентября 2021 г. № ММ-П17-12165:

Fig. 2. Excerpt of the document used by the attackers

It had been a while before another attack followed. The file was spotted on April 12, 2022 and contained a resume (fig. 3).



Резюме

Дата рождения:
Гражданство: Россия
Телефон:
Эл. почта:

Семейное положение:
не женат
Желаемый график работы:
полный рабочий день

Fig. 3. Excerpt of the document used by the attackers

The file from the next attack was uploaded on April 18, 2022 and targeted the employees of some defense organizations (fig. 4).

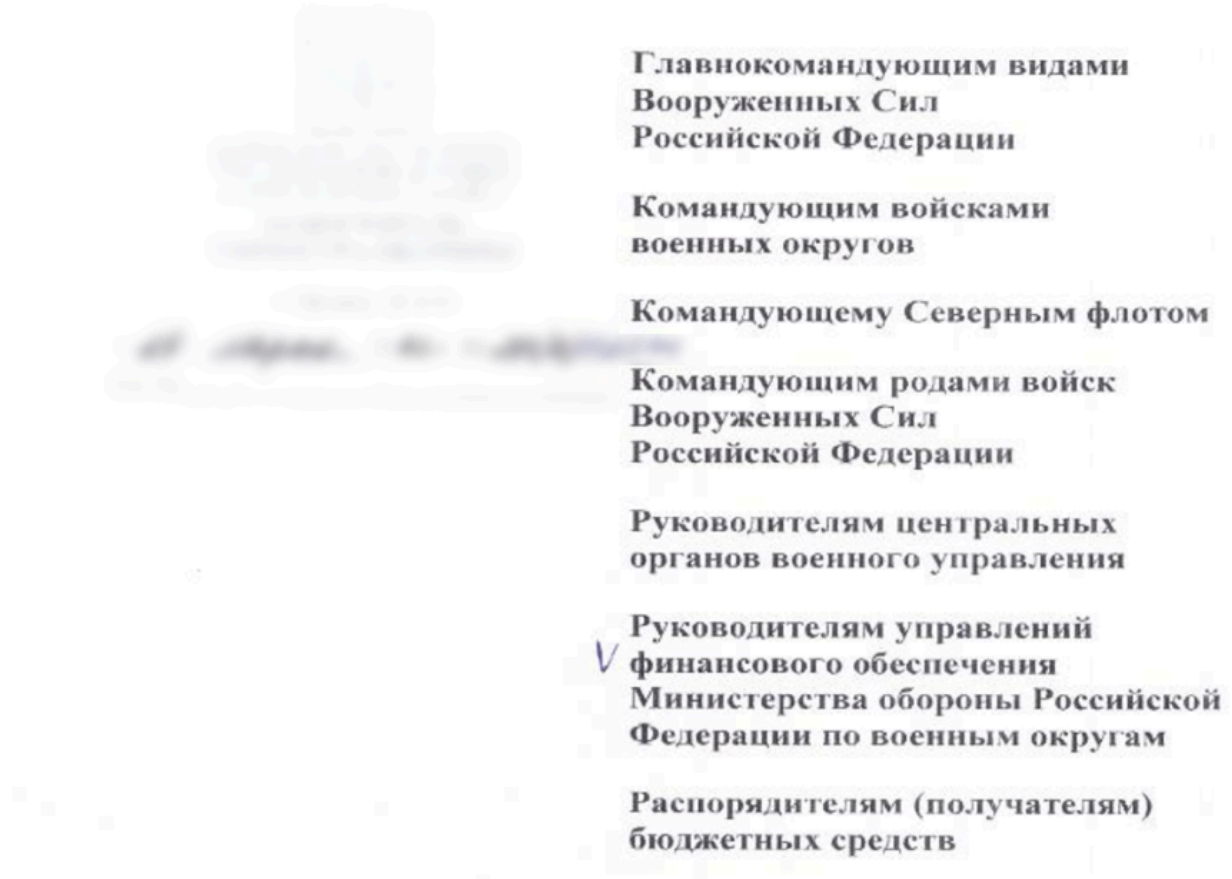
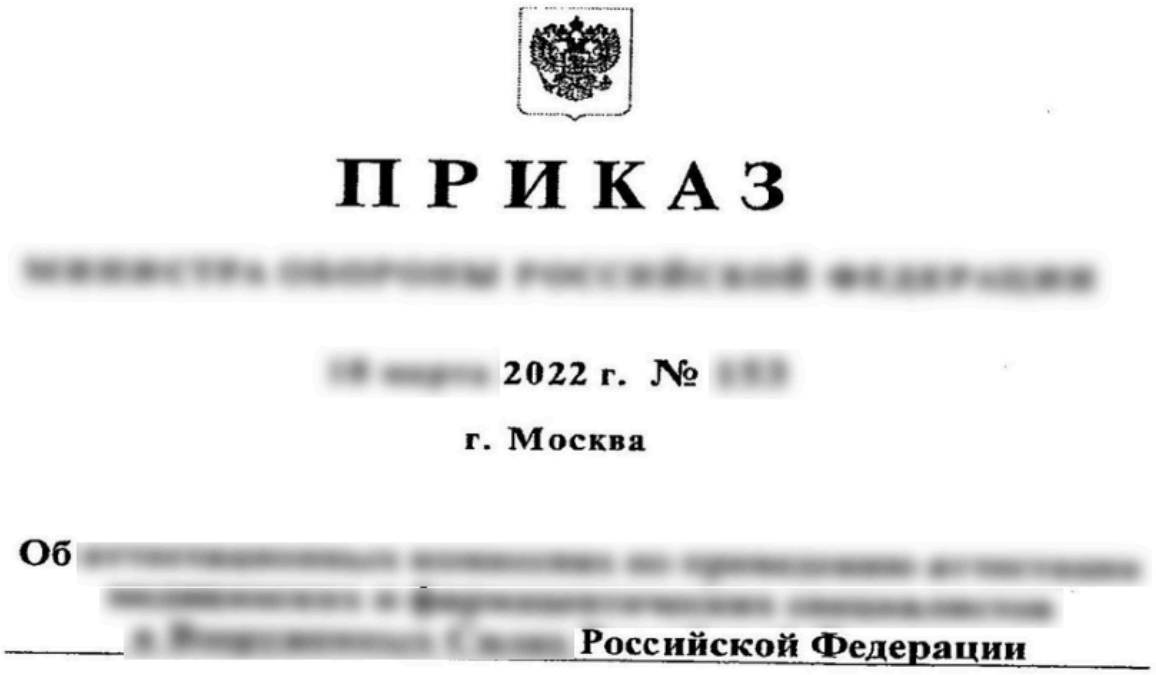


Fig. 4. Excerpt of the document used by the attackers

Another file was posted on April 27, 2022 and was dedicated to the military discharge (fig. 5).

