DK•CERT

Trendrapport

It-sikkerhed i andet kvartal 2010

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

Redaktion: Shehzad Ahmad, Jens Borup Pedersen, DK•CERT

Grafisk arbejde: Kirsten Tobine Hougaard, UNI•C

Foto: colourbox.com

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.

Indholdsfortegnelse

1.	**Resume**		3
2.	**Andet kvartal 2010 i tal**		4
	2.1.	Sikkerhedshændelser i andet kvartal 2010	4
	2.2.	Scanninger	5
	2.3.	Malware m.m.	5
	2.4.	Sårbarheder	6
3.	**Overskrifter fra første kvartal 2010**		8
	3.1.	Defacement - hærværk for sjov	8
	3.2.	Google og privatlivet fred	8
	3.3.	Ip-telefoni under angreb	9
	3.4.	WM i fodbold – katastrofen der udeblev	9
	3.5.	Clickjacking kaprer museklik	9
	3.6.	Porno-sites er mindre risikable end ventet	10
4.	**Ordliste**		11
5.	**Figuroversigt**		13
6.	**Referencer**		14

1. Resume

Andet kvartal 2010 var på mange måder anderledes, end vi havde forventet. Mens både april og juni bød på usædvanligt få anmeldelser til DK•CERT om sikkerhedshændelser, fik vi til gengæld i maj usædvanligt mange. I alt endte vi med cirka ti procent flere anmeldelser end i kvartalet forinden.

Den væsentligste årsag til maj måneds mange anmeldelser, var at DK•CERT blev gjort bekendt med danske systemer, der var blevet kompromitteret. I flere omgange blev brugernavne og passwords til danske systemer opsnappet fra udenlandske *botnet-servere*, hvor vi bistod i at varsle systemejerne.

Trojanske heste var også i andet kvartal den mest udbredte *malware*-type herhjemme. Men generelt faldt antallet af danske *malware*-inficeringer, og det gav færre anmeldelser til DK•CERT af danske websites inficeret med *trojanske heste* og *phishing*-sider. Sårbare legale webservere er dog stadig en central del af forsyningskæden for spredning af *malware*.

Offentliggørelserne af de *sårbarheder*, der udstyres med et *CVE-nummer*, steg i andet kvartal af 2010 fra 1.140 til 1.412. En stigning på knap 24 procent. Knap en tredjedel konstateres stadig i standard webapplikationer. Mere usædvanligt er det, at både Mac OSX og Microsofts browser Internet Explorer ikke længere befandt sig blandt de mest sårbare. Listen over de applikationer hvori der i andet kvartal 2010 blev offentliggjort flest *CVE-nummererede sårbarheder*, toppedes ellers stadig af styresystemer og browsere.

Selv om sommerens verdensmesterskaber i fodbold for mange blev en katastrofe, kunne vi fra it-sikkerhedens elfenbenstårn konstatere, at den forventede bølge af angreb udeblev. Kun i meget få tilfælde oplevede vi, at kriminelle grupperinger forsøgte eller havde held med, at udnytte begivenheden. Eller også oplevede vi det ikke, mailboksen hos DK•CERT forblev tom.

På trods af de skuffende fodboldresultater bød kvartalet på godt nyt for de danske husarer. Porno-websites er nu ikke så farlige, som vi gik og troede. I hvert fald var der næsten hundrede gange flere *malware*-spredende websites, der ikke indeholdt porno. Med en inficerings-grad på 3,25 procent af websider med porno, skal der dog ikke mange liderlige klik til, før man udsætter sin computer for fare.

Historien om ulovlige internetaktiviteter begået for sjov brød med vores forestillinger om organiserede og professionelle kriminelle grupperinger. Disse findes dog og er stadig aktive, selv om deres aktiviteter i andet kvartal af 2010 var mindre synlige.

2. Andet kvartal 2010 i tal

I dette afsnit beskriver DK•CERT statistik fra årets andet kvartal. Den enkelte statistik er med til at tegne et billede af it-kriminalitetens udvikling i Danmark såvel som i udlandet. Billedet er ikke fuldstændigt, men bør i kombination med egne erfaringer give et fingerpeg om, hvad vi i fremtiden skal beskytte vores it-aktiver imod.

