

Malware

Pure computercriminaliteit

Wees op uw hoede!



Computerclub Delft
voor tips en info

Febr. 2009

Als het gaat om virusbestrijding, komt de term malware steeds meer in beeld. Het is een nieuwe vorm van computercriminaliteit. De zoveelste poging om onze privacy aan te tasten of om gegevens te stelen. Het woord malware is een samenvoeging van het Engelse *malicious software* (kwaadwillende software). Malware is geen op zichzelf staand virus. Nee, we hebben hier te maken met een verzamelnaam voor kwaadaardige software, met als doel schade aan te richten bij degene die software installeren. Bekende voorbeelden die onder de noemer malware vallen zijn virussen, wormen, Trojaanse paarden, rootkits en spyware.

Computervirussen en malware

Een computervirus is een programma dat is ontworpen om zich van de ene computer naar een ander te distribueren. Computervirussen bestaan al meer dan twintig jaar. Van simpele programma's die zichzelf kopiëren van computer naar computer, zijn virussen geëvolueerd tot malware in vele verschijningsvormen. Waar virussen vroeger bestanden wisten of harde schijven vernielden, worden virussen (ook Trojaanse paarden en wormen) tegenwoordig steeds meer gebruikt om financiële gegevens te stelen of grootscheepse aanvallen te plegen.

Malware presenteert zich vaak als een programma of zit daar in verborgen. Vermomt als een plugin om "die fantastische video" af te spelen. Of in de nieuwste player, die je 'Hier' kunt downloaden. Volgens de laatste berichten is ook Photoshop CS4, verspreid via BitTorrent, besmet met malware. Omdat malware (als programma) vaak onder de vleugels van software meelift, wordt het niet als zodanig herkend door anti-virus- en/of anti spyware programma's. En als ze überhaupt deze cybercriminaliteit ontdekken is het te laat: de computer is al besmet.

Omdat malware, zoals eerder vermeld, aanwezig is in verschillende verschijningsvormen, zullen we eerst de meest voorkomende de revue laten passeren.

Wormen

Een **worm** is een programma dat zichzelf verspreidt, bijvoorbeeld door een kopie van zichzelf op elke gedeelde harde schijf op hetzelfde netwerk te installeren. Een worm is daarnaast geprogrammeerd om een bepaalde actie uit te voeren, zoals het installeren van een achterdeur op geïnfecteerde systemen zodat die door de verspreider van de worm kunnen worden gecontroleerd.

Tegenwoordig verspreiden de meeste wormen zich door zichzelf als bijlage aan een e-mail toe te voegen (die ze dan meestal ook zelf automatisch versturen). De ontvanger denkt dan een legitieme e-mail te krijgen omdat de afzender bekend is.



Het belangrijkste verschil tussen een virus en een worm is dat een worm zich zelfstandig verspreidt en een virus niet. Een virus verspreidt zich alleen maar wanneer de gebruiker een geïnfecteerd bestand of programma opent. Een worm kan zich al verspreiden als de computer alleen maar aan staat.

Virussen

Vaak worden de termen 'virus' en 'worm' door elkaar gebruikt. Een **virus** lijkt qua functionaliteit op een worm, maar verspreid zichzelf niet automatisch. Een virus hecht zich aan een bestaand programma (of document) en kopieert zichzelf pas wanneer dit programma wordt uitgevoerd. Een virus kan zich ook hechten aan het besturingssysteem ('bootsector virus') en wordt dan automatisch actief zodra de computer opstart.



Trojaanse paarden

Een **Trojaans paard** is een programma met kwade bedoelingen dat zich voordoeft als legitieme software. Een geïnstalleerde screensaver die stiekem alle bestanden uit de map 'Mijn documenten' verstuurt naar een server, is een Trojaans Paard. Een ander voorbeeld: een programma dat wordt geadverteerd als een verbetering van Internet Explorer, maar tevens een stukje software installeert waarmee de computer op afstand te besturen is, is ook een Trojaans Paard.



