Алексей Викторович Лукацкий,
Бизнес-консультант по безопасности Cisco Systems

Определение источника кибератак

5.42 по тихоокеанскому времени сержант военно-воздушных сил США Томас Блейк зафиксировал подготовку к пуску баллистической ракеты с территории Китайской Народной Республики… Бывший морпех, отправленный в отставку и случайно оказавшийся на о.Хайнань в отпуске в сопровождении своей несовершеннолетней племянницы, скрытно проникает на засекреченный китайский объект, пробирается в шахту с ядерной боеприпасами и с помощью перочинного ножа и курса квантовой физики, прочитанного в самолете, обезвреживает боеголовку за 7 секунд до старта, тем самым в очередной раз спасая мир от катастрофы.

Таким мог бы быть сценарий фильма, посвященного ядерному терроризму и доблестным американским спецслужбам, невидимые бойцы которых в одиночку обезвредят сотни китайских экстремистов, решивших развязать Третью мировую войну. Но мы живем не в павильонах Голливуда, и я с трудом представляю себе, чтобы какие-либо государства в здравом уме решили пойти по описанному сценарию, по сути приговорив и свои народы тоже. Гораздо более реальным мне кажется сценарий киберапокалипсиса, в котором угрозы если и реализуются, то

через киберпространство. И вот тут мы сталкиваемся с определенной сложностью, связанной с атрибуцией киберугроз, то есть с определением стоящей за угрозой стороны.

Когда мы имеем дело с миром материальным, в котором присутствуют ядерные боеголовки, находящиеся в шахтах, воинские формирования, находящиеся в местах своей дислокации, эскадрильи самолетов, боевые группы кораблей, то не составляет большого труда определить, кто за ними стоит. Вряд ли стоит ожидать, что морская группировка может быть создана каким-либо олигархом, а шахты с ядерным оружием «прорыты» любителями. С киберугрозами ситуация прямо противоположная.

Ситуация усугубляется тем, что сейчас ведутся работы по выпуску 2-й версии Таллиннского руководства, в котором признается возможность физического ответа на кибернападение. Очевидно, что в такой ситуации как никогда важна правильная атрибуция источника киберугроз. Неправильная его идентификация может привести к развязыванию войны (локальной, региональной или крупномасштабной) или наоборот, будет упущен нужный момент и потеряно время, так необходимое для подготовки к отражению агрессии. Незнание истинного виновника и, возможно, посредников, не позволяет в полной мере задействовать имеющиеся в распоряжении каждого государства дипломатические, политические и юридические рычаги.

Поэтому атрибуция нам нужна для того чтобы понять, кто против нас действует, а также чтобы выстроить свою оборонительную стратегию и спланировать защитные мероприятия. Если это нарушитель, за которым стоит государство, то это один набор действий; если угроза реализована негосударственным актором, то и действия должны быть предприняты другие. Причем, если на техническом уровне механизмы защиты будут практически одинаковым (если не рассматривать возможность бомбардировок в ответ на сканирование сети), то на дипломатическом и правовом - именно атрибуция определит набор шагов, которые будет предпринимать государство. В конце концов, перспектива обнаружения и правильной атрибуции может стать сдерживающим фактором для, как минимум, государственных акторов.

Последние примеры атрибуции киберугроз

Истории с атрибуцией атак встречаются еще на заре формирования отрасли информационной безопасности, но на новый уровень эта тема вышла в 2010-м году, когда на заводе по обогащению ядерного топлива в иранском Натанзе был обнаружен вредоносный код, позже получивший название “Stuxnet”. Именно тогда специалисты всерьез задумались о том, как идентифицировать силы, стоящие за данным вредоносным кодом. Ведь данный код находился на изолированном от Интернет объекте; да еще и сам код присутствовал как минимум год до начала

официального расследования. То есть отследить его реального автора ни по Интернет-активности, ни по записям журнала прохода на территорию завода не представлялось возможным. В процессе расследования было высказано предположение о том, что автором Stuxnet являются спецслужбы США и Израиля, что косвенно было подтверждено как разоблачениями Сноудена, так и рядом других публикаций последнего времени. Однако общепризнанных доказательств, которые могли бы быть проанализированы независимыми экспертами, так и не было представлено, что и понятно, учитывая специфику и самого объекта, и самой ситуации.

