Забастовка

О Crowdstrike и я позволю ИТ-анализы

#CrowdStrike #DNC #Clinton #FBI

Орлы - невероятно добрые охотники. Их способность идентифицировать даже самое маленькое животное с высоты птичьего полета легендарна. Любой, кто когда-либо имел возможность наблюдать, как орел переключается в режим атаки, зажигая свое быстрое, но решительное падение на землю, вряд ли забудет это зрелище. По совпадению, именно такой орел является частью логотипа Crowdstrike, компании, предоставляющей ИТ-программное обеспечение и услуги, связанные с сетевой безопасностью. Компания была основана в 2011 году Джорджем Курцем, бывшим техническим директором компании McAfee, занимающейся защитой персональных компьютеров, и Дмитрием Альперовичем, экспертом по ИТ-безопасности российского происхождения и бывшим вице-президентом McAfee. В 2012 году к фирме присоединился бывший сотрудник ФБР по имени Шон Генри, еще через 12 месяцев компания выпустила свой первый продукт под названием Crowdstrike Falcon.

Подобно настоящим соколам, программное обеспечение было создано для постоянного наблюдения за компьютерными сетями и их огромным трафиком данных для злоумышленников, которые стремились украсть конфиденциальную информацию, IP-адреса и многое другое в этой сети. После того, как компания смогла выявить ряд атак на различные корпоративные и отраслевые сети, предположительно из Китая, Северной Кореи и России в 2014 и 2015 годах, Crowdstrike получила крупномасштабное финансирование от Google, общая сумма которых превысит 480 миллионов долларов к 2019 году. Компания также получила оценку более чем в 3 миллиарда долларов в 2018 году с годовой выручкой от продаж всего в 100 миллионов долларов и была зарегистрирована на NASDAQ в 2019 году.

Три крупнейших акционера Crowdstrike перечисляют две крупные инвестиции в Кремниевую долину. компаний и - что странно - в Мюнхене, Германия, с офисом Allianz Asset Management GmbH. В настоящее время компания имеет рыночную капитализацию более 15 миллиардов долларов и немногим более 2000 сотрудников, не имеет долгов и в октябре 2019 года у нее было более 800 миллионов долларов наличными - неплохо для того, чтобы быть «всего лишь» компанией-разработчиком программного обеспечения.

В рамках всего этого неоспоримого стремительного успеха появился довольно странный инцидент в 2016 году, когда Crowdstrike выпустил нарядный и красочный отчет о том, как российская группа под названием «Fancy Медведь» якобы взломал украинское военное приложение под названием «Артос», программное обеспечение , которое может быть установлено на планшетных ПК и используется для управления огнем « чтобы внести изменения в условии стрельбы баллистических и метеорологических систем», так разработчик приложения Ярослав Шерстук. Crowdstrike сделал ряд политических оценок на высоком уровне и заявил, что украинские военные понесли «тяжелые потери» в артиллерии, в основном из-за российских взломов.

> В течение этого предложенного периода разработки между Украиной, Россией и международным сообществом произошел ряд значительных событий. В частности, попытки России повлиять на отношения Украины и ЕС привели к крупномасштабному протестному движению на Майдане,

> что в конечном итоге привело к свержению тогдашнего президента Виктора Януковича, вторжению и аннексии Крымского полуострова Россией и затяжному вооруженному конфликту. на востоке Украины. Таким образом, создание приложения [App], которое нацелено на некоторые из передовых сил, играющих ключевую роль в украинской обороне на восточном фронте, вероятно, будет приоритетной задачей для российских разработчиков вредоносных программ, стремящихся переломить ход конфликта в свою пользу. . Для украинских войск артиллерия тоже понесла тяжелые потери ... (Crowdstrike Report «Использование вредоносных программ Fancy Bear и Android в отслеживании украинских полевых артиллерийских подразделений»)

Как ни странно, основные выводы Crowdstrike были быстро отвергнуты. Например, Международный институт стратегических исследований (IISS), опубликовавший следующее заявление:

> В отчете Crowdstrike используются наши данные, но выводы и анализ, сделанные на основе этих данных, принадлежат исключительно авторам отчета. Сделанный ими вывод о том, что сокращение украинских артиллерийских резервов Д-30 в период с 2013 по 2016 год было главным образом результатом боевых потерь, не является выводом, который мы когда-либо делали сами, и мы не считаем его точным. (Заявление IISS от 2017 г.)

