KRZYSZTOF MARZEC

Google Hacking

Stopień trudności

Jeszcze parę lat temu łatwo było znaleźć wielu zaciekłych przeciwników tej wyszukiwarki, chroniących się za proxy i kasujących codziennie cookies, aby uchronić resztki prywatności. Dziś mało kto już oburza się na fakt, że jedna konkretna firma ma dostęp do tak wielkiej ilości informacji, a zapytania w Google wpisuje praktycznie każdy użytkownik Sieci.

Prawie bez echa przeszła informacja, że praktycznie ostatnia istniejąca konkurencja Google, wyszukiwarka Onetu, zaczyna używać ich silnika. Obecnie 97% wszystkich zapytań trafia do Google, a największa konkurencja na silniku MSN posiada 1,3% całości ruchu, który zawdzięcza pewnie bardzo nieświadomym użytkownikom komputerów, z jedynym słusznym systemem i jedyną słuszną przeglądarką. Jednak mało kto wie, że w bazie Google, oprócz danych publicznych, znajdują się również dane poufne: hasła, kopie zapasowe stron czy prywatne zdjęcia. Dostały się tam głównie przez zaniedbanie i postaram się pokazać, jak łatwo je wyszukać.

Opiszę jak dostać się do tych danych, skąd się biorą i jak powinny być odpowiednio zabezpieczone. Nie będzie to artykuł techniczny ani instrukcja do tego jak wykradać dane, choć z konieczności pojawią się takie przykłady. Chcę nakreślić potencjalnemu czytelnikowi obraz i skalę zjawiska oraz uświadomić go o zagrożeniach oraz potencjalnych możliwościach, jakie daje nam Google. Postaram się przedstawić kilka różnych typów danych, do jakich możemy się dostać, przeglądając bazy Google. Pokażę jak osoba o średnim poziomie pomysłowości może dostać się do danych poufnych oraz fakt, że wyszukiwarka to także ciekawe źródło danych statystycznych, marketingowych i demograficznych. Postaram się też nakreślić obraz indeksu Google jako wyników pełnych danych, nie do końca publicznych, i ciekawostek. Na koniec wskaże techniki zabezpieczania się przed wyciekiem danych do indeksu Google, a także pułapki z nimi związane.

Zanim zaczniemy

Zdobywanie haseł i danych za pomocą Google może wydawać się ciekawe i kuszące, ale używanie ich to już zupełnie inna sprawa. Poza kwestią moralną i prawną zwracam uwagę na fakt, że opisywane techniki są powszechnie znane, stąd łatwo trafić na pułapki – sieciową wersje Honey Pot. To specjalnie przygotowane strony, na których widnieją hasła, ale ich użycie spowoduje jedynie zapis naszej aktywności na komputerze osoby zbierającej nasze dane. Dodatkowo Google wdrożyło pewne zabezpieczenia i nawet podczas pisania tego artykułu, przy niektórych zapytaniach pojawiał się komunikat, że mój komputer zadaje automatyczne zapytania.

Kolejną kwestią są strony, które wykorzystują zapał początkujących adeptów Google i są umieszczone wysoko, odpowiadając na niektóre bardzo popularne zapytania wspominane w artykule. Udając wygląd indeksu plików Apache serwują nam reklamy lub przekierowują na strony, które niekoniecznie chcielibyśmy oglądać. Należy

Z ARTYKUŁU DOWIESZ SIĘ

jak wyszukiwać informacje nie przeznaczone do wyszukiwania,

jak zabezpieczyć się przed wyciekiem informacji w Google,

jak budować nowe zapytania, poszukując specyficznych danych.

CO POWINIENEŚ WIEDZIEĆ

jak używać operatorów zapytań Google,

podstawowa obsługa serwera www.

pamiętać, że ta dziedzina miała swój najlepszy czas w latach 2004 – 2006 i powstały nawet aplikacje umożliwiające tworzenie zapytań bez znajomości składni (zobacz: aplikacja Google Hacks *http://code.google.com/p/googlehacks/downloads/list*). Najwięcej stron, które udają pożądane wyniki, znajdziemy przy najpopularniejszych zapytaniach, warto je więc filtrować frazami negatywnymi lub kontynuować poszukiwania na dalszych podstronach wyników wyszukiwania.

