Как любопытство абонента и статья на “Хабре” обрушили сеть питерского провайдера

Удивительная история то ли о человеческой глупости, то ли о банальном разгильдяйстве произошла в Санкт-Петербурге на минувшей неделе. Любопытный и очень дотошный житель Северной столицы с помощью нехитрых манипуляций обрушил сеть одного из крупнейших интернет-провайдеров Санкт-Петербурга SkyNet. О том, как это произошло пользователь рассказал лично на страницах Pikabu.ru. Пост, поднявший уйму хайпа, затем с портала исчез, но доступен в архивах.

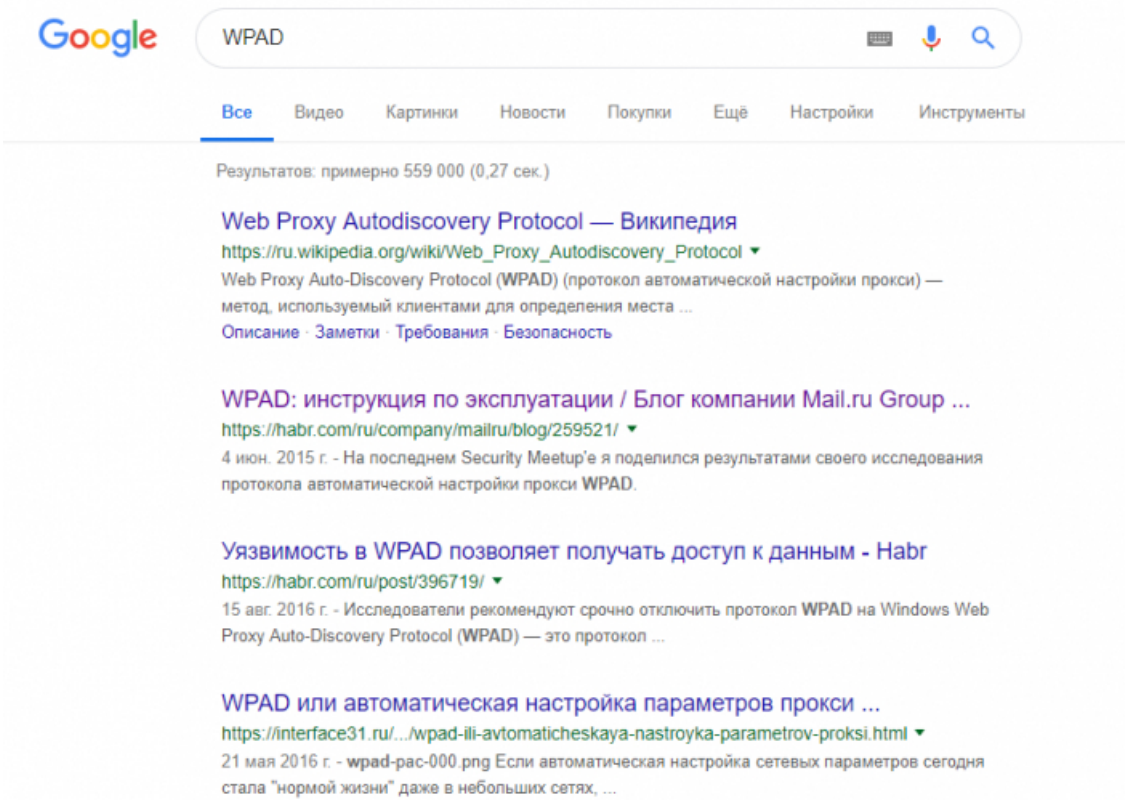
По словам нашего героя, в один прекрасный день он устал постоянно вводить IP-адрес, чтобы удаленно попасть на собственный роутер, и поэтому решил обзавестись доменным именем.

> "Оказалось, что у моего провайдера есть услуга по предоставлению субдоменного имени. Я решил, что это хорошее предложение и завел субдомен wpad.sknt.ru. После чего сразу, как только подключение осуществилось, стали происходить зависания интернета, роутер стал перезагружаться. Я полез в логи роутера и обнаружил, что на него идет GET-запрос с требованием предоставить файл wpad.conf. Что это такое?", – пишет герой истории.

