

Dette er en underside til : <http://www.oz1dis.dk/>

Virus/Malware - det er ikke nemt at beskytte sig imod.

Ud fra min viden om det problem der er skrevet om i dagens nyheder de sidste dage, så er det tydeligt - der er såvel agurketid som sommerferie involveret, ligesom der sås tvivl om hvad er det vi ser og oplever ...

Om det er planlagt eller ej, er svært at afgøre - men i Maj/Juni der var der en del advarsler om Asprox .. Hvis man dengang kikkede i de større anti-Malware fabrikanters info om problemet med Asprox, så fik man tydeligt det indtryk at det var en tussel som ikke betød noget.. se nederst hvor Panda og Symantec's info er vist.

De tal der tales om lige nu er ca 12.000 danske infiserede sider.. Det er dog en del, - uden at jeg kan sige om det er det rigtige antal. Når man ser på at man kan bruge en søgemaskine som Google - til at finde sider som er modtagelige for problemet ASPROX så kan man jo egentligt godt forstå det spreder sig.

Ser man så lidt længere tilbage - så var der en debat om ASP - og aktive X, som begge var problembørn fra Microsoft, og som derfor var noget man skulle undgå. På baggrund af den viden denne debat har givet, ser det ud som om nogen har genoplivet et gammelt problem ASPROX, og forsynet det med nye u-behageligheder. Det tyske magasin Heise.de - fortalte nemlig om dette nye tillæg til ASPROX.. men mon ikke dette druknede i mængden af omtale om emnet.

Ihvertfald så var det snart sommerferie - og vi trængte til den afslappelse - så måtte ikke vigtige ting venttil efter ferien.. så en del web-side administratorer inden for det offentlige de tog på ferie - uden at have opdateret deres sites, eller sikret sig de ikke kunne angribes. Nu er en del offentlige sider konstateret som værende inficeret, og de smitter dem som besøger de sider.. mest ærgerligt er nok at rigtig mange ikke opdager problemet..- i tide, ej heller dem som besøger de inficerede sider..

Journalisterne er hurtige til at spørge om en masse, og et fast spørgsmål er : hvad kan vi gøre for at beskytte os....osv..

Svaret er næsten lige så fast: sørg for at opdatere og ha et opdateret antivirus system.. osv..

Ak - ak, det virker som dagens scoop, her i agurketiden.. hvilket endda får en del til at skrive om det, og nogen reagere som dette fra TDC..

Agurketiden har ramt sommerdanmark. Flere store danske medier melder om et kæmpe virusudbrud.

24. juli 2008 kl. 12:11 Af Erik Jon Sloth <http://sikkerhed.tdconline.dk/publish.php?id=17959>

Der er ingen tvivl. Overskrifterne lyder "[Virus hærger 11.000 danske hjemmesider](#)" og "[Ekspert: Asprox-netvirus et kæmpe problem](#)", og tyder på at den nationale digitale infrastruktur er på randen af sammenbrud.

Gamle sikkerhedshuller

Men bag ordene gemmer sig en mere kedelig virkelighed, nemlig "Asprox" som blandt andet er omtalt i [en artikel fra det danske sikkerhedsfirma DK-Cert og Computerworld Online](#). Artiklerne beskriver det forhold at mange danske og udenlandske hjemmesider er ramt uden at vide det. Hvis du besøger en hjemmeside som er inficeret, vil Asprox forsøge at udnytte sikkerhedshuller på din pc til at sprede sig.

Problemet er blot at Asprox er fra maj i år, og at der for længst er kommet opdateringer, der lapper alle de huller som Asprox forsøger at udnytte.

Hold din pc opdateret

I sagens natur betyder det, at hvis du sørger for at holde din pc opdateret og anvende antivirus, vil alle kendte sikkerhedshuller på din pc være lappede - og så er risikoen for at blive ramt af Asprox minimal. I samme øjeblik Asprox forsøger at udnytte nye sikkerhedshuller, vil det blive opdaget af sikkerhedsfirmaerne, og der vil komme opdateringer til din antivirus eller dit styresystem.

Umiddelbart er der således ikke er nogen grund til at blive inde i det gode vejr af frygt for Asprox.

Tja - for dem som forstår problemet er det åbenbart ikke noget at være bekymret for - hullerne er lappet etc.. så vi kan sove roligt..

Nåja - måske så ikke sove - men se at få de opdateringer på plads, for ikke alle er lige hurtige - Quicktime kom med deres rettelser som lukke de asprox huller så sent som d 28 juli 2008, så hvordan ham fra tdc kan anføre sine kommentarer som gjort - kan vække min forundring..

Men jeg synes dette som den næste artikel berører er måske det bedste alt dette har ført med sig se ...:

Virusværktøjer gør åbenhed mere risikabelt

Hvad er det egentlige problem:

Dem som laver og vedligeholder de forskellige sites ved ikke nok..

mange gange er det folk som kan få sites til at se godt ud som får opgaven med at vedligeholde og udbygge en eller anden hjemmeside.. mon ikke de kan beskrives som dette viser, sakset fra et sted hvor webfolk snakker om dette og hint.

Asprox giver problemer.

Først og fremmest vil jeg lige sige at ASP programmering ikke er min stærkeste side. Alligevel er det, gennem lang tid og med en masse hjælp fra Eksperten, lykkedes mig at sammensætte en fin lille hjemmeside med login, gæstebog, nyhedsbrev osv.

Nu er den imidlertid blevet angrebet af Asprox.

Jeg har i den forbindelse været inde og læse lidt om Asprox og fundet bl.a. følgende:

"Hvad kan man gøre for at beskytte sig? Hvis man har ansvaret for en web-applikation, der kommunikerer med en database, er svaret: Skriv applikationen om.

