DK•CERT

Trendrapport

It-sikkerhed i første kvartal 2011

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

Redaktion: Shehzad Ahmad, Jens Borup Pedersen, Tonny Bjørn og Dennis Panduro Rand, DK•CERT

Grafisk arbejde: Kirsten Tobine Hougaard, UNI•C

Foto: colourbox.com

Om DK•CERT

Det er DK•CERTs mission at skabe øget fokus på it-sikkerhed ved at opbygge og skabe aktuel, relevant og brugbar viden. Denne viden gør DK•CERT i stand til at offentliggøre og udsende advarsler og anden information om potentielle risici og begyndende sikkerhedsproblemer.

DK•CERT bygger på en vision om at skabe samfundsmæssig værdi i form af øget it-sikkerhed. Det sker gennem offentliggørelse af viden om it-sikkerhed skabt gennem samarbejde med den offentlige og private sektor, forsknings- og undervisningsverdenen, samt internationale samarbejdspartnere.

Denne viden benytter DK•CERT til at udvikle services, der skaber merværdi for DK•CERTs kunder og øvrige interessenter og sætter dem i stand til bedre at sikre deres it-systemer.

DK•CERT, det danske Computer Emergency Response Team, blev oprettet i 1991 som en afdeling af UNI•C, Danmarks it-center for uddannelse og forskning, der er en styrelse under Undervisningsministeriet.

DK•CERT var blandt pionererne, der først i 1990'erne tog initiativ til etablering af et internationalt samarbejde om it-sikkerhed med grundidé i CERT/CC i USA. Som led i dette samarbejde overvåger, rådgiver og informerer DK•CERT om it-sikkerhed i Danmark.

DK•CERT samarbejder med GovCERT (Government Computer Emergency Response Team), der er den danske stats internetvarslingstjeneste. DK•CERT bidrager med information rettet mod borgerne og mindre virksomheder om aktuelle trusler og sikkerhedshændelser.

Indholdsfortegnelse

1. Resume

I første kvartal modtog DK•CERT 10.509 rapporter om sikkerhedshændelser. Det er en stigning på 54 procent i forhold til sidste kvartal af 2010. I gennemsnit modtog DK•CERT 3.503 henvendelser om måneden mod 2.990 i 2010.

De fleste sager handlede om piratkopiering. Siden 2010 har DK•CERT ændret på klassificeringen af hændelser. Det medfører, at der er indført en ny hændelsetype, brute-force-angreb. Den var den tredjehyppigst forekommende type hændelse i første kvartal.

Der blev fundet 26 procent flere skadelige programmer i første kvartal 2011 end i sidste kvartal. To tredjedele af de nye trusler er trojanske heste. Trods væksten blev der registreret færre infektioner med skadelige programmer på danske computere.

Mængden af nyopdagede sårbarheder i kvartalet var 1.126. Det svarer til gennemsnitsmængden i de seneste kvartaler.

DK•CERT har i første kvartal gennemført sikkerhedstest af computere på Forskningsnettet. Den viser, at over halvdelen af de IP-adresser, der kan nås fra internettet, indeholder sårbarheder. Kun seks procent af sårbarhederne vurderes at være kritiske.

I første kvartal modtog DK•CERT 30 rapporter om danske pc'er, der indgår i botnet. Rapporterne bygger på analyse af trafikken til de centrale servere, der styrer botnettene.

I februar offentliggjorde GovCERT, at staten i samarbejde med internetudbyderne nu går aktivt ind i kampen mod botnet. Det skal blandt andet blive muligt at blokere for trafik fra pc'er, der indgår i botnet. Indsatsen sker i et samarbejde mellem IT- og Telestyrelsen (GovCERT), DK•CERT og ISP Sikkerhedsforum.

På internationalt plan blev et af de største botnet sat ud af kraft. Via en koordineret indsats fra Microsoft og politimyndighederne blev botnettet Rustock lammet. Det førte til et mindre fald i mængden af spam på verdensplan.

De it-kriminelle bliver stadig mere professionelle og specialiserede. Seneste eksempel på den tendens er fremkomsten af såkaldt Exploit as a Service. Det er en tjeneste, hvor man mod betaling kan leje sig ind på en server, der forsøger at inficere pc'er, som besøger bestemte websteder. Dermed slipper de kriminelle for selv at skulle udvikle angrebsprogrammer og vedligeholde infrastruktur.

På den positive side kan man til gengæld se, at de danske virksomheder har fået råd til at investere i it igen. Når de køber nye pc'er, udstyres de med nye styresystemer. Dermed er det sandsynligt, at der bliver færre computere med gamle og sårbare Windows-versioner.

2. Første kvartal 2011 i tal

Dette afsnit beskriver med udgangspunkt i de systemer og netværk, som DK•CERT har adgang til, udviklingen i første kvartal 2011. Enkelte data er suppleret og/eller perspektiveret med data fra internettets åbne kilder. Selvom det hovedsageligt er hændelser på det danske Forskningsnet, der beskrives, mener vi, at afsnittet er med til at tegne et billede af it-kriminalitetens udvikling på hele den danske del af internettet. Dette billede er ikke fuldstændigt. Vi håber på, at det i kombination med din egen viden og erfaring kan give et fingerpeg om, hvordan du kan være med til at beskytte danskernes it-aktiver nu såvel som i fremtiden.

Vi indleder overordnet med at beskrive de sikkerhedshændelser, der i første kvartal 2011 blev anmeldt til DK•CERT. I det følgende afsnit beskrives statistik vedrørende scanninger. Herefter giver vi en pejling på udviklingen med hensyn til spredning af malwaremalware, spam og phishing. Afslutningsvis beskrives de sårbarheder, som blandt andet forsøges udnyttet ved scanninger, drive-by-attacks og lignende. Med data hentet fra DK•CERTs egen sårbarhedsdatabase beskriver vi kvartalets nye sårbarheder.

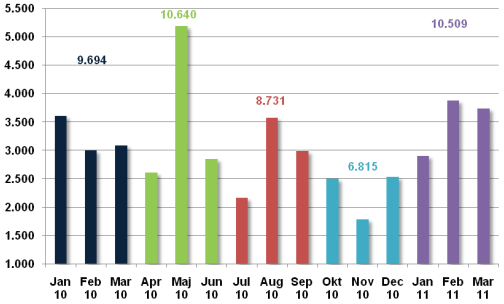
Ved overgangen til 2011 overgik DK•CERT til et nyt system til registrering og behandling af sikkerhedshændelser. Det har medført en ændring både i måden, hvorpå en hændelse registreres, og i klassificeringen af sikkerhedshændelser og de data, der beskriver en sådan. Det betyder, at ikke alle data er direkte sammenlignelige med tidligere, men også at ikke alle data på nuværende tidspunkt er tilgængelige.

