Шпионские страсти

Хакерство с помощью Google

Нельзя быть уверенным на все сто, что ваша информация защищена от хакерских атак. Такому риску подвержены пароли, номера пластиковых карт и устройства, подключенные к Сети. Вы увидите, как легко можно узнать конфиденциальные сведения.

Удивительно, но один из самых опасных сайтов в Сети — это, оказывается, Google.com. Не всем известен тот факт, что Google индексирует все без исключения файлы, которые лежат в незащищенном доступе, начиная от таких незамысловатых данных как пароли и заканчивая строго секретными документами. Винить в этом нужно в первую очередь самих владельцев сайтов, которые размещают незащищенную информацию, совершенно не задумываясь о возможных негативных последствиях.

Взлом с помощью Google — это новый способ, который используют хакеры для проникновения в бережно хранимые корпоративные секреты. Им даже не нужно прибегать к использованию специальных утилит — анализаторов протоколов (password sniffers) или сканеров портов.

Мы решили выяснить, каких же результатов можно достичь, используя Google. Во время рейда по Интернету мы совершенно неожиданно наткнулись на такие данные, как секретные презентации в PowerPoint, созданные для ведущих концернов — Siemens, Sun или Enron. Достойны упоминания и резервные копии электронной почты, доступ к факсовым устройствам, отправленные письма, а также огромное количество паролей и номеров пластиковых карт. При этом нам ни разу не пришлось проходить аутентификацию для просмотра таких данных. Достаточно всего пары простых, но эффективных приемов, чтобы Google преподнес вам желаемый результат на блюдечке с голубой каемочкой.

То, что информация такого рода может быть обнаружена в результате поис- »

ка в Google, совсем не удивительно. Эта поисковая система использует много тысяч ботов, которые непрерывно и, надо заметить, на абсолютно законных основаниях бороздят просторы Интернета, просматривая всю находящуюся там информацию. Вдобавок к этому Google получает списки ссылок от своих партнеров, например Opera. Бесплатная версия браузера, окупаемая исключительно за счет баннерной рекламы, отправляет Google перечень всех сайтов, которые посещает пользователь. Поисковая система классифицирует их согласно категориям, и в итоге пользователь видит в браузере Opera специально отобранные рекламные баннеры, которые, как предполагается, отвечают его интересам.

Между тем по адресу, который пользователь набирает в строке, направляется еще один бот, чья задача заключается в том, чтобы внести эту ссылку в базу данных. Однако примеры, приведенные чуть ниже, должны убедить вас, что некоторым сайтам, которые числятся в базе данных Google, лучше было бы остаться незамеченными.

Секретные файлы компаний и частных лиц

Если правильно сформулировать запрос поиска, то Google в считанные секунды может снабдить вас всеми необходимыми файлами с конфиденциальным содержимым. Для этого вам понадобится знать только волшебное заклинание, состоящее из ключевых слов для поиска и нужного оператора.

Мы решили проверить этот метод на собственном опыте, основываясь при этом на идее, что в последнее время новые стратегические планы многих ведущих компаний преподносятся как презентации, созданные в программе PowerPoint; как известно, такие файлы имеют расширение PPT. Для того чтобы было понятно, что информация предназначается для узкого круга адресатов, каждый слайд обычно снабжается пометкой «Конфиденциально» или «Для служебного пользования». Поэтому в запрос для поиска мы включили соответствующие формулировки. Таким образом, в обычную строку поиска Google мы ввели следующий запрос:

▲ Свыше девяти тысяч ссылок ведут на документы с грифом «ДСП»

```
ext:ppt confidential «for internal use only»
```

Меньше одной секунды потребовалось Google, чтобы сформировать список из нескольких тысяч различных файлов, которые в точности соответствуют заданным критериям. Среди них мы обнаружили документы, принадлежащие таким крупнейшим компаниям как Sun, Siemens или Enron.

