RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International and of the Centre russe d'études politiques.

This issue is for your personal use only.

Published monthly in Russian and in English by *Trialogue Company Ltd.*

Issue № 7 (235), vol.15. 2016

7 ноября 2016 г.

Алексей Лукацкий сообщает из Москвы:

ЧТО НАДО ЗНАТЬ, ЧИТАЯ ОБВИНЕНИЯ В КИБЕРАТКАХ?

АНАЛИЗ ЗАЯВЛЕНИЯ МИНИСТЕРСТВА ВНУТРЕННЕЙ БЕЗОПАСНОСТИ И УПРАВЛЕНИЯ НАЦИОНАЛЬНОЙ РАЗВЕДКИ США С ОБВИНЕНИЕМ РОССИЙСКИХ ВЛАСТЕЙ В ОРГАНИЗАЦИИ КИБЕРАТАК НА АМЕРИКАНСКИЕ ПОЛИТИЧЕСКИЕ СТРУКТУРЫ

АННОТАЦИЯ

В последние месяцы количество обвинений России в кибератаках возросло многократно. Прокремлевские хакеры, по заявлениям американских политиков и СМИ, стоят за самыми громкими взломами недавнего времени – серверов Демократической партии США, антидопингового агентства WADA, американских СМИ, избирательных комиссий нескольких штатов США. Даже утечка архива кибероружия из АНБ также приписывается российским киберпреступникам, за которыми видится рука Кремля. Дело дошло до того, что министерство внутренней безопасности США (DHS) и управления национальной разведки (USIC) выступили с официальным обвинением российских властей в организации кибератак на американские политические структуры. До этого такой чести удостаивались только Китай и Северная Корея.

Член рабочей группы при Экспертном совете ПИР-Центра по международной информационной безопасности и глобальному управлению интернетом, бизнес-консультант по безопасности Cisco Systems Алексей Лукацкий предлагает разобраться в американских обвинениях и российской реакции, показать пределы и возможности определения инициатора кибератак, оценить влияние внутренней политической борьбы и глобального геополитического противостояния на возможности объективного расследования.

АТРИБУЦИЯ АТАКИ

Итак, у нас есть два актора, которые, по заявлениям DHS и USIC, участвовали в кибератаках: США, как жертва, и Россия, как нападающая сторона. Так ли это на самом деле? Когда мы имеем дело с миром материальным, в котором присутствуют ядерные боеголовки, находящиеся в шахтах на определенной территории, воинские формирования, эскадрильи самолетов или боевые группы кораблей, пребывающих в местах своей дислокации, не составляет большого труда определить, кому эти силы подчиняются. 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. С технической точки зрения, кибератака на США могла быть осуществлена из России, из самих США или с территории любого иного государства, которое хотело бы подставить Россию и обвинить ее в осуществлении недружественного акта против Штатов. Для этого достаточно было всего лишь арендовать сервер в любом из российских центров обработки данных. Можно было поступить и проще – взломать компьютер в любом из государственных учреждений Российской Федерации и удаленно использовать его в качестве источника атаки.

Для того, чтобы делать выводы о том, кто на самом деле стоит за атаками на правительственные и частные ресурсы в США, необходимо провести так называемую атрибуцию, то есть определение атрибутов кибератаки, к которым относятся ее источник, время осуществления и, самое главное, мотивация атакующего.

Для того, чтобы должным образом провести атрибуцию, необходимо собрать ряд доказательств – индикаторов, по которым и можно делать выводы о личности виновника произошедшего. К ним можно отнести:

Место регистрации IP-адресов и доменов, участвующих в атаке, или предоставляющих инфраструктуру для ее реализации. При этом анализируется не только страна регистрации, но и сопутствующая информация - владелец домена или IP-адреса, его контакты.

Трассировку атаки до ее источника или хотя бы локализация области, в которой источник находится. Такой функционал есть у многих сетевых устройств, на которых построен Интернет.

Временные параметры. 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. И хотя она не может указать на конкретного нарушителя, она позволяет сузить число стран, которые могли бы быть причастны к кибератаке.

Анализ программного кода, в котором могут быть найдены комментарии, ссылки на сайты, домены, IP-адреса, которые участвуют в атаке, тип операционной системы, в которой программа создавалась, используемый ею язык или иные региональные настройки.