Den primære kilde til data er DK•CERTs egne systemer. Enkelte data er suppleret og perspektiveret med internettets åbne kilder. Således beskrives udviklingen hovedsageligt fra Forskningsnettets perspektiv, men også data fra andre netværk er inddraget.

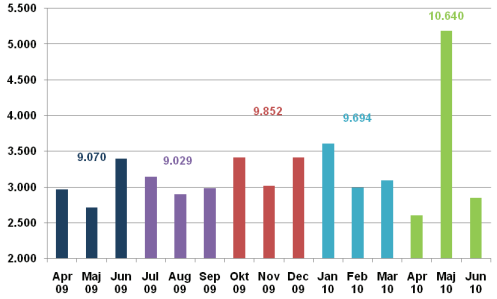
Afsnittet indledes med data, der beskriver de sikkerhedshændelser, som i andet kvartal blev anmeldt til DK•CERT. En væsentlig del af anmeldelserne vedrørte *systemscanninger*, mens en stigende andel vedrørte hændelser, der kan relateres til spredning af *malware*. Afsnittet rundes af med data, der omhandler kvartalets nye *sårbarheder*, samt de *sårbarheder* vi i DK•CERT har konstateret ved *scanninger* af vores kunders systemer.

2.1. Sikkerhedshændelser i andet kvartal 2010

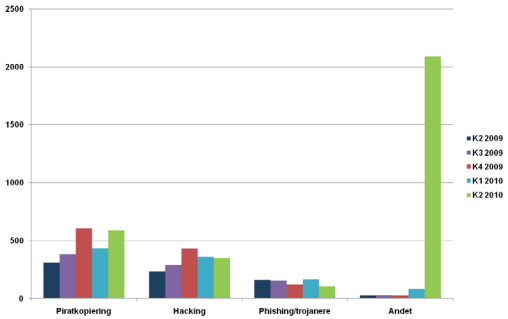
Andet kvartal bød på flere sikkerhedshændelser anmeldt til DK•CERT end tidligere i 2010 (Figur 1). Årsagen til dette skal findes i, at der i maj måned blev anmeldt usædvanligt mange sikkerhedshændelser, mens april og juni bød på færre end vi har været vant til gennem de seneste 15 måneder. Perioden har således været præget af store variationer fra måned til måned, og det er vanskeligt at beskrive en entydig tendens. Med maj måned som en markant undtagelse, synes der dog gennem årets første seks måneder at være sket et fald. Kun fremtiden kan vise, om det er en egentlig tendens.

Den væsentligste årsag til maj måneds mange anmeldelser var flere sager, hvor DK•CERT blev gjort opmærksom på danske systemer, hvor brugernavne og passwords var blevet opsnappet på udenlandske *botnet*-servere. Disse figurerer i Figur 2 under hændelsestypen "Andet". I forhold til første kvartal er der tilsvarende sket en stigning i anmeldelser om distribution og/eller download af kopibeskyttet materiale (*warez*), mens antallet af sager om *phishing*- og *trojansk hest*-inficerede websites er faldet (Figur 2). I begge tilfælde synes dette at være del af en tendens.

Tilsvarende er der gennem de seneste kvartaler sket et fald i hændelser kategoriseret som "Hacking". Dette kan dog bero på tilfældigheder, da hacking i denne sammenhæng ikke er en entydig kategori. Hacking dækker i Figur 2 over både vellykkede systemkompromitteringer såvel som i enkelte tilfælde mistanke om og forsøg på kompromittering. Hvorvidt der er tale om en egentlig tendens, må fremtiden derfor vise.



Figur 1. Sikkerhedshændelser anmeldt til DK•CERT.



Figur 2. Væsentligste hændelsestyper anmeldt til DK•CERT i andet kvartal 2010.

