ТЕЛЕКОМ

интернет-сообщество

«Антиплагиат» не пройдет

(Окончание. Начало на стр. 25)

Корреспонденту «Ъ-Телекома» удалось связаться с разработчиком «Киллера». Им оказался программист из Москвы. Представившись Георгием, он рассказал о причинах, которые побудили его создать эту программу: «Мой знакомый, который сейчас в аспирантуре учится и готовится защищать кандидатскую, столько сказок и страшных историй мне рассказывал, что я просто диву дался, как далеко прогресс ушел». Однако затем, поработав с программой, Георгий обнаружил, что ее легко обмануть: «Идея реализована из рук вон плохо. А ВАК утвердил. Недоглядели академики». Довольно быстро Георгий разгадал «уникальные алгоритмы» программы и придумал к ним отмычки: «Сперва я обнаружил информацию, что систему уже пытались обмануть с помощью транслитерации — замены русских букв на аналогичные по виду английские. Разработчик исправил это. Но я подумал, что, видимо, не такой уж и крутой алгоритм у этой хваленой системы. На примере текста, который есть у них в базе, я вычислил способы, с помощью которых можно со стопроцентной вероятностью обойти систему».

Обманутые дети

Оказалось, что «Антиплагиат» сравнивает тексты по предложениям и для того, чтобы его обмануть, достаточно выбрать одно из четырех действий — добавить в предложение уникальное слово (хотя бы союз), удалить слово, разбить предложение на два или объединить два предложения в одно.

Для примера скачаем наугад любой реферат с интернет-ресурса и выберем оттуда первую попавшуюся фразу: «Солженицын заставляет каждого читателя представить себя „туземцем“ Архипелага — подозреваемым, арестованным, допрашиваемым, пытаемым. Заключенным тюрьмы и лагеря... Любой поневоле проникается противоестественной, извращенной психологией человека, изуродованного террором, даже одной нависшей над ним тенью террора, страхом; вживается в роль реального и потенциального зэка». Результат предсказуем: данный фрагмент является полностью заимствованным. Далее с помощью программы-киллера вносим ряд изменений: убираем слова «арестованным» и «извращенной», ставим двоеточие вместо тире, союз «или» вместо «и». Теперь «Антиплагиат» говорит, что текст полностью оригинальный.

На самом деле «Киллер» лишь подсказывает пользователю, к каким фразам «придерется» система. Заместив следы можно и самостоятельно. «Моя программа делает процесс обмана более простым и удобным,— поясняет Георгий.— Используя ее, вы в разы увеличите скорость написания „уникальной“ работы из оригинала. Да и „Киллер“ не даст вам пропустить ни одного неисправленного предложения». Исправить же найденные в программе дыры будет нелегко, ведь для этого придется изменить весь алгоритм проверки.

Впрочем, на этом проблемы у «Антиплагиата» не заканчиваются. Как утверждает в упомянутом запросе Вячеслав Мустакимов, в базе «Антиплагиата» ведущие коллекции рефератов проиндексированы не полностью, но при этом занесены форумы, не имеющие никакого отношения к науке, а также художественная литература и порноресурсы.

В качестве доказательства господин Мустакимов приводит следующий пример. С помощью быстрой проверки анализируем невинную на первый взгляд фразу: «Однажды утром, когда мои родители были на работе, я услышал ароматный запах готовящегося завтрака». Программа выдает стопроцентное заимствование. Идем по ссылке, которая предполагается источником цитаты, и читаем буквально следующее после «Однажды утром…» предложение: «Я лежал в постели и мастурбировал, думая о моей бабуле». Как выясняется, это рассказ «Бабушкин завтрак», проходящий по категории «инцест» на одном из порнографических ресурсов. Сколько подобных ресурсов среди заявленных 10 млн и, главное, какое отношение они имеют к науке, неизвестно. Не удалось выяснить и позицию ВАК по данному вопросу: там от комментариев отказались с формулировкой «мы уже все рассказали». «Антиплагиат» действительно получил широкую огласку и неплохой пиар. Воспользоваться им — а значит, открыть подобный рассказ про «завтрак» — могут в том числе несовершеннолетние граждане. Это, по словам господина Мустакимова, противоречит ст. 14 федерального закона РФ «Об основных гарантиях прав ребенка в Российской Федерации».