2.1. Sikkerhedshændelser i første kvartal 2011

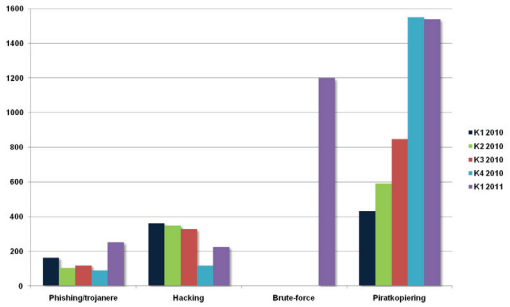
2011 startede i forhold til kvartalerne inden med en stigning i antallet af henvendelser til DK•CERT om sikkerhedshændelser på internettet (Figur 1). I første kvartal af 2011 modtog vi i alt 10.509 rapporter om sikkerhedshændelser, hvilket gav anledning til registrering af 9.208 unikke hændelser vedrørende 4.877 forskellige IP-adresser placeret over det meste af verden. I gennemsnit modtog vi 3.503 henvendelser om måneden mod 2.990 i 2010.

Antallet af unikke hændelser, hvor legale danske websites var blevet kompromitteret og medvirkede til phishing eller spredning af malware, steg i første kvartal 2011 til 253. Det er det højeste antal, DK•CERT hidtil har registreret (Figur 2). Flere af disse websites modtog vi henvendelser om fra mange forskellige parter. På nogle fik vi flere henvendelser fra samme part, da den ansvarlige hostingudbyder ikke hurtigt nok fik løst problemet. I enkelte tilfælde tog det op til tre uger, før en phishing-side blev fjernet. Tallene dokumenterer, at udnyttelse af sårbare legale websites indgår som en væsentlig del af de it-kriminelles aktiviteter. Løsningen skal primært findes hos hostingudbyderne, som bør have større fokus på sikring af kundernes websites, samt i større grad udvise rettidig omhu når det går galt.

Når sikkerhedshændelser kategoriseret som "hacking" i første fjerdel af 2011 er faldet i antal i forhold til hele 2010, kan det skyldes måden, hændelserne kategoriseres på. Det lave antal i fjerde kvartal 2010 skyldes, at mange hændelser blev kategoriseret anderledes. Enkelte hændelser, som tidligere blev kategoriseret som "hacking", kategoriseres i dag som brute-force angreb, hvor man forsøger at "gætte" kombinationer af brugernavne og passwords til SSH-tjenester, mail og



Figur 1. Sikkerhedshændelser rapporteret til DK•CERT.



Figur 2. Væsentligste typer sikkerhedshændelser rapporteret til DK•CERT.

lignende. DK•CERT modtog i første kvartal 2011 i alt 1.198 rapporter om forsøg på brute-force angreb.

Første kvartal 2011 bød på 1.538 henvendelser om krænkelse af rettigheder til film, musik og software foretaget fra danske IP-adresser, primært placeret på Forskningsnettet. Det høje antal hændelser om piratkopiering er på niveau med fjerde kvartal 2010. Tallet er foruroligende, da 25 procent af al piratsoftware er inficeret med malware. Piratkopiering er således ikke blot et spørgsmål om at snyde kunstnere og organisationer, men i lige så høj grad om mulig kompromittering af sikkerheden på de systemer, der benyttes.

De øvrige hændelsestyper, som i første kvartal 2011 blev rapporteret til DK•CERT, behandles til dels i de kommende afsnit.

2.2. Scanninger

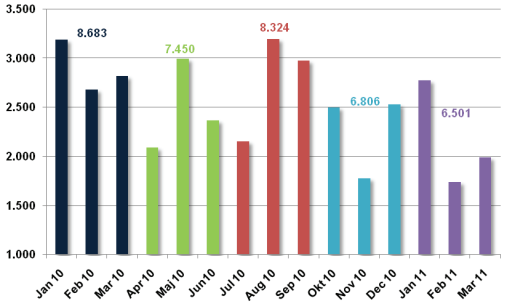
Overgangen til et nyt system til registrering og behandling af sikkerhedshændelser har blandt andet medført, at en del scanninger fra februar måned mere korrekt er blevet kategoriseret som forsøg på brute-force angreb. Det kan forklare, hvad der umiddelbart ligner et fald i antallet af scanninger i første kvartal 2011 (Figur 3). I alt registrerede DK•CERT 6.501 rapporter om sikkerhedshændelser, som blev kategoriseret som scanninger.

DK•CERT betragter scanninger som et mindre, om end forstyrrende problem. Det skyldes, at de it-kriminelle der er ude efter penge, kun i begrænset omfang benytter sig af scanninger. Den største andel af scanningerne formodes at have rod i ældre malware, som stadig florerer i egne af verden, hvor nyeste softwareversioner og opdateringer er mindre almindelige end i Danmark. I Asien og Afrika, hvor antallet af internetforbindelser vokser hastigt, må det formodes, at sikkerhedssoftware ikke er en del af "standardpakken". Her gives der mulighed for, at ældre malware stadig kan sprede sig, hvilket kan aflæses i vores statistikker

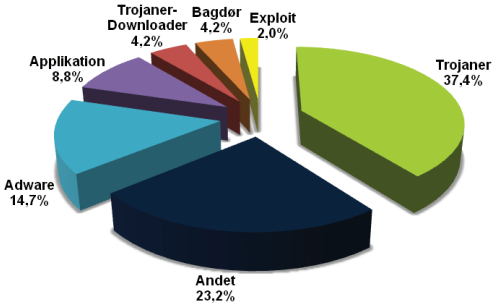
2.3. Malware, spam og phishing

Mængden af ny malware steg i første kvartal 2011 med 26 procent i forhold til fjerde kvartal 2010. I gennemsnit identificerede sikkerhedsfirmaet PandaLabs 73.000 nye malware-stammer om dagen, hvoraf næsten 70 procent var trojanske heste[1]. Næsten en fjerdedel af den webbaserede malware, som blev blokeret i marts måned, var ny ifølge virksomheden MessageLabs[2]. Det står i kontrast til, at sikkerhedsfirmaet F-Secure kun identificerede 2.082 danske malware-inficeringer i første kvartal 2011, eller kun cirka en tredjedel i forhold til året inden. DK•CERT tager dette som udtryk for sikkerhedsindustriens stigende udfordringer med at identificerer og fjerne ny malware.

Den hyppigste malware som blev identificeret af F-Secure i Danmark, var også i første kvartal 2011 trojanske heste, som stod for 37,4 procent (Figur 4). Det er et fald i forhold til tidligere. Derimod var der flere inficeringer, der blot blev kategori-



Figur 3. Antal scanninger rapporteret til DK•CERT.



Figur 4. Danske malware-infektioner identificeret af F-Secure i første kvartal i 2011[3].

1 Pandasecurity.com, 2011; "*Creation of New Malware Increases by 26 Percent to Reach More than 73,000 Samples Every Day, PandaLabs reports*".

