

Internetbedreigingen in 2003

De belangrijkste trends in 2003

Kwetsbaarheden*

- Het aantal kwetsbaarheden stijgt.
- De tijd tussen het ontdekken van kwetsbaarheden en het uitbreken van een aanval wordt steeds korter.
- Ongeveer 60% van alle kwetsbaarheden wordt binnen één jaar misbruikt.
- De aard van de kwetsbaarheden verandert. Meer dan 80% is uit te buiten op afstand. Een groot aantal is gericht op publieke diensten of algemene protocollen, die vooral worden gebruikt op intranet.

Blended Threats*

- Blended Threats waren in 2003 geheel volgens verwachting de grootste bedreiging.
- [W32.Bugbear.B@mm](#) is de grootste internetbedreiging van 2003 (zie top 10).
- Zes van de 10 grootste aanvallen zijn mass-mailing wormen* die zich snel verspreiden.
- De grootste bedreiging van 2002, [W32.Klez.H@mm](#), staat in de top 10 van 2003 nog altijd op de tweede plaats.

Payload*

- De payload verschuift van het verspreiden van een bericht en vernietigen van gegevens naar het naar buiten brengen van gegevens zoals wachtwoorden, creditcard nummers etcetera.
- Symantec Security Response heeft een toename van 50% vastgesteld van Trojaanse Paarden* met kwaadaardige code of *backdoors*, waarschijnlijk voor het naar buiten brengen van gegevens.

Spam*

- Spammers gaan dezelfde technieken gebruiken als virusschrijvers om spam te verspreiden.
- Spammers gebruiken alle beschikbare technologieën. Spammers gebruiken nu proxy servers die vaak op slachtoffersystemen staan die ADSL, kabel etc. gebruiken. Zo kunnen ze anoniem blijven en maakt het niet uit als één of twee systemen ontdekt worden. Het doel is immers om honderden of duizenden van deze gecontroleerde systemen (*bot nets*) te gebruiken.

De belangrijkste verwachtingen voor 2004

- Het aantal kwetsbaarheden blijft stijgen.
- Een zero-day attack* is niet onwaarschijnlijk. Voor een recente kwetsbaarheid van Cisco was binnen twee dagen een exploit* gecreëerd.
- Blended Threats blijven de grootste bedreiging, worden steeds complexer, zullen toenemen in volume en zich steeds sneller verspreiden.
- De kans bestaat dat we volgend jaar een aantal Blended Threats zien met vergelijkbare impact als Blaster en Slammer.
- Nieuwe bedreigingen en aanvallen worden verwacht op draadloze en mobiele devices, waarschijnlijk binnen een tijdsbestek van 2-5 jaar.
- De hoeveelheid spam blijft toenemen, onder andere door het gebruik van dezelfde verspreidingstechnieken als kwaadaardige code en virussen.
- Spyware vormt een toenemende bedreiging voor de privacy van de gebruiker.

Top 10 virussen/wormen in 2003 – wereldwijd

Gebaseerd op het aantal meldingen bij Symantec Security Response.

Aantal meldingen	Virus/Worm	% van totaal aantal meldingen
117,396	W32.Bugbear.B@mm	11.06%
82,763	W32.Klez.H@mm	7.80%
39,236	HTML.Redlof.A	3.70%
23,556	W95.Hybris.worm	2.22%
21,751	W32.Sobig.F@mm	2.05%
20,271	W32.Blaster.Worm	1.91%
17,700	W32.Swen.A@mm	1.67%
12,211	W32.Nimda.E@mm	1.15%
10,781	W32.Bugbear.B.Dam	1.02%
10,393	W32.Sobig.A@mm	0.98%

Top 10 kwetsbaarheden in 2003 - wereldwijd

- 1. Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability**
<http://www.securityfocus.com/bid/8205>
- 2. Microsoft RPCSS DCOM Interface Long Filename Heap Corruption Vulnerability**
<http://www.securityfocus.com/bid/8459>
- 3. Microsoft Windows ntdll.dll Buffer Overflow Vulnerability**
<http://www.securityfocus.com/bid/7116>
- 4. Sun Solaris SAdmin Client Credentials Remote Administrative Access Vulnerability**
<http://www.securityfocus.com/bid/8615>
- 5. Sendmail Address Prescan Memory Corruption Vulnerability**
<http://www.securityfocus.com/bid/7230>
- 6. Multiple Microsoft Internet Explorer Script Execution Vulnerabilities**
<http://www.securityfocus.com/bid/8577>
- 7. Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability**
<http://www.securityfocus.com/bid/9011>
- 8. Samba 'call_trans2open' Remote Buffer Overflow Vulnerability**
<http://www.securityfocus.com/bid/7294>