Возможно, самое неожиданное последствие «Антиплагиата» в том, что используют его не только преподаватели, но и сами студенты. Ведь программа находится в открытом доступе и не ставит перед пользователями никаких ограничений. Получается такая игра: кто кого перехитрит. «Теперь прежде, чем сдать скачанный реферат,— рассказывает студент МГУ Андрей Гаврилов,— я обязательно прогоняю его через программу». Тем не менее даже автор «Киллера» Георгий признает, что система может быть полезна. Правда, не в том виде, в котором она существует сейчас: «Нужно понять, что это ни в коем случае не панацея. Главная роль в проверке работ на самостоятельность я отвожу все-таки преподавателю».

Егор Андреев

Сетевой шпионаж

В этом году начались тотальные гонения на пользователей интернета. Депутат Госдумы Виктор Алкснис успешно судится с якобы оклеветавшим его блогером, а Дмитрий Ширинкин может угодить в тюрьму за двусмысленную запись в сетевом дневнике. Эти истории напрямую связаны с проблемой анонимности в интернете. Кто, как и зачем собирает на нас виртуальное досье, разбирался корреспондент «Ъ-Телекома» АЛЕКСЕЙ ДОЛЯ.

На работе

Интернет на рабочем месте давно стал средством отвлечься от работы на развлекательных сайтах либо каналом слива конфиденциальной информации компании. Естественно, что работодателей не устраивает такое положение вещей, поэтому системные администраторы обычно анализируют трафик сотрудников. В этой связи слежка за сотрудниками стала наиболее распространенной среди всех видов сетевого шпионажа.

Специалисты по сетевой безопасности выделяют три группы современных работодателей. Для боссов-параноиков слежка в интернете является чем-то вроде хобби. Такие работодатели постоянно напоминают сотрудникам о том, что за ними следят, и используют первую возможность для обличения виновных. Типичный пример — компания «Евросеть», вешавшая на стену фотографии провинившихся сотрудников вместе со списком посещаемых сайтов. Сотрудникам таких компаний приходится непросто, поскольку их внимание сконцентрировано не столько на работе, сколько на том, чтобы не допустить нарушений.

Компании-смотрители также следят за своими сотрудниками, но делают это осторожно. Их цель заключается не в тотальном контроле над сотрудниками, а предотвращении утечек конфиденциальных сведений. Служащие таких компаний не замечают слежки, но это не отменяет ее наличия.

Компании, которые вообще не следят за сотрудниками, как правило, небольшие. Работодатель либо не осознает необходимость контроля трафика, либо полностью доверяет своему персоналу. Если же речь идет о крупных корпорациях, то отсутствие слежки в принципе невозможно, поскольку оно тут же приведет к серьезным материальным потерям в результате утечек и нецелевому использованию рабочего времени.

Работодатели имеют широкий выбор способов слежки. Они могут просто просматривать лог-файлы, запрещать доступ к некоторым сайтам или использовать удаленные подключения к локальным компьютерам. В некоторых случаях корпоративная слежка связана не с бизнесом компании, а с капризами отдельно взятого сисадмина, который может наблюдать за пользователями под предлогом контроля их работы. Проблема здесь заключается в том, что за самими сисадминами, как правило, никто не следит.

Самые «продвинутые» компании устанавливают специальные автоматизированные системы, следящие за действиями пользователей сети, включая самих сисадминов. «Такие системы позволяют предотвратить утечку информации, причем сделать это незаметно для пользователей,— считает директор по маркетингу компании InfoWatch Денис Зенкин.— Служащим не стоит опасаться за то, что кто-то будет копаться в их грязном белье, поскольку эту функцию берет на себя машина».

Так или иначе, слежка со стороны работодателей (в том или ином виде) неизбежна, и ее следует принимать как данность, поскольку защититься от нее невозможно. Однако работодатели — это далеко не самые опасные детективы, собирающие информацию о пользователях сети.

На службе

Кроме работодателей серьезный интерес к интернет-слежке проявляют и госструктуры. Оно и понятно: на фоне всеобщей истерии по поводу терроризма интернет представлялся едва ли не самой незащищенной средой. Под этим предлогом многие страны внедрили специальные системы контроля над виртуальной жизнью.

Российский вариант подобного рода решений — «Система оперативно-розыскных мероприятий» (СОРМ) — успешно функционирует в сетях операторов связи и интернет-провайдеров уже несколько лет. Для внедрения СОРМ была выбрана типично российская схема: силовики заставили провайдеров установить соответствующее оборудование. В результате ФСБ получила доступ к трафику операторов, в частности электронной переписке пользователей. СОРМ — это не миф, она действительно работает. Тот же депутат Алкснис грозился засудить всех остальных пользователей, которые его обматерили. Таковых набралось немало, и засечь их вручную не представлялось возможным. По словам господина Алксниса, силовики определили личности интернет-пользователей именно с помощью СОРМ.