Szukamy: hasła

Indeks Google dla potencjalnego szperacza to bardzo łakomy kąsek. Całą sztukę wyszukiwania poufnych informacji i haseł można opisać w jednym słowie: *zapytanie*. (W dalszej części tekstu zapytania będą wyróżnione kursywą.) Jedyne co musimy zrobić to wymyślić ciekawe zapytanie, które poda nam jak na tacy to, czego szukamy. Dla przykładu Total Commander jest jednym z popularnych klientów FTP dla Windows. Jego główną wadą jest fakt przechowywania haseł w pliku, łatwym do namierzenia i złamania. Tworzymy zatem zapytanie: *„inurl: wcx_ftp" filetype:ini*, szukające plików o nazwie *wcx_ftp.ini*. Wyniki trochę nas załamią, bo bardzo niedobrze świadczą o właścicielach plików na jakie trafimy. Tym prostym zapytaniem mogłem dostać się momentalnie na kilkanaście serwerów FTP już z pierwszego pliku jaki wyszukałem. Tu od razu uwaga – sporo danych, na które można tak trafić będzie przeterminowanych, a hasła zmienione. Wynika to z prostego faktu, że osób wyszukujących takie pliki jest mnóstwo. Napisanie automatu, który informuje na bieżąco o nowych plikach, które trafiły do indeksu jest proste, a Google udostępnia narzędzie – Google Alerts (*http://www.google.com/alerts*), które samo poinformuje nas o takim zdarzeniu. Dobrze, ale bądźmy bardziej bezczelni: *„inurl:hasla" filetype:txt. W* pierwszej dziesiątce wyniki zaśmiecone, ale w drugiej mam już hasło do czyjegoś routera, konta hostingowego, bazy danych i kilkunastu serwerów FTP. Inny adres już nieaktualny, więc klikam link do kopii w Google i trafiam na kolejne hasła. Czy idea tworzenia zapytań jest już jasna?

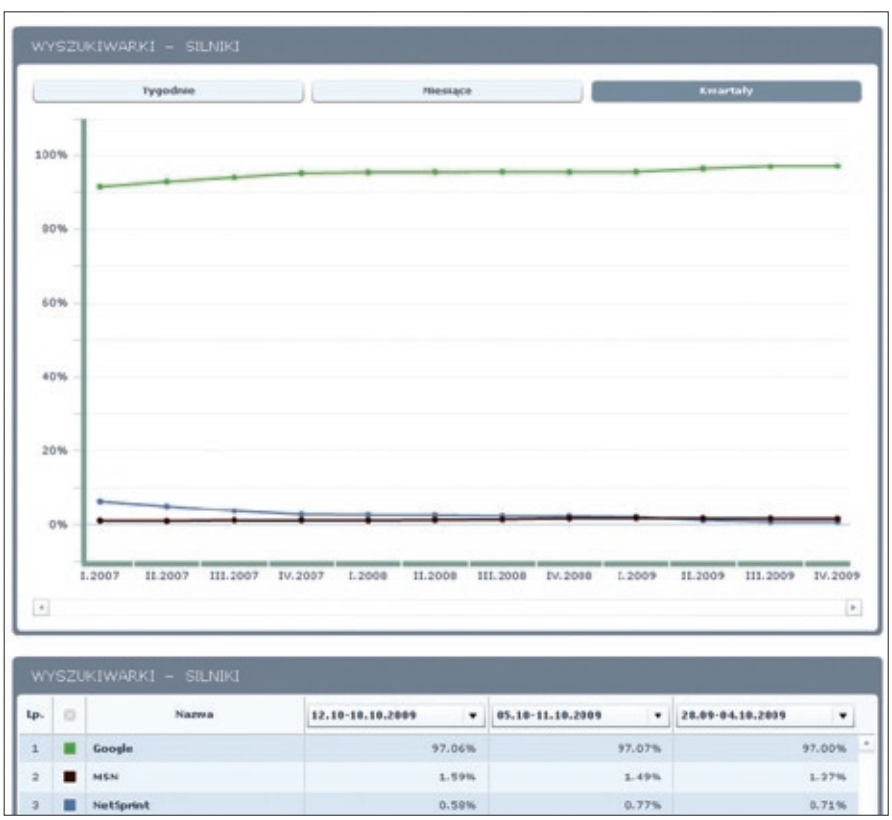
Wspomniane zapytania to bardzo proste przykłady, ale wystarczy zastanowić się jak jest przechowywane dane hasło, aby do niego dotrzeć. Zapytanie *ext:pwd inurl:(service | authors | administrators | users) "# -FrontPage-"* wyszukuje około setki wyników, które w połączeniu z jakimkolwiek programem do ripowania haseł mogą umożliwić nieuprawniony dostęp.