In tegenstelling tot virussen en wormen verspreidt Trojaanse paard-software zichzelf niet. Deze software wordt door gebruikers doorgegeven die niet doorhebben dat de software niet legitiem is. Trojaanse paard-software richt meestal hooguit indirecte schade aan, bijvoorbeeld door andere software te installeren. Meestal zal dit hooguit kunnen worden gezien als een hulpmiddel voor computervredebreuk.

Rootkits

Een **rootkit** draait ongemerkt op de computer van het slachtoffer en verbergt bepaalde activiteiten die daarop plaatsvinden. Zo kan een rootkit bijvoorbeeld de aanwezigheid van een virus verhullen, door besmette bestanden te laten zien alsof ze dat niet zijn. Een rootkit kan ook een achterdeur verborgen houden, waarmee de inbreker later gemakkelijk de computer binnen kan dringen of op afstand besturen.

Rootkits wordt vaak als onderdeel van andere malware geïnstalleerd. Zo kan een Trojaans paard of een worm bijvoorbeeld een rootkit met zich meedragen en deze bij het slachtoffer installeren.

Rootkits zijn doorgaans zeer moeilijk te verwijderen. Daar is speciale software voor nodig en geoefend personeel.

Achterdeuren

Een **achterdeur** ('backdoor') is precies wat de naam aangeeft: een programma dat toegang biedt tot de computer waarop het is geïnstalleerd. Vaak wordt achterdeur-software of *backdoors* geïnstalleerd door wormen of Trojaanse paarden. Ze houden zich meestal verborgen door gebruik te maken van rootkit-technieken.

Via de achterdeur kan de computer op afstand worden bestuurd. Een veel gebruikte toepassing hiervan is het versturen van reclame-mail (spam). Ook kan hiermee bijvoorbeeld een verstikkingsaanval worden uitgevoerd. Als de aanvaller dit met veel computers tegelijk doet, is de aanval bijzonder lastig te stoppen door het slachtoffer. Zo'n verzameling computers die voorzien zijn van achterdeuren wordt ook wel een **botnek** genoemd, omdat ze in wezen als een netwerk van willoze robots ingezet kunnen worden door de beheerder van de software. Vanwege de willoosheid heten de slachtoffers soms ook wel *zombies*.

Spyware

Spyware geeft stiekem gegevens over de gebruiker of diens PC door aan derden. Zo zijn er programma's die het surfgedrag van gebruikers bijhouden en dat doorgeven aan een centrale site, die zo passende advertenties kan aanleveren.

Niet elk programma dat gegevens doorstuurt, is spyware. Veel software biedt de mogelijkheid

tot registratie. Als het expliciet gevraagd wordt, en de gebruiker kan weigeren, dan is het geen spyware. Zou de software zelfstandig de naam en het e-mail adres van de gebruiker opsturen zonder dit te melden, dan was het wel spyware.

Deze opsomming van computercriminaliteit is slechts een deel van de bedreigingen waar u, als argeloze gebruiker, aan kunt worden blootgesteld. Het zou te ver gaan om alle virusvarianten hieraan toe te voegen. De hier beschreven vorm van kwaadwillende software zult u het meest tegenkomen. Het is dan ook van groot belang, vreemd gedrag van uw computer tijdig te onderkennen.