И до и после Stuxnet бездоказательные заявления об атаках со стороны различных государств делались в рамках конфликта в Северной Осетии, Югославии, Украине, Ливии, Сирии и т.п. Но новую кровь в данный процесс влила американская компания Mandiant, позже купленная компанией FireEye, также американской. За последнее время FireEye выпустила несколько отчетов, подробно исследующих различные кибершпионские и хакерские кампании, например, действия китайской хакерской группы APT1 (в качестве одного из атрибутов называлось время максимальной активности, совпадающее с часовым поясом Шанхая), российской хакерской группы APT28, иранской группы Ajax Security Team, взлом Sony Pictures Entertainment.

Помимо FireEye аналогичные исследования проводились компаниями:

- Cylance, которая изучала кампанию Cleaver (“нож мясника”) иранских хакеров,
- iSight Partners, которая раскрыла операцию Newscaster (“телекомментатор”), также исходившую из Ирана,
- Лабораторией Касперского, которая раскрыла кампании “Маска” и “Красный октябрь”,
- Group-IB, нашедшей след “Исламского государства” в атаках на многие российские организации,
- BAE Systems, исследовавшая атаки на украинские компьютеры и нашедшая на них “русские” отпечатки,
- Check Point, раскрывшая ливанскую хакерскую группу Volatile Cedar (“Летучий кедр”),
- Taia Global, которая вопреки распространенному мнению, что компанию Sony взломали хакеры из Северн Кореи, доказала, что Sony все-таки атаковали из России.

И во всех случаях использовались различные обоснования для атрибуции. Например, в марте 2014-го года американская BAE Systems обнаружила на украинских компьютерах след “хорошо подготовленных профессионалов”, использующих вредоносное ПО Snake (“Змея”) из часового пояса, в котором находится Москва (почему была названа Москва, а не, например, Йемен, Ирак, Мадагаскар или Эфиопия, находящиеся в том же часовом поясе?). Позже тот же вредоносный код был найден на ряде компьютеров бельгийского МИДа. Затем

“русский” след был найден финской компанией F-Secure в вредоносном коде BlackEnergy, а потом подоспел и отчет FireEye про хакерскую группу APT28, действующую из Москвы и пишущую вредоносные программы в то время, когда в Москве рабочие часы. Видимо проявляется классический стереотип иностранца - “Россия - это Москва” и “Россия расположена всего в одном часовом поясе”.

В случае с атаками ИГИЛ на российские ресурсы атрибуция была достаточно простой - группировки Cyber Caliphate, Team System Dz, FallaGa Team и Global Islamic Caliphate массово взламывали Интернет-ресурсы с хорошей посещаемостью, на которых они размещали свои лозунги и мгновенно публиковали информацию об этом в социальных сетях Twitter и Facebook. По этому сценарию действовала и Сирийская электронная армия. Примерно так же идентифицировались и действия КиберБеркута, который не скрываясь, публиковал данные о своих “подвигах” на своем сайте, что облегчало поиск виновных.

DDoS-атака Ирана против финансовых институтов США (операция Ababil), а также против компаний из сферы ТЭК Катара и Саудовской Аравии в конце 2012-го - начале 2013-го годов была идентифицирована по регистрации используемых для атаки IP-адресов.