Fig. 5. Excerpt of the document used by the attackers

In their new attack, with the respective file uploaded on May 8, 2022, the criminals again attached an order of a defense organization (fig. 6).



ПРИКАЗ

[redacted]

[redacted] 2022 г. № [redacted]

г. Москва

Об [redacted] Российской Федерации

Fig. 6. Excerpt of the document used by the attackers

On May 12, 2022, a new file was published on VirusTotal. This time, the attackers sent methodological recommendations of another defense organization (fig. 7).

УТВЕРЖДАЮ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

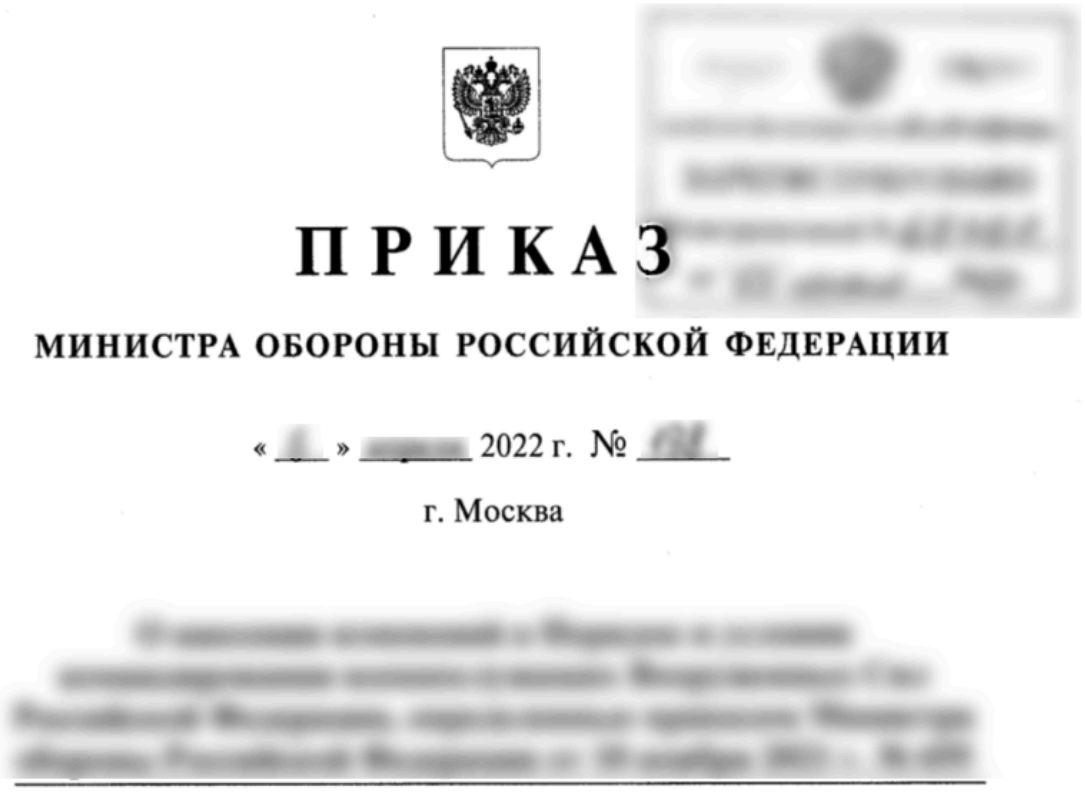
по порядку

в 2022 году

1. Общие положения

Fig. 7. Excerpt of the document used by the attackers

The file uploaded on May 27, 2022 again contained an order (fig. 8).



ПРИКАЗ

МИНИСТРА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

« » 2022 г. №

г. Москва

Fig. 8. Excerpt of the document used by the attackers

The summer attacks started with a file posted on June 13, 2022. Disguised as a decree of the Government of the Russian Federation, the document amended the state regulation of prices for products supplied under the state defense order (fig. 9).

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 21 мая 2022 г. № 935

МОСКВА

О внесении изменений в Положение о государственном регулировании цен на продукцию, поставляемую по государственному оборонному заказу

Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые изменения, которые вносятся в Положение о государственном регулировании цен на продукцию, поставляемую по государственному оборонному заказу, утвержденное

Fig. 9. Excerpt of the document used by the attackers

The next attack, with the file uploaded on June 28, 2022, used some guidelines to victimize the users (fig. 10).


Экз. № 1

Методическое пособие по порядку представления военнослужащих, проходящих военную службу по контракту, к досрочному увольнению с военной службы в связи с невыполнением военнослужащим условий контракта

2022

Fig. 10. Excerpt of the document used by the attackers

July was marked by an attack that leveraged a document issued by the Department of the Federal Service for Technical and Export Control (FSTEK) of Russia for the Northwestern Federal District. It described the measures to reinforce the protection of information infrastructure facilities in Russia.

The file published on VirusTotal on July 20, 2022 contained another administrative document related to the defense sector.

The file uploaded on July 27, 2022 came as a resume, yet of a different person (fig. 11).

