Rekenaarvirusse in Suid-Afrika

Martin Olivier
Sentrum vir Gevorderde Reken- en Besluitnemingsondersteuning
WNNR, Posbus 395, Pretoria 0001

September 1989

Abstrak

Die algemene voorkoms van die 'springende bal'-virus in Suid-Afrika het Suid-Afrikaners opnuut bewus gemaak van rekenaarvirusse.

'n Span van die Sentrum vir Gevorderde Reken- en Besluitnemingsondersteuning van WNNR is tans besig met 'n ondersoek van rekenaarvirusse. Daar word op teenmiddels en teenmaatreëls gekonsentreer. Verskeie ander instansies is ook tans besig om beleid te formuleer ten opsigte van rekenaarvirusse sodat die potensiële bedreiging geminimeer kan word.

Hierdie referaat definieer 'n rekenaarvirus, gee 'n oorsig van die tipes rekenaarvirusse en kyk meer spesifiek na enkele voorbeelde. Voorts word die situasie in Suid-Afrika bespreek.

1 Inleiding

'n Rekenaarvirus is 'n program wat homself van een plek na 'n ander kopieer sonder dat die gebruiker daarvan bewus hoef te wees. So 'n program kan dan van 'n besmette rekenaar na ander rekenaars oorgedra word met behulp van skywe wat eers op die besmette rekenaar gebruik is en dan op ander rekenaars gebruik word. 'n Virus kan ook 'n rekenaarnetwerk gebruik om na ander rekenaars te versprei.

As 'n virus eers na 'n rekenaar versprei het, kan dit die werking van die rekenaar op verskeie wyses beïnvloed. Dit kan enigiets vanaf die vertoon van 'n grappige boodskap tot vernietiging van data behels.

Die indringing van rekenaars deur ongemagtigde gebruikers is niks nuuts nie—verskeie handboeke is al oor die onderwerp geskryf en groter rekenaars maak in hulle bedryfstelsels en apparatuur voorsiening om sulke pogings te fnuik. Daar is egter twee belangrike verskille tussen tradisionele indringingstegnieke en virusse:

- Die “onbetrokkenheid” van die virusskrywer—so persoon het selde enige bande met slagoffers van sy virus; gewoonlik word die skrywer van ’n virus nie geïdentifiseer nie.

- Almal word deur virusse bedreig—van die kleinste privaat gebruiker waar indringing geen ekonomiese voordeel inhou nie tot die grootste maatskappy.

Die grootste motivering wat virusskrywers en tradisionele indringers in gemeen het, is waarskynlik die uitdaging wat dit bied.

Hoekom het virusse nou eers ’n probleem geword? Die volgende kan moontlike redes wees:

- Mikrorekenaars het geen sekerheidskontroles soos dié van die groter rekenaars nie.

- Baie gebruikers kan (veral mikro-) rekenaars op ’n tegniese vlak leer ken soos net opgeleide spesialiste ’n rekenaar ’n dekade gelede geken het.

- Die gebruikersgemeenskap van rekenaars groei daagliks en programme word op ’n groot skaal uitgeruil—programme word nie net meer tussen vriende uitgeruil nie, maar met behulp van bulletinborde en netwerke word programme wêreldwyd versprei.

Dit is relatief moeilik om virusse te bestudeer: Die media het gou die sensasionele aspek van virusse besef en ongegronde berigte gepubliseer. Selfs in die meer tegniese tydskrifte word onwaarhede verkondig: neem enige bekende virus en slaan na watter skade dit kan aanrig—daar sal ten minste twee of drie verskillende verhale wees. Die groot probleem is dat die meeste van die artikels op hoorsê gebaseer is en nie op eie ondervinding nie.

Mutasies van virusse is nog ’n moontlikheid wat die bestudering van virusse bemoeilik. Daar is niks wat ’n gesoute programmeerder verhoed om ’n virus na sy smaak te wysig nie. Indien mens een variasie van ’n virus bestudeer, kan mens moeilik gevolgtrekkings maak aangaande die ander variasies. Daar is dus nie ’n “standaarduitgawe” van die virus wat as verwysing gebruik kan word nie.

2 Klassifikasie

Die term *rekenaarvirus* word verskillend deur verskillende mense gebruik. Die puriste (wat die outeur insluit) gebruik dit slegs om te verwys na ’n program wat, soos ’n griepvirus, byna op eie stoom van een draer na ’n ander draer beweeg.

