REKENEN AAN MALWARE

De heer Henk-Jan van der Molen, Hogeschool Wageningen

Na zijn KMA-opleiding (Verbindingsdienst) heeft Henk-Jan van der Molen van 1984 tot 1998 bij de KL zowel operationele als ICT-functies vervuld. Hij is sinds 2002 terug de overheid, na ruim drie jaar in het bedrijfsleven te hebben gewerkt. Daarnaast is hij docent en verbonden aan de Hogeschool Wageningen. Hij doceert binnen de opleiding Bedrijfskundige Informatica onder meer *Business Intelligence*, Informatiebeveiliging en Verandermanagement. Vanuit zijn praktijkervaringen heeft hij diverse artikelen gepubliceerd, waaronder drie in Intercom. Dit artikel sluit aan op het artikel 'Verdeel en heers' uit Intercom 2009-3 en schetst de contouren van een comprehensive *Cyber Defense*.

INLEIDING

In een research-document over computervirussen[i], concludeert IBM eind 1998 dat de antivirustechnologie de afgelopen 10 jaar zeer succesvol is geweest bij bekende virussen, maar dat er toch nog een paar belangrijke problemen overblijven voor nader onderzoek. Eén daarvan is dat het gangbare model voor de verspreiding van computervirussen niet leek te kloppen met de praktijk.

In dit artikel wordt een eenvoudig netwerkmodel beschreven dat de verspreiding van malware (computervirussen, wormen en *spyware*) over het internet beschrijft. In de tekst worden de termen exploit en malware beschouwd als synoniemen, hoewel een *exploit* meestal een kwetsbaarheid in software misbruikt en daardoor op de computer malware kan downloaden en installeren.
Met het gekozen netwerkmodel wordt globaal het effect verklaard van maatregelen, die tegen malware kunnen worden ingezet, zoals:

- antivirussoftware;
- procedures voor *incident- en change management*, inclusief een *Incident Response Plan*;
- kennis en bewustzijn op veiligheidsgebied;
- regels en voorwaarden voor thuiswerken;
- periodieke vervanging van software en
- het inrichten van software compartimenten.

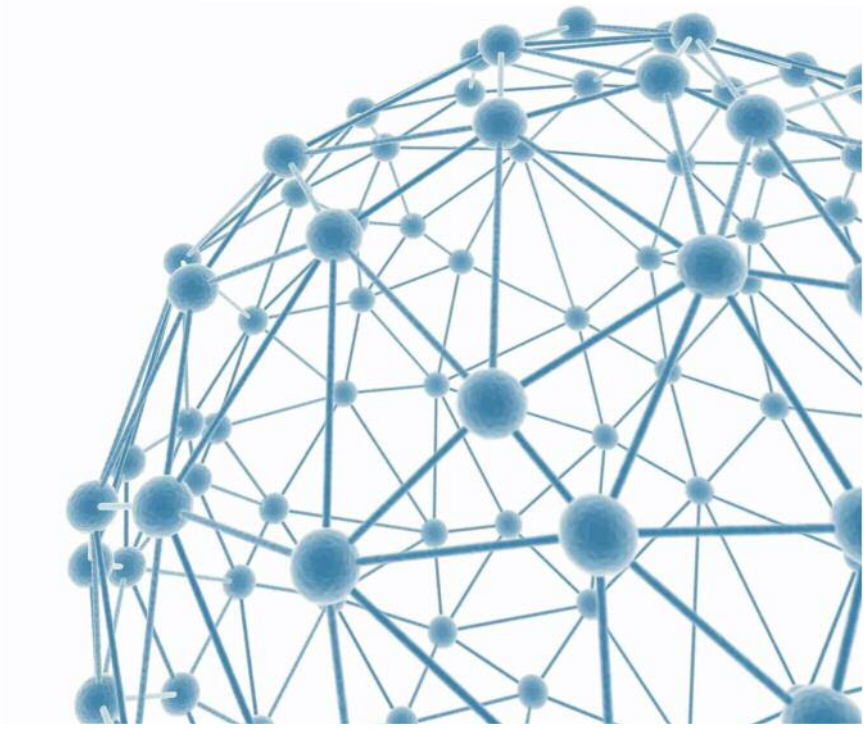
Het doel van het artikel is de discussie te bevorderen hoe de aanpak van het malware probleem kan worden verbeterd. Zoals uit het artikel blijkt, is het malware probleem namelijk nu al ernstig en is het waarschijnlijk dat de situatie nog zal verslechteren.

SOORTEN NETWERKEN

Een netwerk is een set van knooppunten die onderling verbonden kunnen zijn (zie afbeelding). Dergelijke netwerken worden soms ook aangeduid als 'grafen'. Onderzoek kan zich richten op de eigenschappen van individuele knooppunten, maar deze kennis devalueert als het netwerk veel knooppunten bevat, zoals het internet. Het onderzoek van een groot netwerk levert vooral statistische eigenschappen op, waarmee het gedrag ervan beter kan worden begrepen en voorspeld.

Er zijn verschillende soorten netwerken. Het gedrag van informatienetwerken (bijv. verwijzingen op webpagina's), biologische netwerken (zoals roofdier – prooi relaties) en sociale netwerken (bijv. belgedrag), kan ook relevant zijn voor technologische netwerken, zoals het internet met zijn miljarden knooppunten (servers, clients en routers). Het internet is opgezet om robuust te zijn tegen uitval van willekeurig gekozen knooppunten. Wel is het internet zeer kwetsbaar als de knooppunten in aflopende volgorde van het aantal verbindingen gericht worden aangevallen.

