

Spyware en overige malware in de Benelux

André Post

High-low Research
Noordeinde 37
2514 GC Den Haag

In samenwerking met Symantec Benelux

November 2004

Inhoud

1 Inleiding	3
2 Opzet van het onderzoek	4
3 Onderzoeksresultaten	5
3.1 Enqueteresultaten	5
3.2 Malware penetratiegraad	6
3.3 Bestandsinfecties niveau	9
3.4 Computerinfecties niveau	10
4 Conclusie	12
5 Aanbevelingen	13
Appendix: Verklarende woordenlijst	14

1 Inleiding

In augustus en september 2004 is een onderzoek uitgevoerd naar de computerbeveiliging onder thuisgebruikers in Nederland, België en Luxemburg. De focus van dit onderzoek ligt op het duidelijk maken in hoeverre een computer besmet is met kwaadaardige software. Recentelijk is er onder deze noemer de term spyware toegevoegd. Reeds enkele jaren is er in de beveiligingsindustrie een discussie over de rol die spyware vervult. En vele beveiligingsexperts zijn het er over eens dat spyware moet worden beschouwd als kwaadaardig. Het is dan ook een logisch gevolg dat beschermingssoftware als Norton AntiVirus 2004, bescherming biedt tegen spyware. Binnen dit rapport wordt veel gebruik gemaakt van de verzamelnaam “malware”, waarmee alle kwaadaardige programmatuur wordt aangeduid. In dit rapport valt spyware dus ook binnen de malware definitie.

In hoofdstuk 2 wordt uitgelegd welke onderzoeksmethode is gehanteerd en met welk doel is gekozen voor die methode. In dit hele rapport wordt veel gebruik gemaakt van de term “Malware”, waartoe Spyware ook wordt gerekend. Malware is een samentrekking van de woorden “Malicious software” wat betekent “Kwaadaardige programmatuur”. De meest bekende voorbeelden van malware zijn virussen en wormen. De resultaten van het onderzoek naar malware wordt in hoofdstuk 3 gepresenteerd in drie onderwerpen, te weten:

1. Hoezeer zijn de onderzochte computersystemen geïnfecteerd door malware?
2. Welke malwares hebben de meeste bestanden geïnfecteerd?
3. Welke malwares hebben de meeste computersystemen geïnfecteerd?

Alle vormen van malware kunnen worden voorkomen door veilig gebruik te maken van de computer en het internet. De samenvattende conclusies zijn te vinden in hoofdstuk 4. Daarna volgen een aantal aanbevelingen die kunnen leiden tot veiliger computergebruik. De appendix sluit het rapport af met een verklarende woordenlijst.

2 Opzet van het onderzoek

Aan het onderzoek naar malware in de Benelux namen 200 personen deel die zich vrijwillig hadden aangemeld na een oproep in de dagbladen. Om een goed beeld te kunnen krijgen van de penetratiegraad van spyware waren vrijwilligers gevraagd die geen spyware filter gebruiken. De deelnemers hebben vervolgens Norton AntiVirus 2004 op hun computer geïnstalleerd. De deelnemers werden verzocht hun computer te scannen en de logbestanden op te sturen naar Symantec Benelux. Hieruit zijn vervolgens 140 valide logbestanden geanalyseerd. De door de deelnemers ingevulde vragenlijst over hun internetgebruik, zoals informatievergaring, regelen van bankzaken en productaankopen, is in de analyse meegenomen.