Пиратские MP3-файлы в каталогах архивов и резервных копий

Google позволяет найти не только отдельные документы, выложенные в Сети. Многие владельцы сайтов используют принадлежащее им веб-пространство для хранения резервных копий системы. При этом можно попасть под огонь охотников за пиратами, например Международной ассоциации звукозаписывающей отрасли (IFPI) или Альянса производителей программного обеспечения для бизнеса (BSA). В случае если на сервере обнаружат MP3-файлы или коммерческие утилиты, которые можно скачать, это могут посчитать нарушением авторских прав.

И снова мы начали думать, какое же ключевое слово укажет путь к папкам файлов, выложенных в Сети. Сначала мы выбрали тот же оператор «ext:», однако результат нас не вдохновил. Поэтому мы использовали тот факт, что каталоги начинаются со стандартного заголовка «Index of/», вслед за которым идет перечень файлов, находящихся в папке. На такой запрос Google выдал более 700 млн ответов. Поэтому интересующую область нужно определить более четко.

▲ Веб-камера, не защищенная паролем, доступна для всех

MP3-файлы мы искали с помощью следующего запроса:

```
«Index of /» +MP3
```

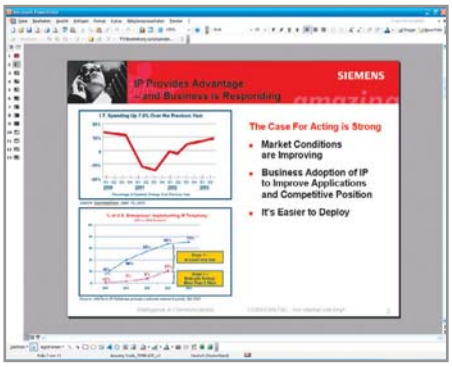
Интернет-магазины выдают тайну данных пользователя

Несмотря на то что системы аутентификации становятся все более изощренными, во многих онлайн-магазинах все еще наблюдаются огромные бреши. Клиенты при этом вполне могут остаться ни с чем, ведь хакеры с завидной легкостью добираются до, казалось бы, хорошо защищенных паролей и номеров пластиковых карт.

Мы попробовали разыскать с помощью сайта Google номера карт. Для этого сначала решено было воспользоваться оператором Numrange. Сравнив различные карты Visa, мы взяли за основу кода для Google «visa 4060000000000000... 4060999999999999». Дело в том, что все номера карт начинаются с цифр 4060, а далее любые комбинации можно охватить подбором от 0 до 9. Однако такой поиск не принес желаемого результата, так как Google, судя по всему, сознательно отфильтровывает запрос подобного рода, чтобы получить номера было не слишком просто. Но существует и другой вариант: мы начали охоту за базами данных и сайтами, где можно найти пользовательские данные, и не прогадали. С помощью безобидного кода мы искали ссылки, которые ведут к информации, необходимой для входа в профиль:

```
inurl:«login.asp»
```

▲ Добавить нового пользователя вы можете самостоятельно



▲ Закрытая презентация Siemens найдена в открытом доступе

» Таким образом было обнаружено более трех миллионов веб-сайтов — то есть каждый из них потенциально может подвергнуться атаке SQL Injection. Мы ограничили список результатов, добавив оператор «intitle:», что позволило целенаправленно искать среди магазинов, специализирующихся на продаже программного обеспечения. Результат эксперимента оказался несколько пугающим: с помощью одной вредоносной команды мы вторгнулись в первый же онлайн-магазин из нашего списка. Наряду с паролями административного доступа мы нашли и полный архив клиентских данных, содержащий перечень заказов, положенных в корзину, номера пластиковых карт, адреса доставки товаров и тому подобное.

Промышленный шпионаж через факс, веб-камеры и принтер

Огромное количество факсов, принтеров, веб-камер и прочих периферийных устройств подключены к Сети без какого-либо пароля и открыты таким образом для всех желающих. Мы решили выяснить, какие секреты хранят в себе эти устройства. Начав розыск с фразы «Network Attached Devices» (устройства, подсоединенные к Сети), мы снова воспользовались оператором «intitle:». Нашей первой попыткой стал запрос:

```
intitle: «Home» «Xerox Corporation» «Refresh Status»
```

Поисковая машина выдала список из пары десятков факсовых устройств фирмы Xerox, подключенных к Интернету. В некоторых случаях нам даже удалось просмотреть документы, с которых делали копии на этих аппаратах.