Applikationen må ikke sende tekststrengene fra brugerinput direkte videre til databasen.

I stedet skal man enten rense input eller kalde stored procedures med parametre i stedet for direkte at udføre SQL-kald."

Det er lettere sagt end gjort for en anti-nørd som mig.

Hvordan gør man det rent praktisk?

Er der nogen steder jeg kan læse mere om det?

Desværre er der ikke nogen lette løsninger - for dem som laver de forskellige sites, de aner ikke hvad der skal gøres, og selv om der findes masser af værktøjer, såvel gratis som betalings udgaver, så er det ikke sikkeret at budskabet når frem til dem - og ydermere så opstår næste problem, erkendelsen af problemet, og ansvarfraskrivningen efterhånden som problmet bliver kendt opad i systemet, især inden for det offentlige.

En programmør jeg kender vedligeholder en del offentlige sider og han udtrykker; Ansvaret kan ikke placeres på en enkelt, for de enkelte dele er lavet over et utal af gange - og fortæller man dem som skal betale at det bliver dyrt... - fordi et eller andet skal skrives radikalt om pga sikkerhed..- så får man svaret det er der ikke penge til, lav det med det som vi har tilrådighed.

Med den indstilling så kan vi jo måske ikke forvente andet - vi må og skal selv sikre os..

Men kan vi så det???

Selvfølgelig dukker det ting som dette op..- uden at jeg ved om det virker..

Sponsorerede links

Asprox Fjerner du her

Prisvindende Anti Virus Program.

Få en Gratis 30 dages fuld version!

www.virusfighter.dk/Asprox

Det er ikke blevet lettere med den åbenhed der er om emnet, og så det at alle vil forsøge at opnå det bedste resultat, og derfor ligesom kopiere lidt rigeligt fra hinanden.

Lad os derfor se et på et eks.. :

Kan i huske jeg skrev om problemet med E-boks og crosssite scriptning. - og iflg de "kloge supportere" hos Eboks var det ikke noget problem.. og hvis jeg opfattede det som et problem, kunne jeg jo bare benytte en anden browser en IE, feks Firefox eller Opera. Ok - det var da et forslag ... men de nævnte browsere kopiere nu en hel del fra Microsoft IE - for se dette fra www.secunia.dk

eliminate the impact of these vulnerabilities.

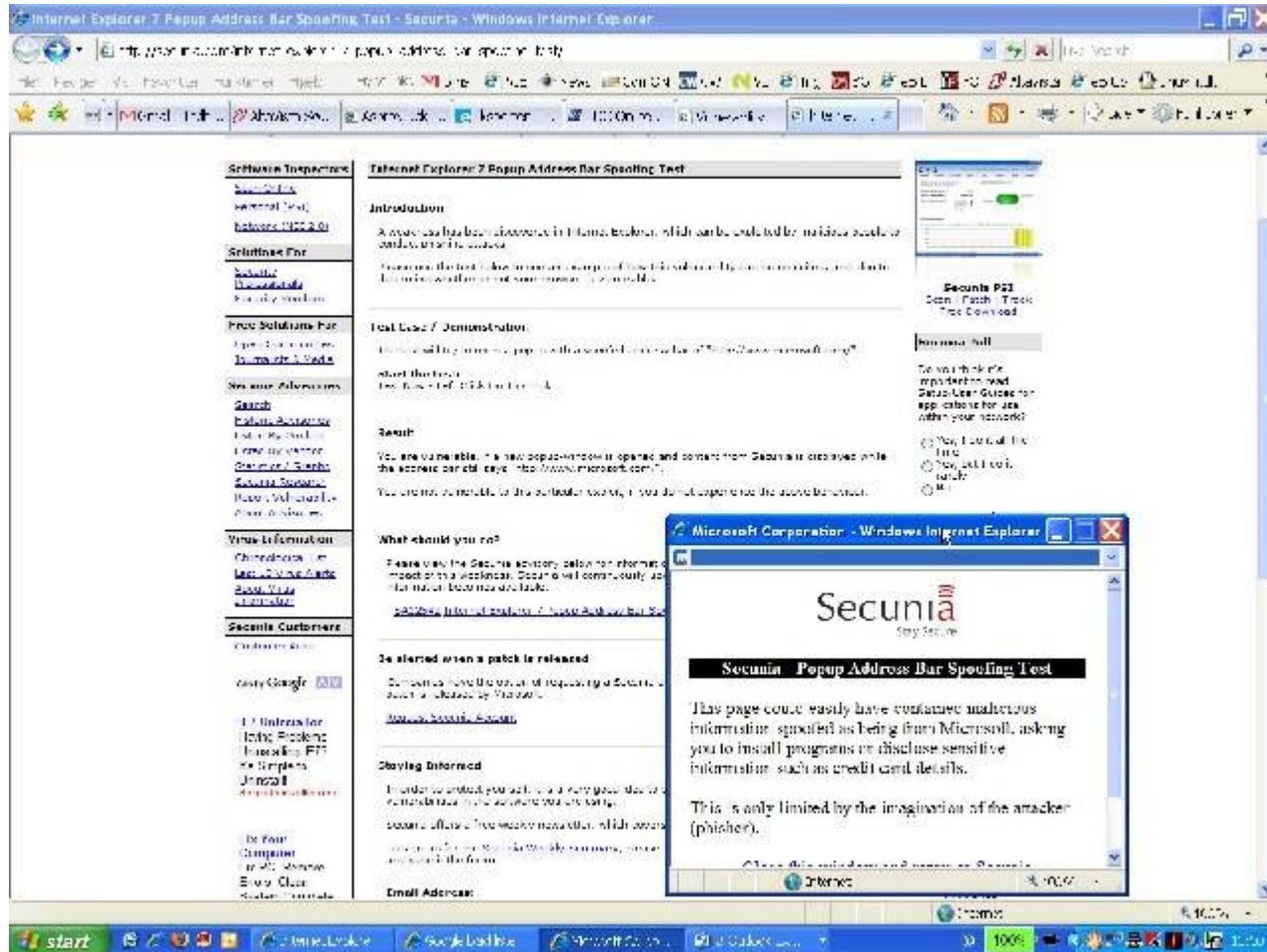
Internet Explorer 7 Popup Address Bar Spoofing Test