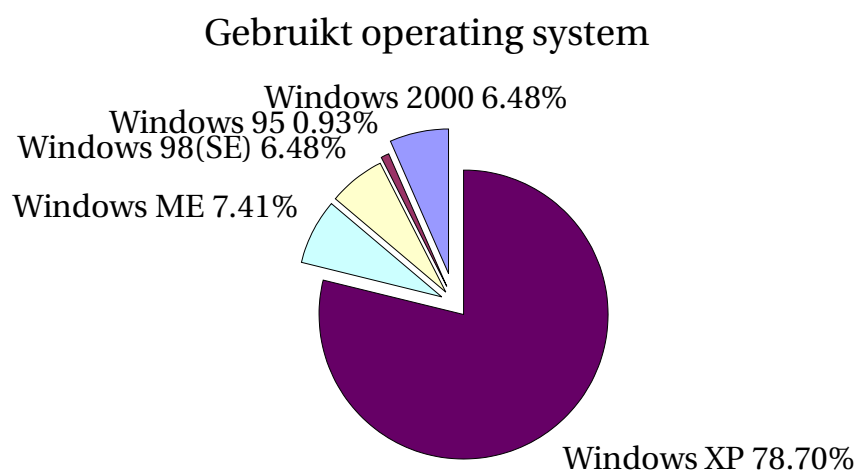
De onderzoeksresultaten zijn grotendeels gevonden door de ingezonden logbestanden te analyseren op aangetroffen malware. Om de meest optimale analyseresultaten te behalen is er speciale analysesoftware ontwikkeld voor dit project. De analyse zelf is uitgevoerd op een BSD gebaseerd operating system zodat de analysesoftware efficiënt en stabiel functioneert. Door op een dergelijk grondige wijze te werk te gaan is een goed beeld ontstaan van wat de gemiddelde beveiligingssituatie op het moment van dit schrijven is. Het volgende hoofdstuk presenteert de onderzoeksresultaten. Daarin zijn vele malware besmettingen met de aanduiding “Adware” te vinden. De overeenkomsten van adware met spyware zijn zo groot dat binnen dit rapport beide malwaregroepen worden aangeduid met “Spyware”. In de verklarende woordenlijst in de appendix is verder uiteengezet wat de termen spyware en adware precies inhouden.

3 Onderzoeksresultaten

In dit hoofdstuk worden de resultaten gepresenteerd die zijn voortgekomen uit de analyse van de enqueteresultaten en de logbestanden. In totaal zijn er 140 valide logbestanden ingezonden. Dit hoofdstuk is opgebouwd in vier paragrafen. Eerst worden de resultaten van de enquête gepresenteerd. Ten tweede wordt belicht hoe erg de onderzochte computers zijn geïnfecteerd en door welke typen malware. Daarna wordt nader gekeken naar de specifieke malware bedreigingen die het meeste worden aangetroffen. Hierbij zijn er twee invalshoeken: Het aantal geïnfecteerde computers en het aantal geïnfecteerde bestanden.

3.1 Enqueteresultaten

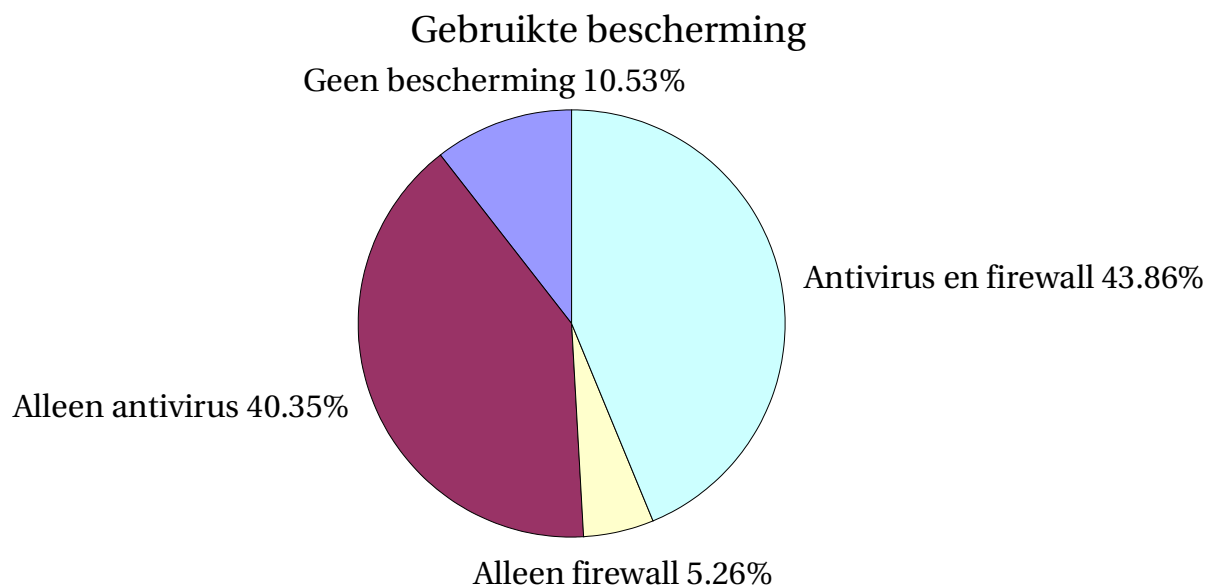
Uit de enquête is een aantal zaken naar voren gekomen die in het kader van dit onderzoek extra informatie verschaffen. Hieruit is gebleken dat 79% van de ondervraagden informatie verstuurt van vertrouwlijke aard zoals credit card gegevens, bankzaken, wachtwoorden, etc. Hieruit blijkt het belang om op systeemniveau en op netwerkniveau goed beschermd te zijn. De bescherming van informatie wordt extra belangrijk in het licht van spyware, dat poogt om informatie te versturen over het internet. Bijna alle malware is ontworpen om op Windows systemen te functioneren. In figuur 1 is de verdeling te zien in het gebruik van operating system.



