UNDETECTABLE BACKDOOR : THE ART OF MALICIOUS SOFTWARE AND SOCIAL ENGINEERING

Faizal Achmad
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
faizal.achmad@students.itb.ac.id

ABSTRAK
Malicious Software atau malware adalah perangkat lunak yang dirancang untuk menyusup ke sistem komputer tanpa adanya persetujuan pemilik komputer. Keberadaan antivirus dan firewall dipercaya untuk menjamin atau menjaga sistem komputer dari bahaya malware dengan melakukan pendeteksian secara dini. Akan tetapi adanya antivirus dan firewall yang terpasang belum menjamin sistem komputer aman dari ancaman bahaya malware, salah satu ancaman nyata malware saat ini adalah undetectable backdoor, yaitu salah satu jenis malware yang tidak dapat terdeteksi oleh antivirus dan firewall. Penulisan ini berusaha menjelaskan dan melakukan simulasi akan bahaya ancaman suatu undetectable backdoor terhadap data informasi yang tersimpan dalam komputer, dengan cara simulasi pembuatan, pengemasan dan penyebaran undetectable backdoor, serta simulasi pencurian data informasi.

Kata Kunci : *Undetectable Backdoor, Malicious Software, Social Engineering*

1. Pendahuluan

1.1 Latar Belakang Masalah

Malicious Software atau yang biasa disebut sebagai *Malware* merupakan salah satu ancaman terbesar pada era teknologi informasi saat ini, karena jenis *malware* yang selalu berkembang dan berevolusi, seiring dengan perkembangan teknologi antivirus yang merupakan pengamanan terhadap serangan *malware*.

Antivirus sebagai teknologi untuk menangkal *malware* tidaklah selalu menjamin bahwa suatu perangkat bisa terhindar atau terbebas dari ancaman *malware*, walaupun antivirus yang digunakan selalu diperbaharui (*update*).

Dalam penulisan ini penulis ingin menunjukkan berbahayanya suatu *malware* terhadap data dan informasi yang kita miliki. Penulis mencoba mengkombinasikan metode dan teknik pembuatan *malware* dengan *social engineering*, guna menghasilkan *undetectable backdoor* yang tidak terdeteksi antivirus dan firewall, untuk kemudian dikemas dan disebarluaskan secara mekanisme interaksi sosial, agar dapat diterima serta dijalankan oleh seorang calon korban tanpa menimbulkan adanya kecurigaan.

1.2 Tujuan Penulisan

Memberikan gambaran akan bahaya *malware*, terhadap keamanan informasi, melalui penjelasan dan simulasi metode serta teknik pada *malware* dan *social engineering* yang dapat digunakan dalam pembuatan, pengemasan dan penyebaran *undetectable backdoor*, yaitu *backdoor* yang tidak terdeteksi oleh antivirus dan *firewall*, serta memiliki tampilan yang tidak dicurigai sebagai *backdoor*.

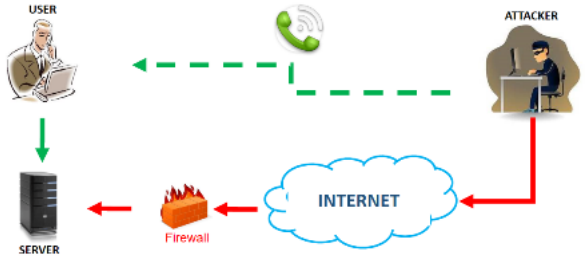
1.3 Perumusan Masalah

Dalam rangka pembuatan, pengemasan dan penyebaran *undetectable backdoor*, maka perlu dirumuskan suatu cara bagaimana metode pembuatan *malware* dan teknik *social engineering* dapat dikombinasikan, sehingga menghasilkan *undetectable backdoor* yang kemudian dikemas dan disebarluaskan secara mekanisme interaksi sosial, dan dapat diterima serta dijalankan oleh calon korban tanpa menimbulkan adanya kecurigaan.

2. Landasan Teori

2.1 Social Engineering[1]

Social Engineering adalah suatu teknik untuk memperoleh informasi dari seseorang dengan cara menggunakan pendekatan manusiawi melalui mekanisme interaksi sosial.

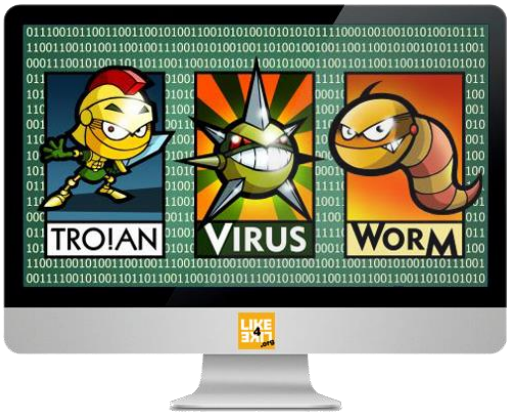


Gambar 1. Skema *Social Engineering*

2.2 *Malicious Software (Malware)*[2]

Malware merupakan kependekan dari *Malicious Software*, yaitu perangkat lunak yang dirancang untuk menyusup ke sistem komputer tanpa persetujuan pemilik atau program komputer yang di rancang untuk tujuan jahat.

Malware sendiri terdiri dari berbagai jenis seperti *virus*, *worm*, *trojan*, dan *backdoor*.



Gambar 2. Ilustrasi *Malware*

- ***Virus*[2]**
  Virus Komputer merupakan jenis *malware* yang menyerang file eksekusi (.exe), yang akan menyerang dan menggandakan diri ketika file exe yang terinfeksi di jalankan. *Malware* jenis ini menyebar melalui interaksi langsung pengguna yang tanpa sadar menjalankan atau memindahkan file yang terinsfeksi virus melalui CD, flashdisk, transfer jaringan atau internet.

- ***Worm*[2]**
  Worm (Cacing) komputer merupakan jenis *malware* yang menyerang dan menyebar melalui jaringan. Perbedaan antara *worm* dan *virus* adalah dari segi cara penyebaran dan penyerangan. Seperti dijelaskan sebelumnya *virus* komputer menyebar melalui interaksi pengguna, menyerang file dan aktif jika dijalankan oleh pengguna. Sedangkan *worm* menyerang jaringan komputer dengan memenuhi jaringan dengan paket-paket sampah yang membuat koneksi jaringan terhambat dan tidak seperti *virus*. *Worm* mampu menyebar kan diri sendiri melalui jaringan dengan memanfaatkan celah keamanan yang terdapat pada sistem komputer tanpa memerlukan interaksi dari pengguna dan akan terus menyebar membentuk sebuah jaringan komputer yang terserang *malware* yang dikenal sebagai Botnet.

- ***Trojan Horse*[2]**
  Trojan Horse atau *Trojan* merupakan perangkat lunak yang tampak berjalan sesuai fungsinya namun pada kenyataannya menfasilitasi akses yang tidak berhak ke komputer korban. Tujuan dari *Trojan* adalah memperoleh informasi dari Target (*password*, kebiasaan *user* yang tercatat dalam system log, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target).

- ***Backdoor*[2]**
  Backdoor merupakan metode yang di gunakan untuk melewati autentifikasi normal (login) dan berusaha tidak terdeteksi. *Backdoor* sendiri sering kali disusupkan melalui *trojan* dan *worm*.

2.3 *Phishing*[1]

Phishing adalah penipuan yang menggunakan *email* atau *website* untuk menipu pengguna agar mengungkapkan informasi seperti nomor kartu kredit, *email*, *password*, atau informasi sensitif lainnya.

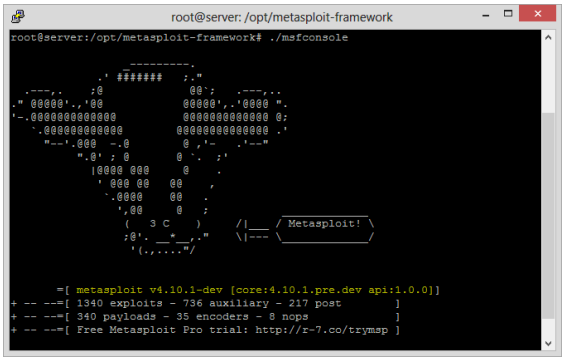
2.4 *Social Engineering Toolkit* (SET)[3]

SET dibuat oleh pendiri TrustedSec. SET merupakan tools *open-source* berbasis bahasa pemrograman Python yang bertujuan untuk melakukan *penetration testing* (pentest) yang berkaitan dengan *Social-engineering*. SET telah dipresentasikan pada konferensi berskala besar termasuk Blackhat, DerbyCon, Defcon, dan ShmooCon. Dengan lebih dari 2 juta jumlah unduhan, SET menjadi standar untuk *social-engineering pentest* dan sangat didukung oleh komuitas penggiat keamanan.

Gambar 3. Ilustrasi Produk SET

2.5 *Metasploit*[4]

Metaspoit adalah *tools pentest open-source* yang digunakan untuk mengembangkan dan mengeksekusi kode eksploit terhadap mesin *remote target*. *Metasploit* memiliki basis data terbesar eksploit yang teruji. Secara sederhana *Metasploit* dapat digunakan untuk menguji kerentanan dari sistem komputer dengan tujuan untuk melindunginya, tapi sisi lainnya *Metasploit* juga dapat digunakan untuk menembus ke dalam suatu sistem remote. Tampilan awal *Metasploit* terlihat pada gambar 4. dibawah ini.



Gambar 4. Tampilan Tools *Metasploit*

3. Metode Penelitian

Metode Penelitian yang dilakukan pada kegiatan penelitian ini adalah sebagai berikut :

- Melakukan studi literatur dan pengumpulan data dari berbagai sumber seperti buku dan internet mengenai metode dan teknik yang digunakan dalam membuat *backdoor* yang dapat melewati deteksi antivirus dan *firewall* atau yang biasa disebut *undetectable backdoor*.
- Melakukan simulasi metode dan teknik pembuatan *undetectable backdoor*.
- Melakukan simulasi penerapan konsep *social engineering* dalam mengemas dan menyebarkan *undetectable backdoor*, agar tidak mengundang kecurigaan dari target.
- Melakukan simulasi penggunaan hak akses yang didapat terhadap komputer korban yang menjalankan *backdoor*, seperti instalasi aplikasi sampai pengambilan file dari komputer korban.

4. Pembahasan

Pada bagian ini akan dilakukan simulasi kegiatan-kegiatan seperti yang telah disebutkan pada metode penelitian. Teknik-teknik yang digunakan pada simulasi ini dilakukan berdasarkan metode dan teknik terkini pada akhir bulan September 2014.

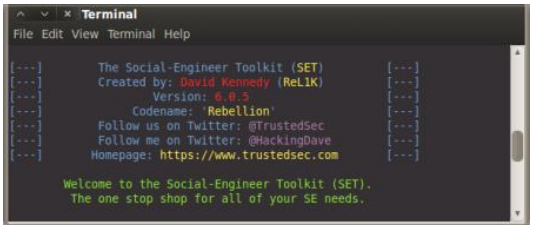
4.1 Pembuatan *Undetecable Backdoor*

Saat in banyak tools atau tutorial yang menawarkan dan memberi pengajaran bagaimana cara membuat suatu *backdoor*, namun tidak semua tools atau tutorial tersebut mampu menghasilkan suatu *undetectable backdoor*. Sebagai contoh *undetectable backdoor* yang pernah penulis buat pada tahun 2013, saat ini menggunakan Antivirus Avira 2014 sudah dapat terdeteksi. Sehingga diperlukan penelitian dan percobaan yang selalu *up-to-date* mengenai *undetectable backdoor*.

Tools yang penulis gunakan dalam membuat *undetectable backdoor* adalah *Social Engineering Toolkit* (SET) yang biasa digunakan sebagai salah satu tools dalam melakukan *penetration testing* (pentest).

- **SET**

  Pada penelitian ini penulis menjalankan tools SET versi 6.0.5 (Rebellion) pada sistem operasi Linux Backtrack 5 R3 seperti yang terlihat pada gambar5.

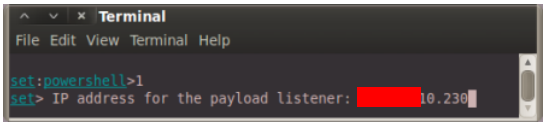


Gambar 5. Tampilan tools SET

SET menyediakan banyak pilihan menu tergantung tujuan yang dinginkan untuk melakukan pentest, tujuan penulis adalah membuat suatu *undetectable backdoor*, maka menu yang dipilih adalah *Social-Engineering Attacks*.

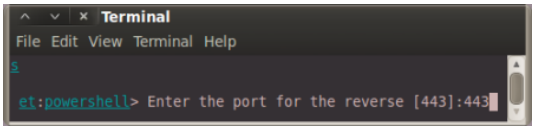
Gambar 6. Tampilan Menu SET

Untuk selanjutnya masih terdapat banyak pilihan menu lagi dan semuanya dapat dicoba untuk menghasilkan *undetectable backdoor*, proses pemilihan ini tidak penulis jelaskan dan langsung menuju setting IP Address dan Port yang akan dituju oleh *undetectable backdoor* sebagai server *listener*. Penulis menggunakan server yang berlokasi di Kanada dengan IP Address xxx.xxx.10.230 seperti yang terlihat pada gambar.7 dibawah ini.



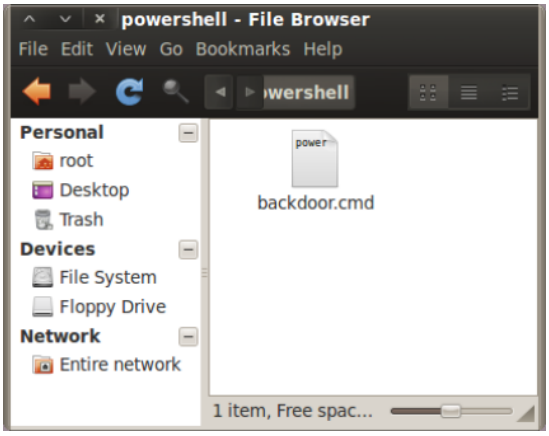
Gambar 7. Setting IP Server Listener

Untuk setting port penulis menggunakan port 443 yang umumnya biasa digunakan sebagai port *Hypertext Transfer Protocol Secure* (HTTPS) secara *default*, terlihat pada gambar.8 dibawah ini.



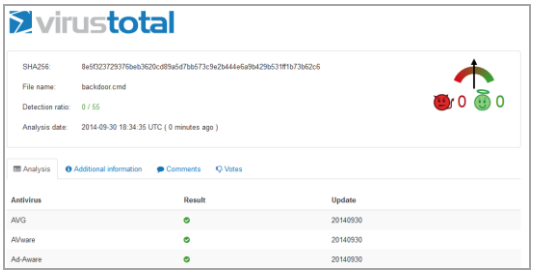
Gambar 8. Setting Port Server Listener

Backdoor yang dihasilkan akan tersimpan dalam folder "Powershell", kemudian penulis mengubah nama *backdoor* menjadi "backdoor.cmd", terlihat seperti pada gambar9. dibawah ini.



Gambar 9. Setting IP Server Listener

Selanjutnya adalah melakukan pengujian seberapa baik kemampuan antivirus dalam mendeteksi *undetectable backdoor* yang kita hasilkan.



Gambar 10. Hasil *Scanning* dari www.virustotal.com

Dari pemindaian situs www.virustotal.com (gambar 10) dengan update antivirus per 30 September 2014, didapatkan hasil **"0/55"** yang berarti bahwa dari 55 antivirus yang digunakan **tidak ada satupun yang mendeteksi** *undetectable backdoor* yang dihasilkan sebagai *malware* berbahaya.

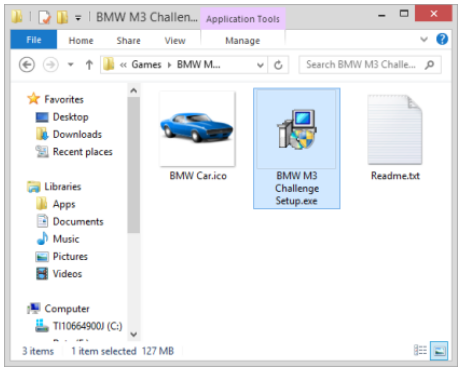
4.2 Pengemasan dan Penyebaran *Undetectable Backdoor*

Untuk mendapatkan korban, *undetectable backdoor* yang kita hasilkan tidak serta merta bisa langsung disebarkan (walaupun tidak terdeteksi sebagian besar antivirus), karena wujud file *undetectable backdoor* yang berupa "backdoor.cmd" pastinya tidak akan menarik perhatian orang untuk menjalankannya, bahkan malah akan menimbulkan kecurigaan sebagai virus. Disinilah perlunya konsep *social engineering* dalam melakukan pengemasan dan penyebaran *undetectable backdoor*, posisikan diri kita sebagai calon korban, apa yang dapat menarik perhatian korban sehingga *undetectable backdoor* dijalankan secara sengaja ataupun tidak sengaja.

- **Pengemasan *Undetecable Backdoor***
  Pada simulasi ini penulis akan melakukan pengemasan *undetectable backdoor* kedalam aplikasi game dan antivirus. Aplikasi game merupakan salah satu aplikasi komputer yang digemari dan dicari sebagai hiburan, sedangkan pengemasan ke dalam aplikasi antivirus juga tidak akan menimbulkan kecurigaan calon korban karena *undetectable backdoor* yang telah dibuat tidak akan terdeteksi sebagai *malware*. Berikut merupakan 2 (dua) contoh pengemasan *undetectable backdoor* yang penulis lakukan dengan menggunakan tools WinRar.
  - **Pengemasan ke dalam aplikasi Game**
    Sebelumnya carilah suatu file instalasi game yang banyak digemari dan dicari, dalam contoh penulis menggunakan game BMW M3 Challenge (gambar.11)

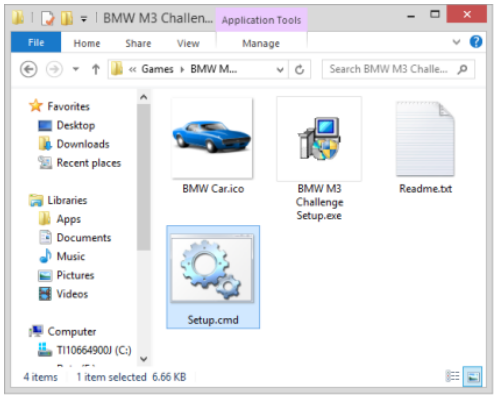
Gambar 11. Tampilan Game BMW M3 Challenge

Paket file instalasi untuk game BMW M3 Challenge awalnya hanya terdiri dari 3 file, seperti yang terlihat pada gambar.12 dibawah ini.



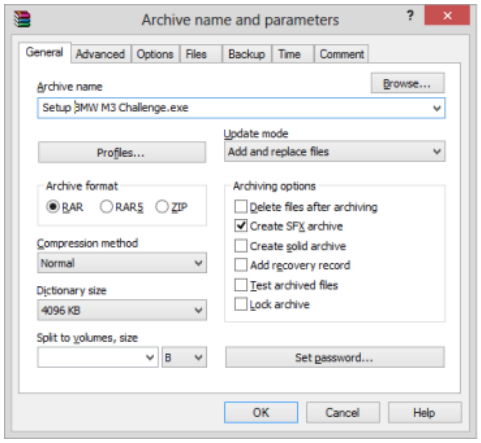
Gambar 12. File Instalasi Asli

Kemudian penulis menyisipkan file *undetectable backdoor* kedalam folder instalasi games setelah sebelumnya merubah nama "backdoor.cmd" menjadi "setup.cmd", sehingga kini dalam folder instalasi ada 4 (empat) file seperti yang terlihat pada gambar.13 dibawah ini.



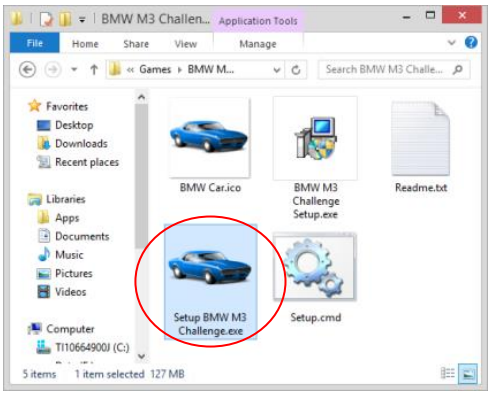
Gambar 13. Penambahan Backdoor Pada File Instalasi

Selanjutnya gunakan WinRar (gambar.14) untuk menjadikan keseluruhan file tersebut menjadi hanya satu file eksekusi (EXE) untuk instalasi,



Gambar 14. Winrar Archive

yaitu file "Setup BMW M3 Challenge.exe" yang nantinya akan disebarluaskan, dapat dilihat pada gambar.15 dibawah ini.



Gambar 15. Hasil Akhir File Setup

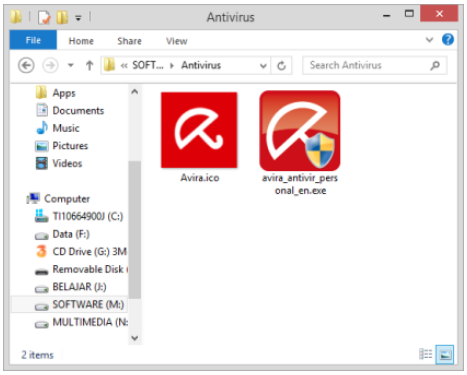
File instalasi ini nantinya saat dijalankan oleh korban akan mengeksekusi "Setup.cmd" yang merupakan *undetectable backdoor* terlebih dahulu baru kemudian "BMW M3 Challenge Setup.exe", hal ini tidak akan menimbulkan kecurigaan, karena terlihat seperti proses instalasi game pada umumnya.

– Pengemasan ke dalam aplikasi Antivirus

Sebelumnya carilah suatu file instalasi antivirus yang banyak diminati dan dicari, dalam contoh penulis menggunakan antivirus Avira (gambar.16)

Gambar 16. Logo Antivirus Avira

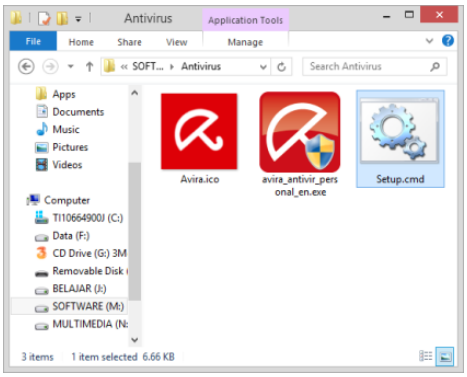
Paket file instalasi untuk antivirus Avira awalnya hanya terdiri dari 2 (dua) file, seperti yang terlihat pada gambar 17.



Gambar 17. File Instalasi Asli

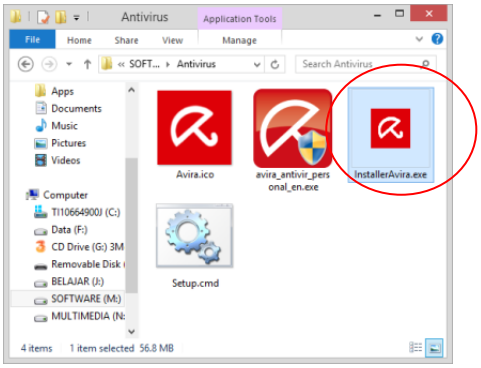
Kemudian penulis menyisipkan file *undetectable backdoor* kedalam folder instalasi antivirus setelah sebelumnya merubah nama "backdoor.cmd" menjadi

"setup.cmd", sehingga kini dalam folder instalasi ada 3 (tiga) file seperti yang terlihat pada gambar.18 dibawah ini.



Gambar 18. Penambahan Backdoor Pada File Instalasi

Proses selanjutnya menggunakan tools WinRar sama dengan yang dilakukan pada proses pengemasan pada aplikasi Game, hingga akhirnya didapatkan satu file eksekusi (EXE) untuk instalasi yaitu file "InstallerAvira.exe" yang sudah menggunakan tampilan icon Avira antivirus, terlihat pada gambar.19 dibawah ini.



Gambar 19. Hasil Akhir File Installer

Sebenarnya masih banyak lagi cara pengemasan *undetectable backdoor*, sesuai dengan analisa *social engineering* terhadap calon korban. Namun pada penulisan ini hanya diberikan contoh seperti yang sudah dijelaskan diatas.

- **Penyebaran *Undetectable Backdoor***
  Undetectable backdoor yang sudah dikemas dalam aplikasi games dan antivirus, dapat disebarluaskan untuk mencari korban, misalnya dengan menyebarkannya pada forum media sosial, blog atau website, *email phising* dan *file sharing.*

– **Forum media sosial**
  Suatu forum media sosial biasanya terdiri dari banyak pengguna yang berasal dari berbagai kalangan, hal ini bisa menjadikannya sasaran yang potensial dalam mendapatkan korban. Misalnya *undetectable backdoor* yang dikemas dalam aplikasi games, dapat diposting pada suatu forum games. Seperti contoh postingan penulis mengenai *share game* BMW M3 Challenge pada suatu forum games, seperti terlihat pada gambar.20 dibawah ini.

Gambar 20. Share Games Berisi Backdoor Pada Salah Satu Forum Game

– **Blog atau website**
  Blog maupun website dapat digunakan sebagai sarana penyebaran *undetectable backdoor* dengan menggunakan modus berbagi aplikasi games atau software secara gratis. Seperti contoh website pada gambar.21 dibawah ini.

Gambar 21. Blog Sharing Games & Software Yang Memuat Backdoor

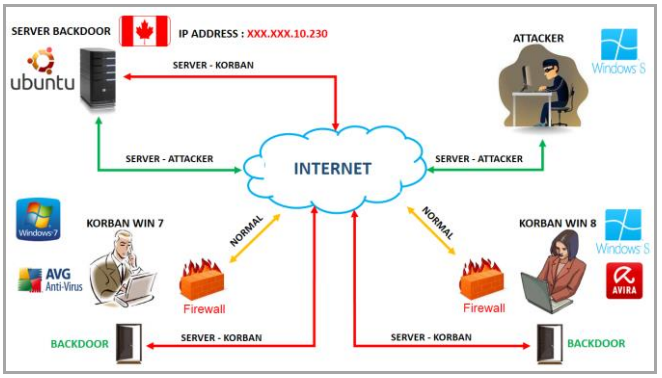
– **Email phishing**
Suatu email phishing akan berusaha meyakinkan korban bahwa email yang diterimanya adalah otentik dari pengirim yang resmi, biasanya email phising menggunakan alamat pengirim email seolah-olah berasal dari pengirim yang resmi dan dapat dipercaya. Misalnya penerima email akan diarahkan untuk menuju *forum*, *blog/website*, atau *file sharing* yang berisi *backdoor*.

– ***File sharing***
File sharing merupakan tempat para peselancar dunia maya berbagi berbagai file, seperti film, musik, game dan aplikasi. File sharing dapat menjadi salah satu sarana untuk menyebarkan *undetectable backdoor*. Seperti contoh, penulis mencoba *upload* kedua file *installer* tersebut ke salah satu situs *file sharing*, proses upload berhasil dengan sukses (gambar 22. dan gambar 23), padahal situs tersebut menggunakan antivirus untuk mengecek konten yang diupload.

Gambar 22. Upload Setup Games

Gambar 23. Upload Installer Games

4.3 Simulasi menggunakan hak akses komputer korban yang menjalankan *undetectable backdoor*



Gambar 24. Skema Skenario Simulasi

- **Skenario Simulasi**
Pada simulasi akan terdiri dari 4 (empat) pihak yang terlibat yaitu Server Backdoor, Attacker, User Windows 7 dan User Windows 8. Gambar.24 diatas menggambarkan skema hubungan antar semua pihak. Berikut merupakan informasi detail dari masing-masing pihak.

  – **Server Backdoor**
  Sistem Operasi : Ubuntu 12.0.4
  Lokasi Server : Kanada
  IP Address : xxx.xxx.10.230

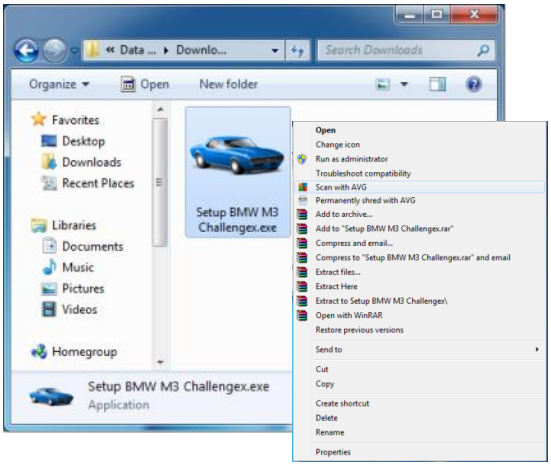
  – **Attacker**
  Sistem Operasi : Windows 8

  – **User Windows 7**
  Sistem Operasi : Windows 7 Pro
  Antivirus : AVG 2015
  Update : 27 September 2014
  Win 7 Firewall : ON

  – **User Windows 8**
  Sistem Operasi : Windows 8.1
  Antivirus : Avira 2014
  Update : 29 September 2014
  Win 8 Firewall : ON

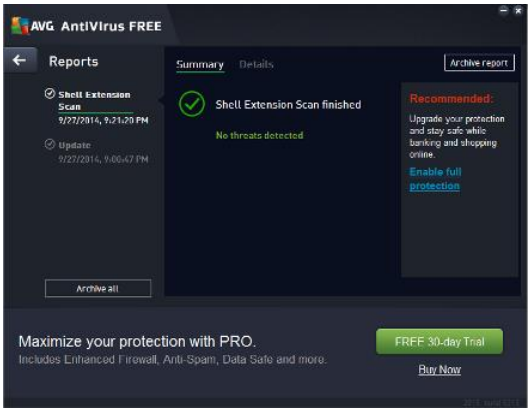
  Simulasi yang dilakukan terdiri dari 2 (dua) skenario yaitu **SKENARIO-1** dimana User Windows 7 akan menjadi korban dari *undetectable backdoor* yang dikemas dalam aplikasi games, dan **SKENARIO-2** dimana User Windows 8 akan menjadi korban dari *undetectable backdoor* yang dikemas dalam aplikasi antivirus.

- **SKENARIO-1**
  Misal User Windows 7 telah mendownload file "Setup BMW M3 Challenge.exe" dari forum games di internet, dan menyimpannya didalam folder "Downloads" pada komputer miliknya, seperti terlihat pada gambar 25 dibawah ini.



Gambar 25. File Setup Games Berisi Backdoor di Komputer Calon Korban

Untuk meyakinkan bahwa file tesebut aman, maka sebelum menjalankan file program "Setup BMW M3 Challenge.exe" User Windows 7 melakukan *scanning* dengan menggunakan antivirus AVG 2015 (Update 27 September 2014), dengan hasil *scanning* terlihat pada gambar.26 dibawah ini.



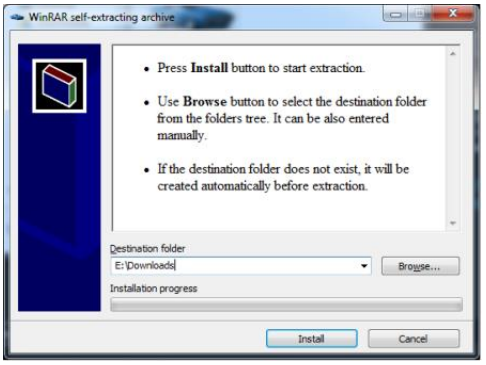
Gambar 26. Hasil Scan File Setup Games Berisi Backdoor

Hasil *scanning* menyatakan bahwa file *setup* game tersebut bebas dari *threat* (ancaman), padahal didalam file tersebut terdapat *backdoor* tetapi tidak terdeteksi oleh antivirus.

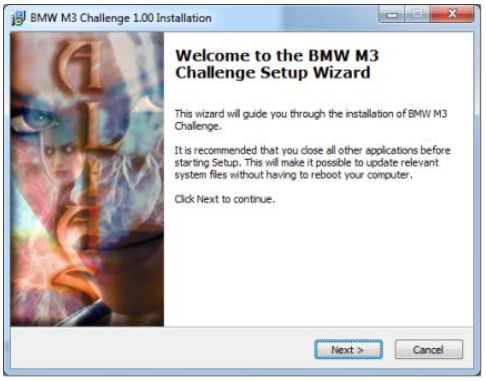
User Windows 7 juga memastikan Windows Firewall dalam kondisi "ON" seperti terlihat pada gambar 27 dibawah ini.

Gambar 27. Status "ON" Firewall Windows 7

Kemudian User Windows 7 mengeksekusi file *setup* game, tampilan setelah mengeksekusi file *setup* game adalah sama seperti proses instalasi game pada umumnya, seperti yang terlihat pada gambar.28 dan gambar 29. dibawah ini, tanpa disadari User Windows 7 mengaktifkan *backdoor* pada komputernya



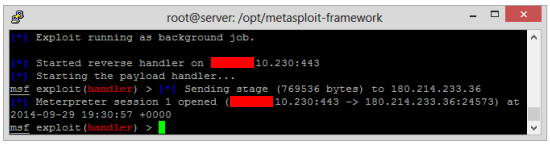
Gambar 28. Memilih Directory Extract



Gambar 29. Menu Awal Instalasi Games

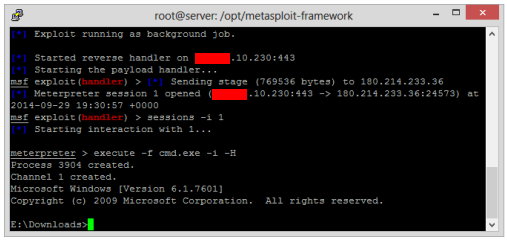
Sesaat sesudah User Windows 7 mengaktifkan *backdoor*, maka terciptalah saluran komunikasi

antara Server Backdoor dan komputer User Windows 7 dalam bentuk *sessions*, seperti tampilan pada gambar.30 dibawah ini.



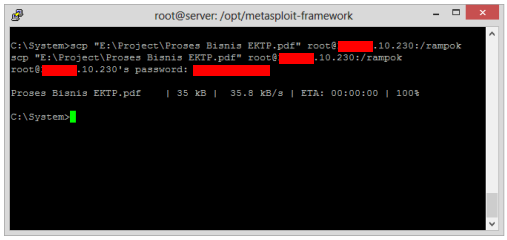
Gambar 30. Tampilan *Sessions* Pada Server Backdoor

Attacker mengendalikan komputer User Windows 7 melalui perantara Server Backdoor. Attacker berkomunikasi dengan Server Backdoor menggunakan protokol *Secure Shell* (SSH) di port 22. Terlihat bahwa attacker dapat mengakses *Command Prompt* dari User Windows 7, terlihat pada gambar.31 dibawah ini.



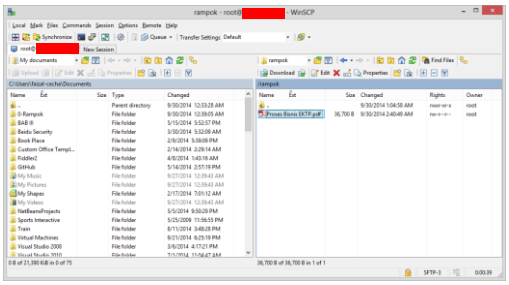
Gambar 31. Attacker Dapat Mengakses *Command Prompt* Komputer User Windows 7

Dengan dapat diaksesnya *Command Prompt* maka seorang attacker dapat mengatur banyak hal termasuk sistem pada computer tersebut. Pada simulasi gambar.32, Attacker dapat menyalin file "Proses Bisnis EKTP.pdf" dari komputer User Windows 7 menuju folder "rampok" pada Server Backdoor menggunakan *Secure Copy* (SCP), secara *default* sistem operasi Windows tidak memiliki fasilitas SCP, karena itu Attacker harus menginstallnya terlebih dahulu menggunakan akses *Command Prompt* yang dimiliki.



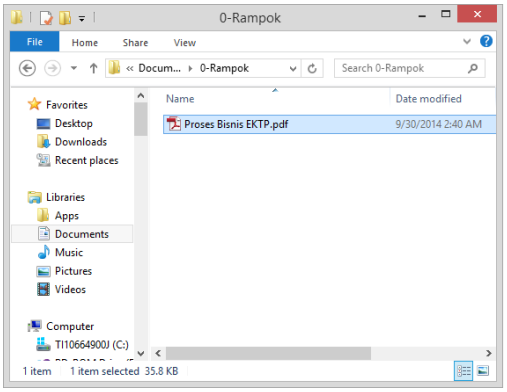
Gambar 32. Attacker Menyalin File Korban Ke Server Backdoor

Setelah proses penyalinan selesai, Attacker dapat memindahkan file tersebut dari Server Backdoor menuju komputernya menggunakan WinSCP (SCP GUI berbasis windows) terlihat pada gambar.33 dibawah ini.



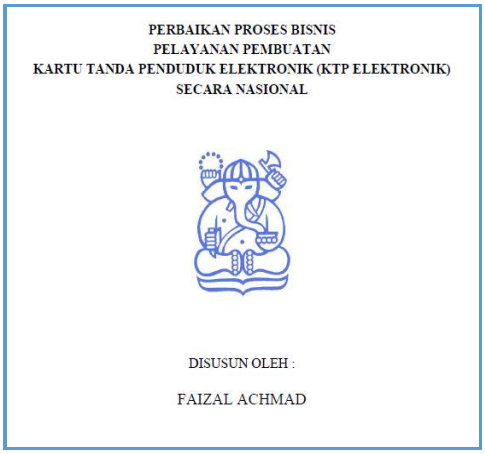
Gambar 33.Penyalinan File Korban Dari Server Backdoor Menuju Komputer Attacker

File "Proses Bisnis EKTP.pdf" dari User Windows 7 telah berada pada Komputer Attacker (gambar 34).



Gambar 34. File Milik User Windows 7 Berada Pada Komputer Attacker

Attacker kemudian membuka isi file "Proses Bisnis EKTP.pdf" milik User Windows 7 (gambar 35).


PERBAIKAN PROSES BISNIS
PELAYANAN PEMBUATAN
KARTU TANDA PENDUDUK ELEKTRONIK (KTP ELEKTRONIK)
SECARA NASIONAL

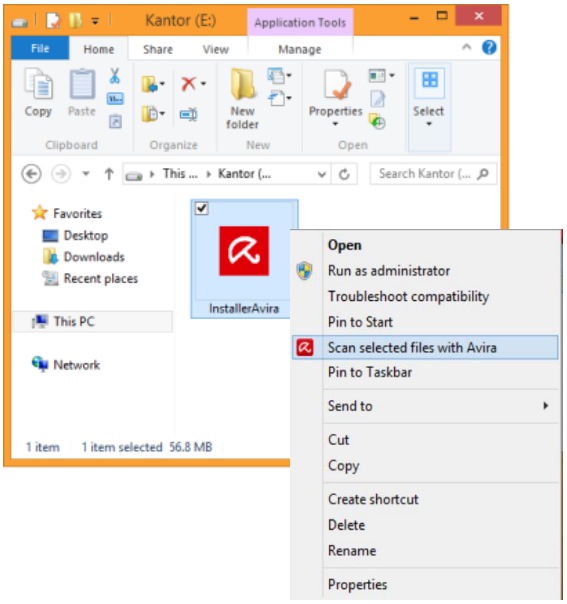
DISUSUN OLEH :

FAIZAL ACHMAD

Gambar 35. Tampilan Isi File "Proses Bisnis EKTP.pdf"

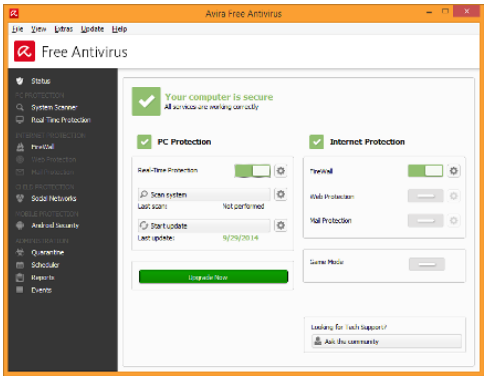
- **SKENARIO-2**

  Misal User Windows 8 telah mendownload file installer antivirus “Installer Avira.exe” dari sebuah website di internet, dan menyimpannya didalam folder “Downloads” komputer miliknya, seperti terlihat pada gambar.36 dibawah ini.

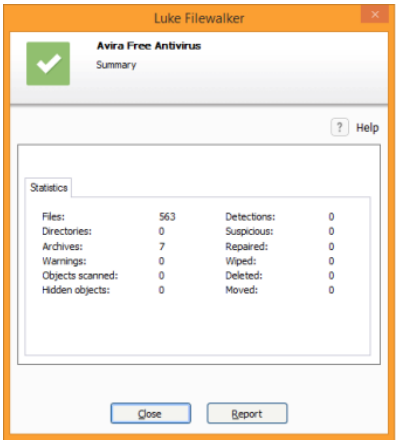


Gambar 36.File InstallerAntivirus Berisi Backdoor di Komputer Calon Korban

Untuk meyakinkan bahwa file tesebut aman, maka sebelum menjalankan file program “Installer Avira.exe” User Windows 8 melakukan *scanning* dengan menggunakan antivirus Avira 2014 (Update 29 September 2014) dengan hasil *scanning* terlihat pada gambar.37 dan gambar 38 dibawah ini.



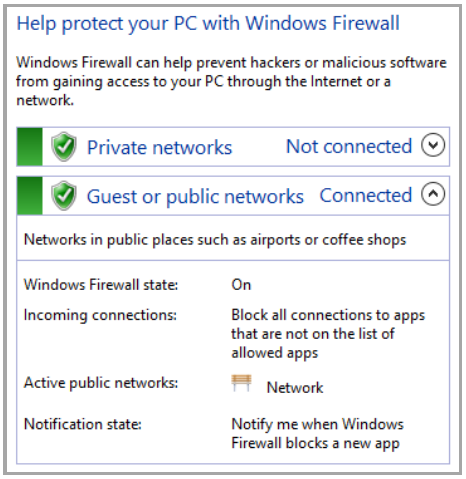
Gambar 37. Attribut Setting Antivirus Avira



Gambar 38. Hasil Scan File Installer Antivirus Berisi Backdoor

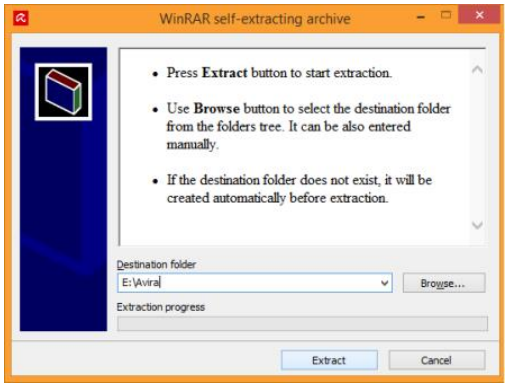
Hasil *scanning* menyatakan bahwa file *installer* antivirus tersebut bebas dari *threat* (ancaman), padahal didalam file tersebut terdapat *backdoor* tetapi tidak terdeteksi oleh antivirus.

User Windows 8 juga memastikan Windows Firewall dalam kondisi “ON” seperti terlihat pada gambar 39 dibawah ini.

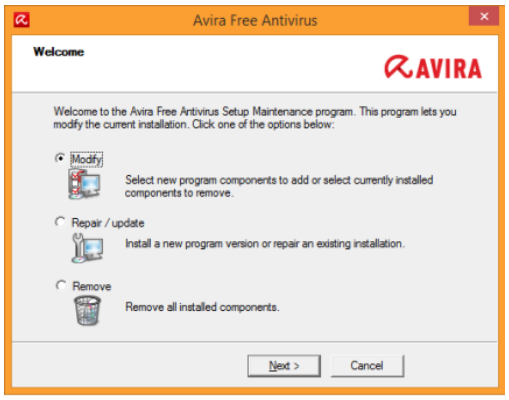


Gambar 39. Status “ON” Firewall Windows 8

User Windows 8 kemudian mengeksekusi file *installer* antivirus, tampilan setelah mengeksekusi file *installer* antivirus adalah sama seperti proses instalasi antivirus pada umumnya, seperti yang terlihat pada gambar.40 dan gambar 41. dibawah ini, tanpa disadari User Windows 8 mengaktifkan *backdoor* pada komputernya.

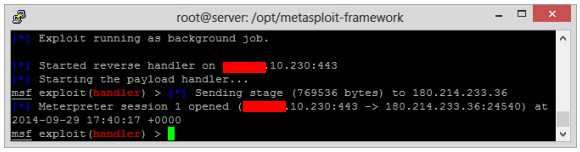


Gambar 40. Memilih Directory Extract



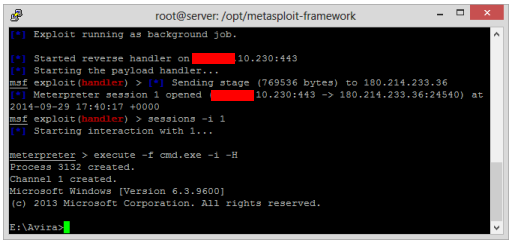
Gambar 41. Menu Awal Instalasi Antivirus

Sesaat sesudah User Windows 8 mengaktifkan *backdoor*, maka terciptalah saluran komunikasi antara Server Backdoor dan komputer User Windows 8, seperti tampilan pada gambar.42 dibawah ini.