Szukamy listy plików

Niezabezpieczony serwer, pokazujący wszystkie pliki użytkowników z poziomu przeglądarki, to poważna wpadka administratora. Jak je wyszukać? Trzeba znać wygląd konkretnych stron najpopularniejszych serwerów. Potem szukamy wspólnego mianownika – np.: frazy *index.of* w adresie i występujących na niej słów: *parent directory* lub *name, size*. Przykłady *intitle:index.of name size* lub *intitle:index.of "parent directory"* pozwolą odnaleźć setki list plików publicznych, ale też wiele zwyczajnie niezabezpieczonych. Poszukiwania są wyjątkowo skuteczne, jeśli dodamy na końcu komendę *site:* z adresem dużej uczelni. Takich zapytań możemy tworzyć tyle, ile znamy typów serwerów. Oglądamy stronę wynikową – np.: apache i wiemy, że wszystkie inne wyszukamy zapytaniem *intext:"Apache Server at * Port"* lub analizujemy serwer Tomcat i wiemy, że zapytanie powinno wyglądać następująco: *intitle:"Directory Listing For" intext:Tomcat -intitle:Tomcat.*

Takie zapytania dają dostęp do prywatnych zdjęć, dokumentów i innych plików. Łatwo wyszukać w ten sposób filmy: *" "parent directory " DVDRip -xxx -html -htm -php -shtml -opendivx -md5 -md5sums*, czy inne pliki, na przykład czyjeś CV : *"parent directory " cv.pdf site:.pl.*

Systemami bardzo podatnymi na takie wyszukiwanie są duże hostingi, gdzie użytkownik dostaje własną subdomenę w domenie hostingu. Zapytanie *"intitle:index of" site:nazwa-hostingu.pl* daje przeważnie dostęp do plików, które nigdy nie miały być publiczne lub list katalogów, pozwalających bardzo łatwo sprawdzić ile i jakie domeny są podłączone do tego samego konta hostingowego.



Rysunek 1. *Statystyki z Ranking.pl pokazują ogromną dominację silnika Google*

Szukamy systemów podatnych na włamania

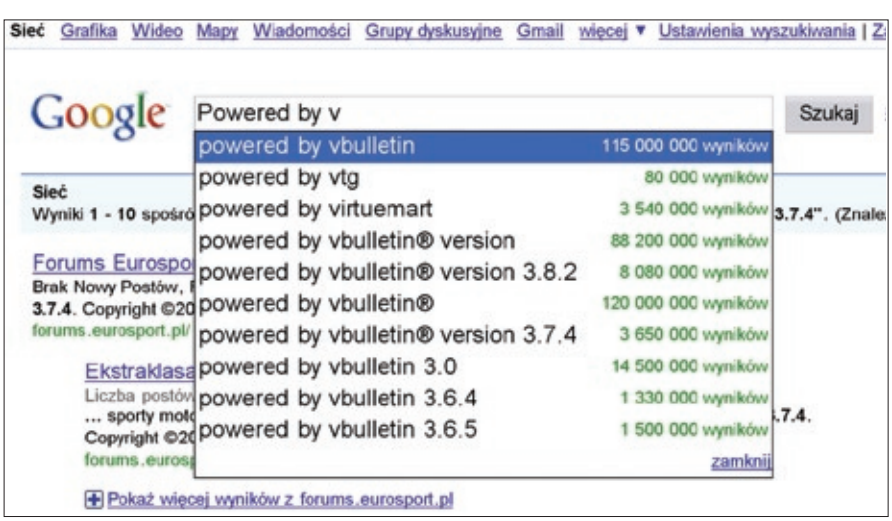
Każdy ogólnodostępny i popularny system forum, sklepu internetowego czy blogowy wymaga stałych aktualizacji bezpieczeństwa. Nie wszyscy jednak to robią, nie zdając sobie sprawy, że właśnie na to czeka mnóstwo scriptkiddies. Gdy w Sieci ukazuje się nowy exploit, potencjalny atakujący może momentalnie wyszukać w Google wszystkie stare wersje danego skryptu i łatwo je uszkodzić. Tak wyglądał między innymi zeszłoroczny atak tureckich pseudohackerów na polskie strony. Atakujący wyszukali w Google niezaktualizowane skrypty Joomla i użyli gotowych rozwiązań na włamanie. Skalę problemu może obrazować fakt, że zaraz po atakach Google pozwalało wyszukać ponad 400 uszkodzonych skryptów Joomla. Wyszukiwania takie są niezwykle proste: *intext:Powered by: vBulletin Version 3.7.4*. Dają nam listę adresów z zainstalowaną starą, mało bezpieczną wersją skryptu forum. Sporo osób o tym wie i aktywnie to wykorzystuje, o czym świadczą sugestie samego Google, oparte na historii zapytań (Rysunek 2).

