DK•CERT

Trendrapport

It-sikkerhed i andet kvartal 2012

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

Redaktion: Shehzad Ahmad og Jens Borup Pedersen, 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 informationssikkerhed 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 informationssikkerhed. 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 Ministeriet for Børn og Undervisning.

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

Efter en relativ stille april, registrerede DK•CERT i både maj og juni flere sikkerhedshændelse end i de forgangne måneder. I hele andet kvartal registrerede vi en stigning på mere end 25 procent i forhold til årets første tre måneder. Det skyldes hovedsageligt flere hændelser om systematisk afprøvning af kombinationer af brugernavne og password på diverse online tjenester.

Sådanne angreb er relativt lette at beskytte sig mod. Det handler om, at man ikke benytter den pågældende tjenestes standard brugernavn, og at en fornuftig politik er implementeret for brug af passwords.

Tilsvarende gælder for mange af de sårbarheder som frigives i it-systemer. Har man sørget for at aktivere automatisk opdatering hvor det er muligt, er opgaven ikke så uoverkommelig. De fleste sårbarheder kan nemlig rettes uden det store besvær.

De 1.060 nye CVE-nummererede sårbarheder, der blev offentliggjort i andet kvartal, burde derfor ikke give anledning til panderynker eller hævede øjenbryn. Når de alligevel gør det, er det fordi mange ikke er opmærksomme på sårbarheder, der ikke rettes automatisk. Dertil kommer at sårbarhederne udnyttes stadig hurtigere. Den trojanske hest Flashback udnyttede en sårbarhed til at sprede sig til 600.000 Machintosh-computere, før Apple den sjette april udsendte en opdatering, der lukkede hullet.

Samtidig er malware blevet mere avanceret og målrettet. Som Flame, der med et falsk Microsoft certifikat kunne installere sig via Windows Update-funktionen. I modsætning til Flame er det dog oftest ikke det iranske atomprogram, men vores data og penge der er målet.

Her spiller tillid, nysgerrighed og grådighed ind. Ved at udnytte det, kan de it-kriminelle få os til selv at installere malware på vores computer eller smartphone, svare på mails om gevinster fra et lotteri vi aldrig har deltaget i, eller frivilligt aflevere vores kreditkortinformationer. Det er de blevet bedre til. Det ser vi i forbindelse med optakten til de Olympiske lege i London.

Blandt det øvrige du kan læse om i denne rapport, er et angreb på tre styrelser under Erhvervs- og Vækstministeriet. Læs også om, at Datatilsynet har sat døren på klem for brug af cloud-tjenester til personfølsomme oplysninger, og lækkede passwords til linkedIn.

God fornøjelse med læsningen!

Shehzad Ahmad

Chef for DK•CERT

”I modsætning til Flame er det dog oftest ikke det iranske atomprogram, men vores data og penge der er målet.”

2. Andet kvartal 2012 i tal

I andet kvartal var der fred herhjemme. Fred for hacktivisterne som tidligere har hærget. Eller i det mindste så vidt offentligheden er orienteret. Kommunikationen i forbindelse med angrebet på tre styrelser under Erhvervs- og Vækstministeriet i slutningen af april må nemlig siges at være noget uforløst. Historien om, hvad der egentlig skete, hvem der stod bag og hvad deres mål var, er nemlig aldrig blevet fortalt.

Mens brugen af mobile enheder gennem det sidste år herhjemme er mere end fordoblet, er også mængden af malware, som er rettet mod dem, vokset. Det samme er mængden af phishingsider og websites der er oprettet med det formål at sprede skadelig kode. Set i lyset af de seneste års udvikling kan det ligne business as usual.

Også mængden af skadelig kode rettet mod banker er steget i første halvdel af 2012. Her har Kaspersky lab registreret en stigning i malware på danskernes computere, der var målrettet banker. Selvom dette tilsyneladende har medført en stigning i vellykkede indbrud i netbanker, er det ikke noget, der bør komme som en overraskelse. NemID Løsningen er nu kendt også hos de kriminelle. Således siger juridisk konsulent hos Finansrådet, Jesper Goul:

"*I en periode med NemID kunne vi se, at tallene faldt, men vi vidste godt, at det ikke ville holde. Nu sker det så. Første kvartal var ikke sjovt, og der kan vi se, at der skal en større indsats til.*"

Her tager vi udgangspunkt i data fra de systemer og netværk, DK•CERT har adgang til. Således tager afsnittet udgangspunkt i hændelser fra det danske net til forsknings- og uddannelsesinstitutioner samt de hændelser, der rapporteres til os fra den øvrige del af det danske internet. Egne data suppleres og perspektiveres i afsnittet med data fra internettets åbne kilder.

Herefter sætter vi fokus på udbredelsen af malware, spam og phishing, som i dag er de største trusler mod organisationer og brugere på internettet. Ingen af disse hændelsestyper kan ses isoleret og indgår i den samme digitale kriminelle værdikæde.

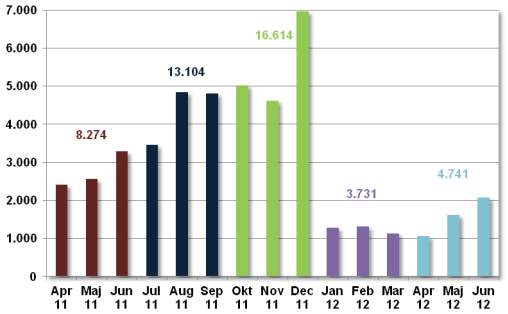
Afsnittet sluttes med en beskrivelse af kvartalets sårbarheder. Det vil sige de sårbarheder, der udnyttes af de kriminelle til at placerer malware og anden kode på vores systemer. Vi beskriver her kvartalets nye sårbarheder, de sårbarheder der blev forsøgt udnyttet, samt de sårbarheder vi fandt ved scanning af vores kunders systemer.

Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Operativsystemer*".
Google online security blog, 2012; "*Safe browsing - protecting web users for 5 years and counting*".
Version2, 2012; "*Antallet af netbankindbrud stiger trods NemID*".

2.1. Kvartalets sikkerhedshændelser

I andet kvartal 2012 modtog DK•CERT 4.741 rapporter om sikkerhedshændelser, det er en stigning på mere end 25 procent i forhold til årets første kvartal (Figur 1).

"I en periode med NemID kunne vi se, at tallene faldt, men vi vidste godt, at det ikke ville holde. Nu sker det så. Første kvartal var ikke sjovt, og der kan vi se, at der skal en større indsats til."



Figur 1. Sikkerhedshændelser rapporteret til DK•CERT.

Hvor antallet var relativt konstant i årets første fire måneder, modtog vi i både maj og juni et stigende antal rapporter. I alt registrerede vi 4.051 unikke sikkerheds-hændelser med udspring i 2.343 forskellige IP-adresser fra både Danmark og udlandet.

Faldet i rapporterede sikkerhedshændelser ved årsskiftet skyldes bortfaldet af en række scannings-hændelser, som tidligere blev rapporteret og behandlet automatisk. For øvrige hændelsestyper har det ikke betydning for sammenligneligheden med tidligere.

Den største andel af kvartalets sikkerhedshændelser var forsøg på at logge på en tjeneste ved systematisk at afprøve kombinationer af brugernavne og password (Figur 2). I alt blev 1.305 hændelser registreret som brute force-angreb. 400 forsøg omhandlede udenlandske computere, der forsøgte at logge på danske SSH-tjenester placeret på danske universiteter. Ved de øvrige hændelser var det danske computere, der forsøgte at logge på tjenester i udlandet. Det drejede sig primært om SSH- og mailtjenester.

Antallet af hændelser vedrørende uretmæssige download af kopibeskyttede værker fra fil-delingstjenester var stort set konstant i forhold til første kvartal. I alt registrerede vi 976 hændelser fra 273 forskellige IP-adresser på det danske Forskningsnet, hvor repræsentanter for rettighedshaverne gjorde opmærksom på piratdownload af film, musik og software.

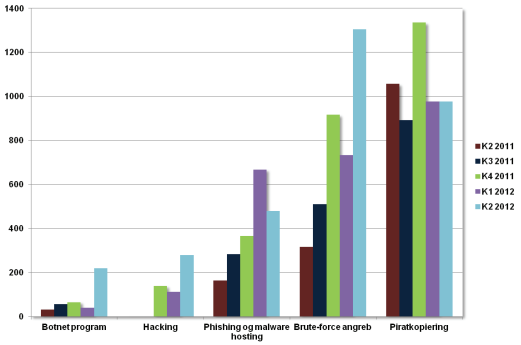
I andet kvartal 2012 registrerede vi 480 hændelser, hvor danske websites blev udnyttet til hosting af malware og phishing-sider. Selvom det er et fald i forhold til første kvartal, er det stadig mange i forhold til tidligere. Det understreger, at kompromittering af sårbare legale websites stadig er den væsentligste kilde til spredning af malware.

Måske tegner det også et billede af, at hostingudbyderne generelt har fået større fokus på sikkerhed. Vi har en oplevelse af, at svarprocenten er stigende, reaktionstiden er blevet kortere, og vi i mindre grad modtager gentagne henvendelser på samme kompromitterede host.

I 280 tilfælde blev en hændelse registreret som hacking. Det vil sige kompromittering af systemer og/eller informationer. Reelt kan en del af disse hændelser også dække over defacements eller maskiner inficeret med malware eller phishing, da det fra den modtagne information kan være vanskeligt entydigt at kategorisere hændelsen. Stigningen i denne type hændelser afspejler at de angreb, vi oplever, ikke altid er så nemme at kategorisere som tidligere. Ofte benyttes flere teknikker og angrebsvektorer.

