

Courbois Software

AntivirusSoftware

Antivirussoftware zijn computerprogramma's die proberen om computervirussen en andere kwaadaardige software (malware) te identificeren, tegen te houden en te verwijderen.

Antivirussoftware gebruikt daarvoor typisch twee verschillende technieken:

1. Onderzoeken (scannen) van bestanden om te zoeken naar virussen die overeenkomen met de definities uit een lijst van bekende virussen
2. Identificeren van verdacht gedrag door eender welk computerprogramma, wat op een besmetting kan wijzen

De meeste commerciële antivirussoftware gebruikt beide technieken, met de nadruk op de eerste aanpak.

Methodes voor virusdetectie

Viruslijst

In de aanpak met viruslijsten, inspecteert de software een bestand en gebruikt daarbij een lijst van bekende virussen die door de makers van de software zijn geïdentificeerd. Wanneer een stuk code in het bestand overeenkomt met een virus uit de lijst, kan de software één van de volgende acties ondernemen (in volgorde waarin de actie verkozen wordt):

1. proberen het bestand te repareren door het virus zelf uit het bestand te verwijderen
2. het bestand in quarantaine plaatsen (zodat het bestand niet meer toegankelijk is voor andere programma's, en het virus zich niet langer kan verspreiden)
3. het geïnfekteerde bestand verwijderen

Opdat deze aanpak op middellange en lange termijn succesvol zou blijven, moeten de virusdefinities regelmatig bijgewerkt worden (meestal online). Wanneer nieuwe virussen "in het wild" geïdentificeerd worden, kunnen gebruikers en technici hun geïnfekteerde bestanden opsturen naar de auteurs van de antivirussoftware, zodat de informatie kan verwerkt worden in toekomstige virusdefinities.

De aanpak met virusdatabases onderzoekt typisch de bestanden wanneer het besturingssysteem deze aanmaakt, opent, sluit of verzendt via e-mail. Op deze manier kan een virus onmiddellijk bij ontvangst herkend worden. Een systeembeheerder kan er ook voor zorgen dat de software op een regelmatig tijdstip alle bestanden op de harde schijf van de gebruiker scant.

Hoewel deze aanpak op een efficiënte manier de uitbraak van een virus kan tegenhouden in de juiste omstandigheden, hebben schrijvers van virussen geprobeerd de software te omzeilen door het schrijven van "oligomorfe", "polymorfe" en meer recent "metamorfe" virussen, die stukken van zichzelf encrypteren of zichzelf op een andere manier aanpassen om zich te camoufleren, zodat ze niet overeenkomen met hun bekende virusdefinities.

Detectie van verdacht gedrag

In tegenstelling tot de vorige methode, probeert deze methode niet om bekende virussen te identificeren; in de plaats daarvan houdt men het gedrag van alle programma's in de gaten. Wanneer bijvoorbeeld een programma probeert gegevens te schrijven naar een ander uitvoerbaar programma, kan de antivirussoftware dit zien als verdacht gedrag, en de gebruiker waarschuwen en om een reactie vragen.

In tegenstelling tot de aanpak met een virusdatabase, kan men zo bescherming bieden tegen splinternieuwe virussen die nog niet in de lijsten voorkomen. Dit zorgt echter ook voor een groot aantal fout-positieven, en gebruikers worden vlug achteloos voor de waarschuwingen. Wanneer een gebruiker elke waarschuwing zomaar wegklikt, heeft de antivirussoftware vanzelfsprekend geen nut meer voor die gebruiker. Dit probleem is enkel erger geworden, aangezien meer ontwerpen van niet kwaadaardige programma's andere .exe-bestanden aanpassen zonder deze fout-positiefkwestie in acht te nemen. Moderne antivirussoftware gebruikt deze techniek daarom steeds minder.

Andere methodes

Sommige antivirussoftware probeert het begin van de code van elk nieuw uitvoerbaar bestand dat het systeem aanroept te emuleren, vooraleer de controle aan het nieuwe bestand zelf wordt overgedragen. Als het programma zelfmodificerende code lijkt te gebruiken of op een andere manier het gedrag van een virus lijkt te vertonen (het zoekt bijvoorbeeld onmiddellijk naar andere uitvoerbare bestanden), kan men veronderstellen dat het bestand door een virus is geïnfecteerd. Ook deze methode resulteert echter in veel fout-positieven.

