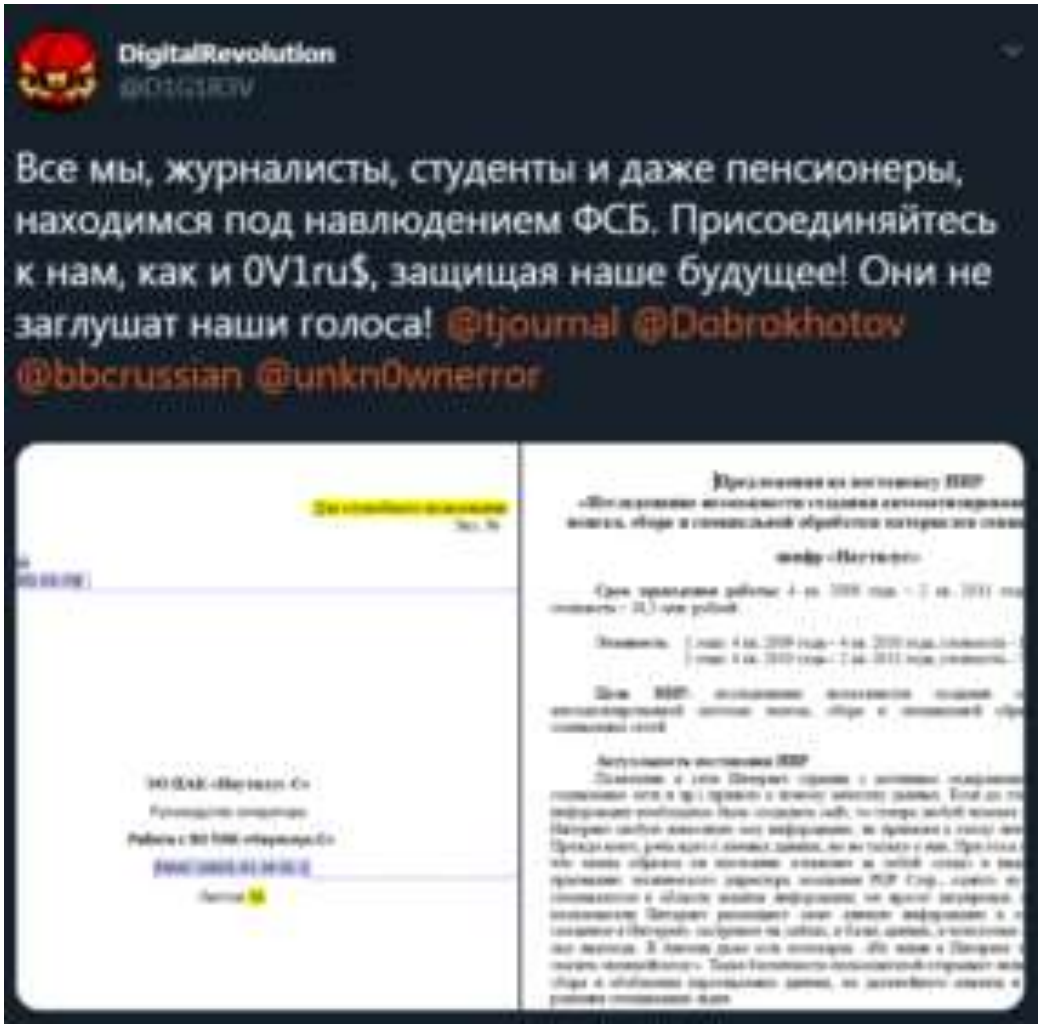
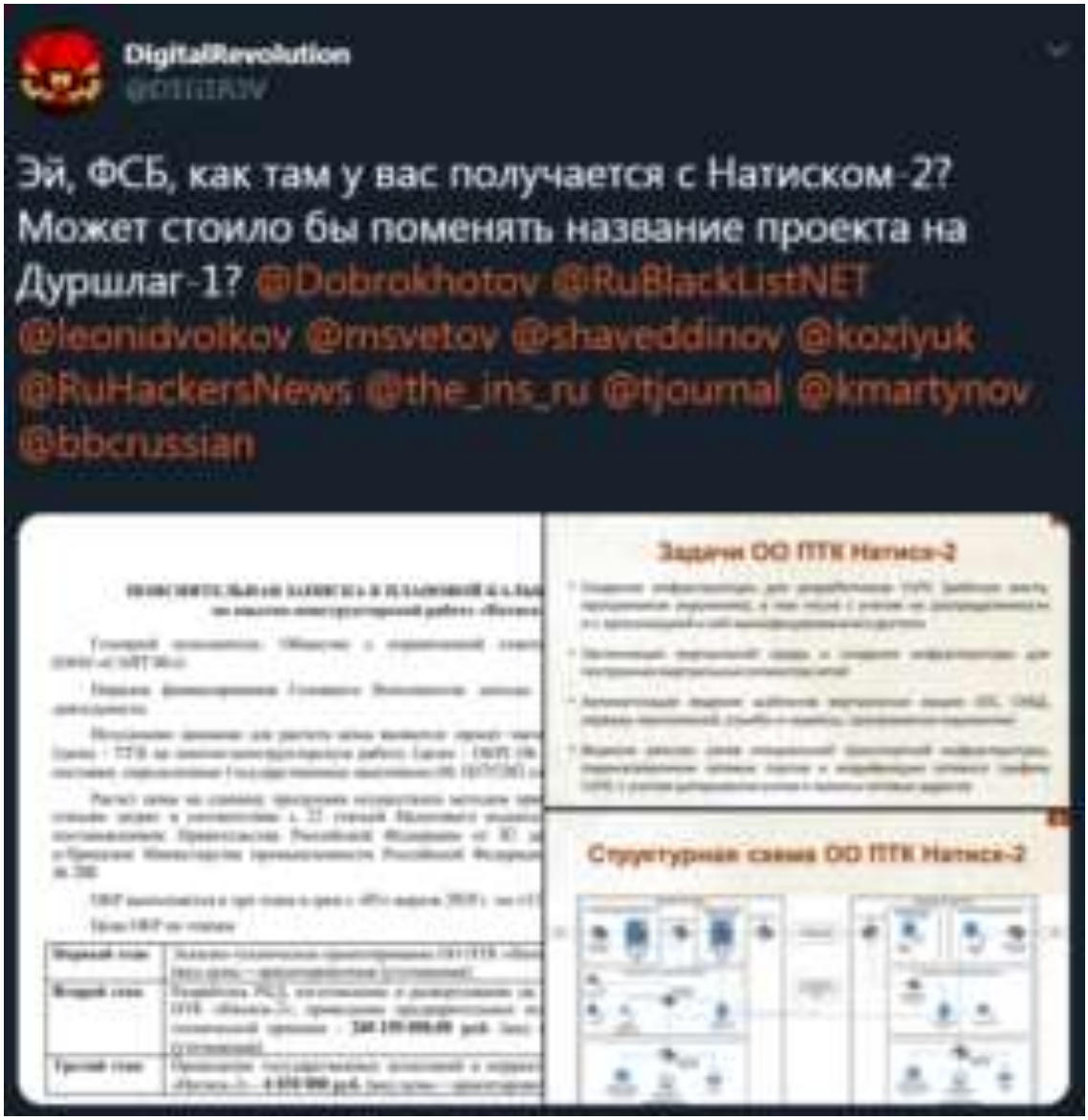
Взломан подрядчик ФСБ, стало известно о проектах по деанонимизации Tor и не только