Операция “Нож мясника” была атрибутирована сразу по ряду параметров. Во-первых, в рамках операции использовались персидские имена хакеров, а во-вторых, домены, IP-адреса и инфраструктура, используемые в рамках атаки, были зарегистрированы в Иране. Также и действия “Летучего кедра” были идентифицированы по нескольким параметрам - командным серверам, расположенным на площадке ливанской хостинговой компании, DNS-запросы вели в Ливан, а e-mail, на которые были зарегистрированы некоторые домены были связаны с ливанскими политическими активистами.

Конфуз случился в истории с проникновением в сеть компании Sony, которое произошло в ноябре 2014-го года и которое послужило причиной очередного витка серьезного внимания США к теме кибербезопасности и разработки целого пакета нормативных актов, которые направлены на усиление борьбы с хакерами. США практически сразу обвинили в атаке на Sony северокорейских хакеров, которые предупреждали, что за выпуском в прокат фильм “Интервью” про северокорейского лидеры Ким Чен Ына, последуют определенные действия. И хотя “после” не значит “вследствие”. американские власти поспешили назвать виновника всех бед, попутно введя против Северной Кореи очередные санкции. Доказательства участия в деле корейских злоумышленников вновь добывала FireEye. Однако американская корпорация Taia Global поставила под сомнение выводы FireEye о северокорейском следе, представив доказательства, что за атаками на Sony стоят вновь россияне.

Почему все так плохо с определением источника киберугроз?

Можно выделить несколько причин, которые мешают адекватному и стопроцентному определению источников спецопераций в киберпространстве:

- геополитические
- правовые
- технические
- экономические
- психологические.

Геополитическая ситуация

Кибератвность военного предназначения сегодня превратилась в инструмент геополитической борьбы. Что может быть проще, чем обвинить то или иное государство в агрессии только на том основании, что с его территории зафиксирована кибератака? И мы прекрасно видим в последнее время, что отдельные страны и блоки этим активно пользуются. Кто взломал Пентагон? Русские хакеры. Кто взломал “Белый дом” и получил доступ к переписке Барака Обамы? Русские хакеры! Кто взломал лабораторию в Лос-Аламосе, занимающуюся разработками ядерного вооружения? Опять русские хакеры! Так и формируется имидж всесильного, но почему-то неуловимого русского хакера, который ломает все, что ему попадется под клавиатуру. Правда, Россия тоже не отстает, регулярно заявляя об атаках, идущих с территории Украины или Грузии (в зависимости от напряженности во взаимоотношениях с тем или иным нашим бывшим “партнером” по Советскому Союзу). Недавно стало известно, что Россию активно атакуют представители “Исламского государства”.

Желание связать конкретную атаку с конкретным государством, не разбираясь в реальных источниках и причинах, вполне себе цель в геополитической борьбе, когда надо быстро создать образ врага. Да и подпитывать его несложно - достаточно на какой-либо пресс-конференции вскользь упомянуть про “русский”, “исламский”, “украинский” след и журналисты дальше сами раздуют вокруг этого кибер-пожар.

Отдельно стоит упомянуть, что идентификация источника в сложной атаке, проходящей через несколько государственных границ и континентов, требует активного взаимодействия представителей возможно враждующих или агрессивно настроенных друг к другу государств, находящихся в разных юрисдикциях. Можно ли быть уверенным, что такое сотрудничество будет налажено? Иногда да. Например, во время подготовки и проведения Зимних Олимпийских Игр в Сочи, американские и российские спецслужбы достаточно активно взаимодействовали в рамках обеспечения безопасности игр. И это несмотря на уже произошедшее охлаждение дипломатических отношений и заморозку отдельных контактов и действия рабочих групп. Хотя, конечно, возможна и обратная картина.

