Faktor Exacta 9(1): 102-108, 2016
ISSN: 1979-276X

PEMANFAATAN CURL PADA PHP GUNA MENDAPATKAN INFORMASI MALWARE DENGAN MEMANFAATKAN AVG THREAD LABS

HENDRO PURWOKO
hendroprwk08@gmail.com
Program Studi Teknik Informatika, Fakultas Teknik, Matematika dan IPA
Universitas Indraprasta PGRI

Abstrak. Malware telah ada selama lebih dari 40 tahun, menurut laporan dari Panda Security pada laporan tahunannya, dalam 3 bulan saja ada rata-rata 205,000 hingga 225,000 varian baru. Malware tidak hanya menyerang PC (Personal Computer), tetapi juga ponsel yang memiliki sistem operasi. Masuknya malware kedalam *gadget* diakibatkan oleh pengguna ketika melakukan kegiatan ber-*social media, download,* membuka lampiran email atau bahkan ketika tanpa sengaja menekan iklan yang ternyata berisi malware. Penelitian ini membahas proses pembuatan aplikasi berbasis web yang dapat digunakan untuk mendeteksi malware dengan menggunakan fasilitas CURL sebagai *trigger* pada proses pemindaian yang dapat memberikan perintah kepada AVG Theard Labs untuk memeriksa URL.

Kata kunci: malware, pemindai malware,CURL, PHP, web

Abstract. Malware has existed for more than 40 years, according to the report from Panda Security on it's annual report, only within 3 months there's been about 205.000 until 225.000 new variants. Malware does not only attack the PC (Personal Computer), but also a mobile phone which has an operating system. The enterance of malware into gadget is caused by users when doing activities such as social media, download, open email attachments or even when accidentally press the advertisement which containing malware. This study discusses about the process of making a web-based application which can be used to detect malware using CURL as a trigger in the process of scanning that can give orders to the AVG Theard Labs to check the URL.

Keywords: malware, malware scanner, CURL, PHP, web

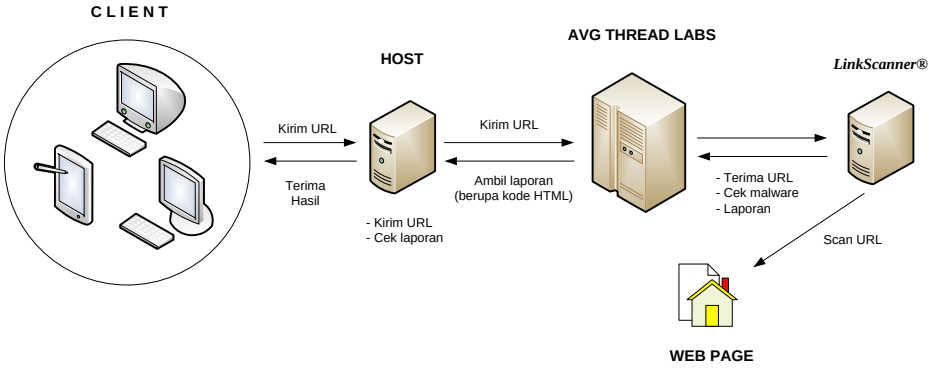
PENDAHULUAN

Malware telah ada selama lebih dari 40 tahun, menurut laporan dari Panda Security pada laporan tahunannya, ada rata-rata 205,000 hingga 225,000 varian baru, dengan total perputaran 20 milliar serangan pada Januari hingga Maret 2015. Dalam kondisi tersebut Trojan masih merupakan salah satu malware yang sering digunakan. Menurut data: Cina berada pada urutan pertama dengan *infection rate* 48.01%, kemudian Turkey 43.33% dan Peru 42.18%. PandaSecurity pun melaporkan bahwa ada empat perusahaan teknologi yang menjadi korban, yaitu Twitter ditargetkan sejak bulan Februari tahun 2013, diikuti oleh Facebook, Apple, dan Microsoft.