Narzędzia

Wystarczy nam interface Google, a najlepiej wyszukiwanie zaawansowane (*http://www.google.pl/advanced_search?hl=pl*) oraz kilka podstawowych komend. Pisząc zapytanie do Google trzeba pamiętać, że wyszukiwarka pomija niektóre słowa, np.: a, an, i, or, the. Nie zadziałają też za długie zapytania i te niedokładne. Możemy używać operatorów:

OR – jako alternatywa,
„+" – jako zaznaczenie elementu, który musi wystąpić,
„-" – jako wykluczenie elementu,
„" – cudzysłów, aby wyszukać dokładnie taką frazę,
* – gwiazdka nie działa jako uzupełnianie wyrazów (Krak*w), ale zadziała jako *wildcard*: „tanie * w Krakowie".
cache: – zwraca kopię lokalną strony,
intext: – wyszukiwane słowa mają znajdywać się w treści strony,
inurl: – wyszukiwane słowa mają znajdywać się w adresie strony,
intitle: – wyszukiwane słowa mają znajdywać się w tytule strony,
filetype:, ext: – wyszukiwanie określonych typów plików,
site: – przeszukuje tylko podstrony w danej domenie, adresie.

Pełna lista typów znajduję się m. in. na stronie:
http://www.googleguide.com/advanced_operators_reference.html



Rysunek 2. *Podpowiedzi Google – jak widać wiele osób przed nami próbowało wyszukać podatne na ataki wersje tego forum*

Szukamy kart kredytowych, numerów seryjnych, baz danych

Niegdyś bardzo niebezpieczny trick z zapytaniem o numery kart kredytowych jest już dziś bezużyteczny. Opisało go tak wiele stron, że zapytanie *visa+4 356000000000000..43569999999 99999* przestało być użyteczne. Nie zapominajmy jednak, że pewne dane można wyłowić z Google znając pewien wzorzec. Jeśli np.: osoba próbująca złamać zabezpieczania programu poszukuje numeru seryjnego wystarczy, żeby znalazła dwa, a kolejne odnajdzie już bez żadnego problemu. Wpisuje wtedy oba w Google, wyszukując kolejne listy numerów seryjnych publikowanych na stronach czy forach. Analogiczna zasada działa z bazami danych, bazami adresowymi czy listami serwerów FTP. Powstrzymam się od podawania przykładów, ale parę godzin z tym zagadnieniem daje dostęp do bardzo ciekawych danych, a nawet całych baz i plików z danymi.

Innym sposobem wyszukiwania baz danych są zapytania o pliki baz: *.mdb, *.sql czy arkuszy: *.xls. Wystarczy skojarzyć odpowiednie zapytanie, frazy występujące w pliku i typ pliku, aby wyszukać bazy pełne danych.

Szukamy ciekawostek

Wiele razy podczas szybkiej aktualizacji strony zdarzało mi się wysłać na serwer skrypt do zarządzania bazą danych – PhpMyAdmin, ręcznie skonfigurowany do połączenia z bazą. Bardzo sprytnie zmieniałem nazwę katalogu, w którym go instalowałem, tak aby nikt nie na niego nie trafił. Oczywiście popełniałem duży błąd, bo wyszukanie takich danych jest dziecinnie proste: *intitle: phpMyAdmin "Welcome to phpMyAdmin ***" "running on * as root@*" /*. Z dostępem do takiego folderu możliwość edycji treści strony czy wykradnięcie haseł użytkowników to kwestia kilku chwil. Podobnie jest ze skryptem PHP Photo Album, który wyszukany zapytaniem: *inurl:"phphotoalbum/upload"* daje dostęp do wysyłania plików graficznych do cudzych albumów.