9. Microsoft Windows Locator Service Buffer Overflow Vulnerability
<http://www.securityfocus.com/bid/6666>

10. Cisco IOS Malicious IPV4 Packet Sequence Denial Of Service Vulnerability
<http://www.securityfocus.com/bid/8211>

De belangrijkste gebeurtenissen in 2003

Januari – De Slammer worm wordt ontdekt, een zeer schadelijke worm gericht op SQL servers, waardoor internet in principe volledig uitgeschakeld zou kunnen worden. In tegenstelling tot andere wormen, is Slammer niet gebaseerd op bestanden waardoor het zich snel kan verspreiden. De worm is gericht op systemen die draaien op Microsoft SQL Server 2000 en op Microsoft Desktop Engine (MSDE) 2000. De worm stuurt 376 bytes naar UDP poort 1434, de SQL Server Resolution Service Port. Slammer heeft een onbedoelde payload van een Denial-of-Service aanval vanwege het grote aantal pakketjes die hij verstuurt. Bedrijven zijn het belangrijkste doelwit van de Slammer worm, terwijl consumenten mogelijk geen toegang konden krijgen tot internet. Wereldwijd raken meer dan 75.000 hosts geïnfecteerd en gedurende een aantal uren is er vertraagde toegang tot internet. De omvang van Slammer verdubbelde elke 8,5 seconde gedurende de eerste minuut en binnen 10 minuten waren de meeste kwetsbare hosts allemaal geïnfecteerd.

De SoBig worm wordt voor het eerst ontdekt. Sobig is een mass-mailing network-aware worm die zichzelf stuurt naar alle e-mailadressen die hij vindt in documenten met bepaalde extensies. Alle volgende varianten van Sobig vervalsen ook het veld van de afzender. Het e-mailadres van de afzender wordt vervalst door een willekeurig e-mailadres te kiezen op de geïnfecteerde PC. Naast e-mailen op grote schaal geeft Sobig ook vertrouwelijke informatie vrij die soms wordt 'gestolen' van het systeem. SoBig en varianten zijn uniek vanwege de hard gecodeerde de-activeringsdata; zodra één variant gedeactiveerd wordt, wordt er direct een nieuwe variant gelanceerd.

Maart – De BAT911 worm wordt ontdekt. Deze worm gebruikt .bat bestanden en doorzoekt een reeks IP-adressen van bekende ISP's om een toegankelijke computer te vinden. Als een computer de C: schijf toegankelijk maakt en niet beschermd is met een wachtwoord dan kopieert de worm bestanden op die computer. BAT911.worm is uniek omdat hij de modem van het geïnfecteerde systeem gebruikt om 911 te bellen.

Juni – De Bugbear.B worm wordt ontdekt; het is een variant van de Bugbear.A worm. De worm is polymorfisch, bevat keystroke logging* en backdoor-capaciteiten en probeert verschillende antivirus en firewallprogramma's te beëindigen. De worm maakt gebruik van de 'Incorrect MIME Header Can Cause IE' om de kwetsbaarheid van de e-mailbijlage te activeren. Bij niet gepatchte systemen wordt de worm dan automatisch geactiveerd wanneer een bericht gelezen wordt (ook bij previewing). Hiernaast bevat de worm een lijst met meer dan 1300 domeinnamen van financiële instellingen. Als W32.Bugbear.B vaststelt dat de domeinnaam van het geïnfecteerde systeem toebehoort aan een bank, wordt auto-dialing geactiveerd. Hierdoor kan de computer zonder tussenkomst van de gebruiker verbinding maken met het internet. Auto-dialing, in combinatie met keystroke logging, is waarschijnlijk een poging om wachtwoorden effectiever te kunnen achterhalen. Bugbear.B behoort tot een nieuwe categorie e-mailwormen die

serieuze criminele activiteiten proberen te ontplooiën. Dit is een voorbeeld van diefstal van vertrouwelijke informatie.

Augustus – De Mimail worm wordt ontdekt. Mimail is een worm die zich verspreidt per e-mail en informatie steelt van de computer van de gebruiker. De worm verzamelt informatie van bepaalde schermen van de desktop en stuurt deze vervolgens naar bepaalde e-mailadressen. Mimail buit bekende kwetsbaarheden uit en de worm is verpakt in UPX. Ongebruikelijk aan Mimail is dat het zich verspreidt in de vorm van een zipbestand wat nogal wat inspanning vraagt van de gebruiker; die moet immers dubbelklikken om het bestand te openen en vervolgens de inhoud uitpakken. De worm is vooral succesvol omdat de kwetsbaarheden die hij misbruikt automatisch worden uitgevoerd. Hiernaast wordt effectieve social engineering gebruikt voor de verspreiding door zich voor te doen als een bericht betreffende het e-mailaccount van de gebruiker en dat afkomstig is van de systeembeheerder.

De Blaster worm wordt ontdekt. Blaster is een wijd verspreide worm die vereist dat ook thuisgebruikers een firewall en antivirussoftware gebruiken, en ook een update van Windows patches. De Blaster worm gebruikt de DCOM RPC met TCP poort 135. De worm besmet alleen Windows 2000- en Windows XP-systemen. Alhoewel Windows NT- en Windows 2003 Server-machines kwetsbaar zijn voor de genoemde exploit (als niet juist gepatched), is de worm niet gecodeerd om deze systemen te besmetten en te repliceren. Blaster voerde een Distributed Denial-of-Service* aanval uit op de Windows update site van Microsoft.

