

Odense den 5. oktober 2008

## Om Virus, Spam, Phishing m.v..

---

### Trusselsbilledet er ændret

Det er uhyggeligt at konstatere at trusselsbilledet er ændret fra, at vi skulle bekymre os over enkeltpersoner's evner til at skabe en vira der kunne give omtale, til at vi i dag skal beskytte os mod organiseret kriminalitet, hvor forbrydere uden samvittighed vil stjæle vores identitet og udnytte denne.

Det er mange forbrydere derude, som bruger internettet til at stjæle dine oplysninger eller til at lokke dig på hjemmesider der ser professionelle og uskyldige ud, men hvor hjemmesiden i virkeligheden er lavet for at få dig til (uden at vide det) at installere en bagdør på din computer. Uanset hvilken form for Malware der kommer på virksomhedens computere, er det skadeligt for din virksomhed, dine kunder og dit omdømme. Du skal fange truslerne i realtid, før de når dine computere.

Målet i dag for alle der fremstiller vira og spyware er at tjene penge. Jo flere intetanende bruges computere man kan få med i et inficeret net, jo voldsommere kan man sprede vira og spammails, hvilket betyder øget indtjening for de kriminelle, og det er stort set uden risiko for at de reelle bagmænd blive fanget.

Seneste udvikling er, at ellers troværdige hjemmesider bliver hacket, herefter placeres en ganske lille kode på hjemmesiden, hvorefter intetanende besøgende på hjemmesiden får deres computer inficeret med malware.

Læs evt. artiklerne:

**"Porno er en bombe under it-sikkerheden" fra ComputerWorld 18. juni 2008.**

<http://www.computerworld.dk/art/46457?page=1>

**"Hackeren er død" fra ComputerWorld 23. september 2008.**

<http://www.computerworld.dk/art/48078?a=newsletter&i=1732&cid=18>

Vi hjælper virksomheder med indkøb, installation og vedligehold af det meget anerkendte Trend Micro Worry Free. Læs mere herunder.



Anti Virus

Et antivirus-program har til formål til at forhindre skadelige vira i at komme ind på computeren og spredes. De fleste antivirus-programmer har en "realtime" beskyttelse mod vira, og en scanner som bruges til at afsløre og fjerne vira som er kommet ind i computeren. Da vira ofte kommer ind via e-mails, så har antivirus-programmet som regel også en mailscanner.

### Trend Micro's prisbelønnede antivirusystem giver beskyttelse i realtid.

Trend Micros antivirusystem beskytter alle udgangspunkter til netværket med en gennemtestet og effektiv teknologi til malware-beskyttelse. Det betyder, at der blokeres for virus, orme og trojanske heste.



Anti Spam

Spam er en betegnelse for reklamer, man ikke selv har bedt om, som sendes via e-mail eller i nyhedsgrupper. Reklamerne har i bedste fald til formål at lokke modtageren til at købe forskellige produkter via internettet, i værste fald at få brugere til at besøge en hjemmeside der kan inficere computeren voldsomt. Spammail udsendes fra en afsender, der almindeligvis søger at skjule sin egentlige identitet ligesom han - med forskellige metoder - opsnapper e-mail-adresser fra intetanende, der



surfer på internettet.

For personer, som udsender spam, kan det være en lukrativ forretning, hvilket formentligt er den primære årsag til, at de uønskede reklamer fortsat udsendes. Det koster således kun få kroner, at udsende millioner af e-mails, og hvis bare én person for hver udsendt million reklamer køber produktet, kan forretningen så at sige løbe rundt.

### **Trend Micro´s Antispam blokerer webtrusler, der kommer via e-mail.**

Trend Micros førsteklasses anti-spam-løsning blokerer -mails, der indeholder skadelige URL-adresser, så netværksressourcerne bevares, og dine medarbejdere slipper for at bruge værdifuld tid på at løse problemer.



Anti Spyware

Betegnelsen spyware eller spionprogrammer bruges om computerprogrammer, der installerer sig selv hos en klient, som regel uden at klienten ved noget om dette. Man kan beskytte sin computer mod spyware med programmer, men disse skal typisk opdateres tit, for at kunne følge med fremvæksten af nye spyware-programmer.

