# Обзор самых крупных кибератак

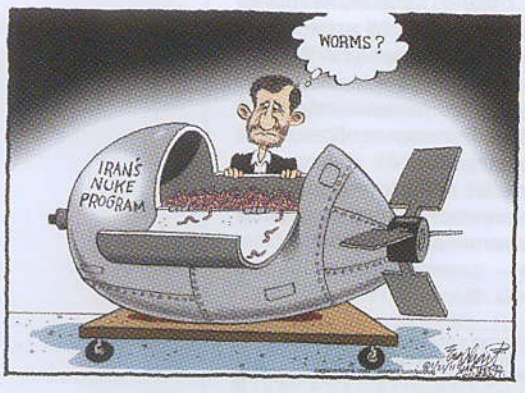
**Денис Гасилин,** *руководитель отдела маркетинга SafenSoft*

Крупномасштабные кибероперации не происходят только между представителями разных стран и идеологий. Высокоорганизованные криминальные элементы вносят свой вклад в развитие средств нападения на элементы информационной сети.

Каждый год мы становимся свидетелями достаточно крупных кибератак, которые наносят значительный урон не только финансовым структурам, но и, что более серьезно, объектам с критически важной инфраструктурой.

Атаки на страны и финансовые институты не сводятся только к прямым атакам на их инфраструктуру. Взлом твиттер-аккаунта Associated Press так называемой сирийской электронной армией с последующим размещением информации о покушении на президента США Барака Обаму привел к кратковременному, но очень серьезному биржевому хаосу – индекс Dow Jones Industrial average упал более чем на 100 пунктов, а Standard & Poor's 500 потерял более $130 млрд.

Менее крупные инциденты происходят постоянно, в качестве примера можно привести публикацию информации с 400 тыс. украденных израильских кредитных карт в Интернете хакерами из Саудовской Аравии с обещанием опубликовать еще миллион, в ответ на что израильские хакеры начали публиковать в открытом доступе украденные карты граждан Саудовской Аравии. Впрочем, финансовые потери от кибердаров иногда бледнеют по сравнению с угрозами для критически важной инфраструктуры государства, такими как возможность отключения электростанций или целых систем минобороны через Интернет.




Еще в 2002 г. безработный системный администратор из Хорсни, Северный Лондон, 36-летний Гарри Маккиннон был осужден судом США за взлом более 90 военных компьютеров в NASA, Пентагоне и министерстве обороны. Все, что понадобилось ему для взлома, – общедоступное ПО, сканирующее большое количество адресов на наличие известных уязвимостей в автоматическом режиме. Обнаруженные с тех пор уязвимости на самых разных уровнях защиты различных объектов не были использованы злоумышленниками по одной простой причине – первыми эти дыры в защите обнаруживали лояльные своим странам хакеры.

При этом важно понимать, что крупномасштабные кибероперации не происходят только между представителями разных стран и идеологий. Высокоорганизованные криминальные элементы вносят свой вклад в развитие средств нападения на элементы информационной сети. Так, Silk Road ("Шелковый путь"), один из наиболее известных ресурсов внутри полностью децентрализованной системы TOR, использовавшийся в первую очередь ради торговли наркотиками и оружием, был захвачен и выведен из строя службами правопорядка США исключительно благодаря действиям спецслужб в информационной сфере. Череда допущенных администратором ресурса промахов, среди которых было использование почты от Google с настоящим именем в качестве имени пользователя и заказ киллера в Канаде с целью устранения одного из поставщиков наркотиков, шантажировавшего администратора передачей данных покупателей в свободный доступ, привела специальных агентов к следам подозреваемого в публичной части сети Интернет. Установление его паспортных данных с этого момента являлось делом времени благодаря неафишируемому на тот момент сотрудничеству крупнейших IT-компаний со спецслужбами США, после чего и был обнаружен физический сервер, обеспечивающий работу ресурса. Перехват контроля над этим сервером позволил органам госбезопасности завладеть всей имевшейся на нем информацией, а впоследствии – закрыть ресурс и привлечь администратора к ответственности. Несмотря на не поддавшуюся с технической точки зрения защиту сети, один из крупнейших ее ресурсов был захвачен и выведен из строя с помощью применения в нужном сочетании информационных технологий, социальной инженерии и административного ресурса.

Кроме того, необходимо помнить, что понятие криминальности приобретает различные формы в разных уголках земного шара.

Использующаяся в том числе для расчетов между пользователями "скрытой сети" на ресурсах вроде Silk Road виртуальная валюта Bitcoin уже долгое время обращает на себя пристальное внимание различных судебных инстанций.

В мае этого года Department of Homeland Security в США захватил учетную запись одного из крупнейших международных процессинг-центров этой "валюты" на основе обвинения в фальсификации финансовых документов. Но по-настоящему распределенную сеть невозможно уничтожить или захватить традиционными средствами, так что война за существование таких сервисов неизбежно перетекает в информационное пространство. Например, внезапное раскрытие подробностей атаки на Silk Road вкупе с про-

сочившимися слухами о компрометации сети TOR на несколько дней серьезно пошатнуло курс Bitcoin, не только замедлив его стремительный рост по отношению к традиционным валютам, но и понизив его на несколько дней. Да и сама сеть TOR, отличающаяся от обычного Интернета повышенным уровнем анонимности пользователя, давно привлекает внимание неустановленных официально лиц, обладающих тем не менее весьма обширными ресурсами. В этом году на ресурсы сети Freedom Hosting ("Хостинг свободы"), после ареста его владельца в Ирландии и экстрадиции в США, была внедрена уязвимость нулевого дня, использовавшая слабость стандартного для сборки Tor Bundle браузера к определенной javascript-инъекции, на протяжении неустановленного времени собиравшая информацию обо всех посетителях сайтов данного хостинга, не отключивших javascript вручную, и отправлявшая полученную информацию в неустановленную базу данных. Впрочем, даже использование TOR само по себе не гарантирует безопасность – перехват трафика на одном из экзит-нодов сети, не использовавших надежное шифрование входящей и исходящей информации, позволила держателю нода еще в 2007 г. завладеть учетными записями и паролями, среди прочих, сотрудников посольства России в Швеции и центра получения заявок на визу в Великобританию в Непале. Посольства различных стран зачастую используют эту сеть с целью избежать контроля со стороны местных провайдеров доступа к сети Интернет.

Захват серверов торрент-трекеров, как в случае с ресурсом Demonoid.me, и отключение отдельных ресурсов всего лишь по подозрению в распространении нелегального контента вписываются во все ту же мировую тенденцию завершать конфликты интересов в информационном пространстве силой. Недавние откровения бежавшего в нашу страну Эдварда Сноудена о мировой сети перехвата и сбора информации служат лишь дополнительным подтверждением того, о чем миру и так было неофициально известно на протяжении последнего десятилетия.

## Заключение

Таким образом, в наше время любой человек может попасть под направленную на какую-либо страну или какой-либо сервис массированную кибератаку вне зависимости от его желания участвовать в киберконфликтах. Вопросы безопасности становятся критичными для каждого пользователя, причем они включают в себя не только защиту от вредоносного кода, но и сопротивляемость к атакам с применением социальной инженерии, административного ресурса и внедренных в программное обеспечение уязвимостей еще до выхода на рынок. Как только же речь заходит о бизнесе, государственных организациях или последователях некой идеологии, к кибервойнам становится недостаточно просто готовиться – они уже идут.

**Ваше мнение и вопросы присылайте по адресу**
**infosec@groteck.ru**

Необходимо помнить, что понятие криминальности приобретает различные формы в разных уголках земного шара.