Inną ciekawostką jest formułka, pozwalająca wyszukiwać kamery monitoringu na podstawie ścieżki typowej dla danej aplikacji:

inurl:"viewerframe?mode=motion"
– requires
intitle:"snc-rz30 home"
intitle:"WJ-NT104 Main"
inurl:LvAppl intitle:liveapplet
intitle:"Live View / - AXIS"
inurl:indexFrame.shtml "Axis Video Server"
inurl:"viewerframe?mode=refresh"

Zapytania dają niesamowite efekty. Możemy oglądać wnętrza biur, obrazy rejestrowane na żywo z kamer ulicznych i prywatnych.

Kolejne ciekawe zapytanie pozwoli nam wyszukać pulpity, udostępniane do zdalnego dostępu przez aplikację typu VNC: *"vnc desktop" inurl:5800*. Pozostaje jedynie złamać hasło, a dostęp do danych stoi otworem. Ale nie musimy wcale włamać się do czyjegoś komputera, aby oglądać jego prywatne zdjęcia. Jak to zrobić? Nic prostszego – sporo aparatów domyślnie przechowuje zdjęcia w folderze DCIM (od *Digital Camera Images*) i przerzucone bezpośrednio na serwer pojawią się dla nas po wpisaniu w Google zapytania *intitle:DCIM index.of*. Jeśli aparat to np. Nikon D80 to folder będzie nazywał się inaczej i potrzebne nam będzie zapytanie *intitle:100NCD80 index.of*. Możemy też użyć wyszukiwarki grafiki, aby przeglądać konkretne zdjęcia, nazywane domyślnie *„DSC_0001.jpg"* i kolejnymi numerami.

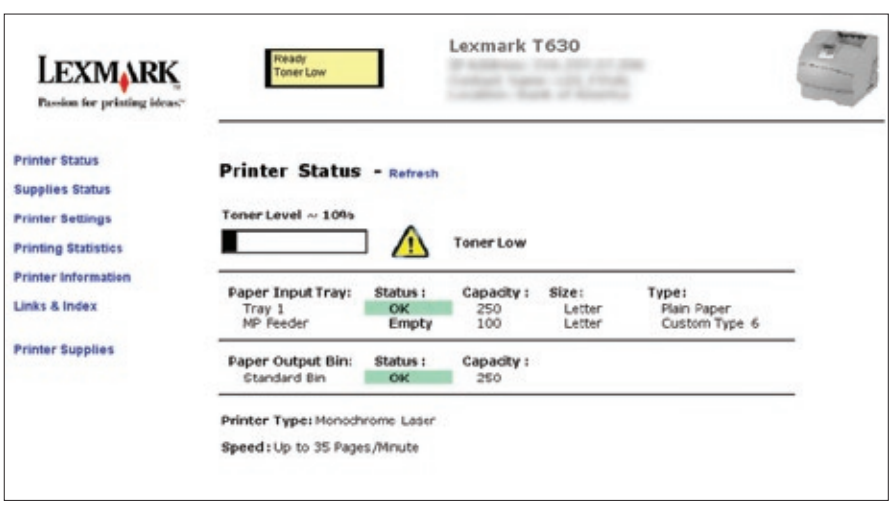
Jeśli chcemy pobawić się ustawieniami czyjejś drukarki sieciowej musimy wiedzieć jakich fraz szukać w konkretnym interfejsie panelu konfiguracyjnego. Dla przykładu panel drukarek Lexmark: intext:"UAA(MSB)" Lexmark -ext:pdf intitle:lexmark zaprasza nas do zmiany ustawień kolorów i podglądania statystyk. Gdybym tylko chciał to w jednym z banków w USA drukarka drukowałaby tylko monochromatycznie. Jednak jestem w miarę miły, dlatego za pomocą tego panelu wydrukowałem kartkę z napisem, że wkrótce skończy się toner. Czy na pewno się wydrukowało? Tak, sprawdziłem to na liczniku stron, do którego też był dostęp. Jak wspomniałem – możliwości są zadziwiające.

