Babr24.com

Автор: Полина Чехова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 3021 08.01.2017, 16:42
18

Есть ли реальные доказательства хакерских атак России на серверы в США?

В конце 2016 года США ввели санкции в отношении российских спецслужб и граждан – якобы за кибератаки. Россия отрицает все обвинения. Тем временем было опубликовано два отчета, посвященных российскому «кибервмешательству» в выборы. Неужели ни в одном из них нет никаких доказательств причастности нашей страны к кибератакам? SmartBabr проанализировал публикует главное из двух докладов спецслужб США.

За что, согласно официальному заявлению американского правительства, введены санкции?

Санкции США стали ответом на «агрессивное преследование российским правительством американских должностных лиц, и на кибероперации, нацеленные на выборы в США в 2016 году», сказано на официальном сайте Белого дома. Первое подразумевает притеснение американских дипломатов в Москве, второе – попытку России повлиять на выборы, *«подорвать веру американцев в демократические институты», «посеять сомнение в целостности избирательного процесса»* и подорвать доверие к правительству США.

Введение санкций за вредоносную киберактивность предусмотрено принятым в апреле 2015 года законом (он применялся лишь раз – в отношении Северной Кореи). Для ответа на «деятельность России» этот закон был **дополнен**. В нем появилось положение, позволяющее вводить санкции против тех, кто «подделывает, изменяет или вызывает незаконное присвоение информации с целью затруднить или подорвать избирательные процессы или институты».

Таким образом, кибератаки сами по себе не являются основным поводом введения санкций. Тем не менее о них очень много говорится. Более того, как 6 января сообщил Reuters, получение якобы исчерпывающих доказательств о причастности России к кибератакам, стало «последней каплей» для введения санкций против нашей страны.

После объявления санкций было опубликовано два официальных документа, описывающих «вредоносную деятельность России».

Какие доказательства содержит первый документ?

В день официального введения санкций в открытом доступе появился совместный отчет ФБР и Министерства внутренней безопасности США. По сообщению Белого дома, этот отчет содержит «техническую информацию о вредоносной кибер-деятельности российских гражданских и военных разведслужб». Цель публикации отчета – «помощь в выявлении, обнаружении и срыве вредоносной кибердеятельности России».

В отчете есть:

абстрактная характеристика действий российских спецслужб, которая в итоге сводится к обвинению во взломе сетей демократической партии США двух хакерских группировок– APT29 и APT28. APT29 и APT28 известны также как Fancy Bear (хакерская группировка с таким названием взяла на себя ответственность за публикацию информации о допинге в американском спорте), COZYBEAR и др.

Рисунок 1. Тактика и техника, используемая APT 28 и APT 29 для кибер-вторжения

описание технологии кражи данных: фишинговая атака, кража паролей, внедрение в сеть, фильтрация почты, закладка возможностей повторного внедрения; повторное внедрение, собственно кража информации, передача этой информации через третьих лиц СМИ.

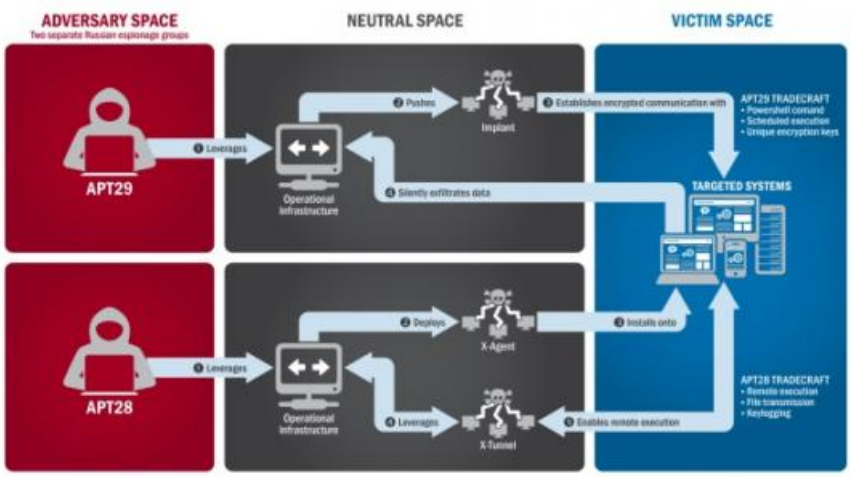

Figure 1: The tactics and techniques used by APT29 and APT 28 to conduct cyber intrusions against target systems

Рисунок 2. APT 28 использует фишинговые атаки и украденные логины и пароли

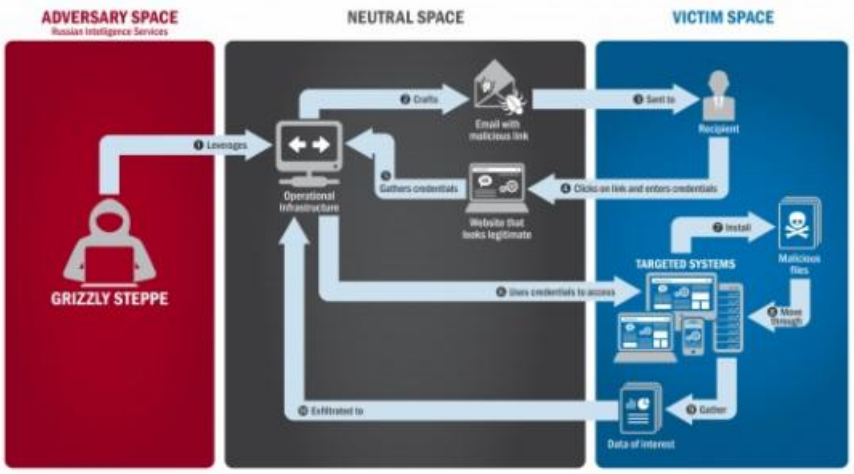

Figure 2: APT28's Use of Spearphishing and Stolen Credentials

файл (в двух форматах) с «индикаторами», позволяющими определить «российских хакеров»: GRIZZLY STEPPE Indicators (CSV). В нем содержатся, в частности, IP-адреса.

