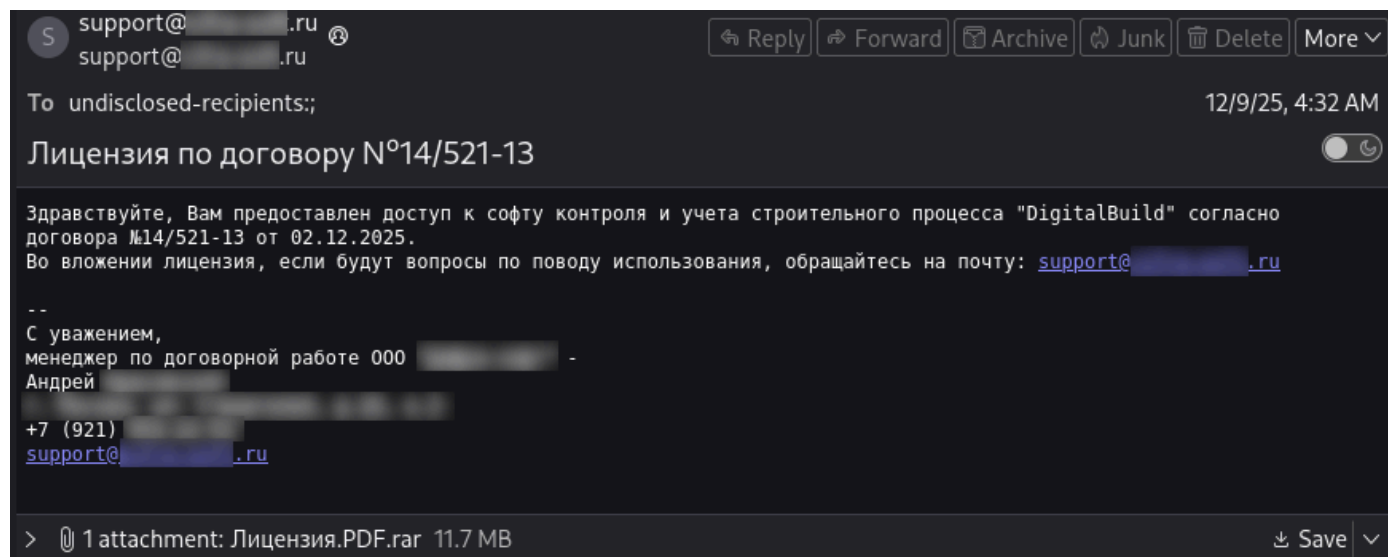


Липкий след: исследуем атаки группировки PseudoSticky

f6.ru/blog/pseudo-sticky

February 18, 2026



В ноябре 2025 года специалисты F6 обнаружили вредоносную кампанию, в которой атакующие использовали [LLM при проведении атаки с ВПО PureCrypter и DarkTrackRAT](#). Дальнейшее исследование активности группировки показало: речь идёт не просто о нескольких атаках, выполняемых с использованием LLM, а о полноценной группировке, проводящей вредоносные кампании и связывающей себя со **Sticky Werewolf** как посредством TTPs и используемых инструментов, так и прямым их упоминанием.

Sticky Werewolf (известна также под псевдонимами *MimiStick*, *Angry Likho*, *PhaseShifters*) – одна из наиболее активных проукраинских APT-группировок. Действует с апреля 2023 года, атакует предприятия в России и Беларуси. Одна из особенностей **Sticky Werewolf** – рассылки писем с вредоносным ПО от имени госведомств, например, Минпромторга, Минобрнауки России, Росгвардии. Цели группировки – предприятия в сфере энергетики, промышленности, ОПК, строительства, ЖКХ, транспорта.

Злоумышленники из группировки, применившей LLM в ноябрьской атаке, используют похожие TTPs и виды вредоносного ПО, которые внешне напоминают инструменты, связанные со **Sticky Werewolf**. В одном из случаев киберпреступники даже использовали название этой группировки в качестве пароля для вредоносного архива. Однако при более внимательном анализе становятся заметны отличия в инфраструктуре, реализации вредоносного кода и отдельных элементах тактики, что позволило нам предположить – вероятно, между группировками нет прямой связи, а есть сознательная мимикрия. По этой причине мы назвали новую группировку **PseudoSticky**.

В этом блоге мы представляем результаты исследования атак, которые группировка проводила зимой 2025-2026 годов. Целью этих атак стали компании из разных сфер деятельности – от ретейлеров и девелоперов до научно-исследовательских организаций и приборостроительных предприятий.

Как правило, злоумышленники использовали во вредоносных рассылках в качестве приманок файлы, названия которых были связаны с продукцией военного назначения – от авиационных ракет до беспилотных летательных аппаратов. При этом PseudoSticky компрометировали домены или почтовые ящики на доменах, названия которых созвучны с названиями предприятий и организаций, от имени которых злоумышленники впоследствии проводили рассылку вредоносных писем — включая областной суд. В некоторых случаях злоумышленники отправляли письма от имени несуществующих предприятий (таких, например, как ООО «Челябинский завод двигателей для авиации» и его филиал в Петрозаводске), а также генерировали фейковые документы с указанием таких вымышленных организаций (например, АО «Владимирский государственный радиозавод»).

Декабрь 2025 года: троян под ёлочку

В декабре 2025 года специалисты F6 обнаружили фишинговые рассылки группировки PseudoSticky на компании, действующие в сфере ретейла и строительства.

Письма были направлены с легитимного электронного почтового адреса, принадлежащего IT-компании из Владимирской области, что позволяет сделать вывод о его возможной компрометации. В письме содержалось уведомление о предоставлении организации доступа к платформе контроля и учёта строительного процесса, а вредоносный файл замаскировали под лицензию для указанного софта.

