30-05-2024

Hvad er virus

NewTech IT´ support har udfærdiget et lille kompendium omkring virus mv.

Kompendium er sendt til korrektur.

Kim Kulebjerg
NEWTECH IT

Indhold

Forord

Undertegnede er bevist om, at denne artikel er meget teknisk/fagligt anlagt, ikke desto mindre tænker jeg det kan give den almindelige computerbrugere en indsigt i hvilken størrelse Adware, Malware og Virus er og ikke mindst om man er inficeret af Adware, eller Malware eller noget helt tredje.

Generelt har vi gode resultater med at rense en inficeret computer hvis det drejer sig om Adware og Malware, men hvis din computer har været inficeret med mere ondsindet former for virus, anbefaler NewTech IT altid en gendannelse til fabriksindstilling eller reinstallation af Windows. Det er der 2 grunde til denne ene er som du kan læse mere om i denne guide at virus kan gemme sig i software som man ellers har tillid til. Der er derfor kun en udvej og det er at slette alt hvad der er på harddisken og geninstallerer Windows, software (programmer) og data. (Billeder, Dokumenter og andet). Den anden grund er at det ville kræve mange mandetimer, altså blive for dyrt i længden at prøve at fjerne en virus og du vil aldrig kunne være 100% sikker på at du har fået fjernet alt. Det kan du hvis du reinstallerer eller geninstallerer Windows.

Den bedste måde du kan beskytte dig imod Adware, Malware og virus er ved at have et Image af din harddisk, hvis den ikke er inficeret og at du foretager backup af dine data, hver gang, du bruger din computer.

NewTech IT kan naturligvis hjælpe dig med begge dele, men de fleste kan finde ud af at tage backup selv.

Image af din harddisk kan vi udføre til en fornuftig pris. Så hvis du gerne vil være forsikret imod Adware, Malware og Virus, så tøv ikke med at ringe og husk ingen Antivirus programmer beskytter dig 100% heller ikke betalte Antivirus programmer.

NewTech IT´s support hjælper naturligvis gerne hvis du mener du er inficeret med virus.

Du ønskes god læselyst!

Med venlig hilsen

Kim Kulebjerg NewTech IT
Tlf. 2299 9097
E-mail: info@newtechit.dk

Adware

Kilde: Wikipedia.

Adware, eller reklame-understøttet software, er en softwarepakke, der udgiver reklamerer for at generere indtægter for dens forfatter. Reklamer kan være i brugergrænsefladen af softwaren eller på skærmen der vises for brugeren under installationen. Funktioner kan være designet til at analysere hvilke internetsider brugeren besøger og dermed gøre nuværende reklamer relevant for varer eller tjenesteydelser der skal vises. Udtrykket er undertiden brugt til at henvise til software, der viser uønskede reklamer.

Link

Reklame-understøttet programmel

I overførelse via programmel

I software som en service

Som malware

Reklame-understøttet programmel

I lovlig software, er reklame funktioner integreret i eller bundtet sammen med programmet. Adware ses normalt af udvikleren som en måde hvorpå han/hun kan tjene penge til udvikling, og i nogle tilfælde dermed udbyde softwaren til brugerne gratis eller til nedsat pris. Indtægter fra reklamerne til udvikleren kan motivere udvikleren til at fortsætte med at udvikle, vedligeholde og opgradere softwareproduktet. Anvendelsen af reklame-understøttet programmel i erhvervslivet bliver stadig mere populært, en undersøgelse fra 2007 af McKinsey & Company viste at en tredjedel af erhvervslederne, planlægger at bruge annonce-finansieret software inden for de følgende to år. Annonce-finansieret software er også en af forretningsmodeller for open source-software.

Adware overføres i programmel

Nogle software tilbydes i både en reklame-understøttet version og en betalte, annonce-fri version. Sidstnævnte er normalt tilgængelige ved et online køb af en licens eller registrerings kode for den software, der låser op, eller køb og download af en separat version af softwaren. Nogle softwareproducenter tilbyder reklame-understøttet versioner af deres software som en alternativ mulighed for virksomheder der prøver at undgå at betale store summer for softwarelicenser, hvorved annoncørerne støtter udviklingen af software. Eksempler på reklame-understøttet software er Windows-versionen af programmet Skype, og Amazon Kindle 3 e-bog læsere, der har versioner kaldet "Kindle med specielle tilbud" der vise reklamer på hjemmesiden og i dvaletilstand til gengæld mod væsentligt lavere priser.

I 2012, meddelte Microsoft og dets reklame division, Microsoft Advertising, at Windows 8, den kommende store udgivelse af Microsoft Windows-operativsystemet, ville have indbyggede metoder for programudviklere til at bruge reklame som en forretningsmodel. Idéen var udtænkt allerede i 2005.

Software som en service

Understøttelse af reklame er en populære forretnings model af software som en service (SaaS) på internettet. Som bemærkelsesværdige eksempler kan nævnes E-mail servicen Gmail og andre Google Apps produkter, samt det sociale netværk Facebook. Microsoft har også vedtaget den reklame-støttede model for mange af dens sociale software SaaS tilbud. Microsoft Office Live-tjeneste, var også tilgængelige i en reklame-understøttet tilstand.

I udgivelsen af Federal Trade Commission synes der kun at være generel enighed om at software bør betragtes som "spyware", hvis det er downloadet eller installeret på en computer uden brugerens viden og/eller samtykke. Der er dog fortsat uløste spørgsmål om hvordan, hvad og Hvornår forbrugerne skal informeres om inden softwaren installeres på deres computere for at samtykke er tilstrækkelig. For eksempel, afsløre distributører ofte i deres slutbruger licensaftale, at der er ekstra software bundled sammen med den primære software, nogle paneldeltagere og kommentatorer ser ikke sådanne videregivelser som tilstrækkelig for samtykke fra brugerens side til installationen af den medfølgende software.

Som malware

Udtrykket adware er ofte bruget til at beskrive en form for malware (skadelig software] som normalt, præsenterer uønskede reklamer til brugeren af en computer i form af et pop-up vindue.

Når udtrykket bruges i denne form, varierer sværhedsgraden af dens konsekvenser. Mens nogle kilder kun vurderer adware som en "lokalirriterende" adware, klassificere andre det som en "online trussel" eller endog ligeså alvorligt som computervira og trojanske heste. Den præcise definition af begrebet i denne sammenhæng kan altså variere. Adware, der overvåger computerbrugerens aktiviteter uden deres samtykke og rapporter det til softwareforfatteren kaldes spyware.

