

Internetbedreigingen in 2002

*De belangrijkste gebeurtenissen,
trends, en verwachtingen voor 2003*

André Post
High-low Research
In opdracht van Symantec Ltd.

www.symantec.nl

www.high-low.net

Inleiding

Dit rapport beschrijft de belangrijkste internetbedreigingen in 2002. Alvorens de gebeurtenissen van 2002 te behandelen, wordt eerst een overzicht van de situatie in 2001 geschetst. Hierdoor is het duidelijk hoe de internetomgeving eruit zag toen 2002 begon.

Situatie eind 2001

In 2001 vond een grote verandering plaats op het gebied van internetbedreigingen, namelijk de ondergang van Visual Basic Script wormen en de opkomst van Blended Threats, de zogenoemde gecombineerde aanvallen. Visual Basic Script wormen waren afhankelijk van social engineering om mensen ertoe te krijgen de attachment van een geïnfecteerd e-mail bericht te openen. Blended Threats zijn dusdanig ontworpen dat ze misbruik maken van programmeerfouten in bepaalde software om zich zonder menselijke tussenkomst te kunnen activeren. In de tweede helft van 2001 hadden CodeRed en W32.Nimda.A@mm de hele internetwereld een krachtig signaal gegeven door te bewijzen dat het Blended Threats concept werkt. Al snel bleek dat een worm alleen kans op verspreiding maakt als het een Blended Threat is. Eind 2001 verwachtte Symantec dat Blended Threats in 2002 verder terrein zouden winnen. Op langere termijn verwachtte Symantec dat mobiele devices als PDA's en Pocket PC's vaker aangevallen zouden worden.

Impact voor consumenten en bedrijven

Met de opkomst van de Blended Threats in 2001 werd internetbeveiliging veel complexer. De aard van Blended Threats maakte het ingewikkelder om computersystemen en netwerken vrij te houden van dergelijke bedreigingen. CodeRed had hoofdzakelijk succes op computers in het midden- en kleinbedrijf (MKB). Bedrijven in het MKB hebben vaak geen full-time IT personeel in dienst om de systemen beschermd te houden. Voor consumenten vormde CodeRed in eerste instantie geen gevaar, maar er volgden Blended Threats die vooral computers van consumenten geïnfecteerd hebben, zoals W32.Nimda.A@mm, W32.Badtrans.B@mm, W32.Klez.H@mm en W32.Yaha.F@mm. Het verspreidingsgedrag van de gemiddelde Blended Threat is zodanig dat bedrijven gedurende de eerste week van uitbraak geïnfecteerd raken. Daarna blijft de Blended Threat nog hoofdzakelijk op computers van consumenten voortbestaan. Doorgaans zijn de eigenaren van deze computers zich er niet van bewust dat hun computer een worm bevat en zo een gevaar vormt voor andere internetgebruikers.

De belangrijkste gebeurtenissen van 2002

De belangrijkste internetbedreigingen in 2002:

- 22 januari - Chat sessie van Willem-Alexander en Maxima door hackers afgebroken.
- 17 april - W32.Klez.H@mm breekt wereldwijd uit.
- 17 juni - W32.Yaha.F@mm verspreidt zich succesvol, met name in Nederland.
- 13 september - Linux.Slapper.Worm infecteert duizenden Linux computers.
- 14 september – Informatie over Miljoenennota wordt anoniem voortijdig op internet gezet
- 18 september – ‘verjaardag’ Nimda
- 30 september - W32.Bugbear@mm breekt wereldwijd uit.
- 21 oktober - De 13 hoofd DNS servers worden aangevallen door hackers.
- 28 oktober - De maker van de Kournikova worm wordt in hoger beroep veroordeeld.