Figuur 1: De gebruikte operating systems.

Oudere operating systems worden door de fabrikant daarvan meestal niet meer bijgewerkt op nieuw ontdekte beveiligingsgaten. Ook bevatten

nieuwere operating systems de mogelijkheid om bijgewerkt te blijven. Met een bijgewerkt operating system kan veel malware worden geweerd, maar met extra beveiligingssoftware wordt malware nog minder ruimte gegund. In figuur 2 is weergegeven welke bescherming wordt gebruikt door de deelnemers.



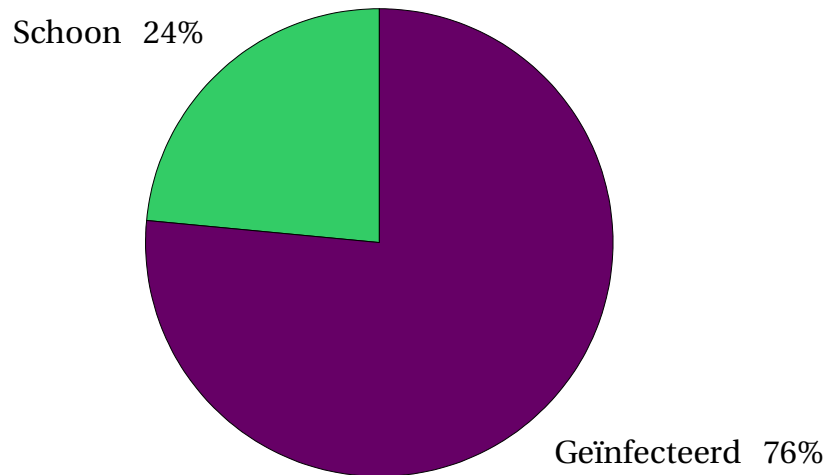
Figuur 2: De verdeling tussen gebruikte beschermingsmethoden.

Hieruit is af te leiden dat de meeste mensen de noodzaak van een antivirus pakket wel inzien. Opvallend is dat het aantal firewallgebruikers aanzienlijk lager ligt. Een firewall is voor iedere netwerkende computer een belangrijk preventief gereedschap tegen vele soorten malware die zich over het internet verspreiden. Om goed tegen spyware beschermd te zijn is een spywarefilter noodzakelijk. Van de ondervraagden ervaart 79% spyware als een bedreiging. Deze resultaten vullen de analyseresultaten van de logbestanden aan die in de volgende paragrafen worden gepresenteerd.

