МИР

Грозит 10 лет тюрьмы. Россиянин подозревается в кибератаках в ЕС и США

Майк Экель

2 часа(-ов) назад

Приоритетный источник в Google

Денис Обрезко работал в ФСБ и Министерстве по чрезвычайным ситуациям РФ

В сентябре 2024 года голландские эксперты по кибербезопасности обнаружили, что кто-то проник в компьютерные системы Национальной полиции Нидерландов и получил доступ к электронной почте одного из сотрудников. Злоумышленник или группа злоумышленников использовали украденный файл cookie (фрагмент данных, который временно сохраняют веб-браузеры на устройстве пользователя) для доступа к электронной адресной книге.

Злоумышленник таким образом получил доступ ко всем контактам в электронной почте сотрудника полиции, а возможно и к контактам всех 64 тысяч сотрудников ведомства, не говоря уже о потенциальных именах источников или информаторов, с которыми полиция работает.

"Нидерланды впервые стали жертвой целенаправленного кибersаботажа со стороны группы, поддерживаемой Россией", – сообщила в своем отчете военная разведка страны. Группа, позже названная Laundry Bear, "продемонстрировала немалую эффективность".

"Этот случай вызвал резонанс в СМИ, и, следовательно, значительное беспокойство законодателей, сотрудников спецслужб и широкой общественности Нидерландов, – говорит **Барт ван ден Берг**, бывший ведущий аналитик разведки и специалист по кризисному управлению в Национальном центре кибербезопасности Нидерландов. – Это был чувствительный вопрос".

6 ноября прошлого года 35-летний программист Денис Обрезко из Самарской области был задержан полицией Таиланда на основании ордера на арест, выданного в США. В его гостиничном номере в курортном городе Пхукет полиция изъяла ноутбук, мобильный телефон и электронный кошелек.

На прошлой неделе, примерно через месяц после экстрадиции, Обрезко впервые предстал перед федеральным судом в Бостоне, где он был обвинен во взломах в случае почти дюжины американских компаний и государственных учреждений. Вину он не признал, ему грозит до 10 лет тюремного заключения.

Арест и экстрадиция российских хакеров на основании ордеров США в разных странах мира раньше были обычным явлением. В какой-то момент Кремль даже обвинял США в "охоте" на российских граждан.

В последние пять лет такое стало случаться реже – и это одна из причин, по которой дело Обрезко можно считать нестандартным. Еще одной особенностью является то, что Обрезко ранее работал в Федеральной службе безопасности РФ. А частная компания, в которой он работал на момент предполагаемых взломов, по некоторым данным, была связана с другим бывшим сотрудником ФСБ.

Возможно, Обрезко проявил неосторожность, считает ван ден Берг: "О чём он думал, отправляясь в Таиланд? Когда находишься за пределами России, есть риск быть арестованным. Видимо, что-то пошло не так в случае российских расчетов. Или он недооценил западные спецслужбы. Или переоценил свою защиту [со стороны российского государства]".

"Господин Обрезко заявил о своей невиновности и намерен активно защищаться в суде как с юридической, так и с фактической точки зрения, – сказал адвокат

Максим Немцев. - Поскольку дело находится на рассмотрении, мы не считаем уместным обсуждать факты в прессе".

Местный бизнес

Приблизительно за три года до взлома системы полиции Нидерландов, Фонд борьбы с коррупцией, основанный российским оппозиционером Алексеем Навальным, сообщил, что были похищены более полумиллиона адресов электронной почты, использовавшихся для регистрации на сайте "Свободу Навальному!". Многие из тех, чьи адреса были в этой базе данных, позже сообщили о получении сообщений с угрозами. Тогда к случившемуся якобы были причастны не хакеры, а бывший сотрудник организации, как объяснили в ФБК.

Согласно документам американского суда, Обрезко был заместителем директора компании "ЮТЕК", к работе которой он присоединился в 2023 году. О том, что это за компания, говорится в одном из расследований, проведенном в 2021 году журналистами телеканала "Настоящее Время". По цифровым следам тогда удалось установить, с каких адресов электронной почты рассылались угрозы сторонникам Навального из украденной базы данных. Один из адресов был привязан к ряду фиктивных доменов, использовавшихся, например, для дискредитации самарского онлайн-издания "Засекин".

Домены, как выяснилось, были связаны с бизнесменом Михаилом Дудиным, который, по имеющимся данным, сотрудничал с бывшим сотрудником ФСБ из этого региона Павлом Селезневым. Ни у Дудина, ни у Селезнева комментарии получить не удалось. При этом имя Дудина фигурирует в базе данных, используемой приложением GetContact – популярным сервисом, помогающим пользователям фильтровать телефонные звонки. Приложение позволяет проводить перекрестный поиск по номеру телефона, сопоставляя его с другими номерами и именами учетных записей.

Как выяснило "Настоящее Время", аккаунт Дудина в приложении GetContact зарегистрирован под ником "Итан Хант" – это отсылка к главному герою сериала "Миссия невыполнима".

