BLOKIR MALWARE BERBAHAYA MELEWATI PROXY MENGGUNAKAN ROUTER PFSENSE DAN PAKET HAVP

Dedi Irawan[1]
[1]Program Diploma-III Sistem Informasi – Fakultas Ilmu Komputer
Universitas Muhammadiyah Metro
[1]Alamat: Jl. Gatot Subroto No.100 Yosodadi Kota Metro, Telpon: (0725) 42445
[1]Email: dedi.mti@gmail.com

Abstrack

Reporting from the Apple Support page, malware is malicious software, containing viruses, worms, Trojan horses, and other programs that may affect your Mac or your privacy. Software You can install items from emails, messages, and websites. Source: https://support.apple.com/kb/PH25640?locale=id_ID&viewlocale=id_ID. This program can change, damage, search for loopholes, and steal personal data of someone who is certainly very harmful. Malware can generate when downloading data via email, messages, and websites. One of the most widely used devices today is the smartphone as a device to access websites. Although all computers have antivirus installed, it should be added to another computer, in this case HAVP works very well.

Keywords: malware, malicious software, antivirus HAVP

Abstrak

Dilansir dari halaman *Support Apple*, malware adalah perangkat lunak berbahaya, yang berisi virus, worm, trojan horse, dan program lainnya yang dapat membahayakan Mac atau privasi Anda. Malware dapat diinstal saat Anda mengunduh item dari email, pesan, dan situs web. Sumber: https://support.apple.com/kb/PH25640?locale=id_ID&viewlocale=id_ID. Program ini dapat mengubah, merusak, mencari celah, dan mencuri data pribadi seseorang yang tentu sangat merugikan. Malware dapat menghasilkan saat mengunduh data melalui email, pesan, dan situs web. Salah satu perangkat yang paling banyak digunakaan saat ini adalah smartphone sebagai perangkat untuk mengakses situs web. Meskipun semua komputer sudah terinstal antivirus, harus ditambahkan lapisan perlindungan lain ke jaringan komputer, dalam hal ini HAVP bekerja dengan sangat baik.

Kata Kunci: malware, malicious software, antivirus HAVP

PENDAHULUAN

Malware adalah perangkat lunak berbahaya, yang berisi virus, worm, trojan horse, dan program lainnya yang dapat membahayakan perangkat keras (PC) atau pencurian data pribadi. Malware merupakan sebuah singkatan dari “Malicious Software” yang berarti perangkat lunak mencurigakan. Sebuah malware dapat mengakibatkan dampak buruk bagi sebuah komputer maupun user (pengguna komputer). Program ini dapat mengubah, merusak, mencari celah, dan mencuri data pribadi seseorang yang tentu sangat merugikan.

Malware dapat diinstal saat melakukan download data melalui email, pesan, dan situs web. Salah satu perangkat yang paling banyak digunakaan saat ini adalah smartphone sebagai perangkat untuk mengakses situs web. Dilansir dari merdeka.com, malware menyerang ke sistem antrean di RS Dharmais dan Harapan Kita, sehingga efeknya bakal dirasakan oleh pasien. Bahwa efek yang terjadi ini mengakibatkan pasien yang seharusnya ditangani lebih dahulu sesuai jadwal, maka akan mengalami keterlambatan penanganan. Imbas parah dari keterlambatan penanganan ini berdampak pada nyawa seseorang, sumber: https://www.merdeka.com/teknologi/begini-dampak-dari-serangan-malware-wannacrypt.html

a. Rumusan Masalah

Dari latar belakang masalah diatas maka sangat dibutuhkan rumusan masalah, yaitu:

1. Bagaimana memblokir malwaware sebelum memasuki jaringan komputer?
2. Bagaimana menambahkan lapisan perlindungan lain ke jaringan menggunakan HAVP?
3. Bagaimana cara browsing yang tepat agar tidak terkena malware?

b. Tujuan Penelitian

Berdasarkan rumusan masalah diatas maka tujuan dari penelitian ini yaitu:

1. Memblokir malware sebelum memasuki jaringan komputer untuk publik atau hotspot.
2. Melakukan penambahan lapisan perlindungan ke jaringan komputer menggunakan HAVP.
3. Melakukan Browsing yang tepat agar tidak terkena malware kembali.

c. Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah:

1. Mengamankan data pribadi dari pencurian yang dilakukan secara online.
2. Adanya penambahan lapisan perlindungan terhadap serangan malware menggunakan HAVP.
3. Nyaman saat melakukan browsing agar tidak terkena serangan malware kembali.