Неразбериха в международном праве

По итогам Ялтинской и Потстдамской конференций был принят новый порядок мироустройства и, в частности, обеспечения международной безопасности, который, среди прочего, строился на двух ключевых понятиях - “война” и “агрессор”, которые в современных условиях морально устарели. Согласно общепринятой теории субъектами войны и агрессорами признаются целые государства. Ирак, Ливия, Сирия, Россия, Саудовская Аравия, США… Но что делать с незаконными вооруженными формированиями, например, в ДНР и ЛНР? А с международными террористическими организациями, такими как Аль-Кайеда, “Исламское государство”, Талибан? А иные негосударственные акторы, которые могут осуществлять те или иные спецоперации, несущие угрозу, не меньшую, чем со стороны целых государств? Как квалифицировать действия, осуществляемые киберанархистами и иными группами с приставкой “кибер” - Anonymous, LulzSec, КиберСотня, КиберБеркут?.. Это агрессия или нет? Действуют ли такие киберанархисты самостоятельно или они финансируются государственными структурами с целью снятия с себя ответственности и перекладывания ее на самодеятельных и “неуправляемых” хакеров?

По сути, мы сейчас находимся на пороге нового так называемого технологического уклада, когда вся система международного права претерпевает изменения, связанные с активным вторжением в нее информационных технологий. Сегодня у нас в международном праве зафиксированы основные принципы взаимодействия именно государств и в рамках именно “материальных” пространств - наземном, воздушном, морском, космическом. И только киберпространство остается полностью неурегулированным. В конце концов у нас даже общепринятого определения “киберпространства” не существует. Это если не вспоминать про такую нелюбовь представителей российских властей использовать приставку “кибер” в официальной риторике. Знаете ли вы сколько раз ООН образовывала и расформировывала специальные комиссии, которые должны были определиться с с более привычным нам термином “терроризм”? Больше 30 (!) раз. А утвержденного термина до сих пор нет. Так чего же мы хотим в отношении термина “киберпространство”?

Особую соль придает всему этому отсутствие географической привязки в киберпространстве, в отличие от пространств ведения традиционных военных операций. В качестве примера достаточно взять эту статью, которая, не выходя за пределы моего компьютера, успела попутешествовать по миру - я начинал ее писать в Киеве, продолжил в самолете над Тихим океаном, а завершил в Челябинске. И что считать местом создания этого “нематериального” материала? Вот ровно такая же ситуация и с кибератаками - почему-то их автором считается адрес компьютера, с которых зафиксировано обращение к атакуемым ресурсам. А ведь он может быть только последним в цепочке…

Интернет-анархия

Не будем лукавить, если скажем, что Интернету до сих пор присуща определенная анархия. Отсутствие четких определений, общепринятых правил и стандартов по мониторингу, учету и обмену трафиком, постоянные разговоры о privacy… Все это не способствует созданию среды, в которой можно было бы однозначно проследить за каждым сетевым пакетом или сессией. А высокие скорости передачи данных приводят к тому, что они хранятся очень непродолжительное время, за которое бывает сложно отследить злоумышленника.

Технические сложности

Технические причины лежат в основе невозможности простого определения источника атак в киберпространстве. Причем независимо от формы их реализации - в виде DDoS-атак, в виде проникновения через защитные препоны, в виде рассылок вредоносного кода через электронную почту или путем заражения сайтов и флешек с последующим попаданием во внутреннюю сеть предприятия.

Наверно никто при создании в 60-70-х годах протоколов, положивших начало современного Интернета, не задумывался о необходимости однозначной идентификации всей цепочки передачи пакетов данных из точки А в точку Б. Более того, сама по себе технология работы Интернет подразумевает децентрализацию и распределенность. И то, что устраивало всех прошедшие 40 лет, сейчас стало играть с нами дурную шутку. Как определить реального автора пришедшего мне на компьютер сетевого пакета, если я могу изменить адрес отправителя? Текущая, четвертая версия протокола IP, в принципе не подразумевает однозначную идентификацию и аутентификацию инициатора соединения (хотя разговоры об Интернет-паспортах и идентификации всех, кто входит в Интернет ведутся давно). Правда это не мешает официальным лицам и представителям военных структур заявлять об идентификации источника атаки.