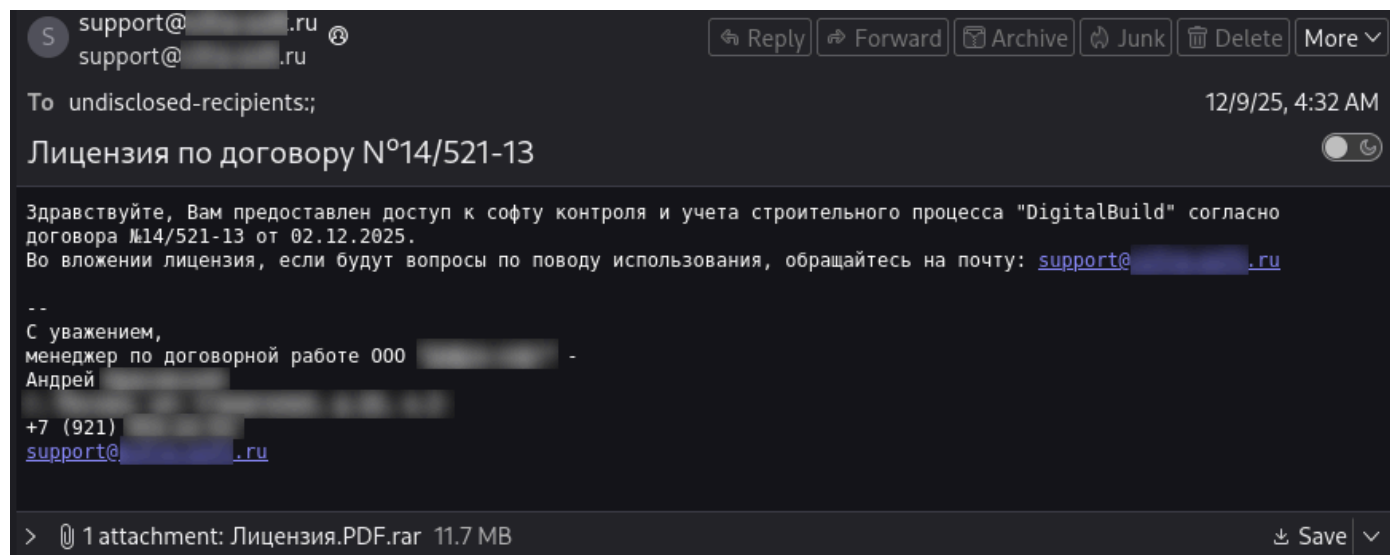


Рис. 1. – Пример фишингового письма от имени IT-компании

Письма содержали вложения в виде архивного файла с именем “*Лицензия.PDF.rar*” (MD5: 3b3f4ba1c4ac64754b2df46f195b2b77), внутри которого находится одноименный exe-файл, замаскированный под PDF-файл (MD5: ba235578635940cb7a9fc41df897d5b2). Данный файл был классифицирован как **DarkTrackRAT**.

DarkTrackRAT – это троян удаленного доступа (RAT). Обладает широкими возможностями, включает функции кейлоггера, управления удалённым рабочим столом, потоковой передачи веб-камеры, захвата микрофона и записи звука, менеджера файлов и многими другими. Данное вредоносное ПО используют в атаках несколько киберпреступных группировок, включая **Sticky Werewolf** и **PseudoSticky**.

В качестве C2-сервера используется [www.yandex\[.\]org](http://www.yandex[.]org) – этот домен уже «засветился» в ноябрьской атаке. Все эти факты позволили отнести новую рассылку к ранее описанной кампании.

Январь 2026 года: пробить диод

В январе 2026 года аналитики F6 зафиксировали новые фишинговые кампании PseudoSticky. После новогодних праздников злоумышленники частично сменили почерк. Вот как изменилась цепочка атаки:

- замена основной полезной нагрузки на **RemcosRAT**;
- внедрение Bitbucket в инфраструктуру доставки вредоносного ПО;
- использование NSIS-упаковщика (Nullsoft Scriptable Install System) на этапе финальной сборки/доставки.

Remcos – троян удалённого доступа, известный с 2016 года. Имеет множество функций, включая шпионаж (онлайн и оффлайн кейлоггер, скринлоггер, доступ к данным веб-камеры, RemoteScripting, FileManager). Как правило, заражение жертвы происходит с помощью фишинговых писем, имеющих вложение с вредоносным макросом, который подгружает ВПО. Remcos RAT используют в атаках более 20 киберпреступных группировок, включая **StickyWerewolf** и **PseudoSticky**.

[Анализ ВПО на платформе MDP F6 \(F6 Malware Detonation Platform\)](#)

Параллельно с изменением цепочки атак злоумышленники расширили спектр целей, включив в него научно-исследовательские организации.

Как и в первоначальных кампаниях, фишинговые письма были направлены с предположительно скомпрометированных электронных почтовых адресов. Один из этих ящиков располагается на домене научно-исследовательского института, занимающегося в том числе разработкой и выпуском продукции военного и двойного назначения, второй – на домене компании из Челябинской области.

Используемые в кампании фишинговые письма содержали в себе вложения в виде архивного файла “Отчет по НИОКР 1427-18 (шифр АИСТ).PDF.rar” (MD5: 00efe94d5c2c4c67e20dd1846c6d29d2), содержащего два decoy-файла “2026 01 Решение 2Д212.doc” (MD5: 7573a316430480e4301c1c28d4a9af7d) и “Расчёт.xlsx” (MD5: c45c10bb8f3a52d82667c1e0be54d63b), а также исполняемые файлы “Отчет по НИОКР 1427-18 (шифр АИСТ).PDF.exe” (MD5: 79ddb58bd757774607b007a09ba1b664) и “План модернизации.PDF.exe” (MD5: 79ddb58bd757774607b007a09ba1b664).

Шифр «Аист», который упоминается в названии писем, согласно открытой информации в сети Интернет, относится к проекту речных пограничных катеров.

Один из файлов-приманок, который оформлен как решение по итогам испытаний диодов, содержит недостоверную информацию – второй стороной в документе обозначено АО «Владимирский государственный радиозавод», информация о котором в открытых источниках отсутствует.

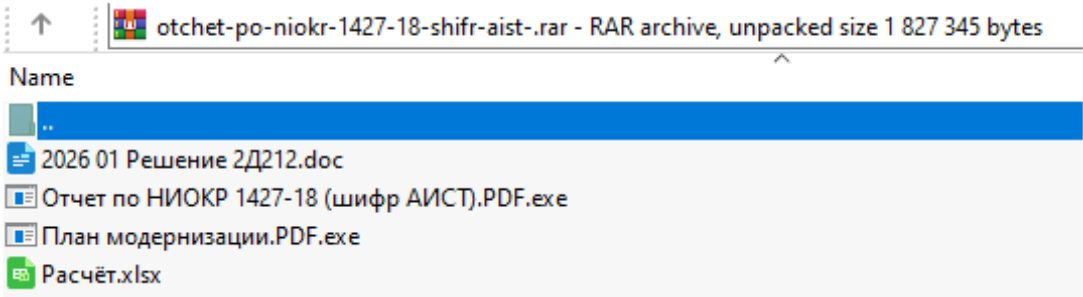


Рис. 2. – Содержимое архивного файла “Отчет по НИОКР 1427-18 (шифр АИСТ).PDF.rar”
(Чтобы увидеть следующее изображение в галерее, нажмите на кнопку справа от картинки)