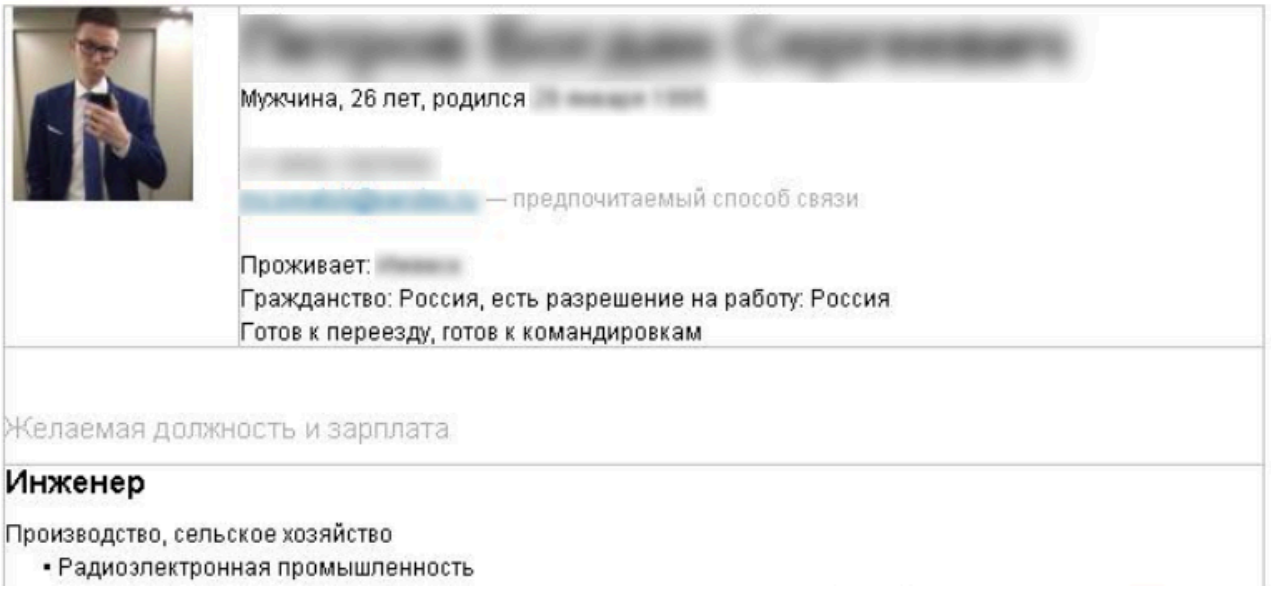


Fig. 11. Excerpt of the document used by the attackers

In August, the criminals once again used an order as a phishing document (fig. 12).

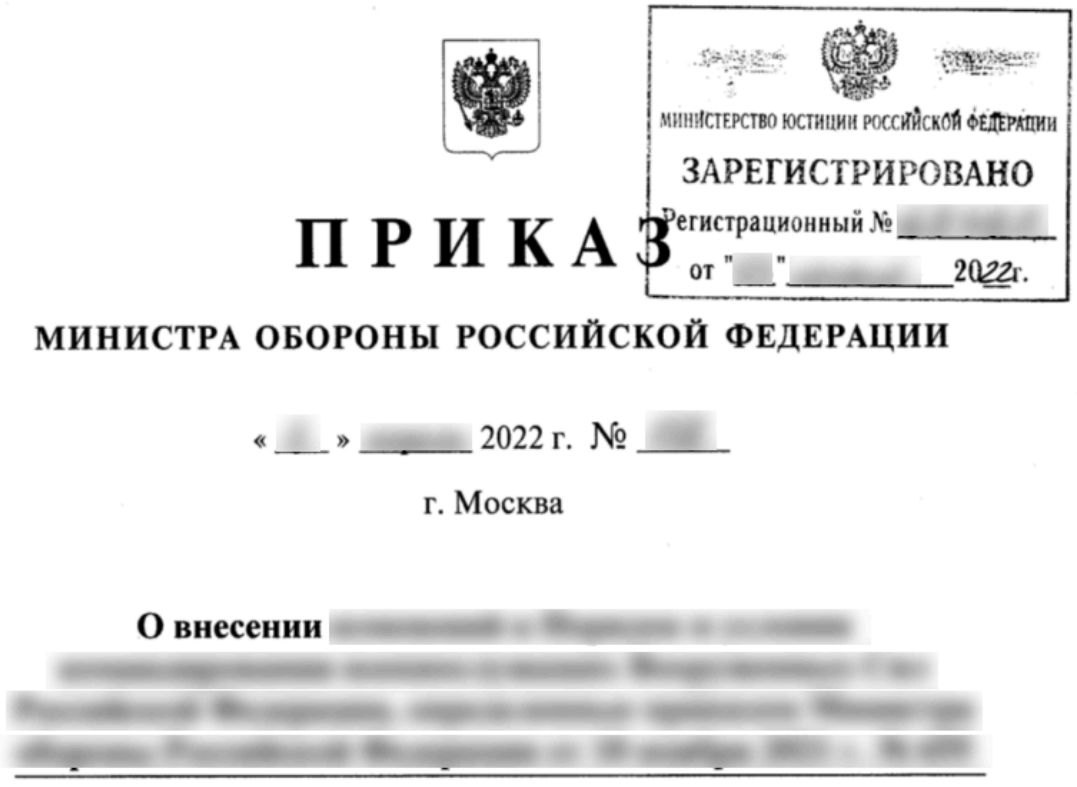


Fig. 12. Excerpt of the document used by the attackers

In September, the attackers went even further and, instead of some regular order, attached a document marked “For official use only.”

The October attack featured yet another decree of the Government of the Russian Federation. The document introduced amendments to the national program on the development of the nuclear power industry (fig. 13).