Но отсутствие в текущей версии протокола IPv4 необходимых атрибутов для определения местоположения источника атаки - это еще не все, что нам мешает. Никто не запрещает злоумышленнику, желающему скрыть свое истинное местоположение, использовать любой из имеющихся в Интернет прокси-серверов (сервер-посредник) или анонимайзеров. В случае реализации атаки через них мы увидим в качестве адреса источника атаки не реальный адрес злоумышленника, а адрес сервера-посредника. И как быть в таком случае? А ведь такие сервера в множестве разбросаны по Интернет, в разных его национальных сегментах. Находясь в Пекине я могу реализовать атаку через посредника в Москве, Гаване, Рейкъявике или Гонолулу.

Ситуация усугубляется тем, что я могу арендовать специальные сервера (так

называемый abuse-устойчивый хостинг), которые будут целенаправленно скрывать мой истинный адрес, получая за эти деньги. И таких промежуточных серверов может быть много - 2, 5, 10, 100… В такой ситуации у нас атака обладает динамически меняющимися пространственными характеристиками, что коренным образом ее отличает от обычных наступательных вооружений. Может ли у нас существовать ядерная боеголовка, динамически меняющая свое местоположение? Если ее возить на специальном автотранспорте или поезде, может. Но и в данном случае ее географические координаты ограничены границами одного государства, в крайнем случае блока (и то маловероятно). Для кибератаки поменять за несколько минут или секунд свою географическую привязку и "числиться" на разных континентах в порядке вещей.

Аналогичная ситуация также возникает, если поднять "выше" по так называемому стеку Интернет-протоколов и посмотреть на электронную почту, которая может содержать угрозы или реальный вредоносный код. Идентифицировать реального отправителя почты, если он того не желает, практически невозможно. Для этого надо пройти по цепочке всех узлов, через которое проходило почтовое сообщение, и которые могут находиться в разных странах и юрисдикциях.

Отдельный вопрос с файлами и вредоносным программным обеспечением. В них нет печати и подписи (как правило, нет) автора, который таким образом желал бы оставить след в истории. Такого нет. Поэтому исследователям приходится просматривать огромные объемы информации в поисках "зерен правды", позволяющих с определенной долей вероятности определиться с источником атаки. Например, в рамках расследования операции "Нож мясника" компания Cylance собрала и изучила свыше 8 Гб данных, 80000 файлов, журналы регистрации на узлах жертв и т.п. И только после этого, правда с оговорками, она смогла заявить об иранском следе. Однако стояло ли за этой операцией государство или это была частная инициатива технический анализ так и не смог дать ответ.

Бизнес превыше всего

Какая задача стоит перед коммерческим предприятием, которое подверглось кибернападению? Долго и мучительно собирать доказательства или быстро вернуться в предатакованное состояние и продолжить прерванные операции? Почему ИТ-директоры многих коммерческих и государственных организаций любят подменять термин "информационной безопасность" термином "непрерывность бизнеса"? Да потому что задача любой организации - будь то министерство, электростанция, система управления вооружениями, банк, - обеспечить непрерывное функционирование и бесперебойность работы всех своих сервисов. И если и произошел какой-то сбой, то надо как можно скорее перегрузить сервер, переустановить операционную систему, переключиться на резервный канал. Мало кого интересует полноценное расследование с атрибуцией, которые

могут и не принести ожидаемого результата. Поэтому концепция современной защиты заключается в улучшении защитных киберстен, отражении атак и их локализации, если они все-таки попали внутрь предприятия. Задачу атрибуции мало кто перед собой ставит. И это я еще не рассматриваю ситуацию, когда организации сознательно мешают расследованию, не желая, чтобы их связывали с кибератаками или обвиняли в слабой защищенности, которая и послужила причиной успешного проникновения.