Расчёт.xlsx - Excel

View			
Normal	Page Break Preview	Page Layout	Custom Views
☒ Ruler	☒ Gridlines	☒ Formula Bar	☒ Headings
Zoom	100%	Zoom to Selection	New Window
Arrange All	Freeze Panes	Split	Hide
Unhide			

A	B	C
1		Трудоёмкость
2	Плата	Лента 10-М-2-НО-2,5
3	Кольцо	Отливка
4	Крышка	АК12
5	Кольцо	Аутсорс
6	Прокладка	Аутсорс
7		Аутсорс
8		Аутсорс
9		

Рис. 3. – Декой-файл “Расчёт.xlsx” (Чтобы увидеть следующее изображение в галерее, нажмите на кнопку справа или слева от картинки)

УТВЕРЖДАЮ Начальник Минобороны России _____ 2026	УТВЕРЖДАЮ Технический директор АО «Владимирский государственный радиозавод» _____ 2026
--	---

Решение №
о переводе приёмо-сдаточных испытаний
диодов выпрямительных 2Д212А1/СО,
2Д212Б1/СО, 2Д212А9/СО, 2Д212Б9/СО в
категорию периодических

В связи с получением положительных результатов испытаний по группам С-4, С-5 на пяти последовательно проведённых испытаниях диодов выпрямительных 2Д212А1/СО, 2Д212Б1/СО, 2Д212А9/СО, 2Д212Б9/СО АЕЯР.432120.177ТУ на основании требований пункта 4.3.9 ГОСТ В 28146 – 89 «Приборы полупроводниковые. Общие технические условия» принимается

Р Е Ш Е Н И Е :

1. Испытания диодов выпрямительных 2Д212А1/СО, 2Д212Б1/СО, 2Д212А9/СО, 2Д212Б9/СО по группам С-4, С-5 перевести в категорию периодических с периодичностью их проведения 1 раз в месяц. Оценка проводится на выборке диодов любого типономинала из перечисленных с соответствующим распространением результатов.

Отв.: СЛК

2. При появлении первого отрицательного результата испытаний, группа, по которой получен отрицательный результат, переводится снова в категорию приёмо-сдаточных испытаний.

Рис. 4. – Декой-файл “2026 01 Решение 2Д212.doc” (Чтобы увидеть следующее изображение в галерее, нажмите на кнопку слева от картинки)

Стоит отметить, что декой-файл “2026 01 Решение 2Д212.doc” содержит вложенный поток данных со списком источников и настройками стиля цитирования, однако он пустой – возможно, его оставили по ошибке. Вместе с тем, название цветовой схемы стиля в данном потоке данных указано как «Офіс»: это можно оценить как косвенное свидетельство создания или редактирования документа в среде с украинскими региональными настройками.

Содержащиеся в архиве исполняемые файлы “Отчет по НИОКР 1427-18 (шифр АИСТ).PDF.exe” и “План модернизации.PDF.exe” идентичны, в связи с чем ниже описан один из них – файл “План модернизации.PDF.exe”.

Он представляет собой PE32-исполняемый файл, собранный с использованием NSIS (Nullsoft Scriptable Install System), и содержит недействительную цифровую подпись на имя *rkn.gov.ru* (на этом домене располагается официальный сайт Роскомнадзора).

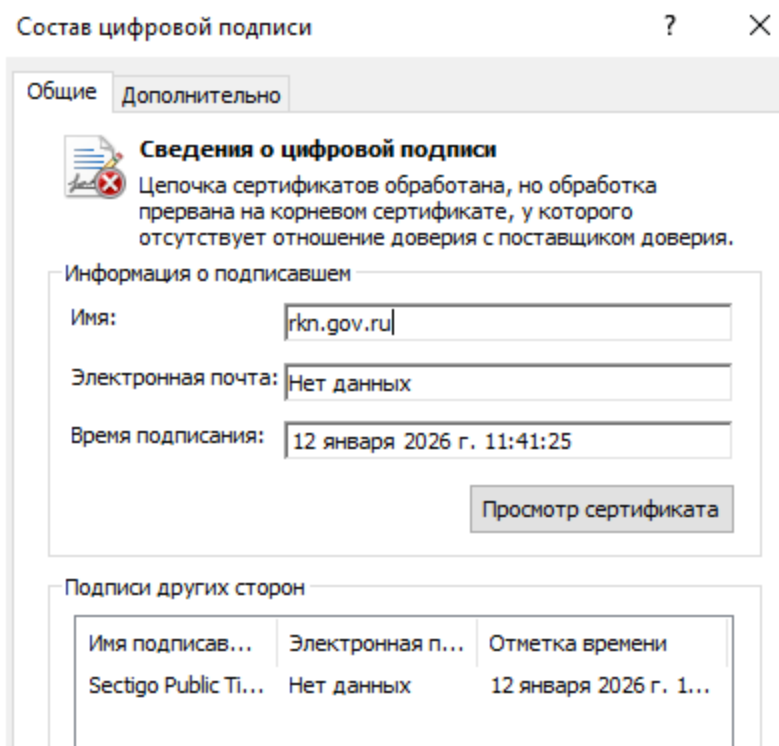


Рис. 5. – Сведения о цифровой подписи файла “План модернизации.PDF.exe”

В ходе исполнения указанный файл помещает в каталог автозапуска файл *%AppData%\Microsoft\Windows\StartMenu\Programs\Startup\swbck.exe* (MD5: *a1e25f9fc4177d6b11bd30deb6135dd9*) и запускает его, тем самым закрепляясь в системе жертвы.

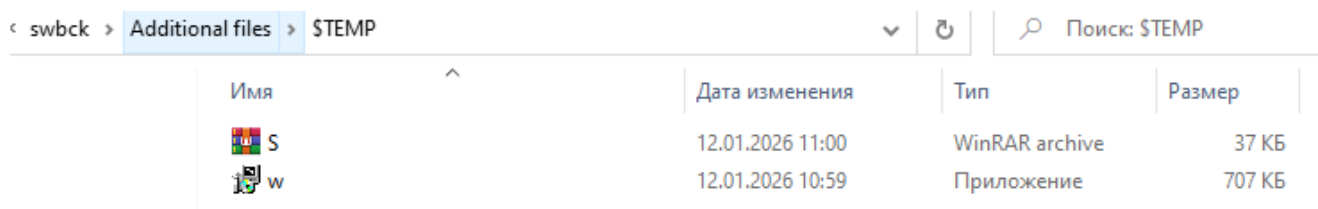
Файл *swbck.exe* – PE32-исполняемый файл, который в ходе исполнения создает в зараженной системе профиль нового пользователя с именем *Adm* и паролем *Zxcasdqwe123*, после чего вносит изменения в реестр, чтобы скрыть этого пользователя

с экрана приветствия (входа в систему).

```
powershell.exe -WindowStyle Hidden -Command "reg add  
'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList' /v  
Adm /t REG_DWORD /d 0
```

Далее для отключения Windows Defender осуществляется обращение к ресурсу [hxxps://dnot\[.\]sh/](https://dnot[.]sh/). Переход по данной ссылке перенаправляет запрос на ресурс [https://github\[.\]com/es3n1n/defendnot](https://github[.]com/es3n1n/defendnot), с которого происходит скачивание и запуск соответствующей утилиты.