Ander verwys na enige program met ’n ongewenste effek as ’n virus. In hierdie referaat word die term *virus* in die suiwer sin gebruik.

Ons gebruik die volgende klassifikasie van programme met ongewenste effekte. Let op dat die klasse nie onderling uitsluitend is nie.

- **Trojaanse perde**
  ’n Trojaanse perd is ’n program wat hom voordoen as ’n ander program. Een van die maniere waarop hierdie programme versprei word, is om ’n program wat, sê maar ’n harde skyf formatteer op ’n bulletinbord te plaas onder die naam van ’n gewilde nutsprogram. Baie gebruikers sal die program dan aflaai en “verras” word wanneer hulle dit probeer gebruik. Sien [8] vir ’n beskrywing van ’n gesofistikeerde Trojaanse perd.

- **Wurms**
  ’n Wurm is ’n program wat stelselhulpbronne “opeet”. Dikwels is wurms programme wat gemors op ’n skyf skryf om algaande meer skyfspasie in beslag te neem.

- **Logiese bomme**
  ’n Logiese bom is ’n program wat in ’n rekenaar geplaas word en wat sal begin uitvoer wanneer aan sekere voorwaardes voldoen word—dit kan byvoorbeeld begin uitvoer op ’n sekere tyd of wanneer ’n sekere ander program uitgevoer word. Die bekendste voorbeeld van ’n logiese bom is die kode in ’n salarisprogram wat veroorsaak dat die program nie meer funksioneer wanneer ’n sekere werknemer se naam nie meer op die salarisrol is nie.

- **Virusse**
  ’n Virus is ’n program wat bedoel is om van een rekenaar na ’n volgende te versprei. So ’n program sal homself tipes aan ’n program op ’n slapskyf heg en, wanneer hierdie slapskyf op ’n ander rekenaar gebruik word, na die harde skyf van hierdie rekenaar versprei word. Die beweeg na die slapskyf en vandaar na ’n ander harde skyf geskied sonder dat die gebruiker dit besef.

Gewoonlik word bostaande tegnieke in kombinasie gebruik: die Jerusalemvirus vee data uit as die datum die dertiende is en dit ’n Vrydag is—dit is dus ’n virus wat elemente van ’n logiese bom bevat. ’n Virus wat homself aan ’n program haak en versprei wanneer die program uitgevoer word, verander die program in ’n Trojaanse perd.

’n Virus se kode moet uitgevoer word vir die virus om enige effek te hê. Daar is drie plekke waar so virus geplaas kan word:

- **Lêervirusse**
  Voeg viruskode by ’n ander program—in die geval van MSDOS word die virus aan ’n .COM- of .EXE-lêer gehaak. Ons kan tussen twee klasse lêervirusse onderskei:

  - **Direkte-aksie lêervirusse**
    So ’n virus versprei net wanneer die besmette lêer uitgevoer word.
  - **Indirekte-aksie lêervirusse**
    So ’n virus installeer homself in die geheue vanwaar dit kan versprei net wanneer dit wil.

- **Bedryfstelselvirusse**
  Plaas viruskode in ’n deel van die bedryfstelsel—by MSDOS kan dit in COMMAND.COM, MSDOS.SYS, IO.SYS of in ’n toesteldrywer geplaas word.

- **Inisialisering-virusse**
  Daar is aktiwiteite in ’n rekenaar laer as die bedryfstelselvlak. Dit sluit die selflaaier (*bootstrap loader*) in wat verantwoordelik is om die bedryfstelsel te laai. Hierdie virusse moet, wanneer ’n deel van die stelsel se inisialiseringskode uitgevoer word, geheue reserveer en dit in hierdie geheue installeer, vanwaar dit kan voortplant. Alhoewel so ’n virus nie werklik fasiliteite van die bedryfstelsel kan gebruik nie (omdat dit geïnstalleer word voor die bedryfstelsel gelaai word) is dit nie onafhanklik van die bedryfstelsel nie—dit is tipies van die skyforganisasie van die bedryfstelsel afhanklik.