Også i andet kvartal blev DK•CERT gjort opmærksom på danske computere, som deltog i botnet-relateret trafik. I alt registrerede vi 220 hændelser om danske computere, der sandsynligvis var inficeret med botnet-programmer. Det er en voldsom stigning i forhold til 40 registreringer i første kvartal, som muligvis afspejler et større fokus på problemet. Alle henvendelser kom fra udlandet, hvor der i enkelte tilfælde var skaffet adgang til en af botnettets centrale Command & Control-servere.

Endelig blev 402 hændelser kategoriseret som portscanninger mod kun 327 i kvartalet inden.



Figur 2. Væsentligste sikkerhedshændelser rapporteret til DK•CERT.

2.2. Malware og andre trusler

Malware står i dag som den største trussel mod danske organisationer og borgeres sikkerhed. Det er i stigende grad malware, der benyttes til at skaffe sig adgang til vores data. I kombination med udspekuleret social engineering metoder målrettes malware til at skaffe sig adgang til for eksempel vores mailkonti, kreditkortinformationer eller andre personlige data, som kan omsættes til penge i den kriminelle fødekæde.

Antivirusproducenten F-secure identificerede i andet kvartal lidt over 2.000 danske malware-infektioner. Også denne gang var det i de fleste tilfælde tale om trojanske heste. De stod for cirka 45 procent af alle inficeringerne (Figur 3). Det er den største andel trojanske heste, vi hidtil har registreret.

Når mængden af trojanske heste på danskernes computere er steget i forhold til tidligere kvartaler, kan det hænge sammen med, at de it-kriminelle igen har fattet interesse for de danske netbanker. Et par vellykkede netbankangreb i årets første kvartal viste, at det er muligt at omgå sikkerheden i NemID ved brug af avancerede trojanske heste. Dette underbygges af antivirusproducenten Kaspersky lab. Herfra fortalte David Jacoby i juni til Version2, at deres sikkerhedssoftware havde registreret en stigning i mængden af malware på danskernes computere, som var målrettet banker.

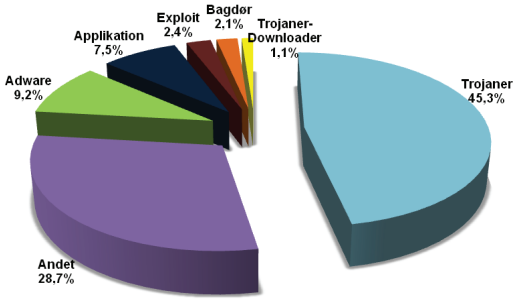
Også andelen af malware, der ikke lod sig entydigt identificere, er steget i andet kvartal. Den stod for små 30 procent af de danske inficeringer. Derimod er andelen af adware, der har til formål at eksponere brugeren for reklamer, faldet til godt ni procent. Som tidligere er det kun en marginal del af den malware, der findes på danskernes computere, der besidder evnen til at sprede sig.

Både herhjemme og i udlandet er websites den hyppigste kilde til spredning af malware og indsamling af oplysninger fra phishing angreb. I alt blokerer Google dagligt næsten 9.500 nye skadelige websites, der indgår i resultatet af 12-14 millioner søgninger. Antivirusproducenten Symantec angiver at de i maj måned dagligt identificerede 4.359 nye websites indeholdende skadelig kode, hvilket er en stigning på næsten 50 procent i forhold til måneden før.

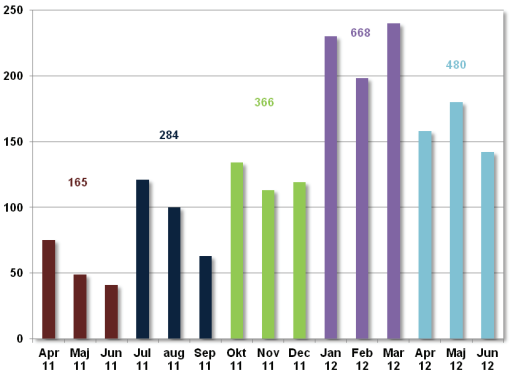
Mens antallet af kompromitterede malware-inficerede websites, der er blevet opdaget af Google, har været svagt faldende siden 2009, er mængden af websites som er oprettet med det formål at sprede malware i samme peridode steget. Flere af dem benytter sig af automatisk generede domænenavne, dynamiske DNS-oplysninger og hyppige skift af hosting-udbyder for at undgå opdagelse. Ifølge Google har også et øget fokus på design af sikre browsere og plugins medført, at social engineering er blevet et vigtigt element af et vellykket malware angreb. Det drejer sig for eksempel om sites til download af falske antivirusprodukter og lignende.

Herhjemme registrerede DK•CERT i andet kvartal 480 hændelser vedrørende legale kompromitterede websider, der forsøgte at inficere de besøgende med malware eller blev benyttet i phishing-angreb (Figur 4). Selv om det er et fald på 28 procent i forhold til kvartalet inden, er det stadig mange i forhold til tidligere. En årsag til dette fald kan være, at hostingudbyderne er blevet bedre til at reagere, således at vi kun i mindre omfang modtager gentagne rapporter om den samme webside. En anden årsag kan være, at phishing-sider er aktive i stadig kortere tid og derfor ikke altid bliver rapporteret til os.

Selvom der stadig er folk, der falder for de samme phishing-tekniker som for fem



Figur 3. Danske malware-infektioner identificeret af F-Secure i andet kvartal 2012.



Figur 4. Danske websites med trojanske heste og phishing-sider rapporteret til DK•CERT.

år siden, er der ifølge Google sket en udvikling. Angrebene er i dag mere kreative og sofistikerede. Således er det ikke ualmindeligt, at en phishingside kun er online i ganske få timer, eller at angrebene er direkte målrettet for eksempel en virksomhed og dens ansatte.

Blandt de foretrukne teknikker der skal lokke os til malware-inficerede websider er søgemaskineoptimering og URL-forkortelser. Sider med skadelig kode optimeres til at figurere højt i resultatet af populære søgninger, og brugen af URL-forkortelser gør det vanskeligt at gennemskue, hvor et link fører hen. Særligt på de sociale netværkssteder hvor URL-forkortelse bruges hyppigt, får det brugere til at klikke på links, som leder til sider med skadelig kode.

En rapport fra antivirus producenten McAfee beskriver, hvordan den globale onlinesvindel er blevet mere avanceret. Et automatiseret netbank-angreb, der startede med Europa som mål, har siden sat fokus på ofre i Latin Amerika og USA. Det bygger på malware-teknikker kendt fra Zeus og SpyEye, men byder ud over det globale fokus på flere nyheder.

Hele transaktionsprocessen var automatiseret og flyttet til tjenester i skyen, som blev hostet hos en bullet-proof ISP. Tjenesterne, der var oprettet til formålet, blev løbende flyttet for at undgå opdagelse, og de nye lokationer blev automatisk distribueret til de inficerede maskiner. Angrebet markerer et skift fra man-in-the-browser angreb til server-side-angreb, hvor serveren tillige har overtaget det traditionelle botnets rolle.

Angrebet, der blev døbt "operation high roller", var som første kvartals angreb på Danske Bank kunder målrettet transaktioner fra konti, hvorfra der kunne overføres relativt store beløb. McAfee estimerede, at der sidst i juni havde været forsøgt overførsler for mere end 60 millioner euro.

En ny version af den trojanske hest Flashback hærgede i starten af april. Den udnyttede en sårbarhed i Java, som endnu ikke var blevet opdateret af Apple. Flash.K spredte sig ifølge Symantec til 600.000 Machintosh-computere, før Apple den sjette april lukkede hullet.

Flame, som blev opdaget i maj, var kvartalets mest omtalte malware. Selvom Flame angiveligt har et par år på bagen, er den blandt de mest avancerede stykker skadelig kode, som hidtil er set. Den har ifølge Kaspersky lab fælles programkode med Stuxnet og udnytter en hidtil ukendt form for kryptografisk kollisionsangreb på MD5-algoritmen. Med et falsk Microsoft certifikat var det muligt at få det skadelige program installeret via Windows Update-funktionen.

Trods den megen omtale udgjorde Flame ikke nogen risiko for de danske netbrugere. Flame var designet til målrettede spionageangreb og var ikke særligt udbredt. Kaspersky lab anslog i maj, at kun 1.000 computere på verdensplan var inficeret.

Trods langt mindre omtale ser malware, der er målrettet de mobile enheder, ud til at udgøre en stigende trussel. Særligt enheder, der benytter Android platformen, er i farezonen. Det skyldes, at brugen af mobile enheder er i vækst, og det er langt lettere at få skadelige applikationer på Android Market, end det er på for eksempel Apples App Store.

Med malware familier som RootSmart, druidKungFu, Stiniter og Opfake er malware målrettet Android steget både i antal og kompleksitet. Antallet af skadelige Android-pakker (APK filer) der blev modtaget af F-secure steg til 3.063 i første

kvartal 2012 mod kun 139 i samme periode af 2011. Stigning må med udbredelsen af Android formodes at fortsætte. Dette set i lyset af at Symantec i maj estimerede, at den trojanske hest Opfake i løbet af 90 dage havde genereret en indtægt til bagmændene på mere end 53.000$.

Mængden af henholdsvis spam-, phishing- og virus-mails, der i maj ramte danskernes indbakker har været relativ lav sammenlignet med tidligere (Figur 5). I figuren, hvor data for marts og april er sat til gennemsnittet for maj måned, ligger alle typer skadelige mails under niveauet fra første kvartal.

