26.02.21

СЛУШАНИЕ ПО ХАКЕРСКОЙ АТАКЕ НА SOLARWINDS И ВИРТУАЛЬНЫЙ САММИТ БАЙДЕНА И ТРУДО

ВНЕШНЯЯ ПОЛИТИКА США 19-25 ФЕВРАЛЯ

На прошедшей неделе Вашингтон всерьез взялся за выяснение подробностей хакерской атаки на SolarWinds, информация о которой впервые появилась в начале декабря. Администрация пообещала принять ответные меры в течение ближайших недель, законодатели начали разработку нового регулирования, а пострадавшие компании попытались выйти из ситуации с наименьшими репутационными потерями. При этом, признавая невозможность достоверно установить, кто организовал атаку, все в один голос обвинили Россию, поскольку «нет данных, указывающих на ложность» данного вывода.

Первым иностранным лидером, удостоенным «виртуальной» аудиенции нового американского президента, стал премьер-министр Канады Джастин Трудо. Наполненные словами о дружбе и сотрудничестве заявления двух лидеров обошли стороной наиболее сложные вопросы о закрытой границе и политике «покупай американское», которые могут стать главным источником проблем в двусторонних отношениях в следующие четыре года.

Слушание по хакерской атаке на SolarWinds

23 февраля в сенатском комитете по разведке прошло первое публичное слушание по т.н. хакерской атаке на IT-компанию SolarWinds. В ходе атаки, информация о которой впервые появилась в начале декабря, хакеры через обновление SolarWinds, ПО которого используется как частным сектором, так и государственными органами, получили доступ к внутренним сетям более ста американских компаний и девяти федеральных агентств. Впоследствии появилась информация, что это был не

единственный вектор атаки, но инцидент по-прежнему называют «SolarWinds hack».

Хотя формальные обвинения не предъявлены, в США сложился консенсус относительно того, что за атакой стоит Россия. 19 февраля советник по национальной безопасности **Джейк Салливан** **отметил**, что «готов пойти дальше», чем предыдущая администрация, заявившая, что атаку совершила «скорее всего Россия», а также пообещал, что ответ последует «в течение ближайших недель, а не месяцев» и будет включать как меры по наказанию виновного, так и шаги по укреплению собственной безопасности. Состоявшееся на этой неделе слушание касалось преимущественно второго аспекта: законодатели попытались определить, как это стало возможным, несмотря на **«многие миллиарды долларов, потраченные правительством США в области кибербезопасности»**, и как можно избежать повторения подобных атак в будущем.

Состав участников

Как отметил председатель комитета сенатор **Марк Уорнер** (дем., Вирджиния), на заседание комитета были приглашены руководители компаний, принявших непосредственное участие в обнаружении и расследовании инцидента (т.н. first-responders). Помимо **Судакара Рамакришна**, исполнительного директора SolarWinds, в их число вошли **Кевин Миранда**, исполнительный директор компании в области кибербезопасности FireEye, которая первой обнаружила взлом, **Бред Смит**, президент Microsoft, доступ к исходному коду которой получили хакеры в ходе атаки, что, учитывая повсеместное распространение продуктов компании, кратно увеличивает потенциальный ущерб от инцидента, и **Джордж Куртц**, глава CrowdStrike, эксперты которой были привлечены FireEye для расследования.

При этом в слушании отказалась принять участие компания Amazon, облачный сервис которой, как предполагается (хотя компания это отрицает), использовался в ходе атаки. «Очевидно, они слишком заняты, чтобы обсудить с нами этот вопрос», - **отметил** во вступительном слове вице-председатель комитета сенатор **Марко Рубио** (респ., Флорида). – Я бы советовал им пересмотреть свой подход». Язвительные выпады в адрес Amazon звучали на протяжении всего слушания, и отказ компании неизбежно **усугубит** уже непростые отношения между компанией и органами власти, обострившиеся в прошлом году в ходе антимонопольного расследования Конгресса. Впрочем, отказ Amazon неудивителен, поскольку признание уязвимости перед хакерами наносит серьезный удар по репутации компании, который может быть использован конкурентами. Это наглядно продемонстрировала ситуация с Microsoft. Как **сообщил** Politico, накануне слушания члены комитета получили многочисленные письма и запросы от Google, в которых основной причиной успеха атаки называлось не столько мастерство хакеров, сколько несовершенство систем Microsoft.

Проблема атрибуции

Подобные сомнения в уязвимости продуктов Microsoft могут объяснить стремление Бреда Смита представить произошедшее как масштабную скоординированную атаку на США (по его **словам**, операцию проводили «минимум тысяча инженеров») и возложить ответственность за произошедшее на Россию. В то время как все участники слушания, хоть и подчеркивая, что не сомневаются в том, кто действительно стоит за атакой, все же избегали прямой атрибуции, Смит **заявил**:

«На данном этапе у нас имеется достаточно информации, указывающей на российские службы внешней разведки, и нет ни одного факта, свидетельствующего об обратном».