3 Newe-effekte van virusse

’n Rekenaargebruiker besef gewoonlik hy het ’n virus wanneer die rekenaar ongewoon begin reageer. Die ‘springende bal’-virus laat byvoorbeeld ’n “balletjie” oor die skerm beweeg, terwyl die Jerusalem-virus lêers kan uitvee. Hierdie eienaardige gedrag van die rekenaar is die oomblik van “triomf” waarop die virusskrywer hoop. Suksesvolle virusse wag relatief lank voor hulle op hierdie wyse hulle teenwoordigheid wys—teen die tyd wat die gebruiker besef dat hy gevang is, moes die virus reeds genoeg versprei het, dat verdere verspreiding nie onmiddellik hokgeslaan kan word nie.

Dit is ook belangrik om te let dat hierdie ongewone reaksie van die rekenaar ’n onbelangrike deel van die virus is; die verspreidingsdeel is die ingewikkelde deel.

Dit is byvoorbeeld eenvoudig om die kode van die ‘springende bal’-virus wat die balletjie laat beweeg te wysig om byna enige ander effek te hê.

3.1 Beplande newe-effekte

Baie virusse word nie geskryf om direkte skade aan te rig deur byvoorbeeld data uit te vee nie.

Die ‘springende bal’-virus is byvoorbeeld nie bedoel om doelbewuste skade te doen nie—die virusskrywer het redelik sorg getref dat die werking van die rekenaar nie geaffekteer word nie. Die effek van die BRAIN-virus is nog minder opsigtelik—die skyfetiket word na `(c) BRAIN` verander.

Ander virusse is meer vandalisties van aard: die Jerusalem-virus maak die rekenaar normaalweg stadiger; op ’n Vrydag die dertiende vee dit egter lêers uit.

Die Lehigh-virus oorskryf die eerste 32 sektore van die harde skyf wat die inligting op die skyf feitlik onbruikbaar maak. Hierdie inligting word oorskryf elke vierde keer wat die virus versprei het. Dit veroorsaak egter dat die draer van die virus so gou vernietig word dat die virus blykbaar nie wyd versprei nie.

’n Rekenaarvirus kan ook meer subtiele effekte hê—’n virus wat aan getalle peuter deur syfers om te ruil kan baie meer skade aanrig—die gebruiker sal dit waarskynlik eers agterkom wanneer sy besigheid verliese begin toon.

3.2 Onbeplande newe-effekte

Daar word dikwels gewonder of die idees agter rekenaarvirusse positief gebruik kan word. Virusse het egter altyd onbeplande newe-effekte wat enige gebruik van die idees onwenslik maak. **Daar is geen onskadelike virus nie.**

Benewens die feit dat ’n virus ’n rekenaar se werking vertraag, wat in sommige gevall kan veroorsaak dat die rekenaar “hang”, kan dit ook ander ongewenste effekte hê—virusse aanvaar byvoorbeeld 100% versoenbaarheid ten opsigte van die rekenaar waarvoor die virus geskryf is.

4 Gevallestudies

In hierdie afdeling word kortliks na ’n paar bekende virusse gekyk om die konsepte te illustreer. Omdat dit moontlik is om ’n virus te wysig, mag daar mutasies van virusse in omloop wees wat verskil van die weergawes wat hier bespreek word.

4.1 Springende bal

Die ‘springende bal’-virus is ook bekend as die Intaliaanse Virus, die 1357-virus en die *Ping Pong* Virus.

Die ‘springende bal’-virus is ’n inisialiseringsvirus. Dit verskuif die selflaaikode vanaf die eerste sektor, baan 0 van die skyf na die eerste beskikbare sektorgroep (*cluster*) op die skyf. (Hierdie kode word in die tweede sektor in die betrokke sektorgroep geplaas.) Viruskode word nou in die selflaaisektor geplaas, asook in die eerste sektor van die sektorgroep wat nou die oorspronklike selflaaisektor hou. Hierdie sektorgroep wat gebruik word, word ‘sleg’ gemerk sodat MSDOS dit nie vir iets anders gebruik nie.