Помимо изучения фрагментов кода, некоторые исследователи пытаются даже изучать «почерк» программистов и определять по нему школу программирования - американская, русская, китайская и т.д.

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.

Обманные системы или honeypot/honeynet - популярный в свое время инструмент, интерес к которому возвращается вновь. Идея его проста - в сети запускается фальшивый, подставной узел – «приманка» для киберпреступников. Ни о чем неподозревающие злоумышленники атакуют его, оставляя следы своей несанкционированной активности на изучение экспертам.

Еще один метод - ***оперативная разработка***, похожая на то, что мы часто видим в боевиках или детективах. 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. В отдельных случаях «автора» можно идентифицировать постфактум по его действиям. Речь идет не только о случаях, когда он осознанно или случайно делится в социальных сетях фактом своей причастности. Например, вторжение в интернет-банк, кража денег и перевод их на подставные или реальные счета позволяют через наблюдение за владельцем счета выйти и на тех, кто стоит за ним. 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.

КАКИЕ ДОКАЗАТЕЛЬСТВА ПРЕДОСТАВЛЕНЫ?

В совместном заявлении DHS и USIC не приводится никаких доказательств кроме общих фраз о том, что используемые методы и мотивация присущи именно России, а атака осуществлялась с серверов, принадлежащих российским компаниям. К сожалению, использование только адреса, с которого осуществляется атака, сегодня не является сколь-нибудь серьезным доказательством того, что именно владелец этого адреса и стоит за атакой. Сервер может быть не единственным в цепочке, или он мог быть взломан, а его владелец даже не подозревает об этом. Однако различные компании, проводившие исследования взломов серверов Демократической партии США (например, ThreatConnect, CrowdStrike, Fidelis, Mandiant), также строят свои доказательства только на самом простом и легко фальсифицируемом атрибуте – принадлежности адреса, с которого фиксировались атаки. В единичных случаях упоминается также часовой пояс, в котором находится Москва, что указывается в качестве доказательства «русского следа». Однако, при этом абсолютно не учитывается, что Россия расположилась в 9-ти часовых поясах, а в «московском» часовом поясе также располагается Турция, Ирак и Сирия (в зависимости от времени года), у которых также может быть своя мотивация осуществлять атаки против США.

Доказательства того, что за хакерами стоят государственные структуры России тоже оставляют желать лучшего. Например, в *Independent* это обосновывается так: "And who was responsible for the leak? Almost certainly, experts say, the Russians, directly or indirectly. For one thing, the Kremlin has a long record in doing this sort of thing, meddling in internal politics across Europe. Back when the DNC hack became public, in mid-June, Russian agents were identified as prime suspects»[1].

[1] «А кто же был ответственен за утечку? По мнению экспертов, почти наверняка это были русские, напрямую или опосредованно. Во-первых, Кремль имеет долгую историю подобных действий, когда Россия пыталась влиять на внутреннюю политику европейский стран. В середине июня, когда стало публично известно о взломе серверов Демократической партии, российские агенты были идентифицированы как главные подозреваемые» *(пер. редактора)*.

Ресурс *CrowdStrike* пишет примерно в том же ключе: «Extensive targeting of defense ministries and other military victims has been observed, the profile of which closely mirrors the strategic interests of the Russian government, and may indicate affiliation with Главное Разведывательное Управление (Main Intelligence Department) or GRU, Russia's premier military intelligence service"[2].

Таким образом, в качестве основного доказательства указывается тот факт, что атака на политические и военные цели в США может быть интересна только российским спецслужбам и никому другому. Однако однозначный ответ на вопрос «Кто?» сегодня тоже получить невозможно, не говоря уже о более сложном и важном вопросе – «Зачем?». Анализ активности в соцсетях, анализ постфактум и оперативная разработка - единственные методы для определения мотивации при совершении кибератаки, но они требуют времени.

Действительно, атрибуция кибератаки, или ответ на вопрос «Кто?», на первый взгляд, кажется менее проблемным мероприятием, чем установление ее причин. Однако и здесь есть множество препятствий, которые можно условно разделить на несколько больших направлений.