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 28 марта 2017 г. № 344-11

МОСКВА

О внесении изменений в государственную программу Российской Федерации "Развитие атомного энергопромышленного комплекса"

Правительство Российской Федерации **п о с т а н о в л я е т:**

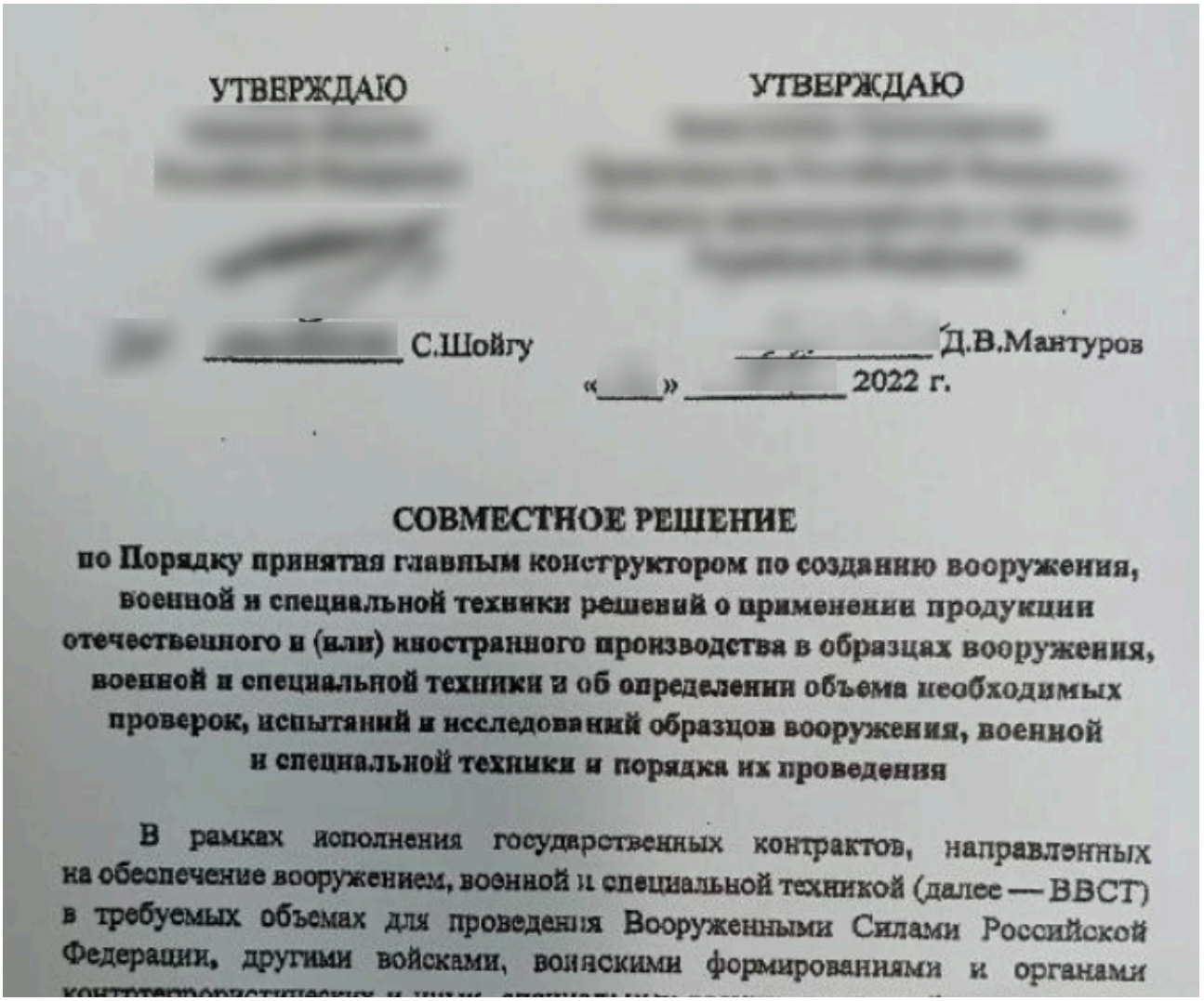
1. Утвердить прилагаемые изменения, которые вносятся в государственную программу Российской Федерации "Развитие атомного энергопромышленного комплекса", утвержденную постановлением Правительства Российской Федерации от 2 июня 2014 г. № 506-12

Fig. 13. Excerpt of the document used by the attackers

The first attack held in November (the malicious file was uploaded on November 2) used a cold supply diagram for a special-purpose high-performance computing complex.

On the following day, a new file was posted, this time containing a set of diagrams.

The next attack in November employed the group’s favored type of document, that is, related to defense industry operations (fig. 14).



УТВЕРЖДАЮ

[redacted] С.Шойгу

«[redacted]» [redacted] 2022 г.

УТВЕРЖДАЮ

[redacted] Д.В.Мантуров

«[redacted]» [redacted] 2022 г.