Другой исследователь IISS заявил, что сокращение воинских частей было в основном связано с перераспределением подразделений в другие военные командования. Украинские военные сообщили, что артиллерийские потери от боевых действий с сепаратистами были «в несколько раз меньше, чем количество, сообщаемое Crowdstrike, и не связаны с конкретной причиной» взлома. Разработчик приложения опубликовал в Facebook заявление о результатах исследований Crowdstrike по Украине, назвав их «бредовыми». Однако он признал, что его электронные письма были скомпрометированы.

Интересно также, что высокопоставленный американский чиновник объяснил на конференции в Дании в 2018 году о том, как США продолжали открыто поддерживать усилия Украины по кибербезопасности на общую сумму 10 миллионов долларов - почти соблазнительно подумать о наведении порядка в Crowdstrike:

> Во время этой поездки - я думаю, это было в сентябре прошлого года [2017] - мы объявили, что увеличиваем объем финансирования помощи Украине на 5 миллионов долларов, уделяя особое внимание кибербезопасности. А затем, когда помощник госсекретаря Митчелл приехал в Украину этой весной [2018 года], он объявил о дополнительных 5 млн долларов США в виде помощи Украине в области кибербезопасности. (Йорган К. Эндрюс, заместитель помощника секретаря, Бюро по международным делам о наркотиках и правоохранительной деятельности, июнь 2018 г., Копенгаген, Дания)

Всего за несколько месяцев до разгрома Crowdstrike в Украине в 2016 году Национальный комитет Демократической партии (DNC) разрешил компании провести расследование на их компьютерных серверах, предположительно взломанных Россией. Кампания Хиллари Клинтон утверждала, что были украдены не только тысячи ее электронных писем, опубликованных Wikileaks за несколько месяцев до президентских выборов в США 2016 года, но и все ее президентство.

Существует еще больше противоречивых заявлений и событий, связанных с последующими расследованиями сервера DNC Crowdstrike - не ограничиваясь довольно большим количеством запутанных заявлений Crowdstrike относительно дат назначения, персонала и методов - чем в извращенной истории о взломе украинских военных. 28 апреля 2016 года DNC официально обнаружило, что его серверы были «взломаны». Несмотря на первый платеж DNC в пользу Crowdstrike 5 мая 2016 года, оба не смогли предотвратить получение электронных писем Клинтона сначала хакером "Guccifer 2" и даже опубликовать на Wikileaks почти два месяца спустя, причем 75% этих электронных писем указывали дату создания позже. чем в первую неделю мая 2016 года.

Генеральный директор Crowdstrike Альперович утверждаетчто группы, связанные с Россией, использовали так называемую программную команду Powershell.exe или X-Agent с загадочными параметрами, которые при выполнении преобразовывались в программный код, способный управлять программным обеспечением Windows Management. Доказательства того, что такие команды на самом деле были внедрены российскими хакерами, трудно, если не почти невозможно доказать, и они вполне могли быть вставлены некоторыми из многих инсайдеров западных правительств, которых мы видели в прошлом, с целью «уничтожить Трампа».