Геополитическое. Дело не только в том, что в геополитической борьбе, когда надо быстро создать и подпитывать образ врага, желание связать конкретную атаку с конкретным государством, не разбираясь в реальных источниках и причинах, часто превалирует над здравым смыслом. Не стоит забывать, что идентификация источника в сложной атаке, проходящей через несколько государственных границ и континентов, требует активного взаимодействия представителей, находящихся в разных юрисдикциях, возможно, враждующих или агрессивно настроенных друг к другу государств. А это очень непросто.

Правовое. Киберпространство сегодня остается единственным из всех пространств, включая земное, воздушное, космическое и морское, которое никак не регулируется международным правом. И все попытки установить хоть какие-то нормы поведения в киберпространстве пока не увенчались успехом. Особую соль придает всему этому отсутствие географической привязки в киберпространстве, в отличие от пространств ведения традиционных военных операций, в которых единственными акторами признаются только государства. По сути мы сейчас находимся на пороге нового технологического уклада, когда вся система международного права претерпевает изменения, связанные с активным вторжением в нее информационных технологий.

Техническое. Наверное, в 60-70-х годах при создании протоколов, положивших начало современному Интернету, никто не задумывался о необходимости однозначной идентификации всей цепочки передачи пакетов данных из точки А в точку Б. Более того, сама по себе технология работы Интернета подразумевает децентрализацию и рассредоточение. А отсутствие четких определений, общепринятых правил и стандартов по мониторингу, учету и обмену трафиком, использование промежуточных серверов-посредников, большие объемы данных и, как следствие, короткие сроки хранения цифровых доказательств только усугубляет ситуацию.

Экономическое. Ни операторы связи, ни хостинг-провайдеры, ни иные участвующие в Интернет-бизнесе компании не заинтересованы в долговременном хранении цифровых доказательств и проведении полноценного расследования кибератак с последующей их

---

[2] «Было замечено широкомасштабное таргетирование министерств обороны и других военных объектов, профиль которых совпадает со стратегическими интересами российского правительства и может сигнализировать о вовлеченности Главного Разведывательного Управления (ГРУ), главной российской службы разведки» *(пер. редактора).*

атрибуцией. Задача бизнеса - обеспечить непрерывное функционирование и бесперебойность работы всех своих сервисов, то есть быстрый возврат в состояние до атаки, что обычно приводит к уничтожению доказательств.

А ЧТО ЖЕ РОССИЯ?

Что российская сторона противопоставляет заявлениям американских СМИ и политиков? Российская Федерация выбрала вполне понятную тактику – не оправдываться и все отрицать, так как любое оправдание будет воспринято как признание вины. В России достаточно специалистов, в том числе и мирового уровня, которые могли бы провести атрибуцию и сформировать свое мнение о том, кто в действительно стоял за атаками на американские ресурсы. К сожалению, по словам министра иностранных дел Лаврова, на просьбу российской стороны обмениваться такой информацией и предоставить соответствующие материалы нашему государству, США ответили отказом. Это может быть связано как с отсутствием таких доказательств, так и наоборот, с доказательствами, которые опровергают американскую версию о «русском следе».

В любом случае у России сейчас нет никакой возможности представить свое видение сложившейся ситуации.

В отличие от катастрофы малазийского Боинга, где Россия имела возможность представить доказательства, собранные собственными средствами мониторинга и контроля, а также результаты натурных экспериментов, в случае с кибератаками такие доказательства, учитывая описанные выше сложности атрибуции, у России отсутствуют (особенно если предположить, что за атаками стоит точно не Россия) – они могут быть только на американской стороне.

Мы увидели, что существуют как объективные, так и субъективные сложности в правильном определении источника операций в киберпространстве. Мы прекрасно 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 поняли, что пусть и не всегда используются, но существуют различные методы, позволяющие хотя бы определиться со страной, которая является источником киберугроз, но...

к сожалению, пока нет методов, позволяющих провести четкую грань между атакой со стороны частного, негосударственного актора, и нападением, за которым стоят государственные органы.

В заключение хотелось бы отметить, что атрибуция киберугроз - достаточно непростая сегодня задача, которая отличается от аналогичной в мире физическом 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 обстановке, когда отдельные государства не доверяют друг другу, а то и прямо готовы безосновательно публично обвинить другую сторону.

Автор статьи: Алексей Лукацкий, член рабочей группы при Экспертном совете ПИР-Центра по международной информационной безопасности и глобальному управлению интернетом, бизнес-консультант по безопасности Cisco Systems

Редактор: Максим Мирошников

Москва-Женева, Ноябрь 2016 г.