Mænden af spammails lå i maj med 67 procent af alle mails på den laveste andel i et år. Det var lidt under det globale gennemsnit på 67,8 procent. Generelt følger danmark den globalt faldende spam-tendens. En forklaring på en svagt faldende kurve kan være, at vi til stadighed sender og modtager flere mails, og at mængden af spam er konstant eller ikke stiger i samme grad.

Næsten 90 procent af de produkter og tjenester, der i maj blev reklameret for i spam, var inden for kategorierne erotiske sider og dating samt medicin. Reklamer for erotiske sider og dating udgjorde 70 procent af alle spam-mails, hvoraf to tredjedele var afsendt fra et com-domæne.

Med hensyn til phishing- og virus-mails har der herhjemme været været større udsving, og gennerelt ligger vi under det globale niveau. I maj måned var 0,11 procent af alle mails herhjemme forsøg på phishing mod 0,18 procent globalt. Tilsvarende indeholdt 0,15 procent af alle mails herhjemme skadelig kode mod 0,27 procent globalt.

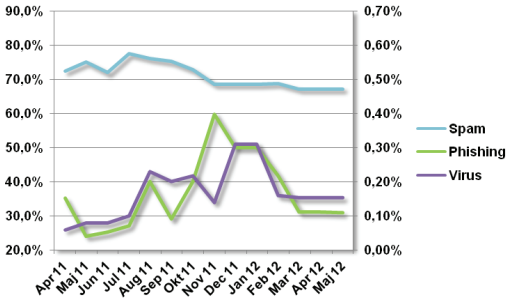
Udover "Nigerianer" mails, der udnytter den politisk ustabile situation i Syrien, har andet kvartals fokus været på de olympiske lege i London. Således fortsætter mails, der foregiver at modtageren har vundet et olympisk lotteri, med at ramme vores indbakker.

F-secure, 2011; "*F-Secure security lab– virusworld map*".
F-secure, 2012; "*Mobile Threat Report Q1 2012*".
Google online security blog, 2012; "*Safe browsing - protecting web users for 5 years and counting*".
Kaspersky lab, 2012; "*Back to Stuxnet: the missing link*".
Mcafee, 2012; "*Dissecting Operation High Roller*".
Securelist, 2012; "*Spam report: April 2012*".
Symantec; "*Intelligence reports*".
Version2, 2012; "*Antallet af netbankindbrud stiger trods NemID*".

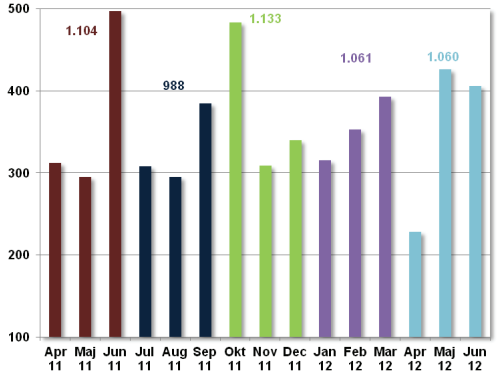
2.3. Sårbarheder

Sårbare applikationer er den væsentligste årsag til kompromittering af data og systemer. Risikovurdering og procedure for opdatering er derfor alfa og omega i sikkerhedsarbejdet. Heldigvis behøver det ikke altid at være så vanskeligt. Flere applikationer kan i dag sættes til at opdatere sig selv og en rapport fra Verizon har vist, at de fleste sikkerhedshuller kan lukkes med relativt simple midler.

Antallet af offentliggjorte nye CVE-nummererede sårbarheder var i andet kvartal på niveau med kvartalet forinden. De 1.061 nye sårbarheder dækker dog over stor månedlig variation (Figur 6).



Figur 5. Danske e-mail-trusler det seneste år registreret af Symantec.



Figur 6. Nye CVE-nummererede sårbarheder offentliggjort af NIST.

Mens det samlede antal sårbarheder har holdt sig konstant, er andelen af sårbarheder, der typisk findes i webapplikationer, faldet for andet kvartal i træk (Figur 7). I alt blev der offentliggjort 204 nye CVE-nummererede sårbarheder i de kategorier, der typisk knytter sig til webapplikationer. Det er et fald på 101 sårbarheder i forhold til første kvartal. 108 af websårbarhederne var af typen Cross-site scripting (XSS).

Ud over Linux-kernen, som der i andet kvartal blev offentliggjort 76 CVE-nummererede sårbarheder i, er det produkter fra Google og Mozilla, der topper listen over produkter med flest nye sårbarheder (Figur 8). Mange af sårbarhederne i Mozillas produkter er dog reelt de samme. For eksempel går sårbarhederne i deres standardversioner igen i ESR versionerne (Extended Support Release), der er rettet mod organisationer som kræver support i implementering og drift.

Når et produkt som Google Chrome er placeret som det næstmest sårbare produkt i andet kvartal, skyldes det til dels, at der i listen ikke er medtaget versionsnumre. I andet kvartal har Google således frigivet to nye versioner af Chrome til Windows, Mac og Linux. Det betyder, at der er blevet offentliggjort og rettet sårbarheder i mindst tre versioner, hvoraf kun to har været i brug samtidig.

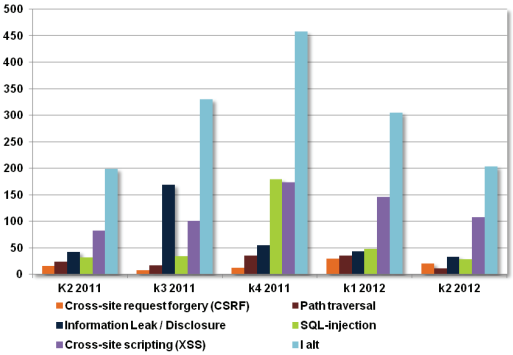
Også Oracle har denne gang skrevet sig på listen over producenter med mange nye sårbarheder i deres produkter, hvoraf flere er erhvervet ved virksomhedsopkøb. Flest sårbarheder blev der offentliggjort til store virksomhedssystemer. Det drejer sig om Oracle Financial Services, der er rettet mod banksektoren og ERP systemet Oracle Peoplesoft Products. Til dem blev der offentliggjort henholdsvis 17 og 15 nye CVE-nummererede sårbarheder. Derudover er det JRE (Java Runtime Enviroment) og JDK (Java Development Kit), som havde henholdsvis 12 og 11 nye sårbarheder. Sårbarheder i Java har gennem den seneste tid været de mest udnyttede.

Mens det er en blandet landhandel af applikationstyper, der topper listen, er de traditionelle browser-plugins og operativsystemer til mobile enheder først at finde længere nede. Således er for eksempel Android og Apples iOS ikke at finde mellem de 100 applikationer, hvortil der blev offentliggjort flest sårbarheder.

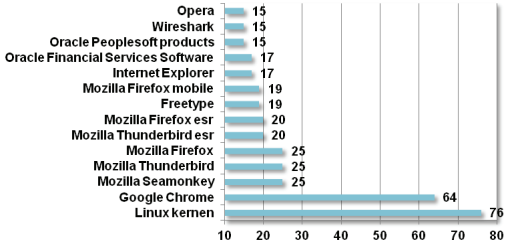
Antallet af sårbarheder, som offentliggøres i en applikation, kan ikke tages som direkte udtryk for applikations generelle sikkerhedsstatus. For eksempel er tilgængeligheden af exploits, der udnytter sårbarhederne og sårbarhedernes potentielle kompromitteringsgrad ikke medregnet. Sikkerhedsfirmaet Secunia har tidligere påvist en sammenhæng mellem udbredelsen af en applikation og tilgængeligheden af exploits. Risikoen for at en sårbarhed forsøges udnyttet, stiger således med applikationens udbredelse.

DK•CERT udførte i andet kvartal sårbarhedsscanninger af 14 institutioner på Forskningsnettet, der er det danske net til forskning og uddannelse. Scanningerne omfattede 6.419 forskellige IP-adresser. På scanningstidspunktet var 426 IP-adresser tilgængelige fra internettet og 136 havde en eller flere sårbarheder. I alt blev der konstateret 631 CVE-nummererede sårbarheder, hvoraf 119 blev risikovurderet som alvorlige. Således havde to procent af de scannede IP-adresser i gennemsnit små 4,5 sårbarheder, hvoraf den ene var risikovurderet til at udgøre en høj risiko.

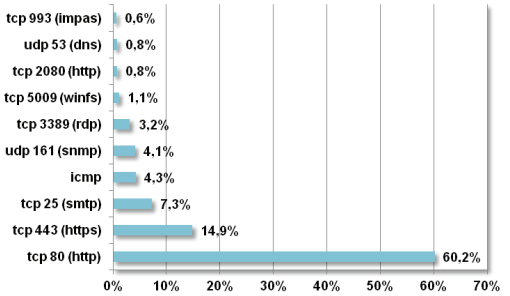
De konstaterede CVE-nummererede sårbarheder fordelte sig på 22 forskellige porte og/eller protokoller, hvoraf 60 procent var i webapplikationer, der lytter på TCP-port 80 (Figur 9). Med små 15 procent af alle sårbarhederne, var det også denne gang de krypterede webapplikationer, der lytter på TCP-port 443 (https), der var de næstmest sårbare. Tre fjerdedele af alle sårbarhederne blev således konstateret i webapplikationer.



Figur 7. Nye CVE-nummererede websårbarheder offentliggjort af NIST.



