

Провайдеры и хакеры

Защита информации является одной из ключевых задач провайдеров. Хакеры, взламывая учетные записи пользователей, незаконно получают бесплатный доступ к сети, закрытые от посторонних личные данные, в том числе пароли, которые используют в преступных целях. В данной статье анализируются некоторые преступления отечественных и зарубежных авторов, а также сравниваются различные методы подхода к борьбе с этими преступниками.

Иностранный опыт. Преступление...

Итак, в июле 2012 один из крупнейших голландских провайдеров обнаружил, что с его серверов неизвестными злоумышленниками было украдено около 800 тыс. учетных записей. Информация выплыла наружу только после того, как пользователь, обладающий аккаунтом с административными правами, не смог в него попасть.

Данные пользователей были похищены с целого ряда популярных веб-ресурсов. При этом методика действия хакеров до последнего момента оставалась неизвестной. Как стало известно, утечку обнаружил один из активных членов сообщества Hack Ende, девушка, которая не смогла зайти в административный аккаунт и поняла, что он был взломан. Провайдер предложил устранить проблему своими силами, но члены Hack Ende настояли, чтобы он обратился в полицию. Как оказалось, параллельно хакеры взломали еще один сервер провайдера, который был немедленно отключен от Интернета. Но, как признаются официальные лица, причастные к расследованию, вычислить хакеров, которые произвели атаку, будет невероятно сложно, несмотря на активную помощь общественности.

Но сколь бы ни был удачен киберпреступник, он все равно понесет заслуженное возмездие. Совсем недавно, американский хакер Райан Харрис, известный в сети под ником DerEngel, был приговорен к трем годам тюрьмы. Он взламывал Интернет-провайдеров, после чего прошивал модемы и реализовывал их потребителям по цене около 100 долларов. Модем обходил фильтры, установленные провайдерами, и покупатель мог пользоваться скоростным безлимитным Интернетом совершенно бесплатно. Он также реализовывал программы типа «Blackcat», «Sigma» или «DreamOS», с помощью которых можно было настроить безлимитный или даже бесплатный выход в Интернет через ничего не подозревающего провайдера.

Незаконная деятельность продолжалась в течение нескольких лет, в течение которых Харрис незаконно получил от своих клиентов около 1 млн. долларов. Уверовав в безнаказанность, он даже начал писать книгу о том, как взламывать кабельные модемы. По информации компании Chapter Communications, которая сильнее всего пострадала от действий хакера, она до сих пор не может определить все фальшивые модемы, что приводит к потере средств и репутации, в случае отключения законопослушных клиентов.

....и методы противодействия

В плане борьбы с кибертерроризмом интересен опыт 18-ти крупнейших мировых провайдеров уровня BT Group, MCI и Deutsche Telekom, которые еще в 2005 году создали антихакерский альянс, противостоящий разгулу сетевой преступности. В техническом плане, основным направлением их деятельности является раннее обнаружение и отражение DDoS-атак. Для этого была создана специальная система, которая отслеживает скачкообразный рост запросов на тот или иной сайт. Количество запросов анализируется, и, если система делает вывод, что это похоже на хакерскую атаку, оповещает провайдера. По расчетам специалистов, эта защита позволяет провайдерам сохранить сотни миллионов долларов.

Для эффективного внедрения проекта компании договорились оборудовать свои серверы двумя дополнительными устройствами. Это детектор со встроенными интеллектуальными функциями, который способен проанализировать плотность запросов на каждый конкретный адрес и распознать DDoS-атаку. Это достаточно сложная операция, поскольку при активном продвижении сайтов, например, размещении ссылок на популярных ресурсах, резкий рост посещаемости можно принять за атаку хакеров. Именно для анализа и отслеживания подобных случаев и нужен детектор. Второе устройство, устанавливаемое на серверах, – блокиратор. В случае если детектор принимает решение, что произошла DDoS-атака, он направляет трафик на блокиратор. Это устройство может заблокировать доступ к ресурсу, но в большинстве случаев достаточно просто замедлить его. В более сложных устройствах отслеженный детектором трафик атаки попросту блокируется, а обычные пользователи, с нормальной частотой запросов продолжают свободно проникать на страницы ресурса. После окончания хакерской атаки, поток снова направляется напрямую. Одновременно информация о DDoS-атаке распространяется среди всех провайдеров, которые состоят в альянсе, сводя вред от действий киберпреступников к минимуму.