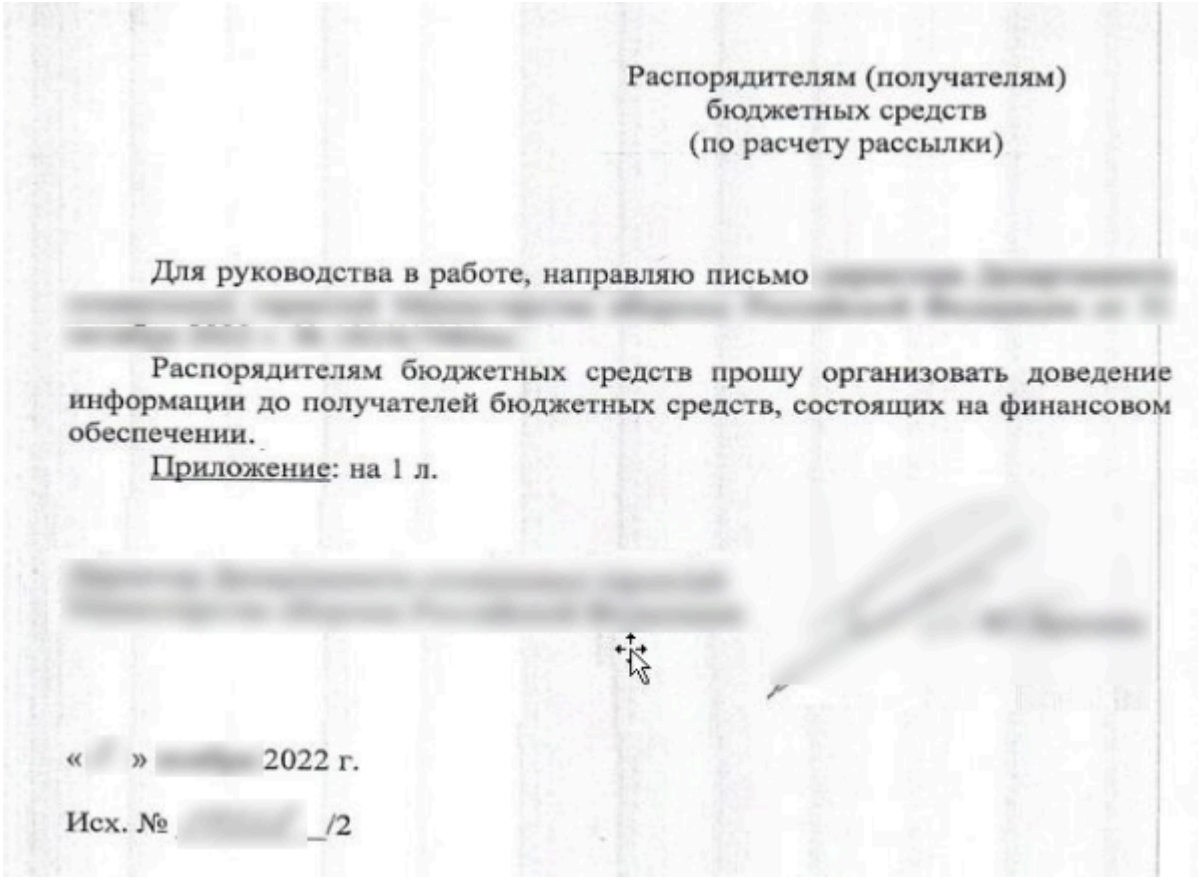
СОВМЕСТНОЕ РЕШЕНИЕ

по Порядку принятая главным конструктором по созданию вооружения, военной и специальной техники решений о применении продукции отечественного и (или) иностранного производства в образцах вооружения, военной и специальной техники и об определении объема необходимых проверок, испытаний и исследований образцов вооружения, военной и специальной техники и порядка их проведения

В рамках исполнения государственных контрактов, направленных на обеспечение вооружением, военной и специальной техникой (далее — ВВСТ) в требуемых объемах для проведения Вооруженными Силами Российской Федерации, другими войсками, воинскими формированиями и органами

Fig. 14. Excerpt of the document used by the attackers

The December attack was once again focused on the defense sector employees (fig. 15).



Распорядителям (получателям)
бюджетных средств
(по расчету рассылки)

Для руководства в работе, направляю письмо [redacted]

Распорядителям бюджетных средств прошу организовать доведение информации до получателей бюджетных средств, состоящих на финансовом обеспечении.

Приложение: на 1 л.

[redacted]

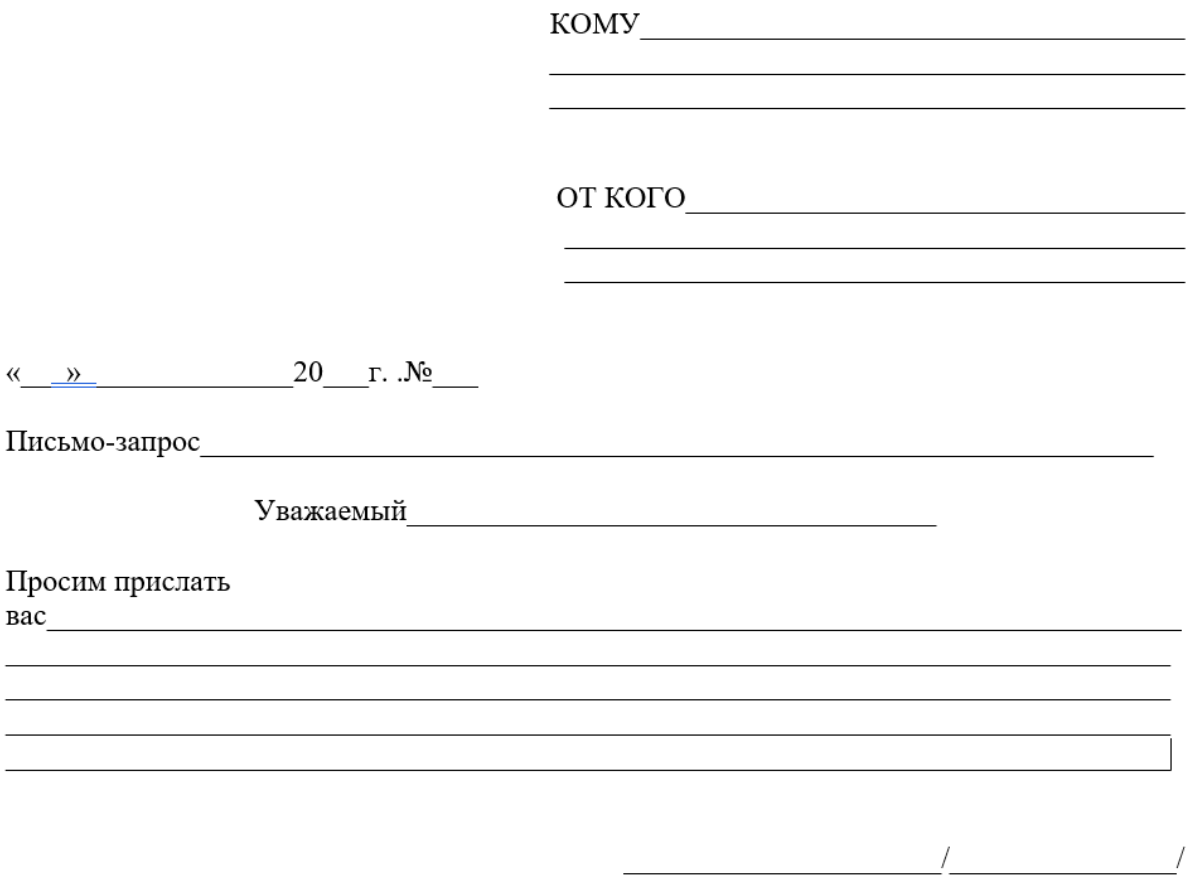
« » [redacted] 2022 г.