Het individuele gebruik van e-mail, P2P en webbrowser vormt een sociaal netwerk. De grootte van een sociaal netwerk is moeilijker te schatten, maar het concept '*six degrees of separation*'[iii] (via 6 stappen kent iedereen iedereen), ook wel bekend als het '*Small World Effect*', bewijst dat de interconnectiviteit ervan hoog is.
Malware kan zich zowel via het internet als via sociale netwerken verspreiden. Een internetworm kan zonder interactie van de gebruiker een online server of werkstation besmetten. Daarnaast kan een gebruiker zelf zijn computer besmetten met malware, bijvoorbeeld door het downloaden en gebruiken van een besmet bestand.



Netwerk weergegeven als verzameling van knooppunten

VERSCHILLENDE PROCESMODELLEN

Vanuit de literatuur[iii] worden drie eenvoudige netwerkmodellen met elkaar vergeleken. Deze modellen zijn niet helemaal realistisch, omdat ervan wordt uitgegaan dat een besmetting 'egaal verdeeld' is over het netwerk, terwijl in werkelijkheid de topologie van een netwerk bepaalt welke knooppunten contact met elkaar kunnen hebben en zo besmettingen kunnen overdragen. De paragraaf 'injectie van malware' gaat hier nader op in. De netwerkmodellen houden daarnaast geen rekening met malware die ontwikkeld is om gericht individuele organisaties aan te vallen. Hieronder een nadere toelichting van de netwerkmodellen.

1. Percolation theory: in dit model kunnen knooppunten en verbindingen 'vrij' (uitgevallen) zijn of 'bezet' (operationeel). Zo kan bijvoorbeeld worden berekend hoeveel elektriciteitscentrales moeten uitvallen voordat de rest van de centrales de gevraagde capaciteit niet meer kan leveren. Voor malware is dit model niet geschikt, omdat een computer door meerdere exploits tegelijk kan worden besmet en toch niet hoeft uit te vallen.

2. Het SIR-model: in dit simpelste model voor de verspreiding van een ziekte wordt uitgegaan van 3 toestanden (*Susceptible, Infected, Recovered*) die een knooppunt éénmalig achter elkaar kan doorlopen. Dit model is geschikt om de verspreiding van een individueel Zero-day-computervirus te beschrijven als de kwetsbaarheid in de software na besmetting werd gepatcht en het virus werd opgeruimd. Ondanks patching zullen er echter altijd kwetsbaarheden in de gebruikte software aanwezig blijven. Doordat standaard beveiligingsmaatregelen steeds slechter besmettingen kunnen voorkòmen, kan een computer meerdere keren achter elkaar door dezelfde malware of gelijktijdig door verschillende malware worden besmet. Daarom is dit model minder geschikt om de verspreiding te beschrijven van malware.

3. Het SIS-model kent 2 toestanden (*S = Susceptible, I = Infected*), zie figuur 1. Niet alle ziekten resulteren nl. in immuniteit voor overlevenden, zodat zij na genezing vatbaar blijven voor de ziekte. Dit geldt bijvoorbeeld voor tuberculose en malware, omdat sommige kwetsbaarheden die exploits misbruiken niet (kunnen) worden gepatcht, zoals bij *social engineering*.[iv] Daarom wordt hier het SIS model gekozen om de verspreiding van malware te beschrijven.

Het SIS-model verdeelt de populatie in twee delen, één deel dat is besmet (i) en de rest dat voor deze besmetting vatbaar is (s). Het model geeft aan dat in het beginstadium een besmetting langzaam groeit, omdat er nog weinig besmette computers zijn die de besmetting kunnen doorgeven. Ook in de eindfase groeit de besmetting langzaam naar de maximale waarde, omdat de kans daalt dat er nog contacten tussen besmette en onbesmette computers plaatsvinden. De besmetting groeit dus evenredig met het product (i.s). Het aantal besmette computers neemt aan de andere kant af door detectie en opruiming van malware. Deze afname is evenredig met het aantal besmette computers (i). De volgende vergelijkingen beschrijven het SIS-model:

$$[1]\quad \partial i/\partial t = \beta is - \gamma i; \qquad i + s = 1$$

De uitdrukking $(\partial i/\partial t)$ staat voor de toename van (i) in de tijd (t). De besmettelijkheidsfactor (β) bepaalt de kans op overdracht van de besmetting per contact tussen een vatbaar en een besmet persoon. De hoogte van (β) hangt af van de effectiviteit van de preventieve veiligheidsmaatregelen.
De kans op 'genezing' van de besmetting (γ) bepaalt de gemiddelde besmettingsduur $(D = 1/\gamma)$ en geeft de effectiviteit van de detectieve en correctieve maatregelen aan.
Uit formule [1] blijkt dat zogenaamde logistische functie[v] of S-kromme de oplossing is van het SIS-model, zie de figuur 2.