Programmer der er udviklet til at registrere, sætte filer i karantæne og fjerne annoncen-fremvisningen af malware, herunder Ad-Aware, AdwCleaner, Malwarebytes' Anti-Malware, Spyware Doctor og Spybot - Search & Destroy. Derudover kan næsten alle kommercielle antivirus software i øjeblikket opdage adware og spyware, eller tilbyde en separat antispyware pakke.

Malware

Kilde: Wikipedia.

Malware, er en forkortelse for skadelig software, software der bruges til at forstyrre computerens drift, indsamle følsomme oplysninger eller få adgang til private data. Malware er defineret ved dens ondsindede hensigter, der er målrettet computerbrugeren, og omfatter ikke software, der forårsager utilsigtet skade på grund af nogle mangler. Udtrykket badware er også undertiden brugt og anvendes ved ægte (skadelig) malware og utilsigtet skadelige software. Malware kan være skjult, beregnet til at stjæle oplysninger eller spionere målrettet imod computerbrugere i en længere periode uden deres viden, som for eksempel Regin, eller det kan være designet til at forårsage skade, ofte som sabotage (fx Stuxnet)eller afpresse en form for betaling (CryptoLocker). "Malware" er en fælles betegnelse, der bruges til at henvise til en række forskellige former for fjendtlig eller påtrængende software, herunder computervira, orme, trojanske heste, ransomware, spyware, scareware og andre skadelige programmer. Det kan tage form af eksekverbar kode, scripts, aktivt indhold og anden software. Malware er ofte forklædt som eller indlejret i ikke-skadelige filer. I 2011 var størstedelen af aktive malwaretruslere orme eller trojanske heste i stedet for virus.

Spyware eller anden malware er undertiden fundet indlejret i programmer leveret af firmaer, der fx kan downloades fra websteder, der formodes at være nyttige eller attraktive, men for eksempel kan have yderligere skjulte sporingsfunktionen, der samler marketings statistik. Et eksempel på en sådan software, der blev beskrevet som uægte, er Sony´s rootkit, en Trojansk hest indlejret i cd'er solgt af Sony, som tavst blev installeret og skjulte sig på købernes computere med det formål at forhindre ulovlig kopiering; Der er også eksempler på brugernes musik vaner blev indsamlet og utilsigtet oprettede sårbarheder, der blev udnyttet af ikke-forretningsmæssigt forbundne malware.

Programmel anti-virus, anti-malware og firewalls er brugt til at beskytte mod aktiviteter identificeret som skadelige og direkte ødelæggende.Formål

Spredning

Smitsomme malware: virus og orme

Infektiøs: Vira, trojanske heste, rootkits, bagdøre og skattesvig

Virus

Trojanske heste

Rootkits

Bagdøre

Unddragelse

Sårbarhed over for malware

Sikkerhed fejl i software

Usikre design eller bruger fejl

Over privilegerede brugere og over privilegeret kode

Brug af det samme operativsystem

Anti-virus og anti-malware-software

Website sikkerhedsscanninger

"Air gap" isolation eller "Parallelle netværk"

Grayware

Historie om vira og orme

Akademisk forskning

Formål

Malware efter kategorier pr. 16 marts 2011. Mange tidlige smitsomme programmer, herunder den første internetorm, var skrevet som eksperimenter eller drengestreger. I dag, bruges malware af både black hat hackere og regeringer, til at stjæle personlige, finansielle, og/eller forretningsoplysninger.

Malware er undertiden brugt bredt mod regeringer eller store virksomheders websites for at indsamle fortrolige oplysninger, eller forstyrre deres virke i almindelighed. Malware bruges dog ofte mod enkeltpersoner til at opnå oplysninger såsom personlige oplysninger eller detaljer, omkring bank eller kreditkort numre og adgangskoder. Er computere ubevogtet, og mangler opdateringer og patches til det installeret programmel, vil personlige og netværksbaseret computere være i en betydelig risiko gruppe for disse trusler. (Disse er oftest beskyttet med forskellige typer af firewall, anti-virusprogrammer og netværkshardware).

Siden fremkomsten af bredbåndsadgang til internettet, har skadelig software oftere været designet til profit. Siden 2003, er de fleste af de udbredte virus og orme designet til at overtage kontrollen af brugernes computere til ulovlige formål. Inficerede "zombie computere" bruges til at sende e-mail-spam, agere som ulovlig data vært for børnepornografi, eller til at computeren virker som distributør for et denial-of-service (DOS) angreb som en form for afpresning.

Programmer der er designet til at overvåge brugerens webbrowsings vaner, og dermed vise reklamer, eller omdirigere brugeren til anden form for marketings indtægter kaldes spyware. Spyware-programmer breder sig ikke som virus; i stedet er de generelt installeret ved at udnytte sikkerhedshuller. De kan også installeres sammen med bruger-installeret software, såsom peer-to-peerprogrammer.

Ransomware påvirker en inficeret computer ved at ”Låse” den og kræve betaling for at ”Låse” den op igen. For eksempel, programmer såsom CryptoLocker kryptere filer sikkert, og kan kun dekrypteres mod betaling af en betydelig sum penge.

Nogle malware bruges til at generere penge ved ”klikbedrageri”, som virker på den måde, at den registrer hvilken reklamer computerbrugeren har klikket på, og dermed genererer en betaling fra annoncøren til programudvikleren (Hackeren). Det blev anslået at i 2012, var omkring 60 til 70% af alle aktive malware en form for klikbedrageri, og 22% af alle ad-klik var bedragerisk.

Malware anvendes normalt til kriminelle formål, men kan også bruges til sabotage, ofte uden direkte gevinst for gerningsmændene. Et eksempel på sabotage var Stuxnet, der blev konstrueret til at ødelægge meget specifikt industrielt udstyr. Der har været politisk motiverede angreb, der blev spredt over landegrænser og have til formål at nedlægge store edb-netværk, herunder massive sletning af filer og korruption af master boot poster, disse beskrives som "computer drab". Sådan et angreb blev foretaget på Sony Pictures Entertainment (25. november 2014, ved hjælp af malwaren kendt som Kristruns eller W32. Disttrack) og Saudi Aramco (August 2012).