Spyware er en almen form for malware, som ligger spredt ud på din computer, og ser efter hvad du laver. Den minder en del om en keylogger, og man kan beskytte sig mod spyware med programmer som bl.a. Trend Micro. Der opstår konstant nyere versioner af spyware, og derfor er de altid svære at finde.

### **Trend Micro´s Anti-spyware blokerer uønskede overførsler.**

Trend Micro blokerer indgående spyware, rootkits og bots og beskytter samtidig udgående data mod at blive registreret og indsamlet af spyware-programmer.



Anti Phishing

Phishing er et relativt nyt internetfænomen (2005), hvor svindlere forsøger at franarre godtroende internetbrugere deres kreditkort- eller netbankoplysninger. Det sker typisk ved at brugeren får tilsendt en e-mail, hvis indhold forsøger at få brugeren til at indsende sine oplysninger pr. e-mail eller logge ind på en falsk internetside, der ligner f.eks. bankens / PayPals eller Googles.

Siden har der udviklet sig et lignende fænomen omkring indholdstakserede sms-beskeder kaldet smishing: Personer lokkes til at købe f.eks. billeder af letpåkledte kvinder og betaler for dette, men modtager i bedste fald noget helt andet.

Målgruppen for phishingangreb var oftest de mere uerfarne brugere, men nyere forskning (2006) udført af Harvard University og University of California i Berkeley viste, at selv de erfarne internetbrugere bliver narret af de bedst udførte phishingangreb. Faktisk viste undersøgelserne at hele 9 ud af 10 blev narret af de veludførte phishingangreb.

### **Trend Micro´s Anti-phishing beskytter mod skadelige aktiviteter.**

Trend Micros anti-phishing-løsning forhindrer identitetstyveri og beskytter dine fortrolige forretningsoplysninger.





Web Reputation

### Trend Micro's Web reputation-tjeneste beskytter mod angreb fra ukendte trusler (såkaldte zero-day-trusler), inden de får adgang til netværket.

Trend Micro registrerer og analyserer flere hundrede millioner domæner og leverer på den baggrund kontinuerlige opdateringer og direkte feeds, der gør det muligt at vurdere websteder, websider eller hyperlink, så brugeren ved, om de er pålidelige.

Vores Web reputation-tjeneste overfører øjeblikkeligt opdateringer fra fem separate beskyttelseslag til integreret registrering, analyse og feedback - og yder dermed en mere finmasket beskyttelse end nogen tilsvarende tjeneste på markedet.

**Malware** er en sammentrækning af de engelske ord malicious og software (på dansk: "ondsindet programkode"). Det bruges som en fællesbetegnelse for en række kategorier af computerprogrammer, der gør skadelige eller uønskede ting på de computere, de kører på.

## Forskellige kategorier af malware

- En **computervirus** er et lille program, som forsøger at inficere andre programmer. Det er ofte skjult i et tilsyneladende harmløst program, da denne type malware skal aktiveres manuelt for at kunne indlede spredningen. Virusprogrammer kan være meget skadelige, f.eks. ved at slette vigtige data og/eller programfiler fra den inficerede computer. En computervirus søger at overføre kopier af sig selv til andre computere uden brugerens viden. Dette tager i sig selv en del af en "smittet" computers processorkraft, da virusen gerne anbringer sig et sted i systemet, hvor computerens mikroprocessor regelmæssigt kommer forbi og udfører programkoden i virussen. I mange tilfælde er en computervirus lavet, så den gør et eller andet, som ejerne og brugerne af de ramte computere ikke er interesserede i: Den kan f.eks. ødelægge vigtige filer på computerens harddisk eller genere brugeren, f.eks. ved at vise skærmtekst modsat den normale læseretning.

En virus lægger sig ind i et eksisterende program og kan ikke fungere alene. Virussen lægger sig typisk ind i starten af programmet, så den afvikles inden det reelle program kommer til at foretage noget. De fleste virusser må kopiere sig et vist antal gange, før den destruktive programkode aktiveres.

