Хактивизм как угроза государственным информационным ресурсам

Обухов Сергей Николаевич, руководитель специальных проектов и программ ЗАО «Позитив Текнолоджиз»

Интернет сегодня объединяет более двух миллиардов человек по всему миру, охватывая большую часть населения развитых стран. Неудивительно, что при такой аудитории он стал не просто средством коммуникации, но площадкой для решения многих задач, в том числе и политических. Интернет активно используется различными политическими силами для организации протестных движений в разных странах, в том числе и в России.

В последнее время получила популярность особая экстремальная форма виртуального протеста — хактивизм. Это организованные целенаправленные атаки большого количества пользователей на информационные ресурсы органов государственной власти и аффилированных с ними коммерческих компаний. Как правило, такие атаки связывают с сообществом Anonymous.

В ряде СМИ Anonymous называют организацией, целью которой является борьба с различными видами социальной несправедливости. Это не совсем корректно: Anonymous не являются организованной силой. Фактически любой участник движения может провозгласить «крестовый поход» во имя какой-либо общественно значимой цели — от защиты арктического шельфа до борьбы за демократию в отдельно взятой стране. К нему присоединяются те участники, которым декларируемая цель особенно близка.

Иногда движение Anonymous называют хакерским, что также неверно. Действительно, хакеры принимают участие в акциях Anonymous. Одна из хакерских групп — Lulzsec — даже объявила об «официальной» поддержке движения, но основная масса участников — обычные пользователи со средним уровнем компьютерной грамотности. Несмотря на громкие заявления о готовности «выключить Интернет» и взломать любые информационные ресурсы органов государственной власти, акции Anonymous, как правило, сводятся к организации DDoS-атак с привлечением большого количества добровольных помощников, домашние компьютеры которых используются в качестве генераторов паразитного трафика. Иногда, тем не менее, участники движения проводят и успешные хакерские атаки на государственные информационные системы.

Хактивизм в России

Хотя акции Anonymous проводятся с 2009 года, организованные акции российских хактивистов начались в феврале 2011 года, когда в Twitter появилась лента @Op_Russia. Поначалу действия хактивистов ограничивались организацией DDoS-атак на сайты органов государственной власти и призывами к участию в уличных протестах.

После президентских выборов и акции на Болотной площади действия хактивистов стал более агрессивными. С марта по май 2012 года делались неоднократные попытки провести DDoS-атаки на веб-сайты силовых ведомств. Публиковались сообщения об успешных атаках на информационные ресурсы Правительства и телеканала НТВ, но эти сообщения опровергались СМИ. В мае появились сообщения об аресте нескольких российских участников движения и призывах к хакерским атакам на веб-сайты МВД, ФСБ и Правительства.

17 мая появилось подтвержденное сообщение о получении хактивистами доступа к одному из FTP-серверов системы госзакупок. С помощью неназванной уязвимости хакерам удалось получить в свое распоряжение имя пользователя и пароль, предоставляющие доступ к файлам данных. Правда, по собственному признанию хактивистов, разобраться со структурой дан-

ных им так и не удалось «в силу природной лени».

20 мая появилось сообщение об успешной атаке на один из почтовых серверов МВД России. Анализ публикаций показал, что хактивисты скопировали не переписку, а конфигурационные файлы и журналы аудита, которые из-за некорректной настройки сервера оказались доступны из сети Интернет. Однако несмотря на то, что реального ущерба эта атака не причинила, в ряде электронных СМИ этот инцидент был охарактеризован как получение хакерами контроля над ведомственной электронной почтой.

13 июня хактивисты опубликовали сообщение о критической уязвимости (внедрение операторов SQL) на сайте Минэкономразвития. Хакеры опубликовали скриншоты, подтверждающие наличие самой уязвимости и возможность чтения с ее помощью файлов операционной системы. Как правило, подобные уязвимости являются удобными точками входа для преодоления периметра защиты и получения контроля над всей информационной системой, но в данном случае хакеры, по-видимому, даже не попытались развить атаку.

15 июня, воспользовавшись уязвимостью в системе управления контентом, хактивисты разместили сообщение с протестом против введения ЕГЭ на информационном портале ЕГЭ Санкт-Петербурга. Как и в предыдущем случае, несмотря на то что ресурс практически находился под контролем хакеров, они ограничились мелкой пакостью.

Наконец 20 августа в знак протеста против вынесения приговора участницам акции Pussy Riot хактивисты организовали атаку на Хамовнический районный суд. На страничке в Facebook был опубликован текст петиции на русском и английском языках, которую предлагалось отправить на адрес электронной почты суда. Кроме того, хакеры провели успешную атаку на веб-сайт суда, скопировав и опубликовав около 500 писем, поступивших на адрес ведомственной электронной почты суда в течение 20 августа. Большая часть писем — поступившие в суд петиции, однако ряд опубликованных сообщений относится к служебной переписке суда с подразделениями судебного департамента. Несмотря на то что доступ к корпоративной электронной почте дает хакеру отличные возможности для проведения атак с использованием социальной инженерии, в данном случае хактивисты снова ограничились демонстрацией самого факта успешной атаки.