Spredning

Foreløbige resultater fra Symantec offentliggjort i 2008 anslog at "mængden af skadelig koder og andre uønskede programmer kan være overskredet af lovlig softwareapplikationer." i følge F-Secure, blev der alene i 2007 fremstillet lige så meget malware som i de foregående 20 år i alt. Malwarens mest almindelige vej fra kriminelle til brugerne er gennem internettet: primært som e- mail og brug af World Wide Web.

Udbredelsen af malware er så massiv en internetkriminalitet, der sammen med udfordringen i at holde antimalware-software opdateret og følge med en kontinuerlig strøm af nye malware, har skabt en ny tankegang for enkeltpersoner og virksomheder i den måde vi skal bruge internettet på. Med mængden af malware der i øjeblikket bliver distribueret, antages det at nogle få procentdele af computere i øjeblikket er smittet. For virksomheder, især dem, der sælger primært via internettet, betyder det at de skal finde en måde at overleve på trods af de sikkerhedsmæssige bekymringer og trusler. Resultatet er at der bør lægges større vægt på back-office beskyttelse designet til at beskytte mod avancerede malware der findes på kundernes computere. En undersøgelse fra 2013 i Webroot viste, at 64% af virksomhederne tillader fjernadgang til deres servere for 25% til 100% af deres arbejdsstyrke, og at virksomheder giver mere end 25% af deres medarbejdere adgang til servere og dermed er i en højere risikogruppe for malware-trusler.

Den 29 marts 2010 udnævnte Symantec Corporation Shaoxing, Kina, som verdens malware hovedstad. En undersøgelse fra University of California, Berkeley og Madrid Institute for Advanced Studies i 2011 offentliggjort i en artikel i Software udviklingsteknologier, beskrev hvordan (”ivæksætter”) hackere hjælper til med spredning af malware ved at sælge adgang til computere. Microsoft rapporteret i maj 2011, at de anslår hver 14. download fra internettet kan indeholde malware kode. Sociale medier, og Facebook har især oplevet en stigning i antallet af angreb, der anvendes til at sprede malware til computere.

En undersøgelse fra 2014 viste, at malware i stigende grad blev rettet mod de stadig mere populære mobile enheder såsom smartphones. Dette skyldes at Smartphones ofte er dårligere beskytte end computere.

Smitsomme malware: virus og orme

De mest kendte typer af malware, vira og orme, er kendt for den måde, hvorpå de spredes, frem for nogen bestemte type af adfærd. Udtrykket computervirus anvendes om et program, der integrerer sig i andre eksekverbar software (herunder selve operativsystemet) på destinationssystemet uden brugerens samtykke eller viden og når det er installeret forårsager at virus kan sprede sig til andre eksekverbare filer. På den anden side er en orm et stand-alone malware-program, som aktivt sender sig selv over et netværk for at inficere andre computere. Disse definitioner fører til den konklusion, at en virus kræver, at brugeren aktivt installerer et inficeret program eller operativsystem, således virussen kan spredes, mens en orm spreder sig af sig selv.

Infektiøs: Vira, trojanske heste, rootkits, bagdøre og skattesvig

Disse kategorier udelukker ikke gensidigt hinanden, så malware kan bruge om flere teknikker. Dette afsnit gælder kun for malware designet til at forblive uopdaget, ødelæggende og/eller ransomware.

Virus

Uddybende artikel: Computer virus og computer orme.

Et virusprogram er som regel skjult i et andet tilsyneladende harmløst program, der producerer kopier af sig selv og indsætter inficeret koder i andre programmer eller filer, og at der normalt udføres en ondsindet handling (såsom at ødelægge data). Trojanske heste.

Trojanske heste

Uddybende artikel: trojansk hest (computing)

For at en ondskabsfuld trojansk hest skal opnå sit formål, skal den kunne køre uden at blive opdaget, og dermed blive lukket ned og/eller slettet. Når en ondsindet virus/program er forklædt som et normalt eller ønskeligt program, kan brugeren uforvarende komme til at installerer det. Denne teknik bruges af Trojanske heste eller trojan. I bred forstand er en trojansk hest et program, der inviterer brugeren til at køre det, skjuler skadelige eller skadelig eksekverbar koder af enhver art. Koden kan træde i kraft straks og kan føre til mange uønskede effekter, såsom kryptering af brugerens filer eller downloade og gennemføre yderligere ondsindede funktionalitet. Det kan også gå i dvale og først blive aktiveret på en bestemt dato eller handling.

For nogle spyware, malware, typer kan leverandøren (Hackeren) kræve at brugeren anerkender eller accepterer dens installation, normalt beskrives dens adfærd i løse termer, der let kan misforstås eller ignoreres, med den hensigt at snyde brugeren til at installere programmet og dermed er leverandøren (Hackeren) teknisk set ikke i strid med loven.

Rootkits

Uddybende artikel: Rootkit (Artiklen er på Engelsk)

Når et ondsindet program er installeret på en computer, er det vigtigt, at det forbliver skjult, for derved at undgå afsløring. Softwarepakker kendt som rootkits tillade denne anonymitet, ved at ændre operativsystemet, således at malwaren er skjult for brugeren. Rootkits kan forhindre, at en ondsindet proces kan ses i systemets liste over processer (Joblisten), eller skjule sine filer i at blive vist.

Nogle ondsindede programmer indeholder rutiner til at forsvare sig mod fjernelse, og ikke blot for at skjule sig. Et tidligt eksempel på denne opførsel er registreret i Jargon File´s beretning om et par programmer der angriber en Xerox CP-V tids sharing-system:

Hvert spøgelse-job ville opdage det faktum, at den anden var blevet slettet, og ville starte en ny kopi af det for nylig stoppede program inden for få millisekunder. Den eneste måde at slette begge spøgelser var at slette dem på samme tid (meget svært), eller bevidst at crashe systemet.

Bagdøre

Uddybende artikel: bagdør (computing)

En bagdør er en metode hvorpå man omgår den normale godkendelses procedurer, normalt via en forbindelse til et netværk som internettet. Når et system er blevet kompromitteret, kan en eller flere bagdøre installeres for at tillade adgang fremover, usynligt for brugeren.

Ideen har ofte været, at computerproducenter forud installeret bagdøre på deres systemer for at yde teknisk support til kunder, men det har aldrig været på pålidelig vis. Det blev rapporteret i 2014, at de amerikanske regeringsorganer havde været impliceret i hemmelige workshops, hvor der blev installeret software eller hardware der tillod agenturet fjernadgang, denne operation anses for at være blandt den mest udbredte operationer for at få adgang til netværk i hele verden. Bagdøre kan installeres af trojanske heste, orme, implantater eller andre metoder.