3.2 Malware penetratiegraad

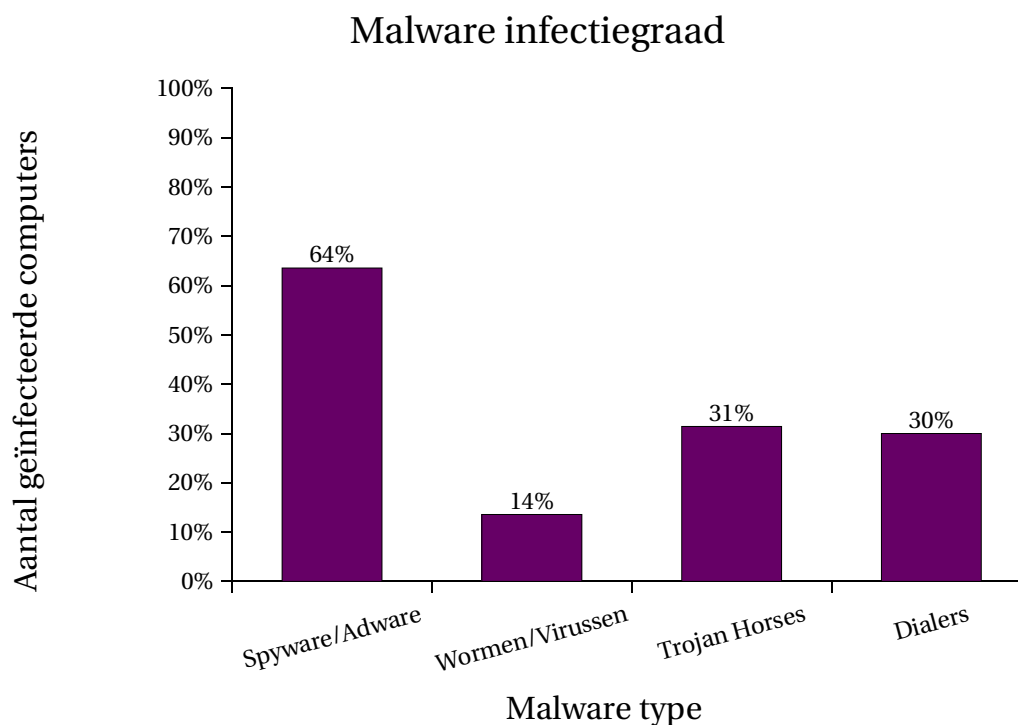
De logbestanden lieten zien dat 76% van de onderzochte computers geïnfecteerd is met een vorm van malware. Dit geeft een indicatie van hoe ernstig malware is doorgedrongen tot de computers van gemiddelde eindgebruikers. Dit had voorkomen kunnen worden door bewuster veilig gebruik te maken van de computer en het internet. Aanbevelingen hiertoe zijn te vinden in hoofdstuk 5 “Aanbevelingen”. In figuur 3 is de verhouding tussen geïnfecteerde en schone computers weergegeven.

Geïnfecteerde computers



Figuur 3: De verhouding tussen geïnfecteerde en schone computers.

Dat de meerderheid is geïnfecteerd met malware vraagt om een nadere kijk op de specifieke malware soorten. Daardoor wordt duidelijk gemaakt op welke malwaregroepen op dit ogenblik de grootste bedreiging vormen. De infectiegraad van de malware typen spyware, wormen, Trojan horses en dialers, is in figuur 4 weergegeven. In de verklarende woordenlijst in de appendix is verder uiteengezet wat de term dialer precies inhoudt.



Figuur 4: Relatief aantal geïnfecteerde computers per malware type.

Uit de analyseresultaten kunnen de volgende conclusies worden getrokken:

- Spyware vormt de grootste infectiegroep
- Bijna een derde van de gebruikers heeft een Trojan horse
- Bijna een derde van de gebruikers heeft een Dialer

Een ander opvallend detail is dat er nog steeds een aanzienlijk aantal computers met wormen is geïnfecteerd; ongeveer één op de zeven computers. Gezien de grote aandacht vanuit de media voor wormuitbraken is dit een redelijk hoog aantal dat in combinatie met de nog hogere overige infectiegraden, erop duidt dat de gemiddelde computer onvoldoende beveiligd is tegen malware.

De afgelopen jaren is er steeds meer aandacht voor spyware. Vanuit de beveiligingsindustrie zijn er steeds vaker waarschuwingen tegen spyware. Dat 64% van de gemiddelde eindgebruiker een spyware geïnfecteerde computer bezit is een bevestiging van de verwachting dat spyware een steeds grotere rol gaat spelen. Dit betekent ook dat beveiligingssoftware heeft moeten evolueren om deze bedreiging het hoofd te kunnen bieden.