Skąd takie dane biorą się w indeksie?

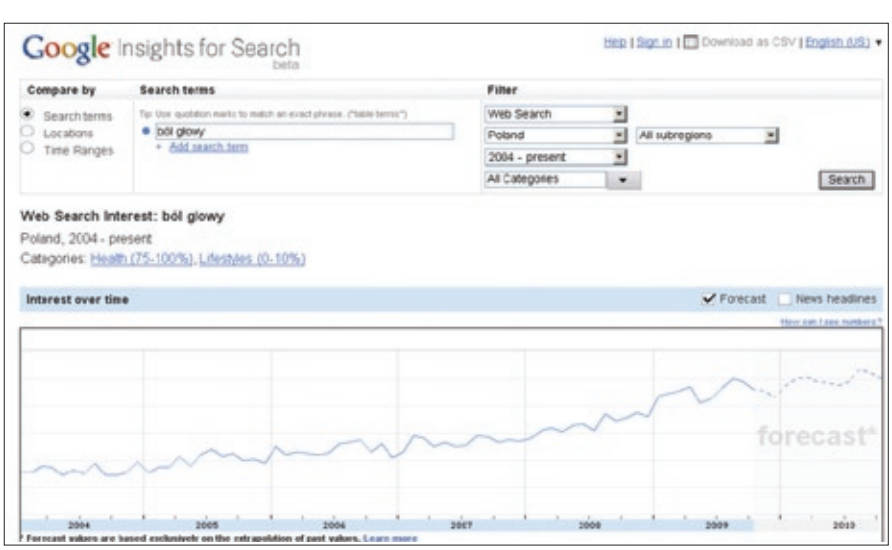
Jeśli myślicie, że jedynym sposobem na indeksacje treści przez Google są linki prowadzące roboty na daną stronę, to jesteście w dużym błędzie. Sam zauważyłem, że strony, których nigdy nigdzie nie linkowałem pojawiały się w indeksie. Skąd zatem te dane? Teorii jest wiele, jednak sporo osób jest zgodnych, że przeglądanie stron niektórymi przeglądarkami lub z zainstalowanym programem Google Desktop powoduje zgłaszanie tych stron do indeksacji. Są to spekulacje, zaś przetestowanie ich pozostawiam czytelnikom. Wspomnę jeszcze tylko o tym, że już parę lat temu wśród wypowiedzi inżynierów wyszukiwarek pojawiały się informacje o innowacyjnych sposobach na indeksację Deep Webu, czyli stron i baz danych, które do tej pory nie były nigdy indeksowane przez żadne wyszukiwarki.

Wszystkie pozostałe dane to zwyczajne zaniedbania administratorów lub niewiedza użytkowników systemów. Sam korzystałem z jednego z serwerów uczelnianych, gdzie jedynym miejscem na przechowywanie plików był *public_html*, ogólnie dostępny z poziomu wyszukiwarki. Bez zabezpieczenia folderu dane były publicznie dostępne, jednak mało który student o tym wiedział.

Aby lepiej zobrazować jak duży problem może stanowić takie chwilowe zapytanie, opiszę prawdopodobną



Rysunek 3. *Panelu drukarki Lexmark w jednym z banków w USA wyszukany za pomocą Google.*



Rysunek 4. *Google już wie, że coraz więcej polaków boli głowa*

wpadkę Google z usługą Voice. W październiku w serwisie YouTube pojawiły się filmy opisujące Google Hack, który przy użyciu zapytania *site: https://www.google.com/voice/fm/**; rzekomo dawał dostęp do zapisów rozmów telefonicznych użytkowników usługi Google Voice. Nie udało mi się potwierdzić tej informacji, więc użyłem wyszukiwarki Bing. Efekt – informacja się potwierdziła, uzyskałem dostęp do zarejestrowanych wiadomości z usługi Google Voice, co do których nie jestem pewien czy rzeczywiście miały być upublicznione. Pozostaje pytanie, czy to wyciek danych czy raczej element kampanii reklamowej nowej usługi?

Jak się zabezpieczać?