Одна из компаний Дудина называлась ООО "ЮТЕК-НН". Она позиционирует себя как компанию, использующую "передовые технологии, инновационные концепции и креативный дизайн". Фирма имела лицензию на продажу специализированного технического оборудования, предназначенного для скрытого сбора информации; такая лицензия обычно выдается ФСБ.

По поручению российского правительства

Согласно информации в аккаунте в российской социальной сети "ВКонтакте", Обрезко окончил Московский технический университет имени Баумана, который называют "кузницей" государственных хакеров. Согласно документам ФБР, обнародованным для процедуры экстрадиции, до прихода в "ЮТЕК" Обрезко работал в ФСБ (с 2012 по 2017 год). Какие именно функции он там выполнял, остается неясным.

Как сообщает Reuters, до прихода в МЧС России Обрезко работал в "Лаборатории Касперского", компании-разработчике антивирусного программного обеспечения; в 2021 году он выступил в качестве приглашенного докладчика на мероприятии, организованном Московским техническим университетом связи и информатики. Его представили как заместителя директора информационно-аналитического центра (ИАЦ) МЧС России.

В 2021 году Денис Оберзко (второй справа) выступил в Московском техническом университете связи и информатики. Его представили как сотрудника МЧС

В июне и июле 2024 года, до того, как стало известно о хакерской атаке на полицию Нидерландов, ФБР получило уведомление из частного сектора в США – предположительно, речь шла о компании Microsoft – о том, что объектами нападений стали американские и европейские компании, а также государственные учреждения.

Согласно показаниям, сотрудники компании "ЮТЕК" скопировали электронные письма "различных правительственных ведомств по всей Европе, являющихся партнерами НАТО, а также других организаций, поддерживающих продолжающееся сопротивление Украины российскому вторжению". ЮТЕК "проводил эти операции по кибершпионажу по поручению российского правительства".

Согласно документам, следователи ФБР отследили путь поддельных электронных писем к набору адресов электронной почты, а затем обнаружили связь ряда транзакций, совершенных в 2024 и 2025 годах, с криптовалютой. Одна из транзакций вела к интернет-провайдеру в Самаре.

В конечном итоге следователи заявили, что один из адресов электронной почты, использовавшийся для транзакций с криптовалютой, был напрямую связан с еще одним почтовым ящиком Google, зарегистрированным на настоящее имя Дениса Обрезко.

> **“ Правительство Нидерландов публично обозначило хакеров как "российскую хакерскую группу, поддерживаемую государством"**

Этот же почтовый ящик Google использовался для регистрации нескольких аккаунтов в социальных сетях, в том числе в X и Instagram, а также учетной записи в PayPal, где был указан тот же номер мобильного телефона, что и был идентифицирован как принадлежащий Обрезко. Там же была указана и дата его рождения. Тот же логин и фотография использовались еще для нескольких аккаунтов в социальных сетях, в том числе в Instagram.

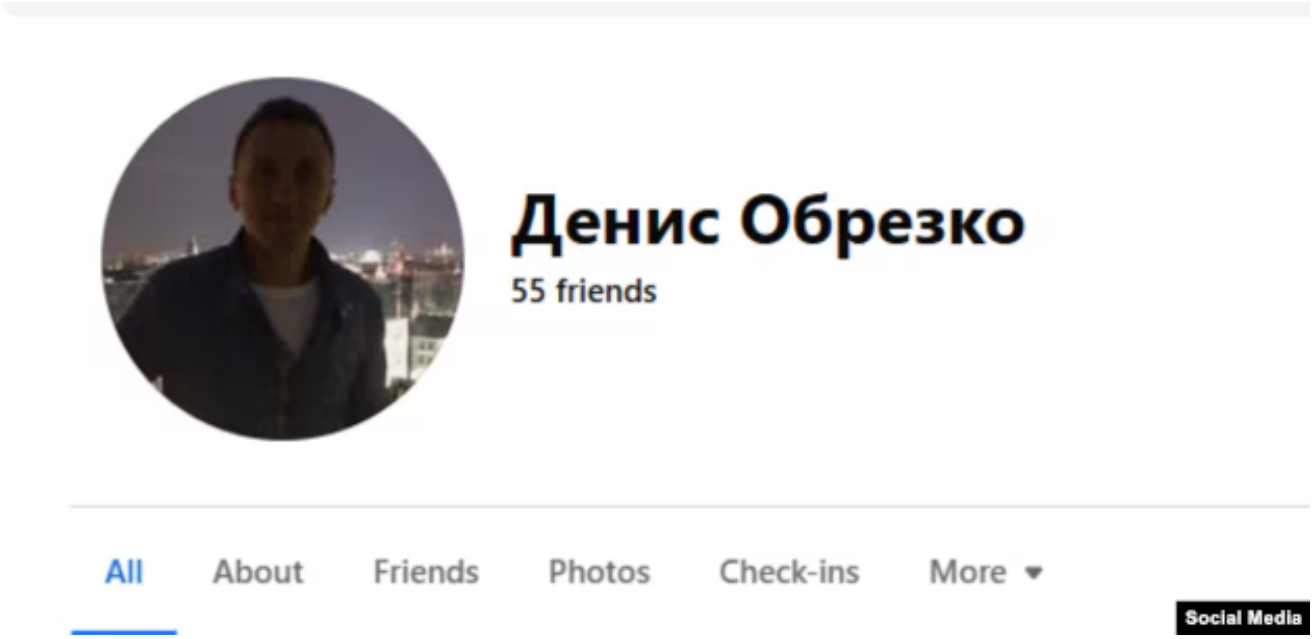
27 мая 2025 года правительство Нидерландов публично обозначило хакеров как "российскую хакерскую группу, поддерживаемую государством", назвав ее Laundry Bear. В отчете Microsoft, опубликованном в тот же день, эта группа была названа Void Blizzard. При этом ни в отчете Нидерландов, ни в отчете Microsoft не указаны конкретные лица или даже конкретные компании, причастные ко взлому.