Исх. № [redacted] /2

Fig. 15.

Excerpt of the document used by the attackers

The first attack in 2023 used a request form as a phishing document (fig. 16).



КОМУ_____
_____
_____

ОТ КОГО_____
_____
_____

«__»_____20___г. .№___

Письмо-запрос_____

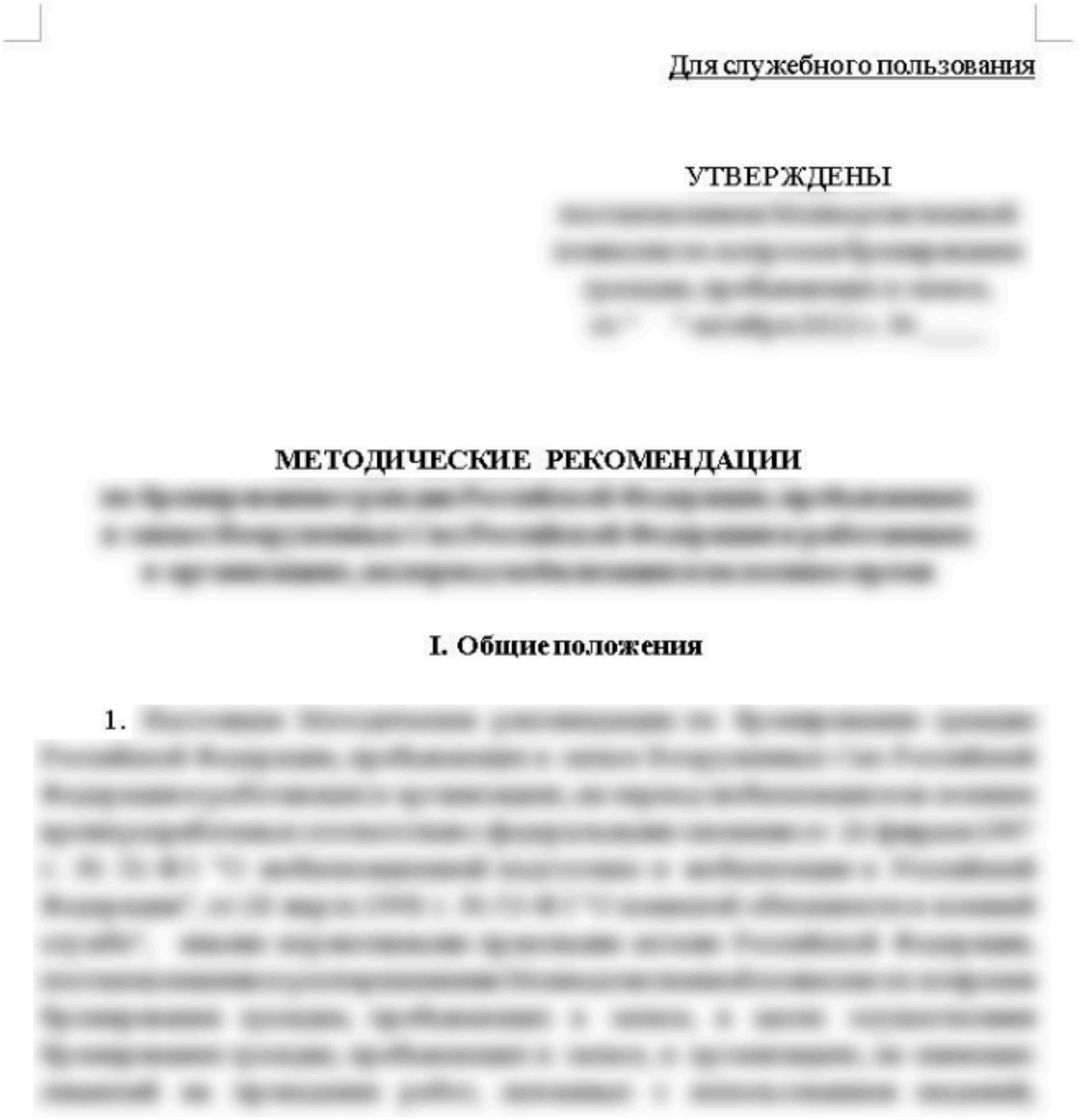
Уважаемый_____

Просим прислать
вас_____
_____
_____
_____
_____

_____/_____/

Fig. 16. Excerpt of the document used by the attackers

The next attack took place in January. The phishing document provided the methodological recommendations on the exemption from active service of Russian citizens being in the military reserves of the Russian Federation and working in certain organizations, for the period of mobilization and wartime (fig. 17).