Выдержки из документа «Международный Клуб Триалог. Условия и правила членства».

3. Права членов Клуба

3.1. Индивидуальные члены Клуба имеют право:
3.1.3. Получать 1 экземпляр бюллетеня эксклюзивной аналитики Russia Confidential по электронной почте, на выбранном языке (русском или английском). По правилам Клуба, передача бюллетеня третьим лицам не допускается.[…]
3.2. Корпоративные члены Клуба имеют право:
3.2.3. Получать 2 экземпляра бюллетеня эксклюзивной аналитики Russia Confidential по электронной почте, на выбранном языке (русском или английском) либо на обоих языках одновременно, передавать этот бюллетень другим представителям корпоративного члена Клуба. По правилам Клуба, передача бюллетеня третьим лицам, не являющимся членами Клуба, не допускается.[…]

4. Обязанности членов Клуба

4.1. Все срочные члены Клуба обязаны:
4.1.6. Не передавать полученные материалы бюллетеня Russia Confidential, а также пароли доступа на сайт Клуба физическим и юридическим лицам, не являющимся членами Клуба. […]

6. Russia Confidential

6.1. Бюллетень эксклюзивной аналитики Russia Confidential выпускается ООО «Триалог» исключительно для личного пользования членов Клуба.
6.2. Бюллетень содержит сжатую эксклюзивную аналитику по вопросам международной безопасности, внешней и внутренней политики России и государств СНГ, подготовленную ведущими экспертами специально для Russia Confidential.
6.3. В течение не менее 30 дней со дня выхода материалы бюллетеня являются конфиденциальными и не могут цитироваться и передаваться лицам, не являющимся членами Клуба.
6.4. По прошествии не менее чем 30 дней ООО «Триалог» может снять эксклюзивный и конфиденциальный статус с материала, после чего в этих случаях он может быть опубликован в других изданиях и может быть использован для цитирования членами Клуба.
6.5. Бюллетень распространяется по электронным адресам членов Клуба 1 раз в месяц по русском или английском языке, по выбору члена Клуба.
6.6. По запросу члена Клуба, он может также получить бумажную версию бюллетеня на выбранном им языке.

Уважаемые члены Международного клуба Триалог,

продолжается сезон-2016 работы Клуба, и мы рады **пригласить Вас продлить членство в Международном клубе *Триалог* на 2017 год или на 2017 - 2018 годы**.

В 2017 г. члены Клуба продолжат получать от нас эксклюзивную информацию по вопросам, связанным с приоритетами внешней политики Российской Федерации, а также современными вызовами и угрозами международной безопасности. На 2017 г. запланировано проведение **5 заседаний Международного клуба *Триалог***, 4 из которых пройдут в Москве, а 1 за рубежом. Члены клуба получат серию журнала *Индекс Безопасности в электронном виде*, **12 номеров** бюллетеня эксклюзивной аналитики *Russia Confidential* (на русском или английском языке), наши электронные информационные и аналитические рассылки.

Как и прежде, специалисты Международного клуба *Триалог* и партнерской организации ПИР-Центра открыты к обмену мнениями по ключевым международным проблемам.

Членство в клубе с 2017 г.

При оплате **до 12 декабря 2016 г.** размер ежегодного членского взноса составляет:

Период	Индивидуальное	Корпоративное
01.01.17 – 31.12.17 (1 год)	45 000 руб.	72 000 руб.
01.01.17 – 31.12.18 (2 года)	81 000 руб.	126 000 руб.

При оплате **до 31 января 2017 г.** размер ежегодного членского взноса составляет:

Период	Индивидуальное	Корпоративное
01.01.17 – 31.12.17 (1 год)	50 000 руб.	80 000 руб.
01.01.17 – 31.12.18 (2 года)	90 000 руб.	140 000 руб.

Напоминаем Вам, что в рамках **корпоративного** членства действует **схема «1+1»**, когда в работе Клуба участвуют **два представителя** одной организации.

По всем вопросам, связанным с членством в Международном клубе *Триалог*, следует обращаться по электронной почте secretary@trialogue-club.ru или по тел.: +7 (985) 764-98-96.

С уважением,

Председатель,
Международный клуб *Триалог* **Д.В. Поликанов**