Panda security juga melaporkan bahwa jenis malware yang paling sering digunakan adalah: trojan (72,75%), worm (4,52%), virus (14,85%), adware / spyware (41,51%), dan jumlah yang sangat kecil (3.37%) yang jatuh ke dalam kategori "lainnya".

Perlu diketahui bahwa Malware tidak hanya menyerang PC (*Personal Computer*), tetapi juga ponsel yang memiliki sistem operasi. Masuknya malware kedalam *gadget* diakibatkan oleh pengguna ketika melakukan kegiatan ber-*social media*, *download*, membuka lampiran email atau bahkan ketika tanpa sengaja menekan iklan yang ternyata berisi malware dan tanpa pengguna sadari, malware tersebut berhasil masuk ke dalam sistem. Ancaman malware terhadap gadget sangat rentan sekali karena itu sebaiknya pengguna memasang *anti-malware*.

Dari kasus tersebut penulis mencoba membuat aplikasi berbasis web yang dapat digunakan untuk mendeteksi malware. Dengan menggunakan fasilitas CURL yang dapat memberikan perintah kepada AVG Theard Labs untuk memeriksa URL yang dikirimkan melalui kode PHP. Setelah AVG Theard Labs berhasil memeriksa URL tersebut, maka CURL akan menarik informasi yang diberikan olehAVG Theard Labs dan menampilkannya pada pengguna aplikasi. Dan dari setiap hasil yang didapatakan, langsung disimpan kedalam log histori.



Gambar 1: Konsep pemindaian URL

Terlihat ada pada gambar diatas bahwa host mengirim perintah kepada AVG Thread Labs dan menarik laporan berupa kode-kode HTML. Kode-kode tersebut diolah oleh host kemudian menampilkan respon kepada*client*. Untuk melalukan proses pemindaian ini pengguna harus menggunakan koneksi internet. Dalam penerapannya mengunakan konsep berorientasi objek.

TINJAUAN PUSTAKA

AVG Thread Labs

Menurut situs resminya:

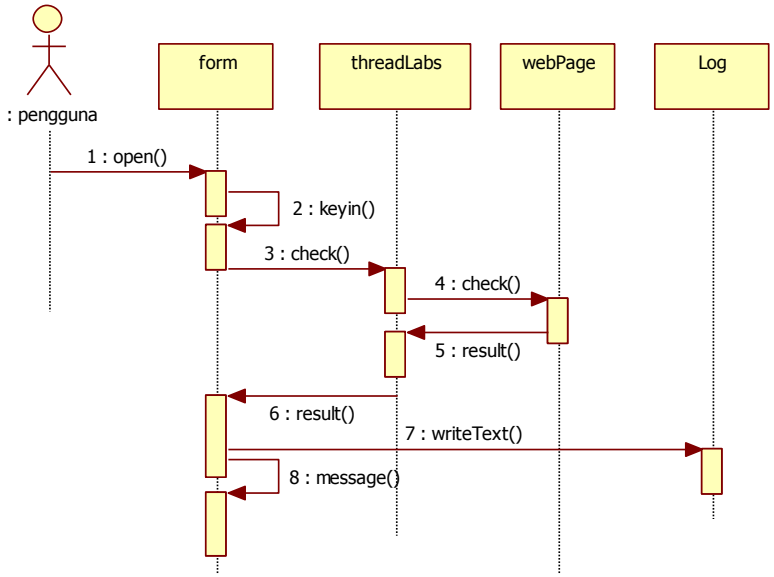
"Threat Labs is AVG's latest security tool, continuing our commitment to malware and virus detection and eradication. With an Internet security and protection policy built heavily around the concept of 'scan before you leap', AVG Threat Labs offers the same kind of pre-click analysis as our unique LinkScanner® real-time surf and search technology, though at a far more comprehensive level."

AVG Threat Labs merupakan situs yang berfungsi seperti "pengalih URL" yang berfungsi untuk mendeteksi virus dan malware. Bentuk web tersebut seperti mesin pencari, tetapi pada tahap selanjutnya AVG Thead Labs akan memberikan laporan mengenai keamanan situs yang dipindai melalui *LinkScanner*®.

