

## *Internetbedreigingen in 2005*

### **DE BELANGRIJKSTE TRENDS IN 2005**

#### **Gerichte aanvallen, botnetwerken, phishing en winstmotieven**

- Grootschalige aanvallen maken plaats voor kleinere, gerichte aanvallen op netwerkgebruikers en desktopsystemen.
- De online wereld wordt in toenemende mate gedomineerd door nieuwe dreigingen zoals botnetwerken (verder: botnets), modulaire kwaadaardige code en gerichte aanvallen op webapplicaties en -browsers.
- Aanvallen worden veelal gedaan uit winstbejag. Middelen: identiteitsdiefstal, afpersing of oplichting.
- Phishing heeft zich in 2005 ontpopt als dé methode voor het ontvreemden van vertrouwelijke gegevens

Enkele cijfers uit het Symantec Internet Security Threat Report (ISTR):

- Symantec nam het eerste halfjaar van 2005 gemiddeld 10.352 actieve botnetcomputers per dag waar, een toename van meer dan 140 procent.
- In het eerste halfjaar steeg het aantal DoS-aanvallen (Denial of Service) met meer dan 680 procent tot een gemiddelde van 927 per dag. Deze toename in DoS-activiteit is grotendeels te wijten is aan de gelijktijdige toename van de botnetactiviteit. Een van de belangrijkste functies van botnets is de uitvoering van DoS-aanvallen.
- In de eerste helft van 2005 maakte 64 procent van de 50 meest gerapporteerde stukken kwaadaardige code de verspreiding van spam mogelijk.
  - De omvang nam toe van gemiddeld 2,99 miljoen tot gemiddeld 5,70 miljoen berichten per dag.
  - De filters van Symantec Brightmail AntiSpam signaleerden gemiddeld meer dan 40 miljoen pogingen tot phishing per week, een cijfer dat in het begin van het jaar nog op 21 miljoen per week lag. In oktober lag het daggemiddelde net onder de 9000.
  - In de eerste helft van 2005 was kwaadaardige code die de vertrouwelijkheid van informatie schond verantwoordelijk voor 74 procent van de 50 meest gerapporteerde stukken kwaadaardige code. In oktober werd met 83 procent van de 50 meest gerapporteerde stukken kwaadaardige code de vertrouwelijkheid van informatie geschonden.

#### **Bedreigingen op niet-traditionele platforms\***

- Symantec onderschepte in oktober Trojan.PSPBrick – de eerste trojan-horse gericht tegen de Sony PlayStation Portable (PSP). Gebruikers moesten dan zogenaamd een applicatie installeren waarmee zij niet-Sony games op de PSP konden spelen. Eenmaal op de PSP geïnstalleerd via (bijvoorbeeld) een geheugenstick, wist het virus systeembestanden waardoor de game-machine onbruikbaar wordt.

## **Draadloos**

- Er bestaan nu 23 virusfamilies voor Symbian, vier voor Palm en twee voor PocketPC. Het gaat daarbij in totaal om 73 varianten. Er zijn 56 nieuwe varianten in Symbian-families ontdekt in 2005. In 2004 werden zeventien nieuwe varianten ontdekt.
- In augustus 2005 werd Car door een groep Europese experts in draadloze beveiliging Car Whisperer ontwikkeld met als doel om de tekortkomingen van een aantal Bluetooth-systemen aan te tonen. Car Whisperer maakt gebruik van het feit dat op veel van deze handsfree systemen slechts een toegangscode van vier cijfers vereist is. Veel autofabrikanten gebruiken dezelfde code voor al hun Bluetooth-systemen. Hierdoor is het voor Car Whisperer erg eenvoudig om audiobestanden uit te wisselen met de auto.
- In februari 2005 wist een hacker zich toegang te verschaffen tot het adressenbestand van de mobiele telefoon van Paris Hilton en een lijst met telefoonnummers en e-mailadressen te stelen. Deze gegevens zijn vervolgens op verschillende websites gepubliceerd. Sommigen menen dat de diefstal mogelijk was door een eenvoudig te raden wachtwoord; volgens anderen zou haar adresboek al in 2003 door dezelfde hacker zijn gestolen toen deze in het netwerk van haar provider inbrak. Eén van de meest waarschijnlijke verklaringen is dat de belager gebruik heeft gemaakt van een fout in de functie voor wachtwoordwijzigingen op de website van de provider.

## **Virusbedreigingen in 2005\***

- Er waren dit jaar in totaal maar 6 bedreigingen in de derde categorie (tegen 32 in 2004):
  - Sober.X in november
  - Zotob.E in augustus
  - Esbot.A in augustus
  - Sober.O in mei
  - MyDoom.AX in februari
  - Beagle.AZ in februari

Er waren in 2005 geen bedreigingen in categorie 4.