Через несколько часов после публикации отчета Microsoft, согласно данным ФБР, Обрезко отправил электронное письмо "Итану Ханту", которого ФБР называет "неустановленным соучастником", – с предложением встретиться позже в тот же день.

По словам **Александра Лесли**, старшего советника американской организации по кибероборонe Recorded Future, Обрезко допустил ошибку, повторно использовав

одно и то же имя пользователя и свой российский номер мобильного телефона для разных учетных записей – электронной почты и для социальных сетей. "Похоже, ФБР не вычислило его благодаря одной катастрофической ошибке. Следователи постепенно собрали цепочку взаимодополняющих доказательств, основанную на ряде мелких оперативных ошибок", – говорит Лесли.

"Хакер может быть чрезвычайно эффективен в получении доступа, краже информации и уклонении от обнаружения, – отметила Лесли, – но при этом менее эффективен в сокрытии своей личности в ходе длительного контрразведывательного расследования".



Скриншот страницы профиля Дениса Обрезко в Facebook

Охота на хакеров

Неясно, чем именно занимался Обрезко в Таиланде, он прибыл туда 31 октября прошлого года.

До 2021 года аресты российских граждан, подозреваемых в совершении киберпреступлений, на основании материалов, собранных в США, происходили регулярно по всему миру. Москва в то время публично выражала несогласие с этими действиями.

В октябре 2016 года россиянин Евгений Никулин был арестован во время попытки въехать в Чехию. Разыскиваемый за организацию взлома социальной сети LinkedIn, Никулин в 2020 году был приговорен к семи годам лишения свободы в США, а три года спустя депортирован в Россию.

В марте 2021года в Швейцарии был арестован Владислав Клюшин, IT-предприниматель, связанный с Кремлем, которому предъявили обвинение в причастности к схеме незаконной торговли акциями с использованием взлома чужих компьютеров. Американские власти установили его связь с офицером российской военной разведки, который обвинен во взломе компьютеров Демократической партии в 2016 году. Приговоренный к девяти годам лишения свободы, Клюшин был освобожден в 2024 году и возвратился в Россию в рамках крупного обмена заключенными, в который были включены американцы, содержавшиеся в российских тюрьмах.

В 2021 году стало известно о серии кибератак с использованием программ-вымогателей – хакеры с помощью вредоносных вирусов блокировали компьютерные системы, а затем требовали выкуп в обмен на деблокирование систем. Нападениям подверглись больницы, компании-разработчики программного обеспечения, мясоперерабатывающие предприятия и другие компании в США. Американские власти заявили, что программой-вымогателем под названием REvil управляли из России.

После того, как в июле 2021 года президент Джо Байден напрямую призвал российского президента Владимира Путина принять меры по решению этой проблемы, ФСБ провела масштабные рейды против предполагаемых членов хакерской группы в Москве и других городах. Ведомство заявило, что эти действия были предприняты по просьбе властей США.

По мнению экспертов и следователей, постоянные проблемы с российской киберпреступностью обусловлены размытостью границ между преступными группировками и спецслужбами, такими как ФСБ.

"Для западного мышления типично представление, что между сферой государства и сферой преступности существует четкое разграничение. Но в России это не так", – говорит ван ден Берг.

По словам западных экспертов, российские киберпреступники, как правило, исходят в своих действиях из того, что, пока они не нацелены на физических лиц, компании или государственные учреждения в России, у них есть полная свобода действий.

В случае с кибератакой на Нидерланды, поясняет ван ден Берг, обычный киберпреступник мог бы попытаться вымогать деньги у жертвы, шантажировать ее или попытаться совершить какую-либо коммерческую сделку. Но в данном случае так не происходит: "Мы имеем дело с преступным нападением или с бизнес-моделью? Поскольку суть бизнес-модели неясна, можно задаться вопросом:

кто платит этому человеку? – говорит эксперт. – Он продает похищенные данные государству или работает непосредственно на него? Если окажется, что дело обстоит именно так, то это означает, что государство в той или иной степени к этому причастно".

Этот контент также в категориях

В России | Выбор Свободы | Мир