Ataki typu referer spoofing

Paweł Szcześniak

Współczesny Internet niesie za sobą możliwość skutecznej reklamy. Główną siłą napędową reklamy w Internecie jest bez wątpienia protokół HTTP – który tworzy powszechnie dziś znana technologia WWW.

linux@software.com.pl

Reklama w Internecie to nie zawsze działalność prowadzona zgodnie z etyką czy nawet z obowiązującym prawem. W niniejszym artykule chciałbym przedstawić ataki typu *referer spoofing* i ich zastosowanie w nieetycznym pozycjonowaniu stron internetowych.

Protokół HTTP

By przedstawić czym jest *referer spoofing*, należy najpierw poznać podstawy protokołu HTTP.

Protokół HTTP został opracowany w roku 1989 przez Sir Tim Berners-Lee w CERT. Pierwszą oficjalną specyfikację protokołu HTTP możemy odnaleźć w dokumencie RFC nr. 1945 z roku 1996.

Istnieje osiem podstawowych metod żądań tego protokołu:

- GET,
- HEAD,
- PUT,
- POST,
- DELETE,
- OPTIONS,
- CONNECT,
- TRACE.

Jednak nas interesuje tylko jedna metoda żądania: GET. Żądanie GET służy do pobrania wskazanego przez klienta zasobu sieci. Przykładowe wywołanie w Listingu 1.

Powyższe wywołanie to żądanie wysłania przez serwer *strona.com* pliku o nazwie *index.html*.

Serwer będzie traktował nas jako przeglądarkę Opera, zaś link dzięki, któremu kliknęliśmy by wejść na *strona.com* znajduje się pod adresem: *strona.biz.pk/linki.html*

Listing 1. Metoda żądania GET

```
GET /index.html HTTP/1.1
HOST: strona.com
User-Agent: "Opera/9.10 (X11; Linux i686; U;
en)"
Referer: "strona.biz.pk/linki.html"
```

Listing 2. Implementacja w języku TCL (dostępny na http://www.tcl.tk)

```
#!/usr/bin/env tclsh
# Istniejący adres serwera (w formie quasi DNS)
set target "refspoof.blox.pl"

# Istniejący adres dokumentu http który zamierzamy atakować
set target_url "http://refspoof.blox.pl/html"

# Fałszywy referer.
set fake_referer "http://tajemnicza-kraina.gov.pl/"

# Fałszywy User-Agent string. Podszywamy się pod przeglądarke.
set ua "Opera/9.10 (X11; Linux i686; U; en)"

# Liczba fałszywych żądań wysłanych do serwera
set imax 7
# Port na którym działa atakowany serwer http. Domyślnie 80.
set port 80
set i 0
puts "Atakowanie adresu: $target udając: $fake_referer"
        while {$i < $imax} {
                incr i
                set connection [socket $target $port]
                puts $connection "GET $target_url HTTP/1.0"
                puts $connection "Connection: Keep-Alive"
                puts $connection "User-Agent: $ua"
                puts $connection "Referer: $fake_referer\n\n"
                puts $connection "\n\n"
                puts $connection "\n\n"
                flush $connection
                close $connection
                puts $i
                after 1000
        }
puts "Zakonczono"
```

Rysunek 1. Screen pokazujący pracę skryptu

Dla *referer spoofing* istotne jest bliższe poznanie opcjonalnych parametrów wchodzących w skład przykładowych metod żądania. Nas interesują tylko dwa:

- `Referer` pozwala na zdefiniowanie strony z której przychodzimy (np. poprzez kliknięcie linka z reklamą)
- `User-Agent`: nazwa klienta dzięki któremu łączymy sie z daną stroną (np. przeglądarka internetowa).

Czym jest ten referer spoofing

Mając już wiedzę o tym, jak mniej więcej funkcjonuje żądanie GET, możemy wreszcie dowiedzieć się czym jest ten rodzaj ataku.

Referer spoofing jest techniką polegającą na sfałszowaniu sekcji *referer* w żądaniu GET.

Dzięki temu możemy wykazać, iż nasze połączanie pochodzi z wybranej przez nas witryny – np. ze strony która chcemy zareklamować.

Atak tego typu jest niczym innym, jak sfalcowanym odpowiednikiem poniższej sytuacji: Na stronie A znajdujemy link do strony B. Klikając na powyższy link, w logach serwera B dowiemy się, iż dzięki nagłówkowi *referer* kliknieciе na link doszło na stronie A.

Fałszując sekcję referer możemy nie tylko wskazać, iż referer pochodził z DOWOLNEJ strony, lecz co więcej, ta strona (i link) nie muszą nawet istnieć.

Przykładowa implemetacja ataku typu referer-spoofing

W przykładzie powyżej zastosowaliśmy atak *referer spoofing* w celu promocji fikcyjnej witryny *http://tajemnicza-kraina.gov.pl/* w popularnym systemie blogowym *blox.pl*. W ten sposób każdy, kto sprawdza statystyki odwiedzin swojego bloga, może przy okazji poznać naszą stronę. Poniższy zrzut ekranu

Listing. 3. Wywołanie programu

```
$tclsh8.4 refspoof.tcl
Atakowanie adresu: refspoof.blox.pl
udając: http://tajemnicza-
kraina.gov.pl/
1
2
3
4
5
6
7
Zakonczono
```

prezentuje efekt tego ataku. Oczywiście jest to dość ograniczona forma reklamy, gdyż jej jedynym odbiorcą jest właściciel strony kontrolujący na bieżąco logi odwiedzin.