Distributed Denial Of Service aanval op koninklijk huis

Op 22 januari zouden kroonprins Willem-Alexander en zijn aanstaande bruid Maxima een chatsessie hebben. Deze chat sessie was opgezet zodat zij via het internet persoonlijk contact zouden hebben met mensen die hen vragen konden stellen. Helaas waren er een aantal hackers die binnen een paar minuten vanaf het begin van de chatsessie een Distributed Denial Of Service aanval uitvoerden op de server die de chat sessie faciliteerde. Deze aanval bleek succesvol te zijn en de chat sessie werd vroegtijdig afgebroken.

De eerste grote worm uitbraak van 2002

Op 17 april breekt wereldwijd een nieuwe worm uit: W32.Klez.H@mm. Deze nieuwe variant van de W32.Klez familie maakt gebruik van verschillende aanvalstechnieken waardoor het zich bijzonder succesvol verspreidt. Deze worm zoekt in allerlei bestanden naar e-mail adressen waar het zichzelf vervolgens naartoe stuurt. Een nare bijkomstigheid is dat er ook een willekeurig bestand van de hard disk wordt meegezonden. Dit kan betekenen dat vertrouwelijke informatie openbaar wordt gemaakt. Binnen netwerken gaat deze worm op zoek naar andere computers om die rechtstreeks te infecteren. W32.Klez.H@mm zorgt er ook voor dat het afzenderveld in de e-mail wordt veranderd in één van de aangetroffen e-mail adressen. Vooral in de beginfase van de uitbraak leidde dit tot een aantal valse beschuldigingen. Ook deze worm is een Blended Threat die misbruik maakt van een programmeerfout om zichzelf te activeren zonder dat de ontvanger de attachment hoeft te openen. Een paar maanden later blijkt deze worm dusdanig schadelijk te zijn dat het W32.Nimda overtreft.

Nederland in het virusnieuws

Op 17 juni breekt de W32.Yaha.F@mm worm uit. Al snel blijkt dat deze worm zich in Nederland het meeste verspreidt. Na onderzoek blijkt er geen technische aanwijsbare reden te zijn waarom deze worm juist in Nederland zoveel schade aanricht. Net als W32.Klez.H@mm heeft ook W32.Yaha.F@mm een uitgebreid opsporingsmechanisme om e-mail adressen te vinden op de geïnfecteerde computer. Deze Blended Threat activeert zichzelf door de e-mail dusdanig te construeren dat de worm automatisch wordt geactiveerd.

Ook Linux servers doelwit van wormen

Op 13 september gebeurt iets dat systeembeheerders tot dat moment als voor onwaarschijnlijk hadden gehouden. De worm Linux.Slapper.Worm infecteert duizenden Linux servers door misbruik te maken van een programmeerfout in de serversoftware. Dit is de eerste grote uitbraak van een Blended Threat die gericht is op het Linux platform.

Cybersecurity in de politiek

Op 17 september wordt de Miljoenennota gepresenteerd en de verwachtingen zijn hoog gespannen, ook voor wat het nieuwe kabinet van plan is op ICT gebied. Een gedeelte van de ANP berichtgeving over de Miljoenennota wordt door de onbekende ‘nh2ba’ voortijdig op internet gezet. De actie zorgt voor enige commotie in de media en de dader blijft anoniem. De Miljoenennota beperkt zich op ICT gebied tot het bevorderen van ICT gebruik door de overheid zelf. Er is geen duidelijk waarneembare aandacht voor beveiliging op internet of het aanscherpen van de strafwet met betrekking tot hacken of virussen programmeren

en verspreiden.

Verjaardag Nimda

Op 18 september is W32.Nimda.A@mm exact 1 jaar actief en verspreidt zich nog steeds agressief. Hiermee bewijst deze worm dat Blended Threats moeilijk te verwijderen zijn van alle systemen wereldwijd.