2 Messagelabs.com, 2011; "*March 2011 intelligence report*".

3 F-secure.com, 2011; "*F-Secure security lab - virus world map*".

seret som "andet" eller "applikation". Inficeringer med orme eller vira er hver især faldet til at udgøre mindre end 1,5 procent af de danske malware-inficeringer. En mindre del af den identificerede malware besidder i dag evnen til at sprede sig uden hjælp fra brugeren.

Globalt set skulle man i første kvartal 2011 kigge lidt længere i indbakken for at finde spam. Spam udgjorde i marts måned på verdensplan "kun" 79,3 procent af alle mails, mens andelen herhjemme var 78,9 procent. En ud af 917 danske mails indeholdt virus, medens en af 1.259 mails var phishing-forsøg[4]. For begge typer er der tale om et fald i forhold til sidste år.

Et fald i andelen af phishingmails har ikke betydet færre danske websites, som blev inficeret med phishing-sider. DK•CERT modtog i første kvartal 2011 et stigende antal rapporter om danske websites, som var inficeret med trojanske heste eller phishing-sider (Figur 5). Hvad der i sidste halvdel af 2010 lignede et fald er således vendt. Noget af denne stigning formodes at kunne tilskrives overgangen til et nyt system til registrering og behandling af sikkerhedshændelser.

Overordnet set mener DK•CERT, at ovenstående udvikling beskriver fire tendenser:

- Det er i dag vanskeligere entydigt at kategorisere malware-typerne. Som et eksempel på det indgår botnet-programmer ikke i F-Secures statistikker. I DK•CERT modtog vi i første kvartal af 2011 30 rapporter om danske computere, der var inficeret med botnet-programmer. Rapporterne byggede på analyse af trafikken til kendte command & control-servere.

- Der er sket en specialisering gennem hele forsyningskæden for it-kriminalitet. Det er ikke længere de samme, som udvikler exploits, kode til indsamling af data fra de inficerede computere, eller den tekniske infrastruktur i for eksempel et botnet. Tilsvarende er de, der udvikler værktøjer, ikke længere de samme som dem, der bruger dem til for eksempel indsamling og misbrug af kreditkortinformationer.

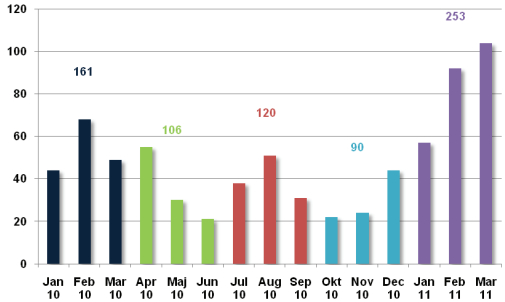
- I takt med at brugerne har blokeret adgangen til computeren gennem firewalls, og der ikke som standard eksekveres kode i mailklienten, foregår spredningen gennem mere effektive medier som for eksempel sociale netværkssider eller websider, brugerne har tillid til.

- For at undgå detektering udføres malware-kampagner over kortere tidsperioder og mere lokalt. Det har nødvendiggjort udvikling af en stigende mængde ny malware.

Exploit as a Service (EaaS) er et begreb vi forventer at se mere til. Servicen, der har hentet sit navn fra cloud-terminologien har eksistert i nogen tid. Den er et udtryk for en specialisering af den it-kriminelle forsyningskæde. Fordelen for de it-kriminelle er, at de ikke som tidligere behøver at tænke på installation, opsætning og hosting. Kombineret med en billig prisstruktur gør det, at vi vil se en stigning i brugen af disse services. Det bekræftes af en sikkerhedsforsker, som har fået indsigt i forretningen bag EaaS-servicen "Robopak Exploit kit", der understøtter udnyttelse af sårbarheder i produkter som for eksempel Java, PDF og Internet Explorer[5]. Prismodellen for servicen er delt op i tre typer:

4 Messagelabs.com, 2011; "*March 2011 intelligence report*".

5 Kahusecurity.com, 2011; "*Robopak Exploit Kit*".



Figur 5. Websites med trojanske heste og phishing-sider rapporteret til DK•CERT.

Exploit as a Service (EaaS)

Exploit as a Service er en tjeneste, hvor udnyttelse af hostet exploit-kode (angrebsprogrammer) tilbydes som en betalbar service. Henvisning til koden placeres på sårbare legale websider. Koden vil efterfølgende forsøge at inficere websidens besøgende med malware.

Tjenestens navn refererer til, at der er tale om en form for Software as a Service (SaaS) i stil med Google Docs, Hotmail og lignende.

- En dag: 30 dollar (ca. 160 kroner).
- En uge: 150 dollar (ca. 790 kroner).
- En måned: 500 dollar (ca. 2.700 roner).

Den type service forventes at blive brugt af nye kriminelle grupperinger, som ønsker at træde ind på markedet for it-kriminalitet.

DK•CERT forventer, at der vil komme flere lignende services. Flere udbydere må forventes at medføre lavere pris, hvorved servicen bliver mere attraktiv at bruge. Særligt hvis de bundles med værktøjer som for eksempel trojanske hest, botnet--programmer og andet i "brugervenlige" crimeware-pakker, der kan håndtere hele processen fra inficering af legale websites over dataindsamling til rekruttering af muldyr.

2.4. Sårbarheder

Der blev i første kvartal 2011 offentliggjort 1.126 CVE-nummererede sårbarheder (Figur 6). Af dem udgjorde 183 sårbarheder, der typisk findes og kan udnyttes i webapplikationer. Det er et fald på 12 procent i forhold til fjerde kvartal 2010.

Andelen af CVE-nummererede sårbarheder, der klassificeres som cross-site scripting, var stigende. De udgjorde i første kvartal 2011 halvdelen af de sårbarheder, som knytter sig til standard webapplikationer (Figur 7). Tidligere har en analyse foretaget af organisationen Veracode vist, at op mod 80 procent af alle webapplikationer havde kendte sårbarheder. Sårbarheder af typen cross-site-scripting var den hyppigst fundne[6].

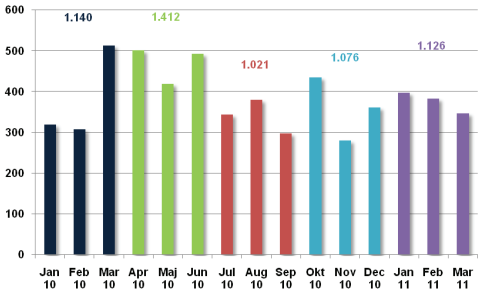
Blandt de applikationer, der i første kvartal 2011 oftest blev offentliggjort nye CVE-nummerede sårbarheder i, var webbrowseren Chrome, Apples styresystem Mac OS X samt Acrobt og Adobe Reader (Figur 8). Mest bemærkelsesværdigt er, at der denne gang ikke er Microsoft-produkter blandt de første på listen, ligesom webbrowserne Mozilla og Safari er fraværende. Ny på listen er ORTS, som er et open source system til varetagelse af opgaver inden for helpdesk og service management.