> Альперович имеет значительный опыт работы в качестве предметного эксперта на всех уровнях правоохранительных органов США и других стран в области анализа, расследования и профилирования транснациональной организованной преступной деятельности и киберугроз со стороны террористов и противников из национальных государств. Его часто цитируют как эксперта в национальных изданиях, включая Associated Press, NBC, New York Times, USA Today и Washington Post. (Дмитрий Альперович, старший научный сотрудник Атлантического совета)

Независимый судебный анализ Zip-файл, содержащего кажущееся подмножество всех писем Клинтона, полученных хакер «Гаккифер 2» пришел к выводу, что отдельные файлы , полученные им - не Wikileaks - в последний раз сохраненные в 2015 году, главным образом, exfiltrated 16 апреля , 2016 г. с использованием медленного - возможно, спутникового - подключения к Интернету, затем сохранены на флэш-накопитель, скопированы с этого флэш-накопителя на компьютер с восточным часовым поясом США и, наконец, сжаты на этом компьютере в один Zip-файл 20 июня 2016 г., если информация о дате всех отдельных файлов не была изменена «взломом». Кроме того, президент CrowdStrike и сам CSO Шон Генри заявил перед Комитетом по разведке 5 декабря 2017 г. (на стр.), что «у нас не было конкретных доказательств того, что данные были украдены из DNC, но у нас есть признаки того, что они были эксфильтрованы».

> **Мистер Генри**: «Адвокат только что напомнил мне, что в отношении DNC у нас есть

> индикаторы того, что данные были эксфильтрованы. У нас не было конкретных доказательств того, что данные были извлечены из DNC, но у нас есть признаки того, что они были эксфильтрованы» (стр. 32)
> ...
> **Мистер Генри**: «Да, сэр. Так что это, опять же, постановка, чего, я имею в виду, нет - аналогия, которую я использовал с мистером Стюартом ранее, заключалась в том, что у нас нет видео с это происходит, но есть признаки того, что это произошло. Бывают случаи, когда мы видим, что данные были извлечены, и мы можем сказать определенно. Но в этом случае, похоже, они были настроены для извлечения, но у нас просто нет свидетельство того, что оно действительно осталось» (стр.32)
> ...
> **Мистер Генри**: «Итак, некоторые из данных, которые мы видели, были инсценированы, но у нас не было указаний на то, что они были высланы, но они были инсценированы - по всей видимости, были инсценированы для высылки, что они были связаны с исследованием, которое проводилось DNC. о кандидатах от оппозиции» (стр. 49)
> ...
> **Мистер Стюарт из Юты**: «Хорошо. Вы что-то сказали, и я хочу повторить это - и сказать мне, если я ошибаюсь - если бы я мог. Вы сказали, я полагаю, говоря о Компьютер DNC, у вас были признаки того, что данные были подготовлены к утечке, но никаких доказательств, которые он фактически не оставил. Я правильно это записал?»
> **Мистер Генри**: «Да»
> **Мистер Стюарт из Юты**: «И в этом случае данные, которые я вам предполагаю»Речь идет об электронной почте, а также обо всем остальном, что они, возможно, пытались получить».
> **Мистер Генри**: «Были файлы, касающиеся проведенного исследования оппозиции».
> **Мистер Стюарт из Юты**: «Хорошо. А как насчет электронных писем, о которых все, как вы знаете, осведомлены? Были ли также признаки того, что они были подготовлены, но не свидетельства того, что они действительно были похищены ?»
> **Мистер Генри**: «Нет никаких доказательств того, что они действительно были увезены. Есть косвенные доказательства -»
> **Мистер Стюарт из Юты**: «Хорошо»,
> **мистер Генри**: «- но нет доказательств того, что они действительно были эксфильтрованы. Но позвольте мне также заявить, что если кто-то следил за почтовым сервером, он мог прочитать всю электронную почту». (п.74/75)
>
> Стенограммы интервью Шона Генри в Комитете по разведке Палаты представителей 5 декабря 2017 г.