Przede wszystkim pomyśleć o tym, czy takich danych przypadkiem nie udostępniamy. Drugim etapem jest skonfigurowanie serwera tak, aby nie pokazywał list plików, jeśli ktoś wywoła katalog. Dla osób chcących mieć większą pewność polecam zapytanie *site:* na własnej domenie lub własnym IP. Bardziej dokładnym sposobem jest ściągnięcie całej swojej strony za pomocą programu typu *HTTrack*. Polecam również program *Gooscan*, który sprawdza dany system za pomocą wielu zapytań podobnych do tych, które opisuje. Ilość różnych zapytań w tym programie jest na tyle imponująca, że może być to doskonałe narzędzie do wyszukiwania prostych luk w zabezpieczeniach serwera.

Oczywiście możemy również zablokować dostęp do domeny dla robotów Google. W tym celu należy założyć konto oraz zweryfikować własność domeny w *Google Webmaster Tools* (*www.google.com/webmasters/tools*). Poprzez umieszczenie na serwerze specjalnego pliku lub meta tagu unikatowego dla naszego konta, informujemy Google o tym, że jesteśmy właścicielem danej strony. Konto w *Google Webmaster Tools* daje nam dostęp do szeregu ciekawych opcji, w tym blokowania całości lub części zasobów przed indeksacją.

Kolejną opcją jest plik *robots.txt*. W pliku tym możemy grzecznie poinformować wyszukiwarki, aby nie szperały po naszych danych. Oczywiście nie wszystkie będą słuchać. Możemy też wpaść w ciekawą pułapkę. Ponieważ plik *robots.txt* jest publiczny, każdy może sprawdzić, co tak skutecznie chcemy ukryć. Może skończyć się na domysłach dlaczego dany portal ukrywa przed Google niektóre artykuły: *http://www.gazeta.pl/robots.txt* lub dlaczego do niedawna oficjalna strona Białego Domu w USA blokowała dostęp wyszukiwarek do kilkudziesięciu plików tekstowych dotyczących m.in. 11 września 2001. Oczywiście nasza wiedza nie poszła w las, więc zaraz możemy stworzyć odpowiednie zapytanie, którym wyszukamy wszystkie takie strony:*"robots.txt" "disallow:" filetype: txt* i dowiemy się kto i co chce przed nami ukryć.

Ostatnią opcją jest prewencja – nie umieszczanie ważnych danych w ogólnie dostępnych folderach. Polecam zabezpieczenie ich za pomocą plików *.htaccess/.htpasswd* hasłem lub skonfigurowanie tak, aby dopuszczały połączenia tylko z konkretnych IP.

Ciekawe dane prosto od Google

Zanim skończę, chciałbym jeszcze pokazać, jak w pełni legalny i darmowy sposób uzyskać dane, o których jeszcze tak niedawno firmy marketingowe mogły pomarzyć. Zawsze ciekawiło mnie co ludzie wpisują w Google, jak często, kiedy zaczynają szukać w Sieci informacji o danym wydarzeniu i tym podobne. Teraz można to bardzo łatwo sprawdzić. Google udostępnia serie narzędzi: *Google Trends* (*http://www.google.com/trends*), *Google Insights For Search* (*http://www.google.com/insights/search/*) oraz *KeyWord Tool External* (*https://adwords.google.pl/select/KeywordToolExternal*). Dwa pierwsze narzędzia potrafią obrazować trendy ilości zapytań na konkretne frazy, przy czym *Google Insight for Search* jest narzędziem dużo bardziej zaawansowanym. *KeyWord Tool External* potrafi wskazać przybliżoną liczbę zapytań, jakie każda z fraz generuje miesięcznie oraz podpowiedzieć frazy zbliżone tematycznie.

Z analizy wykresów wynika wiele ciekawych wniosków – już po chwili dowiemy się, że prawdopodobnie z roku na rok przybywa w Polsce osób cierpiących na ból głowy. Widzimy też, że szał szukania sylwestrowych ofert imprez zaczyna się już w październiku, największe zakupy biżuterii przypadają na grudzień i wtedy też najwięcej osób szuka informacji na temat ciąży. Możemy też zaobserwować smutny spadek ilości zapytań o frazy Debian czy Linux.