Mest kritisk var sårbarheder i Ciscos hardware-firewalls, Cisco ASA (Adaptive Security Appliance), da disse ofte ikke kan opdateres uden for et godkendt servicevindue. Det formodes, at det høje antal offentliggjorte sårbarheder i første kvartal 2011 er en del af en bevidst strategi, hvor sårbarhederne ikke bliver offentliggjort, før rettelserne er tilgængelige.

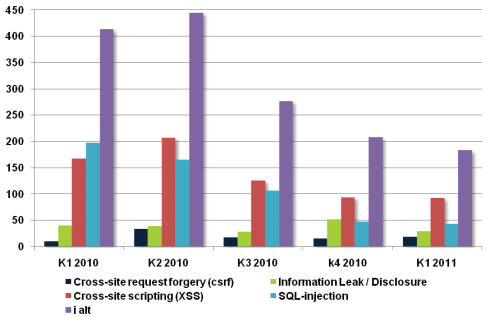
Det skal understreges, at listen ikke er et udtryk for sikkerhedsniveauet af de enkelte systemer. Der inddrages ikke faktorer som, hvor lette de offentliggjorte sårbarheder er at udnytte, hvilken grad af kompromittering de kan forsage, om der findes opdateringer, eller hvor udbredt det sårbare system er. Faktorer der har betydning for, hvor attraktivt det er at udvikle skadelig kode, der udnytter sårbarhederne.

6 Veracode.com, 2010; "*State of software security report*".

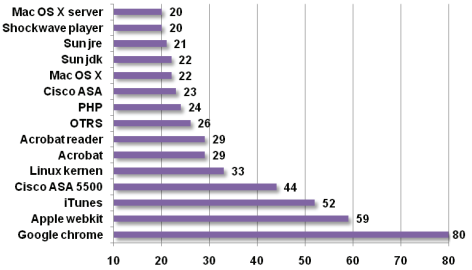
7 nvd.nist.gov; "*CVE and CCE statistics query page*".



Figur 6. Antal offentliggjorte CVE-nummererede sårbarheder.



Figur 7. Offentliggjorte CVE-nummererede websårbarheder per kvartal[7].



Figur 8. CVE-nummererede produktsårbarheder offentliggjort i første kvartal 2011.

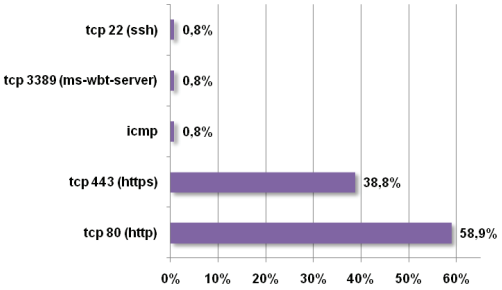
DK•CERT udførte i første kvartal 2011 sårbarhedsscanning af omkring 1.500 forskellige IP-adresser placeret på Forskningsnettet. 2,1 procent af de scannede IP-adresser svarede på forespørgsler fra internettet. Lidt over halvdelen af disse havde i gennemsnit 8,6 CVE-nummererede sårbarheder fordelt på fem forskellige porte/protokoller. 90 procent af de fundne sårbarheder blev risikovurderet til at udgøre en middel risiko, mens seks procent blev vurderet som kritiske. I alt blev der konstateret 43 forskellige CVE-nummererede sårbarheder, hvor cirka 90 procent var offentliggjort mere end et år før scanningen.

Web-applikationer, der som standard lytter på TCP-port 80 og 443, var også i første kvartal af 2011 de mest sårbare. Sårbarheder på disse porte udgjorde 97,5 procent af alle sårbarhederne. Øvrige sårbarheder blev konstateret på ICMP samt TCP portene 22 og 3389, der benyttes af henholdsvis SSH og Microsofts terminal-server (Figur 9). Kvartalets mest betydende sårbarhed berørte de fleste Windows-systemer tidligere end Windows 7.

Den muliggør afvikling af kode på det sårbare system. Sårbarheden (CVE-2010-3970), der vurderes som kritisk, blev offentliggjort første gang den 22. december 2010. Den kræver, at brugeren tilgår et thumbnail-billede indeholdende skadelig kode[8]. Den 5. januar blev der publiceret offentlig kode, der udnyttede sårbarheden. Den 8. februar udsendte Microsoft en opdatering, som rettede fejlen i Windows Shell graphics processor.

Den 16. februar 2011 offentliggjordes sårbarheden CVE-2011-0654, der gør det muligt at udfører Denial of Service-angreb eller fjernovertage et sårbart Windows-system. Sårbarheden er tilgængelig på alle versioner af Windows og blev vurderet som kritisk. Kun kort efter offentliggørelsen af sårbarheden blev der publiceret skadelig kode. Eneste løsning er at blokere computerens TCP-porte 137, 138, 139 og 445[9].

Den 14. marts 2011 udsendte Adobe en sikkerhedsbulletin angående en kritisk sårbarhed i Flash Player, Acrobat og Adobe Reader. Den blev set udnyttet gennem en skadelig Flash-fil (.swf) indlejret i et Microsoft Excel-dokument. Sårbarheden er tilgængelig på alle gængse operativsystemer. Den kan udnyttes til Denial of Service-angreb eller fjernkontrol af det sårbare system. Sårbarheden blev dagen efter registreret med CVE-nummer (CVE-2011-0609). Adobe har siden udgivet opdaterede versioner af deres programmer[10].



Figur 9. CVE-nummererede sårbarheder konstateret ved scanning i første kvartal 2011.

8 Microsoft, 2011; "*Microsoft Security Bulletin MS11-006 – Critical*".

9 Vupen.com, 2011; "*Microsoft Windows SMB "mrxsmb.sys" Remote Heap Overflow Vulnerability*".

10 Adobe.com, 2011; "*Security Advisory for Adobe Flash Player, Adobe Reader and Acrobat*".

3. Overskrifter fra første kvartal 2011

Flere overskrifter og begivenheder har i løbet af kvartalet været med til at præge vores syn på udviklingen med hensyn til it-kriminalitet og -sikkerhed. Udvælgelsen af begivenheder er selvfølgelig præget af vores perspektiv på it-sikkerhed som CERT for Forskningsnettet. Enkelte historier udspringer derfor fra vores verden, snarere end det billede som blev tegnet af medierne. Fælles er dog, at de er med til at tegne et billede af it-sikkerheden i hele det danske samfund.

3.1. Stigende it-investeringer giver øget sikkerhed

På trods af at de danske it-chefer ifølge en undersøgelse foretaget af Dansk IT havde afdæmpede forventninger til it-investeringerne i 2010[12], viste året sig at slå alle rekorder. Grundlæggende betyder den fornyede optimisme i erhvervslivet, at man ud over større effektivitet også opnår bedre sikkerhed.