De stilte doorbroken

Op 30 september breekt W32.Bugbear@mm uit. Na W32.Klez en W32.Yaha was dit de eerste grote uitbraak. Bugbear is net als alle andere succesvolle verspreiders in 2002 een Blended Threat. De worm heeft ook een achterdeur functionaliteit waarmee hackers toegang kunnen krijgen tot een geïnfecteerde computer. Het e-mail mechanisme waarmee deze worm zich verspreidt komt grotendeels overeen met dat van W32.Klez.H@mm en W32.Yaha.F@mm. De worm misbruikt dezelfde programmeerfout om zichzelf te activeren en zoekt ook op de computer naar e-mail adressen.

Aanval op DNS servers

Er zijn 13 hoofd Domain Name System servers die alle internet domein namen en hun corresponderende IP adressen bevatten. Op 21 oktober wordt er een Denial Of Service aanval uitgevoerd op deze 13 servers. Negen daarvan waren tijdens de aanval daadwerkelijk onbereikbaar geworden voor normale internetgebruikers. Deze servers kregen meer dan tien keer zoveel verkeer te verwerken dan wat normaal was. Het Amerikaanse federale onderzoeksburo (FBI) onderzoekt de aanval en heeft ontdekt dat de aanvallen werden uitgevoerd vanuit computers in de Verenigde Staten en Korea.

Maker Kournikova worm veroordeeld

Op 28 oktober wordt de maker van de Kournikova worm in hoger beroep veroordeeld tot 150 uur werkstraf. De maker van de worm, de Nederlander Jan de W., maakte begin 2001 de Kournikova worm met behulp van een worm generator programma en liet de worm vervolgens los. De worm verspreidde zich snel over de hele wereld. Kort daarop plaatste de virusschrijver een bekentenis op een website.