## Opkomende bedreigingen\*

### De opkomst van SMS-spam

De opkomst van SMS-mogelijkheden/-marketingtools op (Noord-Amerikaanse) websites zal waarschijnlijk leiden tot een enorme toename van SMS-spam in 2006.

- Mobiele spam is nu al een plaag voor veel gebruikers buiten de Verenigde Staten. Het Koreaanse staatsbureau voor informatiebeveiliging (KISA) kreeg 244.151 meldingen van mobiele spam tussen januari en oktober 2005, tegenover 78.063 meldingen in dezelfde periode van het voorafgaande jaar.
- De SMS-gateways van providers zouden een aanzienlijk deel van de spam moeten kunnen herkennen en tegenhouden, maar spammers zullen steeds brutaler worden en deze beveiliging weten te omzeilen. Men zal de ontwikkelingen op dit gebied goed moeten blijven volgen.
- Het gevaar voor massale SMS-aanvallen, waarbij de verzender SMS-berichten in zulke hoeveelheden verstuurt dat er sprake is van DoS (Denial of Service), is in principe geweken, omdat de providers dit gevaar grotendeels hebben opgelost op hun SMS-gateways. Bij een DoS-aanval wordt het apparaat of de service (e-mail- of SMS-inbox) overspoeld door berichten van een ander apparaat, waardoor het onmogelijk wordt om van de dienst gebruik te blijven maken.

### Bluetooth blijft zorgwekkend

De draadloze technologie van Bluetooth is bezig met een onstuitbare opmars. Volgens de Bluetooth Special Interest Group (SIG) doorbrak het aantal Bluetooth-leveringen in het tweede kwartaal van 2005 de grens van 5 miljoen per week, een getal dat in het derde kwartaal van 2004 nog op 3 miljoen lag. De meeste groei voor Bluetooth speelt zich af op de markten van mobiele telefoons en PDA's. Momenteel wordt 20 procent van de mobieltjes geleverd met Bluetooth. In het hogere zakelijke segment is dit aandeel zelfs nog groter. In 2006 zal de meerderheid van de nieuwe zakelijke telefoons zijn voorzien van Bluetooth. Door haar aanwezigheid van Bluetooth op pc's brengt deze technologie ook beveiligingsrisico's voor de pc-gebruikers met zich mee.

## **DE BELANGRIJKSTE VERWACHTINGEN VOOR 2006**

### **1. Nieuwe platformen onder vuur**

Ondanks de toevoeging van voorzieningen die aanvallen moeten voorkomen, zullen hackers nieuwe platformen blijven bestoken. Indringers blijven nieuwe wegen vinden om systemen te infiltreren.

### **2. Rootkits**

Het toenemende gebruik van heimelijke technologie, bijvoorbeeld in de vorm van rootkits, maakt deel uit van een natuurlijke evolutie in aanval-methoden. Hackers willen niet gesnapt worden, dus gebruiken ze methoden die een dekmantel verschaffen. Hoewel rootkits al langer bestaan, merkt Symantec dat ze steeds vaker gebruikt worden. Dezelfde tactiek is zichtbaar in gecodeerde virussen, waarbij versleuteling wordt toepast om virusscanners te misleiden.

### **3. Modulaire kwaadaardige code**

Sinds anderhalf jaar neemt Symantec een verontrustende trend waar in kwaadaardige codering. Schrijvers van kwaadaardige code maken gebruik van modules die zichzelf kunnen updaten. Deze zogenaamde modulaire kwaadaardige code is kwaadaardige code – wormen, virussen, trojans – die aanvankelijk maar beperkte functionaliteit heeft. Eenmaal geïnstalleerd op een belaagde computer worden echter andere stukken (modules) kwaadaardige code gedownload met andere functies waardoor de besmette computer verder wordt aangetast of wordt er bijvoorbeeld een DoS-aanval uitgevoerd.

### **4. Phishing**

Het gevaar van phishing blijft toenemen naarmate de belagers nieuwe slachtoffers kunnen gebruiken.

### **5. Adware/Spyware**

Omdat er steeds meer mobiele telefoons, PDA's en apparaten komen die genoemde functionaliteiten combineren (hybride apparaten), is het aannemelijk dat zij vaker het doelwit zullen zijn van beveiligingsrisico's zoals spyware en adware. Symantec verwacht dan ook een toename van de hoeveelheid spam die naar deze apparaten gezonden wordt.

### **6. Gevaren van VoIP**

VoIP (Voice over Internet Protocol) is snel bezig uit te groeien tot een veelgebruikt alternatief voor het traditionele analoge telefoonsysteem. Hoewel er tot nu toe weinig aanvallen op VoIP-systemen zijn gemeld, denkt Symantec dat het door de grootschalige acceptatie van deze nieuwe communicatietechnologie slechts een kwestie van tijd is voordat deze systemen zwaarder onder vuur zullen komen te liggen. Een mogelijk scenario is dat aanvallers vanuit IP toegang weten te krijgen tot conventionele telefoonstelsels via IP-PSTN-gateways.