Мария Нефёдова

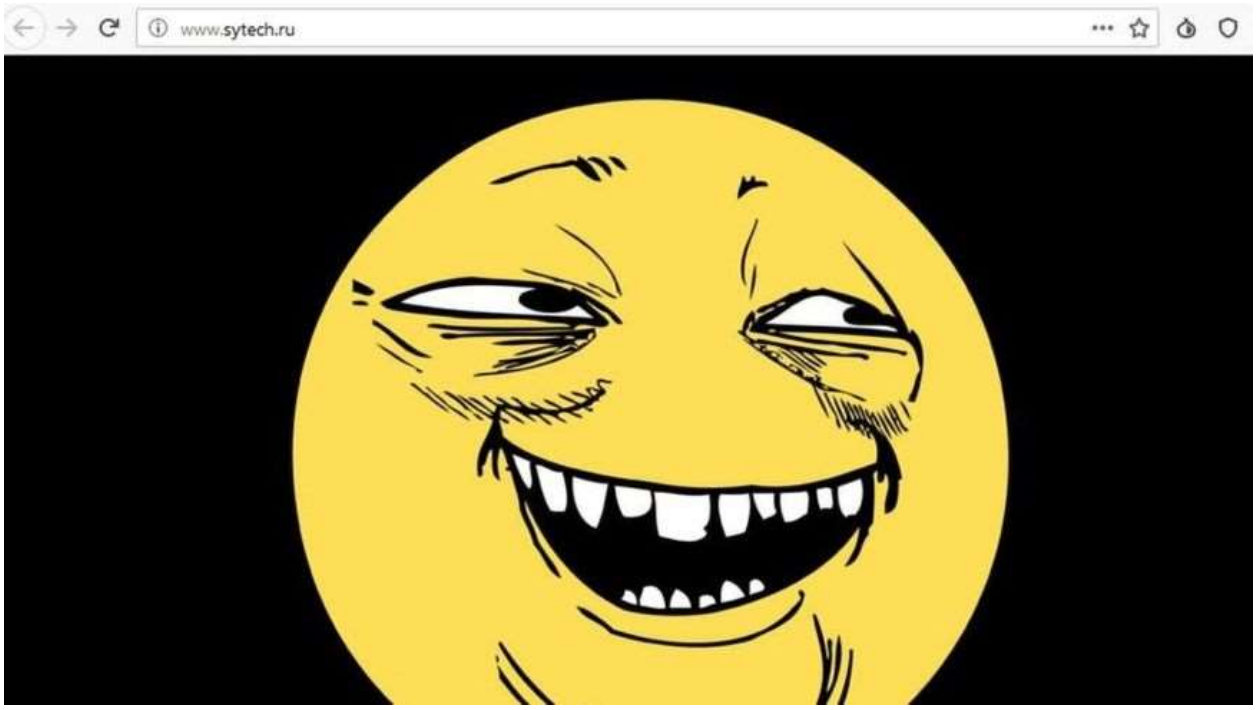
Исочник: https://xakep.ru/2019/07/22/sytech-hack/