Для служебного пользования

УТВЕРЖДЕНЫ

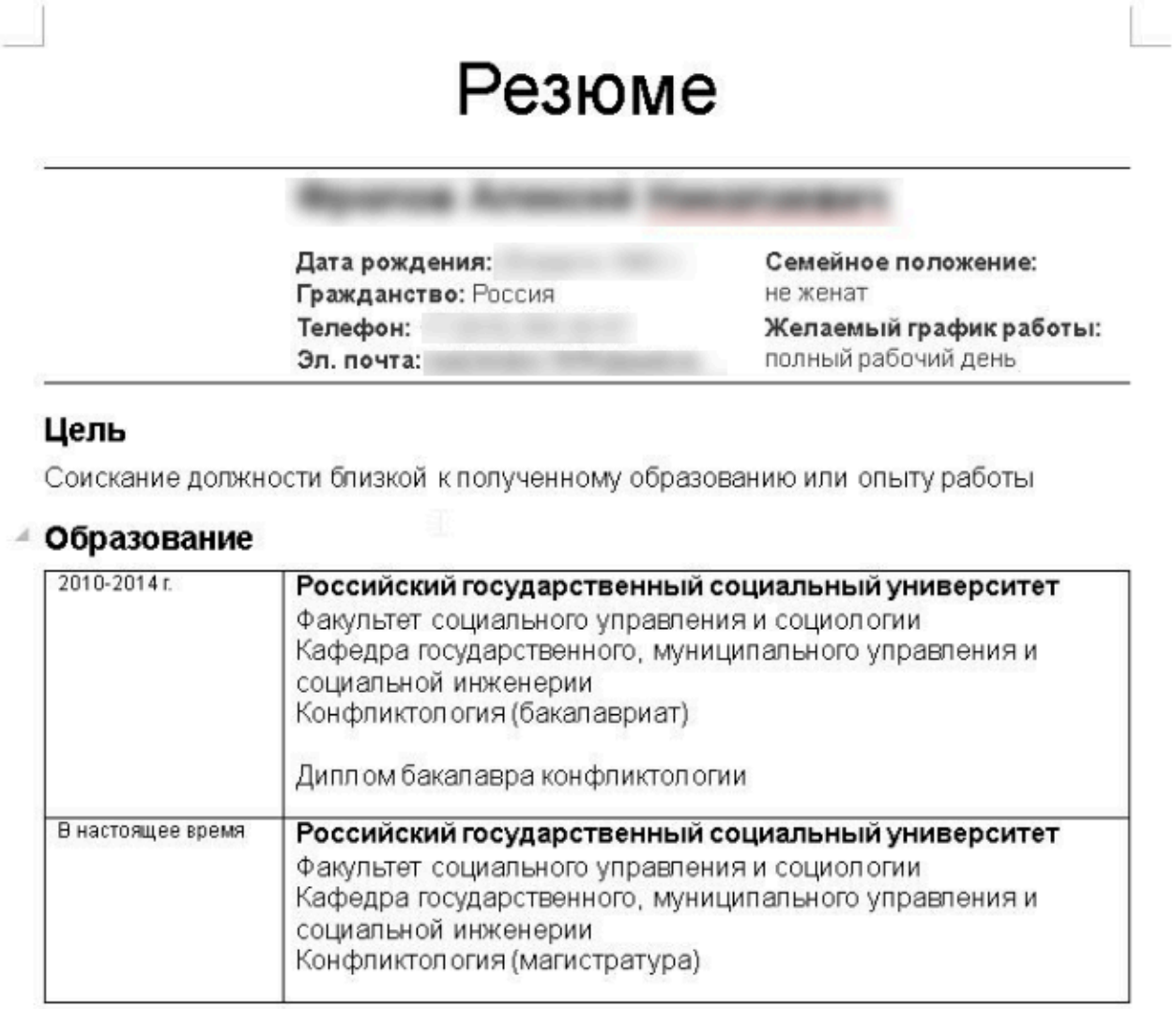
МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

I. Общие положения

1.

Fig. 17. Excerpt of the document used by the attackers

In February 2023, the attackers got back to sending resumes as phishing documents (fig. 18).



Резюме

[redacted]

Дата рождения: [redacted]
Гражданство: Россия
Телефон: [redacted]
Эл. почта: [redacted]

Семейное положение:
не женат
Желаемый график работы:
полный рабочий день

Цель

Соискание должности близкой к полученному образованию или опыту работы

Образование

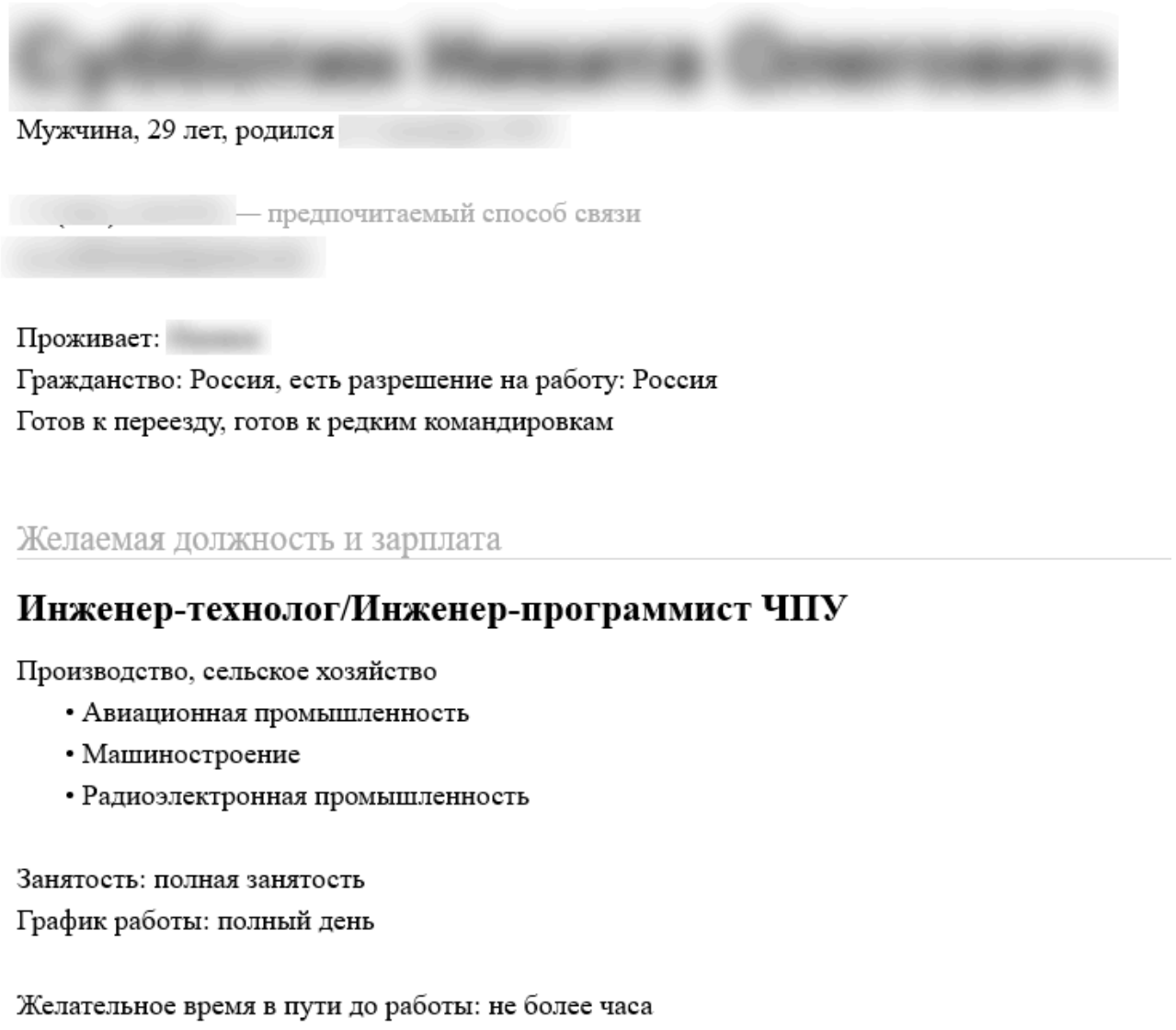
2010-2014 г.	**Российский государственный социальный университет** Факультет социального управления и социологии Кафедра государственного, муниципального управления и социальной инженерии Конфликтология (бакалавриат) Диплом бакалавра конфликтологии
В настоящее время	**Российский государственный социальный университет** Факультет социального управления и социологии Кафедра государственного, муниципального управления и социальной инженерии Конфликтология (магистратура)