В аналогичном ключе, но с большим количеством оговорок высказался глава CrowdStrike – компании, которая имеет богатую историю обвинений России в различных хакерских атаках, некоторые из которых ей позже пришлось «корректировать» либо под **давлением** усомнившегося в выводах экспертного сообщества, либо в ходе **выступлений** под присягой. «Нам известно, что правительство США заявило, что данный государственный актор «скорее всего» имеет российское происхождение, - **отметил** Джордж Куртц, апеллируя к заявлению Майка Помпео. – В данный момент мы не можем подтвердить этот вывод, но мы и не располагаем информацией, указывающей на его ложность».

Таким образом, при нескрываемом **желании** законодателей поскорее разоблачить и наказать виновного, они были вынуждены признать, что прямых доказательств, указывающих на Россию, на данный момент не существует. При этом, описывая колоссальные масштабы произошедшего, как аргумент в пользу атрибуции взлома «государственному актору», участники слушания невольно сообщили, что атака была настолько искусной, что обнаружить следы будет крайне затруднительным. Наконец, ситуация осложняется появившимися в феврале **сообщениями** о том, что параллельно с приписываемой России атакой, уязвимости ПО SolarWinds пыталась эксплуатировать еще одна, предположительно китайская, группа хакеров. Детали их действий еще расследуются, но уже установлено, что злоумышленники проникли в системы начисления зарплаты госслужащим, а значит могли получить доступ к личным данным всего государственного аппарата.

Дальнейшие шаги

Как показывает практика последних лет, отсутствие доказательств не мешает руководству США «решительно» отвечать на угрозы безопасности страны, особенно когда они представлены как нападение со стороны «привычного» врага – России. Возможные внешнеполитические действия по наказанию Москвы, о которых говорил Салливан, не были предметом слушания, и законодатели ограничились призывами к срочным действиям, не останавливаясь на конкретике. Единственным, кто акцентировал данный аспект, стал сенатор Ангус Кинг (незав., Мэн), **посоветовавший** «интернационализировать» данную проблему. Обращаясь к словам Смита о том, что в ходе атаки пострадали компании в Мексике, Канаде, Великобритании, Бельгии, Испании, Израиле и ОАЭ, он предложил работать вместе с союзниками, чтобы, с одной стороны, разработать международные нормы и «красные линии» в вопросах кибербезопасности, с другой – сделать «такие инструменты как санкции намного более эффективными».

С точки зрения внутриполитического ответа, по результатам слушания кристаллизовалась идея создания механизма обязательного оповещения государственных органов о случаях хакерских атак. Сегодня законодательство США не обязывает частные компании сообщать о подобных инцидентах и, учитывая сопутствующие репутационные потери и угрозу передачи выгодных государственных контрактов конкурентам, компании не всегда готовы к сотрудничеству с правительством в данных вопросах. В результате, американские службы в области кибербезопасности, расследуя хакерские атаки, не обладают полной картиной

произошедшего. Представители компаний горячо поддержали введение подобного регулирования, призвав, однако, сделать процедуру оповещения непубличной (чтобы снять угрозу репутации компаний) и придерживаться принципа «одного окна» - единого контактного органа в правительстве (чтобы упростить данный процесс).

На фоне всеобщей поддержки нового регулирования и, хоть и не упоминаемого, но неизбежного в таких случаях, увеличения госрасходов в области кибербезопасности (что означает дополнительные контракты для тех же Microsoft, SolarWinds и FireEye), выделился сенатор Рон Уайден (дем., Орегон), призвавший не поддаваться искушению скрыть собственные провалы за счет раздувания образа врага. «По результатам этого слушания у американцев может сложиться впечатление, что хакеры являются настолько всемогущим противником, что ни американское правительство, ни наши крупнейшие технологические компании были не в силах предотвратить их действия, - весьма точно **охарактеризовал** Уайден истинные мотивы выступавших. – Я считаю, что это ведет к законам, посягающим на частную жизнь, и выделению дополнительных миллиардов долларов налогоплательщиков на кибербезопасность. Возможно, будет стыдно это признать, но, в первую очередь, мы должны разобраться, где мы просчитались и почему уже существующие механизмы по обеспечению кибербезопасности не сработали».

Виртуальная дружба между Байденом и Трудо

23 февраля состоялась первая двусторонняя **встреча** **Джо Байдена** в качестве президента с иностранным лидером, которым стал премьер-министр Канады Джастин Трудо. Виртуальный характер встречи оставил неоднозначные **впечатления**, что, однако, не помешало двум соседям попытаться залечить уже появившиеся раны и наметить курс по восстановлению отношений.