Under den finansielle krise havde man udsat investeringer til blandt andet fornyelse af hardware. Med ny tiltro til fremtiden blev 2010 året, hvor man igen investerede i it, og året endte med et rekordsalg på 65 milliarder kroner. Salget var primært båret af pc'er, servere og software, mens investeringer i strategiske it-projekter og -løsninger var under niveauet for 2008. Også for både 2011 og 2012 har analysehuset IDC en forventning om vækst[13].

Investeringer i nye computere betyder i vid udstrækning også, at softwareplatformen fornys. Således kan det forventes, at mange organisationer planlægger eller allerede er gået over til Windows 7, der vurderes at være mere sikker end Windows XP. Dette skifte kan vi aflæse på webstatistikken for www.cert.dk, hvor andelen af besøgende der benytter Windows XP, fra januar 2010 til januar 2011 er faldet fra 54 procent til 42 procent. Tilsvarende er besøgende med Windows 7 i samme periode steget fra 12 procent til 25 procent.

Med overgangen til Windows 7 følger også en ny og mere sikker version af browseren Internet Explorer. Således var der i januar 2011 kun 28 procent, der benyttede Internet Explorer i ældre versioner end 8 mod 37 procent året tidligere. En stor andel er også overgået til at bruge alternative browsere som for eksempel Mozilla Firefox eller Google Chrome. De stod i januar 2011 for mere end 25 procent af de besøgende. De alternative browsere hentes og bruges primært i nyeste version.

Dansk IT

Dansk IT er en forening for it-professionelle med mere end 5.600 medlemmer. Foreningen er en non-profit organisation, der arbejder uafhængigt af politiske tilhørsforhold, fagforenings- eller brancheforeningsinteresser med det formål at udbrede anvendelsen af it til gavn for professionen, samfundet og den enkelte.

Foreningen repræsenterer medlemmernes interesser på den politiske scene og gennem blandt andet netværk, konferencer, gratis på-vej-hjem-møder og lignende[11].

11 Dansk IT; "*Dansk IT*".

12 Dansk IT, 2010; "*CIOViewpoint - Krisens spor*".

13 Business.dk, 2011; "*IT-salget satte rekord i 2010*".

3.2. Industrispionage og angreb mod it-infrastruktur

En undersøgelse foretaget af Dansk IT blandt 119 danske it-chefer i både den offentlige og private sektor viste, at 26 procent af organisationerne havde været udsat for hacker- eller virusangreb, der havde til formål at lamme it-infrastruktur eller produktionssysemer. Truslen fra Stuxnet og tilsvarende har medført, at 55 procent har indført skærpede it-sikkerhedsforanstaltninger[14].

Omvendt har kun 10 procent af virksomhederne indført særlige it-sikkerhedsforanstaltninger i forhold til nøglemedarbejderes tjenesterejser. Det sker på trods af, at undersøgelsen indikerer, at det bedste værn mod industrispionage er at vanskeliggøre medarbejdernes mulighed for at medbringe data uden for organisationen. Resultatet skal ses i relation til, at kun 5 procent tilkendegav, at deres organisation havde været udsat for industrispionage, mens 29 procent ikke var vidende om det. Kun i ét tilfælde var industrispionage udført som et computerbaseret angreb.

28 procent af undersøgelsens respondenter mente, at det var en national myndighedsopgave at minimere truslen fra angreb som for eksempel Stuxnet mod organisationernes it-infrastruktur og produktionssystemer. Lignende holdninger har i forbindelse med bekæmpelse at botnet været fremført af Dansk Industri. 13 procent mente, at bekæmpelsen burde ske i samarbejde med en aktiv offentlig myndighed og/eller internetudbyderne.

3.3. Dansk samarbejde om bekæmpelse af botnet

Den 16. februar blev det offentliggjort, at Videnskabsministeriet i samarbejde med ISP Sikkerhedsforum går ind i bekæmpelsen af botnet på den danske del af internettet. Samarbejdet leverer svar på et forslag, der tidligere blev stillet af Dansk Industri om statslig bekæmpelse af botnet[15].

Samarbejdsaftalen mellem IT- og Telestyrelsen (GovCERT), DK•CERT og ISP Sikkerhedsforum udstikker rammerne for samarbejdet. Det giver mulighed for at beskytte mod botnet, som for eksempel forsøger at stjæle adgangsoplysninger til borgernes netbank eller andre af deres personlige data. Om aftalen udtalte vicedirektør i IT- og Telestyrelsen, Marie Munk:

"Såkaldte botnet - dvs. computere, der organiseres i netværk gennem ondsindet software og bruges til at udsende spam og foretage koordinerede hackerangreb – er en trussel for danskernes brug af internettet. Det er derfor vigtigt med et solidt samarbejde om at bekæmpe botnet mellem de relevante myndigheder og de udbydere, som leverer internet til virksomheder, myndigheder og borgere. Den netop indgåede aftale styrker dette samarbejde."[16]

ISP Sikkerhedsforum

ISP Sikkerhedsforum blev dannet 6. maj 2004 af en række danske internetudbydere for at styrke udbydernes bidrag til indsatsen mod virus-, orme-, hackerangreb og spam.

ISP Sikkerhedsforum består af repræsentanter fra de fleste danske internetudbydere og repræsenterer størstedelen af internetbrugerne i Danmark.

14 Dansk IT, 2011; "*CIOViewpoint - Industrivirus og industrispionage*".

15 Dr.dk, 2010; "*DI: Staten bør bekæmpe it-kriminelle*".

16 Govcert.dk, 2011; "*Styrket samarbejde i bekæmpelsen af botnet*".

3.4. Danske netbutikker under angreb

"I takt med at netbankerne implementerer sikkerhedsmæssige modforholdsregler, tror vi, at fokus kan flytte sig til større lokale webshops, der ikke i samme grad som bankerne har implementeret it-sikkerhed som del af deres forretningsmodel."[17]

Ovenstående citat fra vores egen "Trendrapport 2009" synes nu at være blevet virkelighed. Med kun seks vellykkede netbankindbrud i 2010[18] er danske netbanker nu blevet så sikre, at de it-kriminelle har fundet andre markeder. Det nye mål er netbutikkerne, som ifølge direktør Poul Thyregod fra Proshop oplever en voldsom stigning i antallet af sager, hvor stjålne kreditkortoplysninger bliver brugt til svindel.

Svindlen foregår ved, at kriminelle med stjålne kreditkortoplysninger køber elektronik fra netbutikkerne. Varen sendes til intetanende muldyr i Danmark, som pakker den om, og sender den videre til modtagere i udlandet, typisk Østeuropa. De danske muldyr, som risikerer en politianmeldelse, er ofte rekrutteret via jobannoncer fra tilsyneladende etablerede shipping- og kurerfirmaer i udlandet. At rekrutteringen lykkes, skyldes troværdigt udformede jobannoncer, udstrakt brug af søgemaskineoptimering, personlig telefonisk kontakt samt brugen af "formelle" ansættelseskontrakter. Som taberne ved svindlen står netbutikken og muldyret.