KAJIAN TEORI

a. Alat dan Bahan

Penelitian ini dilakukan dengan cara melakukan instalasi dan konfigurasi pada router pfsense. Setelah tahapan instalasi dan konfigurasi berhasil dilakukan maka selanjutnya dilakukan ujicoba sistem. Adapun prasyarat untuk mendapatkan paket HAVP bekerja, harus sudah memiliki proxy squid transparan berjalan di pfSense.

b. Software (Perangkat Lunak)

HAVP (*HTTP Anti Virus Proxy*) adalah proxy HTTP dengan pemindai antivirus. Mendukung ClamAV secara gratis, tetapi juga sebagai solusi komersial misalnya Kaspersky, Sophos dan F-Prot. Tujuan utamanya adalah mengunduh/download tanpa henti daan secara terus menerus sehingga lancar dari lalu lintas HTTP. Beberapa fitur-fitur yang terdapat pada HAVP (*HTTP Anti Virus Proxy*), seperti pada tabel 2.1 di bawah ini:

Tabel 2.1 Fitur HAVP (*HTTP Anti Virus Proxy*)

No	Nama Fitur
1.	HTTP Antivirus proxy
2.	Multiple scanner support at the same time
3.	Support free Clamav (GPL antivirus) and commercial AV scanner
4.	Scans complete incomming traffic
5.	Nonblocking downloads
6.	Smooth scanning of dynamic and password protected traffic
7.	Can used with squid or other proxy
8.	Parent proxy support
9.	Transparent proxy support
10.	Logfile

11.	Process change to defined user and group
12.	Daemon
13.	Operating System: Linux
14.	Written in C++
15.	Released under GPL

c. Hardware (Perangkat Keras)

Hardware (perangkat keras) yang digunakan dalam penelitian ini adalah sebagai berikut, seperti pada tabel 2.2 di bawah ini:

Tabel 2.2 Rancangan Hardware (perangkat keras)

No	Nama Komponen	Detail
1.	1 Unit Komputer	Komputer dengan intel Core i3.
2.	2 Unit Lancard (kartu jaringan)	D-Link Gigabit Ethernet Adapter
3.	Switch	D-Link Gigabit Switch

d. Tahapan Instalasi HAVP (*HTTP Anti Virus Proxy*)

Untuk kali pertama, hal yang harus dilakukan harus menginstal paket HAVP. Caranya Klik pada item menu paket dalam menu sistem untuk memuat manajer paket pfSense. Cari paket HAVP kemudian klik simbol plus , di sisi kanan deskripsi paket untuk menginstalnya. Seperti pada gambar 2.1 dibawah ini:

Gambar 2.1 Instal paket HAVP menggunakan manajer paket pfSense.

e. Tahapan Konfigurasi HAVP (*HTTP Anti Virus Proxy*)