Help! Mijn computer doet vreemd

Bekende klachten van ernstig geïnfecteerde computers zijn:

- ◆ Er verschijnen voortdurend ongevraagde (vaak pornografische) advertenties
- ◆ De startpagina van de internetbrowser wordt steeds gewijzigd
- ◆ Er is ongevraagd een zoekbalk in de internetbrowser verschenen
- ◆ Er verschijnen nieuwe icoontjes op het bureaublad
- ◆ De computer werkt, maar reageert langzaam
- ◆ De computer loopt regelmatig vast
- ◆ De internetverbinding loopt traag
- ◆ De computer sluit zich na bepaalde tijd (bijvoorbeeld 60 sec.) automatisch af
- ◆ U ontvangt meer ongewenste e-mail (spam)

Houdt de ellende buiten de deur

Uit bovenstaande opsomming moge duidelijk zijn dat een goede beveiliging van uw computer onontbeerlijk is. Minimaal goede anti-virus software en even zo belangrijk een goed anti-spyware programma mag op geen enkele computer ontbreken.

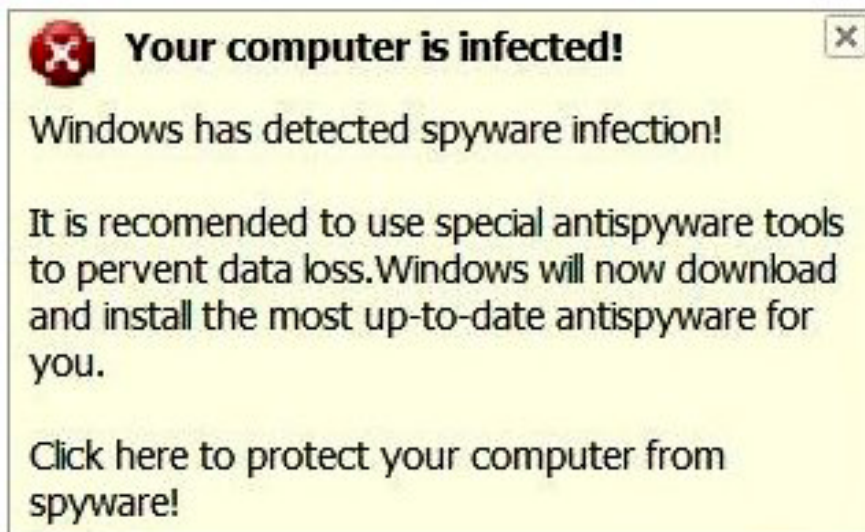
Betekent dat nu, dat u er verder geen omkijken meer naar hebt? Nee, allerm minst. Evenals de bittere noodzaak beveiligingsupdates voor het Windows besturingssysteem binnen te halen, geldt dat ook voor de virus-, en spyware updates van de geïnstalleerde software. Laat deze optie automatisch uitvoeren op een, door u gekozen, tijdstip of bij aanvang van het scannen.

Wel schadelijk zijn de nep anti-spyware programma's die op een onbewaakt ogenblik op uw beeldscherm verschijnen. Zij doen zich voor als anti-spyware (zoals het beruchte XP Antispyware 2009), maar zelf de problemen veroorzaken. Wij kunnen dat het best illustreren met een praktijkvoorbeeld.

Your computer is infected!

Ineens popups met reclame, websites die niet meer bezocht kunnen worden, en dan een systeemmelding dat Windows spyware heeft aangetroffen. Op de vraag of je anti-spyware software wilt downloaden, antwoord je "ja" en Windows installeert een programma met een neutrale naam (bijvoorbeeld XP Antispyware 2009).

Deze checkt, je systeem en komt met een schrikbarende lijst spyware en andere rommel die op je computer is geïnstalleerd. Deze zijn helaas alleen te verwijderen als je online een betaalde versie aanschaft. Omdat er met de laptop of pc niet meer te werken valt (sites zijn niet meer te bezoeken, de e-mail ontvanger werkt niet meer en je wordt gek van alle popups en spyware-meldingen), ga je maar over tot aanschaf van het programma. Dit programma is in staat alles weg te poetsen. Wat een topsoftware!



Helaas, je bent er ingetrapt. Op een slinkse manier is er een nep antispymware programma op je computer terecht gekomen. Dit programma heeft een design dat regelrecht bij de ontwikkelafdeling van Microsoft vandaan lijkt te komen. Hierdoor zien de meeste mensen het aan voor een onderdeel van Windows en volgen braaf de instructies op die gegeven worden. Tot aankoop aan toe.