Выбрав Трудо в качестве первого иностранного лидера для двусторонней встречи, администрация Байдена оказала уважение северному соседу, что было призвано сгладить неприятный осадок от решения об отзыве лицензии для строительства трубопровода Keystone XL. Связывающий нефтедобывающие районы канадской провинции Альберта с перерабатывающими предприятиями американского штата Небраска, трубопровод стал первой жертвой экологической политики Байдена. Помимо убытков для финансирующей строительство канадской компании TransCanada, отзыв лицензии не имел существенных **последствий** для политических позиций Трудо, что обусловило его нежелание обострять противоречия по данному вопросу. Однако манера, в которой было принято это решение – без, хотя бы символических, предварительных консультаций – позволила говорить о **сложном** начале процесса восстановления двусторонних отношений «после Трампа».

Стремление Байдена сгладить совершенную оплошность и желание Трудо продемонстрировать способность выстроить конструктивные отношения с новой администрацией (что традиционно **является** главным фактором при оценке внешнеполитического наследия канадских лидеров) обусловили крайне дружелюбную атмосферу встречи. В таких условиях внимание привлекло не столько содержание заявлений, наполненных дежурными словами о вечной дружбе, сколько вопросы, оставшиеся за рамками повестки дня, где и стоит ожидать наибольших проблем в двусторонних отношениях.

В частности, к давним спорам относительно протекционизма Канады в области молочной и деревообрабатывающей промышленности президентство Байдена грозит добавить новый раздражитель в виде политики «покупай американское». Опубликованный 25 января президентский **указ** предписывает отдавать приоритет американским производителям при совершении госзакупок. В то время как Ассоциация производителей и экспортеров Канады уже **пообещала** «не ослаблять давление» на правительство Трудо до тех пор, пока оно не добьется исключения из этого правила для канадских компаний, американские эксперты **отметили**, что, если «канадцы сумеют найти правильный подход», то политика администрации еще может трансформироваться в «покупай североамериканское».

Еще одной, и более насущной проблемой, о которой умолчали лидеры, является закрытая граница. На протяжении последнего года (ограничения были введены 21 марта 2020 года) американские СМИ пестрели историями о разлученных семьях, ветшающих «вторых домах» американских пенсионеров и банкротящихся в отсутствие канадских туристов бизнесов северных штатов. Канадские издания невозмутимо **отвечали** на это публикациями опросов общественного мнения, в которых поддержка закрытия границы с южным соседом временами достигала 90%.

Откликаясь на настроения в США, уже в первые дни президентства Байден **поручил** ответственным ведомствам связаться с коллегами в Канаде и Мексике и в течение 14 дней разработать единые санитарные протоколы, что было **воспринято** как желание администрации сделать все возможное для скорейшего снятия ограничений. Когда, несмотря на растущее **давление** со стороны конгрессменов из приграничных районов, в указанные сроки ничего не произошло, появились слухи, что лидеры решили приберечь столь символический шаг на двусторонний саммит. На фоне таких завышенных ожиданий отсутствие в заявлениях Трудо и Байдена каких-либо упоминаний о состоянии американо-канадской границы стало глубоким **разочарованием**. Более того, за день до саммита Оттава **ужесточила** требования при пересечении границы, включая предоставление нескольких последовательных отрицательных тестов на COVID-19, цена которых в США может доходить до 2000 долл.

Как гласит известное **выражение**, приписываемое актеру Робину Уильямсу, находящаяся к северу от США Канада похожа на приличную квартиру, расположенную над подпольной лабораторией по производству метамфетамина. Смена нижнего соседа с гангстера на дружелюбного предпринимателя не отменяет наличия лаборатории, и канадцы, судя по всему, предпочитают пока держать дверь закрытой на все замки и встречаться с беспокойным соседом исключительно в виртуальном формате.

Источник: **Слушание по хакерской атаке на SolarWinds и виртуальный саммит Байдена и Трудо**

ОБ АВТОРЕ

Ольга Ребро

Старший эксперт

Местоположение: Москва, Россия

Сфера компетенций: Внешняя политика США

Область экспертизы: Эксперт по внешней и внутренней политике США, американским политическим элитам.

Профессиональный опыт: Выпускница МГИМО МИД России. Автор публикаций по внешней и внутренней политике США, с 2014 года - автор еженедельного дайджеста внешней политики США. В 2016 году – соавтор доклада о психологических профилях кандидатов в президенты США Х. Клинтон и Д. Трампа. Ее комментарии появлялись в изданиях РБК, Лента.ру, Russia Direct, Актуальные комментарии, Russia Beyond the Headlines, Международные процессы, на портале Валдайского клуба и др.