De derde bovengenoemde trend is de opvallend hoge infectiegraad van dialers. Dialers gedragen zich enigszins als een Trojan horse en proberen om een duur telefoonnummer te bellen vanuit de computer. De manier waarop een dialer op een computer terecht komt is via een website. Wanneer een

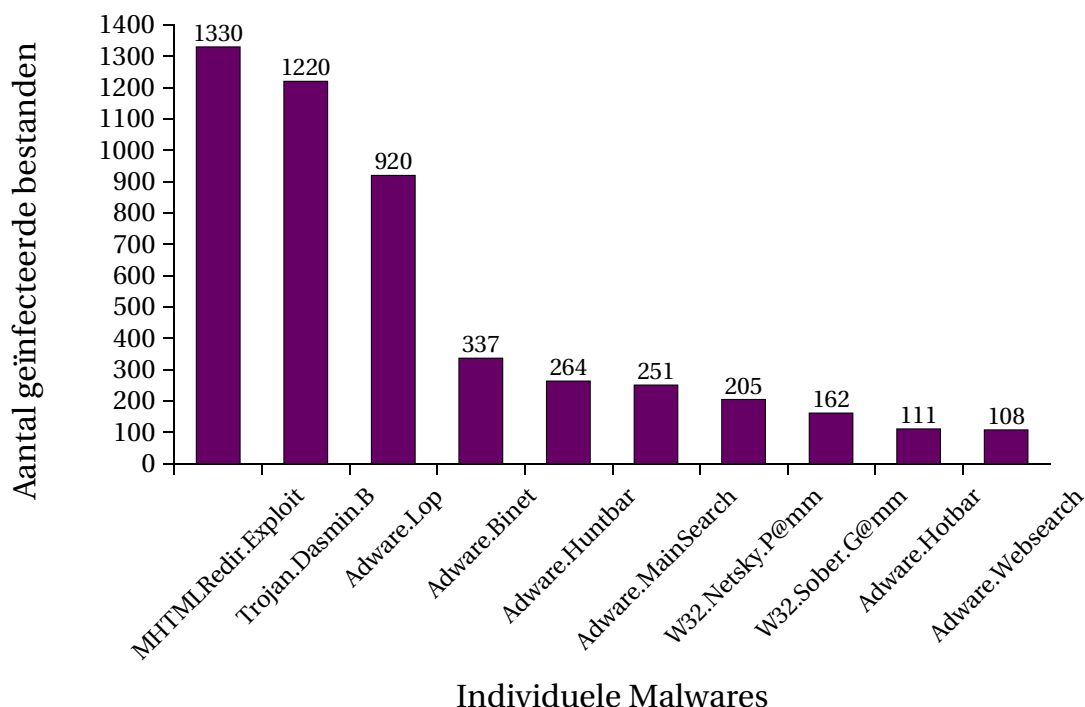
gebruiker een website bezoekt, is het mogelijk dat er met die website een programma wordt meegestuurd. De maker van een website kan dus ook een kwaadaardig programma zoals een dialer meesturen. Afhankelijk van de instellingen van de gebruikte browser en operating system, is het mogelijk om vervolgens onopvallend en automatisch de dialer op de computer te zetten.

3.3 Bestandsinfecties niveau

Om te achterhalen welke malware het ergste is zijn de logbestanden op twee manieren geanalyseerd. De ene manier is om te zien welke malware de meeste bestanden heeft geïnfecteerd en de andere manier is om te zien welke malware de meeste computers heeft geïnfecteerd. De eerste van deze twee methodes wordt in deze paragraaf behandeld.

In figuur 5 zijn de 10 meest agressieve malwares weergegeven met het aantal bestanden dat een ieder van hen heeft geïnfecteerd. Hierin komen veel bedreigingen met de “Adware” aanduiding naar voren zoals dat door Norton AntiVirus 2004 is gedetecteerd. Deze bedreigingen kunnen worden gezien als zijnde spyware. Met “agressief” wordt bedoeld dat deze malwares het meest succesvol zijn in het infecteren van zoveel mogelijk bestanden op de computer waarop ze terecht komen.