Deze misleidende programma's zijn een groot probleem op internet aan het worden. Als je nagaat dat volgens een onderzoek 3,3 procent van de mensen in de betaal-val trapt, en zo'n programma al snel een paar tientjes kost, is het duidelijk dat er heel veel geld aan deze misleiding verdient wordt. Betalen wordt sterk afgeraden. Zo stimuleer je niet alleen dit bedrog, maar vaak helpt het ook weinig. Criminelen die deze programma's verspreiden zijn veel te blij met hun betalende slachtoffers om deze zonder slag of stoot te laten gaan. Ze kunnen de computer ongemerkt besmet houden, om op een later tijdstip een nieuwe truc er op los te laten.

Valse Youtube-filmpjes installeren malware

Cybercriminelen versturen via Youtube links naar valse filmpjes om malware te verspreiden met het bestand AutodeleteG. De afzenders sturen berichten met onderwerpen als '*Hans 1983 heeft je een bericht gestuurd vanaf Youtube*'. In de berichten staat vervolgens dat de ontvanger gefilmd is door een verborgen camera. De link in deze berichten lijkt te leiden naar een Youtube video, maar zorgt in werkelijkheid voor installatie van kwaadaardige software.

Volgens het detectie- en analyselaboratorium Padalabs gaat het om een Trojaans paard dat de computer openstelt voor installatie van andere malware. Volgens de directie van Pandalabs gebruiken criminelen wel vaker populaire diensten om zo het aantal slachtoffers te vergroten. "Zo geven ze de e-mail een vorm van authenticiteit".

Hoe kan dat nou?

Na het lezen van dit artikel moge het duidelijk zijn dat het gevaar vaak in een klein hoekje schuilt. Met slecht twee muisklikken kunt u al ernstig besmet raken. Werkt u met betrouwbare software en surft u selectief over het world wide web, dan komt u zelden voor verrassingen te staan. Het gevaar ligt op de loer als u commerciële sites bezoekt die met naam en faam niet zo goed bekend staan of als u software, games en muziek download van peer to peer netwerken. De controle is ook weg als meerdere huisgenoten gebruik van de computer maken. De virus- en spyware-scanner zullen elke bedreiging correct registreren, maar het gevaar schuilt vooral in de steeds toenemende malware. Dat mag duidelijk zijn.

Besmetting op deze manier ontstaan is moeilijk te verwijderen. Daar is speciale software en veel ervaring voor nodig.

Een lijst met namen die gebruikt worden door nep anti-virus programma's

Advanced Anti Virus	Power Antivirus 2009
AdvancedPrivacyGuard	RapidAntivirus
AdvancedPrivacySuite	Security Scanner 2008
Andromeda AntiVirus	Smart Antivirus 2009
AntiMalware 2009	SpyDevastator
Antimalwareshield	Spyware Guard 2008
AntiMalwareSuite	Spyware Preventer
AntiSpyControl	Storage Protector
AntiSpyware Pro XP	SystemOptimizer 2008
Antispyware XP 2008	SystemOptimizer2008
Antivir64	Total Secure 2009
Antivirus 2010	Ultimate Antivirus 2008
Antivirus Lab 2009	VirtualPC Guard
Antivirus Protection	VirusGuardPlus
AntivirusDoc	VirusResponse Lab 2009
Cleaner2009	Vista Antivirus 2008
ContentEraser	Win Antivir 2008
eAntivirusPro	Windows Antivirus 2008
Internet Antivirus	Winprotector
Micro Antivirus 2009	Xp Antispyware 2009
MS Antivirus (2008)	XP Protector 2009
PC Virusless	XPert Antivirus Enterprise
PersonalAntiSpy	XP-Guard

