Автор: Юрий Ревич © Новая газета ОБЩЕСТВО, РОССИЯ 2200 24.08.2009, 15:36 150

Хакеры в политике

Кибератаки в мире совершаются ежедневно (скорее даже — ежечасно и ежеминутно), и многие из них если и не носят открытой политической окраски, то находятся на грани политики.

Название «кибервойны» слышали, наверное, не только любители фантастических фильмов. В реальности под этим термином подразумеваются не красочные сражения роботов, а невидимые и неслышимые действия — атаки на компьютерные сети. Одна из последних таких крупных атак имеет выраженный политический подтекст — это нарушение работы нескольких крупных международных социальных сетей (сервисов Google, Facebook и Twitter), произошедшее в начале августа, в годовщину российско-грузинской войны.

Связано «обрушение» сетей, как полагают их администраторы, с атакой на одну-единственную персону: активного блоггера прогрузинской ориентации под псевдонимом Сухуми. Однако официально руководители этих сервисов воздерживаются от комментирования причин форс-мажора — точно установить, кто и зачем атаковал сайты, невозможно. 15 августа мощнейшей хакерской атаке подвергся сайт «Движения в защиту Химкинского леса»[1]. И таких новостей о серьезных хакерских атаках только за это лето набралось больше десятка.

…Первым толчком для повышенного интереса к теме кибератак со стороны общественности США как страны, наиболее уязвимой для подобного рода злоупотреблений, стало вполне художественное произведение. Захватывающий фантастический триллер «Военные игры», вышедший в 1983 году, произвел сенсацию во всех слоях американского общества — от обывателей до конгрессменов, а также вызвал озабоченную реакцию и среди специалистов-компьютерщиков, и в спецслужбах. В «Военных играх» некий хакер[2] Дейв проникает в сети Пентагона и непреднамеренно чуть не вызывает третью мировую войну. Этот сценарий и по сей день не дает покоя политикам (равно как и писателям-фантастам) во всем мире.

На самом деле, конечно, запустить стратегическую ракету хакеры не в состоянии при всем желании. По большому счету, они не в состоянии даже парализовать автоматическую систему управления автомобильным движением на перекрестках Манхэттена или проникнуть в узел распределения электроэнергии штата Нью-Йорк. По одной простой причине: все такие сети к Интернету не имеют никакого отношения, ибо физически от него изолированы. Автор своими глазами видел, как устроена компьютерная сеть одного нашего суперсекретного ведомства: доступ к Интернету там предоставляется из отдельной комнаты, до недавнего времени — лишь с письменного разрешения руководителя подразделения. Разумеется, преодолевать по воздуху метры, разделяющие подключенные и неподключенные к Интернету компьютеры, хакеры еще не научились, и помочь им тут вряд ли смогут даже завербованные инсайдеры.

Но вот что хакеры могут — так это получать доступ к информации, в том числе и секретной. Информационные каналы нередко связаны с Интернетом поневоле (хотя бы потому, что правительственным и военным учреждениям приходится обмениваться информацией с внешним миром), и именно с такими злоупотреблениями связано большинство нашумевших скандалов последних лет. Немало помогают хакерам и ошибочные действия администраторов некоторых сетей: скажем, если на одном и том же компьютере имеется доступ и к защищенному участку сети, и к обычному Интернету, то попасть извне в защищенный сектор — лишь дело техники, причем соответствующие приемы хорошо отлажены, а многие из них и общедоступны.

Один из самых впечатляющих скандалов последнего времени, связанных с подобными недостатками сетей, — проникновение взломщиков в компьютеры иностранных представительств по всем миру, обнаруженное осенью прошлого — весной текущего года канадскими службами. Началось с того, что к экспертам по компьютерной безопасности из компании Information Warfare Monitor обратились представители тибетского духовного лидера в изгнании далай-ламы с просьбой проверить, не отслеживается ли содержимое их компьютеров. Десятимесячное расследование показало, что внедренный вирус-троянец контролировал 1295 компьютеров в 103 странах, в основном — в посольствах азиатских стран, однако он был также обнаружен и в представительствах Германии, Португалии, Румынии, Кипра, Мальты и др. Это был один из самых квалифицированных взломов в истории: эксперты говорят, что вирус давал возможность использовать даже аудио- и видеозаписывающие устройства, подключенные к зараженным компьютерам, для того чтобы вести

прослушку и наблюдение в тех комнатах, где они установлены. Разумеется, вирус обезвредили, но официальных обвинений предъявлять некому, и неизвестно даже, было ли это чьей-то самодеятельностью или санкционированной акцией каких-то спецслужб. Следы ведут на территорию Китая, но официально правительство КНР от этой истории, конечно, отмежевалось и проводить расследование у себя также не стало.

Другая известная история, скорее анекдотическая и больше напоминающая сюжет «Военных игр», только без глобальных последствий, тянется уже несколько лет. А начало ее относится к 2001—2002 годам, когда британский хакер Гари Маккиннон взломал 97 компьютеров Пентагона и NASA с единственной целью поискать доказательства существования пришельцев и НЛО. Когда американцы раскрутили всю цепочку его проникновений и представили себе на его месте настоящего злоумышленника, у них волосы встали дыбом: в США и сейчас называют инцидент «крупнейшим взломом военных объектов».