Unddragelse

Siden begyndelsen af 2015 benytter en anselig del af malware en kombination af 500 teknikker, designet til at undgå opdagelse og analyse.

Den mest almindelige unddragelse teknik er når malwaren undviger analyse og påvisning af algoritmemiljøet, når den eksekveres.

Den anden mest almindelige unddragelse teknik er forvirringen af automatiserede værktøjer. Det gør malware i stand til at undgå afsløring af teknologier såsom algoritme-baserede antivirus software ved at ændre den server, der bruges af malwaren.

Den tredje mest almindelige unddragelse teknik, er timing-baseret unddragelse. Dette er når malware kører på bestemte tidspunkter eller efter visse betingelser, der træffes af brugeren, så det udfører i visse perioder, mens den i den resterende tid er i dvale.

Den fjerde mest almindelige unddragelse teknik er ved at sløre interne data, således at værktøjer ikke registrerer malwaren.

Sårbarhed over for malware

Uddybende artikel: sårbarhed (computing) (Artiklen er på Engelsk)

I denne kontekst, og hvad der benævnes "systemet" under angreb kan være alt fra det enkelte software til en computer og operativsystem, eller et stort netværk.

Forskellige faktorer gør et system mere sårbart over for malware:

Sikkerheds fejl i software

Malware udnytter sikkerheds fejl (sikkerhedsfejl eller sårbarheder) i udformningen af operativsystemet, og applikationer (f.eks browsere, ældre versioner af Microsoft Internet Explorer der understøttes af Windows XP) eller i sårbare versioner af browser plugins som Adobe Flash Player, Adobe Acrobat, Adobe Reader eller Java (Se betænkelig udgaver af Java). Gamle versioner fjernes ikke altid automatisk, når nye versioner af disse plugins installeres. Sikkerhedsmeddelelser fra plug-in udbyderne annoncere normalt automatisk når sikkerhedsrelaterede opdateringer er tilgængelig. Almindelig sårbarheder er tildelt CVEid'er og opført i Den Nationale Sårbarheds Database. Secunia PSI. er et eksempel på software, der er gratis til personligt brug, og som vil kontrollere ens computer for sårbar forældet software, og automatisk forsøge at opdatere softwaren.

Malware er målrettet til at udnytte bugs eller smuthuller. En fælles metode er udnyttelse af en bufferoverløb sårbarhed, hvor software designet til at gemme data i et bestemt område af hukommelsen ikke forhindrer mere data end bufferen kan rumme, i at blive leveret. Malware kan dermed levere data, som overløberbufferen med skadelig eksekverbar kode eller data til følge; Når denne eksekverbar kode eller data er tilgået bufferen gør det hvad hackeren har bestemt, og ikke hvad den legitime software, bestemmer. Usikre design eller bruger fejl.

Usikre design eller bruger fejl

De første pc'er skulle startes op fra disketter; Da det blev normalt at starte computeren fra indbyggede harddiske, blev det også muligt at starte fra en anden boot enhed hvis den var tilgængelig, f.eks. en diskette, CD-ROM, DVD-ROM eller USB drev. Det var almindeligt at konfigurere computeren til at starte fra en af disse enheder, når de var tilgængelige. Normalt ville ingen være tilgængelig; brugeren skulle bevidst indsætte, en CD i det optiske drev for at starte computeren fra CD/DVD drevet, for eksempel for at installere et operativsystem. Selv uden opstart, kan computere konfigureres til at køre software på nogle medier, så snart de bliver tilgængelige, fx at udføre autorun fra en CD eller USB-enhed, når den er indsat.

Skadelig software ville narre brugeren til opstart eller kørsel fra en inficeret enhed eller medium; for eksempel kunne en virus inficeret på en computer, tilføje autorun koder til enhver USB-stick der er tilsluttet, der derefter tilsluttet en anden computer ville indstille den til autorun fra USB sticken som så igen ville blive smittet, og således videregive smitten på samme måde. Enhver enhed, der sluttes til en USBport-— "herunder gadgets som lys, fans, højttalere, legetøj, selv en digital microscope" – kan bruges til at sprede malware. Enheder kan være smittet under fremstillingen eller hvis kvalitetskontrollen af hardwaren er utilstrækkelig.

Denne form for infektion kan i stort omfang undgås ved at konfigurere computere til som standard at starte fra den interne harddisk, og ikke at køre autorun fra nogen andre enheder. Opstart fra en anden enhed er altid muligt ved at trykke på nogle bestemte taster under boot.

Ældre e-mail software vil automatisk åbne HTML email der kan indeholde potentielt skadelig JavaScript koder; brugere kan også aktivere skadelig koder ved at klikke på vedhæftede filer i en e-mail- og dermed inficerede computeren.

Over privilegerede brugere og over privilegeret kode

Uddybende artikel: [princippet om færrest mulige rettigheder] (Artiklen er på Engelsk)

I artiklen, henviser der til det privilegium hvor meget en bruger eller program har tilladelse til at ændre et system. I dårligt designet software, kan både brugere og programmer tildeles flere rettigheder end de burde have, og malware kan drage fordel af dette. De to måder at malware gør dette på er gennem overprivilegeret brugere og overprivilegeret kode tilladelser.

Nogle systemer tillader alle brugere at ændre deres interne strukturer, og sådanne brugere ville i dag anses for privilegerede brugere. Dette var standardprocedure for tidlige mikro-computere og hjemme computersystemer, hvor der ikke var nogen forskel mellem en administrator eller en standard bruger af systemet. I nogle systemer, er ikke-administrator brugere over privilegerede af design, i den forstand, at de får lov til at ændre interne strukturer i systemet. I nogle miljøer er brugere over privilegeret, fordi de har fået uhensigtsmæssigt, administrator tilladelse eller tilsvarende status.

Nogle systemer tillader at brugeren kan kører koder, der giver adgang til alle rettighederne for den bruger, det er kendt som over-privilegeret kode. Dette var også standardprocedure for tidlige mikro-computer og hjemmecomputer systemer. Malware, kører som over-privilegeret kode, og kan bruge denne rettighed til at inficerer systemet. Næsten alle populære operativsystemer, og også mange scripting programmer tillader brugeren at kode med for mange privilegier, som regel i den forstand, at når en bruger afvikler kode, vil systemet giver mulighed for at kode alle rettigheder for brugeren. Dette gør brugere sårbare over for malware i form af e-mail-vedhæftede filer, som måske eller måske ikke er skjult.