Веб-камеры также замечательно подходят в качестве средства шпионажа. Как известно, их зачастую используют для охраны офисов и прочих помещений. Мы взяли на прицел программу xpWebcam и сформулировали запрос, используя оператор «inurl:»

```
intitle:«my webcamXP server!» inurl:«:8080»
```

Итог оказался более чем тревожным: в Сети мы нашли несколько десятков веб-камер, многие из которых не были защищены паролем. Мечта вуайериста: через камеры, находящиеся в свободном доступе, можно визуально проникнуть в чужие квартиры или наблюдать за работой сотрудников различных офисов.

Доступ через eMule

Все больше пользователей работают с сервисами удаленного доступа, которыми можно управлять даже через такие клиенты peer-to-peer как eMule. Для хакеров же эти программы являются отличной лазейкой в чужие сети.

Наиболее распространенными системами удаленного управления являются eMule, VNC Desktop и Windows Remote Workplace. Для поиска соответствующих данных хакеры используют в основном операторы «intitle:» или «allintitle:». Мы нашли более тысячи страниц, содержащих информацию про Outlook Web Access, отправив запрос:

```
allintitle:microsoft outlook web access — logon
```

Несколько десятков логинов VNC мы разыскали с помощью строки: »

Важнейшие команды Google

Как с помощью операторов найти все, что нужно

allintitle: Ограничивает результаты поиска только теми страницами, в строке заголовка которых встречаются все параметры поискового запроса.

intitle: В отличие от предыдущего оператора в строке заголовка должно быть найдено только первое слово, указанное в запросе. Остальные слова поиска ищутся в тексте страницы.

allinurl: Используйте этот оператор, если все ключевые слова поиска должны встретиться в адресе.

inurl: Аналог оператора «intitle:» в строке адреса ищет только первое слово запроса.

.. (numrange) При поиске чисел вы можете таким образом сформулировать область значений. К примеру, определив запрос как «100..150», вы найдете все страницы, содержащие числа от 100 до 150.

daterange: С помощью этого оператора вы можете ограничить количество результатов определенным периодом времени. Имейте в виду, что параметры нужно задавать согласно юлианскому календарю.

ext: Так вы можете целенаправленно искать ссылки на какой-либо файловый формат. В качестве альтернативы можно попробовать и «filetype:».

cache: Отдав такую команду, вы загружаете найденный веб-сайт из кеша Google. Это удобно в том случае, если нужный вам сервер больше не существует.

site: Эта команда запускает поиск на каком-либо определенном веб-сайте.

related: При использовании этого оператора Google покажет в результатах поиска похожие сайты.

info: Отправив такой запрос, вы получите краткое описание сайта.

link: Набрав перед запросом этот оператор, вы найдете все сайты, ссылающиеся на указанную страницу.

» intitle:vnc.desktop inurl:5800

Во многих программах не ограничено количество попыток ввода, и хакеры не упускают такой счастливый случай: применяя утилиты, которые перебирают все возможные цепочки знаков, можно без проблем подобрать пароль.

Профили электронной почты для спамеров и веб-мошенников

Для многих администраторов удаленное управление — прекрасный инструмент, позволяющий отдохнуть день-другой и позаниматься своими делами без отрыва от производства. Неважно, идет ли речь о почтовом сервере или маршрутизаторе, сегодня все сервисы можно настроить через Интернет.

Мы задались целью найти почтовый сервер компании Agrosoft. Дело в том, что достаточно всего-навсего одной ошибки в программном обеспечении почтового сервера, чтобы можно было воспользоваться веб-интерфейсом и незаметно создать новые профили без какой-либо аутентификации. С помощью следующего простого взламывающего кода:

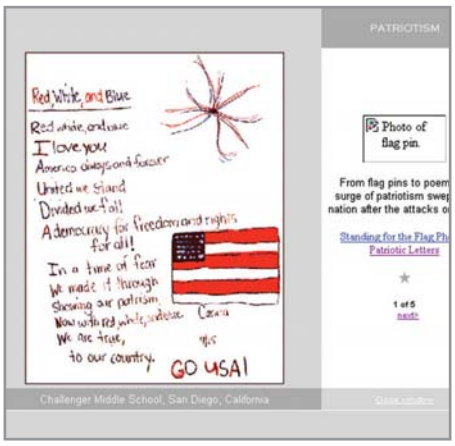
«adding new user» inurl:addnewuser — «there are no domains»

мы обнаружили несколько десятков доменов, где можно создать почтовый ящик. Это не пустяк, если учесть, что адреса можно использовать не просто в обманных целях, но и для рассылки спама.