CURL

Libcurl / CURL, yaitu sebuah *library* pada PHP yang diciptakan oleh Daniel Stenberg, yang memungkinkan Anda untuk terhubung dan berkomunikasi dengan berbagai jenis server dengan berbagai jenis protokol. libcurl saat ini mendukung protokol http, https, ftp, gopher, telnet, dict, file, dan ldap. libcurl juga mendukung sertifikat HTTPS, HTTP POST, HTTP PUT, FTP upload (juga bisa dilakukan dengan ekstensi ftp), proxy, cookies, dan otentikasi pengguna dan password dalam bentuk HTTP. Fungsi-fungsi ini telah ditambahkan di PHP 4.0.2.

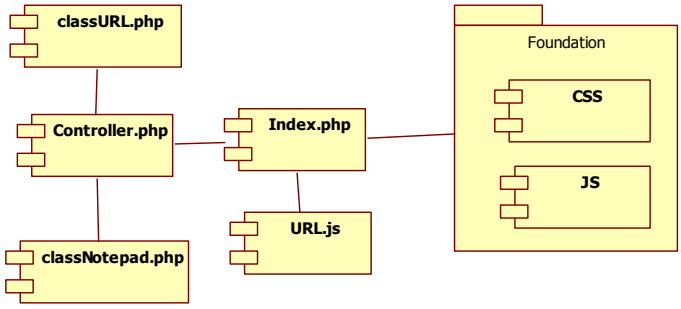
METODE



Gambar 2: Sequence diagram proses kerja sistem

Adapun konsep kerja pada penelitian ini adalah dengan memasukkan alamat web yang akan periksa. Proses selanjutnya dengan kode PHP dan Libcurl, alamat web tersebut dialihkan ke web AVG Thread Labs. Selesai memetakan alamat web tersebut AVG Thread Labs memeriksa kondisi web dan hasil keluaran tersebut diambil dengan kode PHP berupa kode HTML. Kode HTML tak bisa ditampilkan secara langsung, sehingga diperlukan *regular expression* untuk menterjemahkan kode tersebut dan menampilkan hasilnya kepada pengguna web.

Sehingga dalam menerapkan penelitian ini, penulis mengunakan konsep berorientasi objek dengan menggunakan dua class: yaitu classURL.php dan classNotepad.php. Kedua class tersebut dimasukkan kedalam controller.php yang kemudian dimanfaatkan untuk memproses kebutuhan index.php.



Gambar 3: Komponen Aplikasi

Pada classURL ada dua function: setURL($text) dan getURL(). Pada getURL() berisi kode untuk pengiriman alamat URL menggunakan CURL yang ingin dipindai dan membaca hasilnya dengan menggunakan DOMXPATH, seperti tertera pada kode dibawah ini:

```
function getURL(){
        ...
        $SCAN=curl_init($TARGET_LINK);
        ...
        $data=curl_exec($SCAN);
        ...
        $dom=new DOMDocument();

        if(@$dom->loadHTML($data)){
                $xpath = new DOMXPath($dom);

                $elements = $xpath->query('//ul[@class="threatlist"]/li |
                                //h2[@class="green"] | //h2[@class="red"] |
                                //h2[@class="yellow"] |//span[@id="percentage"] |
                                //span[@id="totallikes"] | //p[@class="popularity"]'
                                );
        }
        ...
        $filterArray = array_values(array_filter($myArray));
        $table = array(); $prejson = array();

        for($i=4; $i<=count($filterArray)-1; $i++){
                $exp = explode(" - ", $filterArray[$i]);
                $table[]=array("info" => $exp[0], "url" => $exp[1]);
        }

        $prejson[] = array("web" => $filterArray[0], "warn" => $filterArray[1],
                        "impact" => $filterArray[2], "likes" => $filterArray[3],
                        "tables" => $table);

        print json_encode($prejson);
}
```

Hasil olah dari DOMXPATH kemudian dikonversi menjadi JSON menggunakan json_encode dan kirim ke index.php.

