

ABSTRACT

Malware signature is a special sign (code) taken from a malware sample. This signature then stored in a library (often called Malware Library) in the system. When a new virus-signature is created, the user must download the new signature file. To update the system identification library it uses. Next all the code signatures that have been downloaded will be stored in the virus library that is in the server.

Website scanning process is important since Google will blacklist website that contain malware. Being blacklisted by Google is one of the worst things that can happen to a website. The public shame coming from every visitor being stopped by the Big Red Warning page from Google that can literally destroy any online business.

Handling system from malware attack using signature-base method is expected to detect website script that indicated to contain malware. The system also comes with reset malware data permission action to octal permission. At the end of this research the expected results obtained can provide information about the weakness of the script on the website and increase website security from malware attacks.

Keywords: Malware, Malware Scanning, Website Security, Hardening Website, Google Blacklisted

xii+102 Pages, 46 Figures, 17 Tables, 2 Attachments

References 10 (2009-2016)

UNIVERSITAS
MERCU BUANA

ABSTRAK

Malware signature merupakan tanda khusus (kode) yang diambil dari sebuah *sample virus*. *Signature* ini selanjutnya disimpan dalam suatu *library* (sering disebut *Malware Library*) di dalam sistem. Apabila suatu *signature* baru selesai dibuat, maka pengguna, harus men-*download* file *signature* baru. untuk meng-*update library* sistem identifikasi yang digunakannya. Selanjutnya semua kode *signature* yang telah *download* akan disimpan di dalam *library* yang ada di dalam server.

Pentingnya proses identifikasi *website* terhadap *malware* karena jika *website* terdeteksi *malware* oleh google maka akan *blacklist*. *Blacklist* oleh google merupakan salah satu hal terburuk yang terjadi pada sebuah *website*. Sebuah hal yang memalukan jika *visitor* atau konsumen sebuah *website* melihat tanda *warning malware* dari google. Hal ini bisa menghancurkan sebuah bisnis *online* karena hilangnya kepercayaan dari konsumen.

Sistem penanganan serangan *malware* menggunakan metode *signature-based* diharapkan dapat segera mendeteksi skrip yang terinfeksi *malware*. Sistem juga dilengkapi dengan aksi *reset permission* seluruh data *malware* ke *octal permission*. Pada akhir penelitian diharapkan hasil yang diperoleh memberikan informasi tentang kelemahan skrip pada *website* dan meningkatkan rasa aman dari serangan *malware*.

Kata Kunci: *Malware*, Deteksi *Malware*, Keamanan *Website*, Meningkatkan Keamanan *Website*, *Blacklist* Google

xii+102 Halaman, 46 Gambar, 17 Tabel; 2 Lampiran

Daftar Pustaka 10 (2009-2016)