

Текст · 14 августа 2024, 12:11

Александр Бородихин,

## Подмена писем и шифрованные PDF. Citizen Lab и Access Now рассказали, кто и как охотится на оппозиционеров из России (и как себя обезопасить)

С прошлого года российские активисты и сотрудники международных НКО, чья работа связана с Россией, подвергались масштабной фишинговой атаке. Совместное расследование атаки выпустили [Citizen Lab](#) при Университете Торонто и американская организация [Access Now](#). Они пишут, что хакеры, связанные с ФСБ, рассылали подставные письма с якобы рабочими файлами, представляясь знакомыми и коллегами жертв, чтобы те доверились письмам, подогнанным под известную (или предполагаемую) историю общения, и передали злоумышленникам данные своих почтовых аккаунтов. «Медиазона» коротко пересказывает, как ломали правозащитников и как можно уберечься от подобных атак.

---

Интернет-фишинг, то есть рассылка писем с подложных адресов в попытке заполучить личные данные или деньги жертвы, — метод старый, как сам интернет. При этом по сочетанию эффективности и дешевизны исполнения он по-прежнему лидирует: число сервисов, которыми люди пользуются ежедневно, постоянно растет, проверять все подряд сообщения и письма становится невмоготу, а «разводы» становятся все изощреннее. Впрочем, одно дело, когда мы говорим о финансовом фишинге, когда данные жертвы крадут в обход

закона, а другое — когда фишингом занимается само государство.

Исследователи из *Citizen Lab* при канадском Университете Торонто совместно с американской организацией *Access Now* изучили масштабную кампанию таргетированного фишинга, направленную на активистов и сотрудников НКО, деятельность которых неужодна российским властям. Исследование было проведено при участии [«Первого отдела»](#), *Arjuna Team*, *Resident.ngo* и других некоммерческих организаций.

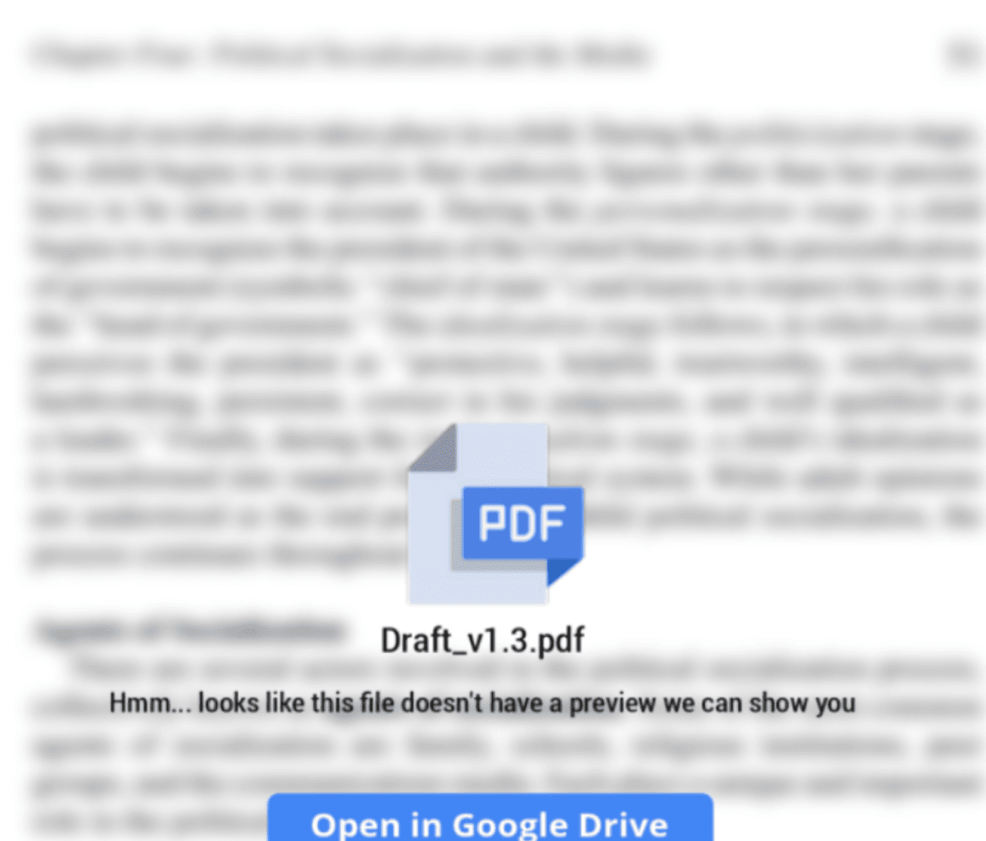
У этой атаки было три вектора, и не совсем понятно, как именно они были связаны между собой.