Rysunek 5. *Widok z przykładowej kamery wyszukanej za pomocą Google*

Oczywiście tak jak samym indeksem Google, tak i tymi danymi można manipulować – świadczy o tym np. wygląd wykresu na słowo *pozycjonowanie*, które zostało zaburzone przez proste osadzenie wyszukiwarki Google, z adresem zadającym właśnie takie zapytanie, w niewidzialnej dla użytkownika ramce (iframe) na dosyć popularnych stronach. Tak wygenerowany ruch spowodował zaburzenie danych statystycznych, co na przykład daje świetny sposób na pokazanie szefowi wzrostu zainteresowania daną marką w Google.

Ciekawostką mogą być też podpowiedzi, jakie Google pokazuje w oknie wyszukiwania pod wpisywanym tekstem. Poza wieloma ciekawymi wnioskami mój ulubiony: należy wpisać w wyszukiwarkę *czy jestem*, a Google bardzo zaskakująco dokończy za nas nasze pytanie.

Przy wyszukiwaniu takich danych nie możemy też zapomnieć o głównej technice opisywanej w artykule, czyli specyficznych zapytaniach. Jeśli jesteśmy ciekawi statystyk odwiedzin innych stron, polecam zapytanie intitle:"usage statistics for" "generated by webalizer", dzięki której dostaniemy się do setek niezabezpieczonych raportów popularnej aplikacji Webalizer. Aplikacja ta służy do generowania raportów odwiedzin strony na podstawie analizy logów serwera i w tym przypadku jest źródłem ciekawych danych nie tylko dla właściciela witryny, ale również dla konkurencji.

Podsumowanie

Mam nadzieje, że udało mi się pokazać, że Google jest pełne bardzo ciekawych danych, źle zamaskowanych przed wprawnym okiem szperaczy. Czy to w wyniku zaniedbania czy błędu udostępniamy mnóstwo danych bez zastanawiania się nad konsekwencjami. Ponieważ problem nie dotyczy tylko jednej wyszukiwarki, opisane tu zjawiska można przełożyć na inne systemy. W zależności od silnika i poziomu skomplikowania składni języka zapytań, osiągniemy różne efekty, lecz wyszukiwarkami skazanymi na sukces w zdobywaniu danych są na pewno te zaimplementowane w klientach plików p2p. Prostą wyszukiwarką eMule można zdobyć dostęp do plików z hasłami przypadkowo udostępnionymi razem z całym dyskiem. Zamiast zapytać wyszukiwarkę o legalne pliki pobierane na co dzień, wpiszmy tam frazy typu: *hasla.txt, wcx_ftp.ini itp*. Udało mi się w ten sposób namierzyć pliki ze zbiorami haseł, wypełnione umowy, prace magisterskie, całe pliki z hasłami TotalCommandera, inne prywatne dokumenty, a nawet całe foldery prywatnych zdjęć. Pokazuje to, jak bardzo lekkomyślni są użytkownicy Sieci, niezdający sobie sprawy z możliwości utraty danych. Na kilkanaście prób kontaktów z osobami, które wśród listy plików miały udostępnione pliki z hasłami tylko kilka odpisało, zaś tylko jedna od razu zrozumiała przed czym ją ostrzegam.

Podsumowując – świadomość potencjalnych zagrożeń jest mała, a amatorów tego typu rozrywki w Google setki. Dlatego w budowaniu zawartości naszych serwerów, zawsze kierujmy się zdrowym rozsądkiem, a odszukując opisane w tym artykule dziury starajmy się pokazać je właścicielom serwera, zamiast wykorzystywać dla chwilowej rozrywki. Kto wie, może kiedyś ktoś będzie na tyle uprzejmy, aby ostrzec nas przed potencjalną luką w zabezpieczeniach, zanim ujawni ją całemu światu?

Krzysztof Marzec
Autor zawodowo zajmuje się tematyką wyszukiwarek internetowych i jest specjalistą ds. optymalizacji i pozycjonowania. Od trzech lat jest głównym konsultantem portalu *Interia.pl* ds. pozycjonowania. Współprowadzi agencję Deva Group *www.devagroup.pl*.
Kontakt z autorem: *krzysztof.marzec@devagroup.pl*.

W Sieci

Zainteresował Cię temat? Polecam największą kopalnię wiedzy na temat Google Hacking. Pod adresem *http://johnny.ihackstuff.com/ghdb/* znajdziesz kilkaset tematycznie posortowanych zapytań i mnóstwo inspiracji do kolejnych.