«Информация о массовом внедрении СОРМ появилась в конце прошлого века. Эта система тут же привлекла внимание правозащитников, которые говорили о ее „неконституционности“ и „нарушениях прав человека“»,— комментирует Максим Скида, руководитель направления защиты персональных данных компании Aladdin.

Кроме технических способов спецслужбы обладают неисчерпаемым административным ресурсом. Для них не составит труда ненавязчиво попросить операторов предоставить доступ к информации с целью слежки за их клиентами. Определенный оптимизм внушает лишь то обстоятельство, что госструктуры вряд ли будут дергать за рычаги влияния по пустякам.

На отдыхе

Отдельное место в иерархии интернет-детективов занимают обычные мошенники, которые следят за объектами с помощью различных технических средств. Иногда ревнивые мужья пользуются услугами хакеров для отслеживания интернет-похождений своей благоверной. Но чаще всего мотивом становятся деньги. Самый простой пример: данные о кредитных картах вводятся при оплате товаров через интернет. Перехватив их, злоумышленник может совершить несколько покупок за счет жертвы.

Как правило, за пользователем следят с помощью шпионской программы, которая попадает в компьютер из-за уязвимостей в программном обеспечении. Или же в результате откровенной глупости пользователя, который решил открыть почтовое вложение, поступившее с неизвестного адреса.

Профессиональная шпионская программа никогда не выдаст своего присутствия на компьютере, и в то же время она следит за происходящими в системе событиями. Программа может пересылать информацию о действиях жертвы своему владельцу или предоставлять ему полный доступ к системе. В обоих случаях владельца компьютера не ждет ничего хорошего — за ним будут пристально следить и воровать его приватные данные. В то же время от троянцев не сложно защититься: банальный антивирус и регулярное обновление базы избавят от большинства проблем.

«С каждым днем создатели вредоносного ПО становятся профессиональнее,— считает Илья Шабанов, ведущий стратегический аналитик „Лаборатории Касперского“.— Если раньше вирусы писались ради забавы или самореализации, то теперь их авторы хотят зарабатывать деньги».

Отдельный тип угроз связан с файлами cookies — небольшими текстовыми файлами, создающимися во время работы с интернет-ресурсом. Как правило, в cookies содержится уникальный идентификатор пользователя, который сайт считывает при повторном заходе того же самого посетителя. В результате сайт «узнает» пользователя и оптимизирует работу ресурса под его потребности. Большинство сайтов создают вполне безопасные cookies, которые не угрожают анонимности пользователей. Однако встречаются и их опасные модификации. К примеру, cookies рейтинговых систем могут отслеживать те сайты, на которых побывал человек, а кража самих cookies может привести к утечке конфиденциальной информации или доступу злоумышленников к ресурсам от имени пользователя. Для защиты от этих угроз рекомендуется удалять cookies перед завершением работы в интернете.

Кроме вирусов и cookies в арсенале злоумышленников имеются и другие средства. В частности, они могут взломать систему, используя уязвимости в системе безопасности компьютера. Чтобы избежать этого, необходимо регулярно скачивать обновления для используемого ПО.

Новая приватность

Те, кому лень самостоятельно добывать сведения о деятельности пользователя в сети, могут обратиться к провайдеру, который не имеет права распространять такие сведения. Некоторые вообще умудряются потерять базу собственных клиентов, как это произошло с хостинг-провайдером ValueHost. Кроме личной информации в базе содержались логины и пароли для доступа к сайтам. В результате произошло массовое заражение ресурсов клиентов ValueHost опасным вирусом Psyme.

Еще одна важная угроза исходит от глобальных поставщиков услуг. В сети существует масса компаний, помогающих осуществлять поиск в интернете, предоставляющих бесплатную почту, средства обмена файлами или фотографиями. Сегодня эти сервисы аккумулируют просто гигантские объемы приватных сведений граждан. Всем известная компания Google, например, постоянно фигурирует в различных скандалах, связанных с индексированием приватных данных в интернете. Но вероятность утечки сведений чрезвычайно мала.

Приватность в интернете давно потеряла свою актуальность. Сообщая все свои персональные данные электронному магазину, банку, работодателю, авиакомпании, человек рано или поздно станет жертвой утечки, а также объектом пристальной слежки со стороны сильных мира сего.

Это означает, что сегодня наступают условия «новой приватности». Ни один пользователь сети не может быть уверен в сохранности собственных приватных данных, а также в том, что за ним не следят в данный момент. И ничего поделать здесь нельзя: переход к «новой приватности» является глобальным трендом развития интернета.