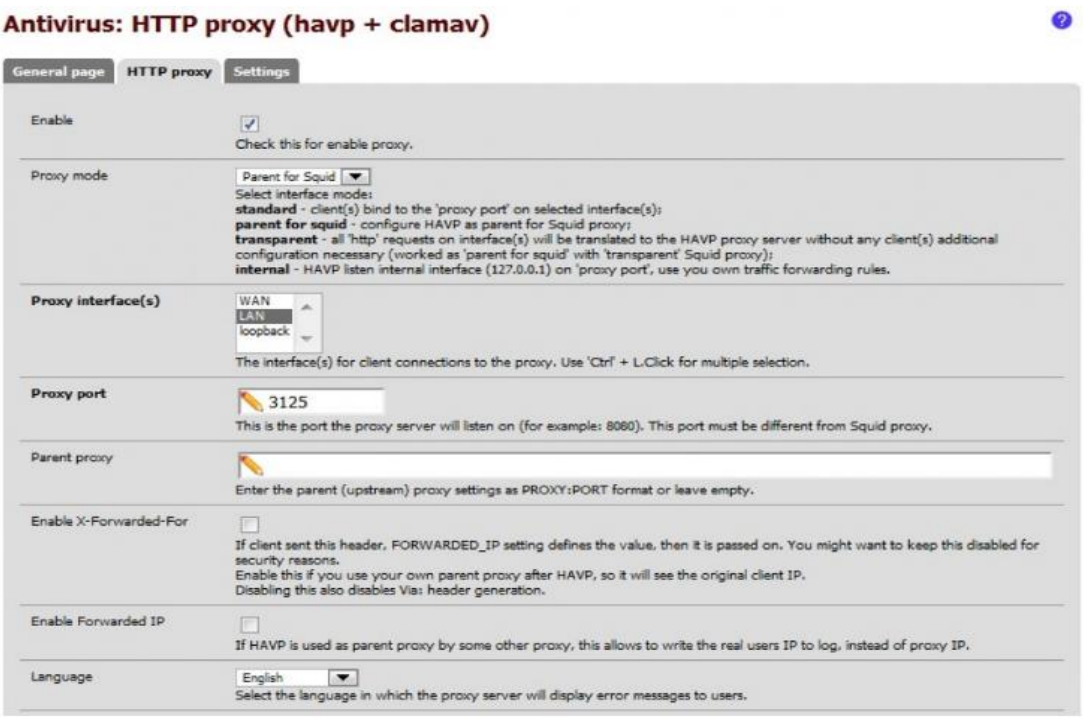
Setelah berhasil melakukan instalasi HAVP, diperlukan beberapa konfigurasi/pengaturan yang perlu dimodifikasi sedemikian rupa sebelum nantinya berfungsi/berjalan dengan benar. Klik pada entri antivirus di menu layanan untuk mengakses pengaturan HAVP.

Langkah berikutnya klik pada tab proxy HTTP dan centang kotak centang yang pertama untuk mengaktifkan proxy. Untuk pengaturan mode proxy pilih parent untuk squid. Dengan mengatur squid sebagai lalu lintas proxy induk akan mengalir seperti yang ditunjukkan di bawah ini:

Client <-> pfSense Gateway <-> Squid Proxy <-> HAVP <-> Internet

Harus dipastikan pada tampilan proxy diatur ke LAN, nomor port default akan berfungsi dengan baik. Lakukan juga pengubahan pemilihan bahasa ke bahasa inggris karena bahasa Inggris bukan standarnya. Bahasa yang dipilih akan mempengaruhi bahasa apa yang akan menampilkan pesan kesalahan klien.

Berikutnya geser sampai kebawah dan klik tombol simpan. Adapun tahapan konfigurasi dapat dilihat pada gambar 2.2 dibawah ini. .