### **7. Bedreigingen van minder traditionele apparatuur**

- In oktober heeft Symantec Trojan.PSPBrick onderschept – de eerste trojan die was gericht tegen de Sony PlayStation Portable (PSP). Gebruikers werden overgehaald om een bestand te installeren dat zogenaamd een applicatie was waarmee zij niet-Sony games konden spelen. Zij konden dit agressieve bestand

op hun computer downloaden en vervolgens met een geheugenstick overzetten naar de PSP. Het op de PSP geïnstalleerde virus verwijderde systeembestanden en maakte de gamecomputer onbruikbaar.

- Op dit soort nieuwe bedreigingen werd al een tijd geanticipeerd. Symantec verwacht meer aanvallen op niet-traditionele platforms in 2006.

## Begrippenlijst 2005

**Backdoors** ('achterdeuren') of **trap doors** ('valluiken') - zijn gaten in de beveiliging van een computersysteem, die opzettelijk open zijn gelaten door ontwerpers of beheerders. Een backdoor is een verborgen software- of hardwaremechanisme dat dient om beveiligingsmaatregelen te omzeilen. Dit soort programma's geeft een belager van buiten vrijwel onbeperkt toegang tot de besmette computer.

**Blended Threats/Gecombineerde Bedreigingen** - 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. Deze bedreigingen kunnen zich snel verspreiden, vaak zonder tussenkomst van de gebruiker, en veroorzaken aanzienlijke schade. Een effectieve bescherming tegen gecombineerde bedreigingen vereist een uitgebreide beveiligingsoplossing inclusief antivirus, firewall en 'intrusion detection' ofwel bescherming tegen indringers.

**Bot** (afgeleid van 'robot') - Is een computerprogramma dat heimelijk wordt geïnstalleerd op een systeem dat als doelwit fungeert. Het stelt een niet-geautoriseerde gebruiker in staat die computer op afstand te bedienen voor uiteenlopende doeleinden. Dankzij een bot kan de belager het systeem besturen via communicatiekanalen zoals IRC. Zo kan de externe belager een groot aantal besmette computers – die samen een **botnet** (of een **botnetwerk**) vormen – aansturen via één enkel betrouwbaar kanaal.

**Bot-netwerken** - Bot-netwerken, ook wel zombie-netwerken genoemd, ontstaan doordat programma's illegaal worden geïnstalleerd op doelwitsystemen waardoor een ongeautoriseerde gebruiker van afstand controle over de computer kan krijgen voor uiteenlopende doeleinden. Aanvallers coördineren vaak grote groepen bot-controlled systemen of bot-netwerken om het internet te scannen op zoek naar kwetsbare systemen.

**Cracking** - Het kraken van wachtwoorden of software.

**Dialers** - Computerdialers zijn een subklasse van Trojaanse Paarden, vaak gebruikt op porno-sites. Dialers proberen een duur telefoonnummer te bellen vanuit de computer zonder dat de gebruiker hier vanaf weet. De makers van de dialers proberen met deze kwaadaardige programmatuur financieel voordeel te behalen. Als een computer met een dialer-infectie een analoog modem gebruikt, dan zal de eigenaar een enorm hoge telefoonrekening krijgen. Het blijkt in dergelijke gevallen vaak moeilijk om de geleden financiële schade teniet te doen.

**Denial of Service (DoS)-aanval** - Een Denial of Service (DoS)-aanval wordt door hackers gebruikt om te voorkomen dat de rechtmatige gebruikers toegang verkrijgen tot een computer. Een DoS-aanval verstuurt pakketjes of verzoeken naar een internetserver waardoor deze server overbelast raakt. De server kan dan niet meer benaderd worden door de gebruikers. 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 (DoS)-aanval** - Een Distributed Denial Of Service-aanval is een type DoS-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.

**Hacking** - Misbruik maken van de kwetsbaarheden, misconfiguratie of de schade aangericht door een ander virus om vervolgens toegang te krijgen tot een systeem. Een hacker met kwaadaardige bedoelingen breekt in op de computer om informatie te stelen van de harde schijf of om het beheer van computersystemen over te nemen voor aanvallen gericht op andere computers.

**Hoax/Nepvirus** - Nepvirussen zijn meestal berichten die via e-mail verzonden worden en bevatten meestal een nepwaarschuwing. Deze loze waarschuwingen zijn even lastig als echte virussen. Ze veroorzaken immers tijdverlies en brengen de computergebruiker aan het twijfelen over de echtheid van de boodschap. Een van de redenen waarom Hoaxes zoveel voorkomen, is dat een beetje creativiteit en schrijverstalent volstaan om een e-mail met valse informatie rond te sturen.