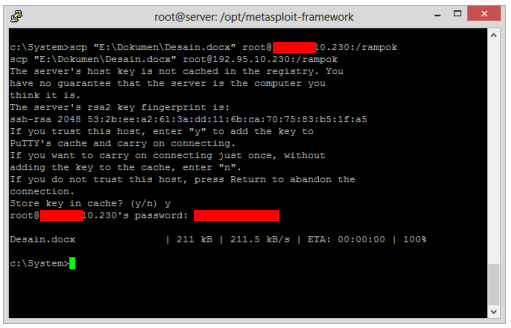
Gambar 42. Tampilan *Sessions* Pada Server Backdoor

Proses selanjutnya sama dengan yang dilakukan pada User Windows 7, yaitu Attacker mengendalikan komputer User Windows 8 melalui perantara Server Backdoor. Attacker berkomunikasi dengan Server Backdoor menggunakan protokol *Secure Shell* (SSH) di port 22. Terlihat bahwa attacker dapat mengakses *Command Prompt* dari User Windows 8, terlihat pada gambar 43.



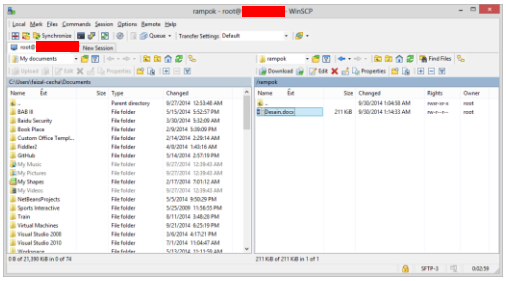
Gambar 43. Attacker Dapat Mengakses *Command Prompt* Komputer User Windows 8

Dengan dapat diaksesnya *Command Prompt* maka seorang attacker dapat mengatur banyak hal termasuk sistem pada komputer tersebut. Pada simulasi gambar.44, Attacker dapat menyalin file "Desain.docx" dari komputer User Windows 8 menuju folder "rampok" pada Server Backdoor menggunakan *Secure Copy* (SCP), secara *default* sistem operasi Windows tidak memiliki fasilitas SCP, karena itu Attacker harus menginstallnya terlebih dahulu menggunakan akses *Command Prompt* yang dimiliki.



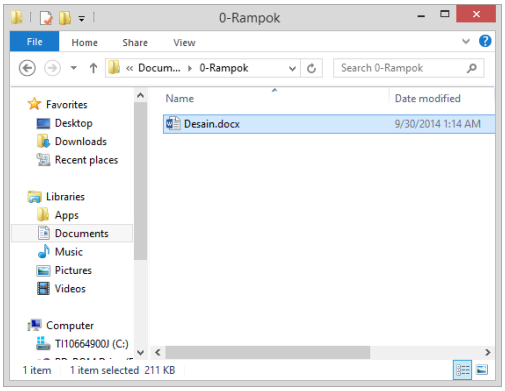
Gambar 44. Attacker Menyalin File Korban Ke Server Backdoor

Setelah proses penyalinan selesai, Attacker dapat memindahkan file tersebut dari Server Backdoor menuju komputernya (gambar 45) menggunakan WinSCP (SCP GUI berbasis windows).



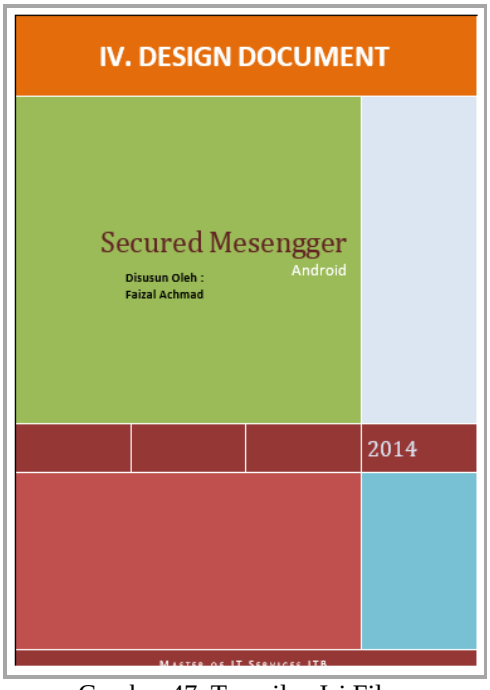
Gambar 45. Penyalinan File Korban Dari Server Backdoor Menuju Komputer Attacker

File "Desain.docx" dari User Windows 8 telah berada pada Komputer Attacker (gambar 46).



Gambar 46. File Milik User Windows 7 Berada Pada Komputer Attacker

Attacker kemudian membuka isi file "Desain.docx" milik User Windows 8 (gambar 47).



Gambar 47. Tampilan Isi File "Desain.docx"

- **Skenario Lebih Lanjut**
  Sebenarnya setelah mendapatkan *Command Prompt* dari komputer User Windows 7 dan User Windows 8, seorang Attacker dapat membuat skenario lebih lanjut sepert membuat akun *User* baru pada komputer tersebut atau menanamkan suatu *persistent backdoor* yang dapat diakses pada lain waktu, hal ini biasa disebut sebagai tahap *maintaining access* pada proses *penetration testing*. Pada penulisan ini, penulis tidak memberikasn simulasi bagaimana tahap *maintaining access* ini dilakukan.

5. Kesimpulan

Hasil kesimpulan dari penulisan ini adalah :

- *Social Engineering* adalah suatu teknik untuk memperoleh informasi dari seseorang dengan cara menggunakan pendekatan manusiawi melalui mekanisme interaksi sosial.
- *Malicious Software* adalah perangkat lunak yang dirancang untuk menyusup ke sistem komputer tanpa persetujuan pemilik atau program komputer yang di rancang untuk tujuan jahat.
- *Backdoor* merupakan salah satu jenis *malware* yang di gunakan untuk melewati autentifikasi normal (login) dan berusaha tidak terdeteksi. *Backdoor* sendiri sering kali disusupkan melalui *trojan* dan *worm*.
- Berdasarkan *scanning* dari situs www.virustotal.com, bahwa dari 55 virus yang tersedia tidak ada satupun yang mengenali *undetectable backdoor* yang penulis buat sebagai *malware* berbahaya.
- Simulasi pengemasan *backdoor* dilakukan dengan menyisipkannya pada file instalasi games dan antivirus.
- Penyebaran file instalasi games dan antivirus yang telah disisipi backdoor dapat dilakukan melalui forum media sosial, *email phising*, blog/website dan situs *file sharing*.

Referensi

1. Faizal Achmad. *Ancaman Keamanan Sistem Informasi E-KTP*. Bimbingan Teknis Keamanan Informasi E-KTP bagi Administrator Database Kabupaten/Kota Tahun 2012.
2. Kudri. *Pengaruh Malware Terhadap kinerja jaringan Komputer Sebuah Kantor (Study Kasus Kantor Bupati Abdya)*. STMIK U'Budiyah Indonesia. 2013.
3. https://www.trustedsec.com/downloads/social-engineer-toolkit/, diakses 30 September 2014.
4. http://www.hackyshacky.com/2013/03/What-is-Metasploit.html, diakses 30 September 2014.