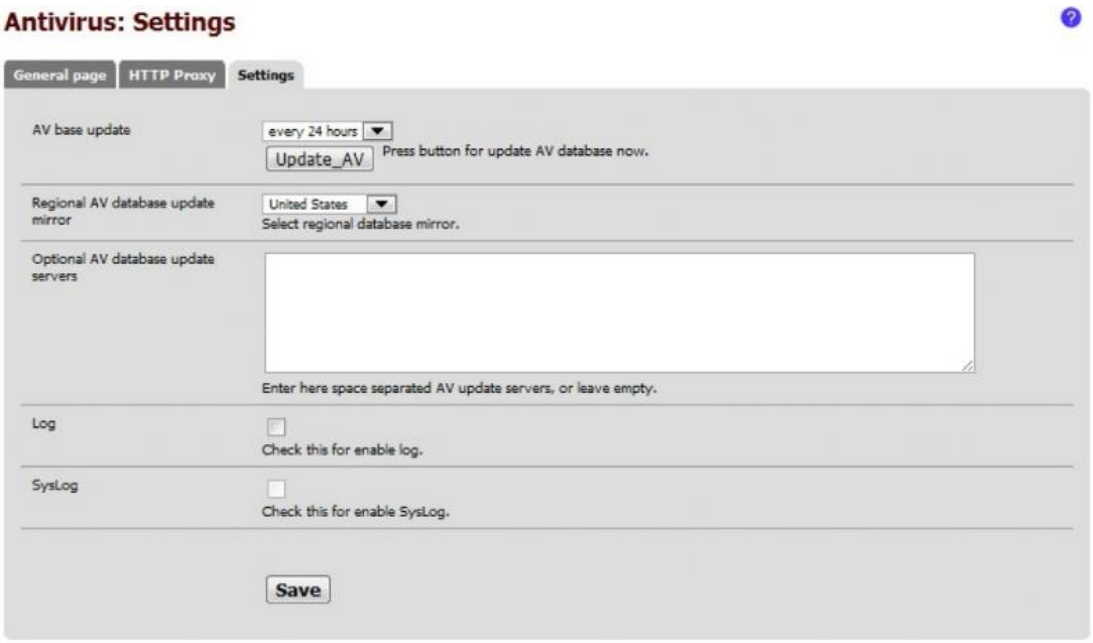
Gambar 2.2 Halaman konfigurasi HAVP

f. Pembaruan Definisi Otomatis (*HTTP Anti Virus Proxy*)

Untuk dapat mengaktifkan pembaruan secara otomatis dari definisi virus, klik pada tab pengaturan. Disarankan untuk mengatur pembaruan basis AV supaya nantinya terjadi setiap 24 jam. Apabila khawatir tentang adanya ancaman *zero*

day, Lakukanpengaturan pembaruan agar terjadi lebih sering meskipun nantinya akan menggunakan lebih banyak bandwidth internet.

Pilih mirror unduhan regional yang posisinya terdekat, sehingga memungkinkan definisi untuk mengunduh lebih cepat. Apabila mengalami kesulitan saat mengunduh pembaruan, dapat mengaktifkan pencatatan yang berguna untuk membantu mencari tahu masalahnya. Adapun konfigurasi untuk mengunduh pembaruan definisi secara otomatis, dapat dilihat pada gambar 2.3 dibawah ini.



Gambar 2.3 Konfigurasi untuk mengunduh pembaruan definisi secara otomatis

METODELOGI

Setelah tahapan instalasi dan konfigurasi telah berhasil dilakukan, maka seharusnya HAVP telah aktif dan berjalan. Pada tahapan pemeriksaan status layanan hanya untuk memastikan semua layanan berjalan dan file definisi telah diunduh/download. Pada halaman HAVP harus melihat gambar panah hijau di sebelah layanan proxy dan server antivirus, seperti pada gambar 3.1 dibawah ini.

Gambar 3.1 HAVP berfungsi proxy dan server antivirus harus berwarna hijau.

Di bidang versi Anda akan melihat ClamAV diikuti oleh tanggal file definisi virus yang Anda gunakan. Jika file sudah kedaluwarsa, buka tab pengaturan dan klik tombol Update_AV untuk memulai proses pembaruan secara manual.

Scan malware dapat dilakukan dengan beberapa pilihan, yaitu:

a) Squid cache path (scan you squid cache now)

Yaitu lokasi/alamat cache yang tersimpan

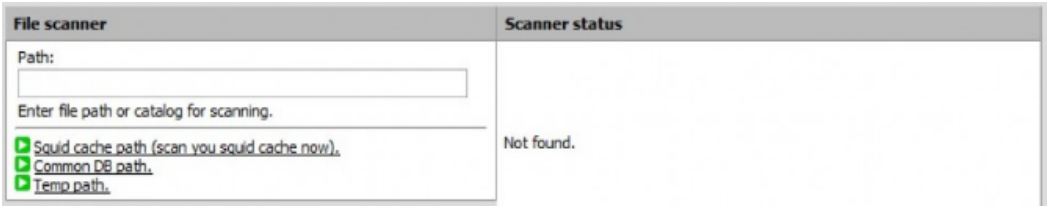
b) Common DB Path yang akan dilakukan scan malware

Yaitu tempat/lokasi database yang akan dilakukan scan malware

c) Temp path

Yaitu tempat sementara yang akan dilakukan scan malware

Adapun pemilihan scan malware, seperti pada gambar 3.2 dibawah ini:



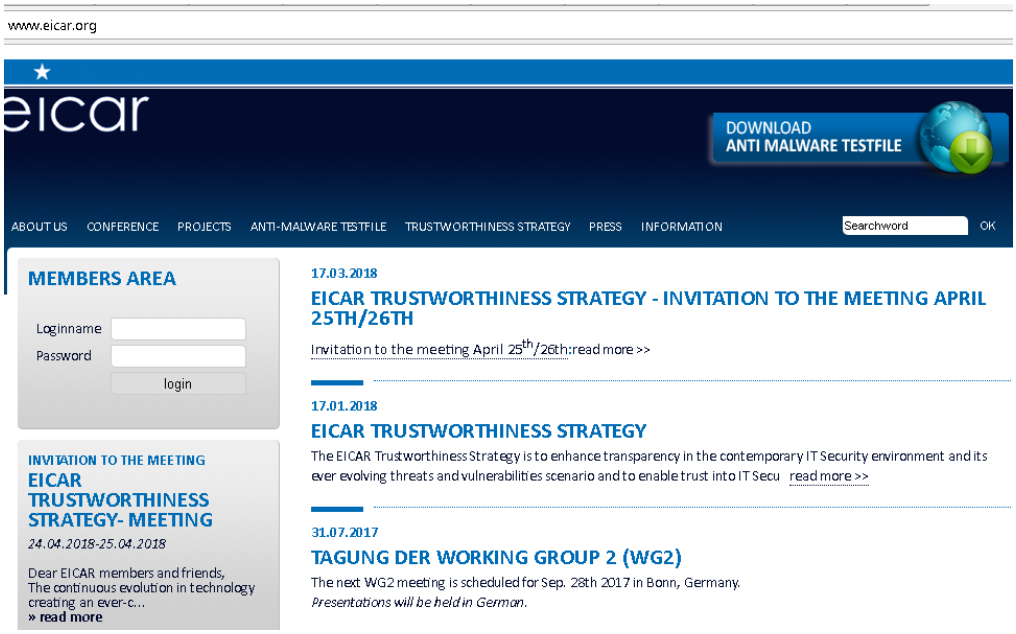
Gambar 3.2 Pilihan scan malware

Pengecekan Malware dapat dilakukan setiap saat oleh pengguna, seperti pada gambar 3.3 dibawah ini.

Gambar 3.3 Pengecekan malware

a. Melihat aktifitas yang dilakukan user/pengguna,

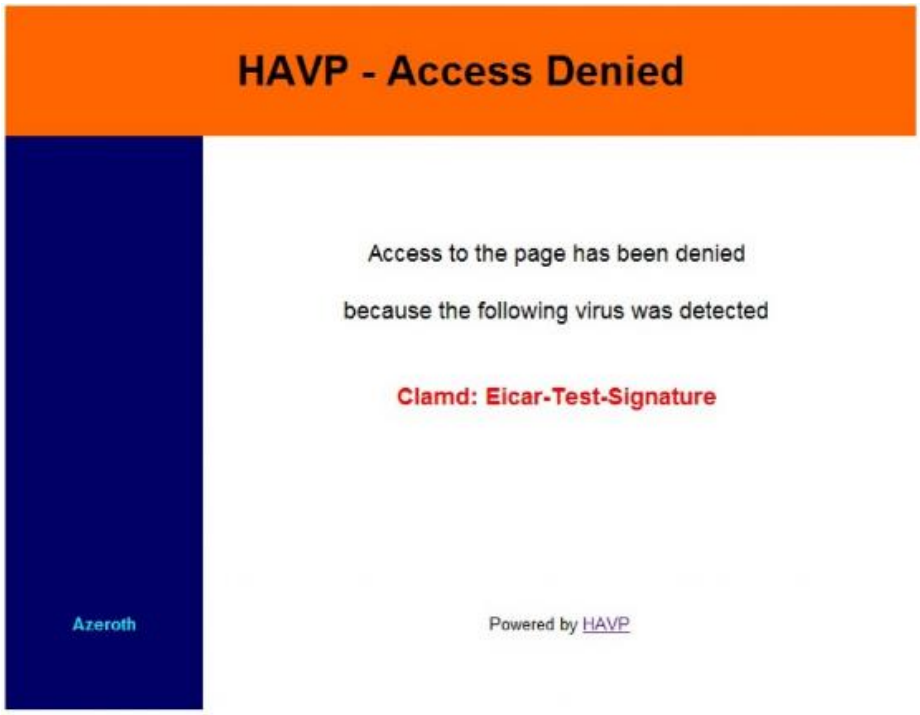
Pengujian dapat dilakukan dengan mencoba mengunduh/download virus. Dapat juga melakukan tes dengan cara mengakses dan mengunduh file tes virus EICAR dari halaman http://www.eicar.org , seperti pada gambar 3.3 dibawah ini.