A vulnerability in Internet Explorer, which can be exploited to spoof the address bar of a popup-window. The vulnerability has been confirmed on a fully patched system with Internet Explorer 7.0 running on Microsoft Windows XP SP2. Other versions may also be affected. **Unpatched for 644 days.**

her gør firmaet opmærksom på at dette problem nu har været tilgængeligt i 644 dag med den dato vi skriver idag : 29 juli 2008. Så microsoft er ikke just hurtige til at lukke hullet.. - ude at jeg vil gætte på hvorfor, måske det ikke er så let endda..

En sådan fejl - tjå den eksisterer såmænd også i de andre browsere - se bare billeder lidt længere nede. så det er ikke kun MS Internet Explore der har problemet - desværre, derfor er brugen af E-boks et stort problem. Prøv bare at benytte en af de 2 andre browsere hvis du er i tvivl - og klik på denne link.. så kommer du frem til en test link. http://secunia.com/internet_explorer_7_popup_address_bar_spoofing_test/

her ses problemet stadig er aktuelt på MS IE7..



her ses problemet stadig er aktuelt på Firefox 3...



her ses problemet stadig er aktuelt på Opera 9.51



Så - det er ikke let at beskytte sin PC..

Det bedste råd fra min side.. : brug PSI fra <https://psi.secunia.com/> til at fortælle om din software er opdateret, husk at lade den teste alt software på din pc.= Se faneblad opsætning .. fjern markering i " vis kun let at opdatere software"... så gør i hvad i kan.

Virusværktøjer gør åbenhed mere risikabelt

Virusgrupperne overlader i højere grad arbejdet med at finde sårbarheder til sikkerhedsekspertter. Nu må eksperterne overveje, om fuld åbenhed er klogt.

Af [Jesper Stein Sandal](#), tirsdag 29. jul 2008 kl. 10:50

Den nye kriminelle underverden på internettet, der slipper virus løs, er mere til automatisering og avancerede værktøjer end til på egen hånd at finde frem til sårbarheder i software.

Derfor venter de på, at sikkerhedsekspertter frigiver detaljer om kendte sårbarheder, som de så kan basere et angreb på og angribe de brugere, der ikke har opdateret.

Tidligere var virusprogrammørerne ofte også dem, der selv forsøgte at finde frem til sårbarheder, men det har ændret sig, skriver IBM Internet Security Systems i dets kommende statusrapport ifølge nyhedsbureauet AP.

»Skurkene er ikke dem, der finder sårbarheder. De har ændret deres forretningsmetode, så de nu bygger videre på sikkerhedsmiljøets arbejde,« siger afdelingschef Kris Lamb fra IBM til AP.

Det betyder, at sikkerhedsekspertterne bør overveje, hvor hurtigt de skal frigive information om en ny sårbarhed, og hvor mange detaljer de skal afsløre.

Ifølge IBM-rapporten er det blevet mere almindeligt, at sikkerhedsekspertter ikke blot frigiver oplysninger om en sårbarhed, men i mange tilfælde også eksempler på kode, der kan udnytte den.

Det gør det let for de kriminelle at tilpasse eksempel-koden til et egentligt exploit, der kan bruges i de værktøjer, som bruges til at lave nye varianter af ondsindede programmer.

Fortalerne for den større åbenhed hævder, at det er med til at lægge pres på softwareleverandørerne, så de gør mere ud af sikkerheden omkring deres software, skriver AP.

Kommentarer (1)

Det er vel ikke en nyhed?
af [Henrik Kramshøj](#), 29. juli 12:37

"Ifølge IBM-rapporten er det blevet mere almindeligt, at sikkerhedsekspertes ikke blot frigiver oplysninger om en sårbarhed, men i mange tilfælde også eksempler på kode, der kan udnytte den."

Mere almindeligt?

Der HAR vi været, udviklingen HAR været at man frigav både information og proof-of-concept. Henover årene blev det så erkendt at man indimellem fik problemer ud af den model og mange valgt at følge i RFPs fodspor med responsible disclosure hvor leverandørerne får lidt ekstra tid. Mange har endda valgt IKKE at frigive kørende kode mod sårbarheder som de publicerer.

Så det er altså en bølgen frem og tilbage, hvor man idag ser begge dele. Respekt til begge lejre, for argumenterne er gode i begge lejre.

Summasummarum, der kommer altid kørende kode ud på internet og jeg ser som sådan ingen ændring i trenden. ... og mere vigtigt resultatet er det samme, der KOMMER kørende kode ret hurtigt efter de fleste advisories, uanset om eksperten der finder og publicerer selv laver koden eller andre gør det.