Top-10 Bestand Infecties



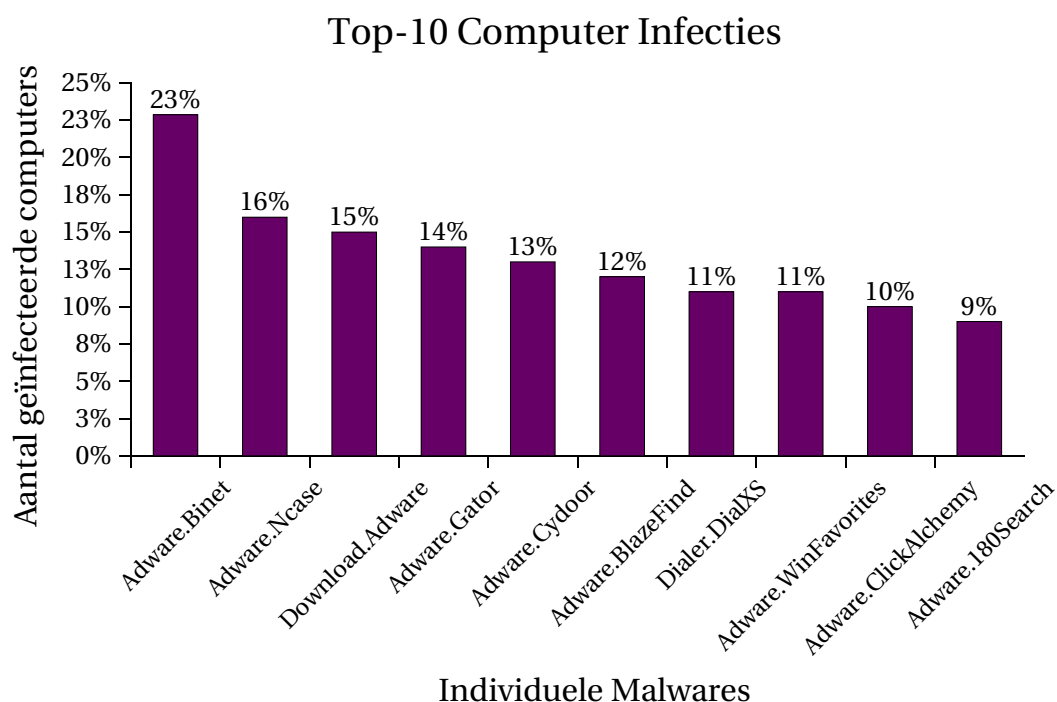
Figuur 5: Aantal geïnfecteerde bestanden per individuele malware.

In deze lijst wordt de top-3 gevormd door “MHTMLRedir.Exploit”, “Trojan.Dasmin.B” en “Adware.Lop”.¹ Deze bedreigingen werden aangetroffen op respectievelijk twee, één en acht computers. Dit betekent dat de kans op besmetting door MHTMLRedir.Exploit en Trojan.Dasmin.B zeer klein is, maar op de systemen die wel besmet zijn, zijn ook heel veel bestanden geïnfecteerd.

3.4 Computerinfecties niveau

In deze paragraaf worden de analyseresultaten behandeld waarbij gekeken is naar malware die de meeste computers heeft geïnfecteerd. De malwares die de meeste computers hebben besmet zijn in figuur 6 weergegeven.

¹ Informatie over specifieke bedreigingen is te vinden op de Internet site <http://securityresponse.symantec.com/avcenter/vinfodb.html>



Figuur 6: Aantal geïnfecteerde computers per individuele malware.

In paragraaf 3.2 is uit figuur 4 al duidelijk dat spyware de meeste besmettingen veroorzaakt. Het is echter wel bijzonder opvallend, dat negen van de tien grootste besmetters spyware zijn. Alleen de zevende plaats wordt ingenomen door een dialer, wat op zich ook opvallend is gezien de methode waarop dialers op een computer terecht kunnen komen.

Vrijwel alle malware infecties kunnen worden voorkomen door preventieve maatregelen te treffen. In het hoofdstuk 5 worden hiertoe een aantal aanbevelingen gedaan.