Een belangrijke indicator is de parameter R_0 $(= \beta/\gamma)$, de groeifactor van het aantal besmettingen. Door (Ro) in te vullen in [1], kan het maximale aantal besmette computers (imax) worden bepaald in de eindfase waarbij $(\partial i/\partial t)$ daalt naar nul.

$$[2]\quad \partial i/\partial t = \beta is - \gamma i = \gamma i(R_0 s - 1) = 0 \rightarrow$$
$$R_0(1 - i_{max}) = 1 \quad \rightarrow i_{max} = 1 - 1/R_0$$

Uit onderzoek van het SIS-model is gebleken dat er altijd besmettingsgevaar blijft bestaan, onafhankelijk van de hoogte van (β).

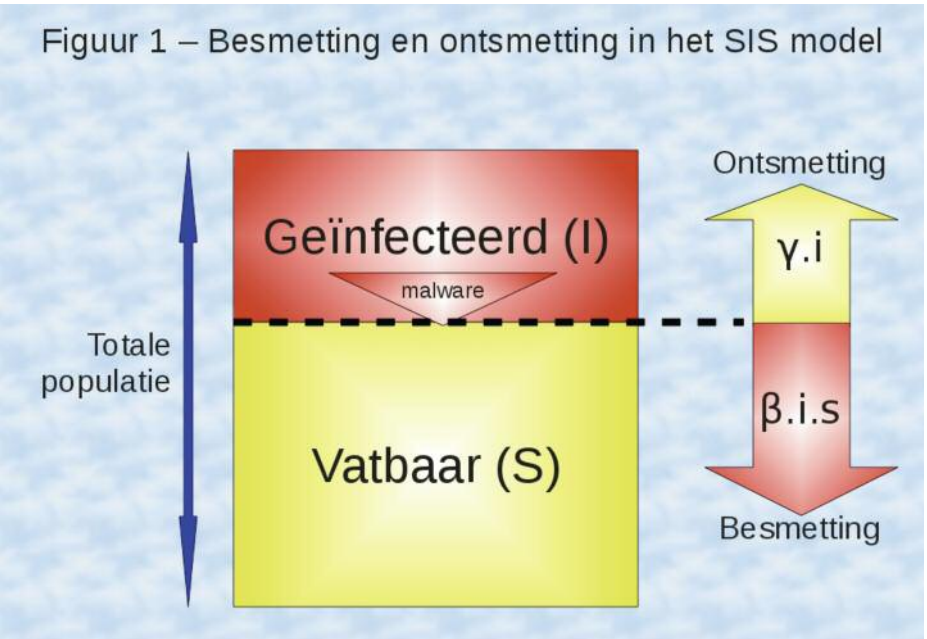
In de eindsituatie is de besmettingsdruk $(F = \beta i_{max})$ maximaal en gelijk aan $(\beta - \gamma)$. Als het product $(R_0.s)$ kleiner blijft dan 1, dan sterft de besmetting uit. Maar zolang $(R_0.s)$ groter is dan 1, groeit de besmetting in de populatie.

HET MALWARE PROBLEEM

De wedloop tussen cybercriminelen en leveranciers van beveiligingsoplossingen is in volle gang. Uit verschillende onderzoeken blijkt dat met actuele malware handtekeningen nog maar tussen de 11% en de 61% van moderne malware kan worden gedetecteerd.[vi] Pas na 4 weken wordt de meeste malware herkend. Hoewel antivirussoftware tegenwoordig ook via heuristiek sommige malware kan detecteren zonder dat daarvan handtekeningen bekend zijn, is de toegevoegde waarde daarvan beperkt. Dat komt omdat antivirussoftware niet teveel valse positieven mag geven, anders haken gebruikers al snel af. Bovendien wordt zowel gesloten source software als malware vaak verpakt in vercijferde zip-bestanden, wat malware detectie veel moeilijker maakt. Doordat alle antivirusproducten ongeveer evenveel achterlopen op moderne malware, verbetert de detectie van malware maar marginaal door tegelijk meerdere virusscanners in te zetten. Met meerdere virusscanners groeit bovendien het aantal valse positieven. Antivirus softwareleverancier Kaspersky meldde hierover al in 2006: *We're losing this game. There are just too many criminals active on the Internet underground, in China, in Latin America, right here in Russia. We have to work all day and all night just to keep up.*[vii]

Soms hebben softwarebedrijven een zodanige onderhoudsachterstand, dat er al maanden zogenaamde Zero-day-exploits circuleren voordat de kwetsbaarheid wordt gepatcht.[viii]

Figuur 1 – Besmetting en ontsmetting in het SIS model



Daarnaast zijn er aanwijzingen dat cybercriminelen patches automatisch kunnen omvormen tot malware[ix], wat langzaam patchen nog gevaarlijker maakt.
Toch hebben sommige organisaties een achterstand in het doorvoeren van patches, waardoor er in de praktijk soms computers worden besmet via kwetsbaarheden waarvoor allang patches zijn uitgegeven. Goede change management procedures hebben dus een positief effect op de veiligheid.

Het snel produceren en doorvoeren van patches is dus absolute noodzaak, maar patches geven tevens aan dat de ontwikkeling van software niet volwassen is. Zo kan de kwaliteit van software onder andere worden uitgedrukt in het aantal fouten per 10.000 regels code. Door de steeds toenemende computercapaciteit kunnen steeds complexere toepassingen van tientallen miljoenen regels code worden ontwikkeld. Maar omdat producten steeds sneller op de markt moeten komen, neemt de tijd om te testen af. Zelfs na veel patches blijven er in de meeste software daardoor genoeg kwetsbaarheden over die malware kan misbruiken.