Brug af det samme operativsystem

Homogenitet: f.eks når alle computere i et netværk kører det samme operativsystem; ved at udnytte en, kan en orm udnytte dem alle. For eksempel, Microsoft Windows eller Mac OS X har sådan en stor andel af markedet, som koncentrerer sig om enten at kunne muliggøre en udnyttet sårbarhed eller undergrave en lang række systemer. I stedet burde man indføre mangfoldighed, af hensyn til robusthed, kortsigtede vil det øge omkostninger til træning og vedligeholdelse. Imidlertid vil det have den fordel med forskellige noder at ved en total nedlukning af nettet, kunne man bruge disse knudepunkter til at hjælpe med genopretning af de inficerede noder. En sådan særskilt, funktionel redundans kunne undgå omkostningerne ved en total nedlukning, men det kommer nok ikke til at ske.

Anti-malware strategier

Uddybende artikel: Antivirus-software

Efterhånden som malware angreb er blevet hyppigere, er opmærksomheden begyndt at flytte sig fra virus og spyware-beskyttelse, til beskyttelse mod skadelig software og programmer, der er specielt udviklet til at bekæmpe malware. (Andre forebyggende og gendannelse foranstaltninger som backup og gendannelse metoder, er nævnt i computervirus artiklen).

Anti-virus og anti-malware-software

En specifik komponent i den anti-virus og anti-malware-software der almindeligvis omtales som on-adgang eller real-time scanner, kommer dybt ind i operativsystemets kerne eller kerne og fungerer på en måde, der svarer til, hvordan visse malware selv ville forsøge at operer, dog med brugerens samtykke til beskyttelse af systemet.

Operativsystemet vil kontinuerligt kontrollere om en fil der ønsker adgang er en »berettiget« fil eller ej. Hvis filen anses som malware ved scanning, vil adgang blive nægtet, og filen vil blive behandlet af scanneren som en foruddefineret opgave (hvordan antivirusprogrammet er konfigureret under / efter installation), og brugeren vil få en meddelelse.

Anti-malware-programmer kan bekæmpe malware på to måder:

De kan give real time beskyttelse mod malware der prøver at installerer sig på en computer. Denne type malware beskyttelse fungerer på samme måde som for antivirus beskyttelse, anti-malwaresoftwaren scanner alle indgående netværksdata for malware og blokerer de trusler der kommer på tværs.

Anti-malware-softwareprogrammer kan bruges udelukkende til registrering og fjernelse af malware, der allerede er installeret på en computer. Denne type anti-malware software, scanner indholdet af Windows-registreringsdatabasen, operativsystemfiler, og installeret programmer på en computer og vil give en liste over eventuelle trusler den har fundet, således kan brugeren vælge hvilken filer han/hun ønsker at slette eller beholde eller sammenligne denne liste med en liste over kendte malware komponenter, og fjerner filer, der matcher.

Real-time beskyttelse af malware fungerer på samme måde som real-time antivirus beskyttelse: softwaren scanner filen på download-tidspunktet, og blokerer komponenter, der er kendt for at repræsentere en malware. I nogle tilfælde kan det også opfange forsøg på at installere start-up elementer eller ændre browser-indstillinger. Fordi mange malwarekomponenter er installeret ved hjælp af browseren, ved brugerfejl, eller ved hjælp af sikkerhedssoftware (hvoraf nogle er anti-malware, men mange ikke er) er "sandkasse" browsere (browser der hovedsagelig isolere computeren og dermed enhver malware inficering) kan også være effektiv i kampen om at begrænse eventuelle skader.

Eksempler på Microsoft Windows antivirus og anti-malware-software omfatter den valgfrie Microsoft Security Essentials (til Windows XP, Vista og Windows 7) for real-time beskyttelse, ”Værktøj til fjernelse af skadelig software” (er nu inkluderet i Windows (sikkerheds) opdateringer på "Patch Tuesday", den anden tirsdag i hver måned), og Windows Defender (en valgfri download i forbindelse med Windows XP, MSE funktionaliteten er indarbejdet i Windows 8 og senere). Derudover er der flere habile antivirus softwareprogrammer tilgængelige til gratis download fra internettet (som regel begrænset til ikke-kommerciel brug). AV comparatives fandt i en test at nogle gratis programmer er lige så konkurrencedygtig som kommercielle. Microsofts System File Checker kan bruges til at kontrollere og reparere beskadigede systemfiler. Nogle virus deaktiverer Systemgendannelse og andre vigtige Windows-værktøjer såsom Jobliste og Kommandoprompt. Mange sådanne vira kan fjernes ved at genstarte computeren, og starte op i fejlsikret tilstand med netværk, og derefter bruge Systemværktøjer eller Microsoft Safety Scanner. Hardwareimplantater kan være af enhver type, så der er ikke nogen generelle måde at registrere dem. Eksempler på Microsoft Windows antivirus og anti-malware-software omfatter den valgfrie Microsoft Security Essentials (til Windows XP, Vista og Windows 7) for real-time beskyttelse, ”Værktøj til fjernelse af skadelig software” (er nu inkluderet i Windows (sikkerheds) opdateringer på "Patch Tuesday", den anden tirsdag i hver måned), og Windows Defender (en valgfri download i forbindelse med Windows XP, MSE funktionaliteten er indarbejdet i Windows 8 og senere). Derudover er der flere habile antivirus softwareprogrammer tilgængelige til gratis download fra internettet (som regel begrænset til ikke-kommerciel brug). AV comparatives fandt i en test at nogle gratis programmer er lige så konkurrencedygtig som kommercielle. Microsofts System File Checker kan bruges til at kontrollere og reparere beskadigede systemfiler.

Nogle virus deaktiverer Systemgendannelse og andre vigtige Windows-værktøjer såsom Jobliste og Kommandoprompt. Mange sådanne vira kan fjernes ved at genstarte computeren, og starte op i fejlsikret tilstand med netværk, og derefter bruge Systemværktøjer eller Microsoft Safety Scanner.

Hardwareimplantater kan være af enhver type, så der er ikke nogen generelle måde at registrere dem.