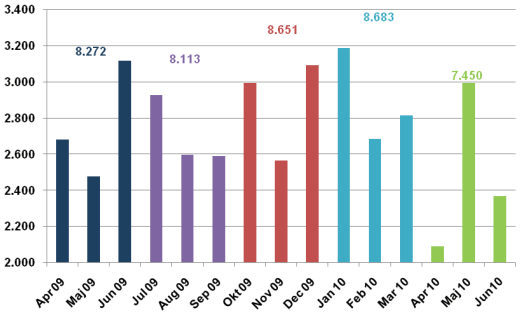
2.2. Scanninger

7.450 anmeldelser om *scanninger* efter svarende og/eller sårbare systemer på internettet i andet kvartal af 2010 er et fald i forhold til kvartalet forinden (Figur 3). Tallet dækker dog over store variationer. Mens de *scanninger*, der i maj måned blev anmeldt til DK•CERT, i antal var i den høje ende af det normale, bød både april og juni måned på langt færre anmeldelser, end vi tidligere har kunnet konstatere. April måneds 2090 anmeldelser om *scanninger* var således det laveste antal gennem de seneste 15 måneder. Tilsvarende var antallet af angribende IP-adresser mindre end første kvartal af 2010. I alt blev der i andet kvartal af 2010 anmeldt 3.996 forskellige scannende ip-adresser mod 4.522 i kvartalet før.

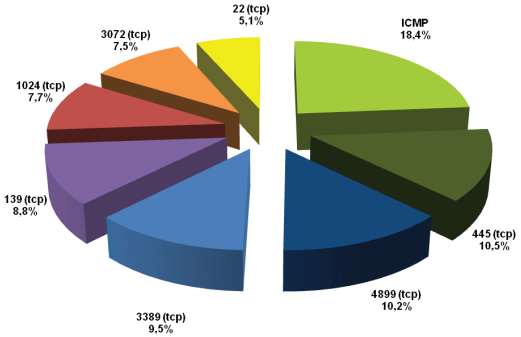
Også i andet kvartal 2010 blev der anmeldt *scanninger* mod 254 forskellige porte og protokoller. Der anmeldes således *scanninger* mod et bredt spekter af porte og dermed mulige systemer og applikationer. Den hyppigst scannede port/protokol er stadig ICMPping af store netsegmenter, der indgik i 18,4 procent af alle anmeldelse om *scanninger* (Figur 4). Ping er som sådan legal trafik og bør isoleret set ikke give anledning til større postyr. Når det i disse tilfælde alligevel har givet anledning til, at ping blev anmeldt til DK•CERT, skyldes det mængden af trafik snarere end arten.

Andelen af *scanninger* mod porte, der benyttes i forbindelse med fjernadgang eller -styring af systemer blandt andet tcp-port 1024, 4899 og 5900, er faldet til cirka 30 procent. Tcp-port 3389, der benyttes i forbindelse med remote desktop på Windowssystemer, var målet i 9,5 procent af *scanningerne* og er ny på listen over de mest scannede porte. Tilsvarende dækker en stor del af angrebene på tcp-port 22 (ssh) over *brute-force* angreb, hvor der forsøges login ved at "gætte" kombinationer af brugernavne og passwords. *Scanninger* mod tcp-port 3072, der blandt andet (mis)bruges af kendte *botnetprogrammer*, er faldet i antal i forhold til første kvartal, hvor de udgjorde 13,5procent.

Scanninger mod websystemer på, der benyttes over HTTP og HTTPS på henholdsvis tcp-port 80 og 443, var heller ikke i andet kvartal af 2010 blandt de hyppigst anmeldte.



Figur 3. Scanninger anmeldt til DK•CERT.

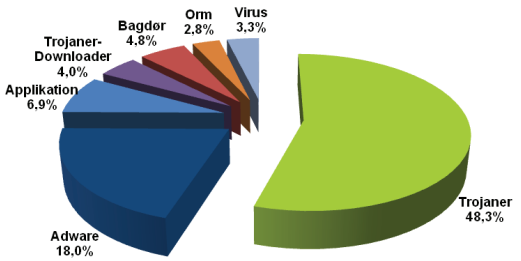


Figur 4. Hyppigst scannede portnumre i andet kvartal 2010.