После отключения Windows Defender ВПО помещает на устройство жертвы два файла: “%Temp%\S.7z” (MD5: *f270e01f8c5a4739bd9141f8f664979f*) и “%Temp%\w.exe” (MD5: *d80a126f41758e1b0a60799eb790c213*), после чего запускает “w.exe”.



Имя	Дата изменения	Тип	Размер
S	12.01.2026 11:00	WinRAR archive	37 КБ
w	12.01.2026 10:59	Приложение	707 КБ

Рис. 6. – Сведения о содержимом каталога “Temp”

Файл “w.exe” представляет собой PE32-исполняемый файл, собранный с использованием NSIS. В ходе исполнения помещает на устройство жертвы файл “%Temp%\[RND].tmp\waf—waf.exe”, который является легитимным файлом архиватора 7-Zip, после чего запускает команду для распаковки ранее указанного архива во временный каталог и запускает содержащийся в нем файл S.exe (MD5: *8456bfc8d524f4f95023e0d2b86295e3*).

```
%Temp%\[RND].tmp\waf-waf.exe x -pStickyWerewolf -y -o"%Temp%" "%Temp%\S.7z"
```

В качестве пароля к указанному архиву атакующие используют строку “StickyWerewolf”

Файл S.exe представляет собой PE-исполняемый файл, собранный с использованием NSIS, классифицированный нами как загрузчик. В ходе исполнения данный файл связывается с ресурсом [hxxp://bitbucket\[.\]org/mlwranalytics/stephen/raw/main/calc](https://bitbucket[.]org/mlwranalytics/stephen/raw/main/calc), где в коммите содержится информация о C2-серверах, и сохраняет ответ в файл “%Temp%\[RND]\f.txt”.

calc

Source ▾

main ▾

450d90c ▾

Full commit

stephen / calc

1

https://cdn-01.anonfiles.wtf/_static/0494edf3-0553-404f-9a43-da7e301b7f2c

Рис. 7. – Содержимое Bitbucket на 21.01.2026

В ходе исследования списка коммитов были получены сведения об иных ресурсах, используемых атакующими, а также адресе электронной почты пользователя, создающего коммиты.

45cf56c



Johny Behl committed **45cf56c**

2026-01-12

12/01/2026

0 comments



Add a comment

1 file

Filter by comments

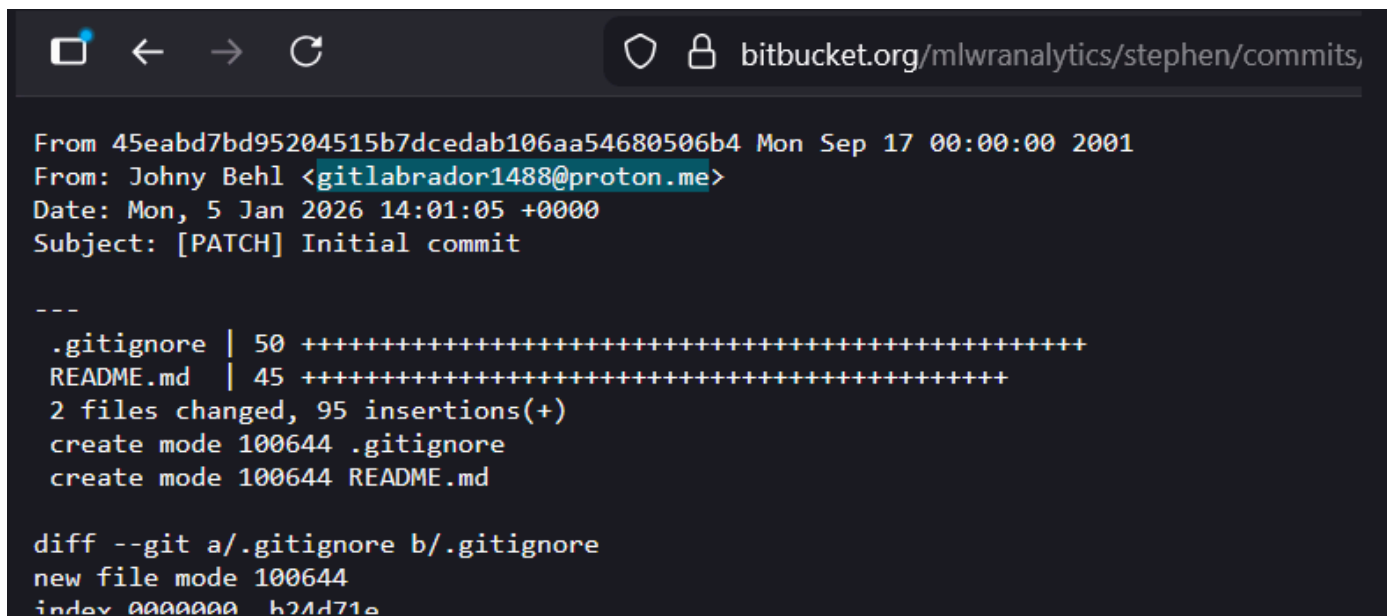


```
▼  calc 
```

```
@@ -1 +1 @@
```

1	- https://bashupload.com/XSkPLv.exe
1	+ https://bashupload.com/Daerjg.exe
↓	(SHIFT + click to expand all lines)

Рис 8. – Ресурсы, указанные атакующими в коммите (Чтобы увидеть следующее изображение в галерее, нажмите на кнопку справа от картинки)



```
From 45eabd7bd95204515b7dcedab106aa54680506b4 Mon Sep 17 00:00:00 2001
From: Johnny Behl <gitlabrador1488@proton.me>
Date: Mon, 5 Jan 2026 14:01:05 +0000
Subject: [PATCH] Initial commit

---
.gitignore | 50 ++++++
README.md | 45 ++++++
2 files changed, 95 insertions(+)
create mode 100644 .gitignore
create mode 100644 README.md

diff --git a/.gitignore b/.gitignore
new file mode 100644
index 0000000..b21d71a
```

Рис. 9. – Адрес электронной почты атакующего, указанный в коммите (Чтобы увидеть следующее изображение в галерее, нажмите на кнопку слева от картинки)

В качестве C2, полученного на момент проведения исследования, выступал ресурс `hxxps://cdn-01.anonfiles[.]jwtf/_static/0494edf3-0553-404f-9a43-da7e301b7f2c`.