- En **makrovirus** er et program, der udnytter det programmeringsmiljø, der findes i mange programmer til kontorarbejde: Et tekstbehandlings- eller regnearks-dokument kan på den måde udgøre en trussel mod computersystemet.
- En **orm** er omtrent det samme som en computervirus, blot med den væsentlige forskel, at en orm kan sprede sig selv fra maskine til maskine uden at blive aktiveret manuelt. Det foregår ofte ved at udnytte sikkerhedsbrister i operativsystemet eller browseren. En orm vil ofte medbringe en skadelig "last", på engelsk: payload(en), i form af et eller flere programmer, f.eks. en trojansk hest eller en computervirus. Flere orme, f.eks. Nimda-ormen, har i deres payload en mailserv, der benyttes til at videresende ormen til eksempelvis de kontaktpersoner, som offeret har registreret i sit e-mail-programms adressebog.
- **Adware** er programmer, hvori div. reklamer vises mens programmet afvikles.
- **Spyware** undersøger typisk hvilke hjemmesider brugeren besøger, og hvilke søgeord han/hun bruger på world wide web, hvorefter det rapporterer tilbage til skaberen af programmet via internettet. Det er ofte nært beslægtet med adware, og de indsamlede oplysninger bruges så til at målrette de reklamer, der vises for den pågældende bruger.
- **Jokeware** er programmer, som prøver at irritere brugerne på forskellige måder. For eksempel ved at styre en enkel brugers markør.
- En **keylogger** er et program, der registrerer, hvad der skrives på tastaturet. Det bruges til at spionere mod den bruger, hvis computer er inficeret med keylogger-programmet, oftest med henblik på at aflure passwords, kontonumre og andre følsomme oplysninger, når



brugeren handler eller ordner bankforretninger via nettet. Oplysningerne kan blive gemt i en logfil på offerets computer og/eller automatisk blive sendt til en forudbestemt e-mail-adresse. Visse programmer til "forældrekontrol" indeholder reelt også en keylogger beregnet på at overvåge børns brug af chatprogrammer mv..

- **Ransomware** er et relativt nyt fænomen (2005). Det er en art virus, hvis skadevirkning består i at kryptere brugerens data, hvorefter man præsenteres for en besked om, at man kan få "nøglen" til at afkode sine data mod at betale en løsesum.
- En **dialer** er et program rettet imod folk, der bruger et modem til at etablere forbindelse til internettet. Det ændrer i computerens indstillinger for brug af modemmet, så det i stedet for den vante internetudbyder ringer op til et andet telefonnummer ofte med store telefonregninger til følge.
- En **trojansk hest** er malware forklædt som noget harmløst. Den har fået sit navn fra Homers skildring af Odysseus' krigslist mod byen Troja. I it-sammenhænge er den indsmuglede "trojaner" eller payload ofte et serverprogram, som gør det muligt for andre at fjernstyre offerets computer. Det kalder man også at installere en bagdør. Adgangen kan f.eks. misbruges til at foretage denial-of-service-angreb mod andre systemer på nettet. Fjernstyringsprogrammet Back Orifice(en) er et af de mest kendte payload-programmer i trojanske heste, selv om programmet i sig selv er lavet til legale formål.
- Et **hoax** (engelsk for "fupnummer") er en advarsel om en fiktiv virus eller anden malware, som sendes rundt, typisk via en kædebrevslignende e-mail, med det formål at få forskrækkede, ukyndige brugere til at slette en ellers nyttig fil fra deres computersystem - eller ganske enkelt for at drille.

Ofte bruges ordet "computervirus" i flæng om flere af de andre former for malware, fordi dette var den første type af malware. Derfor er antivirus-programmer sjældent begrænset til alene at bekæmpe vira, men sikrer også mod flere andre malware-kategorier.

Forvirringen bliver ikke mindre af, at malware ofte optræder som en kombination af flere af ovennævnte typer. F.eks. kan en orm laves, så den automatisk spreder sig til en computer, hvor den dropper en payload bestående af en keylogger og en trojansk hest med et fjernstyringsprogram. Når den trojanske hests payload bliver aktiveret, kan ormens ophavsmand så skaffe sig fjernadgang til offerets computer for at aflæse keyloggerens logfil.

Malware beskrivelsen er hentet fra "<http://da.wikipedia.org/wiki/Malware>" og er lettere modificeret for at lette forståelsen.