описание некоторых используемых хакерами программ.

альтернативные логины и ники якобы работающих на российские спецслужбы хакеров.

Какие доказательства содержит второй документ?

6 января в открытом доступе появился новый отчет под названием «Оценка российской активности и вмешательства в последние выборы». Этот доклад является ограниченной версией засекреченного доклада, который был представлен действующему президенту США Бараку Обаме и избранному президенту Дональду Трампу.

Отчет подготовлен ЦРУ, ФБР и АНБ и опирается на разведывательную информацию, собранную этим тремя организациями. Отчет охватывает «мотивации и намерения Москвы в отношении американских выборов и использования Москвой кибер-инструментов и кампаний в СМИ для влияния на общественное мнение в США».

Прямых доказательств нет и в этом докладе. Он по большей части посвящен общему описанию действий Москвы в попытках «влиять на выборы в США». Собственно кибер-атакам посвещано менее страницы в 25-страничном докладе.

В частности, в докладе утверждается, что:

Президент России Владимир Путин официально утвердил программу поддержки Дональда Трампа. В качестве аргументов приводятся косвенные суждения, основанные на анализе публичных речей Владимира Путина и внешенеполитических действий России. Один из аргументов звучит так: *«Владимир Путин, вероятно, до сих пор "держит зуб" на Хилари Клинтон, за то что она в 2011 году была, по его мнению, организатором беспорядков в России, направленных на свержение путинского режима»*.

В июле 2015 года российские спецслужбы получили доступ к сетям демократической партии и продолжали владеть им до июня 2016 года.

Главное разведовательное управление РФ начало кибер-операцию по выборам в США в марте 2016 года.

Результатом операции ГРУ стала компроментация персонального почтового аккаунта официальных лиц Демократической партии США. В мае ГРУ получила большой объем данных из Демократической партии.

С высокой вероятностью ГРУ использовала персону румынского хакера Guccifer 2.0, а также ресурсы DCLeaks.com и WikiLeaks для публикации полученных в результате атаки данных.

Российские спецслужбы исследуют технические элементы выборной системы США с 2014 года. Совершенные кибератаки не коснулись технологий и оборудования, задействованных в подсчете голосов.

Документ не содержит доказательств, содержит только аргументы.

Являются ли предоставленные доказательства достаточными?

Как следует из описания обоих документов, они не содержат прямых доказательств. Но содержащиеся в первом докладе технические детали и указание во втором докладе на связь с румынским хакером, возможно, являются косвенными доказательствами. SmartBabr обратился к нескольким независимым IT-специалистам чтобы выяснить, можно ли усмотреть в представленных документах доказательства обоснованности обвинений; и какие доказательства обоснованности этих обвинений могут считаться достаточными. Как только ответ будет получен, он будет опубликован.

Официальная позиция России на публикацию этих документов не выражена. Позиция по ситуации в целом неизменна: обвинения признаны недоказанными.

> «Мы считаем эти санкции и решения незаконными и необоснованными. Мы категорически не согласны с такими беспочвенными обвинениями в адрес российской стороны», – сказал 29 декабря пресс-секретарь президента Дмитрий Песков, комментируя введение санкций.

Руководство сайта WikiLeaks заявило, что в несекретной версии доклада спецслужб США о якобы имевшем место вмешательстве России в американские президентские выборы нет никаких доказательств связи между какими-либо государствами и источниками.

> Nothing in today's declassified ODNI report alters our conclusion that WikiLeaks' US election related sources are not state parties.
>
> — WikiLeaks (@wikileaks) 7 января 2017 г.

6 января Дональд Трамп заслушал доклад спецслужб о кибератаках. 7 января он опубликовал в своем твиттере заявление о том, что по данным спецслужб хакерские атаки не повлияли на результаты выборов.

> Intelligence stated very strongly there was absolutely no evidence that hacking affected the election results. Voting machines not touched!
>
> — Donald J. Trump (@realDonaldTrump) 7 января 2017 г.

Сразу после встречи со спецслужбами избранный президент США заявил также:

«Россия, Китай, другие страны и внешние группы и люди постоянно пытаются нарушить цифровую инфраструктуру наших правительственных учреждений, компаний и организаций, включая Национальный комитет Демократической партии, но никакого эффекта на результат выборов не было, как и не было взлома машин для голосования».

При этом он нигде не заявлял, что кибератаки являются недоказанными.

Автор: Полина Чехова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 3021 08.01.2017, 16:42
18

Порекомендовать текст

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:
- *Телеграм*
- *ВКонтакте*

Связаться с редакцией Бабра:
newsbabr@gmail.com

Автор текста: **Полина Чехова**,
журналист.

На сайте опубликовано **494**
текстов этого автора.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта