KEAMANAN JARINGAN KOMPUTER

"Remote Access Trojan"

OLEH:

Doni Saputra (09011181520120)

Dosen Pengampuh : DERIS STIAWAN, M.T., PH.D.

Sistem Komputer

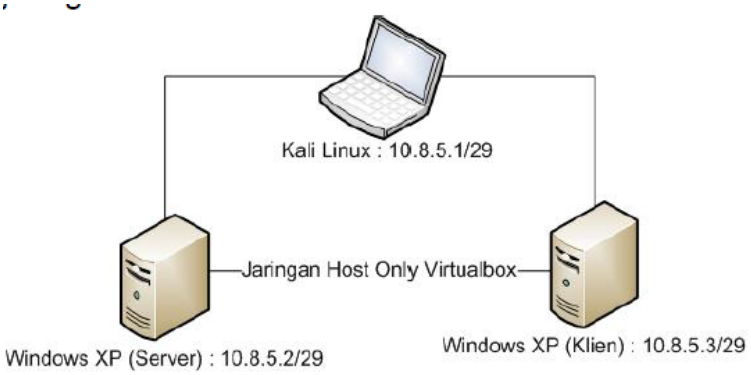
Fakultas Ilmu Komputer

Universitas Sriwijaya

2019

Malicous Software atau yang lebih dikenal sebagai *Malware* merupakan perangkat lunak yang secara eksplisit didesain untuk melakukan aktifitas berbahaya atau perusak perangkat lunak lainnya seperti *Trojan*, *Virus*, *Spyware* dan *Exploit* (Kramer & Bradfield, 2010).

Salah satu media yang digunakan oleh *intruder* untuk mengendalikan komputer pengguna secara diam-diam dari jarak jauh adalah *malware poison ivy*, dikenal sebagai "*trojan access remote*" karena dapat memberikan kontrol penuh kepada *intruder* melalui pintu belakang (*backdoor)*.



Gambar 1. Topologi Arsitektur Jaringan Virtual Lab

Cara kerja program *poison ivy* dapat dianalisis menggunakan dua metode analisis *malware* yaitu

1. metode analisis *malware* dinamis yang dapat memberikan solusi dalam menganalisis program *malware* yang terkendala pada bagian-bagian kode *signature* bersifat polimorfik maupun yang terenkripsi terkait pencarian perilaku dari program *malware*.
   a) Regshot
      - Penambahan registry : hklm\software\microsoft\windows\currentversion\run\secret_agent
      - Penambahan file prefetch : c:\windows\prefetch\piagent.exe-0aebfbee.pf

   b) Cuckoo Sandbox

Files
- C:\DOCUME~1\MALWAR~1\LOCALS~1\Temp\piagent.exe
- C:\WINDOWS\system32:pidriver.exe

Mutexes
-)!VoqA.I4

Registry Keys
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Perilaku yang dilakukan oleh program *malware poison ivy* terhadap mesin *cuckoo sandbox* diantaranya yaitu, membuat 2 *file* baru dengan nama "piagent.exe" dan sebuah *file* dengan nama "pidriver.exe". Adapula perilaku lainnya program *malware poison ivy* mencoba menandai dirinya ketika aktif dalam memori dengan membuat *mutex* (*Mutual Exclusion*) bernama "**)!VoqA.I4**". Dan perilaku yang lain dari program *malware poison ivy* yaitu melakukan penambahan *value key* pada "*startup*" dengan tujuan agar program dapat aktif pada saat komputer pertama kali melakukan *booting*.

c) Wireshark

- Alamat ip program induk (*controller*) :192.168.56.20
- Nomor port untuk jalur komunikasi :3460
- Protokol yang digunakan dalam pengiriman paketdata: tcp (transmission control protocol)

2. Metode yang kedua adalah metode analisis *malware* statis dimana metode ini memungkinkan temuan informasi program *malware* melalui kode-kode *hexa* dan *string* ataupun *binary* yang terkandung didalamnya yang tidak dapat ditemukan jika dilakukan dengan metode analisis *malware* dinamis.