De Welchia worm wordt ontdekt. Deze is uniek omdat hij probeert systemen tegen Blaster te beschermen door een legitieme patch van de Microsoft website te downloaden. Onbedoeld effect van de Welchia worm was dat netwerken en systemen werden vertraagd of zelfs werden uitgeschakeld.

De Sobig.F worm wordt ontdekt. Het is een mass-mailing network-aware worm die zijn eigen SMTP engine gebruikt om zich te verspreiden. De Sobig.F worm maakt gebruik van e-mail spoofing, wat wil zeggen dat de worm een willekeurig e-mailadres zoekt op de computer en deze in het afzenderveld plaatst bij de verspreiding. Deze zesde variant van het Sobig virus is ook opmerkelijk omdat in de tweede fase blijkt dat er op bepaalde tijdstippen binnen een vastgesteld tijdsbestek een onbekende payload* zal worden gedownload door alle geïnfecteerde systemen. Dit werd voorkomen door het afsluiten van de downloadservers. Vooral consumenten en kleine bedrijven raakten besmet met Sobig.F.

September – De Swen.A worm wordt ontdekt. Het is een mass-mailing worm die zijn eigen SMTP engine gebruikt om zich te verspreiden. Het probeert zich te verspreiden via file-sharing zoals KaZaA en IRC, en probeert antivirus en firewall programma's op de computer uit te schakelen.

De worm kan binnenkomen als e-mailbijlage. Het onderwerp, de tekst en het adres van de afzender kan steeds variëren. Sommige berichten doen zich voor als patches voor Microsoft Internet Explorer, of als foutmeldingen van

gmail. De Swen.A worm maakt gebruik van een kwetsbaarheid in Microsoft Outlook en Outlook Express door zichzelf te activeren (execute) als gebruikers het bericht openen (ook bij preview). Het verspreidt zich snel onder thuisgebruikers vanwege de populariteit van peer-to-peer netwerken.

November – De Mimail.J worm wordt ontdekt. Het is een mass-mailing worm die probeert persoonlijke informatie te stelen van de thuisgebruiker. Het e-mailbericht van deze worm heeft als onderwerp 'Your PayPal.com Account Expires' en toont een aantal onechte formulieren van PayPal, een online betalingssysteem, die gebruikers vraagt om een creditcard nummer, de PIN die bij de kaart hoort, en de beveiligingscode. Deze informatie wordt opgeslagen en later verstuurd naar een aantal vooraf vastgestelde e-mailadressen. De Mimail.J worm is net als Bugbear.B een voorbeeld van een nieuwe trend waarbij hackers* niet zozeer willen opvallen maar een crimineel doel nastreven.

December – De Mimail.L worm wordt ontdekt. Het is geprogrammeerd om de websites van anti-spam organisaties te overspoelen met junk e-mail waardoor deze mogelijk ontoegankelijk worden voor legitieme bezoekers. De Mimail.L worm spoort ook ontvangers aan om de organisaties te overspoelen met e-mail door zich voor te doen als een bestelling voor kinderpornografie en een antwoord te vragen om te annuleren.

Begrippenlijst

Backdoor Trojan Horse

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

Blended Threats

Blended Threats zijn internetbedreigingen die meerdere methoden en technieken gebruiken om aan te vallen en zich te verspreiden. Blended Threats, zoals CodeRed of Nimda, zijn een combinatie van hacking, computerwormen, denial-of-service aanvallen en/of het defacen van websites.

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.

Andere vorm: Een Denial Of Service waarbij misbruik wordt gemaakt van een kwetsbaarheid in de server of dienst waardoor deze buiten werking gesteld kan worden.

Distributed Denial Of Service

Een Distributed Denial Of Service aanval is een type Denial Of Service aanval waarbij de aanvaller gebruikmaakt 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.

Exploit

Een manier om misbruik te maken van een kwetsbaarheid.

Hacking

Misbruik maken van de kwetsbaarheden, misconfiguratie of de schade aangericht door een ander virus om vervolgens toegang te krijgen tot een systeem.

Keystroke logging

Opslaan en/of versturen van alle aanslagen op het toetsenbord.

Kwetsbaarheid (Vulnerability)

Een 'bug' of programmeerfout in software.

Payload

Actiegedeelte van een virus, dat vaak pas na enige tijd in werking treedt.

Spam

Spam is een vorm van reclame waarbij de reclameboodschap per e-mail wordt verzonden. 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 zonder gebruik te maken van een bestand. De verspreiding hiervan kan een dergelijke omvang aannemen dat dit de normale gang van zaken ernstig kan verstoren.

Zero-day attack

Een individu ontdekt een kwetsbaarheid en ontwikkelt direct een kwaadaardige bedreiging (exploit) – in plaats van de leverancier in te lichten. Als de bedreiging actief wordt, is niemand ertegen beschermd omdat een patch niet beschikbaar is.