schets) uit een dikke betonnen buis, voorzien van de twee X-ray scanners. De in- en uitgang van de buis zijn van deuren voorzien. De container wordt op een soort oplegger geplaatst en middels een hoogwaardig transportsysteem zeer gelijkmatig door de scan getransporteerd. Vanuit de operatorroom worden de beelden van de totale inhoud van de container en sectiegewijs aan de hand van de beschikbare ladingspapieren gecontroleerd.

Uiteraard worden de beelden ook vastgelegd. Op die wijze is het mogelijk binnen 5 minuten de totale inhoud van een zeecontainer minutieus te controleren. Gelukkig voor de douaneinspectie Rotterdam is, gezien de investeringen, de onderhoudskosten en de personeelskosten, de HI-CO-SCAN een succes. Onlangs kwam in het nieuws, dat het afgelopen half jaar voor omstreeks *f* 30.000.000,00! aan smokkelwaar was onderschept, dus niet in het 'vrije verkeer' was gekomen.

(D. Plaizier)

DE WERKING VAN HET Tequila virus

Door Ronald Eygendaal

WAT IS EEN COMPUTERVIRUS

Een computervirus is een klein computerprogramma dat meestal een saboterende werking heeft. Een groot aantal virussen 'verbergt' zichzelf in andere programma's om vanuit daar ongezien de juiste werking van de software en het computersysteem te saboteren. Ook probeert het virus zichzelf te vermenigvuldigen om anderen te kunnen besmetten. Wie denkt dat het hierbij alleen om DOS systemen gaat heeft het mis. Er zijn al OS/2, Windows 95 & 98, Windows NT, UNIX, MacIntosh en zelfs Atari-virussen.

HOE RAAKT UW COMPUTER BESMET?

Besmettingen vinden meestal plaats door het gebruik van programmatuur van onduidelijke afkomst, die veelal al eerder was besmet. Populaire programma's zoals leuke spelletjes zijn vaak een bron van besmetting waarbij het spoor vaak via schoolse instellingen loopt. Soms blijkt een nieuwe versie van legaal te gebruiken software al een bron van besmetting waardoor het bedrijf in diskrediet komt. Wees dus bedacht op diskettes, CD-roms en mooie demo software. De laatste tijd zien we in toenemende mate dat de besmettingen van computers in bedrijven plaats vinden via het thuiswerken.

EEN BESMETTING MET HET TEQUILA VIRUS

De eerste keer dat er een file (programma) geladen wordt, dat besmet is met het Tequila virus, zal het virus kijken of de Masterbootrecord c.q. 'partition table' van de harde systeemschijf al besmet is. (In een Masterbootrecord staat de 'index' van de harddisk) Als dit niet het geval is, dan zal Tequila een ongecrypte copy van zichzelf naar de laatste sectoren van de harddisk schrijven. Tevens zal hij de Masterbootrecord dusdanig wijzigen dat deze besmettelijk wordt. Tequila zal zichzelf nog niet meteen in het werkgeheugen zetten. Er zullen dan ook nog geen files besmet worden. Pas als de computer opnieuw opgestart wordt, wordt het virus 'memory resident'. (Het Tequila virus laadt zichzelf in het hoogste gedeelte van het werkgeheugen.) Zodra een .EXE file geladen wordt, wordt deze gecontroleerd op een eventuele besmetting. Is dat niet het geval dan wordt deze besmet. Tequila plakt zichzelf aan de .EXE file, waardoor deze met 2468 bytes groeit. Hierdoor neemt het werkgeheugen en het vrije geheugen af. Het Tequila virus wordt pas 4 maanden na de eerste besmetting van de harddisk actief. Dan en iedere maand erna zal het virus de volgende boodschap op het scherm brengen:

```
'EXECUTE: MOV AX, FE03 / Int
21. Key to go on!'
```

Als er een programma geladen wordt wat hieraan voldoet, dan zal het virus deze tekst laten zien

```
'Welcome to T.Tequila's latest
production'
'Contact T.TEQUILA/P.o.Box 543/
6312 St'Hausen Switzerland.'
'Loving thougt to L.I.N.D.A.'
'BEER and TEQUILA forever!'
```

Deze tekst is in geincrypte vorm ook te vinden in de laatste zes sectoren van de harddisk. Het Tequila virus maakt o.a. gebruik van de Stealthtechniek. De Stealthtechniek is een camouflagetechniek om aan detectie en controle te ontsnappen.

'Diskettes, CD-ROM's en demo-software'

VIRUSPREVENTIE

Uiteraard is het bovenstaande een voorbeeld dat veroorzaakt wordt door 'wisselende' computer contacten. Het Tequila virus is een behoorlijk oud virus. Zoals u zult begrijpen is het zorgen voor een goed actuele virusscanner en -killer een must.

TIPS EN GEHEUGENSTEUNTJES

Hieronder nog een aantal tips wat u als gebruiker van de pc kunt doen:

- Stop het gebruik van de verdachte PC. Maar schakel de PC niet uit;
- Als de PC met een netwerk verbonden is, koppel de netwerkverbinding dan los;
- Neem direct contact op met de IT-coördinator of helpdesk;
- Wissel geen software uit met andere gebruikers;
- Markeer de PC duidelijk, zodat anderen deze PC niet zullen gebruiken;

Mocht u zelf aan de slag gaan met scanners en killers, gebruik dan de volgende geheugensteun.

- Ga na of het ongewone verschijnsel wordt veroorzaakt door een virus.
- Wanneer de virusscanner een virus meldt, ga dan met een andere virusscanner na of het een echte of een valse melding is.
- Gebruik een virusscanner van een ander merk als tweede scanner.
- Gebruik bij twijfel een derde virusscanner.
- Stel het aantal 'besmette' pc's vast en zorg dat er geen contact meer is tussen besmette en onbesmette PC's.
- Probeer de oorzaak van de besmetting vast te stellen.
- Neem alle diskettes in beslag en doe deze in een gemarkeerde envelop.
- Bepaal op welke wijze hoe de ontsmetting zal plaats vinden. Hiervoor kan men het programma VSUM van Patricia Hoffman raadplegen.
- Controleer of de backup diskettes besmet zijn.
- Geschoonde zaken kunnen worden teruggegeven.
- Informeer het management, de IT-coördinator of helpdesk.
- Informeer het personeel dat er een virus is gevonden.
- Geef na de ontsmetting de pc's vrij.
- Ga na enkele dagen na of het virus inderdaad verdwenen is.