В июне 2005-го Маккиннона арестовали в Лондоне, но до сих пор ему удается успешно отбиваться от экстрадиции в Штаты, где не делают скидки на цель проникновения, и потому «преступнику» грозит 60 лет заключения. Многие специалисты по компьютерной безопасности уверены, что таких «санитаров леса», как Гари, следует не сажать, а награждать — они ведь реально никаких преступлений не совершили, зато сделали крайне полезное дело, указав службам безопасности на собственные промахи.

Кибератаки в мире совершаются ежедневно (скорее даже — ежечасно и ежеминутно), и многие из них если и не носят открытой политической окраски, то находятся на грани политики. Причем с кражей информации связаны единичные случаи (и, вероятно, большая часть их остается неизвестной широкой публике), основная же цель злоумышленников в таких акциях — навредить супостату. Таковы были, скажем, нашумевшие атаки российских хакеров на эстонские сайты в мае 2007 года, приуроченные к переносу памятника советскому солдату, или атаки на американские и почему-то южнокорейские сайты, предпринятые уже в июле этого года, в День независимости США.

Обычная схема проведения таких атак — простая перегрузка сервера супостата путем непрерывного направления на него тысяч ложных запросов. Она носит название DoS-атаки (от Denial of Service, отказ в обслуживании) и весьма эффективна, потому что даже сайтам, обслуживающим миллионы посетителей и занимающим целые дата-центры[3] (таким как упоминавшиеся социальные сети), не удается справиться с ней сразу, в реальном времени.

Но и для проведения такой атаки на мощный ресурс нужны соответствующие средства. Обычно их роль играют сети зараженных компьютеров — ботнеты. Разумеется, для создания ботнета нужно время и хорошая организация работы, потому невозможно отрицать, что большинство спланированных атак, в том числе и политически мотивированных, производится организованными группами профессионалов. Известный деятель Рунета Александр Венедюхин утверждает, что ряд таких атак производится организованными группами добровольцев: «Можно собрать добровольцев (сторонников), которые осознанно установят на свои компьютеры требуемое ПО (вооружатся) и примут участие в атаках». Но все же, видимо, главную роль играют деньги, а не идеи: увы, компьютерные преступления сейчас стали выгодным бизнесом. Сергей Воробьев из компании «1С-Битрикс»: «Кто хакерам платит, тот их и танцует. И если платит политик, то получаем «политическую мотивацию». Единственная же реальная мотивация исполнителей — деньги».

Если вернуться к атаке на блоггера Сухуми, которая прогремела на весь мир из-за своей масштабности (в частности, суперпопулярный Twitter был почти недоступен целых два часа), то довольно оригинальное мнение об этой акции высказал Павел Шевчук, владелец фирмы из Новой Зеландии, производящей ПО для обеспечения интернет-безопасности: «Одновременный отказ в обслуживании трех крупнейших социальных сетей наводит на мысль, что это была тренировка спецслужб, а грузинский блоггер — лишь прикрытие. Слишком дорогостоящая операция — положить такие крупные кластеры серверов, чтобы стрелять из пушки по воробьям. Службы какой именно страны проводили эту тренировку — сложно сказать. Вроде все указывает на российские, но вполне могут и другие. В общем, это нормально, ничем не хуже возможности США заблокировать GPS или снятия шифрации с GSM на время проведения антитеррористической операции. С этой возможностью придется мириться и надеяться, что события, которые могут привести к такой необходимости, будут случаться не часто».

Как ни крути, но во всех подобных делах приходится полагаться на домыслы, пусть и правдоподобные. Раскрутить дело до конца удается лишь в мизерном количестве случаев — в основном лишь для таких «психов-одиночек», как Гари Маккиннон. А в подавляющем большинстве случаев ни что-то доказать, ни найти какие-то концы, а часто — даже понять явные цели и мотивы взломщиков невозможно. Не потому ли правоохранительные органы США так бросаются на каждый расследованный случай, независимо от

мотивации и последствий, что это позволяет хотя бы ориентировать общественное мнение в нужную сторону?

Резюмируя, можно сказать, что значение и роль кибератак в политике все же заметно преувеличены — сегодня это скорее потенциальная угроза. Подавляющее большинство населения даже развитых стран узнает о таких акциях из телевизионных новостей и больше никак от них не страдает. Беда только в том, что никто не может сказать, в случае каких событий и как быстро эта опасность перейдет во вполне реальную плоскость, оказывая решающее влияние на обстановку. Но в том, что такое в принципе возможно, не сомневается никто.

[1]Атака, скорее всего, была связана с тем, что экологи разместили на сайте письмо в адрес Европейского банка реконструкции и развития. В письме они просили не финансировать строительство автомагистрали Москва — Санкт-Петербург до тех пор, пока проект не будет изменен «в сторону» спасения Химкинского леса.

[2]Вот откуда пошла мода обзывать хакерами зловещих компьютерных преступников, хотя на самом деле это просто самоназвание сообщества компьютерных энтузиастов высокой квалификации. Достаточно указать, что хакерами являются и автор свободной операционной системы Linux Линус Торвальд, и основатель движения за «свободное программное обеспечение» Ричард Столлмен, и многие другие известные своими вполне позитивными достижениями деятели компьютерной отрасли.

[3]Дата-центр — специализированное здание (площадка) для размещения серверного и коммуникационного оборудования.

Автор: Юрий Ревич © Новая газета ОБЩЕСТВО, РОССИЯ 2200 24.08.2009, 15:36 150
URL: https://babr24.com/?ADE=80437 Bytes: 10963 / 10876 Версия для печати

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