Позже любопытный абонент нашел в Википедии статью, посвящённую технологии WPAD, которая автоматически предоставляет настройки прокси.

> "Поняв, что такого потока запросов (около 100 запросов в секунду) мой роутер не выдержит, я через личный кабинет отключил услугу, но это не помогло - услуга по-прежнему работала, запросы сыпались, роутер пыхтел и перезагружался периодически. Тогда я позвонил провайдеру и попросил, чтобы услугу по предоставлению субдомена отключили. Причина: всё висит, и интернет работает через одно место. Они сказали, что не могут вернуть деньги за неиспользованную услугу. Я отказался от денег и попросил в любом случае отключить мне этот субдомен. Девушка на том конце провода сказала, что услугу она отключила", – пишет пользователь.

Однако, даже спустя полчаса ситуация не изменилась, а на роутер по-прежнему поступало 100 запросов файла wpad.conf в секунду. Недолгие поиски в интернете привели нашего героя на интернет-ресур habr.com, где в подробностях были изложены уязвимости в технологии WPAD.



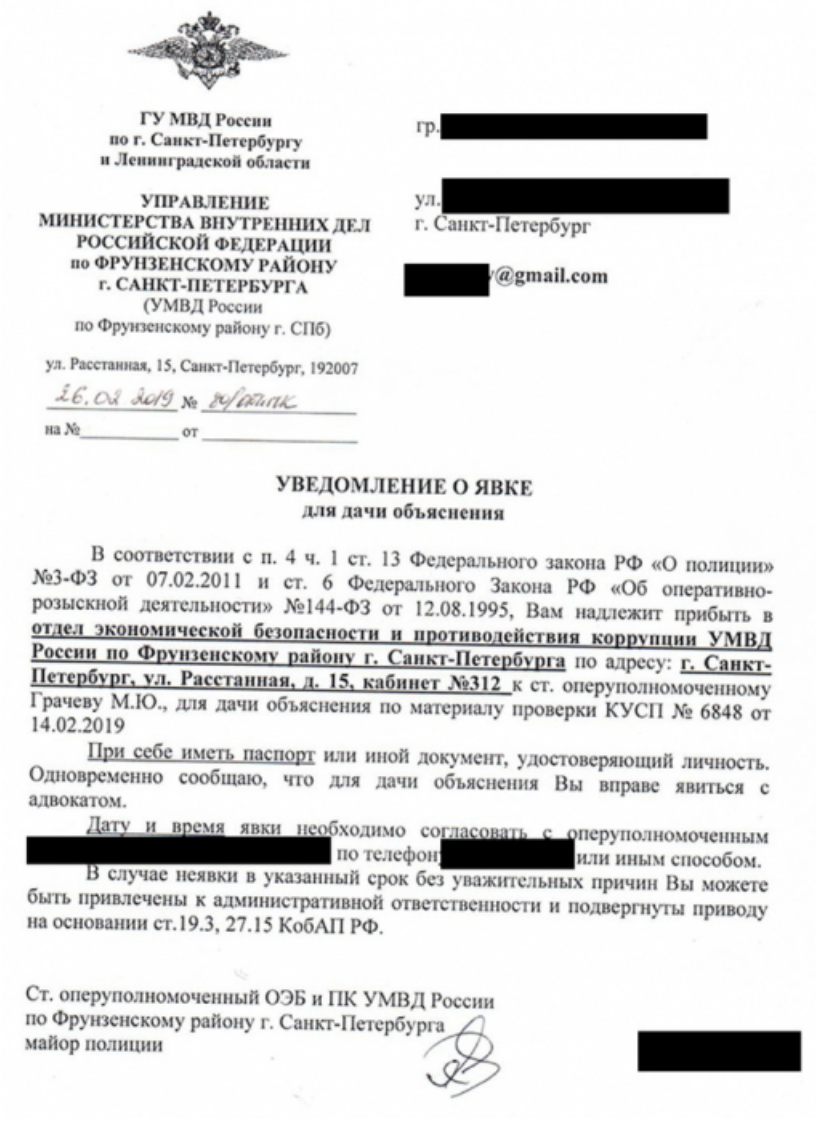
Про найденную уязвимость мужчина сообщил собственному провайдеру SkyNet по телефону, однако там попросили, чтобы о находке он сообщил на почту компании. В своем письме любопытный юзер сообщил компании об уязвимости, намекнув, что хотел бы получить за находку финансовое вознаграждение.