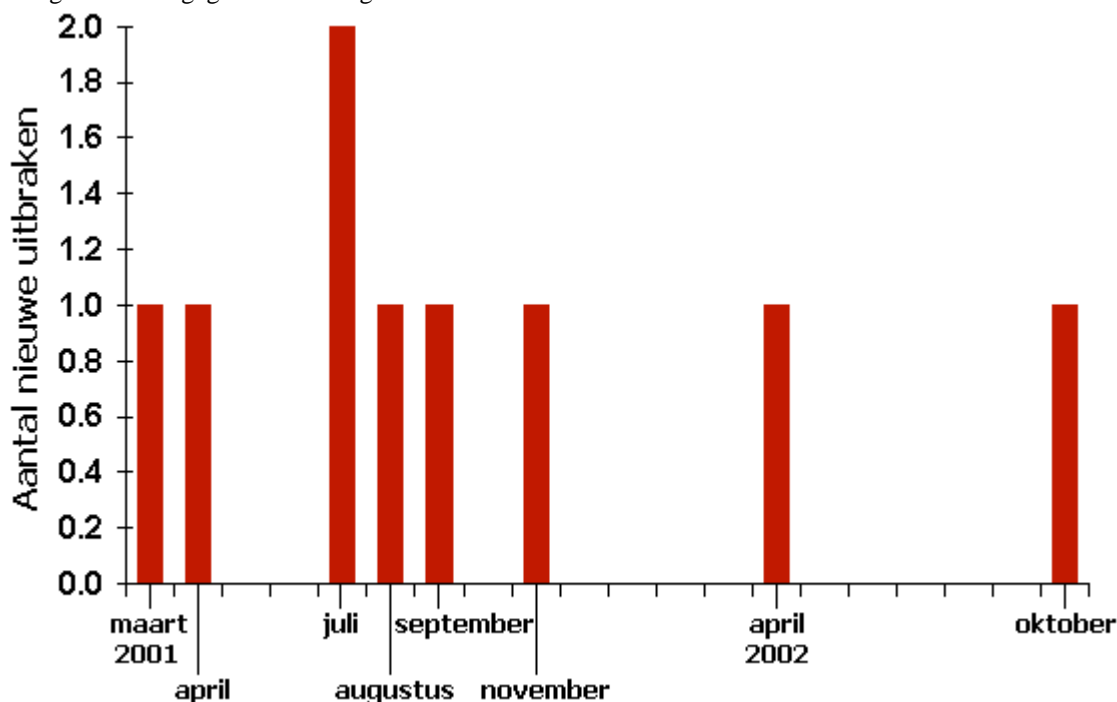
Trends en verwachtingen

Hackers krijgen meer aandacht voor Linux

Hackers zijn constant op zoek naar beveiligingsfouten in allerlei software. Tot en met 2001 was het duidelijk dat de Microsoft programmatuur de grootste aandacht trok voor dergelijke activiteiten. Regelmatig werd er verkondigd dat het Linux platform veilig is en 'de' oplossing zou zijn. In 2002 is er echter een duidelijk waarneembare trend waarbij hackers zich ook richten op het vinden van beveiligingsfouten in Linux software. En met succes. Het eerste bewijs hiervan werd op grote schaal geleverd door Linux.Slapper.Worm die vele duizenden Linux servers wereldwijd infecteerde. Deze situatie maakt duidelijk dat ook de Linux community niet immuun is voor kwaadaardige software zonder zich daartegen te wapenen. Ook Linux systemen moeten regelmatig worden ge-update en extra worden beveiligd.

Onverwachte stilte

2001 had de verwachtingen geschept dat er met grote regelmaat een nieuwe grote worm zou uitbreken. In 2002 werd duidelijk niet voldaan aan die verwachting. Nog steeds worden er iedere dag 10 tot 15 nieuwe virussen gemaakt, maar het overgrote deel daarvan is niet succesvol in verspreiden. Figuur 1 geeft weer wanneer er nieuwe grote worm uitbraken waren en daarin is goed te zien dat 2002 met aanzienlijk minder nieuwe grote worm uitbraken te maken had dan 2001. In april 2002 was het W32.Klez.H@mm en in oktober was W32.Bugbear@mm gegroeid tot een grote uitbraak.



Figuur 1: Het aantal nieuwe grote worm uitbraken tussen maart 2001 en oktober 2002 wereldwijd.

De wormen in figuur 1 zijn:

maart 2001: W32.Magistr.24876@mm

april 2001: VBS.Haptime.A@mm

juli 2001: CodeRed Worm en W32.Sircam.Worm@mm

augustus 2001: CodeRed II Worm

september 2001: W32.Nimda.A@mm

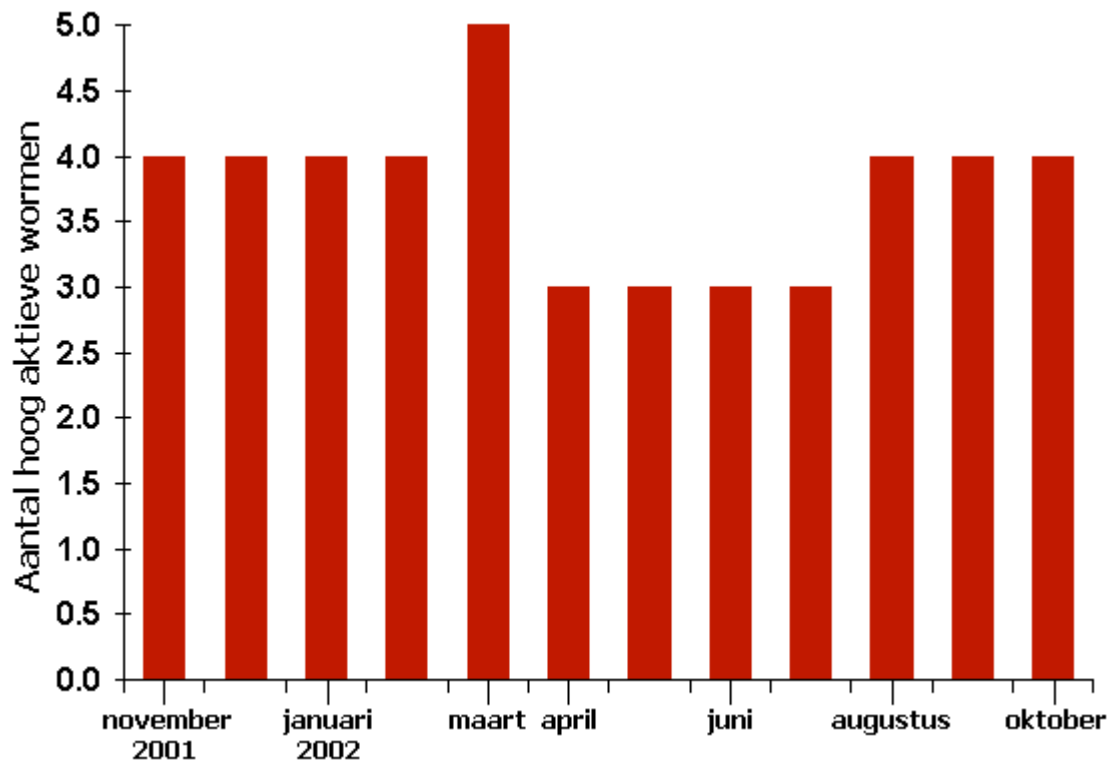
november 2001: W32.Badtrans.B@mm

april 2002: W32.Klez.H@mm

oktober 2002: W32.Bugbear@mm

Deze stilte in 2002 betekent echter niet dat er geen wormen actief waren gedurende de stille periodes van figuur 1. Alle grote worm uitbraken vanaf juli 2001 en later waren Blended Threats. De eigenschappen van deze

kwaadaardige software brengen met zich mee dat deze wormen zeer lang na kunnen blijven werken. De laatste jaren is duidelijk geworden dat er steeds meer bandbreedte van het internet verloren gaat aan dergelijke wormen. Het is dan ook steeds moeilijker om het internet schoon te houden. In figuur 2 is te zien dat een aantal grote worm uitbraken van 2001 gewoon door bleven werken in 2002.