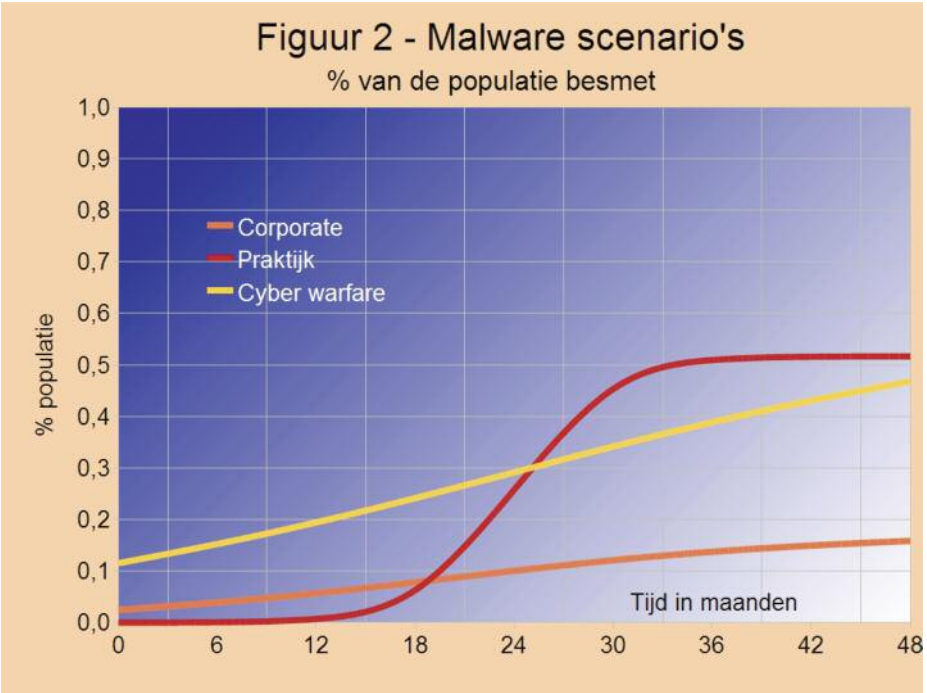
Per maand worden er ca. 300.000 nieuwe malwarepakketten gedistribueerd. Het aantal nieuwe exploits kan zo groot zijn omdat op het internet *'one click'* viruskits voorhanden zijn en dezelfde malware in zelf uitpakkende zip-files met unieke sleutels wordt vercijferd. Door de grote hoeveelheid malware die in omloop is, kan een computer al zijn besmet met verschillende exploits voordat de besmetting wordt opgemerkt. Als een ontsmettingsactie niet alle malware verwijdert, verlaagt dat de waarde van (γ). Incident management procedures moeten daarom voorzien in een beproefd *Incident Response Plan*. Dat verbetert de effectiviteit van een ontsmetting en voorkomt dat onder stress het wiel moet worden uitgevonden.[xi] Het optimaliseren van procedures voor incident- en change management vertaalt zich dus in een vermindering van het aantal en de impact van malware incidenten.
Cybercriminelen verdienen meer geld als (β) hoog is en (γ) laag, zie tabel 1. Op die manier worden meer computers besmet (i_{max}) en duurt de besmetting langer. Een botnet levert bij verkoop direct geld op, maar kan ook per uur worden verhuurd. Zowel de hoogte van de 'huur' als de economische schade door malware is evenredig met (i/γ). Toch kan het voor cybercriminelen ook voordelig zijn om het aantal besmettingen niet te opvallend te laten groeien, omdat snel groeiende malware besmettingen op de radar verschijnen van de leveranciers van antivirussoftware. Door per contact niet elke vatbare computer te besmetten, zijn verschillende scenario's denkbaar, waarvan er drie hieronder worden toegelicht (zie figuur 2).

	Beveiligingsmaatregelen tegen malware (verkleinen R_0)	Tegenacties cybercriminelen (vergroten R_0)
β	Besmettingskans verlagen door preventie met: - *Intrusion Prevention System;* - firewall; - antivirussoftware (on access scan) met patroonherkenning; - legale, *white list* software; - beperkte gebruikersrechten; - *hardening;* - software compartimenten; - goede procedures voor *changes / updates*; - vergroten kennis en bewustzijn; - preventieve *security audits.*	Verhogen besmettingskans malware door: - meerdere aanvalspatronen in malware; - *social engineering;* - delen van kennis en malware code; - testen malware, o.a. met antivirussoftware; - *'fuzz'* testen software op kwetsbaarheden; - website levert malware op maat; - massaal en snel malware verspreiden; - encryptie; - *code obfuscation* in malware; - gerichte malware (*'precision ammo'*).
γ	Verbeter ontsmetting (detectie, correctie) door: - meerdere antivirussoftware pakketten (voor geplande scans); - *Intrusion Detection System;* - logging; - Management procedures voor incidenten en changes, incl. *Incident Response Plan*; - vergroten kennis en bewustzijn; - follow-up security audits.	Verlagen uitval van besmette computers door: - *rootkits;* - *stealth malware;* - encryptie van communicatie; - malware sneller updaten dan antivirussoftware; - imitatie gedrag legitieme software; - malware activeert zichzelf bij bepaalde condities; - patchen van besmette computers (!).