4 Conclusie

Uit de enquête is gebleken dat 78,70% van de gebruikers WindowsXP gebruikt en het overige is een verzameling oudere Windows versies. Van de ondervraagden zei 11% geen beschermende maatregelen te treffen, 40% alleen een antivirus pakket te gebruiken, 5% alleen een firewall te gebruiken en 44% gebruikt een antivirus pakket in combinatie met een firewall. 79% van de ondervraagden verstuurt informatie van vertrouwelijke aard zoals credit card gegevens, bankzaken, wachtwoorden, etc. 79% van de ondervraagden ervaart spyware als een bedreiging.

In totaal zijn er 140 valide logbestanden ingezonden en geanalyseerd. De logbestanden lieten zien dat 76% van de onderzochte computers besmet is met malware. De exacte besmettingsgraad per malwaregroep is als volgt:

64% is besmet met spyware
14% is besmet met wormen en/of virussen
31% is besmet met een Trojan horse
30% is besmet met een dialer

Opvallende resultaten die uit de analyse naar voren komen zijn:

- Spyware vormt de grootste infectiegroep
- Bijna een derde van de gebruikers heeft een Trojan horse
- Bijna een derde van de gebruikers heeft een Dialer

De drie malwares die de meeste bestanden besmet hebben zijn:

1. MHTMLRedir.Exploit
2. Trojan.Dasmin.B
3. Adware.Lop

Deze bedreigingen werden aangetroffen op respectievelijk twee, één en acht computers. Dit betekent dat de kans op besmetting door MHTMLRedir.Exploit en Trojan.Dasmin.B zeer klein is, maar op de systemen die wel besmet zijn, zijn ook heel veel bestanden geïnfecteerd.

Van de tien malwares die de meeste computersystemen hebben besmet, behoren er negen tot de groep van spyware. De enige bedreiging die in die lijst niet tot de spywaregroep behoort, is een dialer. En ook dat is een opvallend feit, gezien het besmettingsgedrag van de verscheidene malware klassen.

5 Aanbevelingen

Wat kan er worden gedaan om malware tegen te houden? Dit hoofdstuk probeert hier antwoord op te geven door een aantal aanbevelingen geven. Sommige aanbevelingen zijn eenvoudiger op te volgen dan andere, maar de preventieve werking die hiervan uitgaat kan de gebruiker veel leed en frustratie besparen.

In het verleden is gebleken dat de beste manier om malware te ontcrachten, is om een ander operating system te gaan gebruiken. Vandaag de dag is het verschil in gebruik tussen Windows, MacOSX en Linux varianten zo klein, dat dit voor veel gebruikers een optie kan zijn. Hierbij moet echter wel in gedachten worden gehouden dat dergelijke overstappen in het verleden malware slechts tijdelijk heeft geremd. Daarom is het altijd raadzaam om extra beveiligingssoftware te gebruiken.

Afhankelijk van de individuele gebruikerswensen kunnen er afwijkingen zijn, maar over het algemeen kan er veel leed worden voorkomen door het volgende in acht te nemen:

- Gebruik zoveel mogelijk automatische update methoden voor zowel het operating system alsmede geïnstalleerde programmatuur. Hierdoor worden beveiligingsgaten gedicht die anders gebruikt zouden kunnen worden om de computer te misbruiken. Een voorbeeld hiervan is WindowsUpdate.
- Wees bekend met de instellingsmogelijkheden van het gebruikte operating system en geïnstalleerde programmatuur. Hierdoor kunnen standaardinstellingen worden aangepast die mogelijk een beveiligingsrisico vormen. Een voorbeeld hiervan is het niet toelaten van ActiveX vanuit de browser.
- Weet wat voor software er op de computer is geïnstalleerd en installeer alleen nieuwe programma's waarvan het bekend is wat het doet. Lees daarbij ook de gebruikersovereenkomst daarvan.
- Gebruik extra beveiligingssoftware zoals antivirussoftware, firewalls en spywarefilters om de risico's nog verder te verlagen. Moderne scanners zoals Norton AntiVirus 2004 beschermen naast virussen, wormen en Trojan horses ook tegen spyware en adware.
- Zorg ervoor dat de beveiligingssoftware ook zo goed mogelijk bijgewerkt wordt met de laatste updates. Beveiligingssoftware dat niet wordt bijgewerkt kan maar weinig bijdragen aan de verlaging van de risico's.