- Ditemukan pendefinisian kode *string* "*secret_agent*" pada *offset* 004016D3 sampai *offset* 004016DE.

Gambar 21. Temuan Kode *String* "secret_agent" pada *IDA Pro*

Keterangan konversi dari gambar 21. :

- 5F (Hexa) = 95 (Decimal) = _ (ASCII)

- 61 (Hexa) = 97 (Decimal) = a (ASCII)
- 63 (Hexa) = 99 (Decimal) = c (ASCII)
- 65 (Hexa) = 101 (Decimal) = e (ASCII)
- 67 (Hexa) = 103 (Decimal) = g (ASCII)
- 6E (Hexa) = 110 (Decimal) = n (ASCII)
- 72 (Hexa) = 114 (Decimal) = r (ASCII)
- 73 (Hexa) = 115 (Decimal) = s (ASCII)
- 74 (Hexa) = 116 (Decimal) = t (ASCII)

Hasil Hexa : 73 65 63 72 65 74 5F 61 67 65 6E 74

Hasil Decimal : 115 101 99 114 101 116 95 97 103 101 110 116

Hasil ASCII : secret_agent

Tabel 1. Hasil Temuan dari Pengujian dan Analisis Dinamis Program *Malware Poison Ivy*

No	Temuan	Analisis Dinamis		
		Regshot	Cuckoo Sandbox	Wireshark
1.	Penambahanregistry : hklm\software\microsoft\windows\currentversion\run\secret_agent	√	√	–
2.	Penambahan file prefetch : c:\windows\prefetch\piagent.exe-0aebfbee.pf	√	–	–
3.	Penambahan file baru : c:\docume~1\user\locals~1\temp\piagent.exe	–	√	–
4.	Penambahan filebaru : c:\windows\system32:pidriver.exe	–	√	–
5.	Alamat ip program induk (*controller*) :192.168.56.20	–	–	√
6.	Nomor port untukjalur komunikasi :3460	–	–	√
7.	Protokol yangdigunakan dalampengiriman paketdata :tcp (transmission control protocol)	–	–	√
8.	Kode string mutualexclusion(pembuatan mutex) :)Ivoqa.i4	–	√	–
9.	Kode string(nama identitas/ id) :pi_agent	–	–	–
10.	Kode stringpassword autentikasi :admin	–	–	–

Tabel 2. Hasil Temuan dari Pengujian dan Analisis Statis Program *Malware Poison Ivy*

No	Temuan	Analisis Statis	
		Strings	IDA Pro
1.	Penambahan registry : hklm\software\microsoft\windows\currentversion\run\secret_agent	√	√
2.	Penambahan file prefetch : c:\windows\prefetch\piagent.exe-0aebfbee.pf	–	–
3.	Penambahan file baru : c:\docume~1\user\locals~1\temp\piagent.exe	–	–
4.	Penambahan filebaru : c:\windows\system32:pidriver.exe	√	–
5.	Alamat ip program induk (*controller*) :192.168.56.20	√	√
6.	Nomor port untukjalur komunikasi :3460	–	–
7.	protokol yangdigunakan dalampengiriman paketdata :tcp (transmission control protocol)	–	–
8.	Kode string mutualexclusion(pembuatan mutex) :)!voqa.i4	√	–
9.	Kode string(nama identitas/ id) :pi_agent	√	√
10.	Kode string password autentikasi :admin	√	√

Teknik Antisipasi Trojan

1. Mengaktifkan Firewall.
2. Install Antivirus.
3. Disable Remote Access.
4. Website Scan :
    - ScanKomputer (http://security.symantec.com/sscv6/home.asp).
    - Scan File (http://www.virustotal.com).
    - Malware Analysis Otomatis (http://anubis.iseclab.org).
    -

DAFTAR PUSTAKA

[1] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, “Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis,” pp. 19–30.

[2] M. F. Agung, “Analisis Teknik Identifikasi dan Antisipasi Trojan di ID-SIRTII,” pp. 1–4.