"Ifølge IBM-rapporten er det blevet mere almindeligt, at sikkerhedsekspertes ikke blot frigiver oplysninger om en sårbarhed, men i mange tilfælde også eksempler på kode, der kan udnytte den." Mere almindeligt? Der HAR vi været, udviklingen HAR været at man frigav både information og proof-of-concept. Henover årene blev det så erkendt at man indimellem fik problemer ud af den model og mange valgt at følge i RFPs fodspor med responsible disclosure hvor leverandørerne får lidt ekstra tid. Mange har endda valgt IKKE at frigive kørende kode mod sårbarheder som de publicerer. Så det er altså en bølgen frem og tilbage, hvor man idag ser begge dele. Respekt til begge lejre, for argumenterne er gode i begge lejre. Summasummarum, der kommer altid kørende kode ud på internet og jeg ser som sådan ingen ændring i trenden. ... og mere vigtigt resultatet er det samme, der KOMMER kørende kode ret hurtigt efter de fleste advisories, uanset om eksperten der finder og publicerer selv laver koden eller andre gør det.

Danske myndigheder fortier virusinfektion

Virussen Asprox har ramt flere danske offentlige hjemmesider - herunder Undervisningsministeriet. Men de ramte hjemmesider har været

tavse om virusinfektionen, og det er kritisabelt, for så ved brugerne ikke om de har været eksponerede, siger ekspert.

Af Jakob Møllerhøj, mandag 28. jul 2008 kl. 11:08

Miljøstyrelsen og Undervisningsministeriet er blandt de danske hjemmesider, som har været ramt af Asprox-virussen. Det kan Version2 i dag afsløre ved hjælp af Microsofts søgetjeneste live.dk.

Flere danske virksomheders hjemmesider er også blandt de ramte. Siderne er velkendte og betragtes normalt som sikre, men de kan have smittet besøgende. Virus-infektionerne er fjernet igen, men siderne har ikke advaret brugerne. Det finder ekspert kritisabelt.

Det er ikke kun i England, at Asprox-virussen har haft sin kedelige sejrgang på hjemmesider. Også i Danmark har Asprox – også kendt som Danmec hærget.

De ramte hjemmesider har fjernet det skadelige javascript, som var blevet injektet, og besøgende på hjemmesiderne risikerer dermed ikke længere at blive en del af Asprox-botnettet med alt, hvad det indebærer. Live.dk's cache funktion afslører dog alligevel, at den har været gal med siderne.

Selvom siderne nu er rensede, så kalder sikkerhedsekspert Peter Kruse fra CSIS det for 'bekymrende', at ingen af de offentlige eller store, private hjemmeside-ejere har været ude at fortælle brugerne, at hjemmesiderne har været inficerede. Problemet er, at brugerne således ikke er blevet bekendte med, hvorvidt de har været udsat for potentiel 'smittefare'.

»Jeg er bekymret for det. Jeg bryder mig ikke om, at folk kryber ned under dynen og gemmer sig for problemerne. Der er ingen grund til at stikke hovedet i jorden. Det her er et problem, som skal adresseres med åbenhed, ikke et problem man skal skjule. Og det er jeg bange for er tilfældet her. De tusindvis af danske websider – fra store til små – som har været eller stadig er inficeret med det skadelige javascript, har alle gjort det samme: De har puttet sig. De har fjernet problemet som en tyv om natten,« siger han.

Asprox er snedigt indrettet på den måde, at botnettet finder sårbare asp-sider, som kan injektes med et skadeligt javascript. Når scriptet ligger på siden, forsøger det at inficere besøgende klienter og indlemme dem ganske 'lydløst' i Asprox-nettet. Det foregår typisk gennem forældet og hullet Quicktime, gammel og gennemhullet java-jvm og ikke mindst uddaterede versioner af Internet Explorer på klienterne.

»Hvis man har eksponeret sine kunder eller de brugere, som kan ske at søge oplysninger hos ens organisation så synes jeg, det er ens forbandede pligt at fortælle om, at man har haft det her problem, så de, der har været eksponerede, kan gøre noget ved deres problem, så de ikke sidder og ikke aner, at de er blevet inficerede,« siger han.

Der er i sig selv ikke noget nyt i den måde javascriptet bliver sneget ind på siderne på. Og det undrer da også Peter Kruse, at folkene bag de virus-ramte hjemmesider ikke har garderet sig bedre mod angrebsmetoden med denne type SQL-injections, som har været kendt

og beskrevet gennem længere tid. Blandt andet her på Version2.dk.

Den Asprox/Danmec-variant, som har plaget flere danske hjemmesider, er født i maj måned i år. Hvilket vil sige, at trods advarsler og medieomtale, så har Asprox-problemet først fået mediernes generelle interesse, da den engelske avis The Times for nyligt kunne berette om massiv Asprox-invasion på engelske hjemmesider.

»Vi gik ud i slutningen af april og advarede omkring det her. Og Version2.dk bragte en artikel om sårbare hjemmesider og sql-injection. Og vi advarede i den forbindelse også specifikt om Asprpx/Danmec, men den blev åbenbart først taget op af den generelle presse som noget alvorligt, da The Times skrev om den,« siger Peter Kruse.

For at beskytte sig mod Asprox, er det vigtigt både at have opdateret sin tredjepartssoftware på klient-siden, men mindst lige så vigtigt også at gennemgå sin serverkode for eventuelle SQL-injectionhuller, fortæller Peter Kruse.

»Forebyggelse er den eneste løsning, der er på Asprox-problemet. Forebyggelse både på klient- og serversiden. Det er løsningen på dette problem, men også løsningen på fremtidige varianter i samme eller anden familie, som misbruger hullede websider som platform for angreb mod klienter. Asprox er snedig indrettet og er man først inficeret, så kan den opdatere sig selv og i al evighed lege kis pus med anti-virus programmerne,« siger Peter Kruse.