Wanneer die rekenaar volgende keer geïnisialiseer word, word die viruskode vanaf die selflaaisektor gelaai en geaktiveer. Die virus skuif die wyser wat na die hoogste geheue (LSG) wys, 2K af en kopieer homself na hierdie boonste 2K van geheue. Die res van die viruskode word vanaf die eerste sektor van die ‘slegte’ sektorgroep gelaai. Die virus verander onderbrekingsvektor 13h (wat alle skyftoegange beheer) om na viruskode te wys en die spronginstruksie aan die einde van hierdie kode word verander om na die oorspronklike onderbrekingshanteerder vir onderbreking 13h te spring. Hierna word die oorspronlike selflaaikode vanaf die tweede sektor van die ‘slegte’ sektorgroep gelaai en geaktiveer. Hierdie selflaaikode laai en aktiveer die bedryfstelsel sodat die rekenaar soos normaalweg werk. Die viruskode word nie deur die bedryfstelsel beïnvloed nie omdat die bedryfstelsel nie eers bewus is van die 2K geheue waarin die viruskode gehou word nie.

Omdat die virus aan onderbreking 13h ‘gehaak’ is, kan dit alle skyftoegange monitor. Wanneer ’n skyftoegang gemaak word, gebeur die volgende voor die virus beheer aan die oorspronklike onderbrekingshanteerder oordra:

- Indien die skyf nog onbesmet is, word die skyf besmet.
- Anders kyk die virus na die interne tyd en besluit op grond hiervan of dit tyd is om die balletjie te aktiveer—die moontlikheid om die balletjie te aktiveer bestaan vir ’n paar sekondes ongeveer elke halfuur.

Die balletjie is ASCII-karakter 7 wat deur ’n deel van die viruskode oor die skyf beweeg word. Wanneer die balletjie geaktiveer moet word, word hierdie kode aan onderbreking 8h gehaak. Hierdie onderbreking word deur ’n interne klok beheer en kom 18.2 keer per sekonde voor—telkens wanneer dit voorkom word die balletjie een posisie aangeskuif.

Vir verdere besonderhede aangaande die ‘springende bal’-virus, sien [3], [4] en [7].

4.2 BRAIN

Die BRAIN-virus is ook bekend as die Pakistan-virus omdat dit in Pakistan geskryf is.

Die BRAIN-virus is ook ’n inisialiseringsvirus en werk soos die ‘springende bal’-virus. Dit verander die skyfetiket van alle besmette skywe na `(C) BRAIN`.

BRAIN besmet net 360K slapskywe. Dit benodig drie naasliggende beskikbare sektorgroepe vir besmetting. Hierdie sektorgroepe word ‘sleg’ gemerk sodat MSDOS dit sal uitlos.

Vir verdere inligting aangaande BRAIN sien [2] en [7].

4.3 Jerusalem

Die Jerusalem-virus is ook bekend as die Israel-virus, Tel Aviv-virus en die 1813-virus.

Die Jerusalem-virus is ’n lêervirus—viruskode word by .COM- en .EXE-lêers gevoeg om dit te besmet. Wanneer so ’n lêer besmet word, word dit 1813 grepe langer. ’n .COM-lêer word net een keer besmet, maar ’n .EXE-lêer kan meermale besmet word—tot op die punt waar dit te groot is om in geheue te laai om uit te voer.

Die virus word in geheue geïnstalleer, vanwaar dit onderbreking 21h funksie 4Bh monitor—telkens wanneer ’n program uitgevoer word, sal die virus dit dus agterkom en die program besmet.

Normaalweg kan dit ook ’n leë lus aan onderbreking 8h haak om die rekenaar stadiger te maak. Op ’n Vrydag die dertiende sal dit egter (deur middel van die onderskepping van onderbreking 13h se funksie 4Bh) elke lêer uitvee wat uitgevoer moet word.

Vir verdere besonderhede aangaande die Jerusalem-virus sien [7]

5 Gevolge van virusse

Rekenaarvirusse het veral ’n invloed op die volgende groepe mense:

- Rekenaarwetenskaplikes wat in die tegniese aspekte belangstel—veral rekenaarsekerheidspesialiste.
- Finansiële deskundiges, veral ouditeure.
- Sekerheidpersoneel wat vir oorhoofse sekerheid in ’n organisasie verantwoordelik is.

Verskillende komitees (in die staatsdiens en in die privaatsektor) is tans besig om die potensiële gevaar van virusse te skat, asook om op teenmaatreëls te besluit. Baie organisasies het reeds hulle beleid ten opsigte van rekenaarsekerheid hersien—veral die huistoe neem van werk op slapkyf, speel van rekenaarspeletjies en kopiëring van programme word aangespreek.