Далее с указанной ссылки скачивается полезная нагрузка и происходит её сохранение в файле `%TEMP%\w.exe`, после чего происходит запуск указанного файла. Затем через 10 секунд ВПО стирает файл `w.exe` из `%TEMP%`, а также отключает защиту UAC.

```
powershell.exe -WindowStyle Hidden -Command "reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v ConsentPromptBehaviorAdmin /t REG_DWORD /d 0 /f" powershell.exe -WindowStyle Hidden -Command "reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v PromptOnSecureDesktop /t REG_DWORD /d 0 /f"
```

После исполнения указанных действий семпл самоуничтожается и завершает работу.

К сожалению, нам не удалось скачать полезную нагрузку, так как на момент проведения исследования домен C2-сервера не был связан с каким-либо IP-адресом. Однако на странице семпла на публичной онлайн-песочнице мы обнаружили комментарий одного из пользователей с информацией о том, что загружаемой полезной нагрузкой является Remcos RAT, а также маркировку с её принадлежностью к группировке StickyWerewolf.

Кроме того, в ходе дальнейшего исследования на другой публичной онлайн-песочнице мы обнаружили извлеченный конфиг данного семпла.

```
Family: RemcosRAT
#RemcosRAT #StickyWerewolf #SuspiciousPE #exe
File Name: S.exe.bin
File Size: 52.99KB
File Type: exe
Origin Country: #RU
```

Family: remcos Version: 3.8.0 Pro Botnet: Telegram
C2: wwwyandex[.]org:5412 Attributes: audio_folder
audio_record_time: 5 connect_delay: 5
connect_interval: 5 copy_file: Telegram.exe
copy_folder: Telegram delete_file: false hide_file: false hide_keylog_file: false install_flag: true
keylog_crypt: false keylog_file: logs.dat keylog_flag: false keylog_folder: remcos mouse_option;
false mutex: Telegram-8JNUGD screenshot_crypt: false screenshot_flag: false screenshot_folder:
Screenshots screenshot_path: %AppData% screenshot_time: 10 startup_value: Telegram
take_screenshot_option: false take_screenshot_time: 5

Рис. 10. – Комментарий, размещенный
на странице семпла в публичной онлайн-
песочнице

Как и в предыдущих семплах, атакующие используют в качестве C2-сервера ресурс wwwyandex[.]org. Вместе с тем, несмотря на определенное сходство TTPs, а также факт использования ВПО DarkTrack RAT, провести уверенную атрибуцию вышеуказанных и ранее описанной атаки группировке **StickyWerewolf** невозможно. Ключевое ограничение — использование группировкой Sticky Werewolf модифицированной версии ВПО **DarkTrackRAT**.

Также в ходе дополнительного исследования инфраструктуры было обнаружено еще одно фишинговое письмо с темой «КД к изделию 170», связанное с описанной вредоносной кампанией. *(Под индексом «изделие 170» обычно упоминается авиационная ракета класса «воздух-воздух».)*