Figur 8. Nye CVE-nummererede produktsårbarheder offentliggjort i første kvartal 2012.



Figur 9. CVE-nummererede sårbarheder konstateret ved scanning i andet kvartal 2012.

Yderligere sårbarheder blev konstateret på mailtjenester (TCP-port 25 og 993), netværks management protokollen (TCP-port 161), fjernskrivebord (TCP-port 3389), windows filsystem (TCP-port 5009) og DNS på UDP-port 53.

Microsofts april opdateringer indeholdt rettelser til 11 sårbarheder, hvoraf flere fik virksomhedens højeste risikovurdering. Størst prioritet fik opdateringen til Windows Common Controls ActiveX-kontrol, som rettede en kritisk sårbarhed (CVE-2012-0158), der tidligere er udnyttet. Derudover lukker en opdatering til Internet Explorer fem sårbarheder, hvoraf tre er kritiske. En opdatering til Windows fjerner en kritisk sårbarhed (CVE-2012-0151) i kontrol af digital signering. Endelig fjerner opdateringerne sårbarheder i .NET Framework, Forefront Unified Access Gateway, Office og Works. Med opdateringerne offentliggjorde Microsoft, at de stopper supporten på Windows XP og Office 2003 i april 2014.

Den sjette april blev der frigivet en opdatering til Java til Mac OS X, der førte den op på samme version som Oracles versioner til Windows og Linux (1.6.0_31). Herved lukkes der 12 sårbarheder, hvoraf den mest alvorlige (CVE-2012-0507) gjorde det muligt at afvikle kode uden for Javas Sandbox. Den blev blandt andet udnyttet af det skadelige program Flashback, som angiveligt havde cirka 600.000 inficerede Macintosh computere i sit botnet.

Oracle udsendte den 17. april sine kvartalsvise opdateringer, der lukker 88 sårbarheder i virksomhedens produkter. Flere af sårbarhederne er alvorlige og kan udnyttes udefra. Mest kritisk er en sårbarhed i Java-værktøjet JRockit (CVE-2012-1695), som fik højeste CVSS score 10. Udover Oracles egne produkter som for eksempel Database Server, Fusion Middleware, Enterprise Manager Grid Control og E-Business Suite indeholdt opdateringen rettelser til de tidligere Sun-produkter Solaris og MySQL.

I alt 14 CVE-nummererede sårbarbarheder lukkes med Mozillas opdatering til Firefox 12 den 25. april. Halvdelen af sårbarhederne er vurderet som kritiske og kan medføre kørsel af programkode fra et angribende website. Udover opdateringen af Firefox frigav Mozilla rettelser til Thunderbird og SeaMonkey. Hidtil har Mozillas opdateringer været underlagt Microsofts UAC (User Account Control). Efter Firefox i version 12 sker opdateringer uden brugerens accept.

Den fjerde maj udsendte Adobe en opdatering af Flash Player til Windows, Macintosh, Linux og Android (APSB12-09). Den nye version fjerner en sårbarhed, som er set udnyttet (CVE-2012-0779). Sårbarheden gør det muligt for en angriber at få fuld kontrol over den sårbare pc.

Den ottende maj udsendte Microsoft sine månedlige opdateringer. De indeholdt syv opdateringer, der fjerner 23 sårbarheder i virksomhedens produkter. Mest kritisk er sårbarhederne CVE-2012-0183 i Word samt CVE-2012-0160 og CVE-2012-0161 i .NET Framework. De gør det muligt at afvikle kode på den sårbare maskine. Derudover blev en opdatering, der lukker ti sårbarheder i Office, Windows, .NET Framework og Silverlight vurderet som kritisk. De øvrige opdateringer retter sårbarheder i .NET Framework, Office, Visio Viewer 2010, TCP/IP-stakken i Windows samt Windows Partition Manager.

Apple udsendte den 9. maj opdateringer, som retter 36 sårbarheder i Mac OS X samt fire i Safari. Med OS X Lion version 10.7.4 og Security Update 2012-002 til version 10.6.8 rettes blandt andet en omtalt sårbarhed (CVE-2012-0652), der giver adgang til passwords ved brug af Filevault. Den nye version af Safari (5.1.7) retter blandt andet en række cross-site scripting-sårbarheder i WebKit.

Den 23. Maj udsendte Google en opdatering til Chrome 19, som var blevet frigivet en uges tid forinden. Opdateringen til version 19.0.1084.52 på Windows, Macintosh og Linux retter 13 sårbarheder. Ni sårbarheder fik Googles næsthøjeste risikovurdering, mens ingen blev vurderet som kritiske.

Igen den ottende juni udsendte Adobe en opdatering af Flash Player. Opdateringen (APSB12-14) er tilgængelig på alle platforme og fjerner syv sårbarheder. Seks sårbarheder er vurderet som alvorlige, da de giver mulighed for at afvikle programkode.

Oracles kvartalsvise opdateringer den12 juni 2012 lukker 14 sårbarheder i Java til Windows, Mac OS X, Solaris og flere Linux-varianter. Seks sårbarheder fik højeste risikovurdering og kan udnyttes over nettet uden at logge ind på det sårbare system.

Juni opdateringerne fra Microsoft den 12. juni 2012 indeholdt i alt rettelser til 26 sårbarheder. De syv opdateringer retter flere alvorlige sårbarheder i Windows, Internet Explorer, .Net Framework, Lync og Dynamics AX. Højest prioriterede opdatering lukker 13 sårbarheder i Internet Explorer og en i Remote Desktop Protocol (RDP) i Windows. En sårbarhed til Internet Explorer (CVE-2012-1875), der indgik i Microsofts juni opdateringer, blev senere set udnyttet.

Den 20 juni udsendte Cisco opdateringer, der lukker fire sårbarheder i VPN-klientprogrammet AnyConnect Secure Mobility Client. Sårbarhederne giver mulighed for at afvikle programkode eller nedgradere til en tidligere version. Tre sårbarheder findes i versionerne til både Windows, Mac OS X og Linux, mens den fjerde kun berører 64-bit Linux.

Adobe, maj 2012; "*Security update available for Adobe Flash Player*".
Adobe, juni 2012; "*Security update available for Adobe Flash Player*".
Apple, 2012; "*About the security content of Java for OS X Lion 2012-002 and Java for Mac OS X 10.6 Update 7*".
Apple, 2012; "*About the security content of OS X Lion v10.7.4 and Security Update 2012-002*".
Apple, 2012; "*About the security content of Safari 5.1.7*".
Cisco, 2012; "*Multiple Vulnerabilities in Cisco AnyConnect Secure Mobility Client*".
Computerworld, 2012; "*Apple patches Mac Java zero-day bug*".
DK•CERT, 2011; "*DK•CERT Sårbarhedsdatabase*".
Google, 2012; "*Google Chrome releases*".
H-online, 2012; "*Russian AV company claims 600,000 Macs infected by Flashback – Update*".
Microsoft, 2012; "*Microsoft security bulletin summary for april 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for june 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for may 2012*".
Mozilla, 2012; "*Security Advisories for Firefox*".
Nvd.nist.gov; "*CVE and CCE statistics query page*".
Oracle, 2012; "*April 2012 critical patch update released*".
Oracle, 2012; "*Oracle critical patch update advisory - april 2012*".
Oracle, 2012; "*Oracle Java SE critical patch update advisory - june 2012*".
Secunia, 2012; "*Secunia yearly report 2011*".
Sophos, 2012; "*IE remote code execution vulnerability being actively exploited in the wild*".
Sophos, 2012; "*Top 5 myths of safe web browsing*".
Verizon, 2012; "*2012 data breach investigations report*".

3. Overskrifter fra andet kvartal 2012

De netop overståede Europa mesterskaber i fodbold sluttede stort set uden at fange de internet-kriminelles opmærksomhed. Derimod har de været aktive op til de olympiske lege i London. Alt fra falske billetter, merchandise, hotelophold og falske lotterigevinster bliver tilbudt i e-mail-kampagner, på online auktioner og falske hjemmesider, der hævder at tilhøre organisationen bag de olympiske lege eller dens sponsorer. Tilsvarende er der set forsøg på spredning af malware i de olympiske leges navn.

Andet kvartal 2012 bød også på andre hændelser, der fangede vores interesse. I dette afsnit kan du således læse om, hvordan tre styrelser under Erhvervs- og Vækstministeriet i slutningen af april var under angreb. Eller hvordan der nu åbnes for myndighedernes brug af tjenester i skyen. En åbning, der hovedsageligt er muliggjort gennem standardisering af kontrakter og it-sikkerheden. Du kan også læse om, hvordan diskussionen om det tidligere så udskældte logningsdirektiv nu er blusset op igen, og hvorfor den i vores optik på nogle områder er forfejlet.

Heller ikke i andet kvartal blev vi forskånet for malware. Denne gang var det den trojanske hest Flame, som ramte mediernes overskrifter. Ligesom Stuxnet var Flame sandsynligvis udviklet for eller af den amerikanske stat. Denne gang med det formål at opsamle informationer fra de inficerede systemer. Det bemærkelsesværdige er, at den tilsyneladende havde huseret i mere end to år uden at blive opdaget. En væsentlig forklaring er dens manglende udbredelse.

I starten af juni måned kunne den sociale netværkstjeneste LinkedIn fortælle, at en fil med 6,5 millioner password til tjenesten var blevet lækket. Skaden var dog umiddelbart ikke så stor. For eksempel indeholdt filen ikke de tilhørende brugernavne.