**Keystroke loggers** - Keystroke loggers volgen ongezien gegevens die computergebruikers in hun pc zetten en sturen deze door naar derde partijen. Wordt vaak gebruikt als hack tool; individuele toetsaanslagen worden opgeslagen en teruggestuurd naar de hacker. Keystroke loggers kunnen op een computer worden geïnstalleerd door een Trojaans Paard.

**Online fraude** - Bij online fraude wordt persoonlijke informatie of geld via het internet van computergebruikers gestolen. Vormen van online fraude zijn onder andere phishing, spyware, Trojaanse Paarden, keystroke loggers en dialers.

**Phishing** - Bij phishing sturen fraudeurs e-mailberichten of pop-ups naar willekeurige computers. De berichten lijken afkomstig te zijn van populaire websites, van de bank, credit card ondernemingen, of internet service providers. De e-mailberichten of pop-ups vragen gebruikers vaak om persoonlijke informatie, zoals een credit card nummer of password om hun bestanden bij te werken. In veel gevallen bevatten de e-mailberichten een URL- link die lijkt op een betrouwbare website, in werkelijkheid is het een namaak site. Als de consument deze namaak site bezoekt, wordt hem gevraagd om persoonlijke informatie in te voeren dat daarna naar de 'phisher' wordt verzonden.

**Rootkit** - Een verzameling tools die door een indringer worden gebruikt nadat deze zich toegang heeft verschaft tot een computersysteem. De tools zijn bedoeld om draaiende processen, bestanden of systeemgegevens te verhullen, zodat de indringer het systeem langer voor dubieuze doeleinden kan blijven gebruiken.

**Sniffing** - Afluisteren van het verkeer op het netwerk met (vaak) als doel het achterhalen van vertrouwelijke informatie. Sniffing wordt vaak door hacker gebruikt om een password te achterhalen of surfgedrag in kaart te brengen.

**Spam** - Spam is elektronische junk mail of ongevraagde e-mail. Vaak gebruiken spammers e-mailberichten om consumenten te overtuigen dat zij een bezoek moeten brengen aan een website of om een product te kopen.

**Spyware** - Spyware is een programma of applicatie dat onopvallend informatie van gebruikers verzamelt en verstuurt. Spyware kan zowel goedaardig als kwaadaardig zijn. Kwaadaardige spyware kan leiden tot online fraude, omdat het de mogelijkheid heeft persoonlijke informatie door te sturen naar derde partijen.

**Trojan Horse** - Een Trojaans Paard is een programma dat zich voordoeft als goedaardige of onschuldige software, terwijl het in werkelijkheid kwaadaardige acties onderneemt. Trojaans Paarden onderscheiden zich van virussen, omdat zij zichzelf niet kunnen repliceren. Trojaanse Paarden bevatten kwaadaardige code. Wanneer deze code geactiveerd wordt, kan dat leiden tot gegevensverlies of –diefstal. Om een Trojaans Paard te verspreiden moeten computergebruikers deze programma's op hun computer toelaten. Dat gebeurt door het openen van e-mailbijlagen of door het downloaden en afspelen van internetfiles.

**Virus** - Een virus is een kwaadaardig programma dat een computer kan binnendringen zonder dat de gebruiker daarvoor toestemming heeft gegeven en zonder dat hij dat weet. Technisch gesproken hecht een klassiek virus zich aan uitvoerende programma's en kopieert het zich systematisch van het ene bestand naar het andere dat de nietsvermoedende computergebruiker opent. Een virus vermenigvuldigt zich niet alleen, het kan ook - schadelijke of onschadelijke - acties uitvoeren, variërend van een tekst die op het scherm verschijnt, tot het permanent wissen van alle gegevens.

**Worm** - Een worm is een onafhankelijk programma dat zichzelf via een netwerk of het internet van de ene computer naar de andere kopieert. Het verschil tussen een worm en een virus is dat de worm zich niet aan een ander programma kan hechten om het te infecteren. De replicatie tast niet alleen een computer aan maar ook het prestatievermogen van het netwerk in een bedrijf. Net als een virus kan een worm schade veroorzaken door bijvoorbeeld gegevens te vernietigen of vertrouwelijke informatie te versturen.

**Zero-day attack** - Bij een zero-day attack ontdekt een individu een kwetsbaarheid (vulnerability) en ontwikkelt direct een kwaadaardige bedreiging (exploit) die hier misbruik van maakt – in plaats van de leverancier in te lichten. Als de bedreiging actief wordt, is niemand er tegen beschermd omdat een patch niet beschikbaar is.