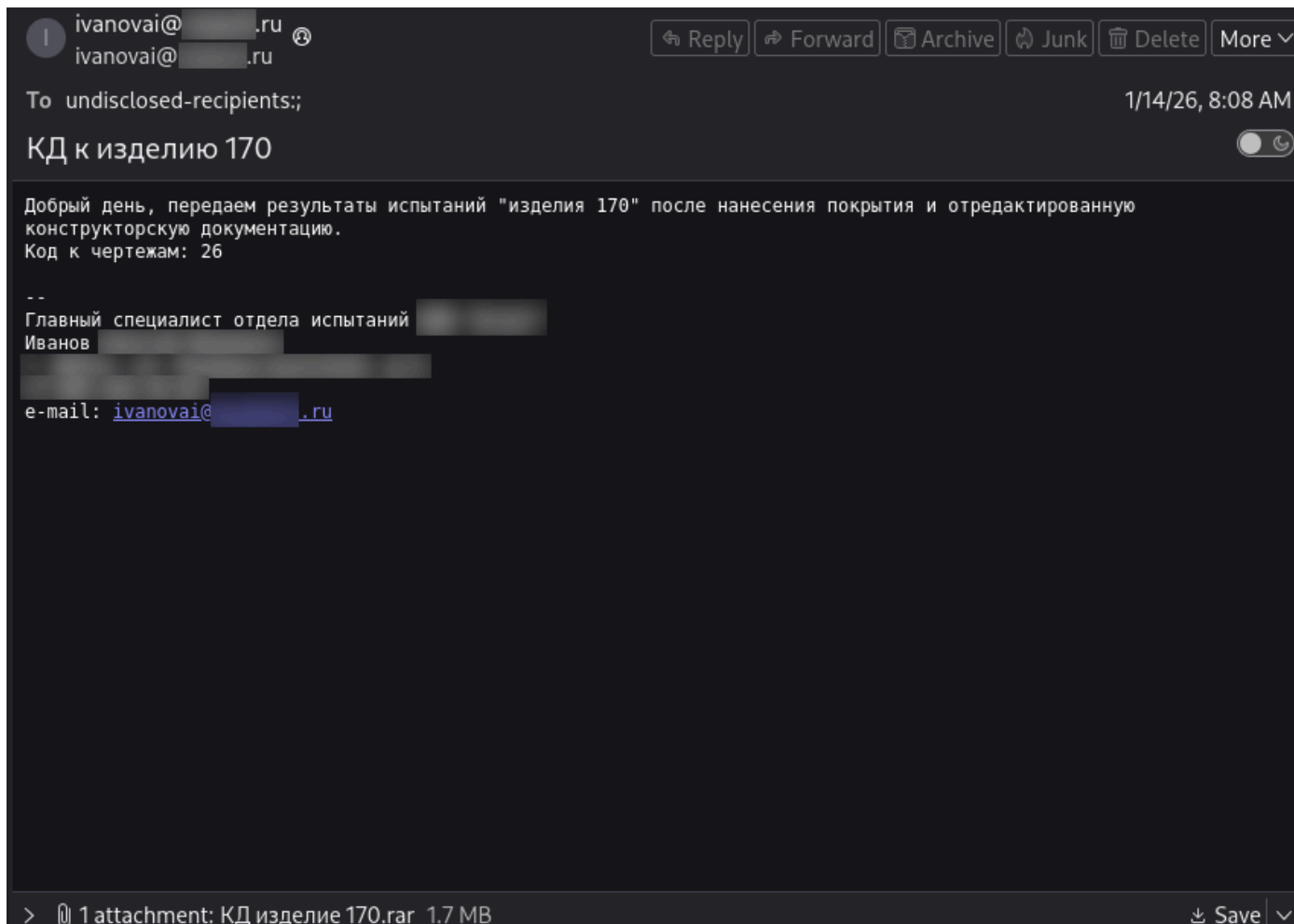


Рис. 11. – Фишинговое письмо

В данное письмо вложен архивный файл “КД изделие 170.rar” (MD5: *b65b6a9b4c7361b60893370870658dfd*), который содержит decoy-файлы “Перечень КД.xlsx” (MD5: *25b0979d43c793d56f28095c8a02dcfe*) и “Испытания 13.01.doc” (MD5: *003063c27efc8ba739632117c4f8fd07*), а также идентичные друг другу исполняемые файлы “Изделие 170 габаритный чертеж.PDF.exe” (MD5: *79ddb58bd757774607b007a09ba1b664*) и “Конструкторская документация к изделию 170.PDF.exe” (MD5: *79ddb58bd757774607b007a09ba1b664*).

Name	Size	Type	Date Modified
Изделие 170 габаритный чертеж.PDF.exe	885.9 kB	Windows or DO...	10 July 2025, 03:41
Испытания 13.01.doc	46.6 kB	Word document	14 January 2026, 04:53
Конструкторская документация к изделию 170.PDF.exe	885.9 kB	Windows or DO...	10 July 2025, 03:41
Перечень КД.xlsx	9.1 kB	Excel 2007 spr...	14 January 2026, 03:25

Рис. 12. — Содержимое архивного файла “КД изделие 170.rar”

Указанное письмо отличается от описанного выше лишь начальным RAR-архивом и первым исполняемым файлом, который размещает на устройстве жертвы файл *swbck.exe*.

Используемые в этой атаке декой-файлы “Перечень КД.xlsx” и “Испытания 13.01.doc” получили лишь незначительные изменения в части смены ФИО и организаций.

Февраль 2026 года: беспилотная тревога

В феврале 2026 года злоумышленники из PseudoSticky продолжили атаки. TTPs и инструменты остались без изменений, а вот список целей и сетевая инфраструктура расширились.

Так, 12 февраля 2026 года системой [F6 Managed XDR](#) были перехвачены и заблокированы фишинговые письма с темами “Конструкторская документация по БЛА «ИТАЛМАС» (Изделие-54)” и “Извещение о судебном заседании по делу №26/1402-19932295123.14”, направленные атакующими с использованием легитимных электронных почтовых адресов в адрес научно-исследовательской организации.

Одно из таких писем отправлено от имени несуществующего ООО «Челябинский завод двигателей для авиации» с почтового ящика на домене предприятия по производству дистилляционных аппаратов. Причём в качестве отправителя указан технический директор филиала фейкового предприятия в Петрозаводске, якобы расположенного по адресу «пр. Победы, 12» – ни проспекта, ни проезда с таким названием в столице Карелии нет.

Второй электронный адрес относится к неофициальному информационному сайту судебной тематики, домен которого отчасти похож на домены официальных органов судебной власти. Данные факты указывают на то, что атакующие целенаправленно использовали скомпрометированные адреса электронной почты, чтобы выдать вредоносные рассылки за письма от конкретных организаций.

Также в ходе исследования обнаружены аналогичные письма, направленные в адрес приборостроительных предприятий.

