Securitatea sistemelor de calcul

Viruși. Rootkit-uri

Marius Minea

19 octombrie 2011

Viruși și alte "animale"

Def: *Malicious logic* (logică malefică/malignă) este un set de instructiuni care au ca efect violarea politicii de securitate (a unui site).

Def: Un *cal troian* este un program cu un efect cunoscut (documentat, *overt*) și un efect ascuns (*covert*).
– putem avea versiuni cu și fără replicare
Exemplu: troianul din `login` în primele versiuni de UNIX [Thompson]

Viruși

Def: Un virus e un program care *se inserează* într-unul sau mai multe fișiere și (eventual) execută ulterior o acțiune. [Bishop]

Proprietate cheie: abilitatea de *replicare*

De regulă, acțiunea executată după replicare e malignă, dar există viruși care efectuează doar replicare, și nimic altceva

Categorii de viruși

După *localizare în fișiere*:
– viruși de sector de încărcare (boot)
– viruși (pentru) executabili
– viruși multi-părți
cu o parte pentru bootsector, și alta pentru executabile
– viruși pentru neexecutabile
viruși *macro* în documente (sau alte fișiere script), PDF, etc.
viruși ascunși în alte fișiere (de date) folosite de aplicații (e.g. exploateaza vulnerabilități tip buffer overflow)

Execuția virușilor

Viruși *nerezidenți*
se activează la rularea (explicită) a unui program infectat

Viruși *rezidenți*
atașați unor rutine ale sistemului de operare
ex. programe TSR (terminate but stay resident)

Conceptual, un virus are:
– un modul de replicare
– un modul prin care găsește fișiere-țintă pentru infecție
    căutare activă de fișiere executabile pe disc
    infectare doar a fișierelor care sunt accesate/executate de utilizator
    infectare selectivă, după anumite criterii (e.g. doar la copiere)

Fast infectors / slow infectors : după factorul de multiplicare la propagare

Cum se ascunde un virus

stealth virus: încearcă să își ascundă prezența pe sistem

Un virus crește de regulă dimensiunea fișierului-gazdă

dar se poate instala în blocuri neutilizate pe disc (incl. fragmente)

sau (mai rar) inlocui porțiuni rar folosite ale programului

Pot modifica funcții de bibliotecă sau apeluri sistem

și raporta informații modificate (ex. dimensiunea originală, etc.)

Se pot dezactiva din fișierul curent la execuție, infestând altele în loc

Detecție și mecanisme de ascundere

Virușii sunt detectați prin *semnătură* (porțiune cunoscută din cod)

și virușii se autodetectează, pt. a evita infecția multiplă

evită detecția prin ascunderea / modificarea semnăturii

Viruși criptați modul mic de decriptare + cod propriu-zis, criptat

criptare cu chei diferite $\Rightarrow$ nu poate fi detectat un tipar

(modulul de criptare e totuși comun)

prin criptare, se îngreunează analiza codului (după tipare suspecte)

Viruși polimorfi și metamorfi

Viruși polimorfi: modifică (parțial) modulul de criptare păstrând algoritmul
(pt. fiecare fișier infectat, codul e identic după decriptare)
$\Rightarrow$ aspect diferit de la o infecție la alta, dificil de detectat tipare

Viruși metamorfici:
mai complicat: rescriu și codul efectiv al virusului la fiecare rulare
(nu doar codul modulului de decriptare)

Cum: prin inserare de instrucțiuni care păstrează funcționalitatea
(înrudit cu tehnica de obfuscare de cod)
inserare de instrucțiuni irelevante, echivalente, modificare de graf de flux de control

Viruși vs. antiviruși

Q: Poate fi detectat orice virus ?
A: E nedecidabil dacă un anumit program conține un virus/logică malignă

O problemă de inginerie / reinginerie pt. a face codul cât mai dificil de înțeles

Alte “animale sălbatice”

– computer worms
  un program care se propagă de la un calculator la altul
  infectează un *sistem*, nu un *program*
– bacterii / “rabbits”
  programe care efectuează un atac de privare de resurse
  nu neapărat complet
– “logic bombs”
  programe care se activează la un anumit eveniment extern

Mecanisme de protecție antivirus

Separarea dintre date și executabil
– sisteme de fișiere care au două atribute distincte
– executabilele nu pot fi modificate / devin “date” dacă da
– un procedeu special de certificare a executabilelor

Reducerea drepturilor
– pentru a nu permite modificarea de către troieni
– implementare: bază de date pentru programe specifice
și restrângere a accesului la lista de argumente

Rootkit

un program / sistem de programe care preia neautorizat controlul asupra unui sistem (asigură accesul la sistem pentru un utilizator neautorizat)
Nivele de rootkits:

– la nivel de aplicație
(înlocuiește un set de programe, incl. care ar putea să-l detecteze)

Rootkit

un program / sistem de programe care preia neautorizat controlul asupra unui sistem (asigură accesul la sistem pentru un utilizator neautorizat)
Nivele de rootkits:

– la nivel de aplicație
    (înlocuiește un set de programe, incl. care ar putea să-l detecteze)
– la nivel de bibliotecă
    interceptează apeluri de funcții de bibliotecă

Rootkit

un program / sistem de programe care preia neautorizat controlul asupra unui sistem (asigură accesul la sistem pentru un utilizator neautorizat)
Nivele de rootkits:

– la nivel de aplicație
    (înlocuiește un set de programe, incl. care ar putea să-l detecteze)
– la nivel de bibliotecă
    interceptează apeluri de funcții de bibliotecă
– la nivel de sistem
    interceptează apeluri sistem

Rootkit

un program / sistem de programe care preia neautorizat controlul asupra unui sistem (asigură accesul la sistem pentru un utilizator neautorizat)
Nivele de rootkits:

– la nivel de aplicație
    (înlocuiește un set de programe, incl. care ar putea să-l detecteze)
– la nivel de bibliotecă
    interceptează apeluri de funcții de bibliotecă
– la nivel de sistem
    interceptează apeluri sistem
– la nivel de nucleu
    în module de nucleu încărcate (loadable kernel modules)

Rootkit

un program / sistem de programe care preia neautorizat controlul asupra unui sistem (asigură accesul la sistem pentru un utilizator neautorizat)
Nivele de rootkits:

– la nivel de aplicație
    (înlocuiește un set de programe, incl. care ar putea să-l detecteze)
– la nivel de bibliotecă
    interceptează apeluri de funcții de bibliotecă
– la nivel de sistem
    interceptează apeluri sistem
– la nivel de nucleu
    în module de nucleu încărcate (loadable kernel modules)
– virtualizate /la nivel de hypervisor (boot)
    încarcă sistemul de operare ca mașină virtuală

Rootkit

un program / sistem de programe care preia neautorizat controlul asupra unui sistem (asigură accesul la sistem pentru un utilizator neautorizat)
Nivele de rootkits:

– la nivel de aplicație
    (înlocuiește un set de programe, incl. care ar putea să-l detecteze)
– la nivel de bibliotecă
    interceptează apeluri de funcții de bibliotecă
– la nivel de sistem
    interceptează apeluri sistem
– la nivel de nucleu
    în module de nucleu încărcate (loadable kernel modules)
– virtualizate /la nivel de hypervisor (boot)
    încarcă sistemul de operare ca mașină virtuală
– la nivel de firmware / microcod programabil