Какую информацию Google не раскрывает, но все же обозначает

Если веб-мастер, например, хочет оградить от посягательств поисковых машин некоторые области сайта, он может создать соответствующий перечень директорий, запрещенных к индексации, в файле robots.txt.

Файл robots.txt представляет собой текстовый файл, а в каждой строке, начинающейся со слова «Disallow:», значится имя подкаталога, который поисковые роботы должны игнорировать при индексации страниц. Это те каталоги, которые находятся в открытом доступе, но никогда не попадут в базу данных поисковых систем. Чтобы все-таки разузнать, какие данные скрыты в подобных перечнях, мы набрали в стро-



▲ Письма детей в Белый дом закрыты для поисковых систем

ке браузера адрес «www.whitehouse.gov/robots.txt». Взламывающий код для сайта Google в общем случае выглядит следующим образом:

ext:txt robots

В результате, например, мы увидели скрытый каталог «/911/patriotism/text/». Почему администраторам сайта Белого дома США было приказано закрыть каталог, который содержал патриотические письма детей президенту, так и осталось для нас секретом. CHIP

Мастер-класс

Как обнаружить бреши в Google и защитить свой сервер

Если вы не желаете становиться жертвой взлома через Google, попробуйте использовать бесплатную утилиту Wikto компании Sensepost. В основе этой программы лежит Google Hacking Database, разработанная Джонни Лонгом, которая позволяет распознать все известные хакерские атаки через Google. Эту программу, а также Google Hacking Database, можно скачать с сайта www.sensepost.com/research/wikto. Следующие действия помогут вам залатать бреши в системе безопасности.

▸ Для установки программы вам понадобится .NET-Framework, а также действующий ключ API от Google. Разработку .NET-Framework вы можете найти по адресу www.microsoft.com/downloads или на диске с пакетом обновлений и исправлений Service Pack 2 в каталоге dotnetfx.

▸ Ключ API понадобится для того, чтобы автоматически пользоваться поисковой службой. Такие ключи абсолютно бесплатны, однако вам придется зарегистрироваться на странице www.google.com/apis. Там вы получите в свое распоряжение шифр, который нужно будет указать в меню «SystemConfig → Google Key» программы Wikto. Далее вызовите пункт меню «Google Hacks» и загрузите, щелкнув «Load GHDB», файл формата XML с Google Hacking Database.

▸ На этом подготовительная стадия завершена. Введите имя своего домена в поле «Target» и запустите поиск нажатием «Start GH». В течение пяти минут утилита автоматически будет пролистывать все ключевые слова поиска, после чего представит на ваш суд список всех найденных ссылок, которые могут служить и лазейками для хакеров.

▸ Чтобы предотвратить взлом, в любом случае стоит удалить все потенциально опасные файлы с сервера — конечно, если это представляется возможным.

▸ Но те каталоги и файлы, которые вы вынуждены выкладывать в Сеть, вполне могут остаться и не засвеченными для Google. Одно из давно сформулированных правил сетевого этикета гласит, что каждый поисковый робот сначала обращается к файлу robots.txt, который лежит в корневом каталоге веб-сервера, и принимает к сведению его содержимое. В этом файле можно определить, каким каталогам не избежать индексации. Точный синтаксис написания такого файла вы найдете на сайте www.robotstxt.org.

▸ Если же ваш сайт уже попал в поле зрения Google, можно попытаться удалить страницы из кеша поисковой машины. Для этого администратор домена должен предпринять несколько шагов, которые подробно описаны на google.com/remove.html. Самый важный пункт этого руководства, на наш взгляд, заключается в том, что файл больше не должен находиться на сервере.