Психология и отсутствие компетенций

В психологии известен факт, что все неизвестное обычно вызывает опасение и чем старше человек, тем меньше у него желания в это неизвестное погрузиться. Кто возглавляет сегодня ключевые военные структуры России, Совет Безопасности, различные межведомственные комиссии? Люди, получившие свое образование во времена, когда компьютеров либо небыло вовсе, либо они занимали целые многоэтажные дома. А уж глобальных сетей в то время не было вовсе. Откуда им черпать знания в области киберпространства? В институтах такого не преподавали, в различных академиях тоже. Ходить на лекции в зрелом возрасте? Маловероятно. И чем старше становится человек, тем более он инертен в своих поступках и решениях. Достаточно посмотреть на текущий текст Военной доктрины РФ. и мы увидим, что используемые в ней термины «военный конфликт», «локальная война», «региональная война», «крупномасштабная война» не могут быть перенесены в киберпространство.

Поэтому мы сталкиваемся с тем, что в большинстве государств (и Россия не исключение) на высших должностях находятся люди, привыкшие оперировать понятиями, традиционными для наземных, воздушных, морских или космических пространств, но неприменимых к киберпространству. Отсюда постоянные “ляпы”, допускаемые даже в самых новых документах, имеющих отношение к рассматриваемой теме. Те, кто могут показать ошибочность такого подхода, не допускаются к разработке таких документов. А если их и допускают, то к мнению этих “безусых младенцев” не всегда прислушиваются.

Есть и другая составляющая данной проблемы. Достаточно вспомнить какой путь прошли мировые державы, вырабатывая основы ядерного сдерживания. Доверие доверием, но не стоит забывать про пословицу “доверяй, но проверяй”. Поэтому дипломатические контакты, многостороннее сотрудничество, дорожные карты, выработанные процессы и процедуры позволили если не гарантировать, то с высокой степенью уверенностью утверждать, что то или иное государство не проводит (или наоборот проводит) определенных ядерных испытаний, а также сокращает стратегические наступательные вооружения (договоры СНВ I, СНВ II и т.д.). В международной информационной безопасности, история которой насчитывает всего чуть больше двадцати лет, такого опыта нет. Более того, иногда складывается впечатление, что отдельные государства специально не идут

навстречу, чтобы скрывать свой потенциал в этой сфере.

Как можно определить участников спецопераций в киберпространстве

Хорошо, с проблемами мы разобрались. Но как же все-таки Group-IB, Лаборатория Касперского, Cisco, Cylance, Taia и другие проводят свои расследования и делают выводы об источнике атак. Как? Обычно в качестве доказательств используются следующие индикаторы (признаки):

- Место регистрации IP-адресов и доменов, участвующих в атаке, или предоставляющих инфраструктуру для реализации атаки. При этом анализируется не только страна регистрации, но и сопутствующая информация, которая может быть вытянута с помощью сервиса WHOIS - владелец домена или IP-адреса, его контакты. Все это позволяет, при превышении определенного порогового значения, сделать вывод о стране, которая "стоит за кибернападением". Если же злоумышленник не очень квалифицированный, то можно идентифицировать и физическое место расположения источника атаки. Правда, это может оказаться Интернет-кафе или библиотека, но даже такая "точность" лучше, чем "стрелять по воробьям", не имея никакого предположения о физическом местонахождении инициатора кибератаки.

- Трассировку атаки до ее источника или хотя бы локализация области, в которой источник находится. Такой функционал есть у многих маршрутизаторов, на которых стоит Интернет. Помимо механизма Traceback на сетевом оборудовании, для идентификации злоумышленников могут быть использованы механизм фильтрации трафика на интерфейсах маршрутизатора (ingress filtering), использование протокола ICMP для возврата отброшенного на жертву трафика обратно его инициатору. Например, шпионская кампания "Лунный лабиринт" (Moonlight Faze), направленная против ВПК США, НАСА и ряда американских государственных структур, "привела" в Россию именно путем анализа обратного маршрута до серверов, зарегистрированных в России (правда, связь с государственными структурами так и не была обнаружена). Аналогичный метод, правда в более сложном варианте, позволил сделать вывод о том, что за хакерской кампанией "Аврора", в рамках которой были атакованы многие технологические компании США (например, Google, Juniper, McAfee, Adobe и т.п.), стоит Китай.