2.3. Malware m.m.

F-Secure detekterede i første halvdel af 2010 11.906 danske infektioner med *malware*. I forhold til 7.347 infektioner i årets første tre måneder, er der således i andet kvartal sket et fald i antallet af danske infektioner. Hvorvidt dette skyldes et reelt fald eller blot er udtryk for forskydninger i markedsandele er uvist.

I forhold til første kvartal er der kun sket mindre forskydninger på de identificerede *malware*-typer (Figur 5). Mest markant var, at andelen af *trojaner*-downloadere og bagdøre, der henholdsvis faldt og steg fra 5,5 procent og 3,4 procent til 4,0 procent og 4,8 procent. At der kun har været mindre forskydninger er et udtryk for, at vi endnu ikke har set væsentlige udbrud af hverken nye vira eller netværksbaserede *orme*, samt at den forventede udnyttelse af verdensmesterskaberne i fodbold ikke har stået mål med de tilsvarende angreb efter jordskælvskatastrofen



Figur 5. Hyppigste danske malware-infektioner identificeret af F-Secure i andet kvartal 2010[1].

1 *F-secure.com, 2009; "F-Secure security lab - virus world map"*

på Haiti.

Andet kvartal gav et markant fald i anmeldelse om danske *phishing*- og/eller *trojaner*-inficerede danske websider (Figur 6). 106 anmeldelser er det laveste siden 2008. Faldet underbygger det markante fald i danske inficeringer med *malware* i andet kvartal af 2010. Samlet set mener vi derfor ikke, at *malware* endnu i væsentlig grad hostes i *botnet*, der benytter fast-flux teknologi, selvom levetiden her mangedobles[2]. Inficering af sårbare legale websites er stadig den primære kilde til spredning af *malware*.

Ifølge en undersøgelse af fem universitetsforskere downloades en del *malware* fra pornowebsteder. På 3,23 procent af de analyserede pornosider blev der kørt programkode, hentet programmer eller ændret i registreringsdatabasen. I alle tilfælde skete det ved udnyttelse af kendte *sårbarheder* i browsere og andre programmer[3].

2.4. Sårbarheder

Andet kvartal bød på offentliggørelse af 1.412 nye *CVE-nummererede sårbarheder*, eller 272 flere en kvartalet før (Figur 7). Af kvartalets nye *CVE-nummererede sårbarheder* udgjorde *sårbarheder*, der typisk findes på webapplikationer cirka 30 procent (Figur 8) svarende til 445 *sårbarheder*. I tillæg til de *CVE-nummererede sårbarheder* vil mange organisationer have *sårbarheder*, der knytter sig til deres specifikke implementering af systemer og applikationer. Disse offentliggøres ikke med et *CVE-nummer*.

De applikationer, der i andet kvartal af 2010 blev fundet flest *CVE-nummerede sårbarheder* i, var overordnet set forskellige versioner af styresystemet Windows, browsere samt programmer, der kan køres gennem browseren (Figur 9). Som eksempel på sidstnævnte er flashafspilleren og pdf-læseren Acrobat Reader.

I modsætning til tidligere, hvor Apples styresystem har toppet listen, er Mac OS X i både server- og klientversioner ikke at finde blandt andet kvartals mest sårbare applikationer. Tilsvarende er Microsofts browser Internet Explorer også røget ned af listen, som denne gang toppes af Flash-afspilleren fra Adobe. Lidt længere nede på en 35. plads er styresystemet til Apples iPhone, hvor til der i andet kvartal blev offentliggjort ti *CVE-nummererede sårbarheder*.

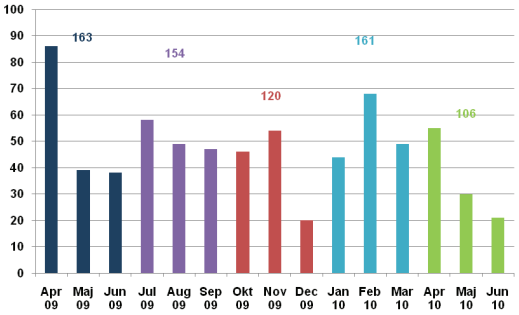
I andet kvartal af 2010 foretog DK•CERT *sårbarhedsscanning* af mere end 10.000 forskellige IP-adresser hovedsagelig placeret på *Forskningsnettet*. Heraf svarede lidt over 3 procent. Af disse havde lidt mere end en tredjedel i gennemsnit ni *CVE-nummererede sårbarheder*. Kvartalet før havde de sårbare systemer i gennemsnit fire *CVE-nummererede sårbarheder*. De IP-adresser, der ikke svarede, må formodes ikke at være i brug eller være beskyttet bag en firewall.