## Письма со знакомых почт с подменой буквы

**2022–2023.** Осенью 2022 года жертвы начали получать электронные письма от сотрудника «известной российской общественной организации», вроде как «по работе» или в продолжение прошлых встреч. Сами письма были оформлены так, чтобы жертва не заметила подмены: хакеры писали с адресов, которые всего на одну букву отличались от настоящих. Сам человек, от имени которого рассылались письма, при этом тоже стал жертвой фишинговой атаки и вовсе потерял доступ к своей электронной почте.

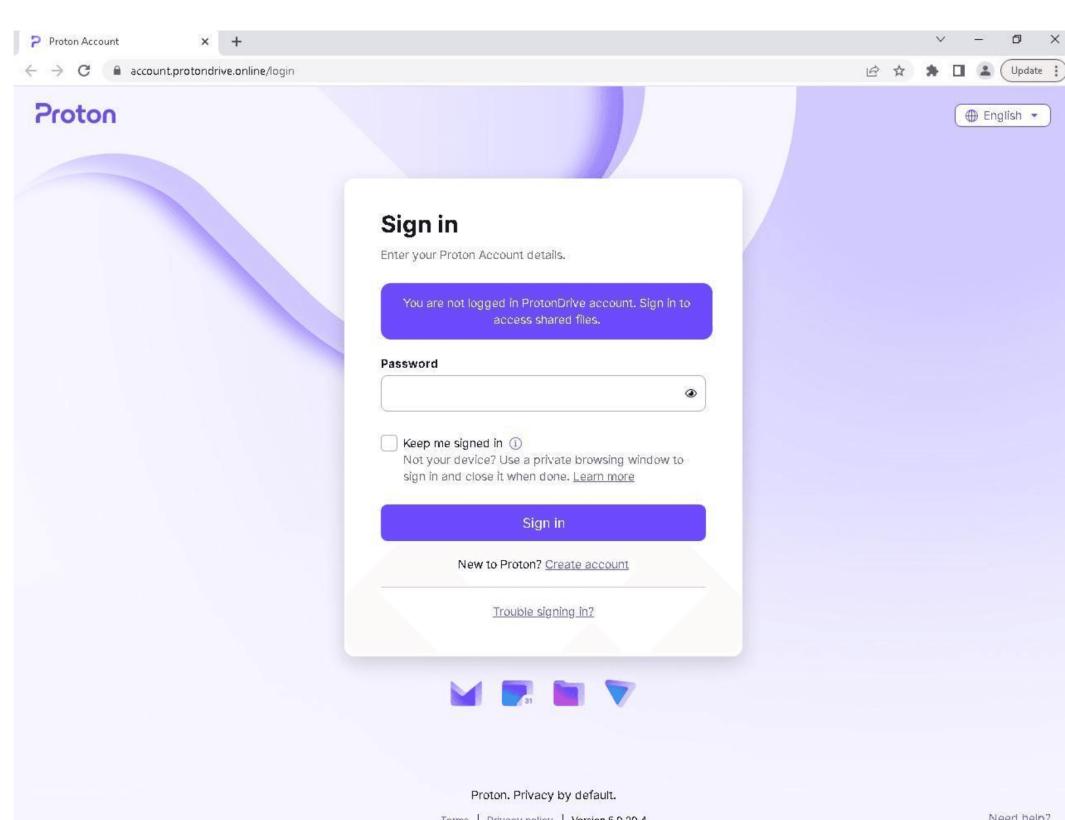
Какое-то время эти попытки взлома некому было собрать воедино: расследование *Access Now* и *Citizen Lab* началось в марте 2023 года,

когда правозащитники из российского «Первого отдела» рассказали специалистам по безопасности о странной фишинговой атаке. Жертвам рассылали *PDF*-файлы, при попытке открыть их пользователя перебрасывало на подменную логин-страницу в *ProtonMail* или *ProtonDrive* с фейковым адресом типа *protondrive[.]online* — там от них требовалось ввести логин и пароль.



Образец предварительного просмотра PDF-файла

Хакерам, стоявшим за этой атакой, исследователи дали кодовое название *COLDWASTREL* — «Холодные бродяги» в дословном переводе на русский. На то, что хакеры из России, указывают косвенные, хотя и не стопроцентные свидетельства: в метаданных *PDF*--файлов сохранились данные о московском часовом поясе и русском языке операционной системы создателя.



Образец поддельной страницы входа в ProtonMail

## Хакеры тщательно маскируются под реальных собеседников

**Первая половина 2024-го.** Более масштабная и сложная по исполнению атака началась в 2024 году: в апреле — июне злоумышленники активно применяли методы социальной инженерии, маскируясь под знакомых своих жертв. Ссылки в рассылаемых *PDF*-файлах содержали скрипты, которые собирали информацию с устройства жертвы, чтобы залогиниться на фейковой странице могла только конкретная жертва; для затруднения исследований хакеры также приняли меры для минимизации следов в файлах.