Особенно важно такое взаимодействие, когда атака производится с привлечением ботов, действующих с огромного количества адресов. При этом адреса, атакующие провайдера, могут быть расположены по всему миру, в этом случае партнерские компании предлагают провайдеру

дополнительные каналы для пропуска информации, для того, чтобы минимизировать ущерб нанесенный DDoS-атакой. На сегодняшний день известны атаки силой до 15 ГБайт в секунду, которые могут полностью заблокировать работу провайдера на неопределенное время, причем методики атаки меняются 2-3 раза в час. Совместные действия крупнейших провайдеров в такой ситуации позволяют не только препятствовать блокированию серверов, но и выявлять злоумышленников, совершающих эти преступления.

А в родном Отечестве....

Многие российские хакеры уверены, что если они не будут трогать серверы отечественных провайдеров, то иностранные службы ничего не смогут с ними сделать. Но это только иллюзия. Интересна история задержания двух челябинских программистов Василия Горшкова и Алексея Иванова, произошедшая в начале 2000-х годов. Хакеры внедрялись в системы провайдеров и за определенную плату предлагали устранить возникающие проблемы. Особенно они насолили компаниям, хранящим базы данных кредитных карт. Американским властям пришлось разработать целую спецоперацию по заманиванию Горшкова и Иванова в Сиэтл и спровоцировав их на незаконные действия. Оба злоумышленника отделались тюремным заключением и солидным штрафом.

С тех пор отечественное законодательство стало гораздо более строгим к киберпреступникам, но количество таких преступлений не уменьшается. Это связано, прежде всего, с лавинообразным увеличением количества пользователей сети Интернет, а также набора сервисов, которые предлагаются в сети. Сегодня стоимость взлома электронной почты колеблется от 2 до 3 тысяч рублей. Это позволяет получать закрытую информацию, находить пароли от всевозможных ресурсов, в том числе и административных аккаунтов провайдеров. Заказы делаются на специальных форумах, доступ в которые закрыт обычным пользователям. Часто хакеры занимаются скупкой случайно отобранных и взломанных аккаунтов электронной почты, для последующего использования полученной информации. В этом случае они готовы платить от 4 до 5 тысяч долларов за несколько тысяч подобных ресурсов.

На сегодняшний день многие наши операторы связи не обращаются со своими проблемами в органы государственной власти, а предпочитают бороться со взломами собственными силами. Для этого они устанавливают специальные системы контроля и защиты, а также нанимают антихакеров, которые отслеживают и удаляют аккаунты своих коллег.

Поскольку провайдеры предпочитают бороться со всеми проблемами самостоятельно, абоненты получают снижение качества предоставляемых услуг. Наверное, нет ни одного пользователя Рунета, который не сталкивался с проблемами при входе на ресурс, заблокированный в результате DDoS-атаки. В данный момент времени компании, предоставляющие коммуникационные услуги, ограничиваются установкой оборудования, отслеживающего и блокирующего хакерские атаки, но это не решает проблему снижения трафика. Только подписание договоров о сотрудничестве и взаимопомощи по примеру западных компаний позволит эффективно противостоять киберпреступникам и избежать огромных убытков, которые из-за их деятельности несут отечественные провайдеры.

В принципе эффективным способом борьбы с хакерами может стать некая некоммерческая организация, которая объединила бы представителей различных провайдеров неким пактом о совместном противодействии хакерам, обменом информацией и совместном использовании ресурсов для противостояния DDoS-атакам.

Более того, такая организация могла бы эффективно сотрудничать с тем же отделом «К» в вопросах выявления хакеров. Примером такого взаимодействия органов правопорядка с некоммерческими объединениями может служить деятельность екатеринбургского фонда «Город без наркотиков» с наркополицией нашего города. «Город» выявляет наркоторговцев, наркополиция проводит оперативные мероприятия. То же самое возможно в нашем случае — провайдеры вычисляют хакеров и сдают их киберполиции.

Так или иначе, а зарубежный опыт наглядно демонстрирует эффективность совместных действий провайдеров против кибер-преступников. Отечественным операторам связи стоит хотя бы попытаться провести переговоры на эту тему и обсудить возможность консолидации усилий в борьбе с хакерами.