- ВременнЫе параметры. Как показали примеры выше нередко исследователи анализируют время создания вредоносного кода, время начала операции в киберпространстве или время наибольшей активности. Пусть и с оговорками, но эта информация, наряду с другой, может заложить основу для дальнейшего анализа.

- Анализ программного кода, в котором могут быть найдены комментарии, ссылки на сайты, домены, IP-адреса, которые участвуют в атаке. Также и анализ функциональности программного кода позволяет сузить число возможных нарушителей. Например, анализ кода Stuxnet показал, что для его создания надо было не только знать, как работают центрифуги IR-1 в Натанзе, но и иметь стенд для проверки работоспособности вредоносного кода, который позже вывел из строя большое количество центрифуг по обогащению ядерного топлива и существенно снизил объемы его производства. Но многие ли акторы способны не только разработать, но и приобрести центрифуги IR-1 для тестирования? Это позволило существенного снизить число возможных нападавших, а с помощью дополнительных сведений, даже были названы государства, которые стояли за разработкой Stuxnet - США и Израиль.

- Помимо изучения фрагментов кода, отдельные исследователи пытаются даже изучать “почерк” программистов и определять по нему школу программирования - американская, русская, китайская и т.п. Хотя пока это скорее из области фантастики и плохо формализуемо. Однако, уже сейчас известны отдельные работы в части автоматизации и алгоритмизации процесса определения почерка программиста для дальнейшего использования этой информации в расследовании и атрибуции.

- С анализом почерка тесно связана и лингвистика, а точнее стилометрия, которая позволяет определить стилистику языка в тех же самых комментариях или сопутствующих текстах. Известно, что в зависимости от того, в какой стране родился человек, в какой культуре он рос, в какой языковой среде он воспитывался, у него будет разный стиль письма, который можно выделить и зафиксировать. Например, выросший в России или Советском Союзе человек, позже уехавщий в Великобританию или США никогда не будет говорить на языке также, как и коренной англичанин или американец. Эти различия и позволили, например, специалистам компании Taia Global сделать вывод, что за атаками на Sony стоят не северокорейские, а русские хакеры. Аналогичным образом эксперты Лаборатории Касперского предположили, что за шпионской кампанией “Маска” стоят испаноговорящие хакеры. Причиной сделать такой вывод послужило использование в коде испанских слов и сленга, которые никогда не используется англоговорящей аудиторией, не являющейся коренными жителями испаноговорящих стран.
- Обманные системы или honeypot/honeynet - популярный в своей время инструмент, интерес к которому со временем поугас, а сейчас возвращается вновь. Идея его проста - в сети запускается фальшивый, подставной узел, который и атакую злоумышленник, оставляя следы своей несанкционированной активности, которая и изучается

экспертами.

- Еще один метод - оперативная разработка, который мало чем отличается от того, что мы знаем из боевиков или детективов. Внедренные агенты, “стукачи”, “сочувствующие” и другие источники информации позволяют идентифицировать или хотя бы сузить спектр возможных акторов, стоящих за той или иной атакой.

- Анализ активности на форумах и в социальных сетях. Так в 2007-м году была выяснена причастность молодежного движения “Наши” к атакам на ряд эстонских ресурсов. Однако связь “Наших” с российскими властными структурами в данном конфликте так и не была подтверждена. Аналогичным образом, после публикации ролика на YouTube иранской хакерской группировки Izz ad-Din al-Qassam Cyber Fighters была “доказана” роль иранских хакеров (но не самого государства) в атаках на американские банки. Наконец, Сирийская электронная армия регулярно берет “на себя” атаки на отдельные американские ресурсы.