Но, даже спустя трое суток, никакой реакции от представителей SkyNet не последовало. Услуга же субдомена продолжала работать, в отличие от роутера и интернета. Такое положение вещей нашему герою надоело, и он решил действовать.

> "В общем, тогда я решил создать файл wpad.conf с настройками, ведущими в никуда, чтобы на мою проблему обратили внимание. Ага, обратили внимание уже через два часа! У меня полностью пропал интернет, вообще тишина была. Если до этого худо-бедно, через раз и открывались сайты, то теперь вообще глухо. Кое-как я пробился до техподдержки, а мне сказали "это же вы нашли уязвимость? Ну, вот мы вас и отключаем навсегда!", и повесили трубку", – рассказывает мужчина.

Спустя некоторое время, он вновь созвонился с провайдером и еще раз разъяснил им свою позицию об уязвимости. Представители SkyNet его внимательно выслушали, однако расторжение договора оставили в силе. По словам абонента, он просто сменил провайдера, а его "роутер наконец вздохнул с облегчением".

И вроде бы, на этом история должна была закончиться хэппи-эндом со счастливым абонентом, у которого нормально работает интернет, и провайдером, исправившим уязвимость в собственной сети. Однако, спустя три недели герою этой истории на почтовый ящик пришла повестка из Отдела экономической безопасности и противодействия коррупции городского УМВД.



ГУ МВД России
по г. Санкт-Петербургу
и Ленинградской области

УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по ФРУНЗЕНСКОМУ РАЙОНУ
г. САНКТ-ПЕТЕРБУРГА
(УМВД России
по Фрунзенскому району г. СПб)

ул. Расстанная, 15, Санкт-Петербург, 192007

26.02.2019 № 80/ОПИК

на №_____ от _____

гр. [redacted]

ул. [redacted]
г. Санкт-Петербург

[redacted]@gmail.com

УВЕДОМЛЕНИЕ О ЯВКЕ
для дачи объяснения

В соответствии с п. 4 ч. 1 ст. 13 Федерального закона РФ «О полиции» №3-ФЗ от 07.02.2011 и ст. 6 Федерального Закона РФ «Об оперативно-розыскной деятельности» №144-ФЗ от 12.08.1995, Вам надлежит прибыть в **отдел экономической безопасности и противодействия коррупции УМВД России по Фрунзенскому району г. Санкт-Петербурга** по адресу: **г. Санкт-Петербург, ул. Расстанная, д. 15, кабинет №312** к ст. оперуполномоченному Грачеву М.Ю., для дачи объяснения по материалу проверки КУСП № 6848 от 14.02.2019