Omvendt måtte hosting-leverandøren Surftown senere på måneden afvise en mistanke om, at deres bagvedliggende systemer var kompromitteret. Surftown øgede sikkerheden, men kunne med fordel også have kigget på hvordan udbyderne af cloud-tjenester, har øget transparensen af deres tjenester. Den udvikling ser dog ud til at være på vej i branchen.

Også udbredelsen har haft betydning for mængden af malware, som i dag florerer på Android-platformen. Malware til Android-smartphones er i eksplosiv vækst, og udviklingen ligner den, vi tidligere har set til både Windows og Macintosh. Mængden af enheder der benytter platformen og tilgængeligheden af udviklingsværktøjer betyder, at den er blevet interessant for de internet-kriminelle.

De valgte historier er tilsammen med til at skitsere, hvordan samfundets brug af informationsteknologi er under stadig udvikling og hermed også de trusler, vi står over for. Et stigende krav om digitalisering medfører samtidig, at vi digitaliserer aktiver, som også har værdi for andre end os selv. Det stiller nye krav til lovgivningen og de måder vi gør tingene på.

Med digitalisering betræder vi på mange måder nyt land. Skal denne proces foregå effektivt, bør vi have større fokus på mellemregningerne og ikke blot kigge på resultatet. Vi bliver nødt til at kunne lære af hinandens viden og erfaringer og have større transparens om, hvorfor vi handlede som vi gjorde, så vi kan forstå, hvorfor resultaterne blev som de blev. Også når det gælder informationssikkerhed.

LONDON 2012

A lottery for the Future 2012 Olympics

Address 61-70 Southampton Row UK
Phone: + 44 703 174 5960
Fax: + 44 844 500 6552
Email: sir.george_ellis.olympic@hotmail.co.uk

Congratulations!

Your E-mail address is one of the 9 lucky selected winning Email Address that won in the London 2012 Olympic Campaign Promotion; you have won the sum of (£800, 000.GBP) Pounds (Eight Hundred Thousand Great British Pounds Sterling), i wish to congratulate you on this Nomination.

Below are your identification numbers, kindly fill the below information's for official Records.

REFERENCE NUMBER: UK/2012 /OLY/CAMP
BATCH NUMBER: UK/2012/153/CAMP/
SECURITY CODE: 2011/2012/8828

1. Your Full name: .....
2. Your Country: .....
3. Contact Address: .....
4. Telephone Number: .....
5. Fax Number: .....
6. Marital Status: .....
7. Occupation: .....
8. Sex: .....
9. Age: .....

You are required to forward the requested details of your winning to the above office contact details, to enable us facilitate the processing of your claim.

NOTE: THE IOC (INTERNATIONAL OLYMPIC COMMITTEE) SUPPORT BARCLAYS TEAM, TO CREATE AWARENESS FOR THE UPCOMING 2012 OLYMPIC GAMES, WHICH IS SPONSORING THIS PROGRAM.

Regards.
Elizabeth Adams.
Promotion Manager

LONDON 2012 OLYMPICS PROMOTION

Figur 10. Phishingmail med Olympisk lotterigevinst.

"… samfundets brug af informationsteknologi er under stadig udvikling og hermed også de trusler, vi står over for."

London2012, 2012; "*Stay safe online*";www.london2012.com/stay-safe-online/.
Trendmicro, 2012; "*Cybercriminals race to the 2012 Olympics*".

3.1. Danske myndigheder under angreb

Den 26. april varslede GovCERT de statslige organisationer om, at et ministeriums installationer var blevet kompromitteret, og man forventede yderligere angreb på danske myndigheder. Siden ramte historien pressen, og den 30. april fortalte GovCERT og Statens It, at angrebene nu var imødegået. Men hvad der egentlig skete, står stadig uklart for offentligheden.

Om eftermiddagen den 26. april konstaterede den statslige varslingstjeneste GovCERT et indbrud i et it-system hos en styrelse under Erhvervs- og Vækstministeriet. Indbruddet var af en sådan karakter, at man forventede yderligere angreb på andre myndigheder. Herefter udsendte GovCERT en advarsel til de statslige organisationer, hvori man opfordrede til skærpet opmærksomhed og logning.

Dagen efter ramte historien medierne, og GovCert advarede igen de statslige organisationer. Denne gang indeholdt advarslen oplysninger om tre udenlandske IP-adresser, som angiveligt havde relation til hændelserne. Siden er det kommet frem, at Sikkerhedsstyrelsen, Søfartsstyrelsen og Erhvervsstyrelsen alle blev ramt af angrebet og i større eller mindre grad havde været nødsaget til at lukke deres systemer ned.

Den 30. april kom den officielle udmelding fra henholdsvis GovCERT og Statens IT. Tre styrelser under Erhvervsministeriet havde været udsat for angrebet, som nu var blevet inddæmmet. Hændelsen var blevet politianmeldt, og man havde blandt andet iværksat øget overvågning af de statslige systemer. Derudover understregede GovCERT sine tidligere anbefalinger om:

"*… at der er aktiveret logning på alle it-systemer.*"

Tilbage står en række ubesvarede spørgsmål om hvem, hvad og hvorfor. Hvorvidt angrebene har relation til Anonymous-bevægelsens tidligere trusler mod blandt andet danske myndigheder, står derfor hen i det uvisse. Det er således ikke muligt at vurdere, om der var tale om en enkeltstående hændelse, eller den skal tages som udtryk for en generel større trussel mod danske interesser.

Selvfølgelig er det ikke muligt at informere i detaljer, da hændelsen er blevet politianmeldt og til dels vedrører rigets sikkerhed. Information kan dog have værdi ved risikovurdering på de øvrige danske installationer. Organisationer ud over de berørte har således ingen mulighed for at drage nytte af de erfaringer, der blev gjort i forhold til risikovurdering, fremtidig sikring, beredskab, korrigerende handlinger med mere.

Govcert, 2012; "*Angreb på Erhvervs- og Væksministeriet*".
Statens it, 2012; "*Erhvervs- og Vækstministeriet angrebet af hackere*".
Version2, 2012; "*GovCERT slår alarm: Advarer alle ministerier mod hackerangreb*".
Version2, 2012; "*Hackerangreb lammer ministerium*".
Version2, 2012; "*Hackerangreb plager ministerium på 4. døgn*".

"Tilbage står en række ubesvarede spørgsmål om hvem, hvad og hvorfor."

3.2. Nye muligheder for brug af cloud-tjenester i det offentlige

Tidligere har brug af tjenester i skyen stort set været forbeholdt private virksomheder, der ikke behandlede og lagrede personfølsomme oplysninger i tjenesterne. Blandt de springende punkter har været usikkerhed om, hvor og hvordan data blev lagret. Fra flere kanter ser der nu ud til at være en opblødning undervejs.

Den 28. maj annoncerede Google, at deres cloudbaserede kontorpakke til erhvervslivet var blevet certificeret efter ISO 27001-standarden. Dermed trådte Google Apps for Business et væsentligt skridt nærmere at blive benyttet af danske organisationer og myndigheder.

Også Microsoft har underkastet sig standarden for deres cloud-baserede kontorpakke Office 365. De har forpligtet sig til at lade sikkerheden i selve løsningen og i datacentrene underkaste audit (revision), som udføres i overensstemmelse med ISO 27001. Blandt andet derfor har Datatilsynet delvist åbnet for, at myndigheder og virksomheder herhjemme kan bruge Office 365. Også når det gælder personfølsomme oplysninger.

For begge tjenester gælder, at man nu har mulighed for at sikre sig, at behandlingen af persondata følger EU's regler. Hos både Google og Microsoft kan man underskrive kontrakter, der opfylder EU-Kommissionens krav til databehandlere. Ved at følge EU-Kommissionens standardkontraktbestemmelser for overførsel af personoplysninger til en databehandler i et tredjeland er de første spadestik taget til brug af cloudbaserede tjenester i det offentlige.

Med Datatilsynets behandling af Microsoft Office 365 er det blevet mere gennemskueligt, hvad der kræves, før man kan bruge tjenester placeret i skyen. I kombination med et stigende marked for cloudbaserede løsninger, der overholder EU-Kommissionens kontraktkrav, kan det være med til at skubbe flere offentlige tjenester ud i skyen.

På længere sigt vil det være til gavn for ikke bare økonomien og miljøet, men også for sikkerheden. For som Director of Security i Google, Eran Feigenbaum, udtalte i forbindelse med certificeringen af Google Apps for Business:

"*... businesses are beginning to realize that companies like Google can invest in security at a scale that's difficult for many businesses to achieve on their own.*"

Datatilsynet, 2012; "*Behandling af personoplysninger i cloud-løsningen Office 365*".
Digitaliseringsstyrelsen, 2011; "*Cloud computing og de juridiske rammer*".
Google, 2012; "*Google Apps receives ISO 27001 certification*".
Version2, 2012; "*Google på vej til at fjerne EU-barriere for Google Apps til danske myndigheder*".

"... businesses are beginning to realize that companies like Google can invest in security at a scale that's difficult for many businesses to achieve on their own."

3.3. Fornyet kritik af logningsbekendtgørelsen

Ved angrebet på tre styrelser under Erhvervs- og Vækstministeriet i april lød rådet fra GovCERT blandt andet, at man aktiverede og skærpede logningen. På politisk plan er der ønske om det modsatte: En lempelse af logningsbekendtgørelsen. Argumentet er, at loggede data kun sjældent bliver brugt.

Det er ikke ualmindeligt, at afdækningen af en sikkerhedshændelse stopper ved, at der ikke er foretaget tilstrækkelig logning. For eksempel i tilfælde, hvor IP-adressen på en malware-inficeret computer peger på en NAT-adresse, et WI-FI-hotspot eller lignende, oplever vi ofte, at det ikke er muligt at opspore og rense den inficerede computer.