- В отдельных случаях “автора” можно идентифицировать пост-фактум по его действиям. Речь идет не только о том, что он осознанно или случайно делится фактом своего участия в социальных сетях. Например, вторжение в интернет-банк, кража денег и перевод их на подставные или реальные счета, позволяет наблюдая за владельцем счета выйти и на тех, кто стоит за ним или кто его нанял. Также украденная информация может появиться на аукционах и биржах - публичных и закрытых. Дальше следователи могут вступить в переговоры с продавцом и провести его атрибуцию или получить важную информацию для дальнейшей атрибуции кибернападения.

Мы видим, что одного, универсального и стопроцентного метода не существует. Более того, далеко не всегда техническими методами можно ограничиться. Например, когда в 2012-м году стало известно об атаке вредоносного кода Гаусс на ливанские банки, многие эксперты задавались вопросом, а зачем это надо делать? Неужели нет иных, более лакомых кусков, чем ливанские банки? И поскольку технические методы не помогли провести правильную атрибуцию, пришлось использовать косвенные признаки. Например, по анализу функций кода Gauss исследователи предположили, что он направлен на изучение счетов организации Хезболла, которая таким образом отмывала деньги, что и интересовало тех, кто стоял за атакой на финансовые институты Ливана. А учитывая, что Хезболла признана террористической организацией в ограниченном числе стран (в частности в США и Израиле), то спектр возможных инициаторов был сужен до пары государств.

Наверное, только полная перестройка архитектуры Интернета помогла бы

решить эту проблему. Но это недостижимая, а может быть и вредная мечта. Остается только совершенствовать указанные технические рецепты, обильно сдабривая их правовыми и дипломатическими приправами, позволяющими с большей уверенностью утверждать, что правильная атрибуция инициаторов спецопераций в киберпространстве возможна. И, конечно же, нельзя забывать про повышение квалификации тех лиц, которые участвуют в определении источника кибернападения. Это могут быть как сотрудники служб информационной безопасности государственных органов и критически важных объектов, так и представители правоохранительных и силовых структур, уполномоченных проводить оперативно-розыскную деятельность в киберпространстве.

Определенным подспорьем в атрибуции кибератак может служить так называемая Q-модель, разработанная Томасом Ридом и Беном Бухананом из Королевского колледжа Лондона, и способная взглянуть на процесс идентификации акторов в киберпространстве с высоты птичьего полета. Множество наводящих вопросов помогают правильно сформулировать задачу расследования и более оперативно найти виновника, стоящего за той или иной атакой.

В качестве заключения

Атрибуция киберугроз - достаточно непростая задача, которая отличается от мира физического тем, что, во-первых, мы не в состоянии идентифицировать нарушителя и его мотивацию только техническими методами. А во-вторых, спецоперации в киберпространстве часто реализуются сразу в нескольких юрисдикциях, что требует взаимодействия и сотрудничества, что не всегда возможно в текущей геополитической ситуации, когда отдельные государства не доверяют друг другу.

В таком небольшом материале достаточно сложно рассказать обо всех особенностях атрибуции киберугроз. Мы видим, что существуют как объективные, так и субъективные сложности в правильном определении источника операций в киберпространстве. Мы понимаем, что в текущей геополитической ситуации, очень часто тому или иному государству выгодно заявлять об атаках со стороны другого государства, даже не предъявляя серьезных доказательств. Мы понимаем, что существуют различные методы, позволяющие хотя бы определиться со страной, которая является источником киберугроз, но… К сожалению, пока у нас нет (исключая, быть может, оперативную разработку) методов, позволяющих провести четкую грань между атакой со стороны частного, негосударственного актора и нападением, за которым стоит держава. А значит тема атрибуции киберугроз не закрыта и будет продолжена.