Version2.dk har forsøgt at indhente kommentarer fra både Miljøstyrelsen og Undervisningsministeriet, men det er ikke lykkedes før denne artikels deadline. Version2.dk følger dog op, såfremt de pågældende myndigheder vender tilbage.

Den finske antivirusproducent F-Secure mener, at antallet af nye vira i 2008 allerede har passeret en million. Malware-eksplosionen skyldes industrialiseringen af virusproduktionen, lyder det fra F-Secure.

Af [Jakob Møllerhøj](#), tirsdag 29. jul 2008 kl. 12:43

Med 2.300 nye vira om dagen i det Herrens år 2008 er antallet af den lede malware eksploderet. Den voldsomme stigning skyldes, at virusproduktionen er blevet industrialiseret, oplyser antivirusproducenten F-Secure i en pressemeddelelse.

Industrialisering betyder i F-Secure-terminologi, at de it-kriminelle arbejder lige så målrettet og professionelt, som de virksomheder, der

forsøger at stoppe [virus](#)

Og desuden er kompleksiteten af de it-kriminelles infrastruktur vokset i en sådan grad, at de kan oversvømme nettet med skadelig kode. Og så er der begrebet 'malware-as-a-service', som også har bidraget til den voldsomme virus-vækst. Begrebet dækker over, at de it-kriminelle hyrer hackerer til at lave virus til eksempelvis denial-of-service angreb.

Endeligt har polymorfe vira eller såkaldt Malware 2.0 godt fat i markedet. Det er computervira, som ændrer koden en kende, hver gang de bliver eksekveret. Derudover angriber Malware 2.0 enhver, der forsøger at undersøge virussen. Fx sikkerhedsekspert der graver i Storm-botnettets virke.

»Denne form for selvforsvarsmekanismer i computervira er et [tegn](#) på, at de it-kriminelle bliver dygtigere og dygtigere og mere og mere professionelle. Kampen på [internettet](#) mellem virus- og antivirusproducenter er blevet meget hårdere, og det er den million vira vi har identificeret på et så tidligt tidspunkt i 2008 et udtryk for,« siger Michael Dahl, Channel Manager for F-Secure i Danmark i følge pressemeddelelsen.

Virus lurer på DMI's hjemmeside

Asprox har uopdaget sneget sig på ind Danmarks Meteorologiske Instituts hjemmeside. Så længe virussens skadelige javascript ikke bliver afviklet, er der ingen kendt fare ved vejr-siderne, forsikrer instituttet. Et problem, at scriptet overhovedet findes på siden, mener sikkerhedsekspert.

Af Mads Nyvold, tirsdag 29. jul 2008 kl. 10:09

Asprox-virussen har også ramt hjemmesiden for Danmarks Meteorologiske Institut. Systemadministratorerne tager dog angrebet med omtrent samme sindsro, som feriefolket under parasollen nær kysten tangblå.

Asprox-virussen har ellers haft en særdeles kedelig sejrsgang hos flere engelske og danske myndigheder. Her har de besøgende risikeret at blive en del af Asprox-botnettet med nærmest alle former for digitale vederstyggeligheder. Endvidere var DMI ikke klar over smitten, før Version2.dk og Ing.dk kunne berette om den.

Virussens skadelige javascript ngg.js lod sig afsløre ved hjælp af Microsofts søgetjeneste live.dk. Hvorfra live.dk har linket fra, er også stadig en gåde for administratorerne af Danmarks mest brugte site, ifølge FDIM.

DMIs besindelse skyldes, at scriptet findes i forlængelse af en [URL](#) under verdensvejr-funktion. Helt præcist forbindelse med den polske by Szczecin.

Scriptet kunne faktisk ligeså vel have ligget under alle andre byer i verden, for i princippet kan alle oprette en [hjemmeside](#)

med et link og ad den vej få Asprox-virusset skadelige javascript ngg.js til at indgå i koden på verdensvejsiden. Mest vigtigt er, at scriptet tilsyneladende ikke afvikles.

»I dette tilfælde ødelægges højest afviklingen af det script, der bør afvikles, hvorimod det skadelige ngg.js ikke bliver afviklet. ngg.js findes ikke på vores sider eller servere, og som det fremgår af URL'en på search.live.com er scriptet placeret eksternt for dmi,« skriver DMI i en mail til Version2.dk.

»Det (ngg.js red.) inkluderes som en parameter i en søgning, der ikke bliver afviklet. Injectionen er altså ikke succesfuld.«.

Peter Kruse, sikkerhedseksperter hos CSIS, synes, at den udlægning af sådan en type SQL-injection er en anelse firkantet.

»Der er tale om en cross-site-scripting sårbarhed, hvor der ikke umiddelbart er nogen fare for brugere, der besøger siden. Det er under alle omstændigheder et problem. Jeg ved godt, at der kan være tusinder af årsager til, at scriptet optræder på siden, men det er typisk på grund af

manglende,« siger Peter Kruse

Published 2008-07-24 12:24

Google blacklister Connies CO2-kampagne Både Google og Firefox advarer mod at besøge hjemmesiden for klimakampagnen et ton mindre efter to angreb fra virussen Asprox. Ejeren er Klima- og Energiministeriet, der nu gennemgår siden for skadelige scripts. Af Mads Nyvold, Jakob Møllerhøj, mandag 28. jul 2008 kl. 16:31

Googles virus-diagnose for ettonmindre.dk

Alle, som besøger hjemmesiden ettonmindre.dk, kan udover miljøvenlige sparetips også meget vel få installeret programmer, der kaprer kodeordet til netbanken eller fjernstyrer computeren til at angribe andres systemer.