Også i andet kvartal blev der konstateret flest *CVE-nummererede sårbarheder* på tcp-port 443 og 80, der benyttes af webapplikationer (Figur 10). Dette er i sig selv

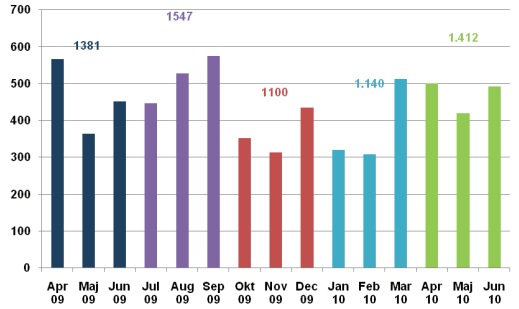
2 *Harvard.edu, 2009; "The economics of online crime".*

3 *iseclab.org, 2010; "Is the Internet for Porn? An Insight Into the Online Adult".*

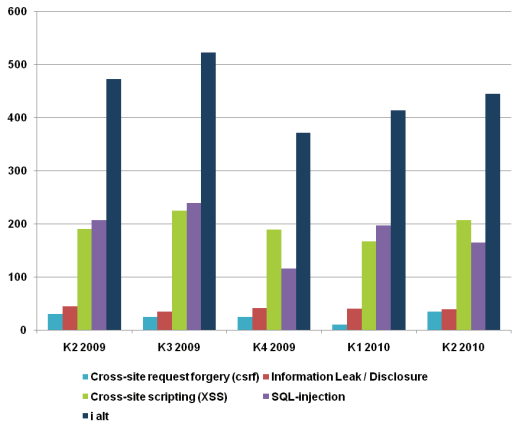
4 *nvd.nist.gov; "CVE and CCE statistics query page".*



Figur 6: Websites med trojanske heste og phishing-sider anmeldt til DK•CERT.

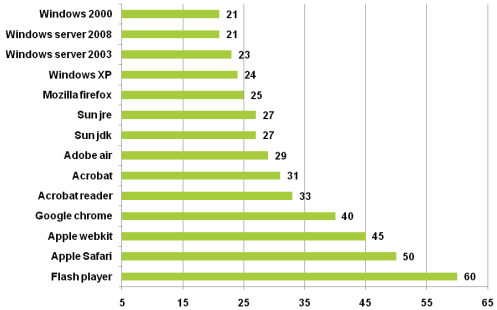


Figur 7. Offentliggjorte CVE-nummererede sårbarheder[4].

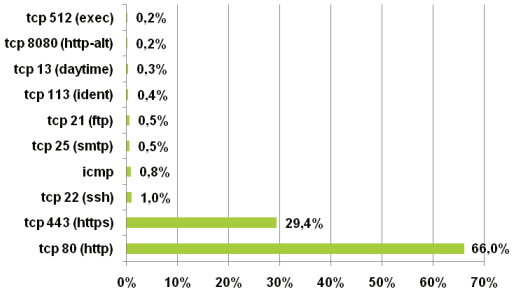


Figur 8. Offentliggjorte CVE-nummererede websårbarheder pr. kvartal.

ikke mærkeligt. I modsætning til kvartalet inden, blev der denne gang konstateret mere end dobbelt så mange *CVE-nummererede sårbarheder* på tcp-port 80 end på port 443. Organisationsspecifikke *sårbarheder* på webapplikationer fremgår ikke af statistikken, da disse ikke offentliggøres med et *CVE-nummer*.



Figur 9. CVE-nummererede sårbarheder offentliggjort i andet kvartal 2010.



Figur 10. CVE-nummererede sårbarheder konstateret ved scanning i andet kvartal 2010.