Tabel 1: wedloop tussen cyberaanval en verdediging

1. Het *'corporate'* scenario is gebaseerd op beschikbare statistieken over malware besmettingen bij organisaties. Uitgaande van de gemeten effectiviteit van antivirus software voor nieuwe malware en uit twee opeenvolgende jaarlijkse onderzoeken over cybercrime,[xii] kunnen de parameters van het SIS-model (β, γ) worden berekend[xiii]. Omdat de scope van het onderzoek beperkt is tot organisaties, is dit scenario niet representatief voor de hele populatie.

2. Het 'praktijk' scenario is erop gericht met een maximale snel een grote groep computers te besmetten.[xiv] Voor dit scenario zijn weinig betrouwbare statistieken bekend. Grootschalige besmettingen verschijnen weliswaar op de radar van de leveranciers van antivirussoftware, maar dat betekent niet dat elke besmetting daarna snel kan worden uitgeroeid. Dat laten de ervaringen met de Conficker-worm zien.[xv]



3. In het onwaarschijnlijke '*cyber warfare*' scenario zijn de (fictieve) parameters zeer laag gekozen, waardoor langzaam en maar ongemerkt veel computers kunnen worden besmet.[xvi] Dit scenario kan eigenlijk alleen werkelijkheid worden als de gekozen kwetsbaarheden langdurig kunnen worden misbruikt, bijvoorbeeld als voor misbruik van de gebruikte kwetsbaarheden kennis van gesloten broncode nodig is. Het is dus essentieel dat de besmette computers niet massaal worden ingezet, zodat de gebruikte kwetsbaarheden niet worden opgepikt door andere cybercriminelen, of worden gepatched.
Dit theoretische scenario is niet bedoeld om speculaties te voeden zoals waarom de Chinese overheid het gebruik van hun 'Red Flag' besturingssysteem wil verplichten[xvii], het gevolg van de inzage in de broncode van Windows die Microsoft de Russische geheime dienst biedt,[xviii] waarom een grote software leverancier in 2002 is vrijgesproken in een federale antitrust zaak of dat er in Roswell (USA) vliegende schotels zijn geland.

PERIODIEKE VERVANGING VAN ALLE SOFTWARE

Vanuit de netwerktheorie is bekend dat als knooppunten met de meeste verbindingen worden uitgeschakeld, de functie van het netwerk snel verslechtert. Zo wordt de verspreiding van spam en malware het beste belemmerd door de bron aan te pakken. Het uitschakelen van bronnen is echter moeilijk, omdat cybercriminelen vaak in het buitenland opereren en voor de verspreiding van spam of malware roulerende webservers inzetten.
Als malware bronnen niet effectief kunnen worden aangepakt, is het een mogelijkheid om preventief op computers regelmatig de (schone) software opnieuw te installeren. Hierbij worden mogelijk besmette computers vervangen door onbesmette exemplaren. Het veiligheidseffect van zo'n periodieke vervanging van software kan worden bepaald door het SIS-model aan te passen. Hierbij is (μ) het gedeelte van de populatie dat gemiddeld per maand wordt vervangen. De instroom bedraagt (μ) onbesmette computers, de uitstroom ($\mu i + \mu s$) (besmet en onbesmet).

[3] $\partial s/\partial t = -\beta is + i\gamma + \mu - \mu s$
$= -\beta is + i(\gamma + \mu);$
$\partial i/\partial t = \beta is - i(\gamma + \mu)$

Deze maatregel verkleint weliswaar de factor (R0), maar de bijdrage van deze vervanging aan (γ) is gering als (μ) veel kleiner is, zoals bij de gebruikelijke 4 jaarlijkse vervanging van hardware. Het automatisch vervangen van alle software op alle computers past sowieso als maatregel in een *Incident Response Plan*. Een dergelijke arbeidsintensieve actie is echter alleen efficiënt uit te voeren als dat kan worden geautomatiseerd.

VERBETEREN THUISWERKVOORZIENINGEN EN BEVEILIGINGSKENNIS

Het is bekend dat de oorzaak van veel incidenten ligt bij de eigen medewerkers. Bijvoorbeeld als een medewerker op zijn besmette pc thuis verder werkt aan een zakelijk document, kan bedrijfsinformatie op straat komen te liggen. Nu zijn zakelijke computers en de privé computers van medewerkers thuis vaak direct gekoppeld via e-mail en USB-stick. Dergelijke koppelingen kunnen malware overdragen. Sommige organisaties stellen daarom regels voor thuiswerken en verstrekken hun medewerkers gratis de zakelijke software voor thuisgebruik, inclusief beveiligingssoftware. Organisaties die hiervoor geen licentiekosten willen maken, kunnen gebruik maken van *freeware* of *open source software*. Deze voorzorgen verminderen tevens de kans dat medewerkers met illegale, besmette software op hun eigen pc hun zakelijke computer besmetten. Daarnaast kunnen deskundige auditors de getroffen beveiligingsmaatregelen beoordelen op effectiviteit en efficiency.