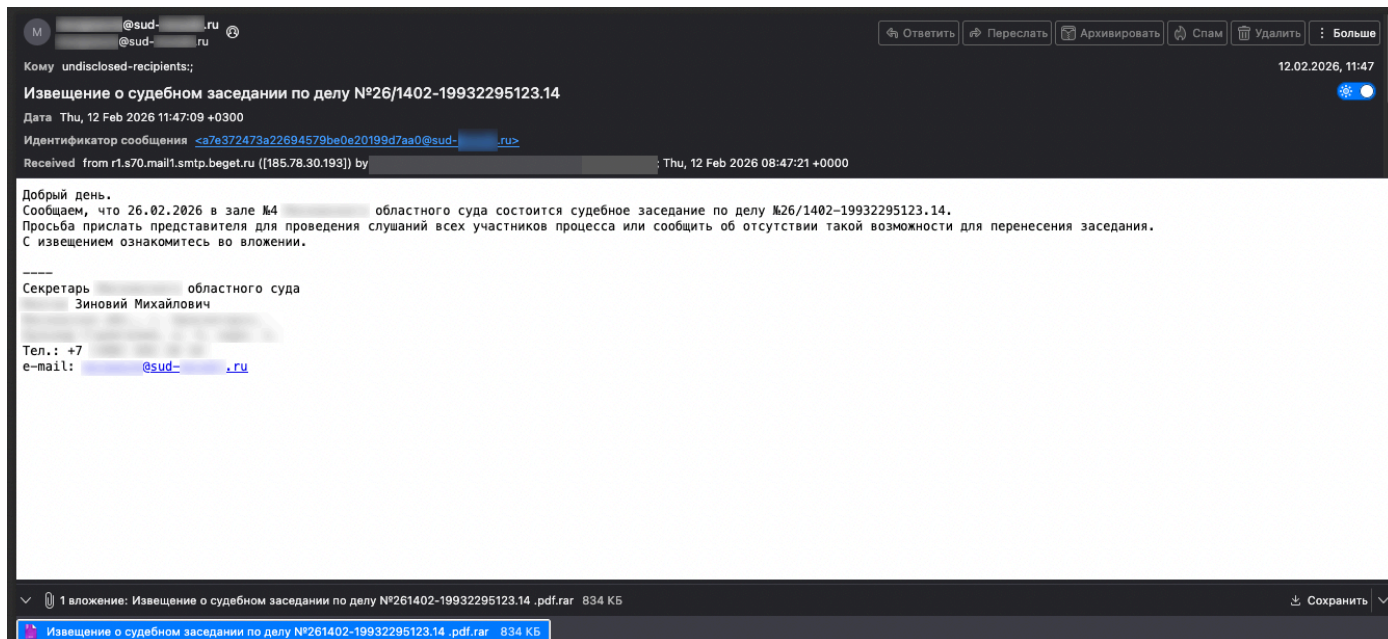


Рис. 13. – Фишинговое письмо

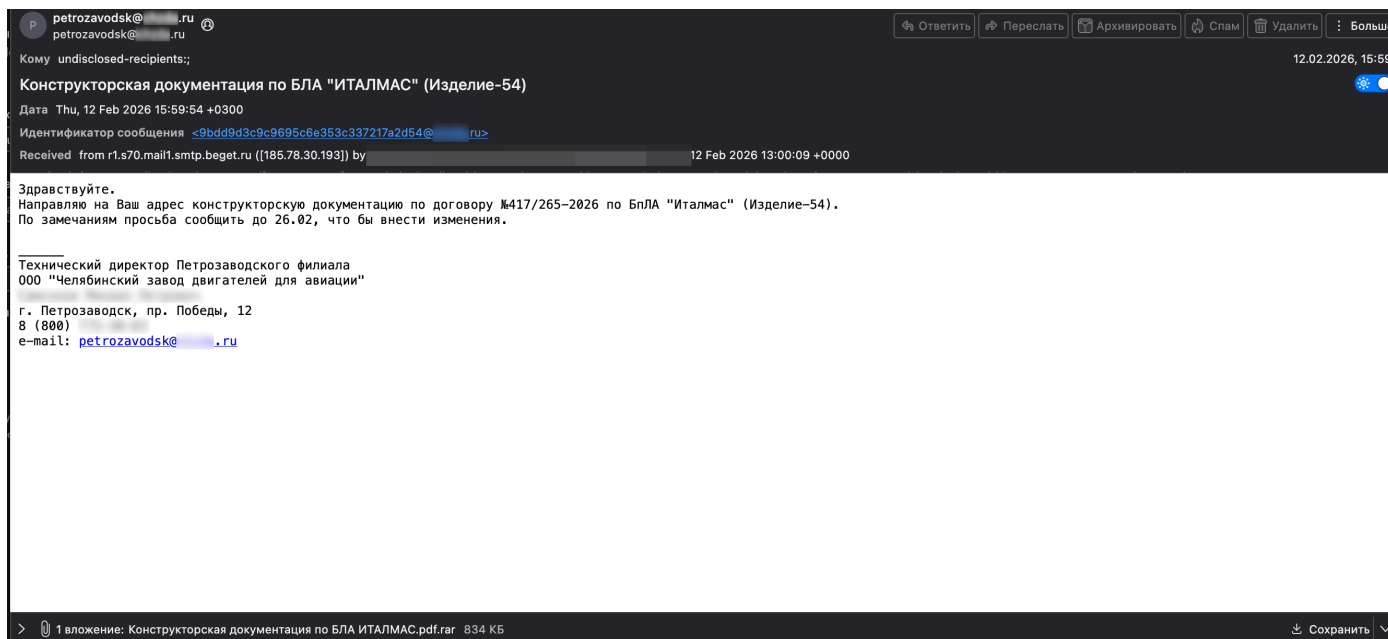


Рис. 14. – Фишинговое письмо

Эти письма содержат вложенные файлы “Конструкторская документация по “БЛА ИТАЛМАС.pdf.rar” (MD5: 66425059faf191f4f4a6b845286b9049) и “Извещение о судебном заседании по делу №261402-19932295123.14 .pdf.rar” (MD5: 2ae4847476dfff3f34b75dfa224be969), в которых находились исполняемые файлы “Конструкторская документация по БЛА ИТАЛМАС.pdf.exe” (MD5: f807f3a307a8ec230d5feb8e921ec82a) и “Извещение о судебном заседании по делу №261402-19932295123.14 .pdf.exe” (MD5: b6ce4a3891f537e00f1a8d779af61e32) соответственно. В ходе исполнения данные файлы размещают на устройстве PE32-исполняемый файл sethc.exe (MD5: 1a5154f7ae03a5051fb14cf24f703c4d).

Указанный файл запускал цепочку атаки, аналогичную вышеописанной, за исключением C2-сервера, передаваемого как коммит в bitbucket, который содержал ссылку на ресурс [https://cdn-01\[.\]johanclothing\[.\]shop/_static/34d9fb7f-14a1-4825-a00c-79da2c8fb949](https://cdn-01[.]johanclothing[.]shop/_static/34d9fb7f-14a1-4825-a00c-79da2c8fb949). В результате доступа к этому ресурсу осуществлялось скачивание файла telegram.exe (MD5: 7af046262b5e0a6c116a7f7be022dc68) с полезной нагрузкой Remcos RAT и следующим конфигурационным файлом.

Family: remcos Version: 3.8.0 Pro Botnet: RemoteHost C2: 79.137.194.178:5412 Attributes: MicRecords audio_record_time: 5 connect_delay: 0 connect_interval: 1 copy_file: Telegram.exe copy_folder: Telegram delete_file: false hide_file: true hide_keylog_file: false install_flag: true keylog_crypt: false keylog_file: logs.dat keylog_flag: false keylog_folder: remcos mouse_option: false mutex: Telegram-JDHTI9 screenshot_crypt: false screenshot_flag: false screenshot_folder: Screenshots screenshot_path: %AppData% screenshot_time: 10 startup_value: Telegram take_screenshot_option: false take_screenshot_time: 5

Вывод

В этом исследовании мы рассмотрели пример возможного мимикрирования злоумышленников под другую киберпреступную группировку, когда намеренно копируется стиль группы, заимствуются её подходы и дорабатывается инструментарий. Стремление выдать свои атаки за действия уже известных киберпреступных групп – одна из распространённых практик, которые могут использовать как новые группировки злоумышленников, так и новые подразделения этих группировок. Второй путь — создавать собственные инструменты и уникальные техники.

В таких случаях только детальное исследование атак, основанное на сопоставлении технических артефактов, инфраструктурных связей и контекстных факторов, позволяет получить максимально полное представление об атакующем, а также адаптировать механизмы обнаружения и реагирования на его атаки.