3. Overskrifter fra andet kvartal 2010

I dette afsnit beskrives overskrifter, som vi mener har været væsentlige i andet kvartal af 2010. Selv om der ikke er umiddelbar sammenhæng mellem de enkelte begivenheder, mener vi at de tegner et billede af it-kriminaliteten og de modforholdsregler, vi i it-sikkerhedsbranchen og samfundet som helhed tager /eller bør tage.

3.1. Defacement – hærværk for sjov

Organisationen zone-h.org offentliggjorde den 27. maj deres statistik over *defacements* (webgraffiti) for de første fire måneder af 2010[5]. Denne viste en markant stigning i antallet af registrerede defacements, i forhold til de tidligere år. Størstedelen af angrebene blev foretaget som masseangreb mod webhoteller, der benyttede Apache og Linux styresystem.

Begrundelserne for de omfattende angreb var ifølge zone-h.org primært at man gjorde det "*for sjov*" eller for at "*blive den bedste defacer*". Kun i ca. 7 procent af tilfælde nævnes politiske motiver. Dette ligner en tilbagevenden til tidligere, hvor internetkriminaliteten var drevet af spænding og prestige i en subkultur, der på mange måder minder om den traditionelle graffitikultur.

3.2. Google og privatlivets fred

I løbet af andet kvartal af 2010 kom Google flere gange i mediernes søgelys for deres forhold til privatlivets fred.

Mens Googles potentielle kendskab til vores online vaner flere gange har haft mediernes og borgerrettighedsforkæmpernes opmærksomhed, var kritikken mod Google Street View anderledes kontant, da det kom frem, at Googles fotobiler havde indsamlet store mængder data fra trådløse netværk. Blandt andet skulle der være indsamlet fragmenter af e-mails, passwords og lignende fra ukrypterede trådløse adgangspunkter[6]. Alt sammen en fejl undskyldte Google.

Googles lancering af søgning over en SSL-krypteret forbindelse tegner derimod et andet perspektiv for privatlivets fred, end hvad virksomheden ellers har været forbundet med. Når søgningen krypteres, har ISP'en, arbejdsgiveren og lignende ingen mulighed for at registrere, hvad vi som privatpersoner har søgt, og søgningen caches ikke på den enkelte pc eller gemmes i historikken[7]. Tilsvarende medsendes de enkelte søgeord ikke til den side, brugeren klikker sig hen på. Dette kan for indholdsleverandøren give udfordringer, da de ikke længere kan se, hvad vi søgte for at nå deres services, og herved kan have vanskeligere ved at optimere deres tjenester i forhold til søgemaskinerne.

Figur 11. Dansk webside efter defacement i juni 2010.

5 *Zone-h.org, 2010, "Defacements statistics 2008 - 2009 - 2010 first quarter".*

6 *Infoworld.com, 2010; "Google's Street View Wi-Fi data included passwords, email".*

7 *DK•CERT, 2010; "Krypteret Google-søgning har lille effekt".*

3.3. Ip-telefoni under angreb

Gennem andet kvartal kunne både vi og andre registrere angreb på port 5600. Porten benyttes blandt andet af SIP-protokollen (Session Initiation Protocol), der anvendes til signalering i ip-telefonisystemer. Blandt andet beskrives en stigning i *brute-force* angreb initieret fra ip-adresser i Amazons sky EC2[8]. Tilsvarende bød andet kvartal for første gang på henvendelser til DK•CERT, der relaterede sig til angreb mod systemer, der benyttes til ip-telefoni.

Systemer til ip-telefoni er i stigende grad blevet mål for angreb. Hvorvidt det er computerkapaciteten eller telefontjenesten, der er det egentlige mål, er dog ikke klart.

3.4. WM i fodbold – katastrofen der udeblev

I forbindelse med verdensmesterskaberne i fodbold i Sydafrika, var der en forventning om stigning i aktiviteter, som forsøgte at udnytte begivenheden. Som en følge heraf oprettede Symantec en hjemmeside[9], der skulle advare mod aktuelle angreb som relaterede til begivenheden.