Website sikkerhedsscanninger

Nogle malware skader også de kompromitterede websteder (ved at bryde omdømmet, sortlistning i søgemaskinerne, etc.), nogle websteder tilbyder sårbarheds scanning. Sådanne scanninger tjekker hjemmesiden, opdager malware, og notere forældet software, og kan efterfølgende rapportere kendte sikkerhedsproblemer.

"Air gap" isolation eller "Parallelle netværk"

Som en sidste udvej, kan computere beskyttes mod malware, og inficerede computere kan være forhindret i at formidle pålidelige oplysninger, ved at indføre en "air gap" (dvs. helt afbryde dem fra alle andre netværk). Men oplysninger kan fremsendes af ukendte veje; i december 2013 påviste forskere i Tyskland en måde hvorpå en tilsyneladende ”lufttæt” computer kunne blive besejret.

Grayware

Se også: Privacy-invasive software og uønsket software bundling

Grayware er en betegnelse der anvendes til uønskede programmer eller filer, der ikke er klassificeret som malware, men kan forværre ydeevnen af computeren og dermed medføre en sikkerhedsrisiko.

Grayware beskriver programmer, som en irriterende eller har en uønsket adfærd, og alligevel er mindre alvorlige eller generende end malware. Grayware omfatter spyware, adware, falske dialers, joke programmer, sen adgang værktøj og andre uønskede programmer, der skade udførelsen af computere kode eller medføre ulempe. Udtrykket kom i brug omkring 2004.

Et andet udtryk, PUP, som står for potentielt uønsket Program (eller PUA potentielt uønskede applikationer), refererer til programmer, der ville blive betragtet som uønskede trods det at de ofte har været downloadet af mange brugere, eventuelt efter man ikke har læst en download aftale. PUPs kan indeholde spyware, adware, falske dialers. Mange sikkerhedsprodukter klassificerer uautoriseret nøgle generatorer som grayware, selv om de ofte bære sand malware ud over deres angiveligt formål.

Software producenten Malwarebytes viser flere kriterier for klassificering af et program som PUP.

Historie om vira og orme

Før internettet blev udbredt, spredes virus på personlige computere ved at inficere eksekverbare bootsektorer på disketter. Ved at indsætte en kopi af sig selv i maskinkode instruktioner i disse eksekverbare filer, forårsager en virus sig selv til at køre, når et program kørte eller disken var opstarts diskette. Tidlig computervirus blev skrevet til Apple II og Macintosh, men det blev mere udbredt med dominans af IBM PC og MS-DOS. Eksekverbare-inficerer virus er afhængige af at brugerne udveksler software eller boot-stand disketter og flash drev (USB stick), så de spredes hurtigere.

De første orme, var netværk-bårne smitsomme programmer, de opstod ikke på personlige computere, men på multitasking Unix systemer. Den første kendte orm var internetorm af 1988, som inficeret SunOS og VAX BSD systemer. I modsætning til en virus, kunne ormen ikke sprede sig selv til andre programmer. I stedet, udnyttet det sikkerhedshuller (svagheder) i netværkets serverprogrammer og begyndte automatisk at kører som en separat proces. Det er den samme funktionsmåde der anvendes af nutidens orme.

Med fremkomsten af Microsoft Windows-platformen i 1990 'erne, og de fleksible makroer af dens applikationer blev det muligt at skrive smitsomme kode i makro-sprog i Microsoft Word og lignende programmer. Disse makrovirus inficerer dokumenter og skabeloner i stedet for programmer (eksekverbare filer), men er afhængige af, at makroer i et Word-dokument er en form for eksekverbar kode.

I dag, er orme oftest skrevet til Windows OS, selv om et par lignende Mare-D og ormen L10n også er skrevet til Linux og Unix-systemer. Orme i dag arbejder på samme grundlæggende måde som 1988's internetorm: de scanner netværket og bruge sårbare computere til at replicerer sig selv. De behøver ingen menneskelig indgriben, og kan sprede sig med utrolig hastighed. Virussen SQL Slammer inficeret tusindvis af computere i løbet af et par minutter i 2003.

Akademisk forskning

Uddybende artikel: Malware forskning

Begrebet om at et computerprogram kan gengive sig selv kan spores tilbage til de oprindelige teorier om komplekse automatdata. John von Neumann vidste, at et program i teorien kunne reproducere sig selv. Fred Cohen eksperimenteret med computervirus og bekræftede Neumanns postulat og undersøgt andre egenskaber af malware såsom sporbarhed, selv-formørkelse ved hjælp rudimentære kryptering, og andre teknikker. Hans ph.d.-afhandling var om emnet computervirus.

Computervirus

Fra Wikipedia, den frie encyklopædi

En computervirus er et lille program, som i samspil med de computere og styresystemer, de er skrevet til, søger at overføre kopier af sig selv til andre computere uden brugerens viden eller tilladelse. Dette tager i sig selv en lille del af en "smittet" computers processor-kraft, da virussen 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 lagringsmedie (harddisk, USB-pen DVD m.v.) 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 vira kopierer sig et vist antal gange, før den destruktive programkode aktiveres.

Indholdsfortegnelse

Referencer

Spredning af vira

En computervirus er kendetegnende ved at den automatisk spreder sig fra en computer til en anden. Tidligere spredtes en computervirus fra computer til computer som "blind passager" på de disketter, man ofte brugte til at transportere programmer og/eller data mellem computere, men da internettet blev "allemandseje" i 1990'erne, opstod en ny "smittevej" og nye muligheder for misbrug: Nu kan en virus installere "bagdøre", der tillader virusprogrammøren at "overtage" den ramte computer og f.eks. beordre den til at udsende spam (uønskede reklamer via e-mail), og virke som "lagerplads" for illegale kopier af computerprogrammer, musik og film eller rapportere tilbage om, hvilke adgangskoder, der bliver indtastet, når brugeren f.eks. køber ind eller ordner bankforretninger over internettet. Dette er dog blevet mere sikker med indførelsen af MitId.

Beskyttelse mod virus

Der findes dog nogle metoder til at beskytte sig mod virus. Man kan f.eks. bruge såkaldte antivirusprogrammer. Desværre kommer der hele tiden nye vira, og pr. definition er antivirusprogrammer reaktive – Det vil sige at en virus skal opdages, før der kan udvikles en kur imod den. Der er desværre også eksempler på at nogle programmer udgiver sig for at være antivirus software, men i virkeligheden blot udnytter den generelle usikkerhed og uvidenhed omkring virus og dermed lokker intetanende computerbrugere til at installere det der senere viser sig i virkeligheden at være netop virus.