Advarslen kommer fra både Google og internetbrowseren Mozilla Firefox. Årsagen er Asprox-virussen i form af et skadeligt javascript. Bag ettonmindre.dk står Klima- og Energiministeriet, og ministeriet oplyser til Ingeniøren, at et konsulentbureau hoster sitet.

Bureauet opdagede et angreb sidste mandag, lukkede siden ned for at rense den og aktiverede den igen tirsdag. Men i løbet af weekenden satte et nyt angreb ind. Sitet blev atter lukket ned, men burde være sikkert nu, oplyser ministeriet.

Ifølge ministeriet bevirkede scriptet, at brugerne blev guidet videre til et japansk clicksitesite.

Version2.dk har berettet, at Asprox-virussen har haft sin kedelige sejrsgang på adskillige engelske butikkers og myndighedernes hjemmesider. Miljøstyrelsen og Undervisningsministeriet hører også til blandt de danske hjemmesider, der har risikeret at have smittet deres brugere, så de lydløst er blevet indlemmet i Asprox-nettet. Smitten foregår typisk gennem forældet Quicktime, gennemhullet java-jvm og gamle versioner af Internet Explorer på klienterne.

Sikkerhedseksperter Peter Kruuse fra CSIS Security Group har over for Version2.dk bebrejdet, at de danske myndigheder, som har fjernet Asprox-virussen fra deres sider ikke samtidig har forsøgt at oplyse deres brugere om sårbarheden.

Det, mener Peter Kruuse, er deres pligt. Ikke mindst fordi Asprox kan opdatere sig selv og snildt lege kis-pus med anti-virus programmerne.

Klima- og Energiministeriet oplyser, at man ikke har nogen planer om eksempelvis at indsætte et banner på ettonmindre.dk om, at sitet har været angrebet af virus. Dels fordi ministeriet ikke vurderer det som værende normal praksis, dels fordi ministeriet hæfter sig ved, at siden blev lukket ned lige så snart, at smitten var konstateret.

I øjeblikket er konsulentbureauet bag ettonmindre.dk ved at sikre sig, at alle skadelige scripts er elimineret fra sitet. Det er årsagen til, at Google og Firefox stadig blacklister det miljøvenlige site.

Blacklistningen foregår gennem organet Stop Badware administreret af Harvard Law School, Oxford University and Consumer Reports WebWatch.

»Det er skadeligt, at branchen fortier virus og ikke tager ordentligt ansvar for, at man havner på sådan en side. I fremtiden vil noget af det mest vigtige for, at folk gider besøge ens side være, at der er garanti for, at den er sikker,« siger Peter Kruuse.

Den seneste bølge af automatiserede SQL-injektion angreb, som bl.a. er gennemført fra BOTnettet Danmec/Asprox har tilsyneladende vækket Microsoft, som nu stiller tre gratis værktøjer til rådighed,

som kan anvendes til bedre at sikre og kontrollere sin hjemmeside for typiske sårbarheder der kan misbruges til at injektive skadelig kode på websiden og derved eksponere koden for almindelige besøgende.

Enhver webside administrator bør kigge nærmere på de tre nye værktøjer der netop er blevet frigivet af Microsoft. En kort beskrivelse af de forskellige værktøjer findes herunder:

1) UrlScan version 3.0 Beta

URLscan er et værktøj som kan anvendes til at stramme sikkerhed på Microsoft IIS servere. Værktøjet har eksisteret i snart flere år, men denne nye version indeholder nogle gode brug udvidelser. Man bør måske notere sig, at der er tale om en beta udgave af URLscan. Vi har imidlertid testet dette værktøj og er generelt meget fint tilfredse med resultatet. Der er mange gode forbedringer at hente i forhold til tidligere udgaver af URLscan.

2) Microsoft Source Code Analyzer

Et nyt værktøj som kan anvendes af webside administratorer til at finde ASP kode der kan være modtagelig overfor SQL injektion

3) Scrawl

En gratis SQL injektion scanner, udviklet af HP Web Security Research Group i samarbejde med Microsoft. Dette gratis værktøj kan anvendes til at scanne websider for SQL injektion sårbarheder.

Værktøjerne, og Microsoft's initiativ til at imødegå den stigende trussel fra automatiserede SQL injektion scanninger, kan findes på følgende URL: <http://www.microsoft.com/technet/security/advisory/954462.msp>

CSIS anbefaler, at webside administratorer og systemadministratorer af webservices internt i virksomhedens netværk, såsom intranet servere, printservere m.v., anvender disse værktøjer til at finde og lukke huller der kan give ondsindet kode eller personer, mulighed for at injektive scripts på dårligt sikrede websider og derved eksponere brugere for drive-by kode.

Den Digitale Vægter (<http://www.csis.dk/dk/produkter/ddv.shtm>), som har opnået PCI (Payment Card Industri) vendor godkendelse, bør naturligvis anvendes i kombination med sådanne gratis værktøjer og særligt hvis websiden tilbyder betalinger med kreditkort.

Voldsom netvirus i Danmark

En meget omtalt computervirus, Asprox, der menes at have ramt to millioner PC'ere verden over, findes også her i Danmark.



Computerviraet Asprox er et kæmpe problem, vurderer direktøren i it-sikkerhedsfirmaet DK-Cert, Shehzad Ahmad.

- Den er et meget stort problem, fordi den har ramt store populære sider. Og fordi den er en intelligent orm, der bliver ved med at sprede sig videre fra de ramte computere, forklarer han til dr.dk/nyheder.

