3TI

Sécurité des réseaux informatiques

2015-2016

Les Malwares

V.Van den Schrieck

Types de malware

Exercice : Par groupe de 2-3, choisissez 5 types de malware dans la liste distribuée, puis proposez une définition pour chacun

Table des matières

- **Types de propagation : Virus, worms, spam/trojans**
- Types d'action : Corruption, agent d'attaque, vol d'information, stealthing
- Contre-mesures

Caractéristiques d'un virus

- Vecteur d'infection
- Evénement déclencheur
- Action

Cycle de vie d'un virus

- Phase de dormance
- Phase de propagation
- Phase de déclenchement
- Phase d'action

Virus

```
program V
1234567;

procedure attach-to-program;
begin
   repeat
        file := get-random-program;
   until first-program-line ≠ 1234567;
   prepend V to file;
end;

procedure execute-payload;
begin
   (* perform payload actions *)
end;

procedure trigger-condition;
begin
   (* return true if trigger condition is true *)
end;

begin (* main action block *)
   attach-to-program;
   if trigger-condition then execute-payload;
   goto main;
end;
```

(a) A simple virus

```
program CV
1234567;

procedure attach-to-program;
begin
   repeat
        file := get-random-program;
   until first-program-line ≠ 1234567;
   compress file;    (* t1 *)
   prepend CV to file;   (* t2 *)
end;

begin (* main action block *)
   attach-to-program;
   uncompress rest of this file into tempfile;   (* t3 *)
   execute tempfile;   (* t4 *)
end;
```

(b) A compression virus

Figure 6.1 Example Virus Logic

Virus compressé

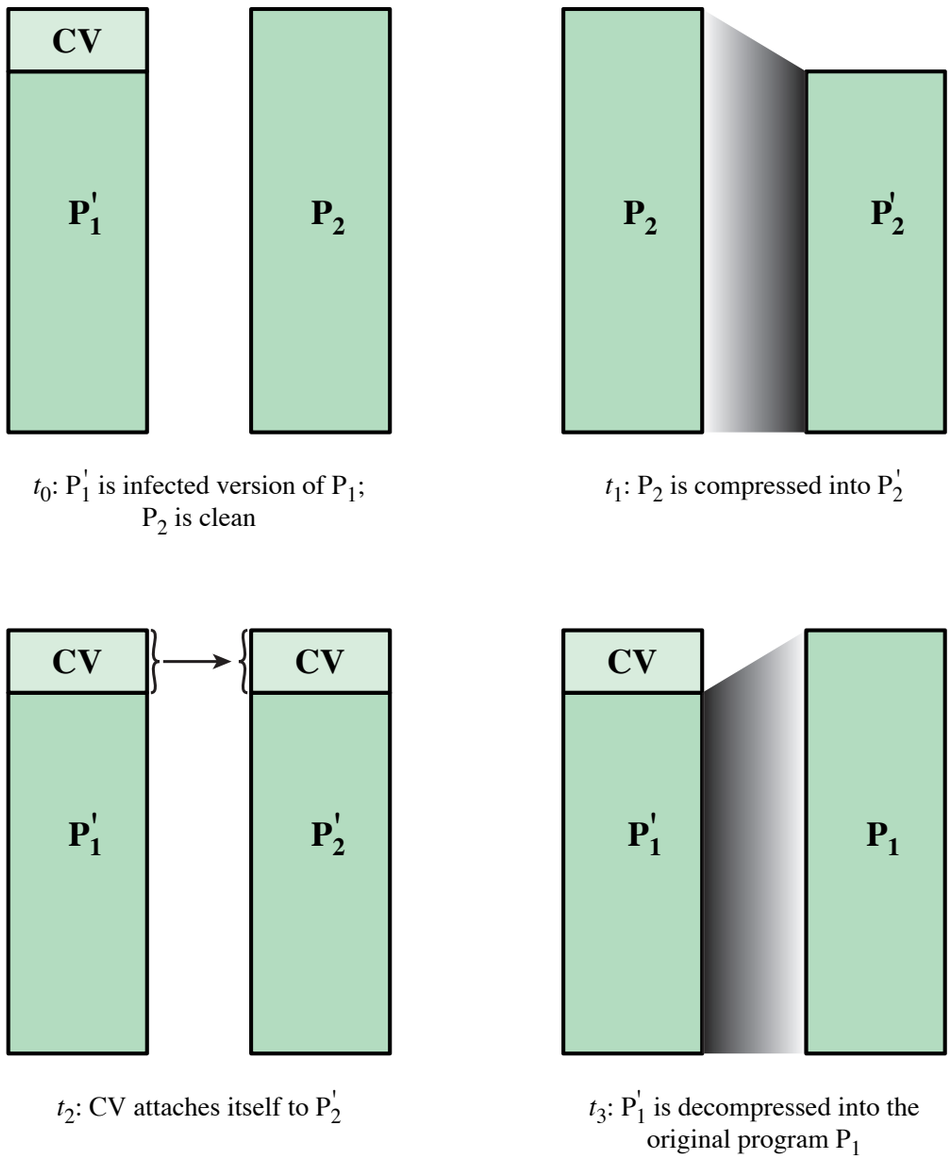

Figure 6.2 A Compression Virus

Exercice

Par groupe de 3, cherchez un exemple de virus et décrivez-le

(historique, mode d'action, effets,…)

Vers

- Qu'est ce qu'un ver? Différence par rapport à un virus?
- Comment un ver se propage-t-il?
- Comment un ver découvre-t-il de nouvelles cibles?

Exercice

Par groupe de 3, cherchez un exemple de ver et décrivez-le

(historique, mode d'action, effets,…)

Spam et chevaux de Troie

- Quels sont les risques liés au spam? Comment contrer le spam?
- Qu'est ce qu'un cheval de Troie? Comment éviter l'infection?
- Donnez un exemple d'un cheval de Troie et expliquez son fonctionnement

Table des matières

- Types de propagation : Virus, worms, spam/ trojans
- **Types d'action : Corruption, agent d'attaque, vol d'information, stealthing**
- Contre-mesures

Corruption du système

- En quoi un malware peut-il corrompre le système?

Agent d'attaque

- Une machine attaquée peut à son tour servir de base à une autre attaque => Bot
- A quoi un botnet peut-il servir?

Vol d'informations

- Comment un malware peut-il accéder à de l'information sensible, et la transmettre à l'attaquant?
- Quelles données seront visées?

Stealthing

- But : Garder un accès privilégié à la machine et se dissimuler
- Backdoor, Rootkits

Table des matières

- Types de propagation :Virus, worms, spam/ trojans
- Types d'action : Corruption, agent d'attaque, vol d'information, stealthing
- **Contre-mesures**

Contre-mesures

- Que faire contre les malwares?