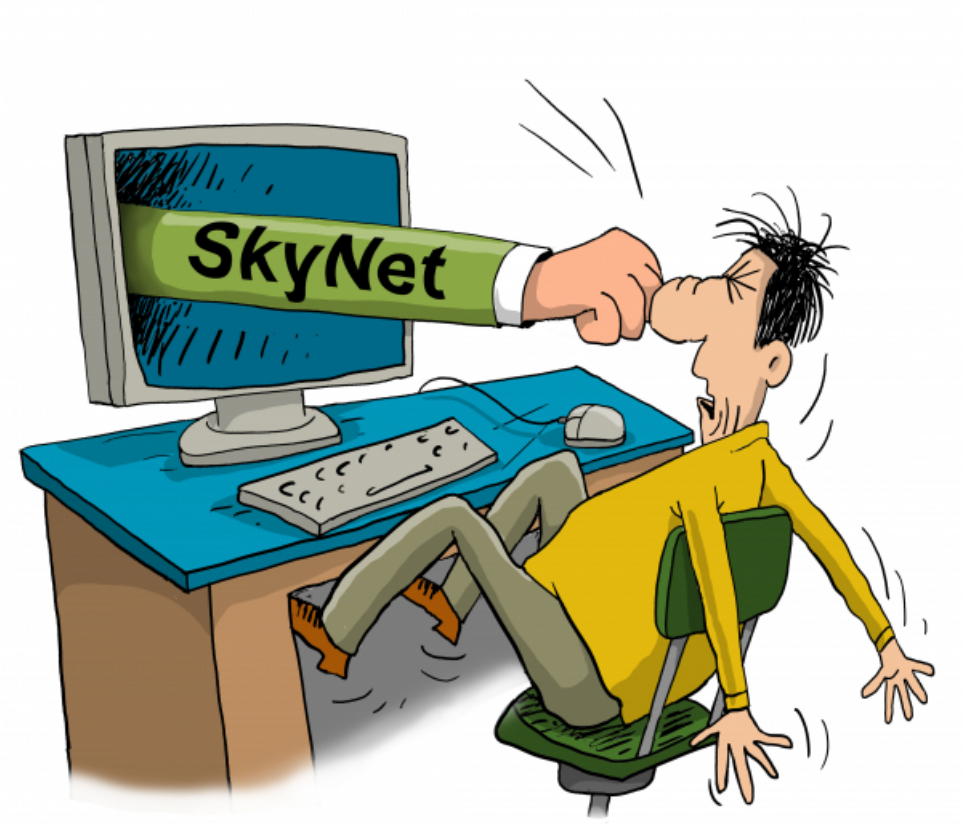
При себе иметь паспорт или иной документ, удостоверяющий личность. Одновременно сообщаю, что для дачи объяснения Вы вправе явиться с адвокатом.

Дату и время явки необходимо согласовать с оперуполномоченным [redacted] по телефон [redacted] или иным способом.

В случае неявки в указанный срок без уважительных причин Вы можете быть привлечены к административной ответственности и подвергнуты приводу на основании ст.19.3, 27.15 КобАП РФ.

Ст. оперуполномоченный ОЭБ и ПК УМВД России
по Фрунзенскому району г. Санкт-Петербурга
майор полиции [redacted]

Теперь мужчине грозит уголовное дело, а SkyNet также хочет возмещения ущерба в размере 2,6 миллиона рублей.



В сети разразилась полемика на тему, кто же все-таки прав: абонент или провайдер. Одни прямо обвиняют пользователя, который по их мнению действовал с преступным умыслом, а другие удивлены действиями технических специалистов SkyNet, которые пропустили столь очевидную уязвимость.

Например, некоторые эксперты считают, что абонент лукавит, говоря о последовательности совершенных им действий. На их взгляд, она была несколько иной. Сначала он прочитал про WPAD, узнав о возможной уязвимости у провайдеров, которые эту систему не используют. Зарегистрировал субдомен WPAD на свой роутер, чтобы уязвимость создать, и, воспользовавшись ею, обвалил настройки у всех пользователей. А самое главное - оставил все следы, прямо указывающие на него, что точно не свидетельствует о профессионализме. Поэтому у правоохранительных органов все складывается в четкую картину преступления.

Также считает и гендиректор SkyNet Александр Крылов, который в своем комментарии для "Фонтанка.ру" пояснил, что от действий абонента пострадала одна из частей сети и несколько тысяч клиентов. Крылов считает, что мужчина действовал целенаправленно, ведь чтобы обрушить сеть, нужно было создать специальный файл с четкими настройками в нем, а после положить документ на специальный домен.