Virus på forskellige styresystemer

Der findes forskellige styresystemer (f.eks. Windows, Linux og Mac OS X), der påvirkes i forskellig grad af virus. Microsofts Windows er uden sammenligning det styresystem, der er skrevet flest vira til og derfor det styresystem, der er mest udsat for angreb. Den første virus blev introduceret i januar 1986 og inficerede Microsofts tidligere styresystem, MS-DOS. Virussen (ved navn "Brain") blev skrevet af brødrene Basit og Amjad Alvi fra Lahore i Pakistan, angiveligt med det formål at beskytte et af deres andre programmer mod piratkopiering. Den mere uskyldige virus (end hvad der i dag kan findes) havde brødrenes firma- og person navne indkodet i den. Siden Apples Mac OS X styresystemet blev frigivet i 2001, har der aldrig været rapporteret om en succesfuld computervirus på Mac OS X, der har spredt sig fra computer til computer og inficeret dem. Der har været rapporteret om få såkaldte trojanske heste og malware, der via brugerinteraktion (altså hvor brugeren selv aktiverer infektionen) kan bevirke at skadelig kode aktiveres. Som udgangspunkt er det derfor vigtigt ikke at installere software fra ukendte kilder, specielt hvis softwaren er pakket ind i et installeringsprogram, der beder om administrator password og/eller rettigheder – en typisk, men dog ikke nødvendig, fremgangsmåde for trojanske heste. Heller ikke spyware, er et udbredt fænomen på Mac OS X.

Idet Windows-styresystemet, hvortil der er udviklet mere end 100.000 kendte vira og et ukendt antal spyware programmer, ikke kan afvikles direkte på Mac OS X, hvilket også gælder de programmer, der er skrevet til Windows-styresystemet, er truslen fra disse Windows-specifikke vira og spion-programmer så godt som ikke eksisterende på Mac OS X.

Mac OS X er ikke usårlig, men Mac OS X er fra fødslen født med et væsentligt anderledes og fra grunden opbygget sikkerhedssystem. Mac OS X bygger således på arven fra UNIX (hvilket også gælder for Linux), der tog udgangspunkt i behovet for at mange brugere på store universiteter i bl.a. USA i starten af 1970'erne benyttede en og samme computer. Der var således behov for at opbygge et styresystem, der sikkert kunne adskille og håndtere mange brugere – et flerbruger-system. Systemet fjernede de helt grundlæggende administrator-rettigheder for almindelige brugere af styresystemet. Denne funktion blev først meget senere delvist tilføjet i Windows og var således aldrig tænkt ind fra starten. Netop denne hindring af adgang til helt grundlæggende administrator-rettigheder gør det mere end almindeligt svært at udføre væsentlige skadelige ændringer ved et eventuelt virusangreb). Manglende sikkerhed eller dårligt design er ofte det der får skylden for sikkerhedstruslen på en Windows computer.

Da UNIX grundlæggende er et åbent (open source) styresystem, er de mest kritiske komponenter i Mac OS X åbne for gennemsyn af en verdensomspændende gruppe af sikkerhedseksperter, der løbende vurderer og tester styresystemet og derved er med til at sikre at systemet hele tiden bliver vedligeholdt og opdateret.

Endvidere spiller det helt sikkert også en rolle, at Mac'en (der i dag benytter Mac OS 13) traditionelt har haft en meget lille markedsandel, der gør den mindre attraktiv for virus- og spyware-udviklere at bruge ressourcer på. Resultatet har været at de fleste Mac-brugere er sluppet for at bruge deres kræfter på opsætning af firewalls, antivirus-, antispyware og anden sikkerhedssoftware, som alle Windows-brugere skal installere og konfigurere for at holde sig (bedst muligt) beskyttet.

Der findes flere antivirusprogrammer til Mac OS X – f.eks. Norton AntiVirus og open source alternativet ClamXav der er gratis.

Virus og andre slags malware

Computervira er blot en af mange former for malware, omend ordet ofte bruges i flæng om flere forskellige typer malware. Andre er adware, spyware, bagdøre og trojanske heste. En anden meget udbredt "virus"- type er en hoax.

En computerorm er et enkeltstående malware program, der replicerer sig selv for at sprede sig til andre computere. Ofte, bruger det et computernetværk for at sprede sig og er afhængig af sikkerheds fejl på målcomputeren for at få adgang til den. I modsætning til en computervirus behøver det ikke at knytte sig til et eksisterende program. Orme forårsager næsten altid skade på netværket, hvorimod virus næsten altid korrupte eller ændre filer på en inficeret computer.

Mange orme, der er blevet lavet er designet til kun at sprede sig, og forsøger ikke at ændre de systemer, de passerer igennem. Men som Morris orm og Mydoom viste, kunne disse "payload " orme også forårsage større forstyrrelser ved at forøge netværkstrafikken og andre utilsigtede virkninger. En "code" er koden i ormen der er designet til mere end at sprede ormen — det kan slette filer på en host-systemet (f.eks. ExploreZip ormen), der kryptere filer i en cryptoviral afpresning eller sender dokumenter via e-mail. En meget almindelig ”code” for orme er at installere en bagdør i den inficerede computer for dermed at tillade oprettelsen af en "zombie" computer som så er under kontrol af forfatteren (Hackeren) af ormen. Netværket på sådanne maskiner er ofte benævnt botnets og er meget almindeligt anvendt af spam afsendere for at sende uønsket e-mail eller til at tilsløre deres hjemmeside-adresse. Spam er derfor anset for at være en finansieringskilde for oprettelsen af sådanne orme, og forfatteren af orme har lister over IPadresser på inficerede maskiner, som sælges til højstbydende. Andre forsøger at afpresse virksomheder så de undgår DDoS-angreb.

Brugere kan minimere truslen fra orme ved at holde deres computeres operativsystem og andre software opdateret, og undgå at åbne ukendte eller uventet emails, og kører firewall og antivirus software.

Bagdøre kan udnyttes af andre malware, herunder orme. Eksempler kan nævnes Doomjuice, som kan spredes ved hjælp af en bagdør åbnet af Mydoom og mindst én forekomst af malware der udnyttet rootkit var da Sony installeret BMG DRM software på millioner af musik cd'er i slutningen af 2005.