På virksomhedsniveau er der generelt forståelse for at, logning er nødvendig. Både i forhold til gældende standarder som for eksempel ISO 27001 og i forhold til afklaring og dokumentation af sikkerhedshændelser. Med den lovpligtige logning af tele- og internettrafik forholder det sig anderledes. De virksomheder, der står med den administrative og økonomiske byrde, har ikke selv nogen interesse i loggen.

Derfor er der fra flere sider herhjemme sat spørgsmålstegn ved, om logningsdirektivet er blevet overimplementeret i forhold til EU's retningslinjer. For eksempel fik en opgørelse, der viste, at politiet havde efterspurgt internetoplysningerne 170 gange i 2010, politikere fra både Enhedslisten og Venstre til at udtale, at de ville stille beslutningsforslag om helt at afskaffe sessionslogningerne.

Forslag om en eventuel lempelse af logningsbekendtgørelsen tager primært udgangspunkt i antallet af gange, politiet har benyttet logfilerne. Der stilles således ikke spørgsmål til, om de kunne være benyttet mere og hvorfor de eventuelt ikke blev det, eller hvordan det eventuelt kan se ud i fremtiden.

Ud over at afskaffelsen af sessionslogning kan være et dårligt signal at sende til organisationerne, kan der i fremtiden vise sig at være større behov for dem, end der er i dag. For eksempel udtalte politiinspektør Magnus Andresen til avisen Information om en stigende mængde data og tjenester placeret i skyen:

"Det kunne gøre, at man i fremtiden fik et større behov for analyse af sessionslogninger."

Tilbage står at logning er et centralt element i forhold til sikkerhedsarbejdet. I forbindelse med en sikkerhedshændelse er loggen ofte det eneste sted at finde svar på spørgsmål om, hvad der skete. De svar kan være med til at forhindre fremtidige hændelser. Det blev delvist illustreret ved aprils angreb på styrelser under Erhvervs- og Vækstministeriet, hvor GovCERT rådede til, at man aktiverede og skærpede logningen.

På trods af et bredt politisk ønske om ændring af logningsbekendtgørelsen kunne dronning Margrethe den 18. juni underskrive en lovændring, der udsatte revisionen af bekendtgørelsen til folketingsåret 2012-13.

Information, 2012; *"Størstedelen af internet-logningen kan sløjfes"*.
Retsinformation, 2012;*"Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige"*.
Version2, 2012; *"Massiv logning af danskernes internetbrug - men politiet bruger kun IP-adressen"*.

3.4. Flame – malware som spionageværktøj

I slutningen af maj fortalte flere kilder om et nyopdaget skadeligt program. Nogle kaldte det Flame, andre Flamer, SkyWiper eller Wiper. FN-organet ITU (den internationale teleunion) havde hyret sikkerhedsfirmaet Kaspersky lab til at undersøge et

angreb, som var gået ud over computere hos Irans olieministerium. Angrebet førte i april til, at Iran koblede flere olieterminalers netværk fra internettet. Kaspersky lab fandt frem til programmet, de kaldte Flame.

Med en samlet størrelse på omkring 20 megabyte er Flame langt større end typiske eksempler på malware. Programmet ser ud til at være skrevet til at udføre målrettet spionage. Ifølge avisen Washington Post er Flame udviklet af USA og Israel med det formål at forsinke Irans atomprogram. Avisen citerer unavngivne kilder for, at Flame blev brugt til at indsamle information.

Hvis det er korrekt, kan den indsamlede information senere have været brugt i et sabotageangreb, hvor ormen Stuxnet saboterede centrifuger, der blev brugt i atomprogrammet. Kaspersky lab har fundet fælles programkode i Flame og Stuxnet.

Teknisk set er Flame interessant ved, at den udnytter en hidtil ukendt form for kryptografisk kollisionsangreb på MD5-algoritmen. Det gør det muligt for bagmændene at udarbejde et certifikat, der ser ud til at være udstedt af Microsoft. Med dette certifikat stemplede de dele af programkoden. Derved blev det muligt at få det skadelige program installeret via Windows Update-funktionen, da programmet så ud til at være signeret af Microsoft. Microsoft udsendte 3. juni en sikkerhedsadvarsel og tog flere skridt til at forhindre, at tricket kunne gentages.

Trods den megen omtale udgør Flame ikke nogen fare for hovedparten af de danske netbrugere. Det skyldes, at programmet er beregnet til målrettede spionageangreb. Derfor er det ikke særlig udbredt – Kaspersky lab anslog i maj, at kun 1.000 computere på verdensplan var inficeret.

Derimod er Flame væsentlig som et eksempel på, hvordan skadelige programmer nu indgår i værktøjskassen hos militær og efterretningsvæsener i jagten på fortrolige informationer.

Centrum Wiskunde & Informatica, 2012; "*CWI cryptanalyst discovers new cryptographic attack variant in Flame spy malware*".
Kaspersky lab, 2012; "*Back to Stuxnet: the missing link*".
Microsoft, 2012; "*Microsoft releases Security Advisory 2718704*".
New York Times, 2012; "*Facing cyberattack, Iranian officials disconnect some oil terminals from internet*".
Washington Post, 2012; "*U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*".
Wikipedia, 2012; "*Flame (malware)*".

3.5. 6,5 millioner passwords til LinkedIn blev lækket

"Our team is currently looking into reports of stolen passwords. Stay tuned for more."

Sådan lød en Twitter-besked fra det sociale netværk LinkedIn den 6. juni. I tiden derefter viste det sig, at rygterne holdt stik: På et russisk websted var der placeret filer med i alt 6,5 millioner passwords til LinkedIn.

Passwordene var lagret i form af hashværdier. Man kunne altså ikke direkte læse de enkelte passwords. Men hvis man gættede sig til et password, kunne man se om det fandtes i listen. Ifølge sikkerhedsfirmaet Sophos blev 60 procent af password-

"Trods den megen omtale udgør Flame ikke nogen fare for hovedparten af de danske netbrugere."

ene gættet i løbet af det første døgn.

Filerne indeholdt ikke de brugernavne, som hørte til de berørte passwords. LinkedIn nulstillede passwords for de konti, hvis passwords befandt sig på listen. Firmaet oplyser, at det ikke har hørt fra brugere, hvis konti er blevet kompromitteret som følge af offentliggørelsen.

Ifølge et blogindlæg fra direktør Vicente Silveira, LinkedIn, havde firmaet i nogen tid arbejdet på at forbedre sikkerheden. Således var der allerede før offentliggørelsen indført et system, hvor passwords ikke kun beskyttes med en hash-funktion. Nu bliver der også tilføjet et såkaldt salt. Det gør det vanskeligere at finde frem til, hvilket password der gemmer sig bag en hashværdi. Det ser altså ud til, at de offentliggjorte passwords ikke var helt nye.

Affæren illustrerer både styrker og svagheder ved autentificering baseret på passwords. Hvis man har et stærkt password, vil det være vanskeligt at knække. Men man risikerer, at webtjenester lagrer ens password på en måde, der gør styrken ligegyldig: Hvis et password er gemt i klartekst, er det ligegyldigt hvor stærkt det er, hvis hackere får fat i det.

Derfor er det vigtigt, at man ikke genbruger passwords på tværs af tjenester. Hvis man har brugt et unikt password til sin LinkedIn-konto, tager det ikke mange sekunder at skifte til et nyt. Men hvis man har genbrugt det samme password til en række andre tjenester, vil det være en større opgave at logge ind på dem alle og ændre password.

LinkedIn, 2012; "*An update on taking steps to protect our members*".
Sophos, 2012; "*LinkedIn confirms hack, over 60% of stolen passwords already cracked*".
Twitter, 2012; "*LinkedIn*".

3.6. Balladen om Surftown

I juni måned stillede Version2 gentagne gange spørgsmålstegn ved sikkerheden på Surftowns webhotel-løsninger. Surftown afviste kritikken og øgede sikkerheden. Sagen rummer dog nogle generelle aspekter om, hvad vi som kunder kan forvente af vores leverandører og hvordan det kommunikeres.

Rene Madsen fra Online Marketing udtalte den 20. juni til nyhedssitet Version2, at han havde oplevet flere hackede hjemmesider på samme IP-adresse. Problemet var ikke specifikt for Surftown, det var blot det seneste tilfælde. Hans konklusion var, at angrebet var sket gennem en root adgang i webhotellets underliggende systemer. Det blev afvist af Kresten Bach Søndergaard, der er kommunikationschef hos Surftown.

En uges tid efter kunne Surftown gentage afvisningen. Man havde nu undersøgt, om der var hold i anklagerne og var i gang med at kigge på logfiler. På baggrund af anklagerne hævede Surftown på nogle områder sikkerheden og forbedrede overvågningen.

Dagen efter kunne Version2 fortælle, at der også havde været lækket lister med brugernavne og passwords til PHPmyadmin hos Surftown. Det blev fejlagtigt tolket som, at den oprindelige anklage måtte være sand. Ved en senere opdatering af artiklen viste det sig, at det kun drejede sig om en enkelt kundes databaseadgang

med PHPmyadmin.

I den aktuelle sag har Surftown afvist alle anklager og kan herefter henvise deres kunder til aftaleteksten for deres webhotelløsninger:

"Surftown påtager sig i øvrigt intet ansvar for uvedkommendes overvågning eller opsamling af eller adgang til Kundens trafik eller data."