Asprox har allerede inficeret 12.000 danske hjemmesider, og hvis man bliver ramt, lænser den computeren for alle oplysninger, fra netbankkoder til e-mail.

- Man registrerer ikke, at man bliver inficeret, og derfor øges risikoen for, at man spreder virussen via sin egen hjemmeside eller mail helt uden at vide det, tilføjer Shehzad Ahmad.

Virussen hæfter sig på ens computer, når man besøger en af de inficerede hjemmesider. Ifølge avisen The Times er det østeuropæiske hackere, der mistænkes for at stå bag virussen, og herhjemme er det både hjemmesider for små lokale rideklubber, slagtere og private blogs, men det er også store websider, som tilhører store danske virksomheder og ministerier, der er ramt.

Shehzad Ahmad råder til, at man laver en komplet scanning af sin computer for at finde ud af, om man er ramt. Samtidig er det vigtigt at holde sit antivirusprogram og sit antispywareprogram opdateret. Og hvis ens antivirusprogram finder Asprox på computeren, vil det fjerne virussen omgående.

Shehzad Ahmad er overrasket over omfanget af Asprox-angrebet.

- Det er sjældent, at det lykkes at sprede en virus så effektivt. Så måske er der nogle antivirusprogrammer, der har svigtet, siger han.

Publiceret
30. maj 2008
Klokken 14:30
på cw.dk/art/46091

Printet 29. juli 2008

DK-CERT: Botnet angriber med SQL-indsætning

Nogle af de massive angreb med SQL-indsætning kommer fra botnet, der bruger dem til at inficere nye pc'er, skriver lederen af DK-CERT, Shehzad Ahmad, i sin månedlige klumme.

Af Shehzad Ahmad

I de seneste måneder har en række legitime websteder spredt skadelig software.

Det sker ved, at der på websiderne står script-kommandoer, der henviser til en anden webside, hvorpå de skadelige programmer kører.

Disse programmer forsøger at udnytte velkendte browsersårbarheder til at installere software.

Den sidste del af angrebet er forholdsvis nem at forstå. Men hvordan går det til, at kendte og respekterede websteder som USA Today, ABC News og Packard Bell spreder skadelige programmer?

Forklaringen er, at de er ramt af SQL-indsætning.

En angriber har udnyttet en sårbarhed i web-applikationer på de pågældende websteder til at snige den skadelige script-kode ind på siderne.

I praksis foregår det ved, at angriberen i et inputfelt eller et argument i en URL-streng tilføjer nogle SQL-kommandoer.

Hvis web-applikationen ikke tjekker input, men bare sender hele tekststrengen videre til databasen, bliver SQL-kommandoerne udført.

Denne angrebsform er velkendt.

Det, der har undret os gennem de seneste måneder, er den store mængde af sider, der tydeligvis var blevet ofre for SQL-indsætning.

Det er så mange, at der må ligge en form for automatiseret angreb bag.

Asprox angriber
Sikkerhedsforsker Joe Stewart fra firmaet SecureWorks fandt for nylig en vigtig brik til puslespillet.

Han følger aktiviteten på botnet, altså netværk af pc'er, der uden deres ejers vidende bliver fjernstyret af nogle bagmænd.

Joe Stewart opdagede, at botnettet Asprox blev opdateret med ny software i begyndelsen af maj.

Den nye software var et værktøj til SQL-indsætning. Værktøjet søger via Google efter websteder, der indeholder .ASP-sider.

Herefter forsøger værktøjet at indsætte SQL-kommandoer på de sider, Google-søgningen har fundet frem til. Hvis det lykkes, bliver der tilføjet en tekststreng til en række felter i databasen.

Tekststrengen indeholder en kommando, der åbner et script i en såkaldt Iframe.

Denne kommando vil blive vist og eventuelt udført, når databasefelterne indgår i en webside, der vises i en browser.

Herefter føres man hen til en ny webside, der prøver at udnytte kendte sårbarheder til at installere programmer med. Hvilke programmer? Det kunne for eksempel være botnet-programmet, så gæsten også bliver indrulleret i det.

Fast flux

En særlig finesse ved dette angreb er, at det er koblet sammen med et såkaldt fast flux-netværk.

I et fast flux-net er et domænenavn koblet til en lang række IP-adresser, der skifter med korte mellemrum.

På ét tidspunkt fører et besøg på domænet til én IP-adresse, nogle minutter efter til en helt anden.

Koblingen er smart, fordi IP-adresserne alle tilhører pc'er i Asprox-botnettet.

Så SQL-angrebet indeholder et Iframe-link til et script på et bestemt domæne.

Dette domæne henviser igen til én ud af en række IP-adresser. Når en af pc'erne forsvinder fra nettet, fx fordi dens ejer scanner sin pc for virus, er der straks nye, som kan tage dens plads.

Problemet er udbredt. En Google-søgning foretaget i denne uge viser, at godt 119.000 websider har været ramt af angrebet fra Asprox-botnettet.

Hvad kan man gøre for at beskytte sig? Hvis man har ansvaret for en web-applikation, der kommunikerer med en database, er svaret: Skriv applikationen om.

Applikationen må ikke sende tekststrengene fra brugerinput direkte videre til databasen.

I stedet skal man enten rense input eller kalde stored procedures med parametre i stedet for direkte at udføre SQL-kald.

DK-CERT (www.cert.dk) er det danske Computer Emergency Response Team.

I samarbejde med tilsvarende CERT'er over hele verden indsamler DK-CERT information om internetsikkerhed. DK-CERT udsender advarsler og tager imod

anmeldelser af **sikkerhedsrelaterede** hændelser på internettet.