Gambar 3.3 Halaman Homepage EICAR

b. Pengalihan halaman jika terdapat malware

Pengujian dilakukan, yaitu file tes yang didownload bukan virus yang sebenarnya, file tersebut berisi tanda tangan standar yang digunakan untuk menguji perangkat lunak antivirus. Jika konfigurasi berhasil maka akan seperti pada gambar 3.4 dibawah ini.



Gambar 3.4 User mencoba mengunduh file berbahaya dialihkan ke halaman kesalahan. Jika HAVP berfungsi dengan baik maka nantinya malware akan diarahkan ke halaman lain dengan pesan akses ditolak. Apabila tidak melihat

halaman peringatan muncul, maka periksa kembali status layanan pada halaman pengaturan HAVP.

Simpulan

Malware adalah perangkat lunak berbahaya, yang berisi virus, worm, trojan horse, dan program lainnya yang dapat membahayakan perangkat keras (PC) atau pencurian data pribadi. Malware berbahaya karena sifat dan tujuan diciptakannya dan perlu diketahui bahwa virus sebenarnya merupakan bagian dari malware. Malware di kelompokkan dalam tiga kategori berdasarkan tujuan pembuatnya, yaitu:

a) Malware yang menginveksi komputer, contohnya virus, dan worm.
b) Malware yang mengintai dan mencuri data, contohnya spyware
c) Malware yang menyerang secara sembunyi, contohnya Trojan, atau backdoor

Dengan menggunakan router pfsense maka dapat memudahkan pengguna dalam melakukan monitor malware pada setiap saat. Selain itu juga pengguna dapat melakukan pemutakhiran/update malware selama 24 jam. Meskipun semua komputer sudah terinstal antivirus, harus ditambahkan lapisan perlindungan lain ke jaringan komputer, dalam hal ini HAVP .

REFERENSI

[1]. Irawan, D. (2015). KEAMANAN JARINGAN KOMPUTER DENGAN METODE BLOCKING PORT PADA LABORATORIUM KOMPUTER PROGRAM DIPLOMA-III SISTEM INFORMASI UNIVERSITAS MUHAMMADIYAH METRO. *MIKROTIK: Jurnal Manajemen Informatika*, *5*(2).

[2]. Irawan, D. (2014). Mempercepat Koneksi Akses Internet Dengan Membangun Lusca Proxy Server Menggunakan Linux Pfsense Pada Universitas Muhammadiyah Metro. *Jurnal Informatika*, *12*(2), 190-197.

[3]. Saputra, D. D., & Sudarmaji, S. (2017). PEMODELAN SISTEM APLIKASI PENGOLAHAN DATA PASIEN PADA RUMAH SAKIT ISLAM KOTA METRO LAMPUNG. *MIKROTIK: Jurnal Manajemen Informatika*, *7*(1).

[4] Wikipedia. (2017, 19 Nopember). Malware. Diperoleh 19 Nopember 2017, dari https://en.wikipedia.org/wiki/Malware

[5]. HAVP. (2017, 14 Nopember). HAVP - HTTP ANTI VIRUS PROXY. Diperoleh 14 Nopember 2017, dari http://www.havp.org/

[6]. Support Apple. (2017, 7 Nopember). HAVP - macOS Sierra: Apa yang dimaksud dengan malware?. Diperoleh 7 Nopember 2017, dari https://support.apple.com/kb/PH25640?locale=id_ID&viewlocale=id_ID.

[7] Begini dampak dari serangan malware WannaCrypt. (2017, 3 Oktober). HAVP - Reporter Merdeka.com: Fauzan Jamaludin: Apa yang dimaksud dengan malware?. Diperoleh 3 Nopember 2017, dari https://www.merdeka.com/teknologi/begini-dampak-dari-serangan-malware-wannacrypt.html.