Indhold

Orme med gode hensigter

I begyndelsen af den første forskning i orme på Xerox PARC, har der været forsøg på at skabe nyttigt orme. Disse orme tillod mulighed for afprøvning af John Shoch og Jon Hupp Ethernet-principperne på deres netværk af Xerox Altoén computere. Nachi ”familien” af orme forsøgte at downloade og installere patches fra Microsofts hjemmeside for at fastsætte sårbarheder i værtssystemet – ved at udnytte de samme svagheder. I praksis, selv om dette kan have gjort disse systemer mere sikker, har det genereret en betydelig netværkstrafik, og genstart af computeren under en patch (opdatering), alt sammen uden samtykke fra computerens ejer eller bruger. Uanset deres værdi eller deres forfattere intentioner betragter de fleste sikkerhedseksperter alle orme som malware.

Flere orme, ligesom XSS orme, er blevet skrevet for at forske i, hvordan orme spredes. For eksempel effekten af ændringer i sociale aktiviteter eller brugeradfærd. En undersøgelse foreslog hvad synes at være den første computer orm, der opererer på det andet lag af OSI-modellen (Data link Layer), den udnytter topologi oplysninger såsom Content-adresser bare hukommelse (CAM) tabeller og Spanning Tree information gemt i Switches til at udbrede og sonder udsatte koder, indtil virksomhedens netværk var sikker.

Beskyttelse mod farlige orme

Orme spredes ved at udnytte sårbarheder i operativsystemerne. Software leverandører med sikkerhedsproblemer leverer regelmæssige sikkerhedsopdateringer (Se "Patch Tuesday"), og hvis disse er installeret på en maskine så vil hovedparten af orme være ude af stand til at sprede sig til computeren. Hvis en sårbarhed offentliggøres før sikkerhedsrettelsen er udgivet af leverandøren, vil et ”nul-dags angreb” være muligt. Brugere skal være på vagt over for åbning af uventet e-mail, og bør ikke køre vedhæftede filer eller programmer, eller besøge websteder, der er knyttet til sådanne e-mails. Men som med ormen ILOVEYOU, og med øget vækst og effektivitet af phishing-angreb, er det fortsat muligt at narre slutbrugeren til at køre skadelig kode.

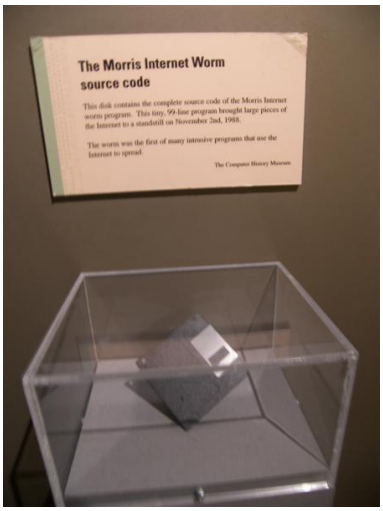
Anti-virus og anti-spyware software er nyttigt, men de skal holdes opdateret med nye opdateringer mindst hver anden dag. Brug af en firewall er også et ”must”. I April-juni beskriver dataloger i 2008, spørgsmålet om IEEE transaktioner på pålidelig og Sikre computer, en potentiel ny måde at bekæmpe internet-orme på. Forskerne opdagede hvordan indholdet af en slags orm, scannet internettet tilfældigt, efter sårbare værter

som kunne inficeres. De opdaget, at nøglen til løsningen var at få software til at overvåge antallet af scanninger, der sendes ud fra computer på et netværk. Når en computer begynder at sende for mange scanninger ud, var det et tegn på at den var blevet inficeret, så administratorer kunne frakoble det netværket og tjekke det for malware. Derudover kan analyse teknikker bruges til at registrere nye orme, ved at analysere deres adfærd på den formodede inficeret computer.

Dæmpningsteknikker

- ACL'erne i routere og switche
- Pakke-filtre
- TCP Wrapper/libwrap aktiveret network service dæmoner
- Nullrouting

Historie



Udtrykket "orm" blev første gang brugt i John Brunner 1975 roman, The Shockwave Rider. I denne roman, af Nichlas Haflinger designer og sætter han gang i en data-indsamlings-orm i en akt af hævn mod de magtfulde mænd, der kører en national elektronisk information web, der inducerer massive overensstemmelse. "Du har den største orm nogensinde løs på nettet, og den vil automatisk saboterer ethvert forsøg på at overvåge den...!"

2 november 1988, udløste Robert Tappan Morris, fra Cornell University, det der blev kendt som Morris ormen. Ormen forstyrret et stort antal computere og fortsatte derefter på internettet, man gættede på et tidspunkt at en tiendedel af alle de tilsluttede computere var inficeret. Under Morris appel proces, anslog den amerikanske appelret udgifterne til at fjerne virussen fra alle computer til at være omkring $200-53.000, pr computer, samtidig opfordrede retten til oprettelse af CERT Coordination Center og Phage postliste. Morris, selv blev den første person der forsøgte og dømt under 1986 Computer Fraud and Abuse Act i Amerika.

Afslutning

Dette var en lille guide/beskrivelse af virus i alle dens udformninger. Er du forvirret? – det er der ikke noget at sige til. It sikkerhed er en hel platform inden for it og virus truslen bliver ikke mindre i de kommende år.

Er det håbløst at bekæmpe virusangreb?

Nej, men det kræver, at man har en plan for hvad man gør den dag man er inficeret med virus. Hvis man kun bruger sin computer til at surfe på nettet og ikke bruger den til netbank e-boks mv., og der ikke er nogen data af værdi på computeren, så kræver det ikke de store forholdsregler. Er man derimod afhængig af at ens computer virker, evt. arbejdsmæssigt, eller har man data (billeder, dokumenter, mail mv.) man for alt i verden ikke vil miste, er det en god ide at have en katastrofeplan for den dag det går galt. Husk: Det er som med din brandforsikring; Du kan ikke tegne en, når huset er brændt ned!

Tilbagemelding

Jeg håber, at denne lille guide gav dig en lille indsigt i, de forskellige former for virus der findes og hvor komplekst det er at rense en computer for virus. Har du kommentarer eller forslag til viden, der bør være med i denne guide, modtager vi gerne RIS & ROS, på info@newtechit.dk

Stay safe and tuned!

Med venlig hilsen

Kim Kulebjerg
Indehaver NewTech IT
Tlf. 2299 9097