I samme aftale fraskriver Surftwon sig ansvaret for kundernes eventuelle tab:

"… medmindre Surftown har handlet forsætligt til skade for Kunden eller groft uagtsomt."

Den manglende dialog og totale ansvarsfraskrivelse er måske det store problem i denne sag. Selv om Surftown har handlet ansvarsfuldt, og der ikke har været et problem på deres ydelser, står kunderne tilbage med tvivlen.

Problemet er, at kunderne ikke kan gennemskue, hvilken sikkerhed de får af leverandøren, og hvad der er deres eget ansvar. Et væsentligt punkt er udformningen af aftalerne, hvor leverandøren bør beskrive deres ansvar, og hvad de gør for at leve op til det. Her kunne man lære af for eksempel cloud-leverandørerne, som på mange områder er i gang med at standardisere deres tjenester. Som her bør den enkelte hosting-udbyder kunne tilbyde sikkerhed, der overgår den enkelte kundes muligheder, da der for alle kunder er tale om samme standartiserede produkt.

Den nyligt stiftede Brancheforening for IT-hostingvirksomheder i Danmark (BFIH) ser ud til at være et skridt i den retning. Den arbejder for at højne kvalitets- og sikkerhedsniveauet på hosting-ydelser samt gøre det lettere at gennemskue og sammenligne ydelsernes kvalitet og sikkerhed. Et væsentligt aspekt af det arbejde hedder standardisering og certificering.

Vi har tidligere været efter hosting-udbyderne for ikke i tilstrækkelig grad at tage vare på kundernes sikkerhed. Vores kritik har primært været rettet mod, hvorvidt og hvor hurtigt der blev reageret, når vi havde konstateret en sikkerhedshændelse. Vores generelle indtryk er, at vi er på vej i den rigtige retning. Vi har i den periode, hvor kritikken af Surftown har været rejst, ikke kunnet konstatere flere hændelser end normalt vedrørende phishing-sider og malware hos Surftowns kunder.

Brancheforeningen for IT-hostingvirksomheder i Danmark (BFIH), 2012; "*Om BFIH*".
Surftown, 2009; "*Forretningsbetingelser*".
Version2, 2012; "*Mystiske hackerangreb hos Surftown-kunder: Hvordan kommer de ind?*".
Version2, 2012; "*Password til Surftown-konto lækket af Anonymous - i marts*".
Version2, 2012; "*Surftown afviser definitivt interne hackerangreb - men hæver sikkerheden*".

3.7. Android – historien der gentager sig

Gennem det seneste år er brugen af bærbare enheder mere end fordoblet. Næsten 13 procent af de danske websider som danskerne kiggede på i april, blev set fra en mobiltelefon eller tavle-pc. Det har betydet, at særligt Android er blevet mål for malware. Det er der mange forklaringer på, og udviklingen ligner noget, vi har set før.

Apples iPhone og iPad, der begge benytter styresystemet iOS, stod ifølge Foreningen af Danske Interaktive Medier (FDIM) for 9,6 procent af de danske sidevisninger

"Selv om Surftown har handlet ansvarsfuldt, og der ikke har været et problem på deres ydelser, står kunderne tilbage med tvivlen."

i april 2012. De forskellige enheder, der benytter Android, stod for 3,2 procent (Figur 11). Selv om udbredelsen og brug af Android ikke overgår iOS, er der herhjemme sket en fordobling i antallet af danskernes visninger af websider fra danske medier gennem perioden maj 2011 til april 2012.

Mens iOS stort set har været forskånet for malware, eksploderer mængden af skadelig kode til Android. Således modtog F-Secure i første kvartal 2012 i alt 3.063 skadelige Android-pakker (APK filer) mod kun 139 i samme periode året før. Samtidig er kompleksiteten af den fundne malware steget både med hensyn til spredning og funktionalitet.

84 procent af de malware-varianter, som blev opdaget til Android i første kvartal 2012, var trojanske heste. Nogle varianter indeholdt desuden botnet-funktionalitet eller evnen til at installere yderligere programmer, foretage opkald og afsende overtakserede sms'er. Derudover var det ikke ualmindeligt, at de fundne malware-varianter for eksempel krypterede data eller gemte dem i billedfiler.

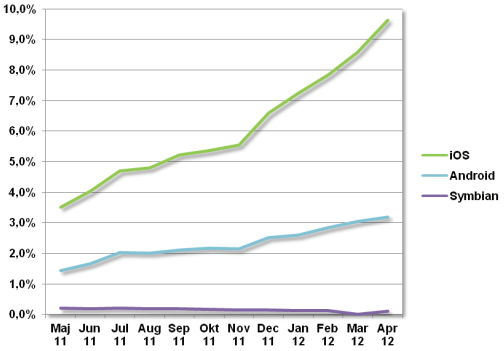
Når de mobile enheder er interessante for malware-udviklerne, skyldes det flere faktorer. Mobiltelefoner og tavle-pc'er er reelt små computere, der benyttes til alt fra e-mail, spil og webtrafik til e-handel. Data på en mobil enhed er i dag ligeså værdifulde som data på en traditionel computer. De mobile enheder slukkes sjældent, og den stigende udbredelse gør dem i sig selv til et attraktivt mål. Derudover har teknologien nået en modenhed, så der findes flere udviklingsmiljøer, der gør det lettere at udvikle malware.

Mange opfatter ikke deres mobil som et potentielt mål for internet-kriminalitet. Derfor er det hovedsageligt i erhvervslivet, der i øjeblikket er et marked for kryptering, antivirus og lignende. Den stigende mængde mobile enheder med adgang til stadig hurtigere mobilt netværk vil sandsynligvis medføre udvikling af endnu mere malware rettet mod de mobile enheder.

At det er Android, de kriminelle har kastet sig over, skyldes platformens åbenhed i forhold til iOS. Her skal alle applikationer godkendes, inden de lægges til download fra Apples App Store. Det er langt lettere at lægge skadelige applikationer på Android Market.

Udviklingen ligner den, vi tidligere har set for både Windows og Macintosh. Mens udbredelsen af internetopkoblede Windows-computere steg op gennem 1990'erne, steg også mængden af orme og virus, hvis udvikling var muliggjort af en stigende mængde tilgængelige udviklingsplatforme. Samme udvikling har vi de senere år set for Macintosh-computerne, der tidligere var forskånet for malware.

De stigende markedsandele i kombination med at mange brugere har ment, at det ikke var nødvendigt med antivirus-software til Macintosh, har gjort platformen til et attraktivt mål. Gennem de seneste år er malware, der også rammer denne platform, derfor eksploderet i antal.



Figur 11. Andel af sidevisninger med mobile enheder på danske websites.

F-secure, 2012; "*Mobile Threat Report Q1 2012*".
Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Operativsystemer*".

4. Ordliste

Adware: Software, der viser reklamer mens applikationen afvikles. Adware betegner både legale applikationer, som er gratis at benytte mod fremvisning af reklamer, samt malware der har til formål at eksponere reklamer på den inficerede computer.

Anonymous-bevægelsen: En løst defineret internetbaseret gruppe, som i 2003 opstod via hjemmesiden 4chan.org. Gruppen benytter sig blandt andet af DDoS angreb i deres kamp for ytringsfrihed og mod hvad de anser som censur og misbrug af nettet. Er særlig kendt for dens modstand mod Scientology Kirken og for sin støtte til Wikileaks og The Pirate Bay. Gruppen stod også bag operation AntiSec i foråret 2011.

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.

Bullet-proof hosting: En service uden restriktioner på det som hostes. Udbydes af ISP'er og hostingvirksomheder, der lægger net og maskiner til alt fra børnepornografi, phishing-sider, botnetaktivitet og lignende. Organisationer, der tilbyder bullet-prof hosting samarbejder ikke med myndighederne og reagerer ikke på klager over det som hostes.

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 sårbarhed på et websted, der gør det muligt at afvikle scriptkode i browseren hos en bruger, der besøger det. 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.

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 fore-

spørgsler. Disse angreb udføres ofte fra flere computere samtidigt, og kaldes i de tilfælde for distributed denial of service (DDoS).

Exploit: Et eksploit er kode, som forsøger at udnytte sårbarheder i software med det formål at kompromittere 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-funktionen (Government Computer Emergency Response Team), der i Danmark er placeret under Forsvarsministeriet, 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 itsikkerheden samt varsle myndigheder om it-sikkerhedsmæssige hændelser og trusler.

Hacker: På dansk betyder hacker en person, der uden foregående tilladelse forsøger at kompromittere computersystemers sikkerhed. På engelsk kan man skelne mellem en hacker og en cracker eller whitehat hacker og blackhat hackere, afhængigt af om aktivitetens formål er at forbedre kode og/eller sikkerhed, eller det er at udføre it-kriminalitet.

Hacktivisme: Sammentræning af hack og aktivisme, eller på dansk "politisk motiveret hacking". Det vil sige forfølgelse af politiske mål gennem brugen af midler som defacement, DDoS-angreb, informationstyveri og lignende.

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

Man-in-the-browser: Et angreb relateret til Man-in-the-middle angreb, hvor en trojansk hest kan modificerer websider og indhold af transaktioner uden brugerens viden. Man-in-the-browser funktioner kan være at overtage sessionen til netbanken, overføre penge fra brugerens konto og herefter ændre indholdet i browseren, således at overførelsen ikke fremgår af kontooversigten.