HASIL DAN PEMBAHASAN

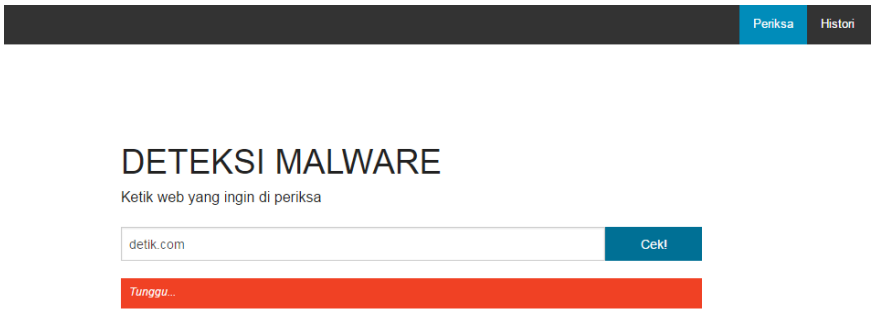
Desain Antar-Muka

Gambar 4: Desain antar muka

Dalam pembuatan sistem ini desain antar muka dibuat dengan menggunakan HTML, FOUNDATION dan JQuery agar tampilan lebih terlihat lebih dinamis.

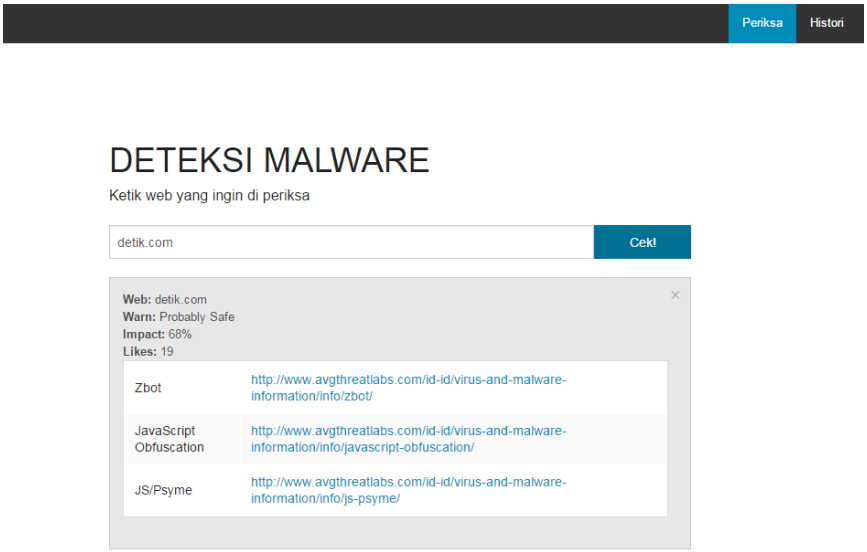
Pada bagian atas disematkan textbox untuk memasukkan alamat web dan tombol sebagai antar-muka untuk mengeksekusi alamat web tersebut. Dibawahnya terdapat dua kotak yang berfungsi sebagai notifikasi dari hasil pemeriksaan alamat web.

Hasil akhir dari proses pengkodean dan desain antar-muka yang dibahas sebelumnya adalah sebagai berikut:



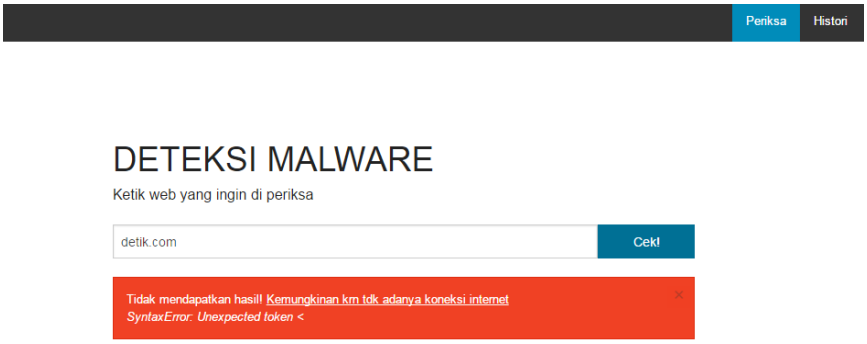
Gambar 5: Halaman index yang sedang memproses URL