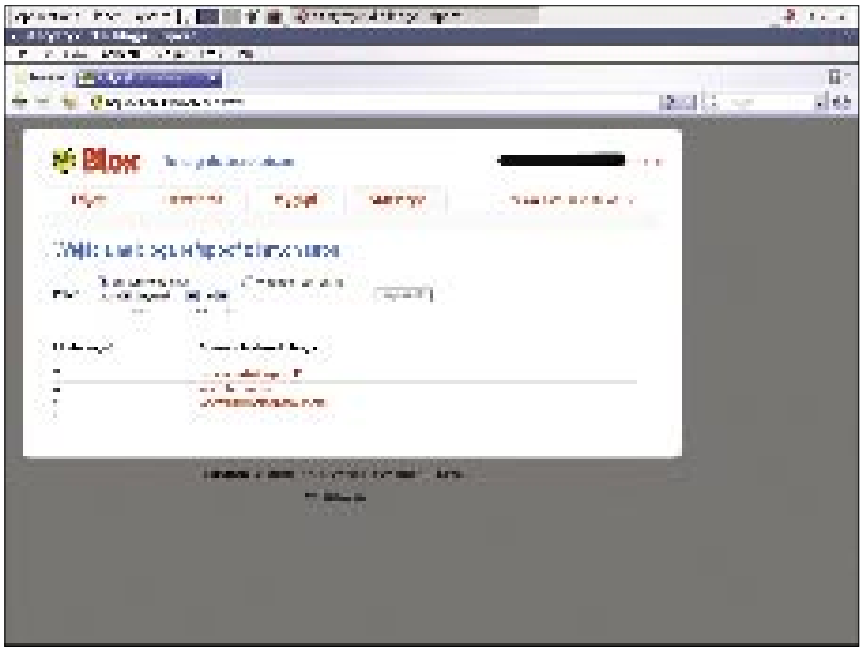
Szerszy zasięg reklamy

Naszym celem jest oczywiście szersze grono odbiorców, a to można uzyskać poprzez skierowane naszych ataków na upublicznione w sieci statystyki odwiedzin danych stron internetowych.

By odnaleźć tego typu strony wystarczy wpisać w google: *Usage Statistics for*. Pozwoli nam to na odnalezienie strony, z automatycznie generowanymi statystykami, tworzonej przez popularną aplikację Webalizer. Grafika numer 3 przedstawia przykładowy efekt ataku na tego typu stronę (nie jest to dzieło autora).

Pojawienie się naszego linku na podobnych stronach, pozwala na bardzo szybkie zindeksowanie jej przez wyszukiwarki internetowe i podwyższenie pozycji naszej strony w wynikach wyszukiwań. Jest to popularna metoda stosowana przez spamerów z całego świata.

Należy jasno zaznaczyć, iż tego typu działania są prawdopodobnie niezgodne z prawem, i nie należy ich stosować w praktyce.



Rysunek 2. Nasze sfałszowane statystyki odwiedzin na blogu

Rysunek 3. Przykład wykorzystania ataku referer spoofing na upublicznione statystyki strony

Czy istnieje jakaś forma obrony ?

Niestety nie istnieje jakaś uniwersalna forma obrony przed atakami *referer-spoofing* , gdyż wykorzystuje on fundamenty protokołu HTTP, którego nie można obejść nie łamiąc przy okazji standardów tego protokołu zdefiniowanego w dokumentach RFC.

Najprostszą formą obrony jest po prostu nieudostępnianie publicznie szczegółowych statystyk dotyczących wejść na naszą stronę.

Inną formą obrony jest logowanie adresów IP atakującego i blokowanie go przy pomocy regułek naszej ściany ogniowej(firewalla). Jednak budowanie tego typu regułek znacząco wybiega ponad tematykę prezentowanego artykułu.

Podsumowanie

Ataki typu *referer spoofing* są ciekawą i stosunkowo rzadko omawianą techniką pozwalającą na pozycjonowanie stron w internecie. Spowodowane jest to zapewne faktem, iż tego typu atak jest niczym innym jak formą fałszerstwa i reklama, przy pomocy tej techniki jest nie tylko wątpliwa moralnie ale i prawdopodobnie niezgodna z obowiązującym prawem.

Z drugiej strony ataki tego typu nie są zbyt dotkliwe dla właściciela strony na której zamierzamy się *reklamować*, wszakże wysyłając nasze żądanie fałszujemy jedynie adres pochodzenia naszego *kliknięcia* po czym zrywamy połączenie nie pobierając żadnych plików z serwera. Dzięki temu potencjalna ofiara nie ponosi kosztów związanych z np. ograniczeniem przepustowości łącza.

W praktyce warto więc ograniczyć się do atakowania stron znajomych, podszywając się pod np. organizacje walczące z piractwem czy policję.

O autorze

Paweł Szcześniak – Pasjonat systemów Unix-like z Gdańska. Zainteresowany w szczególności szeroko pojętym bezpieczeństwem komputerowym oraz tworzeniem użytecznych aplikacji do tego celu. W chwilach wolnych tworzy i testuje giełdowe systemy transakcyjne dla rynku Forex oraz kontraktów terminowych.
Kontakt z autorem: *pawelsz@sdf.lonestar.org*