Selv om der har været angreb, har de fleste danske indbakker været forskånet for spam, svindelmails og lignende, der med verdensmesterskaberne som blikfang har forsøgt at svindle modtageren eller lokke denne over på falske eller *malware*-inficerede websider. Tilsvarende har der ikke været rapporteret nævneværdige angreb på de legale websites, der dækker begivenheden eller solgte rejser og billetter til kampene. Årsagen til disse udeblevne angreb kendes endnu ikke.

3.5. Clickjacking kaprer museklik

I andet kvartal 2010 så vi for første gang *clickjacking* udnyttet på en måde, som kaldes likejacking[11]. Metoden er forbundet med Facebook, hvor det kaprede klik bruges til at angive, at brugeren "synes godt om" en bestemt webside. I det aktuelle tilfælde blev brugeren gjort opmærksom på et link til en side med de 101 hotteste kvinder i verden. Når han kom til siden, skulle han klikke på et link for at komme videre. Men klikket på dette link blev kapret. I stedet for at klikke på det synlige link klikkede brugeren på en usynlig knap, der opdaterede hans Facebook-status med, at han syntes godt om siden. Derefter blev han sendt videre, som om han havde klikket på linket.

Likejacking er forholdsvis uskadeligt. Det kan højst give anledning til, at der spredes information om, at brugeren har besøgt en bestemt webside. Men metoden har potentiale for at kunne misbruges til andre formål. For eksempel kan den side, som brugeren øjensynlig kan lide, bruges til at sprede skadelig software. Flere

8 *Voiptechchat.com, 2010; "Amazon EC2 SIP Brute Force Attacks on Rise"*

9 *Symantec.com, 2010; "2010 net threat".*

10 *Jeremiahgrossman.blogspot.com, 2008; "(Cancelled) / Clickjacking - OWASP AppSec Talk".*

11 *Thompson.blog.avg.com, 2010; "More LikeJacking on Facebook".*

Clickjacking

I 2008 præsenterede to sikkerhedsforskere *Clickjacking*[10] som en ny trussel. *Clickjacking* betyder kapring af museklik. Metoden går ud på, at en angriber placerer en skjult knap eller link på en webside. Når offeret tror, at han klikker på en knap på websiden, klikker han i virkeligheden på den skjulte knap.

Metoden muliggøres af sårbarheder i browseren, og kan blandt andet udnyttes til at kompromittere systemer og data på tværs af webgrænseflader.

potentielle ofre vil besøge den, fordi deres ven har anbefalet den.

3.6. Porno-sites er mindre risikable end ventet

To aktuelle undersøgelser sætter spørgsmålstegn ved opfattelsen af, hvorvidt pornografiske websteder er mere risikable at besøge end andre. Men konklusionen er ikke entydig.

Den ene undersøgelse stammer fra det tjekkiske antivirusfirma Avast[12]. Deres data for websteder, der spreder skadelig software, viser, at for hvert porno-site er der 99 ikke-pornografiske sites. Undersøgelsen viser, at der i dag er stor risiko for, at ens pc bliver forsøgt inficeret, selvom man besøger helt legitime websteder. Det skyldes, at webstederne selv kan være blevet inficeret, for eksempel via *SQL-injection* eller gennem inficerede bannerannoncer.

Hvor stor en del af alle porno-sites, er det så skadeligt at besøge, forsøgte en anden undersøgelse at besvare. Rapporten "*Is the Internet for Porn? An Insight Into the Online Adult Industry*"[13] handler om økonomi og sikkerhed i online pornografi og viser, at godt tre procent af pornosider indeholder skadelig software.

Forskerne analyserede knap 270.000 websider fordelt på godt 700 porno-sites. Når de besøgte websiderne, førte det i 3,23 procent af tilfældene til, at der blev udført programkode, hentet programmer eller ændret i registreringsdatabasen. Rapporten fortæller ikke, om *skadelig kode* i større grad var placeret med vilje på pornosites end på sites, der ikke indeholder porno.

Undersøgelserne siger ikke noget om, hvad der er mest risikabelt at besøge, da de ikke angiver, hvor mange porno-sites der findes i forhold til ikke-porno-sites. Men inden for porno er altså godt 97 procent af siderne sikre at besøge, hvis forskernes sider er repræsentative for helheden.