Problemstillingen bliver ikke mindre ved, at mange danske netbutikker har alvorlige sikkerhedsfejl og således potentielt kan indgå i fødekæden for stjålne kreditkortoplysninger. En undersøgelse foretaget af firmaet Hackavoid viste, at 49 procent af de undersøgte danske netbutikker havde kritiske sårbarheder[19]. Otte procent af de undersøgte butikker havde SQL-injection-sårbarheder, som blandt andet kan misbruges til at læse informationer i databasen eller placere skadelig kode på den besøgenes computer.

3.5. Brute-force angreb fra skyen

Sidst i februar modtog DK•CERT en anmeldelse fra en institution på det danske Forskningsnet. En brugerkonto med svagt password var kompromitteret, og kontoen blev benyttet til at logge på en SSH-tjeneste, hvorfra man scannede efter andre SSH-servere på internettet. På den kompromitterede SSH-server blev der fundet brugernavne og password til andre SSH-servere på internettet.

Som sådan var hændelsen ikke unormal. DK•CERT modtager dagligt rapporter om forsøg på brute-force-angreb. Alligevel giver den stof til eftertanke. I takt med at også de it-kriminelle tager regnekraften fra cloud-services til sig, øges risikoen for at passwords, som tidligere blev betragtet som relativt sikre, kan knækkes. Da en kompromitteret brugerkonto ofte giver potentiel adgang til flere af organisationens interne tjenester, stiller det nye krav til organisationens politikker omkring passwords. Blandt andet bør man på alle tjenester sikre sig, at brugerkonti låses efter eksempelvis tre ugyldige login-forsøg.

17 DK•CERT, 2010; "*Trendrapport 2009*".

18 Finansrådet, 2011; "*Historisk få netbankindbrud*".

19 Version2.dk, 2011; "*Hver anden danske webshop har alvorlige sikkerhedsfejl*".

3.6. Smartphones, det nye mål

Efter tip fra bloggeren Lompolo valgte Google i starten af marts at fjerne 21 malware-inficerede apps fra Android Market. De inficerede apps var alle legale gratis programmer, der var blevet ompakket og igen distribueret til Android Market, nu indeholdende skadelig kode. I løbet af de fem dage de var tilgængelige, estimeredes det, at mindst 50.000 brugere nåede at installere dem på deres Android-telefoner og tavle-pc'er[20].

Efterfølgende udtalte stifteren af antivirusproducenten Kapersky Lab, Eugene Kaspersky, i et interview med Version2, at han mente, at Android ville blive det næste mål for malware-udviklerne. Mobiltelefoner er i dag små computere, der benyttes til alt fra e-mail til nethandel og netbank. Incitamentet for at ramme mobiltelefonerne er til stede, og Googles fokus på udviklerne og operativsystemets åbenhed gør det til et naturligt mål for malware. Således mener han, at Android-platformen vil overtage Windows' position som malware-skribenternes foretrukne mål[21].

I modsætning til Apples App Store er der på Android Market ingen kontrol af de apps, der lægges op. På mobiltelefoner hvor kun de færreste har installeret sikkerhedssoftware, kan det være et problem, når brugerne henter deres apps fra Android Market, som de må formode er en troværdig kilde.

3.7. Nye cookie-regler beskytter privatlivet

Den 25. maj 2011 træder et nyt EU-direktiv i kraft, som har til formål at sikre privatlivets fred ved færdsel på nettet. Artikel 5 stk. 3 i databeskyttelsesdirektivet betyder, at det kan blive betragtet som ulovlig indtrængen, hvis der uden brugerens accept gemmes noget lokalt på dennes harddisk, som ikke er en del af et program eller hjemmesides grundlæggende funktionalitet. Formålet er at sikre forbrugerne kontrol over, hvad for eksempel hjemmesider gemmer og henter af oplysninger på brugernes pc[22].

Hvordan den nye lov skal implementeres og håndhæves, står endnu hen i det uvisse. For eksempel giver spøgsmålet om brugeraccept nogle dilemmaer i forhold til, hvad brugerne skal acceptere og hvordan, samt hvor længe en accept er gældende. Problemet er også, om brugerne af en hjemmeside reelt forstår, hvad de accepterer og hvad det betyder for dem. Dertil kommer håndhævelse af loven for hjemmesider, som er placeret uden for EU.

3.8. Hurtig udnyttelse af jordskælv i Japan

Fredag den 11. marts blev Japan ramt af et jordskælv, som medførte en altødelæggende tsunami. Kun ganske få timer efter jordskælvet kunne antivirusproducenten Trend Micro på deres blog fortælle, at søgninger efter nyheder og video fra katastrofen ledte til sider med falske antivirusprogrammer. Udbredt brug af søgemaskineoptimering medførte, at søgninger efter nyt om

20 Trendmicro.eu, 2011; "*Google Android rooted, backdoored, infected*".

21 Version2.dk, 2011; "*Eugene Kaspersky: Android bliver hackernes nye Windows*".

22 Version2.dk, 2011; "*Fovirret? Få styr på de nye cookie-regler*".

katastrofen ledte til falske nyhedssider. Her blev de besøgende eksponeret for det falske antivirusprogram MalFakeAV-25[23].

Katastrofen er det seneste eksempel på, hvordan interessen for aktuelle begivenheder stadig hurtigere udnyttes til spredning af malware.

3.9. Microsoft knækker det berygtede Rustock botnet

Under kodenavnet "Operation b107" har Microsoft i samarbejde med flere sikkerhedspartnere samt U.S. Marshals Service knækket det berygtede Rustock botnet. Den koordinerede indsats startede ni måneder før, aktionen blev sat i gang den 16. marts 2011.

Der kom skred i tingene, da det lykkedes virksomheden FireEye at udarbejde en signatur på kommunikationen mellem botnetklienterne og -serverne. En unik indikator var, at kompromitterede computere forsøgte at hente de første 200 KB af Windows XP SP2. Formålet har været at teste for aktiv internetforbindelse og måling af hastigheden. Det kunne Microsoft bruge til at identificere inficerede computere – og dermed opnå yderligere indsigt i kommunikationsprocessen[24].

Microsoft udnyttede de juridiske muligheder i forbindelse med misbrug af deres varemærker til at opnå en dommerkendelse. Det gav U.S. Marshals Service lovhjemmel til at beslaglægge 26 command & control-servere fordelt over fem hostingselskaber i syv amerikanske byer. Med hjælp fra backboneleverandører afskar man samtidig de IP-adresser, der blev benyttet til at kontrollere botnettet. Rustock var nu knækket.

Man skønner, at omkring 1.000.000 maskiner stadig er inficeret, men inaktive i øjeblikket. Bagmændene er endnu ikke pågrebet[25].

Om Rustock

I sin storhedstid var Rustock ansvarlig for størstedelen af den udsendte spam på verdensplan. Selv efter lukningen af verdens største spam-affiliate-program var Rustock ansvarlig for mere end 30 procent af den samlede mængde spam.

