

Published based on [Tips: Cara Mengetahui Apakah Spammer Mengubah Website Anda](#)

Tips: Cara Mengetahui Apakah Spammer Mengubah Website Anda

Spam cloaking jenis baru semakin populer belakangan ini: *spammer* meng-hack website populer yang memiliki ranking tinggi di Google dan kemudian memasukkan tautan penuh kata kunci yang diarahkan ke situs-situs lain. Apa yang bisa Anda lakukan untuk memastikan bahwa website Anda tidak disalahgunakan oleh spammer?

[caption id="" align="alignright" width="240" caption="Image by mathowie via Flickr"]



[/caption]

Apa itu cloaking?

Cloaking adalah teknik **spamming** di mana konten yang ditunjukkan kepada spider mesin pencari berbeda dari konten yang disajikan untuk pengguna biasa.

Hal ini dilakukan dengan memberikan konten yang berbeda berdasarkan **user-agent HTTP header** dari pengguna yang mengunjungi halaman situs, alamat **IP** pengunjung, atau halaman yang merujuk:

1. Bila pengguna teridentifikasi sebagai **search engine spider**, skrip pada server akan memberikan versi halaman web yang berbeda.
Spider mesin pencari dapat diidentifikasi berdasarkan alamat IP dan pada **user-agent HTTP header**.
2. Ketika seorang pengguna datang dari halaman tertentu (misalnya halaman hasil pencarian Google), server web memberikan versi halaman yang lain dengan apa yang didapatkan kalau pengguna memasukkan **URL** secara langsung di **browser**.

Metode-metode ini dapat dikombinasikan. Sebuah halaman web dapat melakukan cloaking didasarkan pada alamat IP, user-agent, halaman web perujuk atau kombinasi ketiganya.

Bagaimana spammer penyalahgunaan situs web Anda?

Banyak website yang memiliki lubang keamanan. Spammer menggunakan celah ini untuk meng-hack ke server dan mengubah isi halaman web. Mereka dapat melakukan hal di bawah ini pada halaman website Anda:

1. Memasukkan tautan penuh kata kunci yang merujuk ke situs spammer pada halaman web Anda. Tautan ini hanya dapat dilihat oleh spider pengindeks Google. Dari persepsi Google, tampak seolah-olah website Anda mendukung situs web spammer dengan *link* ini.
2. Mereka mengarahkan (*redirect*) pengunjung website Anda ke halaman web mereka sendiri, sementara Google mendapatkan halaman web Anda. Orang yang mengunjungi halaman web Anda setelah mengklik pada daftar website di hasil pencarian Google akan diarahkan ke situs web spammer.

Bagaimana Anda bisa mengetahui apakah spammer penyalahgunaan situs Anda?

Ada beberapa cara untuk mengetahui apakah spammer telah mengubah halaman web Anda:

1. Gunakan browser yang dapat melakukan simulasi spider mesin pencari. Masukkan satu URL halaman web anda dan pilih "**Googlebot**". Browser ini akan menunjukkan apa yang dilihat oleh Google. Metode ini memungkinkan Anda memeriksa jika halaman web dimaksud menunjukkan isi yang berbeda

berdasarkan user-agent.

2. Lakukan pencarian Google untuk "site: yourdomain.com" (ganti yourdomain.com dengan domain Anda sendiri). Browse halaman hasil pencarian dan periksa judul dan deskripsi yang Google tampilkan untuk halaman web Anda.
Klik pada daftar hasil pencarian untuk memastikan bahwa pengunjung diarahkan ke halaman yang benar.
3. Klik pada tautan "*Cached*" di halaman hasil pencarian Google untuk melihat konten yang telah diindeks oleh Google dari halaman web Anda.
Cari tautan, [Javascript](#) dan elemen-elemen lainnya yang bukan bagian dari halaman web tersebut.

Gunakan tips di atas untuk mengetahui apakah *hacker* telah mengubah isi halaman web Anda. Untuk memastikan bahwa hacker tidak dapat menyalahgunakannya, gunakan versi sistem manajemen konten (*CMS - content management system*) terbaru dan jangan lupa instal update keamanan terbaru.

You can also find this article published on [Tips: Cara Mengetahui Apakah Spammer Mengubah Website Anda](#), and on the tag pages [black hat](#), [google](#), [mesin pencari](#), [seo](#), [web spam](#).