Уроки, которые стоит извлечь

Несмотря на громкие заявления о «безжалостной борьбе с режимом» и техническую возможность причинить серьезный ущерб атакованным информационным ресурсам, российские хактивисты пока ограничиваются PR-акциями. Независимо от того, получат ли их действия продолжение, проведенные акции — серьезный повод для операторов государственных информационных систем провести работу над ошибками. Из сложившейся ситуации можно сделать несколько выводов.

Недооценена угроза хакерских атак. В политиках информационной безопасности российских ведомств возможность хакерских атак рассматривается, в основном, только в контексте целенаправленных действий зарубежных спецслужб. При этом в качестве целей нарушителей рассматриваются только важные для деятельности ведомств информационные ресурсы.

Как видно из примеров выше, все не так просто. Чувство собственной важности оказывается серьезным стимулом, мотивирующим хакеров атаковать государственные информационные ресурсы несмотря на связанную с этим опасность. При этом они не фокусируются на избранных системах, а атакуют любые, в которых обнаруживаются пригодные для эксплуатации уязвимости.

Недооценены последствия хакерских атак. Усилия по защите отдельно взятой государственной информационной системы (ГИС), как правило, пропорциональны важности обрабатываемой в ней информации. Такая стратегия не учитывает два аспекта. Во-первых, любая ставшая публично известной успешная атака на ГИС приводит к общественному резонансу и репутационному ущербу органам государственной власти. В результате такой инци-

дент приводит к заметным последствиям в виде трудозатрат на восстановление нормальной работоспособности и расследование инцидента, а также кадровым изменениям, незапланированной (и не всегда оправданной) закупке дополнительных средств защиты «для галочки» и т. п.— иными словами, к прямому ущербу для бюджета.

Во-вторых, что гораздо хуже, современные информационные системы строятся таким образом, что успешная атака на второстепенный ресурс позволяет хакеру преодолеть периметр защиты и атаковать информационную систему организации изнутри, встречая значительно меньшее противодействие со стороны системы защиты. Это общая беда частного и государственного секторов: наличие даже одного уязвимого узла на периметре защиты предоставляет нарушителю техническую возможность получить контроль над всеми информационными ресурсами организации. Учитывая тенденцию к укрупнению ведомственных информационных систем и централизации информационных ресурсов, уязвимости даже второстепенных ресурсов ставят под угрозу технологические процессы всего ведомства.

Неготовность к отражению угрозы. Как правило, успешные хакерские атаки приводят к предсказуемой реакции — восстановить работоспособность системы и найти виноватых. Беда в том, что подобный реактивный подход не позволяет предотвратить инциденты или снизить причиняемый ущерб. Для того чтобы обеспечить реальную защиту, нужно уметь смотреть на свои ресурсы глазами нарушителя.

В целом инциденты с участием хактивистов вызывают серьезную озабоченность экспертов. Получившие известность акции стали возможными благодаря серьезным уязвимостям государственных информационных систем, которые легко обнаруживаются и используются даже неспециалистами. Квалифицированный хакер в таких условиях способен реализовать гораздо более опасные угрозы вплоть до проникновения в ведомственные вычислительные сети и получения контроля над информационными ресурсами. Можно констатировать, что на сегодняшний день для российских ведомств угроза кибератак более чем актуальна.

Стратегия противодействия

Что же делать на практике? Прежде всего стоит обращать внимание на реальную безопасность. На сегодняшний день принцип самостоятельного контроля защищенности и устранения выявленных недостатков — единственный эффективный ответ угрозе хакерских атак. Требования к реализации подобного контроля закладываются в принимаемые государственными регуляторами нормативные документы.

Как видно из приведенных примеров, российские хактивисты (впрочем, как и зарубежные) — отнюдь не компьютерные гении. Как правило, хакеры добиваются успеха, комбинируя три способа атаки:

- использование уязвимостей веб-приложений;
- использование уязвимостей ПО с помощью уже готовых инструментальных средств;
- поиск учетных записей со словарными или восстанавливаемыми паролями.

Для выполнения таких атак не требуется большой объем ручной работы: поиск и эксплуатация подобных уязвимостей давно автоматизированы. Но точно так же автоматизированы и способы выявления этих уязвимостей операторами информационных систем. На российском рынке представлен ряд автоматизированных средств контроля защищенности, в том числе и сертифицированных ФСТЭК России. Использование таких средств позволяет операторам информационных систем самостоятельно обнаруживать уязвимости и устранять их до того, как они будут использованы нарушителем.