В минувшие выходные сразу ряд изданий сообщили о взломе подрядчика ФСБ, московской компании «Сайтэк».
Атакующие, скрывающиеся под псевдонимом 0v1ru$, разместили несколько скриншотов в Twitter (например, скриншоты папки «Компьютер», предположительно принадлежавшей жертве), а также поделились похищенными данными с «коллегами» из группировки Digital Revolution. Те, в свою очередь, тоже опубликовали Twitter ряд доказательств взлома и привлекли к происходящему внимание прессы. Так, в открытый доступ выложили скриншот интерфейса внутренней сети, а рядом с названиями проектов («Арион», «Реляция», «Гривна» и так далее) стояли имена их кураторов, сотрудников «Сайтэк».





Сообщается, что компрометация «Сайтэк» произошла 13 июля 2019 года, и атакующие взломали сервер Active Directory, откуда проникли к сеть компании, в том числе, получив доступ к JIRA. В итоге было похищено 7,5 Тб данных, а сайт подвергся дефейсу, как видно на иллюстрации ниже.



Похищенными у «Сайтэк» документами хакеры поделились с журналистами нескольких изданий, включая «Русскую службу Би-би-си».

Из архива, который оказался в распоряжении издания, следует, что компания выполняла работы по как минимум 20 непубличным IT-проектам, заказанным российскими спецслужбами и ведомствами. Подчеркивается, что бумаги не содержали каких-либо пометок о государственной тайне или секретности.

Также дамп содержал довольно подробное описание проектов «Сайтэк», в числе которых были:

Наутилус-С: главная задача проекта — деанонимизировать пользователей браузера Tor. Разработан в 2012 году по заказу НИИ «Квант». Включает в себя выходной узел Tor, через который и могла осуществляться слежка или даже подмена трафика. Интересно, что в 2014 году похожие атаки уже обнаруживали специалисты из Университета Карлстада, и часть опасных узлов уже тогда связывали с Россией.

Наутилус: создан для сбора информации о пользователях соцсетей. В документах указан срок работ (2009-2010 годы) и их стоимость (18,5 млн рублей). Журналистами не удалось выяснить, нашла ли «Сайтэк» заказчика на этот проект. Следить предполагалось за пользователями Facebook, MySpace и LinkedIn.

Награда: научно-исследовательская работа, которая проводилась в 2013-2014 годы. Изучались «возможности разработки комплекса проникновения и скрытого использования ресурсов пиринговых и гибридных сетей». Заказчик данного проекта в документах не указан. Похоже, специалисты «Сайтэк» планировали найти уязвимость в протоколе BitTorrent, а также компанию интересовали протоколы Jabber, OpenFT и ED2K.

Наставник: заказчиком этого проекта выступала войсковая часть № 71330 (предположительно, радиоэлектронная разведка ФСБ России). Целью «Наставника» был мониторинг электронной почты по выбору заказчика. Проект был рассчитан на 2013-2014 годы. «Наставник» можно было настроить таким образом, чтобы он проверял почту нужных респондентов в заданный промежуток времени или собирал «интеллектуальную группу добычи» по заданным словосочетаниям.

Надежда: проект посвящен созданию программы, которая накапливает и визуализирует информацию о том, как российский сегмент интернета связан с глобальной сетью. Заказчиком работы, проводившейся в 2013-2014 годы, стала все та же войсковая часть № 71330.

Москит: еще один заказ войсковой части № 71330, имевший место в 2015 году. В рамках проекта проводилась исследовательская работа по созданию «программно-аппаратного комплекса», способного анонимно искать и собирать «информационные материалы сети Интернет», скрывая при этом «информационный интерес».

Налог-3: самый «свежий» проект, упомянутый в похищенных документах, датирован 2018 годом. Его заказало АО «Главный научный инновационным внедренческий центр», подчиняющееся Федеральной налоговой службе. Позволяет в ручном режиме убирать из информационной системы ФНС данные лиц, находящихся под госохраной или госзащитой. В бумагах описывается создание закрытого центра обработки данных лиц, находящихся под защитой. К ним относятся некоторые государственные и муниципальные служащие, судьи, участники уголовного судопроизводства и другие категории граждан.