DK-CERT's leder, Shehzad Ahmad, opdaterer den sidste fredag i hver måned Computerworlds læsere med de seneste tendenser inden for it-sikkerhed.

Panda's Encyclopedia

Asprox.A

[Threat Level](#) [Damage](#) [Distribution](#)

[At a glance](#) [Tech details](#) | [Solution](#)

[Common name:](#)

Asprox.A

[Technical name:](#)

Trj/Asprox.A

[Threat level:](#)

Medium

[Type:](#)

[Trojan](#)

[Effects:](#)

It makes the affected computer become a proxy server, which would allow it to carry out malicious actions from the affected computer, using the IP address of the affected user and avoiding being tracked. It does not spread automatically by its own means.

[Affected platforms:](#)

Windows 2003/XP/2000/NT

[First detected on:](#)

Jan. 21, 2008

[Detection updated on:](#)

Feb. 5, 2008

[Statistics](#)

No

Brief Description

Asprox.A is a [Trojan](#) designed to make the affected computer become a [proxy](#) server. This would allow it to carry out malicious actions

from the affected computer, using the IP address of the affected user.

This way, *Asprox.A* could obtain information from the computer and send it to its creator without being discovered, as the IP address from which the data is sent belongs to the affected user.

Asprox.A does not spread automatically by its own means. It needs an attacking user's intervention in order to reach the affected computer.

Visible Symptoms

Asprox.A is difficult to recognize, as it does not display any messages or warnings that indicate it has reached the computer.

Norton's Encyclopedia (symantec)

Trojan.Asprox

Risk Level 1: Very Low

Discovered: June 8, 2007

Updated: June 11, 2007 3:41:26 PM

Also Known As: TROJ_ASPROX.A [Trend]

Type: Trojan

Infection Length: 40,960 bytes and 61,440 bytes

Systems Affected: Windows 98, Windows 95, Windows XP, Windows Me, Windows NT, Windows Server 2003, Windows 2000

Trojan.Asprox is a Trojan horse that uses the compromised computer as a proxy server.

Protection

- **Initial Rapid Release version** June 8, 2007 revision 022

- **Latest Rapid Release version** July 24, 2008 revision 040
- **Initial Daily Certified version** June 9, 2007 revision 007
- **Latest Daily Certified version** July 24, 2008 revision 067
- **Initial Weekly Certified release date** June 13, 2007

Click [here](#) for a more detailed description of Rapid Release and Daily Certified virus definitions.

Threat Assessment

Wild

- **Wild Level:** Low
- **Number of Infections:** 0 - 49
- **Number of Sites:** 0 - 2
- **Geographical Distribution:** Low
- **Threat Containment:** Easy
- **Removal:** Easy

Damage

- **Damage Level:** Low
- **Payload:** Uses the compromised computer as a proxy server.

Distribution

- **Distribution Level:** Low

Writeup By: Paul Mangan and Fergal Ladley

Asprox botnet malware morphs

Related Articles

- [Asprox botnet rears its ugly head](#)
- [Fortinet: Storm Worm botnet used to mount phishing attacks on Barclays, Halifax banks](#)

- [Thousands more sites infected in SQL injection attack](#)
- [Sony PlayStation website hit by SQL attack](#)
- [Phishing attack targets Monster.com](#)
- [Gartner: US\\$3.2 billion lost to phishing attacks in one year](#)
- [Quebec police break up massive botnet operation](#)

By [Sue Marquette Poremba](#)

May 16, 2008 10:00 AM

According to SecureWorks, provider of managed security services, the attack tool has infected more than 2,000 websites as of Thursday afternoon.

It is used to grab victims while they're surfing the web, building up the Asprox bot family. The same people behind Asprox are responsible for Danmec, a password-stealing trojan.

Joe Stewart, director of malware research at SecureWorks, has been monitoring Asprox for more than a month. He said it had been the only bot focused on phishing, but that focus changed when he noticed a binary on a system performing SQL injection attacks.

"It appears to be trying to build up the size of the botnet, infecting people through web pages by adding an IFRAME," Stewart told SCMagazineUS.com on Thursday.

The attacks occur on websites that are running Microsoft SQL-SVR (Server) that already have some sort of vulnerability, he added.

Also, the botnet takes advantage of unpatched Microsoft Internet Explorer browsers. The attack targets range from small businesses to universities.

"It is basically working through random Google searches," Stewart said. "It feeds random phrases and goes out and searches for those phrases."

The botnet attempts to compromise any page that comes back with an .asp suffix and uses a defined parameter, such as ID.

While Asprox has been a minor player in the botnet field, Stewart said it is obvious it is trying to build itself up in a big way.

[See original article on scmagazineus.com](#)

Asprox botnet now equipped with SQL injection tool

[SecureWorks report](#) that the Asprox botnet is being updated with a binary called msscctr32.exe. This turns out to be an automated SQL injection tool. Masquerading as a "Microsoft Security Center Extension", the tool searches Google for flaws in .asp pages and injects an iframe into the pages that forces visitors to download malicious JavaScript from direct84.com, a domain with a very questionable Whois record registered on May 7 2008, containing the details

Name: norman Company: zevs Address: gellion 13-13 City: Error State: 3562 Country: AU Zip: 123456 Tel No: 749 7983456 Fax No:
Email: zevsanet@gmail.com

which, however, genuinely appears to have been registered from Australia, as "gellion" is a little-known street name in Roxburgh Park, Melbourne.

The link ultimately redirects to a server that, according to the report, attempts to propagate Danmec, Asprox and the SQL injection tool. SecureWorks noted that only Asprox is capable of propagating the malware. The target server was down when tested by SecureWorks.