> "Это четкие, направленные действия. Если бы это можно было сделать случайно, конечно, мы бы не занимались всей этой историей. Но после того, как мы поняли, что это было сделано намеренно, мы решили сразу же обратиться в полицию", – заявил Крылов.

Глава SkyNet подчеркнул, что сумма ущерба, которую компания требует с абонента – это затраты оператора на авральную работу сотрудников, а также компенсации, которые пришлось выплачивать абонентам. Кроме того, после инцидента несколько клиентов попросту расторгли договоры с провайдером.

> "Но это заявление подано не для того, чтобы получить денег и как-то заработать. История не про это, конечно. Действия, которые нарушают работу сети у своих же соседей, коллег и друзей и приводят к таким последствиям, не должны оставаться без ответа", – подытоживает глава SkyNet.

Как считает юрист компании "ОрдерКом" Андрей Медведев, абонента, нашедшего уязвимость в сети провайдера, вряд ли смогут привлечь к уголовной ответственности. Однако сумму ущерба с него, возможно, взыщут, хоть и не полностью.

> "Крайне маловероятно привлечение к уголовной ответственности. Некоторые признаки действий абонента могут совпадать с составом статьи 274 Уголовного кодекса РФ: " Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей". В то же время, данная статья охраняет отношения в сфере информационной безопасности, её могут применять исключительно если действия повлекли: уничтожение, блокирование, модификацию либо копирование компьютерной информации. Такого, исходя из статьи, я не усматриваю.
>
> С другой стороны, между абонентом и оператором был заключён договор об оказании услуг связи, а значит, отношения регулируются и гражданским правом.
>
> Если действия абонента повлекли для оператора убытки, он может обратиться в суд за их взысканием. Убытки, к примеру, за перерыв в оказании услуг связи (перерасчёт для абонентов, может, какие-то абоненты расторгли договор из-за этого), а также за действия

оператора, направленные на восстановление работоспособности сети связи.

При взыскании убытков нужно доказать:

1. что абонент совершил само действие;
2. противоправность действия (действие должно быть запрещено договором или законом);
3. причинно-следственные связи (именно действие абонента повлекло убытки);
4. наступление самих убытков и их размер.

Вина по таким делам презюмируется, пока не доказано обратное.

Исходя из описанного, теоретически требование о взыскании убытков в такой ситуации вполне может быть удовлетворено судом, но оператору нужно очень постараться доказать факт действия абонента, если он будет отрицать его. Наверняка суду потребуется комплексная экспертиза. Не сильно владею технической информацией в данной области, но мне кажется, если абонент будет отрицать факт каких-либо действий, то доказать их оператору будет достаточно сложно.

Наконец, размер ущерба тоже нужно обосновать конкретными расходами (от перерасчёта, факт самого перерасчёта и т.д.), цифры "из головы" суд не удовлетворит.

Резюмируя: оператор точно не виноват в своих убытках. Если получится доказать, что абонент совершил указанные действия и что они стали причиной убытков, оператор вполне может взыскать такие убытки в суде. Далеко не факт, что взыщут всю заявленную сумму.

Абоненту я бы порекомендовал хорошо ознакомиться с технической стороной вопроса, если оператор с достаточной степенью достоверности сможет доказать факт действий абонента - искать юриста, оспаривать противоправность своего действия (может, договор с оператором/закон не предусматривает запрет подобных действий), оспаривать размер убытков. Если доказать оператору самостоятельно не получится, отрицать вообще факт каких-либо действий", – рассказал Андрей Медведев.

Сложно судить, кто в этой истории прав, а кто виноват. Ясно, что абоненту ни в коем случае нельзя было использовать возможность "положить сеть" оператора с помощью, казалось бы, очевидной уязвимости. Это как бить человека, заведомо понимая, что этим его можно убить. С другой стороны, не совсем ясно, чем заняты на своих рабочих местах технические специалисты одного из крупнейших операторов Питера, в чьи обязанности входит обеспечивать стабильную работу сети своих абонентов и их сетевую безопасность.

В любом случае, мы продолжим следить за этой историей.