Rustock var et avanceret botnet i forhold til Waledac, Mega-D og Szerbi. Kommunikation mellem de forskellige noder var kamufleret på en sådan måde, at det lignede almindelig dagligdagstrafik.

Kompromitterede maskiner blev inficeret med malware pakket ved hjælp af en egenudviklet krypteringsteknik, der fik den ondsindede kode til at fremstå som et pakket RA--arkiv. Spredningen foregik ved hjælp af hackede websites, hvor forskellige sårbarheder i internetbrowsere og plugins blev udnyttet.

Botnettets opbygning medførte, at Rustock var aktivt i mere end fire år. At det har været en lukrativ forretning understreges af, at udgiften alene på hosting af botnettets command & control-servere er opgjort til 10.000 dollar om måneden[24].

23 Trendmicro.com, 2011; "*"Most Recent Earthquake in Japan" Searches Lead to FAKEAV*".

24 Channelregister.co.uk, 2011 ; "*Rustock Takedown: How the world's worst botnet was KO'd*".

25 Blogs.technet.com, 2011; "*Operation b107 - Rustock Botnet Takedown*".

4. Ordliste

Botnet: Et botnet er et netværk af computere, som en angriber kan fjernstyre fra centralt hold. Navnet kommer af "robot" og "net". Ejerne af computerne ved ikke, at deres pc er inficeret med et botnet-program og indgår i botnettet. Angriberen udnytter gerne sine "robotter" til at foretage koordinerede denial of service-angreb eller udsende spam- og phishing-mails.

Brute-force: Dækker i datalogien over en udtømmende afsøgning af et løsningsrum. Inden for it-sikkerheden betegner det afprøvningen af kombinationer af brugernavne og kodeord, ofte ud fra foruddefinerede lister og ordbøger.

Cloud computing: Services distribueret i en sky af primært virtuelle ressourcer. Skyen giver mulighed for, at man får adgang til ressourcer efter behov. Skalerbarhed og pris vil ofte være de væsentligste argumenter for at lade sine services outsource til skyen. Overordnet skelnes mellem tre forskellige typer af cloud-services: Software as a Service (SaaS), Platform as a Service (PaaS) og Infrastructure as a Service (IaaS).

Command & control server: Et botnets centrale servere, hvorigennem det er muligt at sende kommandoer, som udføres af computere i botnettet, der er inficeret med botnet programmer.

Cross-site request forgery (CSRF): En metode, der muliggør at uautoriserede parametre og kommandoer eksekveres på serveren gennem henvendelser fra en bruger, som websitet har tillid til. Metoden kan for eksempel medføre overtagelse af brugerens session til det enkelte site.

Cross-site scripting (XSS): En metode, hvor adressen på et sårbart website udnyttes til at vise yderlig information eller afvikle programmer. Der er forskellige former for cross-site scripting, som gør det muligt at udføre komplekse angreb. Metoden kan for eksempel anvendes til phishing, hvor brugeren bliver omdirigeret til et forfalsket website. En angriber kan udnytte et website, som en bruger har tillid til, til at få adgang til fortrolig information.

CVE, CVE-nummer: Common Vulnerabilities and Exposures, forkortet CVE, er en liste over offentligt kendte sårbarheder i software. Listen dækker sårbarheder i de fleste kendte og alment udbredte programmer, men ikke i skræddersyet eller internt udviklet software, der ikke er i distribution, såsom de fleste webapplikationer.

Cookie: En cookie er en slags datapakke, der blandt andet indsamler oplysninger om forbrugerens gøren og laden på nettet. Cookies findes overalt på nettet og er med til at gøre det lettere at navigere på forskellige hjemmesider. Det er for eksempel en cookie, der sørger for, at ens mailadresse allerede står i adressefeltet, så man kun behøver at skrive sit password, når man skal tjekke mails.

Denial of Service (DoS): Et angreb der sætter en tjeneste, funktion eller et system ud af drift, eller på anden måde gør det utilgængeligt for brugerne. Et eksempel kan være et angreb, der overbelaster en webserver ved at sende mange forespørgsler. Disse angreb udføres ofte fra flere computere samtidigt, og kaldes i de tilfælde for distributed denial of service (DDoS).

Drive-by attacks: Angreb hvor tilfældige besøgende på en kompromitteret

hjemmeside forsøges inficeret med. Den inficerede hjemmeside vil ofte være en sårbar legal side, som brugeren har tillid til, og infektionen foregår uden dennes vidende.

Exploit: Et eksploit er kode, som forsøger at udnytte sårbarheder i software programmer med det formål at kompromitterer systemet.

Forskningsnettet: Et højhastighedsnetværk, der forbinder danske universiteter og forskningsinstitutioner. Ud over det fysiske netværk forsyner Forskningsnettet brugerne med en række tjenester til forskning, samarbejde og kommunikation.

GovCERT: GovCERT (Government Computer Emergency Response Team) funktionen, der i Danmark varetages af It- og Telestyrelsen, skal sikre, at der i staten er overblik over trusler og sårbarheder i produkter, tjenester, net og systemer. På den baggrund skal tjenesten foretage en løbende vurdering af it-sikkerheden samt varsle myndigheder om it-sikkerhedsmæssige hændelser og trusler.

Malware, skadelig kode: Sammentrækning af malicious software eller på dansk ondsindet kode. Malware er en samlebetegnelse for vira, orme, trojanske heste, keyloggere, spyware, adware, botnet-programmer og lignende.

Orm: Et program, der spreder sig i netværk ved at udnytte sårbarheder i dets computere. I TCP/IP-verdenen sker det typisk ved, at ormeprogrammet kontakter den port, som det sårbare program lytter på.

P2P, Peer-to-peer: P2P er en betegnelse for et decentralt netværk, hvor de enkelte noder (peers), i modsætning til i en client/server arkitektur, kommunikerer direkte med hinanden. Ansvaret for nettets funktionalitet er tilsvarende distribueret ligeligt mellem de enkelte computere i netværket. En hyppig anvendelse af P2P er fildelingsprogrammer som fx BitTorrent, eDonkey og KaZaA, samt internetbaserede telefonforbindelser som Skype.

Phishing: Svindelmetode, der går ud på at narre fortrolige oplysninger fra ofrene. Forsøg på phishing optræder ofte i e-mails, der henviser til websider. Websiden angiver at tilhøre offerets bank eller kreditkortselskab eller lignende, men er i virkeligheden under svindlernes kontrol.

Scanning, portscanning: Kortlægning af åbne porte på internettet, der har til formål at identificere sårbare services knyttet til dem. En portscanning foregår typisk ved, at der forespørges efter mange porte på få maskiner, eller én port på mange maskiner. Oftest benyttes et program til at foretage portscanninger. Brugen af firewalls vil som udgangspunkt lukke for adgangen til maskinens åbne porte.