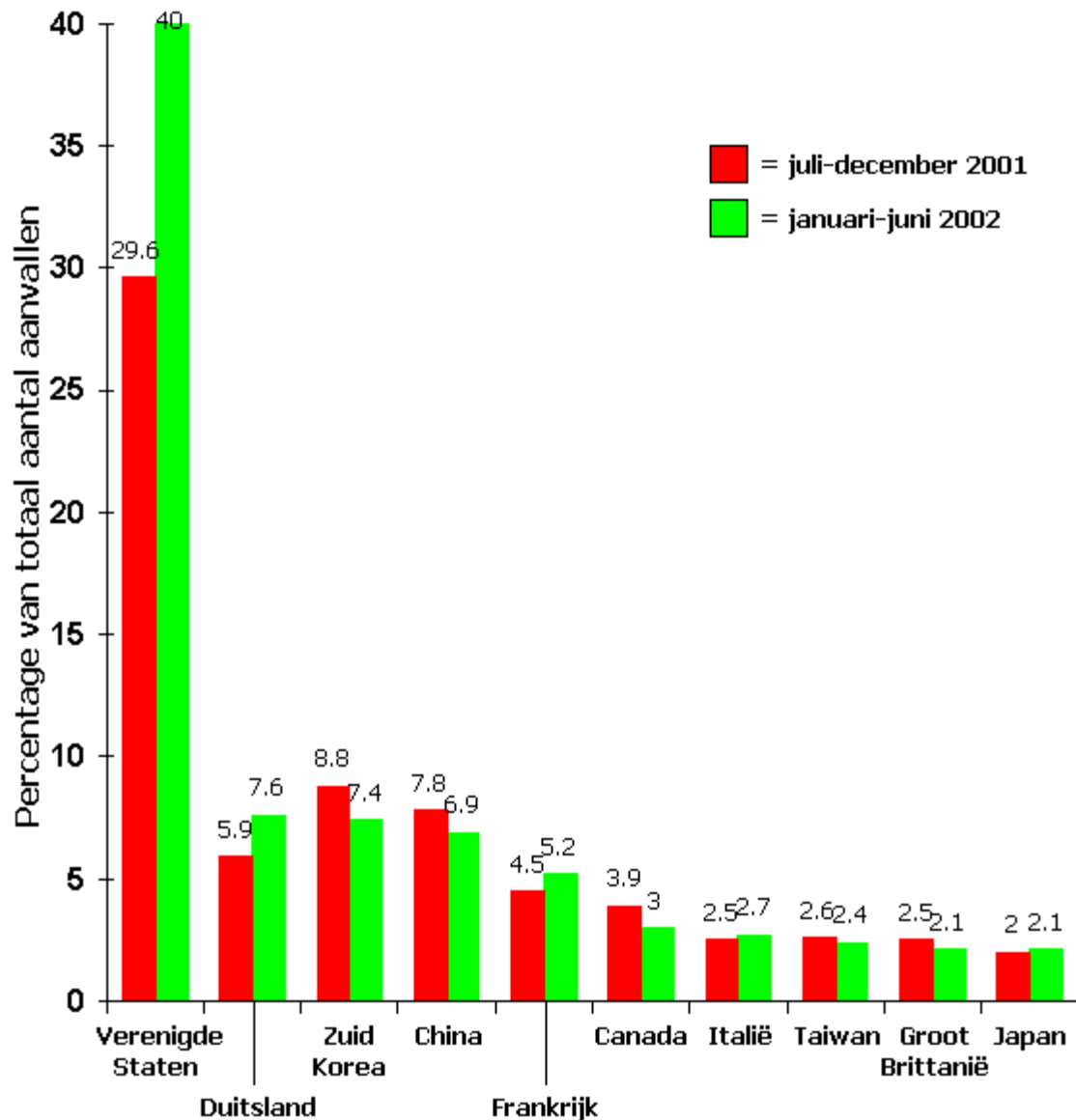


Figuur 2: Het aantal wormen die zich succesvol aan het verspreiden zijn.

Figuur 2 laat zien dat de grote wormen van 2001 zich nog steeds op grote schaal blijven voortplanten in 2002, ondanks de fictieve stilte. Symantec's verwachting in 2001 dat in 2002 de Blended Threats zouden overheersen blijkt geheel juist te zijn geweest. Alle grote worm uitbraken vanaf juli 2001 en daarna zijn Blended Threats.

Waar komen de meeste aanvallen vandaan?

Iedereen die aangesloten is op het internet is een potentieel doelwit van wormen en hackers en vrijwel iedereen krijgt dan ook te maken met aanvallen. De oorsprong van deze aanvallen is in kaart gebracht en figuur 3 toont de top 10 landen waar de meeste aanvallen vandaan komen. In vergelijking met de tweede helft van 2001 is de eerste helft van 2002 niet erg veranderd, met uitzondering van de Verenigde Staten waar het met meer dan 10% van het totaal aantal aanvallen toegenomen is. Ook al staan er vier Europese landen in deze top 10, hun totale aantal aanvallen is nog steeds minder dan de helft dan het aantal aanvallen in de Verenigde Staten.



Figuur 3: De top 10 landen van waaruit de meeste aanvallen worden uitgevoerd.

Peer-to-Peer

Uit een onderzoek dat in opdracht van Symantec in België is uitgevoerd, is gebleken dat Peer-to-Peer applicaties zoals Kazaa, Morpeus en Napster onder de consumenten wereldwijd enorm in populariteit zijn gestegen ten opzichte van eind 2001. Deze toename in Peer-to-Peer software gebruik is op zichzelf niet schadelijk, maar het verdient wel de aanbeveling om extra voorzichtig te zijn aangezien deze Peer-to-Peer netwerken kwetsbaar zijn en ook worden gebruikt voor kwaadaardige software zoals wormen en Backdoor Trojan Horses.