Жертвами атак стали российские и белорусские НКО и независимые СМИ. Эксперты из *Citizen Lab* приписывают эту кампанию российской хакерской группировке *COLDRIVER*, также известной под кодовыми обозначениями *Star Blizzard*, *Callisto* и другими. Эту группу [США](#) и [Великобритания](#) считают связанной с Центром информационной безопасности (ЦИБ) ФСБ.

### «Шалтай-Болтай» и ЦИБ ФСБ

В 2014 году хакерская группа «Анонимный интернационал» (также известная как «Шалтай-Болтай» по аватарке в твиттере) взломала твиттер-аккаунт премьер-министра Дмитрия Медведева. Через несколько дней группа опубликовала содержимое нескольких почтовых ящиков Медведева — его заказы из зарубежных интернет-магазинов впоследствии легли в основу расследования «Он вам не Димон» Алексея Навального.

За свою [недолгую историю](#) группа выложила также переписку замглавы управления внутренней

политики администрации президента Тимура Прокопенко, вице-премьера Аркадия Дворковича, главы Роскомнадзора Александра Жарова и владельца холдинга **News Media** Арама Габрелянова.

В 2016 году предполагаемого лидера группы Владимира Аникеева арестовали, и он, по утверждению источника «Росбалта», дал «развернутые показания, в которых неоднократно упоминался [начальник 2-го управления ЦИБ ФСБ-] Сергей Михайлов — как лицо, связанное с командой». Михайлов был задержан в том же 2016 году по обвинению в госизмене. При этом в интервью «Би-би-си» в феврале 2019 года вышедший на свободу Аникеев отрицал связи с ФСБ и утверждал, что группа действовала автономно. «Коммерсант» утверждал, что, по версии следствия, Сергей Михайлов и другие сотрудники ЦИБ ФСБ передали ФБР информацию о гендиректоре компании **Chronopay** Павле Врублевском, которого власти США считают причастным к кибератакам. Сергей Михайлов в 2019 году был приговорен к 22 годам лишения свободы.

**Август 2024-го.** Незадолго до выхода расследования, уже в текущем августе, *COLDWASTREL* объявился вновь, рассылая *PDF*-файлы со ссылками на *protondrive[.]me* и *protondrive[.]services*. Об этом *Access Now* сообщила одна из организаций, которую уже пытались взломать прежде. В *Citizen Lab* считают, что эта группа хакеров отличается от *COLDRIVER*, потому что технически атака организована иначе, несмотря на сходство в подборе списка жертв.

## Как можно себя обезопасить

Связанные с властями взломщики использовали и будут использовать фишинговые методы, потому что они работают, даже несмотря на наличие в их арсенале более совершенных технических возможностей (тех же эксплойтов «уязвимостей нулевого дня», которые используются в разработках типа израильского *Pegasus*). Пока риск обнаружения остается низким, светить более дорогостоящие инструменты необязательно.

«Российские власти будут продолжать преследовать людей, которые, по их мнению, представляют угрозу, независимо от того, где они находятся», — уверена Ребекка Браун, старшая исследовательница из *Citizen Lab*. По ее словам, «в *COLDRIVER* было внесено достаточно технических изменений - , чтобы оставаться незамеченными в течение продолжительного времени и продолжать работу».

Полностью обезопасить себя от получения таких писем невозможно. Журналистам, правозащитникам и сотрудникам организаций, хоть как-то связанных с Россией, остается лишь соблюдать базовые правила безопасности.

**1. Настройте двухфакторную аутентификацию.** Да, хакеры из *COLDRIVER* и *COLDWASTREL* могут обманом вынудить жертву ввести код, но это первый, самый базовый шаг. Для организаций в зоне риска у почтовых сервисов есть специальные программы по усиленной защите от подложных имейлов.

**2. Проверяйте все адреса входящих писем.** Получили письмо, которого не ждали, — скопируйте его адрес и проверьте, была ли уже с ним переписка. Нет? Тогда есть смысл уточнить у самого человека, отправлял ли он вам письмо, — разумеется, не в почте, а другим способом.

**3. Не открывайте ссылки.** У *Google* и *Microsoft* есть встроенные просмотрщики, они покажут *PDF*-файлы без загрузки содержимого. Но если вы внутри документа кликнете по потенциально опасной ссылке, защитить вас эти компании уже не смогут.

**4. Не логиньтесь нигде, кроме сайта самой почты.** Перебросило на логин-страницу? Закройте.

**5. Используйте менеджеры паролей.** Они безопасно хранят сложные пароли и могут вводить пароли автоматически, проверяя, что форму запрашивает подлинный сайт.

**6. Видите «превью зашифрованного *PDF*»? Такого не бывает, не открывайте.**

**7. Думаете, что вас пытаются взломать?** Свяжитесь с [\*Access Now\*](#), там помогут подтвердить или опровергнуть ваши подозрения.