Appendix: Verklarende woordenlijst

Adware

Adware vertoont grote overeenkomsten met spyware. Het grootste onderscheid tussen spyware en adware is te vinden in de manier waarop informatie wordt verzameld. Spyware gaat actief op zoek naar informatie op het computersysteem van de gebruiker en stuurt dat terug naar de uitgever. Adware presenteert de gebruiker met reclame waarbij informatie wordt verstuurd over de reactie van de gebruiker op de verscheidene reclames. Hierdoor kan de uitgever een profielschets maken van de gebruikers.

Browser

Een programma waarmee internetsites kunnen worden bekeken. Bekende browsers zijn Mozilla, Firefox, internet Explorer.

Dialer

Dialers zijn een subklasse van Trojan horse die proberen om een duur telefoonnummer te bellen vanuit de computer. De makers van de dialers proberen op die manier economisch voordeel te behalen met behulp van deze kwaadaardige programmatuur. De meeste computers die internettoegang hebben zullen geen analoge modem meer gebruiken, maar er is nog steeds een groep die dat wel doet. Als één van die computers een dialer infectie heeft, dan zal de eigenaar een enorm hoge telefoonrekening krijgen. Het blijkt in dergelijke gevallen heel moeilijk om de geleden financiële schade teniet te doen.

Malware

De term malware is een samentrekking van de Engelsche woorden “*Malicious software*” dat betekent kwaadaardige software. Malware is de verzamelnaam voor alle vormen van kwaadaardige software. Virussen en wormen zijn de meest bekende vormen van malware.

Spyware

Spyware is programmatuur die via het internet informatie verstuurt naar de uitgever van het spyware programma². Over het algemeen kan spyware omschreven worden als software met twee gezichten:

1. Naar de gebruiker toe presenteert het zich als een handig programma met bruikbare functionaliteit.
2. In het verborgene verzamelt het allerlei informatie en verstuurt die informatie naar de uitgever van de spyware.

Computergebruikers installeren spyware vanwege de interessante functionaliteit, zonder zich ervan bewust te zijn dat ze te maken hebben met

² Meer informatie over spyware is te vinden in “The Dangers of Spyware”
<http://securityresponse.symantec.com/avcenter/reference/dangers.of.spyware.pdf>

een programma dat onopvallend informatie verzamelt en verstuurt. Die informatie wordt vaak gebruikt voor commerciële doeleinden zoals direct marketing of handel in informatie. De technische implementatie van spyware biedt het de mogelijkheid om alle informatie die zich op de computer bevindt, te verzamelen en te versturen. De verzamelde informatie kan dus bestaan uit bijvoorbeeld persoonsgegevens, creditcard gegevens, computerspecificaties, maar ook surfgedrag en downloadgedrag. Veel mensen stellen prijs op hun privacy en zullen het spyware product nooit gebruikt hebben als ze geweten hadden dat het informatie verstuurt. De manier waarop spyware en adware op de computers komen van de gebruiker is eenvoudig: Via een website wordt de bruikbare functionaliteit gepresenteerd en kan de spyware worden gedownload. In veel gevallen gratis. Een gebruiker downloadt het programma en installeert het op de computer. Meestal staat er in de gebruikerovereenkomst (“End User License Agreement”) wel een verwijzing naar het vergaren van informatie, maar de meeste gebruikers lezen dergelijke overeenkomsten niet.

Trojan horse

Een Trojan horse is een programma dat zich voordoeft als goedaardige of onschuldige software, terwijl het in werkelijkheid kwaadaardige acties onderneemt.

Virus

Een virus is software dat zich zonder toestemming vermenigvuldigt van computerbestand naar computerbestand.

Worm

Een worm is software dat zich zonder toestemming vermenigvuldigt van computersysteem naar computersysteem. Wormen maken hierbij vaak gebruik van internetverbindingen om zich snel op grote schaal te verspreiden.