Spam

Spam e-mail is een toenemend probleem. Deze vorm van ongevraagde reclame per e-mail neemt steeds grotere vormen aan. Uit onderzoek van "Jupiter Media Matrix, 2002" is gebleken dat de gemiddelde e-mail gebruiker in 2002 meer dan 700 spam berichten zal ontvangen. Spam is niet altijd zonder risico. Het is al voorgekomen dat spam berichten vanaf een geïnfecteerde computer werden verstuurd. Spam berichten bevatten ook vaak een website adres waar zich mogelijk kwaadaardige code bevinden. Hiernaast kunnen spam berichten economische schade aanrichten door bijvoorbeeld illegale software aan te bieden of credit card gegevens op te vragen. Veel spam bevat informatie die ongepast is om door minderjarigen te worden gelezen.

Verwachtingen voor 2003

Op basis van de hiervoor genoemde ontwikkelingen, is het te verwachten dat Blended Threats voorlopig op de eerste plaats van kwaadaardige software blijven staan. Aangezien Blended Threats gebruik maken van verschillende aanvalstechnieken wordt het voor zowel consumenten als bedrijven steeds belangrijker om naast antivirus ook een firewall en intrusion detection te gebruiken. Met intrusion detection oplossingen kunnen veel Blended Threats onderschept worden nog voordat ze enige schade kunnen berokkenen. De lange termijn verwachting dat mobiele devices als PDA's en Pocket PC's vaker aangevallen zullen worden blijft bestaan. Die markt zal zich nog verder ontwikkelen totdat het op grotere schaal de aandacht heeft van kwaadwillende programmeurs en hackers.

Begrippenlijst

Backdoor Trojan Horse

Een Backdoor Trojan Horse is een programma waarmee een hacker ongeoorloofd toegang kan krijgen tot een computer.

Blended Threat

Een Blended Threat is een worm die misbruik maakt van programmeerfouten in bepaalde software om zichzelf met minimale afhankelijkheid van de gebruiker bij een computer naar binnen te hacken. Door gebruik te maken van gecombineerde aanvalstechnieken verspreiden Blended Threats zich zeer snel. Deze extra complexiteit vraagt ook weer om een geheel nieuwe aanpak van bestrijding; niet alleen antivirus software is nodig, maar ook een firewall en intrusion detection software.

Denial Of Service

Een Denial Of Service aanval is een digitale aanval op een computer waarbij er een groot aantal data-aanvragen worden verzonden. De aanval is succesvol wanneer de betreffende computer het dermate druk heeft met het afhandelen van die aanvragen dat er geen andere aanvragen meer kunnen worden gehonoreerd.

Distributed Denial Of Service

Een Distributed Denial Of Service aanval is een type Denial Of Service aanval waarbij de aanvaller gebruik maakt van meerdere computers. Meestal zijn deze computers door de aanvaller gehacked en zijn de rechtmatige eigenaren van deze computers er zich niet van bewust dat hun computer voor kwaadaardige doeleinden wordt gebruikt.

Peer-to-Peer

Peer-to-Peer software wordt voornamelijk gebruikt om allerlei bestanden uit te wisselen met andere gebruikers van die Peer-to-Peer software. Iedere gebruiker is via het internet verbonden met het Peer-to-Peer netwerk en op die manier kunnen alle gebruikers bestanden uitwisselen.

Spam

Spam is een vorm van reclame waarbij de reclameboodschap per email wordt verzonden en meestal krijgt de ontvanger deze berichten ongevraagd en ongewenst.

Worm

Een worm is software die zich probeert te verspreiden van computer naar computer over een netwerk. De verspreiding hiervan kan een dergelijke omvang aannemen dat dit de normale gang van zaken ernstig kan verstoren.