Bij nog een andere detectiemethode gebruikt men een sandbox. Een sandbox emuleert het besturingssysteem en voert het programma uit binnen deze simulatie. Nadat het programma is beëindigd, analyseert de software de sandbox op wijzigingen die op een virus kunnen wijzen. Vanwege prestatieproblemen vinden zulke detecties normaal gesproken enkel plaats tijdens manueel gestarte scans.

Aandachtspunten

- De verspreiding van e-mailvirussen (deze horen bij de meest destructieve en verspreide computervirussen) kan op een veel goedkopere en efficiëntere manier tegengegaan worden, zonder dat de installatie van antivirussoftware nodig is, wanneer bugs in e-mailsoftware zouden hersteld worden. Deze fouten laten immers toe dat gedownloade code uitgevoerd kan worden en zich kan verspreiden en schade aanrichten.
- Het opleiden van de gebruikers kan effectief een meerwaarde bieden bovenop de antivirussoftware; eenvoudigweg de gebruikers wijzen op veilig omgaan met computers (zoals het niet downloaden en uitvoeren van onbekende programma's van het Internet) zou de verspreiding van virussen vertragen en de nood aan veel antivirussoftware verminderen.
- Computergebruikers zouden niet altijd hun machine mogen gebruiken als systeembeheerders. Als ze eenvoudigweg zouden werken in gebruikersmodus, zouden veel virustypes zich niet kunnen verspreiden (of hun schade zou minstens beperkt blijven). Dit is een van de verschillende redenen waarom virussen relatief zeldzaam zijn op UNIX-achtige systemen.
- De aanpak met lijsten om virussen te definiëren volstaat niet, wegens de voortdurende aanmaak van nieuwe virussen; maar ook het detecteren van verdacht gedrag werkt niet voldoende wegens het fout-positiefprobleem. Daarom kan de huidige kennis die ingebouwd is in antivirussoftware nooit alle computervirussen bestrijden.
- Er bestaan verschillende methodes om kwaadwillige software te encrypteren en te verpakken, zodat zelfs bekende virussen niet ontdekt kunnen worden door antivirussoftware. Om deze "gecamoufleerde" virussen op te sporen heeft men krachtige code nodig om deze bestanden te ontcijferen alvorens men ze kan onderzoeken. De meeste populaire antivirusprogramma's hebben dit echter niet, en kunnen dus vaak deze virussen niet waarnemen.

- Het voortdurende schrijven en verspreiden van virussen en van de paniek eromheen, maakt dat de verkopers van commerciële antivirussoftware financieel baat hebben bij het blijvende bestaan van virussen.
- Sommige antivirussoftware kan de systeemprestaties aanzienlijk verminderen. Gebruikers schakelen vaak de antivirusbescherming uit om dit prestatieverlies tegen te gaan en lopen zo een verhoogd risico op infectie. Voor maximale bescherming moet de software altijd ingeschakeld zijn, wat vaak tragere prestaties tot gevolg heeft (zie ook Software bloot). Sommige antivirussoftware heeft minder invloed op de prestaties.
- Het is soms nodig om de virusbescherming tijdelijk uit te schakelen wanneer men belangrijke updates uitvoert, zoals de Windows Service Packs, of het updaten van de stuurprogramma's van de grafische kaart. Ingeschakelde antivirussoftware kan er tijdens een belangrijke installatie voor zorgen dat de update niet correct verloopt of helemaal niet lukt.

Antivirussoftwarebedrijven

- Avira uit Duitsland
- avast! uit Tsjechië
- BitDefender uit Roemenië
- Computer Associates uit de VS
- ClamAV - GPL
- ClamWin - GPL ClamAV voor Windows
- Coranti uit Japan
- Eset makers van NOD32 uit Slowakije
- F-Secure uit Finland
- G Data Software uit Duitsland, makers van G Data AntiVirus (voorheen AntiVirusKit)
- Grisoft makers van AVG Anti-Virus uit Tsjechië
- H+BEDV, tegenwoordig bekend als Avira uit Duitsland, makers van AntiVir
- Kaspersky Lab uit Rusland
- McAfee uit de VS
- Norman uit Noorwegen
- Panda Security uit Spanje (Voorheen Panda Software)
- RAV Antivirus uit Roemenië (in 2003 gekocht van GECAD)
- Sophos uit het VK
- Stiller Research
- Symantec makers van Norton AntiVirus/Symantec Antivirus
- Trend Micro uit Japan (in naam uit Taiwan - VS)
- Zone Labs de makers van ZoneAlarm
- AVG
- NOD32
- Microsoft Security Essentials van Microsoft