De populatie van computergebruikers kan worden verdeeld in een deel met veel en een deel met weinig beveiligingskennis. Omdat het SIS-model complex wordt bij heterogene populaties, is het kwantitatieve beeld niet volledig.[xix]
Kwalitatief is voor security-deskundigen het besmettingsgevaar van malware (β) lager en de kans op een succesvolle ontsmetting (γ) groter dan voor ondeskundigen omdat ze veiliger werken en beschikken over een betere technische beveiliging.
Nu is de groep ondeskundigen groter dan de groep deskundigen, omdat lang niet alle zakelijke computers goed worden beveiligd (bijv. in het MKB) en er meer computers privé worden gebruikt dan zakelijk. In de praktijk weet de gemiddelde computergebruiker weinig over beveiliging. Als bij computers van ondeskundigen besmettingen vaker voorkomen en langer duren, is dat ook nadelig voor die deskundigen of organisaties die dezelfde software gebruiken. Dat komt omdat in onderlinge communicatie malware kan worden uitgewisseld. De kans op een 'vruchtbaar' contact is het grootst bij marktleidende software.
Daardoor blijft het malware risico hoog voor de deskundigen die marktleidende software blijven gebruiken en migreren sommige deskundigen naar niet-marktleidende software.

Aan de andere kant vertaalt het verbeteren van het kennis en bewustzijn op veiligheidsgebied van ondeskundige computergebruikers zich dus naar een verlaging van de effectiviteit van malware en een snellere opruiming ervan voor de hele populatie. Dat betekent niet dat het nodig is iedereen op te leiden tot *security-expert*. Met een beperkte inspanning is mogelijk het aantal incidenten terug te dringen, bijvoorbeeld met een voorlichting bij de instroom en een periodieke opfriscursus over beveiliging. Do's en don'ts kunnen medewerkers snel *streetwise* op het internet maken. Een goede vuistregel voor veilig internetten: 'Als iets te mooi is om waar te zijn, dan is het dat ook'. Ook een simpele stelregel is om programmatuur na download niet direct te gebruiken. Als na 4 weken de antivirussoftware daar geen malware in vindt, is de kans veel groter dat dit inderdaad zo is.

Als de beveiliging goed is ingericht, zijn er maatregelen getroffen waardoor ondeskundige gebruikers hun pc niet zomaar kunnen besmetten. Als werknemers weten waarom hun rechten beperkt zijn, de zakelijke *white list* software thuis mogen gebruiken en de '*lessons learned*' van incidenten breed worden gecommuniceerd, bevordert dat het draagvlak én het veiligheidsbewustzijn.

SOFTWARE COMPARTIMENTEN

Voor malware vormt elk code-compartiment een aparte populatie, zoals bijvoorbeeld alle Windows pc's een eigen compartiment vormen naast Macs en Linux pc's. Hoewel software compartimenten verbonden kunnen zijn door gemeenschappelijk code in hardware drivers en netwerkfuncties, is het in de praktijk zeer onwaarschijnlijk dat Windows malware een Mac kan besmetten.

Alle software bevat kwetsbaarheden en computers die dezelfde software gebruiken, bevatten dezelfde kwetsbaarheden. Om hun winst te maximaliseren, richten cybercriminelen hun malware bij voorkeur op de marktleidende software.[xx] Het is dus wel mogelijk een virus te schrijven voor een Mac of een Linux pc, maar tegen dezelfde kosten levert Windows malware veel meer winst op.

Software monopolies zijn kwetsbaar, omdat voor malware de kans om een vatbare pc te besmetten het grootst is. Het ligt dus voor de hand om het economisch rendement van malware te verminderen door meer softwarediversiteit te creëren. Om dat mogelijk te maken, moeten organisaties het idee loslaten dat de uitwisselbaarheid van informatie afhangt van het gebruik van dezelfde software. In plaats daarvan moeten organisaties durven te vertrouwen op gegevensstandaarden. Het gebruik van open standaarden garandeert bovendien dat elektronisch gearchiveerde gegevens in de toekomst opnieuw kunnen worden verwerkt.

Het SIS-model kan voorspellen wat het effect is op de verspreiding van malware als de software populatie meer divers wordt gemaakt. Stel dat het gedeelte (q) van de populatie immuun wordt gemaakt voor de huidige exploits die gericht zijn op de

marktleidende software, bijvoorbeeld door te migreren naar alternatieve software. Als de hoogte van (q) de positie van de marktleidende software niet aantast, blijft verreweg de meeste malware daarop gericht. Dat betekent dat de rest van de populatie (1 – q) marktleidende producten blijft gebruiken en vatbaar blijft voor het gros van de exploits. Door het vervangen van (i + s = 1) met (i + s + q = 1) in [1] verandert de besmettingssnelheid:

[4] $\partial i/\partial t = \beta is - \gamma i = \beta i(1 - i - q) - \gamma i$

Door de diversiteit aan software te vergroten, zullen exploits gericht op de marktleidende software zich dus langzamer verspreiden, omdat het aantal 'vruchtbare' contacten in de populatie vermindert met (βiq). Dit creëert meer reactietijd voor de software branche om op nieuwe malware te reageren. Voor de eindtoestand uit [2] geldt dan:

[5] $R_0 s_{min} = 1 = R_0(1 - i_{max} - q)$
$\rightarrow \quad i_{max} = 1 - q - 1/R_0$

In de eindsituatie neemt dus zowel het aantal vatbare computers als het aantal besmettingen af met (q). Als (q) groter of gelijk is aan de (i_{max}) van een malware variant, dan sterft deze malware gegarandeerd uit. Ook als ($q < i_{max}$) is de nieuwe waarde van imax verhoudingsgewijs lager dan de afname van het aantal vatbare computers (1 – q). Het effect van software compartimenten is grafisch weergegeven in figuur 3.