Fig. 18. Excerpt of the document used by the attackers

In March 2023, Core Werewolf once again attached a copy of a document meant for official use only.

On March 20, 2023, one more file was uploaded to VirusTotal with the phishing document targeting defense industry personnel.

April 2023 saw the group’s repeated attempt to use a resume for phishing purposes (fig. 19).



[redacted]

Мужчина, 29 лет, родился [redacted]

[redacted] — предпочитаемый способ связи

[redacted]

Проживает: [redacted]

Гражданство: Россия, есть разрешение на работу: Россия

Готов к переезду, готов к редким командировкам

Желаемая должность и зарплата

Инженер-технолог/Инженер-программист ЧПУ

Производство, сельское хозяйство

- Авиационная промышленность
- Машиностроение
- Радиоэлектронная промышленность

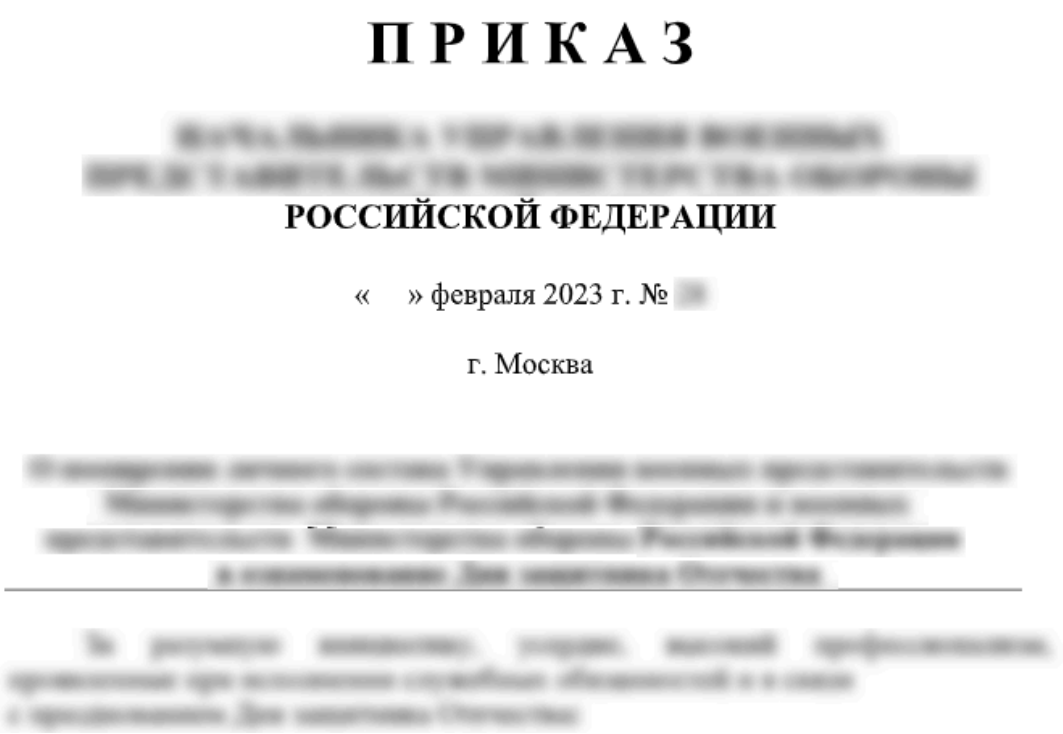
Занятость: полная занятость

График работы: полный день

Желательное время в пути до работы: не более часа

Fig. 19. Excerpt of the document used by the attackers

The attack that occurred in May featured yet another order (fig. 20).



П Р И К А З

[redacted]

РОССИЙСКОЙ ФЕДЕРАЦИИ

« » февраля 2023 г. № [redacted]

г. Москва

[redacted]

Fig. 20. Excerpt of the document used by the attackers

In each of the campaigns, the devices were compromised in a similar way. Therefore, the adversary tactics, techniques, and procedures listed in the section below apply to all of the attacks.

Source: https://bi.zone/eng/expertise/blog/core-werewolf-protiv-opk-i-kriticheskoy-infrastruktury/