12 *Avast.com, 2010; "Legitimate websites "outscore" the adult 99:1".*

13 *Iseclab.org, 2010; "Is the Internet for Porn? An Insight Into the Online Adult Industry".*

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 fra foruddefinerede lister.

Clickjacking: Angreb, hvor besøgendes klik på en hjemmeside udnyttes til at aktivere indhold, som denne ikke er klar over eller ikke kan se. Herved risikerer brugeren for eksempel at klikke på indhold eller aktivere funktioner på anden webside uden dennes viden. Clickjacking kan således benyttes til informationsindsamling fra brugerens sociale netværksprofiler, spredning af *malware* og egentlig systemkompromittering.

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.

Defacement: Defacement eller web-graffiti, betegner et angreb, hvor websider tagges (overskrives) med angriberens signatur og ofte også et politisk budskab.

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.

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 com-

putere. I TCP/IP-verdenen sker det typisk ved, at *ormeprogrammet* kontakter den port, som det sårbare program lytter på.

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.

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.

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 *portscanning*.

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*, *botnet*programmer og lignende. *Trojanske heste* identificeres ofte af antivirus- og antispywareprogrammer.

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: 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

Figur 1. Sikkerhedshændelser anmeldt til DK•CERT. 4
Figur 2. Væsentligste hændelsestyper anmeldt til DK•CERT i andet kvartal 2010. 4
Figur 3. Scanninger anmeldt til DK•CERT. 5
Figur 4. Hyppigst scannede portnumre i andet kvartal 2010. 5
Figur 5. Hyppigste danske malware-infektioner identificeret af F-Secure i andet kvartal 2010. 5
Figur 6: Websites med trojanske heste og phishing-sider anmeldt til DK•CERT. 6
Figur 7. Offentliggjorte CVE-nummererede sårbarheder. 6
Figur 8. Offentliggjorte CVE-nummererede websårbarheder pr. kvartal. 6
Figur 9. CVE-nummererede sårbarheder offentliggjort i andet kvartal 2010. 7
Figur 10. CVE-nummererede sårbarheder konstateret ved scanning i andet kvartal 2010. 7
Figur 11. Dansk webside efter defacement i juni 2010. 8

6. Referencer

Avast.com, 2010; "*Legitimate websites "outscore" the adult 99:1*"; http://www.avast.com/pr-legitimate-websites-outscore-the-adult

F-Secure.com, 2010; "*F-Secure security lab - virus world map*"; www.f-secure.com/en_EMEA/security/worldmap/

Havard.edu, 2009; "*The economics of online crime*"; people.seas.harvard.edu/~tmoore/jep09.pdf

Iseclab.org, 2010; "*Is the Internet for Porn? An Insight Into the Online Adult Industry*"; http://www.iseclab.org/papers/weis2010.pdf

Jeremiahgrossman.blogspot.com, 2008; "*(Cancelled) / Clickjacking - OWASP AppSec Talk*"; http://jeremiahgrossman.blogspot.com/2008/09/cancelled-clickjacking-owasp-appsec.html

DK•CERT, 2010; "*Krypteret Google-søgning har lille effekt*"; https://www.cert.dk/artikler/artikler/CW28052010.shtml

Infoworld.com, 2010; "*Google's Street View Wi-Fi data included passwords, email*"; http://www.infoworld.com/d/networking/googles-street-view-wi-fi-data-included-passwords-email-679?source=rss_infoworld_news

Symantec.com, 2010; "*2010 net threat*"; http://www.2010netthreat.com/default.aspx

Thompson.blog.avg.com, 2010; "*More LikeJacking on Facebook*"; http://thompson.blog.avg.com/2010/06/more-likejacking-on-facebook.html

Voiptechchat.com, 2010; "*Amazon EC2 SIP Brute Force Attacks on Rise*"; http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/

Zone-h.org, 2010; "*Defacements statistics 2008 - 2009 - 2010 first quarter*"; http://www.zone-h.org/news/id/4735

Kontakt:

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

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