Als ($q < i_{max}$) daalt de besmettingsdruk ($F_{max} = i_{max} = \beta - \gamma - \beta q$) voor de hele populatie met ($-\beta q$). In de oude situatie [2] was Fmax = ($\beta - \gamma$), dus zelfs binnen de vatbare populatie (1 – q) daalt de besmettingsdruk:

[6] $F_{max} = \beta i_{max}/(1 - q)$
$= (\beta - \gamma - \beta q)/(1 - q)$
$= \beta - \gamma - \gamma q/(1 - q)$

Stel dat de populatie verdeeld is twee typen software, A met 80% marktaandeel en B 20%. Het is eenvoudig in te zien dat (q = 0,8) voor het compartiment B. Met andere woorden, een besmetting gericht op dat compartiment B kan zich maar moeilijk verspreiden en dooft hoogstwaarschijnlijk snel uit. Besmetting van computers met software B gebeurt in de praktijk alleen via injectie van malware, nauwelijks door onderlinge sociale contacten.

Met deze berekening is meteen het effect van meer standaardisatie op marktleidende software bekend. Door in [5] en [6] de term (–q) te vervangen door (+q) wordt duidelijk dat daardoor (i_{max}) en de besmettingsdruk (F) toe zullen nemen.

INJECTIE VAN MALWARE

Het hier gebruikte SIS-model neemt aan dat de besmettingen al egaal verdeeld zijn over het netwerk, maar dat geldt alleen voor malware die zich al enige tijd aan het verspreiden is. Daarom kan het model niet worden gebruikt voor de beschrijving van de injectie van nieuwe malware in de populatie, omdat daarvoor de topologie van de bron-knooppunten van essentieel belang is. Dit geldt ook voor wormen en de distributie van malware via webservers (*drive-by* exploit). Hoe meer contacten een malware bron heeft, des te groter is de kans dat een besmetting kan worden overgedragen. Het aantal knooppunten dat een directe relatie heeft met de bron(nen) is gelijk aan de som van het aantal verbindingen (k) van het aantal ingezette malware bronnen. Als (n) het totaal aantal vatbare computers is, dan is de kans (p) dat een malware bron een nieuwe exploit (j) kan overdragen dus:

[7] $p_j(1^e \text{ besmetting}) = \beta j \Sigma_m k_m/n$
$p_j(\text{GEEN } 1^e \text{ besmetting}) = (1 - \beta j \Sigma_m k_m/n)$

Hierbij staat K_m voor het aantal verbindingen van bron-knooppunt (m) dat ingezet wordt voor de verspreiding van een exploit. De index (m) geeft aan dat cybercriminelen gelijktijdig meerdere bronnen kunnen inzetten voor de verspreiding van exploit (j). De kans dat een bron de besmetting kan overdragen is overigens gelijk aan het verwachte deel van de populatie dat direct vanuit de bron wordt besmet. Het deel van de populatie dat door GEEN van de exploits wordt besmet, is het product van alle kansen dat elke individuele exploit de besmetting niet kan overdragen.

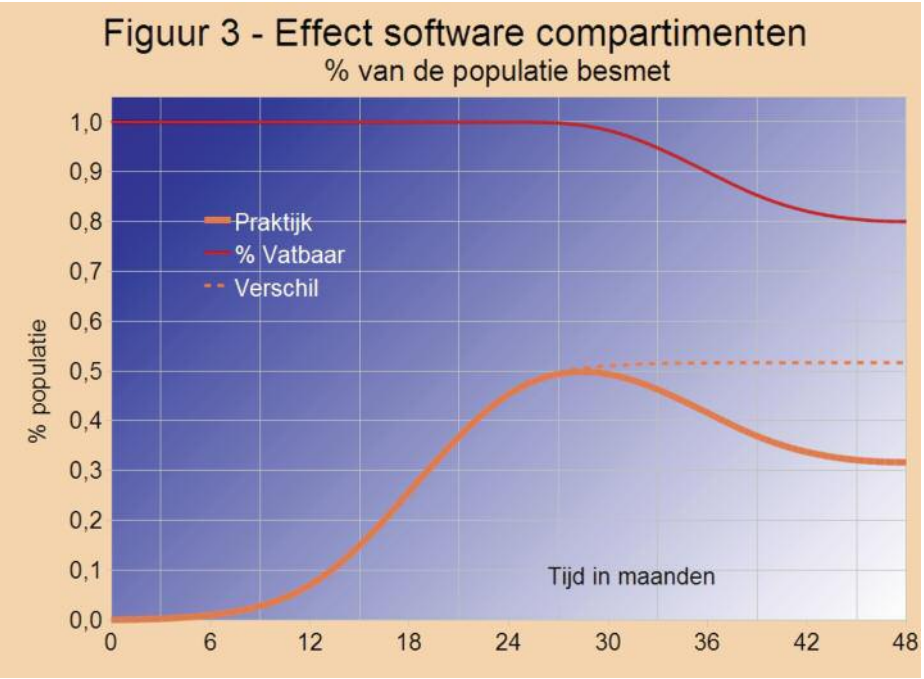
Stel dat er elke maand (c) nieuwe exploits bijkomen. Het deel van de populatie dat als eerste wordt besmet door één of meer van deze nieuwe exploits bedraagt daarom (nogmaals overgaan op complementaire kans):

[8] $\partial i_c/\partial t = 1 - \prod_c(1 - \beta_j \Sigma_m k_m/n)$

Formule [8] kan worden vereenvoudigd tot (βcv) met de volgende aannames:
Stel dat β en het aantal verbindingen van de bron-knooppunten voor alle exploits gelijk is, Stel dat de spreidingsfactor ($v = \Sigma_m k_m/n$) voor alle exploits gelijk is en << 1.