Индикаторы компрометации

Файлы

Лицензия.PDF.rar

MD5: 3b3f4ba1c4ac64754b2df46f195b2b77

SHA-1: 90da7ff031816318cf65d3d184678c0e1112e861

SHA-256: db357a4bf87f9b5630222f9acd2aec3c6566648e878092b6947f2141dd4ea235

Лицензия.PDF.exe

MD5: ba235578635940cb7a9fc41df897d5b2

SHA-1: 76779d0713aa717032c649136dfffab822df91ef

SHA-256: 89a9c6e0595349b950cbb44e9842e8c3ead0e5ef6702594108949145e6d14dad

Изделие-44 ДСП.rar

MD5: d3b6c14b4bbad6fd72881ff6b88a0de4

SHA-1: 83458906e6888b0b20b091ce1250cfc7e0e81ca6

SHA-256: d1c9951d5e219981f9fd21d465491728c2005718be2d96c9814a50c88accd1e7

Изделие-44 ДСП.hta, НИОКР НЛТД.148.12.00.01.hta

MD5: e6846e5074ef5e583df74d989a32833f

SHA-1: 65442d77207892d7668e0899a32a3cae2285b3ab

SHA-256: d6a8e2dfc28abcf9b63ec1827d6568b09d76310d1db1794683ea6ded30dc532e

345cph8xf.exe

MD5: 265dfa924da79d74b1bbaebe348aaf0d

SHA-1: d561018ff9ca536b121ac2ca211ae394d75ac373

SHA-256: dc54a080caeea8f57a7dacfc519d8c17d28ce416a012c37030bfedfb27945a6f

Отчет по НИОКР 1427-18 (шифр АИСТ).rar

MD5: 00efe94d5c2c4c67e20dd1846c6d29d2

SHA-1: 90c2160e1e70cd9d0ce3de06395545d7053f8065

SHA-256: fa3dac010f2bc6eafaaa6409d2ed0ab26510cd16ca611be5509145184308461f

Отчет по НИОКР 1427-18 (шифр АИСТ).PDF.exe

MD5: 79ddb58bd757774607b007a09ba1b664

SHA-1: 3970148591dc727828eb1c459496a6e0f68dd5fd

SHA-256: 944be60b0fbcfb625b47a4ea8064100124d3c0430855da6ec051cd3d494d964b

План модернизации.PDF.exe

MD5: 79ddb58bd757774607b007a09ba1b664

SHA-1: 3970148591dc727828eb1c459496a6e0f68dd5fd

SHA-256: 944be60b0fbcfb625b47a4ea8064100124d3c0430855da6ec051cd3d494d964b

swbck.exe

MD5: a1e25f9fc4177d6b11bd30deb6135dd9

SHA-1: f3bbde729a99185a5e42706e168cd7f6b3b8073f

SHA-256: 68769189f293c9031726a051303e5dc8a4d2b1254e0a62c006e0a84988672a35

w.exe

MD5: d80a126f41758e1b0a60799eb790c213

SHA-1: ea23b2ad7fc58a6c2de3f19f0d12c333525b9a7b

SHA-256: 5d4b9e922576f0203376d98508239b2266b7b43cf591699c181f15797adffad9

S.7z

MD5: f270e01f8c5a4739bd9141f8f664979f

SHA-1: a6d0bcddafb000122be7bd4fa29382e17d2f1f60

SHA-256: e6e320f0e0c052f2ba57ea7698f31eb0ab8bcb4a599fff4257fe20997eb39253

S.exe

MD5: 8456bfc8d524f4f95023e0d2b86295e3

SHA-1: dae944c52ebeebed5655e2c78cdd4da45714c5d1

SHA-256: 37dca3cd3af9524b439678f344f96719c87bbfc722673e79b6de541ce30d5555

КД изделие 170.rar

MD5: b65b6a9b4c7361b60893370870658dfd

SHA-1: 61b316aedfc9d9941f5c9baa3c31776a34ef36cd

SHA-256: 7df7dab4613062227d4043afa32bd42a35669f0e23d63512c8754cf057303156

w.exe

MD5: 2879058452ff1a5c7607ae9d0d42aa2e

SHA1: 252a3417d41a2df9e4e9e877388f518d6f19781a

SHA256: 46018fbcf205ace11c502a5cec83c19c69d3849c2bf99cb977e8ab8de905a5d4

Изделие 170 габаритный чертеж.PDF.exe

MD5: 79ddb58bd757774607b007a09ba1b664

SHA-1: 3970148591dc727828eb1c459496a6e0f68dd5fd

SHA-256: 944be60b0fbcfb625b47a4ea8064100124d3c0430855da6ec051cd3d494d964b

Конструкторская документация к изделию 170.PDF.exe

MD5: 79ddb58bd757774607b007a09ba1b664

SHA-1: 3970148591dc727828eb1c459496a6e0f68dd5fd

SHA-256: 944be60b0fbcfb625b47a4ea8064100124d3c0430855da6ec051cd3d494d964b

Расчёт.xlsx

MD5: c45c10bb8f3a52d82667c1e0be54d63b

SHA-1: 2e03751d70d570b7de9b2939804638e2feded4f4

SHA-256: 5431bba24dbfca9cbcf31a20dd6c1277eb3b07849a461405468328d567ba48f5

2026 01 Решение 2Д212.doc

MD5: 7573a316430480e4301c1c28d4a9af7d

SHA-1: 60b13496b3d8a999972de6b3e55f7fc5732c5a94

SHA-256: 327f383d4ab90cb08efd46d8e8384d0e5d2392f2b5116ae6a477f720862ada70

Перечень КД.xlsx

MD5: 25b0979d43c793d56f28095c8a02dcfe

SHA-1: 55293487ac6e6db25ee62439bee9b47dbb906cfa

SHA-256: e95d9bc6873fde2af82237a682a0fcdf502bd31f3005e8a89f07aae2d820f7f1

Испытания 13.01.doc

MD5: 003063c27efc8ba739632117c4f8fd07

SHA-1: 0bc02de11b887f14ed19e8747232364652816475

SHA-256: 859d93a5053c220d9a33e52df15d7f2f4113e4a23ed74c65d27ea25c079bd0cb

Домены и URL:

hxxp://bitbucket[.]org/mlwranalytics/stephen/raw/main/calc

hxxps://cdn-01.anonfiles[.]wtf/_static/0494edf3-0553-404f-9a43-da7e301b7f2c

[https://cdn-01\[.\]johanclothing\[.\]shop/_static/34d9fb7f-14a1-4825-a00c-79da2c8fb949](https://cdn-01[.]johanclothing[.]shop/_static/34d9fb7f-14a1-4825-a00c-79da2c8fb949)

https://bashupload[.]com/XSkPLv.exe

https://bashupload[.]com/Daerjh.exe

hxxps://dnot[.]sh/

wwwyandex[.]org

© 2003 – 2025 F6 — российский разработчик технологий для борьбы с киберпреступлениями.