Software as a Service (SaaS): Cloud-baseret tjenester, der tilbyder online brug af programmer efter behov. Det kan være online programmer som tekstbehandling, regneark eller CRM-services. Eksempler på SaaS er Google Docs, Hotmail og lignende.

Stuxnet: Stuxnet er blandt de hidtil mest avancerede orme. Ormen spreder sig vi USB-nøgler ved at udnytte en sårbarhed i Windows' behandling af genveje. Herefter angriber den industrielle Siemens WinCC CADA-systemer. Ormen indeholder en trojansk hest, hvorfor det menes, at den er målrettet informationstyveri fra industrien.

Sårbarhed: En fejl i et it-system, som en angriber kan udnytte til at få adgang til systemet, forhindre det i at fungere eller på anden måde misbruge det.

Sårbarhedsscanning: Kortlægning af kendte sårbarheder knyttet til services på et systems åbne porte. Benyttes ofte efter foregående scanning.

SQL-injection: Et angreb der ændrer i indholdet på en webside ved at sende kommandoer til den bagvedliggende SQL-database gennem usikre input-felter på websiden, som for eksempel søgefelter eller kommentarfelter, eller gennem usikre parametre i websidens URL'er.

Trojansk hest: Et program der har andre, ofte ondartede, funktioner end dem som det foregiver at have. Trojanske heste indeholder ofte dialer-, bagdørs- eller keylogger-funktionalitet, eller benyttes til installation af virus, botnetprogrammer og lignende. Trojanske heste identificeres ofte af antivirus- og antispyware-programmer.

Virus: Et program, der inficerer andre programfiler. Når den inficerede programfil køres, aktiveres virussen, og den inficerer andre programfiler. Oprindelig kunne kun egentlige programmer indeholde virus, men dokumenter med makroer kan nu også gøre det. Virus spredes ofte som mail vedlagt en trojansk hest, der indeholder virussen selv.

Warez, pirat software: Begrebet dækker over computerprogrammer, musik film og lignende, der distribueres illegalt og i strid med rettigheder og licensbetingelser. Warez er en sproglig forvanskning af flertalsformen af software.

5. Figuroversigt

6. Referencer

Adobe.com, 2011; "*Security Advisory for Adobe Flash Player, Adobe Reader and Acrobat*"; www.adobe.com/support/security/advisories/apsa11-01.html

blogs.technet.com, 2011; "*Operation b107 - Rustock Botnet Takedown*"; blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx

Business.dk, 2011; "*IT-salget satte rekord i 2010*"; www.business.dk/tech-mobil/it-salget-satte-rekord-i-2010

Channelregister.co.uk, 2011; "*RUSTOCK TAKEDOWN: How the world's worst botnet was KO'd*"; www.channelregister.co.uk/2011/03/23/rustock_takedown_analysis/

Comon.dk, 2011; "*Web-butikker betaler prisen for netsvindel*"; www.comon.dk/nyheder/web-butikker-betaler-prisen-for-netsvindel-1.390917.html

Dansk IT; "*Dansk IT*"; www.dit.dk

Dansk IT, 2011; "*CIOViewpoint - Industrivirus og industrispionage*"; www.dit.dk/aktuelt/Nyt_fra_DIT/Nyheder/~/media/Files/Presse/CIO-Viewpoint_2011_it-sikkerhed.ashx

Dansk IT, 2010; "*CIOViewpoint - Krisens spor*"; www.dit.dk/aktuelt/Nyt_fra_DIT/Nyheder/~/media/Files/Presse/CIO-Viewpoint_2011_it-sikkerhed.ashx

Dr.dk, 2010; "*DI: Staten bør bekæmpe it-kriminelle*"; www.dr.dk/Nyheder/Penge/2010/09/08/072441.htm

DK•CERT, 2010; "*Trendrapport 2009*"; https://www.cert.dk/trendrapport2009/trendrapport2009.pdf

Finansrådet, 2011; "*Historisk få netbankindbrud*"; www.finansraadet.dk/nyheder/artikler-fra-finansraadets-nyhedsbrev/2011/januar/historisk-faa-netbankindbrud.aspx

F-Secure.com, 2011; "*F-Secure security lab - virus world map*"; www.f-secure.com/en_EMEA/security/worldmap/

Govcert.dk, 2011; "*Styrket samarbejde i bekæmpelsen af botnet*"; www.govcert.dk/news/9

Kahusecurity.com, 2011; "*Robopak Exploit Kit*"; www.kahusecurity.com

Messagelabs.com, 2011; "*March 2011 intelligence report*"; www.messagelabs.com/mlireport/MLI_2011_03_March_Final-EN.pdf

Microsoft, 2011; "*Microsoft Security Bulletin MS11-006 – Critical*"; www.microsoft.com/technet/security/advisory/2490606.mspx

Nvd.nist.gov, 2010; "*CVE and CCE statistics query page*"; web.nvd.nist.gov/view/vuln/statistics

Pandasecurity.com, 2011; "**Creation of New Malware Increases by 26 Percent to Reach More than 73,000 Samples Every Day, PandaLabs reports**"; press.pandasecurity.com/news/creation-of-new-malware-increases-by-26-percent-to-reach-more-than-73000-samples-every-day-pandalabs-reports/

Trendmicro.com, 2011; "*Most Recent Earthquake in Japan*" Searches Lead to FAKEAV"; blog.trendmicro.com/most-recent-earthquake-in-japan-searches-lead-to-fakea/

Trendmicro.eu, 2011; "*Google Android rooted, backdoored, infected*"; countermeasures.trendmicro.eu/google-android-rooted-backdoored-infected/

Veracode.com, 2010; "*State of software security report*"; www.veracode.com/images/pdf/soss/executive-summary-veracode-state-of-software-security-report-volume2.pdf

Version2.dk, 2011; "*Eugene Kaspersky: Android bliver hackernes nye Windows*"; www.version2.dk/artikel/18277-eugene-kaspersky-android-bliver-hackernes-nye-windows

Version2.dk, 2011; "*Fovirret? Få styr på de nye cookie-regler*"; www.version2.dk/artikel/18281-forvirret-faa-styr-paa-de-nye-cookie-regler

Version2.dk, 2011; "*Google udrenser ondsindede apps fra butikken*"; www.version2.dk/artikel/18246-google-udrenser-ondsindede-apps-fra-butikken

Version2.dk, 2011; "*Hver anden danske webshop har alvorlige sikkerhedsfejl*"; www.version2.dk/artikel/18132-hver-anden-danske-webshop-har-alvorlige-sikkerhedsfejl

Vupen.com, 2011; "*Microsoft Windows SMB "mrxsmb.sys" Remote Heap Overflow Vulnerability*"; www.vupen.com/english/advisories/2011/0394

Kontakt:

DK•CERT, UNI•C
Centrifugevej, Bygn. 356
Kgs. Lyngby 2800

Tel. +45 3587 8887
URL: https://www.cert.dk
Email: cert@cert.dk