Ongegronde gerugte oor virusse het ook ’n groot invloed op die rekenaaromgewing gehad. So word enige enige probleem (wat voorheen deeglik ondersoek sou word) dikwels sondermeer op ’n rekenaarvirus blameer. Sien byvoorbeeld [1] vir ’n beskrywing van ’n vals alarm.

Teen-virus programmatuur maak ook in ’n al groter mate hul verskyning. Die tempo waarteen sulke programmatuur verskyn laat egter vrae ontstaan oor hul betroubaarheid. Verder is die ‘medisyne’ om virusse te verhoed dikwels erger as wat die virus self sou wees. Sien [6] vir ’n bespreking van teen-virus programmatuur.

6 Suid-Afrika

Suid-Afrika het tot dusver relatief min probleme met rekenaarvirusse gehad—die ‘springende bal’-virus is die enigste wat tans (September 1989) algemeen gerapporteer word. Wat wel kommerwekkend is, is die mate waartoe die virus reeds versprei het—dit kom landswyd voor sonder dat vasgestel kan word presies wanneer dit die land binnegekom het.

Ons kan verwag dat virusse wat tans in die buiteland in omloop is, ook mettertyd na Suid-Afrika sal versprei. Die moontlikheid van plaaslik geskrewe virusse kan ook nie uitgesluit word nie.

Hoe vatbaar is gebruikers in Suid-Afrika vir rekenaarvirusse? Die ongunstige wisselkoers veroorsaak dat ingevoerde programmatuur uiters duur is. Dit kan veroorsaak dat programme meer gekopieer word as elders in die wêreld wat die potensiaal vir die verspreiding van virusse verhoog. Aangesien Suid-Afrika ook programmatuur vanaf beide die VSA en Europa kry, is ons blootgestel aan ’n relatief groot verskeidenheid virusse. Die relatiewe skaarste van netwerke en bulletinborde in Suid-Afrika behoort hierdie gevaar egter ietwat te verminder.

7 Gevolgtrekking

Rekenaarvirusse hou ’n gevaar in en daar is geen onmiddellike oplossings nie. Namate groter rekenaars met meer beskermingsmeganismes egter gebruik word, sal dit al hoe moeiliker raak om suksesvolle virusse te skryf en sal die verhaal van

rekenaarvirusse een van die staaltjies word wat vertel word wanneer oor “rekenaars in die ou dae” gepraat word.

Intussen is gereelde rugsteun, ’n deeglike kennis van bestaande virusse en ’n gesonde beleid aangaan de virusse waarskynlik die beste oplossing.

Hierdie referaat is ’n uitreksel uit [5].

8 Bibliografie

[1] Glath, R M, “The Case of the “Gerbil Virus” that wasn’t”, Computers & Security, **7** (1988), 451–453

[2] Highland, H J, “The BRAIN Virus: Fact and Fantasy”, Computers & Security, **7** (1988), 367–370

[3] Highland, H J, “The Italian Virus”, Computer Fraud & Security Bulletin, **11**, 7 (1989), 7–8

[4] Olivier, M S en Teitge, H W, “Analysis of the Bouncing Ball Virus”, Tegniese verslag PKOMP 89/5, Sentrum vir Gevorderde Reken- en Besluitnemingsondersteuning, WNNR, Julie 1989

[5] Olivier, M S, “Rekenaarvirusse: ’n Suid-Afrikaanse Perspektief”, Tegniese verslag, Sentrum vir Gevorderde Reken- en Besluitnemingsondersteuning, WNNR, Om te verskyn

[6] Rubenking, N J, “Infection Protection”, PC Magazine, April 25 1989, 193–228

[7] Solomon, A, “Dr Solomon’s Anti-Virus Toolkit”, S&S Enterprises, Amersham, 1989

[8] Thompson, K, “Reflections on Trusting Trust”, Communications of the ACM, **27**, 8 (1984), 761–763

MS Olivier, “Rekenaarvirusse in Suid-Afrika”, *Vierde Jaarlikse Konferensie vir M.Sc en Ph.D Rekenaarwetenskapstudente*, Cathedral Peak, Suid-Afrika, September 1989. Onbeoordeeld.