Om zo veel mogelijk computers te besmetten, verspreiden cybercriminelen hun malware via populaire (gehackte) websites, die een hoge waarde hebben voor $\Sigma_m k_m$. Hoewel ca. 300.000 nieuwe exploits per maand (= c) gering is ten opzichte van de miljarden internet knooppunten (n), kunnen zo toch veel computers snel worden besmet.
Daarnaast is het mogelijk malware te verspreiden via een tweetraps raket: besmette computers in een botnet-spam berichten laten versturen met malware. Omdat zo langzamerhand 90% van alle e-mails uit spam bestaat, krijgt vrijwel elke e-mail gebruiker regelmatig spam. Als 2 op de 100.000 ontvangers van een spam bericht ingaan op de 'aanbieding'[xxi], kan met ca. 100 miljard malware berichten per dag 2 miljoen computers worden besmet. En de hoeveelheid spam stijgt nog steeds.
Het effect van diversificatie is dat het (1 – q) gedeelte van de populatie vatbaar is voor een exploit met marktleidende software. Door dit te combineren met [4] en [5], wordt de totale groei van de infecties van bestaande (b) en nieuwe (c) malware dan:

[9] $\partial i/\partial t = di_b/\partial t + di_c/\partial t$
$= \beta i(1 - i - q) - \gamma i + \beta cv(1 - q)$



Zowel bij de initiële besmetting als bij het verder verspreiden van malware is software diversificatie dus zinvol, omdat de term (q) rechtstreeks terugkomt in de snelheid en omvang van de besmetting.

CONCLUSIE

Binnen de aangegeven restricties biedt het uitgebreide SIS-model inzicht in de effectiviteit van beveiligingsmaatregelen. Voor organisaties is het bijvoorbeeld zinvol om veilig thuiswerken te bevorderen door gedragsregels op te leggen en medewerkers de zakelijk gebruikte software te verstrekken. Het toepassen van freeware en open source software elimineert de extra licentiekosten daarvoor. Daarnaast is het aan te bevelen op zakelijke computers met een *white list* het gebruik van vreemde software van internet, USB of disk te blokkeren. Dat vermindert de kans dat malware op privécomputers zakelijke computers kan besmetten. Meer beveiligingskennis bij ondeskundige gebruikers vermindert het besmettingsgevaar in de volle breedte van de populatie, dus ook voor de partijen die op dit vlak wel deskundig zijn.

Gezien de ontwikkelingen zal het malwareprobleem in de nabije toekomst nog toenemen, zeker als cybercriminelen automatisch malware gaan genereren uit patches. Dergelijke aanvallen zal met name de veiligheid van organisaties onder grote druk zetten die patches eerst willen testen. Omdat malware besmettingen met gangbare beveiligingsmaatregelen daardoor steeds minder te voorkomen zijn, doen organisaties er goed aan in hun procedures een *Incident Response Plan* op te nemen en hiermee te oefenen. In Nederland wordt gelukkig al uitgebreid geoefend met cyberaanvallen. Bedrijven die periodiek de software van (mogelijk besmette) computers geautomatiseerd terugzetten, verminderen daarmee hun malware risico.

Een software monopolie maximaliseert het economisch rendement van malware. Het gebruik van niet-marktleidende software vermindert het besmettingsgevaar, omdat voor malware het aantal 'vruchtbare contacten' afneemt. Bedrijven kunnen natuurlijk standaardsoftware kiezen, maar vanuit het oogpunt van cybercrime is het onwenselijk dat alle bedrijven dezelfde software gebruiken. Een voldoende hoog percentage computers met alternatieve software kan malwarebesmettingen uit laten sterven. Deze alternatieve software moet dan bij voorkeur Open Standaarden gebruiken om de uitwisselbaarheid en duurzame ontsluiting van informatie te garanderen.

Met dank aan Prof. Dr. ir. Robert Kooij, Faculteit Elektrotechniek, Wiskunde & Informatica TU Delft.

BRON:
Dit artikel wordt ondersteund door een aantal internetverwijzingen en bronvermeldingen.
Zie hiervoor de website van de VOV.

FOTO IMPRESSIE

EXCURSIE OP HR. MS. JOHAN DE WITT OP 6 SEPTEMBER 2010

Aan land gezet in Den Helder

Hr. Ms. Johan de Witt met landingsboot op de voorgrond

Rondleiding op Hr. Ms. Johan de Witt

Vakkundig uitleg op Hr. Ms. Johan de Witt

Foto's met dank aan de heer R. van der Starre en kap b.d. A.J.J. Buitendam