Вдобавок Хиллари Клинтон использовала частный почтовый сервер в своем личном офисе в Чаппакуа, штат Нью-Йорк, для официальных вопросов Государственного департамента и даже пригласила Google в 2012 году - освещая график атак на посольство США в Бенгази - для управления своей личной официальной учетной записью электронной почты. скорее всего, для того, чтобы обойти обязательство о том, что ее официальные разговоры с правительством поддерживаются и доступны для общественности. На ее частном сервере в Чаппакуа работала программа для управления электронной почтой Windows.

Вдобавок ко всему, не нужно иметь глаза орла, чтобы увидеть явно сомнительные слова бывшего директора ФБР Джеймса Коми, когда в январе 2017 года его спросили в Сенате США о серверах DNC и Crowdstrike:

> **Коми**: «Мы предпочитаем получать доступ к исходному устройству или серверу, это лучшее доказательство»
> **Сенатор**: «Вам был предоставлен доступ для проведения криминалистической экспертизы на этих серверах ?»
> **Коми**: «Мы не были, уважаемая частная компания [Crowdstrike] в конечном итоге получила доступ и поделилась с нами тем, что они там видели».
> **Сенатор**: «ФБР обычно предпочитает проводить судебно-медицинскую экспертизу таким же образом, или вы предпочитаете сами пощупать и увидеть сервер ?»
> **Коми**: «Мы всегда предпочли бы иметь доступ к себе, если это возможно».
> **Сенатор**: «Вы знаете, почему вам отказали в доступе к серверам ?»
> **Коми**: «Точно не знаю.Точно не знаю»
> **Сенатор**: «Был ли запрос один или несколько ?»
> **Коми**: «Множественные запросы на разных уровнях, и, в конечном итоге, было решено, что частная компания поделится с нами тем, что они увидели»
>
> (Экс-директор ФБР Джеймс Коми на слушаниях в Сенате США 10 января 2017 г.)

Похоже, что в 2016 году DNC отвечал за ФБР, а не за Министерство юстиции, Конгресс США и / или Сенат США. Всю сагу о DNC можно было бы поместить в папку 'Massive Corruption', если бы не было знаменитого телефонного разговора президента США Дональда Трампа с новоизбранным президентом Украины Зеленским 25 июля 2019 года, в котором президент США, в частности, упомянул Crowdstrike:

> Но я бы хотел, чтобы вы сделали нам одолжение, потому что наша страна многое пережила, и Украина много об этом знает. Я хотел бы, чтобы вы выяснили, что случилось со всей этой ситуацией с Украиной, **они говорят Crowdstrike**... Я думаю, у вас есть один из ваших богатых людей ... **Сервер, они говорят, что Украина**. Произошло много всего, вся ситуация ... Я бы хотел, чтобы генеральный прокурор позвонил вам или вашим людям, и я хотел бы, чтобы вы разобрались в сути. Как вы видели вчера, вся эта чушь закончилась очень плохим выступлением человека по имени Роберт Мюллер, некомпетентным выступлением, но, говорят, во многом это началось с Украины. (Президент США Дональд Трамп в телефонном разговоре от 25 июля 2019 г.

> с Президентом Украины Зеленским)

Вскоре после этого ад вспыхнул среди политиков-демократов в Конгрессе США, которые всерьез намеревались объявить импичмент президенту США за эти пикантные слова - и в отношении некоторых из них, связанных с коррупцией Джо Байдена на Украине - в его в остальном уместном и регулярном телефонном звонке с Зеленский. Театр импичмента просуществовал недолго, он был окончательно отклонен в Сенате США в начале 2020 года и стал надпартийным, когда все республиканцы в Конгрессе США также отвергли его.

Не может быть другого объяснения, кроме того, что в Украине действительно где-то есть цифровая зеркальная копия этого сервера DNC. Возможно, на нем есть заразные материалы.

Орлы могут ясно видеть это с высоты и издалека.

https://www.sun24.news/ru/zabastovka-o-crowdstrike-i-ya-pozvolyu-it-analizy.html