Pada proses ini pengguna diharuskan memasukkan alamat URL yang ingin dipindai kemudian tekan "Cek!" dan system akan mengirim alamat web (URL) ke AVG untuk diperiksa menggunakan *LinkScanner*®.

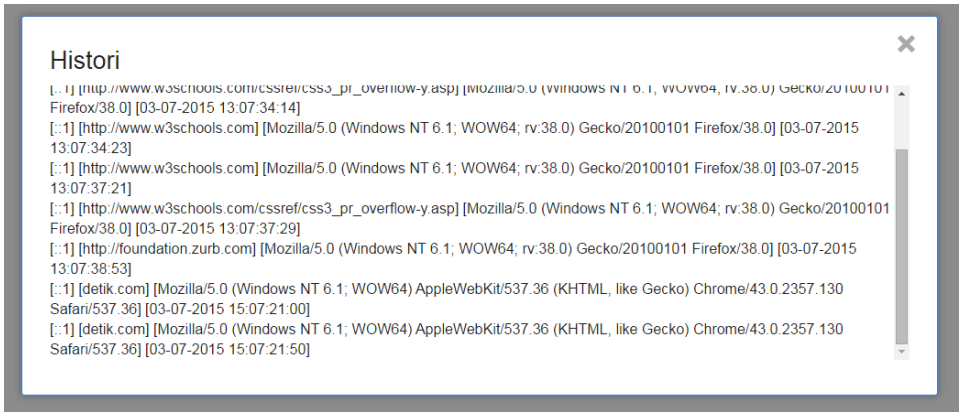


Gambar 6: Hasil akhir dari pemindaian URL detik.com

Hasil tersebut akan dibaca menggunakan kode PHP dan ditarik ke dalam halaman index.php dengan menampilkan informasi web yang sudah diperiksa berikut informasi malware yang ada pada web.



Gambar 7: Contoh pesan kesalahan



Gambar 8: Histori pemindaian

Dalam histori pemindaian terdapat informasi IP si pemindai, halaman web yang dipindai, jenis browser yang digunakan, tanggal dan jam. Informasi tersebut disimpan pada notepad yang ada pada host.

PENUTUP

Simpulan

Penggunaan CURL merupakan cara yang efektif untuk menarik informasi malware dari AVG Thread Labs, walau pun informasi yang dihasilkan berupa kode HTML namun dapat diolah menggunakan DOMXPATH dan ditampilkan ke komputer pengguna.

Saran

Untuk penelitian selanjutnya dapat dibuat pemetaan berisi data malware yang terpusat dan data tersebut diperbarui secara berkala sehingga menjadi sumber informasi bagi pengguna internet secara umum.

DAFTAR PUSTAKA

AVG, 2015. **What is Threat Labs & Why did AVG build it?**. Diakses tanggal 6 Agustus 2015 dari http://www.avgthreatlabs.com/website-safety-reports/article/3/.

Herlawati, Prabowo. 2011. **Menggunakan UML**. Bandung: Informatika.

Ladjamudin, Al-Bahra. 2005. **Analisis dan Desain Sistem Informasi**. Yogyakarta: Graha Ilmu.

Pandalabs, 2015. **Pandalabs report Q1 2015 january-March 2015,** Panda labs.

PHP. 2015. **Libcurl**. Diakses tanggal 6 Agustus 2015 dari http://php.net/manual/en/intro.curl.php.

Roviuddin. 2008. **Web Programming**. Jakarta: Dinamika Ilmu.