Man-in-the-Middle: En angrebsform, hvor kommunikationen mellem to parter uden parternes vidende, videresendes gennem en mellemmand, der aktivt kan kontrollere kommunikationen. I praksis kan et Man-in-the-middle-angreb fx foregå ved en ændring af DNS-registrering enten på DNS-serveren eller ved ændring af hosts-filen.

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.

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, 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.

Social engineering: Manipulation, der har til formål at få folk til at bidrage med informationer eller at udfører handlinger, som fx at klikke på links, svare på mails eller installere malware.

Spear phishing: Phishing-angreb, der er rettet mod en specifik målgruppe. Typisk nøglemedarbejdere i den organisation som er mål for angrebet.

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.

Stuxnet: Stuxnet er blandt de hidtil mest avancerede orme. Ormen spreder sig via USB-nøgler ved at udnytte en sårbarhed i Windows' behandling af genveje. Herefter angriber den industrielle Siemens WinCC SCADA-systemer. Den menes at være udviklet til at sabotere Irans atomprogram.

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.

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 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 også gøre det. Virus spredes ofte som mail vedlagt en trojansk hest, der indeholder virussen selv.

Warez, piratsoftware: 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, maj 2012; "*Security update available for Adobe Flash Player*"; www.adobe.com/support/security/bulletins/apsb12-09.html

Adobe, juni 2012; "*Security update available for Adobe Flash Player*"; www.adobe.com/support/security/bulletins/apsb12-14.html

Apple, 2012; "*About the security content of OS X Lion v10.7.4 and Security Update 2012-002*"; support.apple.com/kb/HT5281

Apple, 2012; "*About the security content of Safari 5.1.7*"; support.apple.com/kb/HT5282

Apple, 2012; "*About the security content of Java for OS X Lion 2012-002 and Java for Mac OS X 10.6 Update 7*". support.apple.com/kb/HT5228

Brancheforeningen for IT-hostingvirksomheder i Danmark (BFIH), 2012; "*Om BFIH*"; www.bfih.dk/om-bfih.aspx

Centrum Wiskunde & Informatica, 2012; "*CWI cryptanalyst discovers new cryptographic attack variant in Flame spy malware*"; cwi.nl/news/2012/cwi-cryptanalist-discovers-new-cryptographic-attack-variant-in-flame-spy-malware

Cisco, 2012; "*Multiple Vulnerabilities in Cisco AnyConnect Secure Mobility Client*"; tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ac

Computerworld, 2012; "*Apple patches Mac Java zero-day bug*"; www.computerworld.com/s/article/9225837/Apple_patches_Mac_Java_zero_day_bug

Datatilsynet, 2012; "*Behandling af personoplysninger i cloud-løsningen Office 365*"; www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/behandling-af-personoplysninger-i-cloud-loesningen-office-365/

Digitaliseringsstyrelsen, 2011; "*Cloud computing og de juridiske rammer*"; digitaliser.dk/resource/2274097/artefact/Cloud+computing+og+de+juridiske+rammer.pdf

DK•CERT, 2011; "*DK•CERT Sårbarhedsdatabase*"; http://sdb.cert.dk/login.php

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

F-secure, 2012; "*Mobile Threat Report Q1 2012*"; www.f-secure.com/weblog/archives/MobileThreatReport_Q1_2012.pdf

Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Operativsystemer*"; www.fdim.dk/Statistik/teknik/operativsystemer

Google, 2012; "*Google Apps receives ISO 27001 certification*"; googleenterprise.blogspot.dk/2012/05/google-apps-receives-iso-27001.html

Google online security blog, 2012; "*Safe browsing - protecting web users for 5 years and counting*"; googleonlinesecurity.blogspot.dk/2012/06/safe-browsing-protecting-web-users-for.html

Google, 2012; "*Google Chrome releases*"; googlechromereleases.blogspot.dk/

Govcert, 2012; "*Angreb på Erhvervs- og Væksministeriet*"; www.govcert.dk/news/19

H-online, 2012; "*Russian AV company claims 600,000 Macs infected by Flashback – Update*"; www.h-online.com/security/news/item/Russian-AV-company-claims-600-000-Macs-infected-by-Flashback-Update-1517180.html

Information, 2012; "*Størstedelen af internet-logningen kan sløjfes*"; www.information.dk/301785

Kaspersky lab, 2012; "*Back to Stuxnet: the missing link*"; securelist.com/en/blog/208193568/Back_to_Stuxnet_the_missing_link

LinkedIn, 2012; "*An update on taking steps to protect our members*"; blog.linkedin.com/2012/06/09/an-update-on-taking-steps-to-protect-our-members/

London 2012, 2012; "*Stay safe online*"; www.london2012.com/stay-safe-online/

Mcafee, 2012; "*Dissecting Operation High Roller*"; www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

Microsoft, 2012; "*Microsoft releases Security Advisory 2718704*"; blogs.technet.com/b/msrc/archive/2012/06/03/microsoft-releases-security-advisory-2718704.aspx

Microsoft, 2012; "*Microsoft security bulletin summary for april 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-apr

Microsoft, 2012; "*Microsoft security bulletin summary for june 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-jun

Microsoft, 2012; "*Microsoft security bulletin summary for may 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-may

Mozilla, 2012; "*Security Advisories for Firefox*"; www.mozilla.org/security/known-vulnerabilities/firefox.html

New York Times, 2012; "*Facing cyberattack, Iranian officials disconnect some oil terminals from internet*"; nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html

Nvd.nist.gov, 2011; "*CVE and CCE statistics query page*"; web.nvd.nist.gov/view/vuln/statistics

Oracle, 2012; "*April 2012 critical patch update released*"; blogs.oracle.com/security/entry/april_2012_critical_patch_update

Oracle, 2012; "*Oracle critical patch update advisory - april 2012*"; www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html

Oracle, 2012; "*Oracle Java SE critical patch update advisory - june 2012*"; www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.html

Retsinformation, 2012; "*Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenlo-*

ven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige"; www.retsinformation.dk/Forms/R0710.aspx?id=142399

Secunia, 2012; "*Secunia yearly report 2011*"; secunia.com/?action=fetch&filename=secunia_yearly_report_2011.pdf

Securelist, 2012; "*Spam report: April 2012*"; www.securelist.com/en/analysis/204792230/Spam_Report_April_2012

Sophos, 2012; "*IE remote code execution vulnerability being actively exploited in the wild*"; nakedsecurity.sophos.com/2012/06/19/ie-remote-code-execution-vulnerability-being-actively-exploited-in-the-wild/

Sophos, 2012; "*LinkedIn confirms hack, over 60% of stolen passwords already cracked*"; nakedsecurity.sophos.com/2012/06/06/linkedin-confirms-hack-over-60-of-stolen-passwords-already-cracked/

Sophos, 2012; "*Top 5 myths of safe web browsing*"; www.sophos.com/medialibrary/Gated%20Assets/white%20papers/sophosmythsforsafewebbrowsingwpna.pdf

Statens it, 2012; "*Erhvervs- og Vækstministeriet angrebet af hackere*"; www.statens-it.dk/omstatensit/nyheder/916.html

Surftown, 2009; "*Forretningsbetingelser*"; surftown.dk/forretningsbetingelser

Symantec; "*Intelligence reports*"; www.symanteccloud.com/da/dk/globalthreats/overview/r_mli_reports

Trendmicro, 2012; "*Cybercriminals race to the 2012 Olympics*"; blog.trendmicro.com/cybercriminals-race-to-the-2012-olympics/

Twitter, 2012; "*LinkedIn*"; twitter.com/LinkedIn/status/210356987576324096

Verizon, 2012; "*2012 data breach investigations report*"; www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Version2, 2012; "*Antallet af netbankindbrud stiger trods NemID*"; version2.dk/artikel/antallet-af-netbankindbrud-eksploderer-trods-nemid-46164

Version2, 2012; "*Google på vej til at fjerne EU-barriere for Google Apps til danske myndigheder*"; www.version2.dk/artikel/google-paa-vej-til-fjerne-eu-barriere-google-apps-til-danske-myndigheder-45835

Version2, 2012; "*GovCERT slår alarm: Advarer alle ministerier mod hackerangreb*"; www.version2.dk/artikel/govcert-advarer-alle-ministerier-mod-hackerangreb-45130

Version2, 2012; "*Hackerangreb lammer ministerium*"; www.version2.dk/artikel/breaking-hackerangreb-lammer-ministerium-45129

Version2, 2012; "*Hackerangreb plager ministerium på 4. døgn*"; www.version2.dk/artikel/hackerangreb-plager-ministerium-paa-4-doegn-45159

Version2, 2012; "*Massiv logning af danskernes internetbrug - men politiet bruger kun IP-adressen*"; www.version2.dk/artikel/massiv-logning-af-danskernes-internetbrug-men-politiet-bruger-kun-ip-adressen-45584

Version2, 2012; "*Mystiske hackerangreb hos Surftown-kunder: Hvordan kommer de ind?*"; www.version2.dk/artikel/boelge-af-mystiske-hackerangreb-hvordan-kommer-de-ind-46082

Version2, 2012; "*Password til Surftown-konto lækket af Anonymous - i marts*"; www.version2.dk/artikel/password-til-surftown-system-laekket-af-anonymous-i-marts-46223

Version2, 2012; "*Surftown afviser definitivt interne hackerangreb - men hæver sikkerheden*"; www.version2.dk/artikel/surftown-haever-sikkerheden-efter-kritik-men-afviser-interne-hackerangreb-46174

Washington Post, 2012; "*U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*"; www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

Wikipedia, 2012; "*Flame (malware)*"; en.wikipedia.org/wiki/Flame_%28malware%29.

Kontakt:

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

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